https://doi.org/10.31891/2307-5740-2026-352-9
УДК 351.86:004.056
JEL classification: H11, H56, D83, L86

ДАБІЖА Віра
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0000-0002-7000-4635
e-mail: verynchik@ukr.net

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

В сучасних умовах глобалізації та цифровізації суспільства інформаційна безпека стає критичною складовою національної безпеки, однак ефективне її забезпечення залишається проблематичним. Незважаючи на розвиток нормативно-правової бази та наявність організаційних механізмів, державне регулювання інформаційної безпеки стикається з рядом системних викликів, серед яких фрагментарність інституційного забезпечення, недостатня координація між органами влади та технологічне відставання від темпів розвитку інформаційних технологій. У статті здійснено комплексний аналіз сучасного стану державного регулювання інформаційної безпеки в умовах глобалізації, цифровізації суспільства та зростання кіберзагроз. Розкрито сутність поняття інформаційної безпеки як складової національної безпеки держави, визначено її ключові елементи та функції в контексті забезпечення суверенітету, стабільності суспільства та захисту інформаційного простору. Особливу увагу приділено виявленню основних проблем державного регулювання у цій сфері, серед яких: недосконаліть нормативно-правової бази, фрагментарність інституційного забезпечення, недостатній рівень координації між органами державної влади, а також відставання від темпів розвитку інформаційних технологій. Проаналізовано виклики, пов'язані з гібридними загрозами, інформаційними операціями та кібератаками, що особливо актуалізуються в умовах сучасних геополітичних трансформацій. У роботі обґрунтовано необхідність удосконалення механізмів державного регулювання інформаційної безпеки шляхом гармонізації національного законодавства з міжнародними стандартами, впровадження сучасних підходів до кіберзахисту, розвитку державно-приватного партнерства та підвищення рівня інформаційної культури суспільства. Окреслено перспективні напрями розвитку державної політики у сфері інформаційної безпеки, зокрема створення інтегрованих систем моніторингу загроз, посилення інституційної спроможності відповідних органів та активізацію міжнародного співробітництва. Зроблено висновок, що ефективне державне регулювання інформаційної безпеки є ключовою умовою забезпечення стійкості держави до сучасних викликів та загроз, а також важливим чинником сталого розвитку інформаційного суспільства.

Ключові слова: інформаційна безпека, державне регулювання, кібербезпека, інформаційні загрози, національна безпека, цифровізація, державна політика.

DABIZHA Vira
Open International University of Human Development "Ukraine"

STATE REGULATION OF INFORMATION SECURITY: PROBLEMS AND PROSPECTS FOR DEVELOPMENT

In today's conditions of globalization and digitalization of society, information security is becoming a critical component of national security, but its effective provision remains problematic. Despite the development of the regulatory framework and the availability of organizational mechanisms, state regulation of information security faces a number of systemic challenges, including fragmentation of institutional support, insufficient coordination between government agencies, and technological lag behind the pace of information technology development. The article provides a comprehensive analysis of the current state of state regulation of information activities in the context of globalization, digitalization of society and the growth of cyber security threats. The essence of the concept of information security as a component of national security of the state is revealed, its key elements and functions are identified in the context of ensuring sovereignty, stability of society and protection of the information space. Particular attention is paid to identifying the main problems of state regulation in this area, including: imperfection of the regulatory framework, fragmentation of institutional support, insufficient level of coordination between state authorities, as well as lagging behind the pace of development of information technologies. The challenges associated with hybrid threats, information operations and cyberattacks, which are especially relevant in the context of modern geopolitical transformations, are analyzed. The paper substantiates the need for security improvement of mechanisms for regulating the state information system by harmonizing national legislation with international standards, implementing modern approaches to cyber security, developing public-private partnerships and increasing the level of information culture of society. Promising directions for the development of state policy in the field of information security are outlined, in particular, the creation of integrated threat monitoring systems, strengthening the institutional capacity of relevant bodies and activating international cooperation. It is concluded that effective state regulation of information security is a key condition for ensuring the state's resilience to modern challenges and threats, as well as an important factor in the sustainable development of the information society.

Keywords: information security, state regulation, cybersecurity, information threats, national security, digitalization, state policy.

Стаття надійшла до редакції / Received 22.02.2026
Прийнята до друку / Accepted 30.03.2026
Опубліковано / Published 31.03.2026

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

У сучасних умовах стрімкої цифровізації, розвитку інформаційно-комунікаційних технологій та загострення глобальних безпекових викликів питання забезпечення інформаційної безпеки набуває особливої актуальності. Інформаційний простір стає ключовою ареною впливу на суспільні процеси, політичну стабільність і національний суверенітет держав, що зумовлює необхідність ефективного державного регулювання у цій сфері.

Водночас чинна система державного регулювання інформаційної безпеки характеризується наявністю низки системних проблем. Серед них — недостатня узгодженість нормативно-правової бази з динамікою розвитку цифрових технологій, фрагментарність інституційного забезпечення, дублювання функцій органів державної влади, а також обмежена ефективність механізмів координації між ними. Додатковим викликом виступає зростання масштабів кіберзагроз, поширення дезінформації, використання інформаційних операцій як інструменту гібридної війни, що суттєво ускладнює забезпечення стійкості держави. Особливої гостроти ця проблема набуває в умовах необхідності інтеграції до міжнародного безпекового та інформаційного простору, що потребує гармонізації національного законодавства з міжнародними стандартами, а також впровадження сучасних підходів до управління ризиками у сфері інформаційної безпеки.

Таким чином, існує об'єктивна потреба у переосмисленні підходів до державного регулювання інформаційної безпеки, визначенні його ключових проблем та обґрунтуванні перспективних напрямів удосконалення відповідних механізмів. Це зумовлює актуальність даного дослідження та визначає його наукову і практичну значущість.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз наукових досліджень і публікацій у сфері управління інформаційною безпекою свідчить про зростання уваги до цієї проблематики з боку наукової та практичної спільноти. У працях [1–3] основний акцент зроблено на ролі державного управління у забезпеченні інформаційної безпеки, де автори розглядають інституційні механізми, функції держави та необхідність удосконалення системи регулювання. Дослідження [4–6] присвячені аналізу сучасних кіберзагроз та їх еволюції, підкреслюючи потребу адаптації державної політики до динамічних змін інформаційного середовища.

У роботах [7–8] значна увага приділяється питанням законодавчого забезпечення та інституційних реформ, спрямованих на підвищення ефективності державного регулювання у сфері інформаційної безпеки. Автори наголошують на необхідності гармонізації національного законодавства з міжнародними стандартами та розвитку відповідних державних інституцій. Дослідження [9-10] акцентують увагу на важливості міжнародного співробітництва як ключового чинника протидії глобальним кіберзагрозам, а також на ролі міждержавної координації у формуванні ефективних механізмів безпеки.

Разом з тим, у наведених дослідженнях інформаційна безпека розглядається як комплексна система, що потребує інтеграції управлінських, технологічних та соціальних складових. Водночас наявні наукові напрацювання виявляють певні прогалини, що зумовлює необхідність подальших досліджень, спрямованих на розроблення комплексних стратегій державного регулювання інформаційної безпеки в умовах сучасних викликів.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на значну кількість наукових праць, присвячених питанням державного регулювання інформаційної безпеки, низка важливих аспектів залишається недостатньо дослідженою. Передусім відсутній єдиний узгоджений підхід до формування комплексної системи державного управління інформаційною безпекою, яка б інтегрувала правові, організаційні, технологічні та соціальні складові. Існуючі дослідження здебільшого розглядають окремі елементи цієї системи, що ускладнює формування цілісного механізму її функціонування.

Недостатньо опрацьованими залишаються питання адаптації державного регулювання до динамічних змін кіберсередовища та зростання гібридних загроз, що потребує розроблення гнучких і проактивних управлінських інструментів. Окремої уваги потребує проблема координації між державними органами, приватним сектором та громадянським суспільством у сфері забезпечення інформаційної безпеки, що наразі не має належного теоретичного та практичного обґрунтування.

Крім того, недостатньо дослідженими є механізми оцінювання ефективності державної політики у сфері інформаційної безпеки, зокрема відсутні універсальні критерії та показники, які б дозволяли здійснювати комплексний моніторинг рівня захищеності інформаційного простору. Потребують подальшого вивчення також питання впровадження інноваційних технологій та розвитку кадрового потенціалу як складових підвищення ефективності державного регулювання.

Таким чином, необхідність подальшого наукового опрацювання зазначених проблем зумовлює актуальність дослідження та визначає його спрямованість на розроблення комплексних підходів до вдосконалення державного регулювання інформаційної безпеки в сучасних умовах.

ФОРМУЛЮВАННЯ МЕТИ СТАТТІ

Метою статті є комплексне дослідження теоретичних та практичних засад державного регулювання інформаційної безпеки, виявлення ключових проблем функціонування відповідної системи в сучасних умовах, а також обґрунтування перспективних напрямів її вдосконалення з урахуванням сучасних викликів, пов'язаних із цифровізацією, зростанням кіберзагроз і необхідністю гармонізації з міжнародними стандартами у сфері безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У сучасному світі інформація дедалі більше набуває статусу стратегічного ресурсу, який визначає не лише рівень розвитку держави та її економічну конкурентоспроможність, а й соціально-політичну стабільність, ефективність управління та здатність протидіяти зовнішнім і внутрішнім загрозам. Цифровізація суспільства, поширення новітніх інформаційних технологій та зростання обсягів даних призводять до того, що інформаційний простір стає ключовим елементом національної безпеки. Водночас динамічне поширення кібератак, гібридних загроз і інформаційних операцій створює додаткові ризики для критичної інфраструктури держави, державних установ, економіки та суспільної свідомості.

В умовах таких трансформацій ефективне державне регулювання інформаційної безпеки набуває особливої актуальності, оскільки забезпечує комплексний захист національних інтересів, контроль за обігом та захистом інформаційних ресурсів, а також підтримує стійкість суспільства до дезінформаційних впливів. Воно передбачає не лише формування нормативно-правових основ і технологічних механізмів захисту, а й координацію діяльності державних органів, взаємодію з приватним сектором і міжнародними партнерами, підвищення інформаційної грамотності громадян. Усе це робить державне регулювання інформаційної безпеки ключовим чинником розвитку інформаційного суспільства та забезпечення стратегічної безпеки держави у глобальному цифровому середовищі [1].

Сутність поняття інформаційної безпеки формується на перетині безпекових, інформаційних і управлінських підходів і відображає стан захищеності особи, суспільства та держави в інформаційній сфері від реальних і потенційних загроз. У сучасних умовах це поняття виходить за межі суто технічного захисту інформації і охоплює ширший спектр явищ — від кіберзахисту до протидії дезінформації та забезпечення інформаційного суверенітету.

У науковій літературі сформувалося кілька основних підходів до трактування інформаційної безпеки:

1. Техніко-технологічний підхід - зосереджується на захисті інформації та інформаційних систем від несанкціонованого доступу, втрати чи пошкодження. Основу становлять принципи конфіденційності, цілісності та доступності (CIA-тріада). У цьому контексті, наприклад, міжнародний стандарт ISO/IEC 27000 визначає інформаційну безпеку як «збереження конфіденційності, цілісності та доступності інформації».

2. Правовий підхід - розглядає інформаційну безпеку як стан врегульованості суспільних відносин у сфері створення, поширення та використання інформації. Так, у Законі України «Про основні засади забезпечення кібербезпеки України» інформаційна безпека пов'язується із захищеністю життєво важливих інтересів людини, суспільства і держави в інформаційній сфері.

3. Соціально-політичний підхід - трактує інформаційну безпеку як захист суспільства і держави від деструктивного інформаційного впливу. Український дослідник Г. Почепцов визначає інформаційну безпеку як стан захищеності інформаційного простору від негативних інформаційно-психологічних впливів, що можуть змінювати поведінку суспільства та підривати державність.

4. Системний (комплексний) підхід - інтегрує технічні, правові, організаційні та соціальні аспекти. Наприклад, український науковець В. Ліпкан розглядає інформаційну безпеку як складову національної безпеки, що забезпечує захист національних інтересів в інформаційній сфері через систему державного управління та відповідних інституцій.

6. Ризик-орієнтований підхід (зарубіжна практика) - представлений у працях західних дослідників, зокрема Eugene Spafford, який трактує інформаційну безпеку як процес управління ризиками, пов'язаними з використанням інформаційних систем, з метою мінімізації загроз і забезпечення безперервності функціонування [2].

Узагальнюючи позиції вітчизняних і зарубіжних дослідників, доцільно сформулювати таке визначення «інформаційної безпеки» — це комплексний стан захищеності інформаційного простору, інформаційних ресурсів, інфраструктури та суспільної свідомості, за якого забезпечується стійкість до внутрішніх і зовнішніх загроз, гарантується реалізація національних інтересів, прав і свобод людини, а також підтримується суверенітет і стабільний розвиток держави в умовах цифрового середовища.

Таким чином, різноманіття підходів і наукових трактувань свідчить про багатовимірність поняття інформаційної безпеки, що охоплює як технічні аспекти захисту інформації, так і ширший соціально-політичний та управлінський контекст її забезпечення.

Доцільно зазначити, що інформаційна безпека як складова національної безпеки, безпосередньо пов'язана із захистом державного суверенітету, територіальної цілісності та конституційного ладу. В умовах гібридних загроз інформаційний простір стає інструментом впливу на політичні процеси, громадську думку та соціальну стабільність, що зумовлює необхідність системного підходу до його регулювання та захисту.

Ключовими елементами інформаційної безпеки є багаторівнева система складових, взаємодія яких забезпечує захист інформаційного простору та стійкість держави до кібер- та інформаційних загроз:

- інформаційні ресурси включають дані, знання та інформаційні продукти, які становлять стратегічну основу діяльності держави, бізнесу та громадянського суспільства. Забезпечення їхньої цілісності, конфіденційності та доступності є критично важливим для стабільності державних систем і прийняття ефективних управлінських рішень;
- інформаційна інфраструктура охоплює телекомунікаційні мережі, інформаційні системи, бази даних та обчислювальні ресурси. Її надійність і безпека визначають спроможність держави забезпечувати безперервність роботи критичних секторів економіки, оборони, енергетики та соціальної сфери;
- суб'єкти забезпечення безпеки включають органи державної влади, приватний сектор та громадянське суспільство. Їхня взаємодія, координація дій і розподіл відповідальності дозволяють створити ефективну систему захисту, здатну оперативно реагувати на сучасні загрози та забезпечувати контроль за інформаційними потоками.
- механізми правового регулювання охоплюють нормативно-правову базу, стандарти та політики, які визначають правила обігу інформації, порядок реагування на загрози та відповідальність за порушення. Гармонізація національних норм із міжнародними стандартами забезпечує інтеграцію в глобальну систему кібербезпеки та підвищує ефективність правового захисту.
- система кіберзахисту включає технічні та програмні засоби, що забезпечують захист інформації від несанкціонованого доступу, втрати, модифікації чи пошкодження. Використання сучасних технологій шифрування, систем моніторингу, антивірусного програмного забезпечення та методів штучного інтелекту дозволяє своєчасно виявляти загрози і мінімізувати їхній негативний вплив.
- інформаційна культура суспільства визначає рівень обізнаності громадян, критичне мислення та здатність протидіяти дезінформації. Підвищення інформаційної грамотності населення сприяє формуванню стійкого інформаційного середовища, зменшенню ризиків маніпуляцій і підвищенню ефективності державних і приватних заходів із захисту інформаційного простору [3].

Таким чином, ключові елементи інформаційної безпеки утворюють комплексну систему, де кожен елемент взаємопов'язаний із іншими і виконує критично важливі функції для забезпечення національного суверенітету, стабільності суспільства та безпеки держави в умовах сучасних технологічних і геополітичних викликів.

Визначені ключові елементи інформаційної безпеки формують цілісну систему, функціонування якої забезпечує належний рівень захищеності інформаційного простору держави. Водночас ефективність цієї системи проявляється не лише через наявність її структурних компонентів, а й через реалізацію відповідних функцій, які відображають основні напрями впливу та механізми забезпечення інформаційної безпеки.

У цьому контексті логічним є перехід до розгляду функціонального призначення інформаційної безпеки, що дозволяє глибше зрозуміти її роль у забезпеченні суверенітету держави, стабільності суспільства та захисту інформаційного простору (табл. 1)

Аналіз функцій інформаційної безпеки свідчить, що їх ефективна реалізація потребує комплексного підходу, який поєднує технічні, правові, організаційні та соціально-політичні інструменти. Захисна, превентивна, регуляторна, стабілізаційна та комунікаційна функції взаємопов'язані та доповнюють одна одну, забезпечуючи цілісність, стійкість та надійність інформаційного простору держави. Такий системний підхід дозволяє не лише протидіяти сучасним інформаційним загрозам, а й підтримувати національний суверенітет, соціальну стабільність і довіру громадян до державних інститутів.

Розглянуті ключові елементи та функції інформаційної безпеки дозволяють усвідомити, що її ефективність значною мірою залежить від організаційно-правових механізмів та здатності держави координувати дії всіх зацікавлених суб'єктів. Незважаючи на наявність нормативних документів, технологічних рішень та стратегічних підходів, сучасне державне регулювання інформаційної безпеки стикається з низкою системних перешкод, що обмежують його дієвість. Складність цих перешкод полягає в тому, що вони одночасно охоплюють правову, інституційну, технічну та координаційну сфери, створюючи середовище підвищеної вразливості для критично важливих інформаційних ресурсів. Саме тому для формування ефективної державної політики у сфері інформаційної безпеки необхідно чітко визначити та проаналізувати основні проблеми, що сьогодні стримують розвиток системи захисту інформаційного простору та забезпечення національного суверенітету [5].

Далі виділяються головні проблеми державного регулювання у цій сфері, серед яких: недосконаліть нормативно-правової бази, фрагментарність інституційного забезпечення, недостатній рівень координації між органами державної влади, а також відставання від темпів розвитку інформаційних технологій:

1. Недосконаліть нормативно-правової бази - багато законодавчих актів та підзаконних нормативних документів не враховують швидкі темпи розвитку інформаційних технологій та нові форми кіберзагроз. Це

створює прогалини у правовому регулюванні, що ускладнює захист критичної інформаційної інфраструктури та забезпечення інформаційного суверенітету держави.

2. Фрагментарність інституційного забезпечення - система органів державної влади, відповідальних за інформаційну безпеку, часто є розрізненою, з дублюванням функцій та відсутністю єдиної координаційної структури. Така фрагментація знижує ефективність управління загрозами та уповільнює прийняття оперативних рішень.

3. Недостатній рівень координації між органами державної влади - відсутність чітких механізмів взаємодії між різними державними структурами — оборонними, правоохоронними, регуляторними та аналітичними — призводить до уповільнення реагування на інформаційні загрози та обмежує обмін даними про кіберінциденти.

4. Відставання від темпів розвитку інформаційних технологій - технологічне відставання державних систем захисту інформації від сучасних IT-рішень та кібератак призводить до підвищеної вразливості державних і критично важливих інфраструктур. Це зокрема проявляється у використанні застарілих протоколів безпеки, недостатньому впровадженні сучасних засобів криптографічного захисту та автоматизованого моніторингу загроз [6].

Таблиця 1

Функції інформаційної безпеки: сутність, механізми реалізації та практична значущість

№	Функції інформаційної безпеки	Сутність та завдання	Основні механізми реалізації	Приклади застосування	Науково-практична значущість
1	Захисна функція	Охорона інформаційних ресурсів і систем від несанкціонованого доступу, витоку, модифікації або знищення інформації	Криптографічні засоби, системи контролю доступу, антивірусний захист, резервне копіювання	Захист державних баз даних, фінансових систем, критичної інфраструктури	Забезпечує конфіденційність, цілісність та доступність інформації, є основою кібербезпеки
2	Превентивна функція	Виявлення, прогнозування та запобігання потенційним інформаційним загрозам та ризикам	Моніторинг інформаційних потоків, аналіз загроз, оцінка вразливостей, раннє попередження про кібератаки	Системи раннього виявлення кібератак, аналіз соціальних мереж на дезінформацію	Зменшує ризики реалізації загроз, дозволяє оперативно реагувати на потенційні кризи
3	Регуляторна функція	Формування та реалізація державної політики і правових норм у сфері інформаційної безпеки	Законодавство, стандарти ISO/IEC, державні нормативні документи, внутрішні політики організацій	Закон України «Про основні засади забезпечення кібербезпеки», стандарти ISO/IEC 27001	Гарантує правову визначеність, координацію між державними органами та суб'єктами інформаційного середовища
4	Стабілізаційна функція	Підтримка суспільної злагоди, протидія маніпуляціям свідомістю та поширенню дезінформації	Моніторинг медіапростору, аналітика контенту, інформаційні кампанії, освітні програми	Запобігання поширенню фейкових новин під час виборчих кампаній	Забезпечує соціальну стійкість, підтримує довіру до державних інститутів
5	Комунікаційна функція	Забезпечення безпечного та надійного обміну інформацією між суб'єктами суспільних відносин	Захищені канали зв'язку, протоколи шифрування, системи автентифікації	Використання VPN, шифрування електронної пошти, безпечні державні портали	Гарантує інтеграцію та взаємодію суб'єктів, мінімізує ризики витоку та маніпуляцій даними

Джерело: сформовано автором на основі даних [4]

Сукупність цих проблем ускладнює формування ефективної державної політики в сфері інформаційної безпеки та знижує здатність держави оперативно реагувати на сучасні кіберзагрози. Вирішення зазначених проблем потребує комплексного підходу, що поєднує законодавче удосконалення, розвиток інституційної спроможності, модернізацію технічних систем захисту та підвищення рівня координації між усіма зацікавленими сторонами.

Аналіз основних проблем державного регулювання інформаційної безпеки свідчить, що традиційних заходів захисту недостатньо для ефективного протистояння сучасним викликам. Зокрема, в умовах геополітичних трансформацій дедалі більшого значення набувають гібридні загрози, інформаційні операції та кібератаки, які поєднують технічні, психологічні та соціально-політичні інструменти впливу. Вони здатні одночасно порушувати роботу критичної інфраструктури, впливати на суспільну свідомість та підривати довіру до державних інститутів, що вимагає від держави нових комплексних підходів до регулювання та захисту інформаційного простору (табл. 2).

Сучасні виклики у сфері інформаційної безпеки мають комплексний характер і виходять за рамки класичних технічних загроз. Гібридні загрози, інформаційні операції та кібератаки поєднують технічні, соціально-психологічні та політичні інструменти впливу, що значно ускладнює роботу державних органів і підвищує ризики для національної безпеки. Для ефективного протидіяння цим загрозам необхідне інтегроване

управління, яке поєднує правове регулювання, технологічні рішення, моніторинг інформаційного простору та підвищення інформаційної культури суспільства.

Таблиця 2

Основні виклики сучасних гібридних загроз та інформаційних операцій

№	Виклик	Сутність та характеристики	Механізми реалізації/приклади	Наслідки для держави та суспільства
1	Гібридні загрози	Поєднання військових, економічних, інформаційних та психологічних методів впливу на державу	Кібератаки на енергетичну або фінансову інфраструктуру, пропагандистські кампанії, економічний тиск	Порушення стабільності критичної інфраструктури, підрив національної безпеки, дестабілізація економіки
2	Інформаційні операції	Цілеспрямоване формування або маніпулювання інформаційним простором з метою зміни поведінки суспільства або впливу на політичні рішення	Поширення фейкових новин, бот-мережі у соціальних мережах, пропагандистські матеріали	Дезінформація громадян, зростання соціальної напруженості, підрив довіри до державних інститутів
3	Кібератаки	Несанкціоноване втручання у роботу інформаційних систем з метою викрадення, модифікації або знищення даних	Хакерські атаки, шкідливе ПЗ, DDoS-атаки, кібершпигунство	Витік конфіденційної інформації, параліч державних систем, економічні збитки, загроза національному суверенітету
4	Комплексні загрози (гібрид + кібер)	Синергетичний ефект одночасного застосування кількох видів атак та маніпуляцій	Кіберінциденти на фоні дезінформаційних кампаній у соцмережах і ЗМІ	Масштабне порушення національної безпеки, дестабілізація політичної системи, зниження соціальної стійкості

Джерело: сформовано автором на основі даних [7]

Ураховуючи комплексність сучасних загроз та системні проблеми державного регулювання інформаційної безпеки, стає очевидним, що існуючі механізми захисту є недостатньо ефективними. Традиційні підходи не завжди здатні адекватно реагувати на динамічні гібридні загрози, масштабні кібератаки та інформаційні операції, які поєднують технічні, психологічні та соціально-політичні чинники впливу. Саме тому актуальним є питання удосконалення державного регулювання у цій сфері. Воно включає не лише модернізацію нормативно-правової бази та технічних систем кіберзахисту, а й інтеграцію міжнародних стандартів, розвиток державно-приватного партнерства та підвищення рівня інформаційної культури суспільства. Такий комплексний підхід дозволяє забезпечити не лише оперативний захист інформаційного простору, а й формування стійкої системи, здатної протистояти сучасним викликам і гарантувати національну безпеку.

Враховуючи зазначене, необхідність удосконалення механізмів державного регулювання інформаційної безпеки обумовлена комплексністю сучасних загроз, їхньою динамічністю та міждисциплінарним характером. Сучасні гібридні загрози, інформаційні операції та кібератаки демонструють, що існуючі правові, інституційні та технологічні механізми часто не відповідають вимогам часу, що створює ризики для національного суверенітету, критичної інфраструктури та суспільної стабільності [8].

Гармонізація національного законодавства з міжнародними стандартами є ключовим напрямом удосконалення, оскільки сучасна інформаційна безпека не має державних кордонів. Використання міжнародних норм, таких як стандарти ISO/IEC 27001 щодо управління інформаційною безпекою, дозволяє створити єдині критерії захисту даних, забезпечити сумісність національних систем з глобальними практиками та підвищити довіру міжнародних партнерів.

Впровадження сучасних підходів до кіберзахисту включає використання автоматизованих систем моніторингу загроз, штучного інтелекту для аналізу аномалій у мережевому трафіку, сучасних протоколів шифрування та багаторівневих систем доступу. Це дозволяє швидко виявляти, локалізувати та нейтралізувати кіберзагрози, зменшуючи потенційні втрати та збої у роботі критичних інформаційних систем.

Розвиток державно-приватного партнерства є необхідним через те, що значна частина критичної інфраструктури і високотехнологічних ресурсів належить приватним компаніям. Спільні програми обміну інформацією про загрози, координація реагування на кіберінциденти та спільні навчальні проєкти дозволяють підвищити ефективність заходів з інформаційного захисту та зменшити часові та ресурсні витрати держави. Підвищення рівня інформаційної культури суспільства є стратегічним компонентом. Обізнані громадяни та працівники державних установ, які критично оцінюють інформаційні потоки та дотримуються правил кібергігієни, значно знижують ризики успішного впливу дезінформаційних кампаній та кібератак. Це створює умови для формування стійкого інформаційного середовища, у якому державні та приватні системи взаємодіють більш ефективно [9].

Удосконалення державного регулювання інформаційної безпеки шляхом інтеграції міжнародних стандартів, впровадження сучасних технологічних рішень, розвитку державно-приватного партнерства та підвищення інформаційної культури суспільства дозволяє формувати багаторівневу, стійку та адаптивну

систему захисту інформаційного простору. Це забезпечує збереження національних інтересів, зміцнює суверенітет держави та підвищує її здатність протистояти сучасним кібер- та інформаційним загрозам. Враховуючи сучасні виклики у сфері інформаційної безпеки, стає очевидним, що удосконалення державного регулювання потребує не лише оновлення законодавства та технологічної модернізації, а й стратегічного розвитку політики захисту інформаційного простору. Поступове ускладнення гібридних загроз, кібератак та інформаційних операцій вимагає створення більш інтегрованих, координаційно взаємопов'язаних механізмів.

Саме на цьому тлі визначаються перспективні напрями державної політики у сфері інформаційної безпеки, які передбачають комплексний підхід: впровадження інтегрованих систем моніторингу загроз, посилення інституційної спроможності відповідних органів та активізацію міжнародного співробітництва. Такий підхід забезпечує не лише оперативний захист критичних інформаційних ресурсів, а й формування стійкої, адаптивної системи, здатної протистояти сучасним кібер- і інформаційним загрозам, а також гарантувати довгострокову безпеку держави та суспільства [10].

Як підсумок, перспективні напрями розвитку державної політики у сфері інформаційної безпеки формуються з урахуванням сучасних викликів, динаміки технологічного розвитку та зростання масштабів кіберзагроз. Основна мета таких напрямів — забезпечити стійкий, інтегрований та ефективний механізм захисту національного інформаційного простору, здатний оперативно реагувати на загрози та запобігати їх негативним наслідкам:

1. Створення інтегрованих систем моніторингу загроз - впровадження комплексних систем моніторингу дозволяє здійснювати цілодобовий контроль за станом інформаційного простору, виявляти потенційні кіберзагрози та інформаційні атаки на ранніх стадіях. Інтеграція таких систем із національними та міжнародними базами даних загроз забезпечує обмін актуальною інформацією, дозволяє прогнозувати розвиток кризових ситуацій та координувати швидке реагування державних і приватних структур.

2. Посилення інституційної спроможності відповідних органів - розвиток кадрового, технічного та організаційного потенціалу державних органів, відповідальних за інформаційну безпеку, є критично важливим для забезпечення ефективного управління загрозами. Це передбачає створення чіткої структури повноважень, підвищення кваліфікації фахівців, впровадження сучасних технологічних рішень для аналізу загроз і координації дій між відомствами.

3. Активізація міжнародного співробітництва - у сучасних умовах інформаційні загрози не визнають державних кордонів, тому ефективний захист неможливий без взаємодії з міжнародними партнерами. Спільні навчальні програми, обмін даними про кіберзагрози, участь у міжнародних організаціях та стандартизаційних ініціативах сприяють підвищенню рівня безпеки, інтеграції національних систем з глобальними та розвитку найкращих практик захисту інформаційного простору.

Реалізація зазначених напрямів дозволяє створити багаторівневу систему державного регулювання інформаційної безпеки, яка поєднує технологічні, правові та організаційні заходи, це сприятиме не лише зниженню ризиків кібератак і інформаційних загроз, а й підвищенню здатності держави забезпечувати національний суверенітет, стабільність суспільства та довгостроковий розвиток інформаційного середовища.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Ефективне державне регулювання інформаційної безпеки є визначальним чинником забезпечення стійкості держави перед сучасними кібер- та інформаційними загрозами, а також гарантією захисту національних інтересів у цифровому середовищі. Воно вимагає комплексного підходу, який поєднує правове регулювання, сучасні технологічні рішення, координацію дій органів державної влади, розвиток державно-приватного партнерства та підвищення рівня інформаційної культури суспільства. Такий підхід дозволяє своєчасно виявляти і нейтралізувати загрози, ефективно протидіяти гібридним атакам, дезінформаційним кампаніям і кібератакам, що набувають особливої актуальності в умовах геополітичних трансформацій.

Крім того, системне управління інформаційною безпекою сприяє збереженню національного суверенітету, стабільності критичної інфраструктури та безпеки стратегічних інформаційних ресурсів. Воно також підвищує довіру громадян до державних інститутів, створює умови для прозорої та безпечної взаємодії між державою, бізнесом і суспільством, а отже, є важливим чинником формування стійкого і ефективного інформаційного середовища.

З огляду на це, удосконалення механізмів державного регулювання — включно з гармонізацією національного законодавства з міжнародними стандартами, впровадженням інтегрованих систем моніторингу загроз, модернізацією технологічних рішень, підвищенням інституційної спроможності відповідних органів та активізацією міжнародного співробітництва — стає стратегічною умовою розвитку інформаційного суспільства та забезпечення довгострокової національної безпеки. Ефективне управління інформаційною безпекою водночас формує платформу для сталого розвитку держави у цифровій економіці та глобальному інформаційному просторі.

Враховуючи зазначене, перспективи подальших досліджень у сфері державного регулювання інформаційної безпеки доцільно пов'язати з поглибленням наукового обґрунтування комплексних підходів до управління цією сферою в умовах зростання кібер- та інформаційних загроз, до того ж актуальним є

розроблення інтегрованих моделей державного регулювання, що поєднуватимуть правові, організаційні та технологічні інструменти забезпечення інформаційної безпеки з урахуванням динаміки цифрового середовища.

Література

1. Кондратенко В. М., Сокуренко О. А. Адміністративно-правові засади забезпечення інформаційної безпеки та доступу до публічної інформації в діяльності правоохоронних органів сектору національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Т. 2 No 89. С. 452-457.
2. Білко С. Інституційне забезпечення інформаційної безпеки України. Економіка і регіон. 2021. № 3(82). С. 36–41. URL: https://journals-nupp-edu-ua.translate.goog/eir/article/view/2361?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc
3. Мотлях О. Сучасна державна інформаційна політика України у сфері масмедіа. *Український інформаційний простір.* 2022. Вип. 10. С. 156–170.
4. Кобко Є.В., Кобко В.А. Актуальні проблеми реалізації державної політики у сфері забезпечення інформаційної безпеки України. *Право і Безпека.* 2021. № 2. С. 104–110.
5. Гетьманчук М., Зазуляк З. Інформаційна сфера - ключовий фактор гібридної агресії Росії проти України. *Соціальні комунікації: теорія і практика* 2019. № 5(1). С. 7–12. DOI: https://doi.org/10.23939/shv2019.01.007
6. Коваль Я.С., Дудецький Д.В. Удосконалення механізмів державного управління в умовах діджиталізації. *Державне управління: удосконалення та розвиток*. 2024. №6. DOI: https://doi.org/10.32702/2307-2156.2024.6.14
7. Глобенко С. Становлення й розвиток правового поля України щодо захисту інформаційного простору держави. *Науковий вісник: Державне управління*. 2023. № 2(14). С. 64–79.
8. Мазуренко Л. І. Інформаційна безпека в умовах російськоукраїнської війни: виклики та загрози. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології».* 2022. № 42. С. 50-57. https://doi.org/10.26565/2220-8089-2022-42-08
9. Горєлова В. Ю., Вихрист С. М. Правове забезпечення та перспективи розвитку державної політики у сфері інформаційної безпеки. *Legal Bulletin.* 2024. № 3(13). С. 79–85.
10. Бондарь О. В. Суб'єкти реалізації адміністративно-правового механізму доступу до публічної інформації. *Науковий вісник Ужгородського національного університету. Серія Право.* 2025. Вип. 89. Ч. 2. С. 360-365.

References

1. Kondratenko, V. M., Sokurenko, O. A. (2025), "Administrative and Legal Principles of Ensuring Information Security and Access to Public Information in the Activities of Law Enforcement Agencies of the National Security Sector", *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo,* vol. 2, no. 89, pp. 452–457.
2. Bilko, S. (2021), "Institutional Support of Information Security of Ukraine", *Ekonomika i rehion,* no. 3 (82), pp. 36–41. URL: https://journals-nupp-edu-ua.translate.goog/eir/article/view/2361.
3. Motliakh, O. (2022), "Modern State Information Policy of Ukraine in the Field of Mass Media", *Ukrainskyi informatsiinyi prostir,* issue 10, pp. 156–170.
4. Kobko, Ye. V., Kobko, V. A. (2021), "Current Problems of Implementation of State Policy in the Field of Information Security of Ukraine", *Pravo i Bezpeka,* no. 2, pp. 104–110.
5. Hetmanchuk, M., Zazuliak, Z. (2019), "Information Sphere as a Key Factor of Hybrid Aggression of Russia against Ukraine", *Sotsialni komunikatsii: teoriia i praktyka*, no. 5 (1), pp. 7–12. DOI : https://doi.org/10.23939/shv2019.01.007
6. Koval, Ya. S., Dudetskyi, D. V. (2024), "Improvement of Public Administration Mechanisms in the Conditions of Digitalization", *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, no. 6. DOI : https://doi.org/10.32702/2307-2156.2024.6.14
7. Hlubenko, S. (2023), "Formation and Development of the Legal Framework of Ukraine for the Protection of the State Information Space", *Naukovyi visnyk: Derzhavne upravlinnia,* no. 2 (14), pp. 64–79.
8. Mazurenko, L. I. (2022), "Information Security in the Conditions of the Russian-Ukrainian War: Challenges and Threats", *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
9. Horielova, V. Yu., Vykhryst, S. M. (2024), "Legal Support and Prospects for the Development of State Policy in the Field of Information Security", *Legal Bulletin,* no. 3 (13), pp. 79–85.
10. Bondar, O. V. (2025), "Subjects of Implementation of the Administrative and Legal Mechanism of Access to Public Information", *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo,* issue 89, part 2, pp. 360–365.