УДК 351.86:004.056
JEL Classification: H11, H56, L86, O33

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА СУЧАСНИХ ВОЄННИХ ЗАГРОЗ

СОРОКІВСЬКА Олена
Тернопільський національний технічний університет імені Івана Пулюя
https://orcid.org/0000-0001-8549-2910
e-mail: sorokivska_o@tntu.edu.ua

У статті досліджено теоретико-методологічні та практичні засади державного регулювання інформаційної безпеки в умовах розвитку інформаційного суспільства та сучасних воєнних загроз. Обґрунтовано, що повномасштабна військова агресія Російської Федерації проти України засвідчила необхідність переосмислення традиційних механізмів державного управління інформаційною сферою та формування комплексної моделі забезпечення інформаційної стійкості держави. Запропоновано концептуальні напрями модернізації системи державного регулювання інформаційної безпеки, які передбачають формування інтегрованої моделі управління інформаційними ризиками, розвиток цифрової стійкості держави, удосконалення механізмів стратегічних комунікацій, впровадження сучасних технологій штучного інтелекту для аналізу інформаційного середовища, посилення захисту державних інформаційних ресурсів, критичної цифрової інфраструктури та підвищення ефективності міжвідомчого інформаційного обміну.

Ключові слова: державне регулювання, стратегічні комунікації, інформаційна безпека, інформаційне суспільство, воєнні загрози, ризики, кібербезпека.

https://doi.org/10.31891/mdes/2026-21-14

Стаття надійшла до редакції / Received 02.07.2026
Прийнята до друку / Accepted 20.08.2026
Опубліковано / Published 27.08.2026

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

Стрімкий розвиток інформаційного суспільства, масштабна цифровізація публічного управління, широке впровадження інформаційно-комунікаційних технологій та інтеграція цифрових сервісів у діяльність органів державної влади суттєво трансформують механізми забезпечення національної безпеки. Одночасно цифрова трансформація створює нові виклики, пов'язані зі зростанням кіберзагроз, поширенням дезінформації, інформаційно-психологічних операцій, маніпулятивного впливу на суспільну свідомість, несанкціонованим доступом до інформаційних ресурсів та порушенням функціонування критичної інформаційної інфраструктури.

Особливої актуальності зазначені проблеми набули в умовах повномасштабної військової агресії проти України, коли інформаційний простір став одним із ключових театрів сучасного протиборства. Використання інформаційних операцій, кібератак, цифрових платформ, соціальних мереж і технологій штучного інтелекту як інструментів ведення гібридної війни істотно ускладнює реалізацію державної політики у сфері інформаційної безпеки та потребує адаптації існуючих механізмів державного регулювання до нових безпекових умов.

Попри значний розвиток нормативно-правового забезпечення інформаційної безпеки та цифрової трансформації, залишаються актуальними питання підвищення ефективності інституційного забезпечення, міжвідомчої координації, управління інформаційними ризиками, розвитку стратегічних комунікацій, забезпечення інформаційної стійкості держави та гармонізації національної системи державного регулювання із сучасними європейськими стандартами. У зв'язку з цим виникає об'єктивна потреба в комплексному дослідженні теоретичних засад, сучасного стану та перспектив удосконалення державного регулювання інформаційної безпеки в умовах розвитку інформаційного суспільства та сучасних воєнних загроз.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Теоретико-методологічні засади формування інформаційного суспільства, цифрової трансформації та розвитку інформаційної економіки знайшли відображення у працях зарубіжних учених, зокрема Д. Белла [1], М. Кастельса [2], Е. Тоффлера [3], Ф. Вебстера [4], які обґрунтували закономірності переходу до інформаційного суспільства, визначили роль інформації та знань як

стратегічних ресурсів суспільного розвитку, а також окреслили вплив цифрових технологій на функціонування держави, економіки й соціальних інститутів.

Проблематику інформаційної безпеки, державної інформаційної політики, кібербезпеки та державного регулювання інформаційної сфери досліджували як зарубіжні, так і українські науковці. Значний внесок у розвиток теоретичних засад інформаційної безпеки зробили К. Шеннон [5], Б. Шнайєр [6], Ю. Бенклер [7], праці яких присвячені питанням захисту інформаційних систем, кібербезпеки та функціонування цифрового середовища. Серед українських учених вагомими є дослідження В. Ліпкана [8], О. Дзьобаня [9], В. Горбуліна [10], Г. Почепцова [11], В. Пилипчука [12], присвячені проблемам забезпечення інформаційної безпеки держави, розвитку стратегічних комунікацій, інформаційного суверенітету, протидії інформаційним загрозам та вдосконаленню державної політики у безпековій сфері.

Незважаючи на значну кількість наукових праць, недостатньо дослідженими залишаються питання модернізації організаційно-інституційних механізмів державного регулювання інформаційної безпеки, формування інтегрованої системи управління інформаційними ризиками, розвитку цифрової стійкості держави, а також використання технологій штучного інтелекту й прогнозної аналітики для забезпечення інформаційної безпеки в умовах сучасних воєнних загроз. Саме необхідність комплексного вирішення зазначених питань визначає актуальність і наукову доцільність цього дослідження.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Попри значний обсяг наукових праць, присвячених інформаційній безпеці, недостатньо дослідженими залишаються питання модернізації організаційно-інституційних механізмів державного регулювання. Потребують подальшого вивчення процеси формування інтегрованої системи управління інформаційними ризиками та розвитку цифрової стійкості держави. Окремої уваги вимагає практичне використання технологій штучного інтелекту й прогнозної аналітики в умовах сучасних воєнних загроз.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження теоретико-методологічних засад державного регулювання інформаційної безпеки в умовах розвитку інформаційного суспільства та сучасних воєнних загроз, аналіз сучасних викликів і тенденцій функціонування інформаційного простору, оцінювання ефективності існуючих механізмів державного регулювання та обґрунтування пріоритетних напрямів їх удосконалення для забезпечення інформаційної стійкості, захисту національних інтересів і зміцнення національної безпеки України.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Сучасний етап розвитку суспільства характеризується інтенсивною цифровою трансформацією всіх сфер суспільного життя, що зумовлює докорінні зміни у функціонуванні системи публічного управління та механізмах забезпечення національної безпеки. За таких умов державне регулювання інформаційної безпеки набуває стратегічного значення, оскільки від його ефективності залежить стійкість державних інституцій, захищеність інформаційного простору та здатність держави своєчасно реагувати на сучасні інформаційні й воєнні виклики.

Зазначені трансформаційні процеси обумовлюють переосмислення традиційних підходів до забезпечення національної безпеки, оскільки інформаційний простір дедалі більше перетворюється на стратегічну сферу реалізації державної політики та захисту національних інтересів. Стрімка цифровізація суспільних відносин, масштабне впровадження інформаційно-комунікаційних технологій, зростання обсягів цифрових даних, інтеграція штучного інтелекту у сферу публічного управління та активізація гібридних форм протиборства суттєво трансформують підходи до забезпечення національної безпеки. За таких умов безпекова політика вже не може обмежуватися традиційними інструментами захисту, а потребує комплексного державного регулювання інформаційної сфери, яке поєднує правові, організаційні, технологічні та інституційні механізми запобігання інформаційним і кібернетичним загрозам, зміцнення інформаційної стійкості держави та забезпечення безпечного функціонування цифрового середовища [1].

Розвиток інформаційного суспільства є одним із визначальних чинників трансформації сучасної системи публічного управління. Інтенсивне впровадження цифрових технологій змінює

характер взаємодії між державою, громадянами та бізнесом, сприяє автоматизації управлінських процесів, підвищенню відкритості влади та формуванню нових моделей надання публічних послуг. Водночас цифрова трансформація супроводжується появою нових викликів, пов'язаних із забезпеченням інформаційної безпеки, захистом персональних даних, кіберстійкістю державних інформаційних ресурсів та протидією інформаційним загрозам. Аналіз сучасних тенденцій дозволяє визначити основні напрями розвитку інформаційного суспільства, які безпосередньо впливають на механізми державного регулювання [2]:

1. Розширення цифрової взаємодії між державою, громадянами та бізнесом - однією з провідних тенденцій є перехід до цифрової моделі взаємодії, що забезпечує отримання адміністративних послуг, здійснення електронних комунікацій, подання документів та участь громадян у процесах державного управління через цифрові сервіси. Такий підхід підвищує доступність публічних послуг, скорочує адміністративні процедури та сприяє розвитку людиноцентричного врядування.

2. Розвиток електронного урядування та цифрового врядування - цифровізація діяльності органів державної влади супроводжується переходом від окремих електронних сервісів до інтегрованих систем цифрового врядування, що забезпечують автоматизацію управлінських процесів, електронний документообіг, міжвідомчу взаємодію та прийняття управлінських рішень на основі цифрових даних.

3. Поширення цифрових платформ як інструменту державного управління - важливою тенденцією є створення єдиних цифрових платформ, які забезпечують інтеграцію державних реєстрів, інформаційних систем та електронних сервісів. Використання платформенного підходу підвищує ефективність міжвідомчої взаємодії, мінімізує дублювання інформації та забезпечує безперервність надання публічних послуг.

4. Розвиток політики відкритих даних та підвищення прозорості діяльності органів влади - відкритість державних даних сприяє розвитку цифрової економіки, громадського контролю, підвищенню прозорості діяльності органів влади та створює передумови для розроблення нових цифрових сервісів. Водночас актуалізуються питання захисту конфіденційної інформації, інформаційного суверенітету та управління доступом до даних.

5. Активне впровадження хмарних технологій - перехід до хмарної інфраструктури забезпечує масштабованість державних інформаційних систем, підвищує їх доступність, безперервність функціонування та стійкість до кризових ситуацій. Особливої актуальності використання хмарних технологій набуло в умовах воєнного стану, коли виникла необхідність забезпечення збереження державних інформаційних ресурсів та безперервності функціонування цифрових сервісів.

6. Використання технологій великих даних (Big Data) - сучасне державне управління дедалі активніше використовує технології аналізу великих даних для прогнозування соціально-економічних процесів, оцінювання ризиків, моніторингу суспільних процесів та підтримки прийняття управлінських рішень. Це сприяє підвищенню обґрунтованості державної політики та оперативності реагування на внутрішні й зовнішні виклики.

7. Інтеграція технологій штучного інтелекту у сферу публічного управління - штучний інтелект поступово стає одним із ключових інструментів цифрової трансформації державного сектору. Його застосування охоплює автоматизацію адміністративних процедур, аналітичну підтримку управлінських рішень, прогнозування кризових ситуацій, виявлення інформаційних загроз, аналіз великих масивів даних та підвищення ефективності функціонування державних інституцій.

8. Посилення вимог до інформаційної та кібербезпеки цифрового середовища - розширення цифрового простору одночасно супроводжується збільшенням кількості кібератак, інформаційних операцій, витоків даних та інших цифрових ризиків. Це зумовлює необхідність розвитку комплексних систем захисту інформації, підвищення кіберстійкості критичної інформаційної інфраструктури, удосконалення механізмів державного регулювання та формування культури інформаційної безпеки.

Отже, сучасний розвиток інформаційного суспільства характеризується комплексною цифровою трансформацією публічного управління, що охоплює цифровізацію взаємодії між державою, громадянами та бізнесом, розвиток електронного врядування, цифрових платформ, відкритих даних, хмарних технологій, технологій великих даних і штучного інтелекту. Водночас розширення цифрового середовища супроводжується зростанням інформаційних і кібернетичних ризиків, що актуалізує необхідність удосконалення механізмів державного регулювання

інформаційної безпеки, розвитку цифрової стійкості та впровадження сучасних інструментів захисту національного інформаційного простору.

Розвиток інформаційного суспільства та масштабна цифровізація публічного управління суттєво розширили можливості використання цифрових технологій у діяльності органів державної влади, однак водночас значно підвищили їхню вразливість до сучасних інформаційних і кібернетичних загроз. Повномасштабна військова агресія Російської Федерації проти України засвідчила, що інформаційний простір став одним із ключових театрів сучасного протиборства, де інформаційні операції, кібератаки, дезінформація та психологічний вплив застосовуються поряд із традиційними військовими засобами [3]. За таких умов державне регулювання інформаційної безпеки набуває комплексного характеру та потребує постійної адаптації до нових викликів, що обумовлює необхідність оцінювання впливу сучасних воєнних загроз на функціонування системи державного регулювання інформаційної безпеки України (табл. 1).

Таблиця 1

Вплив сучасних воєнних загроз на систему державного регулювання інформаційної безпеки України

Сучасна воєнна загроза	**Вплив на систему державного регулювання**	**Необхідні напрями реагування**
Масштабні кібератаки на державні інформаційні ресурси	Посилення вимог до захисту державних інформаційних систем, критичної інформаційної інфраструктури та державних реєстрів	Розвиток комплексної системи кіберзахисту, резервування даних, безперервного моніторингу та реагування на інциденти
Дезінформація та інформаційно-психологічні операції	Зниження довіри до органів державної влади, маніпулювання громадською думкою, поширення панічних настроїв	Удосконалення стратегічних комунікацій, розвиток систем протидії дезінформації та підвищення медіаграмотності населення
Гібридні інформаційні впливи	Поєднання інформаційних, кібернетичних, політичних та економічних інструментів впливу на державу	Формування інтегрованої системи управління інформаційними ризиками та міжвідомчої координації
Використання штучного інтелекту в інформаційному протиборстві	Автоматизація створення дезінформаційного контенту, інформаційних кампаній та цифрових маніпуляцій	Розроблення механізмів державного регулювання використання технологій штучного інтелекту та впровадження систем автоматизованого виявлення загроз
Атаки на критичну інформаційну інфраструктуру	Ризик порушення функціонування державних сервісів, енергетики, транспорту, фінансової системи та зв'язку	Посилення захисту критичної інформаційної інфраструктури, розвиток кризового управління та резервних цифрових рішень
Інформаційний вплив через цифрові платформи та соціальні мережі	Швидке поширення маніпулятивної інформації, координація інформаційних кампаній	Удосконалення взаємодії держави з цифровими платформами, моніторинг інформаційного середовища та розвиток цифрової аналітики
Зростання кількості кіберінцидентів у державному секторі	Необхідність оперативного обміну інформацією між суб'єктами кібербезпеки	Розвиток єдиної системи обміну інформацією про кіберінциденти, посилення міжвідомчої взаємодії та координації

Джерело: сформовано автором на основі даних [4-6]

Проведений аналіз свідчить, що сучасні воєнні загрози суттєво трансформували підходи до державного регулювання інформаційної безпеки України. Якщо раніше пріоритетними завданнями були переважно захист інформаційних ресурсів і розвиток цифрових сервісів, то нині система державного регулювання орієнтується на забезпечення інформаційної стійкості держави, безперервності функціонування критичної інформаційної інфраструктури, протидію гібридним інформаційним впливам, розвиток стратегічних комунікацій та інтеграцію сучасних цифрових технологій у процеси управління безпекою, що зумовлює необхідність переходу до ризик-орієнтованої моделі державного регулювання, заснованої на міжвідомчій взаємодії, використанні штучного інтелекту, прогнозній аналітиці та гармонізації національної системи інформаційної безпеки з європейськими і євроатлантичними стандартами.

Разом з тим, повномасштабна військова агресія Російської Федерації проти України засвідчила необхідність переосмислення традиційних механізмів державного управління інформаційною сферою та формування комплексної моделі забезпечення інформаційної стійкості держави. Практика функціонування органів державної влади в умовах воєнного стану продемонструвала, що інформаційна безпека більше не може розглядатися виключно як напрям

захисту інформаційних ресурсів чи інформаційно-телекомунікаційних систем. Вона перетворилася на один із ключових елементів національної безпеки, який безпосередньо впливає на стійкість державного управління, безперервність функціонування критичної інформаційної інфраструктури, обороноздатність країни, суспільну довіру до державних інституцій та ефективність реалізації державної політики [7].

Сучасний воєнний конфлікт підтвердив, що поряд із традиційними бойовими діями активно використовуються інформаційно-психологічні операції, масштабні кібератаки, кампанії з дезінформації, цифрові маніпуляції, втручання у функціонування державних інформаційних систем, а також засоби штучного інтелекту для автоматизації інформаційного впливу. Такі загрози мають комплексний характер, швидко адаптуються до змін інформаційного середовища та здатні одночасно впливати на діяльність органів влади, об'єкти критичної інфраструктури, економіку, оборонний сектор і громадську свідомість.

За цих умов традиційна модель державного регулювання, орієнтована переважно на реагування на окремі інформаційні інциденти, поступово втрачає свою ефективність. Натомість виникає потреба у формуванні проактивної системи державного регулювання інформаційної безпеки, яка базується на ризик-орієнтованому управлінні, безперервному моніторингу інформаційного простору, прогнозуванні потенційних загроз, інтеграції механізмів кіберзахисту та стратегічних комунікацій, широкому використанні цифрової аналітики і технологій штучного інтелекту, а також посиленні міжвідомчої взаємодії та міжнародного співробітництва [8].

У цьому контексті інформаційна стійкість держави набуває стратегічного значення як здатність системи публічного управління своєчасно виявляти, запобігати, нейтралізувати та швидко відновлюватися після інформаційних і кібернетичних впливів, забезпечуючи безперервність виконання державою своїх функцій навіть в умовах воєнних загроз. Саме тому одним із пріоритетних напрямів державної політики має стати розбудова комплексної моделі державного регулювання інформаційної безпеки, яка поєднуватиме правові, організаційні, технологічні, інституційні та комунікаційні механізми забезпечення інформаційного суверенітету, цифрової стійкості та захисту національних інтересів України.

Крім того, сформована в умовах цифрової трансформації архітектура інформаційного простору суттєво змінила характер сучасних воєнних конфліктів. Поряд із традиційними засобами збройної боротьби дедалі активніше застосовуються інформаційні, кібернетичні та цифрові інструменти, спрямовані на досягнення військових, політичних, економічних і психологічних цілей. Це свідчить про перехід до багатовимірного формату протиборства, у якому інформаційна перевага стає одним із визначальних чинників забезпечення національної безпеки та ефективності державного управління [9].

Особливістю сучасних воєнних конфліктів є інтегроване використання інформаційних операцій, кібернетичних атак, цифрового шпигунства, технологій штучного інтелекту, автоматизованих систем аналізу інформації, соціальних мереж і цифрових платформ. Застосування зазначених інструментів дозволяє противнику здійснювати комплексний вплив на державні інституції, критичну інформаційну інфраструктуру, інформаційний простір та суспільну свідомість, що зумовлює необхідність адаптації механізмів державного регулювання інформаційної безпеки до нових форм гібридного протиборства (табл. 2).

Таблиця 2

Особливості використання цифрових технологій у сучасних воєнних конфліктах

Інструмент	**Основне призначення**	**Вплив на державне регулювання інформаційної безпеки**
Інформаційні операції	Маніпулювання інформаційним середовищем	Посилення стратегічних комунікацій та протидії дезінформації
Кібернетичні атаки	Порушення роботи інформаційних систем	Розвиток системи кіберзахисту та захисту критичної інфраструктури
Цифрове шпигунство	Отримання конфіденційної інформації	Посилення захисту державних інформаційних ресурсів
Штучний інтелект	Автоматизація інформаційного впливу та аналізу даних	Регулювання використання ШІ та впровадження інтелектуальних систем моніторингу
Автоматизований аналіз інформації	Виявлення ризиків і прогнозування	Використання цифрової аналітики у прийнятті управлінських рішень
Соціальні мережі та цифрові платформи	Поширення інформації та координація інформаційних кампаній	Моніторинг інформаційного простору та протидія маніпулятивному контенту

Джерело: сформовано автором на основі даних [10-12]

Проведений аналіз свідчить, що сучасні воєнні конфлікти характеризуються інтегрованим використанням цифрових технологій, які охоплюють інформаційні операції, кібератаки, цифрове шпигунство, штучний інтелект, автоматизовані системи аналізу інформації, соціальні мережі та цифрові платформи. Їх комплексне застосування істотно розширює спектр інформаційних загроз і змінює характер впливу на систему державного управління, поєднуючи технічні, інформаційні, психологічні та організаційні засоби протиборства. За таких умов забезпечення інформаційної безпеки потребує переходу від реагування на окремі інциденти до формування інтегрованої системи державного регулювання, заснованої на прогнозуванні ризиків, міжвідомчій координації, використанні сучасних цифрових технологій та розвитку інформаційної стійкості як одного з ключових елементів національної безпеки України.

Зростання складності сучасних інформаційних загроз, їх багаторівневий характер та висока швидкість поширення обумовлюють необхідність модернізації існуючої системи державного регулювання інформаційної безпеки. Ефективне реагування на сучасні виклики вже не може забезпечуватися виключно окремими державними органами або традиційними адміністративними механізмами, оскільки інформаційні загрози одночасно охоплюють безпекову, політичну, економічну, соціальну та технологічну сфери. Це потребує формування інтегрованої системи державного управління, заснованої на координації діяльності всіх суб'єктів забезпечення інформаційної безпеки, оперативному обміні інформацією та використанні сучасних цифрових технологій [13].

У цьому контексті особливої актуальності набуває удосконалення організаційно-інституційного механізму державного регулювання інформаційної безпеки шляхом розвитку міжвідомчої координації, інтеграції цифрових технологій у процеси управління безпекою, запровадження інтелектуальних систем моніторингу інформаційного простору, використання засобів прогнозної аналітики, автоматизованого виявлення інформаційних загроз та підтримки прийняття управлінських рішень. Реалізація зазначених напрямів сприятиме переходу від переважно реактивної моделі державного регулювання до проактивної, орієнтованої на своєчасне прогнозування ризиків, раннє виявлення потенційних загроз та запобігання їх негативним наслідкам.

Важливим напрямом модернізації є створення єдиного інформаційно-аналітичного середовища взаємодії між органами державної влади, сектором безпеки і оборони, суб'єктами кібербезпеки та операторами критичної інформаційної інфраструктури. Це забезпечить оперативний обмін інформацією про інциденти, координацію дій під час кризових ситуацій, уніфікацію процедур реагування та підвищення ефективності управлінських рішень. Одночасно використання технологій штучного інтелекту, аналізу великих даних і автоматизованих систем підтримки прийняття рішень дозволить здійснювати безперервний моніторинг інформаційного простору, виявляти приховані закономірності розвитку інформаційних загроз, прогнозувати можливі сценарії їх реалізації та визначати найбільш ефективні заходи реагування [14].

Таким чином, удосконалення організаційно-інституційного механізму державного регулювання інформаційної безпеки має здійснюватися на засадах інтегрованого управління, цифрової взаємодії та аналітичної підтримки прийняття рішень. Такий підхід забезпечить підвищення адаптивності системи публічного управління до сучасних воєнних і гібридних викликів, зміцнення інформаційної стійкості держави, підвищення ефективності міжвідомчої взаємодії та створення передумов для реалізації комплексної державної політики у сфері інформаційної безпеки.

Враховуючи сучасні тенденції розвитку інформаційного суспільства, зростання масштабів цифровізації публічного управління та трансформацію характеру інформаційних і воєнних загроз, виникає необхідність комплексної модернізації системи державного регулювання інформаційної безпеки [15]. Така модернізація має бути спрямована не лише на вдосконалення існуючих механізмів реагування на інформаційні загрози, а й на формування адаптивної системи управління, здатної забезпечувати прогнозування ризиків, своєчасне прийняття управлінських рішень та підвищення інформаційної стійкості держави. У цьому контексті доцільно виокремити такі концептуальні напрями модернізації (рис.).

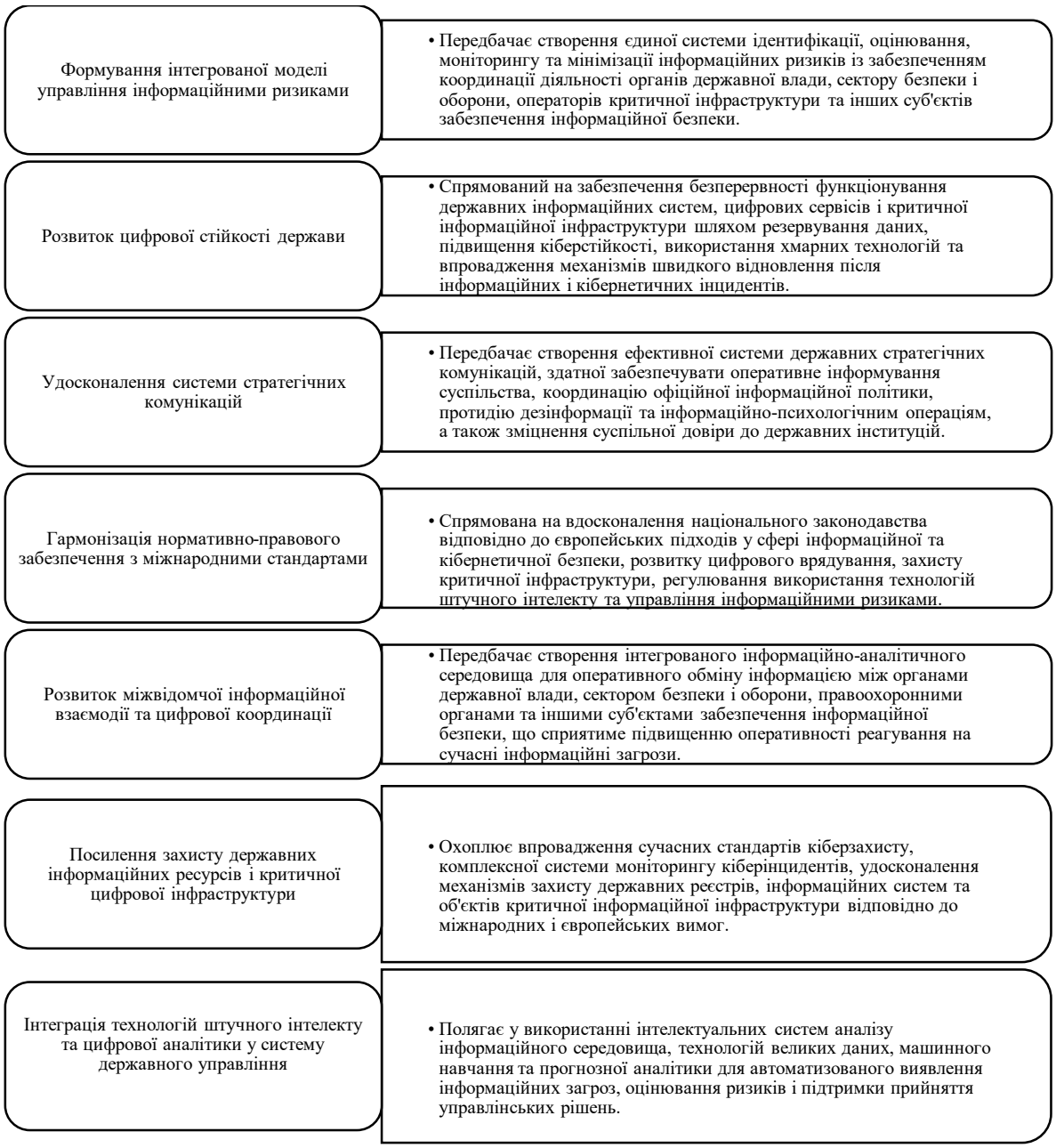

Рис. 1. Концептуальні напрями модернізації системи державного регулювання інформаційної безпеки
Джерело: сформовано автором на основі даних [16-18]

Підсумовуючи, доцільно відмітити, що модернізація системи державного регулювання інформаційної безпеки має здійснюватися на засадах комплексності, адаптивності та технологічної інноваційності. Реалізація запропонованих концептуальних напрямів забезпечить формування інтегрованої системи управління інформаційними ризиками, підвищення цифрової стійкості держави, ефективну протидію сучасним інформаційним і воєнним загрозам, удосконалення міжвідомчої взаємодії та підтримку прийняття управлінських рішень на основі сучасних цифрових технологій. У сукупності це сприятиме зміцненню інформаційного суверенітету України, підвищенню ефективності державного управління та забезпеченню надійного захисту національних інтересів в умовах розвитку інформаційного суспільства й трансформації глобального безпекового середовища.

Проведений аналіз сучасних тенденцій розвитку інформаційного суспільства, особливостей сучасних воєнних конфліктів та функціонування системи державного регулювання інформаційної безпеки засвідчив необхідність її подальшої модернізації відповідно до нових безпекових викликів і технологічних змін, що зумовлює потребу у формуванні комплексного підходу, що поєднуватиме нормативно-правові, організаційно-інституційні, технологічні та інформаційно-аналітичні

механізми забезпечення інформаційної безпеки, орієнтовані на підвищення адаптивності системи публічного управління, зміцнення інформаційного суверенітету та забезпечення стійкості держави в умовах розвитку інформаційного суспільства і сучасних воєнних загроз. У цьому контексті запропоновано такі концептуальні напрями модернізації системи державного регулювання інформаційної безпеки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отож, проведене дослідження підтвердило, що розвиток інформаційного суспільства, цифровізація публічного управління та трансформація сучасних воєнних загроз зумовлюють необхідність переосмислення існуючих підходів до державного регулювання інформаційної безпеки. Встановлено, що сучасна система інформаційної безпеки має базуватися на комплексному поєднанні правових, організаційно-інституційних і технологічних механізмів, здатних забезпечити своєчасне виявлення, прогнозування та нейтралізацію інформаційних і кібернетичних загроз.

Обґрунтовано доцільність модернізації організаційно-інституційного механізму державного регулювання шляхом розвитку міжвідомчої взаємодії, впровадження інтелектуальних систем моніторингу інформаційного простору, використання технологій штучного інтелекту та прогнозної аналітики, а також посилення захисту державних інформаційних ресурсів і критичної цифрової інфраструктури. Запропоновані концептуальні напрями модернізації спрямовані на формування інтегрованої моделі управління інформаційними ризиками, підвищення цифрової стійкості держави, удосконалення стратегічних комунікацій та зміцнення інформаційного суверенітету України, що в сукупності сприятиме підвищенню ефективності державного регулювання інформаційної безпеки в умовах розвитку інформаційного суспільства та сучасних воєнних загроз.

ЛІТЕРАТУРА:

1. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York : Basic Books, 1973. 507 p.
2. Castells M. The Rise of the Network Society. 2nd ed. Chichester : Wiley-Blackwell, 2010. 597 p. https://doi.org/10.1002/9781444319514
3. Toffler A. The Third Wave. New York : William Morrow and Company, 1980. 544 p.
4. Webster F. Theories of the Information Society. 4th ed. London ; New York : Routledge, 2014. 384 p.
5. Shannon C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948. Vol. 27. No. 3. P. 379–423; No. 4. P. 623–656. URL : https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf.
6. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York : John Wiley & Sons, 1996. 784 p.
7. Benkler Y. The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven ; London : Yale University Press, 2006. 515 p.
8. Ліпкан В. А. Інформаційна безпека України : навч. посіб. Київ : КНТ, 2009. 576 с.
9. Дзьобань О. П. Філософія інформаційного права: світоглядні й загальнотеоретичні засади : монографія. Харків : Майдан, 2013. 360 с.
10. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.
11. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Вид. дім «Києво-Могилянська академія», 2015. 497 с.
12. Пилипчук В. Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми правового регулювання. Київ : НДІІП НАПрН України, 2016. 418 с.
13. 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.
14. 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.

15. Білко С. Інституційне забезпечення інформаційної безпеки України. *Економіка і регіон.* 2021. № 3(82). С. 36–41. URL: https://journals-nupp-eduua.translate.goog/eir/article/view/2361?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc.

16. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. І*нформаційна безпека людини, суспільства, держави.* 2015. № 2 (18). С. 16-22.

REFERENCES:

1. Bell D. (1973) The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York: Basic Books.
2. Castells M. (2010) The Rise of the Network Society. 2nd ed. Chichester: Wiley-Blackwell. DOI: https://doi.org/10.1002/9781444319514
3. Toffler A. (1980) The Third Wave. New York: William Morrow and Company.
4. Webster F. (2014) Theories of the Information Society. 4th ed. London; New York: Routledge.
5. Shannon C.E. (1948) A Mathematical Theory of Communication. Bell System Technical Journal, vol. 27, no. 3, pp. 379–423; no. 4, pp. 623–656. Available at: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf
6. Schneier B. (1996) Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons.
7. Benkler Y. (2006) The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven; London: Yale University Press.
8. Lipkan V.A. (2009) Informatsiina bezpeka Ukrainy [Information Security of Ukraine]. Kyiv: KNT.
9. Dzoban O.P. (2013) Filosofiia informatsiinoho prava: svitohliadni y zahalnoteoretychni zasady [Philosophy of Information Law: Worldview and General Theoretical Foundations]. Kharkiv: Maidan.
10. Horbulin V.P. (2017) Svitova hibrydna viina: ukrainskyi front [World Hybrid War: Ukrainian Front]. Kyiv: NISD.
11. Pocheptsov H.H. (2015) Suchasni informatsiini viiny [Modern Information Wars]. Kyiv: Vydavnychyi dim «Kyievo-Mohylianska akademiia».
12. Pylypchuk V.H. (2016) Zabezpechennia informatsiinoi bezpeky Ukrainy: suchasni tendentsii ta problemy pravovoho rehuliuvannia [Ensuring Information Security of Ukraine: Current Trends and Problems of Legal Regulation]. Kyiv: NDIIP NAPrN Ukrainy.
13. Koval Ya.S., Dudetskyi D.V. (2024) Udoskonalennia mekhanizmiv derzhavnoho upravlinnia v umovakh didzhytalizatsii [Improvement of public administration mechanisms under digitalization]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok – Public Administration: Improvement and Development*, no. 6. DOI: https://doi.org/10.32702/2307-2156.2024.6.14
14. Kondratenko V.M., Sokurenko O.A. (2025) Administratyvno-pravovi zasady zabezpechennia informatsiinoi bezpeky ta dostupu do publichnoi informatsii v diialnosti pravookhoronnykh orhaniv sektoru natsionalnoi bezpeky [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 – Uzhhorod National University Herald. Series: Law*, vol. 2, no. 89, pp. 452–457.
15. Bilko S. (2021) Instytutsiine zabezpechennia informatsiinoi bezpeky Ukrainy [Institutional support of information security of Ukraine]. *Ekonomika i rehion – Economy and Region*, no. 3(82), pp. 36–41. Available at: https://journals-nupp-eduua.translate.goog/eir/article/view/2361?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc
16. Dereko V.N. (2015) Teoretyko-metodolohichni zasady klasyfikatsii zahroz obiektam informatsiinoi bezpeky [Theoretical and methodological principles of classification of threats to information security objects]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy – Information Security of the Individual, Society and State*, no. 2(18), pp. 16–22.

GOVERNMENT REGULATION OF INFORMATION SECURITY IN THE CONTEXT OF THE DEVELOPMENT OF THE INFORMATION SOCIETY AND CONTEMPORARY MILITARY THREATS

SOROKIVSKA Olena
Ternopil Ivan Puluj National Technical University

This article examines the theoretical, methodological, and practical foundations of state regulation of information security in the context of the development of the information society and contemporary military threats. It is argued that the rapid digitization of social relations, the large-scale implementation of information and communication technologies, the growth in the volume of digital data, the integration of artificial intelligence into the sphere of public administration, and the intensification of hybrid forms of conflict are significantly transforming approaches to ensuring national security. The article analyzes current trends in the development of the information society, characterized by increasing digital interaction between the state, citizens, and businesses, as well as the development of e-government, digital platforms, open data, cloud technologies, big data, and artificial intelligence. Particular attention is paid to examining the impact of contemporary military threats on Ukraine's system of state regulation of information security. It has been demonstrated that the Russian Federation's full-scale military aggression against Ukraine has highlighted the need to rethink traditional mechanisms of state governance in the information sphere and to develop a comprehensive model for ensuring the state's information resilience. It has been determined that modern military conflicts are characterized by the widespread use of information operations, cyberattacks, digital espionage, artificial intelligence technologies, automated information analysis systems, social networks, and digital platforms as instruments of warfare. The paper justifies the need to improve the organizational and institutional mechanisms of state regulation of information security by developing interagency coordination, integrating digital technologies into security management processes, introducing intelligent systems for monitoring the information space, and utilizing predictive analytics, automated detection of information threats, and support for managerial decision-making. Conceptual directions for modernizing the system of state regulation of

information security have been proposed, which include the development of an integrated model for managing information risks, the advancement of the state's digital resilience, the improvement of strategic communication mechanisms, the implementation of modern artificial intelligence technologies for analyzing the information environment, strengthening the protection of state information resources and critical digital infrastructure, and improving the effectiveness of interagency information exchange.

Keywords: state regulation, strategic communications, information security, information society, military threats, risks, cybersecurity.