МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

КОТЛЯРОВ Валерій Олександрович

УДК 351.816/.817:351.746.1:004

МЕХАНІЗМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

Спеціальність 25.00.02 – механізми державного управління

Реферат
дисертації на здобуття наукового ступеня
доктора наук з державного управління

Харків 2026

Дисертацією є рукопис.
Робота виконана здобувачем шляхом самостійної підготовки наукових досліджень до захисту.

Офіційні опоненти: доктор наук з державного управління, професор
ПОМАЗА-ПОНОМАРЕНКО Аліна Леонідівна,
Національний університет цивільного захисту України,
завідувач науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту навчально-наукового інституту цивільного захисту

доктор наук з державного управління, професор
АНТОНОВА Людмила Володимирівна,
Чорноморський національний університет імені Петра Могили, професор кафедри обліку і аудиту

доктор наук з державного управління, професор
ЩЕПАНСЬКИЙ Едуард Валерійович
Хмельницький університет управління та права імені Леоніда Юзькова, завідувач кафедри публічного управління та адміністрування

Захист відбудеться «26» червня 2026 р. об 11.00 годині на засіданні Спеціалізованої Вченої ради Д 64.062.09 Національного аерокосмічного університету «Харківський авіаційний інститут» за адресою: 61070, м. Харків, вул. Вадима Манька 17.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Національного аерокосмічного університету «Харківський авіаційний інститут» за адресою: 61070, м. Харків, вул. Вадима Манька, 17.

Учений секретар
спеціалізованої вченої ради Надія КАРПЕКО

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. На сучасному етапі інформаційна безпека держави є фундаментальною складовою публічного управління, яка забезпечує захист її стратегічних інтересів як на внутрішньому національному, так і на міжнародному рівнях. У контексті публічного управління інформаційна безпека виступає як самостійний управлінський конструкт, що охоплює: захищеність, доступність, цілісність та конфіденційність інформаційних ресурсів, якими оперує держава; спрямування та координацію національного інформаційного простору з метою забезпечення його інформаційної гігієни.

Інформаційна безпека в системі публічно-управлінського забезпечення має чітко визначену структуру, модель, а також потребує ефективних механізмів реалізації та системної суб'єктності. Для цілей нашого дослідження є доцільним зосередити увагу на аналізі механізмів правового забезпечення та управлінської практики, застосовуючи порівняльний підхід на прикладі України та країн-партнерів (зокрема, ЄС та США).

Затребуваність тематики дослідження механізмів реалізації інформаційної безпеки у системі публічного управління особливо гостро проявилася в умовах повномасштабного вторгнення рф в Україну (з 24.02.2022 р.). Ця агресія спричинила безпрецедентні виклики для сфери інформаційної безпеки як ключового складника безпеки національної.

У зв'язку з цим, актуальним є огляд управлінської діяльності профільних органів, які відповідають за забезпечення інформаційної гігієни та безпеки держави в умовах воєнного стану: Міністерство культури та інформаційної політики України; Рада національної безпеки і оборони України (РНБО) та підпорядкований їй Центр протидії дезінформації; Кабінет Міністрів України (як головний суб'єкт управління).

Окремим завданням є дослідження нормативно-правового інструментарію, який використовується цими органами та інституціями для формування та підтримки безпечного інформаційного простору.

Аналіз наукових праць підтверджує, що проблематика механізмів реалізації інформаційної безпеки та її стратегічних цілей є об'єктом пильної уваги фахівців у галузях публічного управління та адміністрування, права, політології та філософії.

Теоретико-методологічні засади, структура правового механізму, міжнародна практика та аналіз загроз є предметом досліджень таких вітчизняних вчених, як: Л. Кочубей, А. Войціховський, О. Олійник, П. Діхтієвський, З. Гбур, Н. Цибульник, В. Торічний, У. Ільницька, В. Панченко, І. Боднар, О. Архипов, В. Шемчук, І. Валюшко, Л. Мазуренко, І. Поліщук, І. Ломака, В. Шишко, В. Горовий, С. Петренко, Н. Назаренко, Є. Рогова, К. Захаренко, Т. Амро, Б. Кормич та інші.

Незважаючи на достатньо велику загальну кількість робіт з проблем механізмів реалізації інформаційної безпеки держави, потребують вирішення наукові питання щодо: комплексної розробки та обґрунтування інтегративної моделі механізмів реалізації інформаційної безпеки у системі публічного

управління України, яка б поєднувала інституційно-правовий, комунікаційно-стратегічний та міжсекторальний аспекти в умовах гібридних загроз та викликів воєнного часу; формування цілісної концепції стратегічного управління інформаційною безпекою, що включає діагностику управлінських обмежень та розробку науково обґрунтованих напрямів удосконалення функціоналу ключових суб'єктів (РНБО, Центр протидії дезінформації; Кабінет Міністрів України) з урахуванням сучасного міжнародного досвіду.

Потреба у теоретичному, методологічному та практичному вирішенні окреслених завдань підтверджує актуальність дослідження, його наукову новизну та зумовлює мету, завдання, предмет і об’єкт роботи.

Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження проведено в межах науково-дослідної роботи, яка виконувалась Національним авіаційним університетом за темою: «Традиції і новації у сучасній український державності та правовому житті» (державний реєстраційний номер 0106U004970). Внесок автора полягає у теоретичному обґрунтуванні теоретико-методологічних засад забезпечення інформаційної безпеки в умовах глобалізації, означенні та науковому аналізі структури механізму правового забезпечення інформаційної безпеки безпосередньо в Україні, дослідженні міжнародних норм та практик забезпечення інформаційної безпеки, аналізі сучасних загроз інформаційній безпеці України. Окремим кластерним пунктом внеску автора дослідження доцільно визначити розробку Стратегії-моделі національної інформаційної стійкості України.

Мета і задачі дослідження. Мета дослідження полягає у теоретичному обґрунтуванні та науково-практичному аналізі механізмів реалізації інформаційної безпеки у системі публічного управління, визначенні їх стратегічних цілей і функціонального призначення, а також у з’ясуванні особливостей формування та функціонування інформаційно-безпекового середовища України в особливий період.

Реалізація визначеної мети зумовила постановку й вирішення наступних завдань :

– обґрунтувати та розробити інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України;

– уточнити теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління;

– обґрунтувати підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління;

– систематизувати та концептуалізувати методологічні засади дослідження інформаційної безпеки у системі публічного управління;

– розкрити сутнісні характеристики механізму правового регулювання інформаційної безпеки;

– систематизувати та науково обґрунтувати методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії;

– розробити концептуальну модель переходу до адаптивної архітектури забезпечення інформаційної безпеки;

– розвинути теоретичні засади стратегічного управління інформаційною

безпекою;

– узагальнити та систематизувати сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави;

– обґрунтувати теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки;

– розробити та науково обґрунтувати стратегію-модель національної цифрової стійкості України.

Об'єкт дослідження – інформаційна безпека держави як система суспільних відносин інформаційна безпека держави як система суспільних відносин у сфері публічного управління.

Предмет дослідження – механізми реалізації інформаційної безпеки у системі публічного управління.

Методи дослідження.

Методологічну основу проведеного дослідження становить сукупність взаємопов'язаних загальнонаукових і спеціалізованих підходів, серед яких застосовано системний, історико-ретроспективний, компаративний, структурно-функціональний методи, а також методи аналізу й синтезу, узагальнення та класифікації, індуктивного й дедуктивного мислення, принципи взаємозв'язку частини та цілого, проблемного і прогностичного аналізу. Застосування історико-ретроспективного методу дало змогу здійснити концептуалізацію термінологічного та категоріального апарату поняття «інформаційна безпека» в межах системи національної безпеки [параграф 1.1]. У свою чергу, через узагальнення й систематизацію вітчизняних наукових джерел було проаналізовано інформаційну безпеку як багатовимірну систему суспільних відносин і водночас – як об'єкт правової охорони [параграф 1.2], а також виокремлено ключові методологічні орієнтири для подальшого дослідження даного феномену [параграф 1.3].

Системний та структурно-функціональний підходи надали можливість розкрити сутність та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки, концептуалізувавши нормативні особливості такого процесу та систему суб'єктів забезпечення інформаційної безпеки [параграф 2.1; параграф 2.2; параграф 2.3]. Використання емпіричних методів, індукції й дедукції забезпечило розкриття сутності, мети та особливостей стратегічного управління забезпеченням інформаційної безпеки [параграф 3.1]. Завдяки проблемному й прогностичному підходам проаналізовано глобальний характер інформаційної безпеки крізь призму інституційних можливостей та ризиків, а також комунікаційну стратегію як складову національного управління інформаційною безпекою та, на додаток, класифіковано загрози інформаційній безпеці України і систематизовано методичні підходи протидії загрозам інформаційній безпеці України.

Наукова новизна одержаних результатів полягає у комплексному теоретичному обгрунтуванні стратегічних орієнтирів та інституційно-правових механізмів реалізації інформаційної безпеки (ІБ) у системі публічного управління як автономного, системно організованого феномену в контексті сучасних трансформаційних викликів. Найбільш вагомими науковими

результатами дисертаційного дослідження є такі:

уперше

– обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури та інформаційної політики); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства;

– обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік – ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA, Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам);

– розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством у протидії гібридним загрозам, включає чотири ключові принципи (проактивність, багаторівнева координація, гнучкість, демократичний контроль), що формують методологічний каркас стратегії-моделі, забезпечуючи перехід від реактивного до прогнозно-превентивного управління інформаційною безпекою, та інституційно-інструментальне забезпечення (створення Єдиного національного центру стратегічних комунікацій як ключової координуючої інституції, що інтегрує моніторинг загроз, міжрівневу координацію та стратегічні комунікації);

удосконалено

– підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб'єктів –

Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) – виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб'єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція);

– концептуалізацію сутнісного призначення механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування «інформаційного суспільства»); 2) теоретичне обґрунтування власного підходу до кореляції між механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового опису дванáдцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри;

– систематизацію та наукове обґрунтування методичних підходів протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта»

та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft;

– концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію нової системної логіки та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування);

дістали подальшого розвитку:

– поглиблено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів: інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб'єкти: держава, громадянське суспільство, бізнес; об'єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості (суб'єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони: Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об'єктів правової охорони;

– систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної

політики;

– теоретичні засади стратегічного управління інформаційною безпекою (ІБ) шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ);

– узагальнення та систематизація сучасних викликів та тенденцій розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні мережі та цифрові платформи є феноменом подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих алгоритмічних процесів); обґрунтувати необхідність інтеграції нових підходів до зміцнення кіберстійкості суспільства та сформувати двопланову модель протидії ризикам (поведінковий/освітній вимір: акцентовано на інформаційній гігієні та медіаграмотності як базових елементах зменшення вразливості громадян (приклад Швеції та Фінляндії); інституційно-правовий вимір: систематизовано нові регуляторні механізми (зокрема, Digital Services Act (DSA) та Data Governance Act (DGA) ЄС), які створюють інституційну рамку для боротьби з дезінформацією та забезпечення прозорості алгоритмів, що є прикладом збалансованого регулювання).

Практичне значення одержаних результатів. Основні ідеї та висновки дослідження доведено до конкретних положень, методик і рекомендацій. Вони

можуть бути використані у практичній діяльності органами публічного управління на національному й регіональному рівнях, підприємствами, громадськими організаціями.

Результати дисертації були впроваджені у діяльність Національної акціонерної компанії «Надра України» (довідка про впровадження НАК «Надра України»). Зокрема, розроблені у межах дослідження рекомендації використані для удосконалення механізмів захисту інформаційного простору національної акціонерної компанії, забезпечення кіберстійкості державних підприємств та протидії інформаційним загрозам в умовах воєнного стану. Результати наукового дослідження були впроваджені у діяльність Національного агентства кваліфікацій в таких напрямах: оцінка ризиків у сфері кваліфікаційної безпеки (інтегровано методику класифікації інформаційних загроз та ризиків в регламенти роботи із даними Реєстру кваліфікацій); модернізація аналітичних систем (алгоритми прогнозування загроз, запропоновані в дисертації, стали основою вдосконалення цифрової інфраструктури аналітичних модулів); оновлення професійних стандартів (наукові положення використано при оновленні кваліфікаційних вимог для фахівців з кібербезпеки, зареєстрованих у Національному реєстрі кваліфікацій); аналітична підтримка державної політики Результати дисертації були впроваджені у діяльність Департаменту кадрової політики Міністерства оборони України (довідка про впровадження Департаменту кадрової політики Міністерства оборони України). Зокрема, розроблені у межах дослідження автора рекомендації використані для удосконалення механізмів захисту інформаційного простору департаменту та протидії інформаційним загрозам в умовах воєнного стану.

У межах науково-дослідної діяльності Центрального науково- дослідного інституту Збройних Сил України використані результати докторської дисертації, які спрямованої на вдосконалення системи інформаційної безпеки в умовах гібридних загроз (довідка про впровадження №172/2950 від 07.11.2025 р.).

У межах діяльності Департаменту захисту критичної інфраструктури Адміністрації Державної служби спеціального зв’язку та захисту інформації України, під час підготовки щорічної оцінки ризиків та загроз у сфері критичної інфраструктури, було здійснено аналіз наукових напрацювань, що стосуються стратегічного реагування на гібридні загрози, захисту інформаційного простору та забезпечення кіберстійкості державних і приватних суб’єктів (довідка від 12.11.2025 р. № 1451).

Висновки дисертації включено до експертних матеріалів щодо гармонізації українських кваліфікаційних норм з європейськими рамками (довідка про впровадження Національного агентства кваліфікацій від 22.07.2025 р. № 01/01.01-06/1647).

Особистий внесок здобувача. Представлена дисертація є результатом самостійного наукового дослідження, в якому автор формулює власне бачення вирішення актуальних проблем публічного управління у сфері стратегічного забезпечення інформаційної безпеки держави в умовах посилення зовнішніх і внутрішніх викликів. Усі положення, що виносяться на захист, а також ключові

висновки сформульовані дисертантом особисто. У разі використання наукових напрацювань, створених у співавторстві, до тексту дисертації включено виключно ті ідеї й концептуальні підходи, які є результатом індивідуальної наукової діяльності автора.

У працях, що опубліковані в співавторстві, особистий внесок зазначено у переліку наукових праць автора.

Апробація результатів дослідження. Основні положення дисертаційного дослідження були представлені та пройшли апробацію на міжнародних науково-практичних конференціях, а саме: «3rd International Conference on Corporation Management (ICCM-2023)» (Estonia, 2023), «ICEAF-2023» (Estonia, 2023), «II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology» (Варшава, Польща, 2023), «II International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research» (Амстердам, Нідерланди, 2023).

Публікації. Основні положення дисертаційної роботи опубліковано у 36 наукових працях, загальним обсягом 29,3 обл.-вид. арк. (24,7 обл.-вид. арк. належить автору), зокрема у розділі колективної монографії, 4 статтях, опублікованих у періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України та у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus, 18 статтях у наукових фахових виданнях з державного управління, 9 статтях у інших періодичних виданнях України, 4 тезах доповідей на науково-практичних конференціях.

Обсяг та структура роботи. Дисертація складається зі вступу, п’яти розділів, висновків, списку використаних джерел, додатків. Повний обсяг роботи – 398 сторінок. Дисертація містить 1 таблицю та 4 рисунки. Список використаних джерел містить 300 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертації, її зв’язок з напрямами, програмами і темами наукових досліджень. Сформульовано мету і завдання дослідження, охарактеризовано наукову новизну та практичне значення одержаних результатів, наведено апробацію основних положень.

У **першому розділі** – «Науково-теоретичні засади механізмів реалізації інформаційної безпеки у системі публічного управління» уточнено понятійно-категоріальний апарат реалізації механізмів інформаційної безпеки у системі публічного управління. Визначено інформаційну безпеку як систему суспільних відносин та об’єктом публічного управління. Досліджено систему суб’єктів забезпечення інформаційної безпеки в публічному управлінні.

У межах дослідження було здійснено комплексний аналіз та критичне осмислення теоретико-методологічних засад забезпечення інформаційної безпеки (ІБ), що дозволило систематизувати та уточнити ключовий понятійно-категоріальний апарат для його подальшої коректної імплементації у системі

публічного управління. Аналіз здійснювався у двох взаємопоєднаних проєкціях: автономній (як самостійного конструкту) та системній (як складової національної безпеки) (табл. 1).

Таблиця 1

Систематизація теоретико-методологічних засад та інституційної архітектури ІБ

Категорія / Інституція	Авторське дефініціювання / Роль	Ключові аспекти та функції
Інформаційна безпека (ІБ)	Захищеність інформаційних систем та баз даних від зовнішнього втручання, а також послідовність внутрішньодержавної інформаційної політики, що гарантує безпеку даних у контексті їхнього зберігання та споживання в політико-соціальному вимірі.	Розглядається у двох проєкціях: автономній та системній (як системоутворюючий елемент державної безпеки).
Механізм забезпечення ІБ	Сукупність організаційно-правових та інституційних елементів забезпечення інформаційно-безпекового простору, котрі співвідносяться як зміст та форма реалізації зазначеної феноменологічної конструкції.	Необхідність інституційного складника для практично-прикладного впровадження правової та організаційної складових.
Співвідношення ІБ та Національної безпеки	Реалізація за допомогою ІБ завдань Національної безпеки, а саме: інформаційна захищеність держави та населення, безпека нації, захищеність даних та інформації, що складають державну таємницю.	Обґрунтовано нерозривний зв'язок, де ІБ детермінує виміри державної стабільності.
Безпека (розширене)	Комплексний феномен, що включає в себе стан спокою та захищеності регулярних державних дій та ситуацій на рівні публічної служби, інституційного забезпечення, інформаційного простору, соціальної сфери тощо.	Усунення обмеженості терміну рамками виключно державно-управлінської теорії.
Управління інформацією	Цілісний процес координації даних, у якому інформація виступає одночасно і ресурсом, і об’єктом, і засобом впливу.	Має яскраво виражений публічно-управлінський аспект, визначальний для формування цифрової держави та її підзвітності.
Структура ІБ	Структурний тріумвірат інституційно-методичного впорядкування.	ІБ систематизовано як система суспільних відносин та об'єкт правової охорони з визначенням відповідальних суб'єктів.

Критичний аналіз та авторське дефініціювання ключових понять. На основі порівняльного аналізу наукових напрацювань вітчизняних (В. Шемчук, Л. Мазуренко, В. Торічний, А. Войціховський, А. Нашинець-Наумова та ін.) та

зарубіжних учених, виявлено необхідність доопрацювання існуючих доктринальних дефініцій з огляду на реалії глобалізації, інформатизації та діджиталізації. Зокрема, критично переосмислено підхід, що трактує ІБ виключно як захист від несанкціонованого внутрішнього втручання.

За результатами дослідження запропоновано авторські визначення ключових категорій. Поняття «інформаційна безпека» доцільно визначати як: «захищеність інформаційних систем та баз даних від зовнішнього втручання, а також послідовність внутрішньодержавної інформаційної політики, що гарантує безпеку даних у контексті їхнього зберігання та споживання в політико-соціальному вимірі». Термін «механізм забезпечення інформаційної безпеки» визначено на доктринально-теоретичному рівні як: «сукупність організаційно-правових та інституційних елементів забезпечення інформаційно-безпекового простору, котрі співвідносяться як зміст та форма реалізації зазначеної феноменологічної конструкції». Це уточнення дозволило усунути контраверсію щодо незастосовності інституційного складника, який є необхідним для практично-прикладного впровадження правової та організаційної складових.

У контексті дослідження системних рис глобального характеру інформаційної безпеки, особливо в умовах російсько-української військової агресії, обґрунтовано нерозривний зв’язок ІБ з національно-безпековою парадигмою. Для доктринально-теоретичного дефініціювання їхньої змістовно-формальної взаємної залежності введено в науковий обіг дефініцію «співвідношення інформаційної безпеки та національної безпеки», яке полягає: «у реалізації за допомогою першої завдань другої, а саме таких кластерів, як інформаційна захищеність держави та населення, безпека нації та населення, захищеність даних та інформації, що складають державну таємницю та ін., котрі власне детермінують виміри державної стабільності на внутрішньодержавному рівні».

Виходячи з необхідності усунення обмеженості терміну «безпека» лише рамками державно-управлінської теорії, запропоновано його розширене визначення: комплексний феномен, що включає в себе стан спокою та захищеності регулярних державних дій та ситуацій на рівні публічної служби, інституційного забезпечення, інформаційного простору, соціальної сфери тощо.

Підтверджено, що «безпека держави» є багатовимірним і найбільш комплексним явищем (за А. Войціховським), яке поєднує управлінські, законодавчі, соціально-комунікаційні та інформаційно-аналітичні елементи. Зроблено висновок, що в умовах глобальних інформаційних викликів інформаційна безпека постає не просто складовою частиною, а системоутворюючим елементом державної безпеки, оскільки забезпечує стабільність комунікацій, достовірність інформаційних потоків і підтримує легітимність влади через довіру громадян. Підтверджено, що «управління інформацією» має яскраво виражений публічно-управлінський аспект, розглядаючись як цілісний процес координації даних, у якому інформація виступає одночасно і ресурсом, і об’єктом, і засобом впливу, що є визначальним для формування цифрової держави та забезпечення її підзвітності.

Феномен інформаційної безпеки (ІБ) розглянуто у двох ключових проєкціях: як система суспільних відносин та як об’єкт правової охорони. Іноземні наукові парадигми (М. Віттмен, Г. Метторд, М. Воркмен) визначають ІБ як кластерний

складник національної безпеки, що передбачає скоординовану діяльність держави, спрямовану на захист критичної інфраструктури, протидію кіберзлочинності, кібертероризму та інформаційно-психологічним впливам. ІБ трактується як складна державна конструкція, що має власні завдання. ІБ розкривається як сукупність інтеракцій між суб'єктами державного управління та суспільства, які забезпечують належний рівень координаційного захисту інформаційного простору від загроз.

Ключові елементи системи:

– суб'єкти: держава (гарант нормативного та інфраструктурного забезпечення), громадянське суспільство (споживачі/генератори даних, відповідальні за інформаційну гігієну), бізнес (розробка пз та надання захисних послуг), міжнародні організації (глобальна координація стандартів);

– об'єкт: інформаційне середовище, що включає ресурси (бази даних, хмарні сховища), комунікаційні засоби (інтернет, медіапростір) та інфраструктуру;

– регулювання: нормативно-правова база, що визначає права, обов'язки та юридичну відповідальність суб'єктів.

Серед особливостей системи виділено суб'єктну взаємозалежність, громадянську участь, інформаційну грамотність (критичне мислення, детекція дезінформації) та етику з відповідальністю.

Зроблено проміжні висновки та пропозиції: ІБ є структурним тріумвіратом інституційно-методичного впорядкування. Для ефективних трансформацій у розумінні ІБ як об'єкта правової охорони доцільно впровадити законодавче ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина», а також систематизувати ІБ як систему суспільних відносин та об'єкт правової охорони із визначенням відповідальних суб'єктів.

Забезпечення інформаційної безпеки в Україні є багатоскладним процесом, що складається із нормативного та інституційного складника реалізації зазначеної ініціативи, які доповнюють один одного. Інституційний складник забезпечення інформаційної безпеки України реалізується за допомогою системи суб'єктів, відповідальної за даний напрям пропорційно колу власної компетенції. До таких суб'єктів належать: Служба безпеки України (СБУ); Рада національної безпеки і оборони України (РНБО); Міністерство цифрової трансформації України (Мінцифра); Національна поліція України (Нацполіція); Міністерство культури та стратегічних комунікацій України (Мінкульт).

Пропонуємо нижче зосередити увагу на аналізі ролі та місця кожного у формуванні інформаційно-гігієнічного та інформаційно-безпекового поля в Україні в умовах глобальних викликів та трансформацій.

1. Служба безпеки України (СБУ). Законодавча кореляція між діяльністю СБУ та її компетенцією щодо забезпечення інформаційної безпеки України наявна у ст. 10 Розділу II Закону України «Про службу безпеки України» № 2229-XII. Тут законодавцем зазначено, що центральним управлінням СБУ може бути здійснено заходи щодо контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. Категорія «інтереси держави у сфері інформаційної безпеки» розкривається за напрямами: захист державних інформаційних ресурсів, протидія інформаційним загрозам та дезінформації, а також координація дотримання законодавства у сфері ІБ задля забезпечення інформаційної

обороноздатності держави. СБУ виконує мультифункціональну роль щодо контролю та нагляду за елементами формування національної інформаційної політики, підтримання інформаційної гігієни та мінімізації або нівелювання правопорушень у сфері ІБ. Свою діяльність СБУ провадить у тісному взаємозв'язку та на засадах взаємодії із іншими органами, що забезпечує системність.

2. Рада національної безпеки та оборони України (РНБО). Компетенція РНБО концептуалізується відповідно до Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР. Згідно з абз. 2 п. 1 ч. 1 ст. 4, компетенція РНБО поширюється на сферу протидії порушень стратегічних національних інтересів держави в інформаційній сфері. РНБО проводить поточні заходи зі стабілізації національної безпекової карти, тоді як СБУ здійснює контроль за діяльністю органів, що знаходяться відносно неї нижче за юрисдикцією. Інформаційна безпека тут розглядається крізь призму глобального національного інтересу.

3. Міністерство цифрової трансформації України (Мінцифра). Діяльність Мінцифри регламентується Постановою КМУ № 856 від 18.09.2019 р. Роль Мінцифри формується на основі необхідності балансування та впорядкування даних та інформаційних систем в умовах діджиталізації. Основні напрями діяльності, пристосовні до ІБ, – розвиток інформаційного суспільства та національних електронних інформаційних ресурсів. Мінцифра бере участь у веденні інформаційної взаємодії між органами влади та функціонуванні електронних реєстрів публічної формації, що сприяє детінізації діяльності та формуванню захищеності інформації.

Тривимірна архітектурна модель взаємодії (СБУ, РНБО, Мінцифра) передбачає спільну мету: функціонування всіх трьох інституцій безпосередньо в інтересах інформаційної безпеки України.

4. Національна поліція України (Нацполіція). Нацполіція має факультативне значення, проте концептуально доповнює систему. Згідно із Законом України «Про Національну поліцію України» № 580-VIII, Нацполіція бере участь у притягненні до відповідальності винних за порушення використання інформаційних ресурсів (ст. 28), що мало наслідком порушення прав, свобод, інтересів людини. Роль Нацполіції є фрагментарною, але ключовою на рівні притягнення до відповідальності за правопорушення, що негативно впливають на внутрішнє інформаційне середовище.

5. Міністерство культури та стратегічних комунікацій України (Мінкульт). Діяльність Мінкульту (Постанова КМУ № 885 від 16.10.2019 р.) формує «соціальний» наратив ІБ-моделі. До його основних цілей віднесено культивацію інформаційної політики України та, зокрема, інформаційної безпеки України як її складника (абз. 3 пп. 1 п. 3). Мінкульт також здійснює нормативно-правове регулювання, пріоритезацію та перспективне рамкування ІБ-галузі та надає методико-практичну допомогу. Його соціальна роль полягає у забезпеченні культурно-інформаційної стійкості та зміцненні національної ідентичності.

Зроблено висновок, що СБУ, РНБО, Мінцифра, Нацполіція та Мінкульт є ключовими елементами державної системи забезпечення ІБ. Їхня діяльність є взаємодоповнюючою: СБУ протидіє загрозам, РНБО визначає стратегію, Мінцифра розвиває цифрову інфраструктуру захисту, Нацполіція розслідує злочини, а

Мінкульт забезпечує культурно-інформаційну стійкість. Спільна діяльність цих органів створює комплексний підхід до захисту національних інтересів в інформаційному просторі України.

У **другому розділі** – «Методологічні засади механізмів реалізації інформаційної безпеки у системі публічного управління» обґрунтовано концептуальні підходи до дослідження інформаційної безпеки в публічному управлінні та уточнено методологічні орієнтири її реалізації. Визначено принципи функціонування механізмів забезпечення інформаційної безпеки, що забезпечують їх системність, адаптивність і результативність. Проаналізовано правове регулювання у сфері інформаційної безпеки, окреслено прогалини та напрямки його удосконалення з урахуванням сучасних викликів.

Встановлено, що інформаційна безпека (ІБ) на сучасному етапі є чутливим аспектом державно-управлінського апарату через глобальні виклики та динамічні кіберзагрози. Загрози ІБ мають не лише технічний прояв (DDoS-атаки), але й соціально-психологічний (маніпулювання громадською думкою) та політико-економічний (кібершпигунство, кібертерор). Дослідження ІБ потребує чітких методологічних засад, заснованих на системності, міждисциплінарності та комплексному аналізі.

Визначено основні методологічні засади (табл. 2).

Таблиця 2

Методологічні засади механізмів реалізації інформаційної безпеки

Категорія	Сутність / Визначення	Ключові складові та функції
Основні методологічні засади	Системність, міждисциплінарність, комплексність аналізу.	Системність: Аналіз ІБ як упорядкованої структури стабільних елементів (суб'єктів, об'єктів, загроз, механізмів захисту). Міждисциплінарність: Інтеграція знань з технічної, правової, соціальної, економічної, міжнародної та психологічної сфер.
Спеціалізовані підходи	Системний, структурно-функціональний, історико-ретроспективний, проблемний, прогностичний.	Використовуються для розкриття сутності, принципів побудови механізму правового регулювання ІБ, концептуалізації термінологічного апарату та формування стратегії протидії загрозам.
Принципи дослідження ІБ	Комплексність, прогнозованість, глобальність.	Комплексність: Кореляція теоретичних підходів, міжнародних концепцій та національної практики. Глобальність: Урахування міжнародних стандартів (GDPR, ISO/IEC 27001) та потенційна рецепція міжнародних практик.
Філософські основи ІБ	Діалектичне співставлення категорій «безпека» та «свобода».	Інформація як ресурс та актив; ІБ як прояв свободи індивіда вільно споживати та аналізувати дані.

Системність передбачає аналіз ІБ як упорядкованої структури сталих елементів (суб'єктів, об'єктів, загроз та механізмів захисту) з урахуванням їхньої взаємодії та прогностичного моделювання. Міждисциплінарність виступає інтегрованим підходом для всебічного аналізу ІБ, детермінованим складністю

проблеми та динамізмом кіберзагроз. Сфери інтеграції знань охоплюють: технічну, правову, соціальну, економічну, міжнародну та психологічну складові. Наприклад, правова сфера аналізує ІБ як частину державного суверенітету, тоді як соціальна — вивчає поведінку користувачів та громадську думку. Комплексність аналізу узагальнює системний та міждисциплінарний підходи, вимагаючи дослідження ІБ не лише в межах науки державного управління, а й із залученням суміжних наукових полів для встановлення її ролі в усіх форматах життя держави.

Методологічну основу дослідження становить сукупність взаємопов'язаних загальнонаукових (аналіз, синтез, індукція, дедукція) і спеціалізованих підходів: системний та структурно-функціональний – для розкриття сутності та принципів побудови механізму правового регулювання ІБ; історико-ретроспективний – для концептуалізації термінологічного апарату; проблемний і прогностичний – для аналізу глобального характеру ІБ, класифікації загроз та формування стратегії протидії.

Принципами дослідження ІБ, застосованими у роботі, є: комплексність (кореляція загальних теоретичних підходів, міжнародних концепцій та національної практики забезпечення ІБ в Україні); прогнозованість (орієнтація на майбутні виклики та розробка індивідуальних підходів для нівелювання протиріч); глобальність (урахування міжнародних стандартів (Будапештська конвенція, GDPR, ISO/IEC 27001) та потенційна рецепція міжнародних практик у національне інституційне поле.

Обґрунтовано філософські та правові основи ІБ. Філософія ІБ визначає інформацію як ресурс та актив. Важливим є діалектичне співставлення категорій «безпека» та «свобода». Інформаційна безпека розглядається як прояв свободи індивіда вільно споживати дані та аналізувати їх. Правові основи полягають в опрацюванні законодавства України та міжнародних стандартів, а також аналізі діяльності міжнародних інституцій (Єврокомісія, Міжнародна організація стандартизації) у сфері ІБ.

Визначено сутність механізму правового регулювання забезпечення інформаційної безпеки (МПРЗІБ) як динамічної, багаторівневої системи правових, нормативних та інституційних засобів, що інтегрує законодавчі, виконавчі та судові органи для захисту інформаційного середовища держави, суспільства та особи.

Встановлено ключові компоненти МПРЗІБ: формальні (нормативні акти) та функціональні (контроль, моніторинг, реагування), а також чотири базові складові – нормативна, суб'єктна, правова та стратегічна бази. Визначено суб'єктну складову, що забезпечується діяльністю СБУ, РНБО, Мінцифри, Нацполіції, та нормативну базу (ЗУ «Про інформацію», ЗУ «Про кібербезпеку»).

Обґрунтовано призначення МПРЗІБ не лише як захист інтересів суб'єктів (держава, ЗМІ, громадяни), але й як активне регулювання інформаційної діяльності та розвиток інформаційного середовища шляхом інтеграції інновацій та формування «інформаційного суспільства».

Доведено недостатню ефективність національного механізму в умовах новітніх загроз через його надмірну орієнтацію на декларативну нормативність та статичність, що вимагає глибшої інтеграції технологічних, кадрових та громадських елементів.

Встановлено концептуальну кореляцію МПРЗІБ із правом людини на інформацію (ст. 5 ЗУ «Про інформацію»). Доведено, що МПРЗІБ є інтегральною частиною загальної системи прав людини, формуючи «інформаційний суверенітет особи» через забезпечення можливості одержання, використання та захисту даних. Визначено необхідність балансування між захистом інформаційного простору (суверенітету) та забезпеченням прав і свобод громадян (взаємне забезпечення прав).

Обґрунтовано принципи побудови МПРЗІБ як засади практичної реалізації політики, спрямовані на баланс між захистом інформаційної гігієни та правами людини в умовах сучасних викликів, таких як військова агресія та політика дезінформації. Надано перелік основних принципів, що будуть деталізовані: законності, захисту прав/свобод, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, пропорційності, відповідальності, безперервності.

У результаті дослідження теоретико-доктринальних та нормативно-практичних засад правового регулювання забезпечення інформаційної безпеки (ІБ) у системі публічного управління визначено сутність правового регулювання ІБ як багатофакторного феномену, що потребує узгодження конституційних гарантій (ст. 32, 34) із необхідністю національного захисту.

Доведено, що ефективність правового регулювання ІБ визначається якістю концептуальних засад та цілісної архітектури, а не кількістю нормативних актів. Обґрунтовано необхідність кореляції національних норм із глобальним контекстом (ЄС та НАТО).

Визначено три ключові теоретико-доктринальні підходи: системний (формування ціннісних орієнтирів), інституційно-нормативний (інтеграція гарантій та багатовекторний суб’єктний склад) та управлінський (пріоритет загальнонаціональних інтересів та оперативності управління в умовах агресії).

Доведено, що державне регулювання ІБ в умовах воєнного стану є організаційно-координаційним механізмом публічного управління, що ґрунтується на превенції дезінформації та забезпеченні інформаційної стійкості.

Визначено чотири основні напрями нормативно-правового інструментарію, що формують правовий базис системи:

– захист національних інтересів: доведено Законом України «Про інформацію» № 2657-XII, який закріплює ІБ пріоритетним полем державної політики;

– контроль інформаційного простору: визначено Закон України «Про доступ до публічної інформації» № 2939-VI, який встановлює багаторівневий контроль (парламентський, громадський, державний) як ключовий механізм прозорості та підзвітності;

– протидія дезінформації: визначено інституціоналізацією Центру протидії дезінформації (ЦПД) при РНБО (Указ Президента № 187/2021), що змістило фокус публічного управління на когнітивну безпеку;

– правове регулювання моделі ІБ: доведено системною архітектурою, встановленою Законом «Про основні засади забезпечення кібербезпеки України» № 2163-VIII (Національна система кібербезпеки), та довгостроковими цілями,

визначеними Стратегіями інформаційної та кібербезпеки (Укази № 685/2021 та № 447/2021).

Доведено, що сукупність нормативно-правових актів слугує основою для формування цілісної стратегії стійкості (resilience), яка інтегрує правову, технологічну та комунікаційну складові публічного управління в умовах гібридної агресії.

У **третьому розділі** – «Діагностика сучасного стану механізмів реалізації інформаційної безпеки у системі публічного управління України» проаналізовано підходи до протидії загрозам інформаційній безпеці та виявлено тенденції їх трансформації в умовах гібридних впливів. Здійснено функціональний аналіз суб'єктів забезпечення інформаційної безпеки України та визначено рівень їх взаємодії й координації. Розкрито інституційно-правові особливості реалізації механізмів інформаційної безпеки та встановлено ключові управлінські обмеження, що впливають на їх ефективність.

В умовах повномасштабної агресії та необхідності відбудови держави після війни, питання протидії загрозам інформаційній безпеці (ІБ) набуває критичної актуальності. У ході аналізу концептуальних, методичних та інструментальних підходів протидії загрозам ІБ у системі публічного управління визначено сукупність методичних підходів до протидії загрозам ІБ України, які формують декілька взаємодоповнюваних кластерних категорій, необхідних для підвищення публічно-управлінської респонсивності.

Доведено, що ключовим сегментом протидії загрозам ІБ є використання нормативно-правових та організаційних механізмів, які становлять основу державної політики. Правовою базою цього процесу визначено положення ст. 1 та ст. 17 Закону України «Про національну безпеку України» № 2469-VIII, де доведено статус кібербезпеки як невід'ємної складової загальної системи безпеки держави. Додатково визначено Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII (ст. 5, ст. 10), який доводить необхідність державно-приватного партнерства та окреслює суб'єктний склад (КМУ, РНБО, СБУ, НПУ, НБУ та ін.).

Визначено, що, попри наявність законодавчої бази, актуальною проблемою доведено залишається низька ефективність практичного застосування норм через відсутність деталізованих підзаконних актів та недостатню регламентацію взаємодії ключових суб'єктів (РНБО, СБУ, Держспецзв'язку, МВС).

У контексті технічних засобів та методології кіберзахисту визначено, що технологічна протидія ґрунтується на системах моніторингу та аналізу кіберзагроз, зокрема рішеннях класу SIEM (Security Information and Event Management), які доведено є ефективними для централізованого збору та кореляції подій безпеки. Додатково визначено необхідність застосування систем виявлення та запобігання вторгненням (IDS/IPS) для захисту критично важливих інфраструктурних об'єктів.

Доведено вагоме значення інформаційно-психологічної безпеки як методу боротьби з маніпуляціями та пропагандою. Визначено, що цей процес передбачає підвищення медіаграмотності, а також інституційні дії Центру протидії дезінформації (ЦПД) та Міністерства культури та стратегічних комунікацій. Як інноваційні засоби визначено програмне забезпечення VoxCheck та StopFake для

оперативного спростування недостовірної інформації. Результати аналізу відображено у табл. 3.

Таблиця 3

Діагностика сучасного стану механізмів реалізації інформаційної безпеки в Україні

Аспект діагностики	Ключові висновки та підходи	Проблеми та управлінські обмеження
1. Нормативно-правові та організаційні механізми	Основа державної політики. Законодавча база: ЗУ «Про національну безпеку України» (ст. 1, 17) та ЗУ «Про основні засади забезпечення кібербезпеки України» (ст. 5, 10), що закріплює державно-приватне партнерство.	Низька ефективність практичного застосування норм через відсутність деталізованих підзаконних актів та недостатню регламентацію взаємодії суб'єктів (РНБО, СБУ, Держспецзв'язку).
2. Технологічні засоби кіберзахисту	Застосування систем класу SIEM (централізований збір та кореляція подій) та IDS/IPS (виявлення та запобігання вторгненням) для критичної інфраструктури.	Застарілість технічного рівня захисту критичної інфраструктури; брак інтеграції ШІ та автоматизованих систем для проактивного захисту.
3. Інформаційно-психологічна безпека	Боротьба з маніпуляціями та пропагандою (інституційно: ЦПД, Мінкульт; інструментально: VoxCheck, StopFake).	Недостатність інтеграції обов'язкових навчальних модулів із кібергігієни у шкільні програми та ЗВО.
4. Освітні ініціативи	Підвищення цифрової грамотності (наприклад, «Дія. Цифрова освіта»).	
5. Міжнародна співпраця та інтеграція	Ефективний складник політики. Нормативна рамка: Угода про асоціацію з ЄС. Стратегічне партнерство: НАТО CCDCOE, Microsoft DART. Залучення до CRRTs та EU Cybersecurity Competence Network.	Необхідність подальшого посилення інтеграції для впровадження передових практик.
6. Співробітництво з ІТ-компаніями	Надання технологічної підтримки, підвищення стійкості, перенесення критичних даних у хмарні сховища (AWS, 2022).	Платформа MISP (Malware Information Sharing Platform) як ключовий інструмент обміну даними про загрози.

Визначено важливість освітніх ініціатив для підвищення цифрової грамотності, прикладом чого доведено є національна ініціатива «Дія. Цифрова освіта». Водночас, визначено недостатність інтеграції обов’язкових навчальних модулів із кібергігієни у шкільні програми та ЗВО. Як приклад ідеологічного та безпекового складника доведено факт блокування месенджера «Telegram» у низці закладів вищої освіти.

Доведено, що інтеграція міжнародної співпраці є екстрактивним та ефективним складником національної політики. Нормативною рамкою визначено положення Угоди про асоціацію з ЄС (пп. f) п. 2 ст. 22 Розділу ІІІ). Визначено

стратегічну співпрацю з НАТО CCDCOE та Microsoft DART. Крім того, доведено залучення України до ініціативи Cyber Rapid Response Teams (CRRTs) та інтеграцію в EU Cybersecurity Competence Network (2022 рік).

Доведено ключову роль співробітництва з провідними світовими IT-компаніями (Google, Amazon, Microsoft, Cisco), які надають технологічну підтримку, сприяють підвищенню стійкості кіберінфраструктури та забезпечили перенесення критично важливих даних у хмарні сховища (AWS, 2022). Визначено платформу MISP (Malware Information Sharing Platform) як ключовий інструмент оперативного обміну даними про кіберзагрози, що сприяє підвищенню ефективності реагування.

Визначено, що для подальшого вдосконалення системи необхідно подолати такі проблеми: недостатня адаптованість нормативної бази до швидкозмінних загроз, застарілість технічного рівня захисту критичної інфраструктури (брак ШІ та автоматизованих систем), а також недостатній рівень цифрової грамотності населення.

У результаті функціонального аналізу суб’єктного складу забезпечення інформаційної безпеки (ІБ) України в умовах великої війни та стрімкої цифровізації доведено необхідність системного підходу, що вимагає чіткої взаємодії державних інституцій, приватного сектору та міжнародної спільноти.

Доведено, що державні органи є головними суб’єктами ІБ, і кожен з них має чітко визначену компетенцію. Доведено, що Служба безпеки України (СБУ) виконує функцію контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, що закріплено у Законі України «Про Службу безпеки України» (ст. 10). СБУ виступає найвищим органом контролю та взаємодіє з іншими державними структурами. Рада національної безпеки і оборони України (РНБО) забезпечує стратегічне планування та координацію, охоплюючи сферу протидії порушень стратегічних національних інтересів в інформаційній сфері (ЗУ «Про РНБО України», ст. 4). Роль РНБО полягає у формуванні загальної безпекової парадигми. Міністерство цифрової трансформації України (Мінцифра) відіграє сутнісне значення у формуванні підвалин ІБ шляхом балансування та впорядкування даних, розвитку інформаційного суспільства та національних електронних інформаційних ресурсів (ПКМУ № 856). Мінцифра уніфікує впровадження концепцій ІБ за допомогою ІКТ.

Доведено існування тривимірної архітектурної моделі взаємодії між СБУ, РНБО та Мінцифрою, де функціонування усіх трьох інституцій спрямоване на реалізацію цілісної національної інформаційно-безпекової політики. Доведено, що Національна поліція України (Нацполіція) доповнює цю систему, зосереджуючись на притягненні до відповідальності винних за порушення використання інформаційних ресурсів та несанкціоноване використання ІКТ (ЗУ «Про Національну поліцію», ст. 28). Доведено, що Міністерство культури та стратегічних комунікацій (Мінкульт) виконує важливу роль у "соціальному" вимірі, культивуючи інформаційну політику, що включає зміцнення національно-безпекового державного профілю через інформаційно-культурні інтереси (ПКМУ № 885).

Визначено обов’язковість залучення приватного сектору через механізм

державно-приватного партнерства у сфері кібербезпеки (ст. 10 ЗУ «Про основні засади забезпечення кібербезпеки України»). Приватні компанії (ІТ-компанії, фінансові установи, оператори зв'язку) реалізують функцію захисту мереж та запобігання шахрайству.

Доведено, що громадський сектор та медіа є потужним інструментом протидії пропаганді. Їхня роль була перепрофільована прийняттям Закону України «Про медіа» № 2849-IX, яким доведено встановлення обмежень щодо змістовно-інформаційного наповнення (ст. 36) з метою запобігання поширенню матеріалів, що загрожують територіальній цілісності та національній безпеці.

Доведено, що міжнародна інтеграція (НАТО CCDCOE, Microsoft DART, Угода про асоціацію з ЄС) сприяє впровадженню передових практик, наданню технологічної підтримки та обміну новітніми аналітичними даними. Долучення до ініціативи Cyber Rapid Response Teams (CRRTs) та EU Cybersecurity Competence Network доведено як необхідний крок для посилення кіберстійкості.

У контексті аналізу методичних підходів та суб'єктного складу системи ІБ, визначено особливості реалізації механізмів забезпечення інформаційної безпеки (ІБ) в Україні, зосереджуючись на інституційно-правовій конструкції та управлінських обмеженнях. Механізм ІБ обґрунтовано трактується як системно організована сукупність норм, повноважень, процедур та інституційних акторів, спрямована на захист інформаційного простору та функціонування критичної інфраструктури.

Українська модель є гібридною, намагаючись поєднати централізовану стратегічну координацію з децентралізованою відомчою відповідальністю. Однак проведений системний аналіз доводить наявність критичних внутрішньосистемних вад, що знижують її ефективність, особливо в умовах гібридної та повномасштабної агресії.

Спостерігається низький рівень функціональної інтеграції між органами влади, що призводить до дублювання функцій, нормативної колізійності та повільної, несинхронізованої реакції на багатофакторні інформаційні загрози. Фактично, органи діють у режимі «інституційної замкненості», що унеможливлює формування єдиної інформаційної картини.

Ефективність блокується політичною фрагментацією, яка проявляється у постійній зміні пріоритетів, відсутності довгострокового бачення та втраті інституційної пам'яті. Додатковою проблемою є ресурсне та кадрове виснаження сектору ІБ, зокрема дефіцит висококваліфікованих фахівців із кіберзахисту.

Фактичний механізм реалізації інформаційної політики залишається реактивним, тоді як сучасні виклики вимагають проактивного прогнозування, сценарного планування та симуляційного аналізу.

На підставі цих обмежень обґрунтовано необхідність докорінного переходу до концепції адаптивного управління ризиками (adaptive security governance). Пропонується формалізувати трирівневу архітектуру: стратегічний рівень (прогностичний аналітичний центр), оперативний рівень (спільні міжвідомчі центри реагування) та тактичний рівень (локальні сценарії дій). Така інтегрована модель дозволить подолати вузькість компетенцій та забезпечити гнучку цифрову стійкість України.

У **четвертому розділі** – «Напрями удосконалення механізмів реалізації інформаційної безпеки у системі публічного управління» сформульовано підходи до розбудови стратегічного управління у сфері інформаційної безпеки. Обґрунтовано напрями розвитку інституційних механізмів із урахуванням зміни функцій, ролей та повноважень суб'єктів публічного управління. Запропоновано розроблення комунікаційної стратегії як інструменту підвищення стійкості системи публічного управління до інформаційних загроз та забезпечення суспільної довіри.

Напрями удосконалення механізмів реалізації інформаційної безпеки наведено у табл. 4.

Використання механізмів реалізації інформаційної безпеки у системі публічного управління дозволяє не лише оперативно реагувати на існуючі загрози, а й прогнозувати їхню появу та розвиток. Зокрема, технології ШІ та машинного навчання (ML) застосовуються для автоматизації процесів виявлення аномалій у мережевому трафіку, аналізу великих масивів даних (Big Data) про кіберінциденти та посилення проактивного захисту критичної інфраструктури. Це доведено успішною практикою Ізраїлю та США, де державна політика акцентує на технологічному домінуванні як ключовому елементі національної безпеки, що сприяє не лише обороноздатності, але й комерціалізації інноваційного потенціалу.

Таким чином, на основі аналізу міжнародних норм та практик сформульовано, що стратегічне управління забезпеченням інформаційної безпеки є багатокомпонентним, адаптивним та цілісним процесом публічного управління. Його сутність обґрунтована необхідністю синхронізації правових, інституційних та технологічних засобів для захисту суверенітету, економічних та соціальних інтересів держави в умовах цифрової трансформації. Головна мета стратегічного управління полягає у забезпеченні стійкості інформаційного середовища, підвищенні обізнаності громадян та активній підтримці національних технологічних інновацій.

Доведено, що особливості реалізації цього управління істотно варіюються: від моделі «державно-приватного партнерства» та технологічного домінування (США), через централізовану правову уніфікацію «згори донизу» з акцентом на захисті приватності (ЄС), та інституційне домінування з високим рівнем адаптивності (Ізраїль), до суворого державного контролю та цензури (Китай). Проте спільним для всіх розвинених держав є принцип інтеграції кібербезпеки та інформаційної безпеки у єдину стратегічну рамку, а також усвідомлення критичної ролі міжнародної співпраці та постійного проактивного впровадження ІКТ, зокрема ШІ та ML, для забезпечення стійкості. Це дозволяє констатувати, що ефективність стратегічного управління прямо залежить від його гнучкості та здатності до постійної інституційної та технологічної еволюції у відповідь на динаміку гібридних та цифрових загроз, а також від здатності держави сформувати національний технологічний суверенітет.

Встановлено, що розвиток інституційних механізмів забезпечення інформаційної безпеки у системі публічного управління, виявляє фундаментальний перехід від традиційної, оборонної моделі захисту до інтегрованої, проактивної архітектоніки. Це архітектурне рішення формується на основі чотирьох ключових інституційних можливостей, які детально розглянуто.

Таблиця 4

Напрями удосконалення механізмів реалізації інформаційної безпеки

Категорія удосконалення	Ключова сутність та мета	Запропоновані/Обґрунтовані механізми та світові практики
I. Стратегічне управління ІБ		
Сутність та Мета	Багатокомпонентний, адаптивний та цілісний процес синхронізації правових, інституційних та технологічних засобів. Мета: Забезпечення стійкості інформаційного середовища, підвищення обізнаності громадян та підтримка інновацій.	Технологічне домінування: Впровадження ШІ та машинного навчання (ML) для проактивного виявлення аномалій та захисту критичної інфраструктури (приклад Ізраїлю, США).
Особливості реалізації	Інтеграція кібербезпеки та ІБ у єдину стратегічну рамку. Ефективність залежить від гнучкості, постійної інституційної та технологічної еволюції.	Світові моделі: Державно-приватне партнерство (США), Централізована правова уніфікація (ЄС), Інституційне домінування (Ізраїль), Суворий державний контроль (Китай).
Ключовий висновок	Необхідність формування національного технологічного суверенітету.	
II. Розвиток інституційних механізмів		
Перехід від моделі	Перехід від традиційної, оборонної моделі захисту до інтегрованої, проактивної архітектоніки.	Забезпечення системної координації та уніфікованих міжнародних стандартів (Глобальний форум із кіберекономіки).
1. Багатостороння співпраця	Системна координація для протидії транснаціональним загрозам.	
2. Інтеграція державно-приватного партнерства (ДПП)	Ефективний розподіл ресурсів, технологій та знань між державою та приватними операторами критичної інфраструктури.	Світові приклади: США CISA, ЄС Cybersecurity Atlas.
3. Інвестиційно-технологічне та людсько-ресурсне забезпечення	Стратегічне інвестування в інновації та підготовку висококваліфікованих кадрів.	Запорука технологічного суверенітету (приклад Великої Британії, Ізраїлю).
4. Удосконалення нормативно-правової бази	Технологічна адаптація законодавства до викликів ШІ, ІР та ІКТ.	Основа для оперативного та ефективного державного реагування.

Багатостороння співпраця забезпечує системну координацію та формування уніфікованих міжнародних стандартів, що критично важливо для протидії транснаціональним загрозам (як продемонстровано на прикладі Глобального форуму із кіберекономіки).

Інтеграція державно-приватного партнерства (ДПП) спрямована на

ефективний розподіл ресурсів, технологій та знань між державним сектором і приватними операторами критичної інфраструктури, гарантуючи стійкість на внутрішньому рівні (США CISA, ЄС Cybersecurity Atlas).

Інвестиційно-технологічне та людсько-ресурсне забезпечення фокусується на стратегічному інвестуванні в інновації та підготовку висококваліфікованих кадрів, що є запорукою технологічного суверенітету та здатності до швидкої адаптації (Велика Британія, Ізраїль).

Удосконалення нормативно-правової бази передбачає технологічну адаптацію законодавства до викликів ШІ, IP та ІКТ, що є основою для оперативного та ефективного державного реагування.

Ці механізми діють синергетично, відображаючи усвідомлення того, що інформаційна безпека в умовах глобалізації є не лише функцією внутрішнього контролю, але й критичною складовою міжнародної взаємозалежності та колективної стабільності. Кожен із зазначених елементів формує інституційну матрицю, в межах якої публічне управління отримує інструменти для забезпечення цілісності інформаційного простору, захисту національних інтересів та збереження інформаційного суверенітету держави в умовах постійних геополітичних та технологічних трансформацій.

Таким чином, ефективність забезпечення інформаційної безпеки прямо пропорційна здатності системи публічного управління інтегрувати міжнародні, державно-приватні, ресурсні та правові аспекти у цілісну управлінську стратегію.

Визначено, що комунікаційна стратегія (КС) є ключовим інструментом національного управління інформаційною безпекою (ІБ). Вона визначається як механізм ефективного інформаційного захисту держави через легітимні засоби: організацію потоків інформації, стратегічні комунікації, інформаційну протидію загрозам та підтримку стійкості суспільства. Її кінцеве завдання — формування довіри до влади та відкритих джерел інформації в умовах гібридних загроз і кризових явищ.

Обґрунтовано такі концептуальні основи: побудова КС детермінується трьома основними концепціями ІБ: цифровий суверенітет (незалежність держави у сфері цифрових технологій, контроль над державною інфраструктурою, розвиток національного ПЗ, що має технологічний та економічний виміри); інформаційний нейтралітет (баланс між національною безпекою та інформаційною відкритістю, політика невтручання у міжнародні інфоконфлікти, що базується на інформаційній освіті громадян, розвитку медіаграмотності та підтримці свободи слова); стратегічні комунікації (комплексна модель кооперації «держава–суспільство», спрямована на протидію дезінформації та маніпуляціям, що інтегрує правові, технологічні, соціально-психологічні та культурні компоненти для забезпечення стійкості інформаційного простору).

Доведено, що практична реалізація КС залежить від обраного державою політичного курсу:

– моделі цифрового суверенітету (США, Франція, Китай) (США: захист критичної інфраструктури, підтримка хмарних технологій (AWS/Azure), санкціонування іноземного ПЗ (Huawei, TikTok), Франція: акцент на розвитку національного "софту" (Nextcloud, BlueMind) як альтернативи глобальним гігантам,

Китай: жорсткий державний контроль (Великий фаєрвол), запровадження національних альтернатив (WeChat, Baidu), що формує цілісну модель цифрового протекціонізму та ідеологічного контролю (Закон про кібербезпеку 2017 р.);

– моделі інформаційного нейтралітету (Швейцарія, Швеція, Канада): реалізація двовимірного формату – зовнішній політичний нейтралітет та внутрішнє забезпечення свободи слова та інформаційного доступу, закріплене в історичних та сучасних законодавчих актах (напр., Акт про свободу друку Швеції 1766 р., Конституційний акт Канади 1982 р.).

У **п'ятому розділі** – «Стратегічні напрями розвитку механізмів реалізації інформаційної безпеки у системі публічного управління» визначено механізми розвитку інформаційної безпеки держави в умовах ескалації сучасних викликів та загроз. Розкрито державно-управлінські та міжсекторальні механізми забезпечення інформаційної безпеки, орієнтовані на синергію держави, бізнесу та громадянського суспільства. Сформовано концептуальні положення розвитку механізмів інформаційної безпеки, що забезпечують довгострокову стійкість та стратегічну готовність держави до гібридних впливів.

На основі проведеного теоретико-методологічного та нормативно-правового аналізу, що був здійснений у попередніх розділах, визначено ключове завдання даного підрозділу – окреслення сучасних викликів та тенденцій, що формують основу для розроблення концептуально-стратегічного бачення розвитку механізмів інформаційної безпеки держави.

У ході дослідження доведено системний характер сучасних ризиків, серед яких домінують гібридні війни, масштабні дезінформаційні кампанії та кібератаки, спрямовані на критичну інфраструктуру. Досвід України з 2014 року доведено як показовий приклад, де інформаційні операції стали невіддільним інструментом військової агресії, що посилюється феноменом інформаційної асиметрії між державою та суспільством.

З огляду на динаміку цифрової трансформації, визначено, що стрімкий розвиток новітніх технологій, зокрема штучного інтелекту (ШІ), аналітики Big Data та технологій синтетичного контенту (deepfake), створює нову конфігурацію інформаційних загроз. Обґрунтовано, що ці інструменти, маючи подвійну природу, здатні як посилювати можливості захисту, так і радикально змінювати баланс сил, сприяючи створенню складних фішингових схем та персоналізованих дезінформаційних кампаній. Монополізація доступу до Big Data транснаціональними корпораціями, як доведено, генерує нову форму інформаційної асиметрії, що загрожує втратою контролю над критичними потоками.

Аналізуючи комунікаційне середовище, визначено, що соціальні мережі та цифрові платформи виступають подвійним чинником: вони є ареною для демократизації суспільства та водночас сприятливим середовищем для поширення маніпуляцій. Обґрунтовано, що алгоритмічна архітектура цих платформ, орієнтована на максимізацію «залучення», є ключовим каталізатором формування «інформаційних бульбашок» і поляризації громадської думки, що прискорює поширення неправдивих повідомлень.

Відтак, обґрунтовано необхідність двопланового підходу до зміцнення інформаційної безпеки, який включає технологічні засоби захисту та розвиток культури кіберстійкості. Доведено критичну важливість системного формування інформаційної гігієни та медіаграмотності у суспільстві, відзначено необхідність інтеграції освітніх програм на всіх рівнях (школи, ЗВО, державні інституції) для зниження вразливості громадян до маніпулятивних впливів. Це дозволяє сформувати свідомого користувача, який усвідомлює відповідальність за безпеку інформаційного простору.

На інституційному рівні визначено, що регуляторні та правові механізми (зокрема, Digital Services Act, Data Governance Act та національні стратегії) є необхідним підґрунтям для протидії транснаціональним загрозам. Обґрунтовано критичну важливість пошуку балансу між забезпеченням безпеки та захистом прав людини і свободи слова, що вимагає прозорості ухвалення рішень та міжнародної координації.

Доведено, що ефективна стратегія розвитку механізмів інформаційної безпеки повинна бути комплексною, адаптивною та інтегрувати технологічні, правові й поведінкові елементи для забезпечення стійкості держави та суспільства до сучасних викликів і загроз.

Сучасні гібридні загрози вимагають від держави гнучкої та комплексної системи управління інформаційною безпекою, що поєднує військово-політичні, економічні та кібернетичні інструменти. Управління інформаційною безпекою в цьому контексті ґрунтується на трьох основних моделях, кожна з яких має свої сильні та слабкі сторони.

1. Централізована модель. Цей підхід передбачає концентрацію функцій координації, планування та реагування в руках спеціально уповноважених державних органів. Його перевагами є швидкість ухвалення рішень, уніфікація стандартів і чітка вертикаль відповідальності (наприклад, досвід CISA у США, INCD в Ізраїлі та NCSC у Великій Британії). Однак, основними недоліками є ризик надмірної бюрократизації, обмежена гнучкість у міжсекторальній взаємодії та недостатня чутливість до специфіки окремих галузей. В Україні централізований підхід реалізується через діяльність РНБО та СБУ.

2. Децентралізована модель. Модель передбачає розподіл повноважень між різними державними структурами та секторними органами, де кожен суб’єкт відповідає за безпеку у межах своєї компетенції (наприклад, Німеччина, Японія, а також діяльність Мінцифри та НБУ в Україні). Ключові переваги – високий рівень адаптивності та гнучкості, можливість врахування специфіки окремих секторів та швидке реагування на локальні загрози. Основні виклики – ймовірність розрізненості стандартів, низька узгодженість між органами та ризик дублювання функцій.

3. Модель публічно-приватного партнерства (ППП). ППП передбачає спільну розробку, впровадження та контроль заходів захисту інформаційного простору державними органами та приватними суб’єктами, що володіють необхідними технічними та експертними ресурсами (наприклад, CISA у США, CiSP у Великій

Британії). Це забезпечує інтеграцію експертного потенціалу приватного сектору, оперативний обмін інформацією про загрози та швидку адаптацію до нових технологій. Водночас, ця модель вимагає чіткої нормативної бази захисту даних і забезпечення високого рівня довіри між державою та бізнесом.

Науковий аналіз доводить, що ефективна багаторівнева система управління інформаційною безпекою неможлива без синергії всіх трьох вимірів. Вона повинна поєднувати стратегічне централізоване планування та уніфікацію стандартів, адаптивну децентралізацію для врахування локальних та галузевих особливостей, а також інтеграцію технологічного потенціалу приватного сектору через ППП.

Ключова проблематика, що об’єднує всі моделі, стосується:

– координації: уникнення дублювання повноважень та конфліктів компетенцій між центральними та секторними органами;

– довіри та взаємодії: створення прозорих, законодавчо закріплених механізмів обміну конфіденційною інформацією між державою та приватним сектором;

– інтеграції стандартів: забезпечення балансу між швидким впровадженням національного законодавства та адаптацією до міжнародних стандартів кібербезпеки.

Таким чином, ефективність національної системи залежить від її здатності інтегрувати ці управлінські механізми, формуючи багаторівневу та стійку архітектуру протидії гібридним загрозам.

Сучасні реалії воєнної агресії та гібридних впливів зумовлюють нагальну потребу вдосконалення системи інформаційної безпеки України. Чинна архітектура характеризується фрагментарністю та браком системної координації між державними органами, приватним сектором і громадянським суспільством.

Ключова новизна – вибудовування синергії суб'єктів для формування цілісної, стійкої та адаптивної системи.

Стратегічний рівень визначає базові принципи, пріоритети й цілі державної політики, забезпечує демократичний контроль та інтеграцію із загальною системою нацбезпеки.

Тактичний рівень забезпечує узгодженість через міжвідомчу координацію, секторальні плани та спільні ситуаційні центри.

Операційний рівень охоплює конкретні інструменти протидії загрозам, моніторинг, кризовий менеджмент та формування безпекової культури.

Визначено чотири ключові принципи Стратегії-моделі:

– принцип проактивності: дії на випередження, прогнозної аналітики та розвиток «культури безпеки» (системна медіаосвіта) для зміцнення резистентності громадян;

– принцип багаторівневої координації: узгодженість між вертикальними (стратегія-дія) та горизонтальними (держава-бізнес-суспільство) рівнями;

– принцип гнучкості: інституційна спроможність швидко переглядати політики та нормативну базу (перехід до циклу безперервного вдосконалення),

технологічна диверсифікація (нульова довіра/zero trust), кадрова політика;

– принцип демократичного контролю: прозорість політик, громадський нагляд та дотримання міжнародних стандартів прав людини, що є запобіжником проти надмірної централізації.

Інструментами реалізації визначені наступні. Єдиний національний центр стратегічних комунікацій (ЄНЦСК) є ключовою інституцією для моніторингу загроз, міжрівневої координації та стратегічних комунікацій під час криз (за прикладом CISA/ENISA). Пропонується внесення змін до Законів України «Про основні засади забезпечення кібербезпеки України», «Про електронні комунікації», «Про захист персональних даних» та Стратегії кібербезпеки України для забезпечення гнучкості та інтеграції з європейськими стандартами (GDPR).

Авторська Концепція розвитку механізмів інформаційної безпеки України, що ґрунтується на інтегральній трирівневій моделі та принципах Стратегії-моделі національної цифрової стійкості наведена на рис. 1.

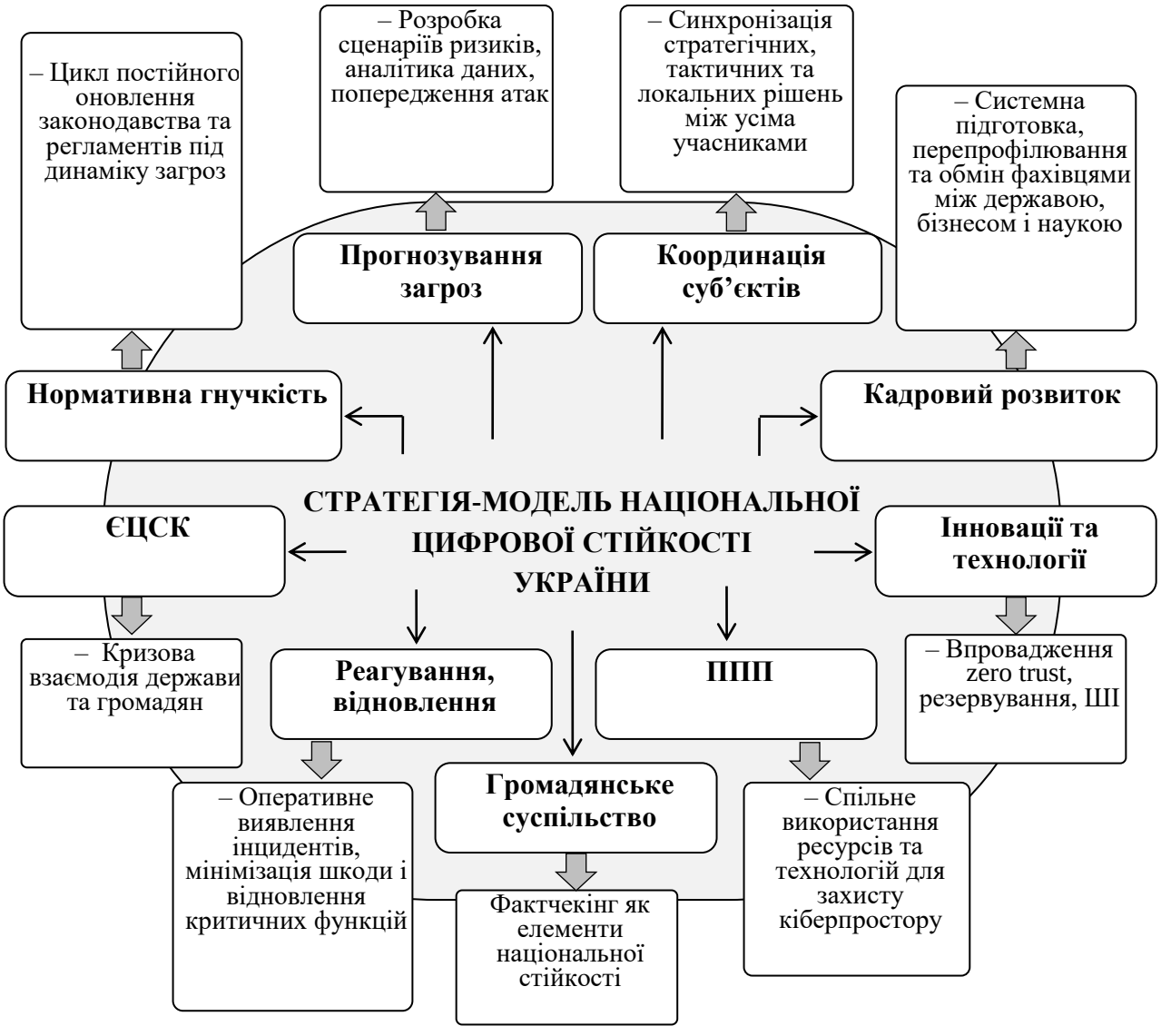

Рис. 1. Стратегія-модель національної цифрової стійкості України

Пропонується створення Національного центру кіберреагування (НЦКР) як підрозділу ЄНЦСК, мобільних оперативних груп та Єдиної платформи обміну загрозовими індикаторами (threat intelligence).

У результаті виникає динамічна екосистема – трикутник взаємодії «держава – бізнес – громадянське суспільство» – де ефективність формується виключно завдяки синергії та багаторівневій координації. Модель є «щитом», що забезпечує стійкість та здатність до саморегуляції в умовах високої змінності цифрового середовища.

ВИСНОВКИ

У ході проведеного наукового дослідження було системно розглянуто проблематику інформаційної безпеки як складової національної безпеки держави, її нормативно-правові засади та інституційні механізми реалізації. Формування висновків ґрунтується на досягненні цілей і виконанні завдань, визначених у дисертації, що дозволяє консолідувати отримані результати та окреслити основні тенденції, виклики й перспективи розвитку системи забезпечення інформаційної безпеки в Україні в контексті публічного управління.

1. Обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб’єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури та інформаційної політики); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства.

2. Уточнено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів: інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб’єкти: держава, громадянське суспільство, бізнес; об’єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості (суб’єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони: Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які

включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об’єктів правової охорони.

3. Обґрунтовано підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб’єктів – Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) – виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб’єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція).

4. Систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики.

5. Розкрито сутнісні характеристики механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування "інформаційного суспільства"); 2) теоретичне обґрунтування власного підходу до кореляції між механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового

опису дванáдцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри.

6. Систематизовано та науково обґрунтовано методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft.

7. Розроблено концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію нової системної логіки та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування).

8. Розвинуто теоретичні засади стратегічного управління інформаційною безпекою шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним

закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ).

9. Узагальнено та систематизовано сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні мережі та цифрові платформи є феноменом подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих алгоритмічних процесів); обґрунтувати необхідність інтеграції нових підходів до зміцнення кіберстійкості суспільства та сформувати двопланову модель протидії ризикам (поведінковий/освітній вимір: акцентовано на інформаційній гігієні та медіаграмотності як базових елементах зменшення вразливості громадян (приклад Швеції та Фінляндії); інституційно-правовий вимір: систематизовано нові регуляторні механізми (зокрема, Digital Services Act (DSA) та Data Governance Act (DGA) ЄС), які створюють інституційну рамку для боротьби з дезінформацією та забезпечення прозорості алгоритмів, що є прикладом збалансованого регулювання).

10. Обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та

дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік — ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA, Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам).

11. Розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством у протидії гібридним загрозам, включає чотири ключові принципи (проактивність, багаторівнева координація, гнучкість, демократичний контроль), що формують методологічний каркас стратегії-моделі, забезпечуючи перехід від реактивного до прогнозно-превентивного управління інформаційною безпекою, та інституційно-інструментальне забезпечення (створення Єдиного національного центру стратегічних комунікацій як ключової координуючої інституції, що інтегрує моніторинг загроз, міжрівневу координацію та стратегічні комунікації).

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ
Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографії:

1. Загородня А.С., Котляров В. Управління економічною безпекою: стратегічні цілі та механізми реалізації. Київ: Національний університет біоресурсів і природокористування, 2024. 200 с. *Особистий внесок: розроблено механізми управління економічною безпекою в системі публічного управління.*

Статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

2. Zbarsky, V.K., Reznik, N.P., Ostapchuk, A.D., Alekseieva, K.A., Kotliarov, V.O. (2025). Institutional and Informational Prerequisites of Secure Development of Farms in the Agrarian Economy Model of Ukraine. In: Alareeni, B., Elgedawy, I. (eds) Opportunities and Risks in AI for Business Development. Studies in Systems, Decision and Control, vol 546. Springer, Cham. https://doi.org/10.1007/978-3-031-65207-3_53. *Особистий внесок: розроблено концептуальну модель інформаційної безпеки аграрних господарств, адаптованої до умов цифрової трансформації та європейських стандартів.*

3. Rogovskii, I., Kotliarov, V., Bondarenko, V., Havrylyuk, V., Gaojiang, C., Zehao, L. (2024). Engineering and Security Management of Smart Technology of Agrotronics of Crop Production. In: Mansour, N., Bujosa Vadell, L.M. (eds) Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-75960-4_10 *Особистий внесок: формалізовано ризики кібербезпеки в агротехнологічних системах та розробці алгоритмів управління інформаційними загрозами в агровиробництві.полягає у формалізації ризиків інформаційної безпеки в агротрониках.*

4. Cherep A., Voronkova V., Cherep O., Ohrenych Y., Dashko I., Kotliarov V. (2024). Impact of Artificial Intelligence on the Level of Socio-Economic Security of Ukraine in the Conditions of Current European Integration Challenges. In: Alareeni, B., Hamdan, A. (eds) Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation. ICBT 2024. Lecture Notes in Networks and Systems, vol 1082. Springer, Cham. https://doi.org/10.1007/978-3-031-67434-1_30. *Особистий внесок: визначено критичні точки впливу штучного інтелекту на соціально-економічну стабільність України та розробці рекомендацій щодо інформаційного захисту.*

5. Kotliarov V.O., Kovalchuk O.V., Kovalchuk O.V., Kovalchuk T.V., Kovalchuk O.V. Study of Structural Imbalances in Agricultural Engineering. E3S Web of Conferences. 2022. Vol. 363. Article 01037. URL: https://doi.org/10.1051/e3sconf/202236301037. *Особистий внесок: виявлено інформаційні дисбаланси у системах агроінжинірингу та обґрунтуванні напрямів їх оптимізації з точки зору стратегічної безпеки.*

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

6. Котляров В.О. Еволюція міжнародно-політичної взаємодії у сфері інформаційних відносин. Публічне управління і адміністрування в Україні. 2023. Вип. 37. С. 76–81. DOI: 10.32782/pma2663-5240-2023.37.14

7. Котляров В.О. Комплексний підхід щодо розуміння інформаційної безпеки. Публічне управління і адміністрування в Україні. 2023. Вип. 38. С. 168–172. DOI https://doi.org/10.32782/pma2663-5240-2023.38.30

8. Котляров В.О. Особливості категорії «Інформаційна безпека» у міжнародному контексті. Наукові праці МАУП. Політичні науки та публічне управління. 2023. № 4(70). С. 21–26. DOI: 10.32689/2523-4625-2023-4(70)-3

9. Котляров В.О. Система забезпечення інформаційної безпеки України. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 2(74). С. 40–44. DOI: 10.32689/2523-4625-2024-2(74)-6

10. Котляров В.О. Інформаційне забезпечення безпеки вітчизняної та світової спільноти. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 1(73). С. 45–52. DOI: 10.32689/2523-4625-2024-1(73)-6

11. Котляров В.О. Теоретичні засади сутності та концепції

інформаційної безпеки. Наукові перспективи. 2023. № 6(36). С. 131–142. DOI: 10.52058/2708-7530-2023-6(36)-131-142

12. Котляров В.О. Формування державної політики кібергігієни. Наукові перспективи. 2025. № 7(61). С. 162–174. DOI: 10.52058/2708-7530-2025-7(61)-162-174

13. Котляров В.О. Категоріальний апарат інформаційної безпеки. Суспільство та національні інтереси. 2025. № 8(16). С. 615–629. DOI: 10.52058/3041-1572-2025-8(16)-615-629

14. Котляров В.О. Стратегічні цілі інформаційної безпеки: державне планування та механізми моніторингу ефективності. Національні інтереси України. 2025. № 8(13). С. 903–914. DOI: 10.52058/3041-1793-2025-8(13)-903-914%20

15. Котляров В.О. Інформаційна безпека України: цілі, механізми та адаптація до стандартів ЄС і НАТО. Наукові інновації та передові технології. 2025. № 8(48). С. 180–192. DOI: 10.52058/2786-5274-2025-8(48)-180-192

16. Котляров В.О. Інформаційна безпека як система правовідносин: теоретико-правовий вимір. Актуальні питання у сучасній науці. 2025. № 8(38). С. 245–259. DOI: 10.52058/2786-6300-2025-8(38)-245-259

17. Котляров В.О. Механізми раннього виявлення інформаційних атак: роль штучного інтелекту в прогнозуванні. Успіхи і досягнення у науці. 2025. № 8(18). С. 443–455. DOI: 10.52058/3041-1254-2025-8(18)-443-455

18. Котляров В.О. Інформаційна безпека в умовах глобальної взаємозалежності: міжнародно-правовий контекст та стратегічні практики. Успіхи і досягнення у науці. 2025. № 7(17). С. 474–486. DOI: 10.52058/3041-1254-2025-7(17)-474-486

19. Котляров В.О. Механізми управління репутаційними ризиками у державній інформаційній політиці. Суспільство та національні інтереси. 2025. № 9(17). С. 624–637. DOI: 10.52058/3041-1572-2025-9(17)-624-637

20. Котляров В.О. Методологічні засади дослідження інформаційної безпеки в умовах трансформаційних викликів. Наукові інновації та передові технології. 2025. № 9(49). С. 187–199. DOI: 10.52058/2786-5274-2025-9(49)-187-199

21. Котляров, В.О. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 2023, 5(71), 46-54. DOI: 10.32689/2523-4625-2023-5(71)-6

22. Котляров В.О. Правовий механізм забезпечення інформаційної безпеки: структура, принципи та інституційна модель України. Наукові перспективи. 2025. № 8 (62). С. 907-919. DOI: 10.52058/2708-7530-2025-8(62)-907-919.

23. Котляров В.О. Проблеми інформаційної боротьби у контексті забезпечення національних інтересів. Наукові інновації та передові технології. 2023, № 1(15), DOI: 10.52058/2786-5274-2023-1(15)-499-51

Статті в інших періодичних виданнях України

24. Котляров, В.О. Стратегічне управління інформаційною безпекою України. Київський економічний науковий журнал, 2024, 6, 66-69. DOI: 10.32782/2786-765X/2024-6-9

25. Котляров В.О. Стратегічне управління безпекою організацій. Mechanism of an Economic Regulation, 2024, 1 (103), 41-45. DOI: 10.32782/mer.2024.103.06

26. Котляров В.О. Особливості державної системи стратегічного планування національної безпеки в умовах інформатизації суспільства. Український журнал прикладної економіки та техніки. Том 7, № 4, 2022, С. 225–233. DOI: 10.36887/2415-8453-2022-4-33.

27. Котляров В.О. Стратегічна безпека підприємства: підходи, особливості, механізм та проблеми забезпечення. Український журнал прикладної економіки та техніки. 2022. №3. 214-222 pp. DOI: 10.36887/2415-8453-2022-3-29.

28. Котляров В.О. Поняття стратегічного управління національною безпекою. Український журнал прикладної економіки та техніки. 2023. №1. 159-165 pp. DOI: 10.36887/2415-8453-2023-1-23

29. Котляров В.О. Кібертероризм як загроза міжнародній безпеці. Український журнал прикладної економіки та техніки. 2023. №2. 314-321 pp. DOI: 10.36887/2415-8453-2023-2-45

30. Bytov V., Horbach L., Kotliarov V.O. Production as a Main Source of Consumer Goods to Society in the Current Environment. Economic Forum. 2022. Vol. 12, No. 3. P. 138–144. DOI: 10.36910/6775-2308-8559-2022-3-18. *Особистий внесок: розроблено аналітичну модель взаємозв'язку між виробничими процесами та рівнем забезпечення суспільства споживчими товарами, з урахуванням інформаційно-економічних чинників сучасного середовища.*

31. Котляров В.О. Механізм стратегічного управління економічною безпекою підприємства. Наука та освіта як основа модернізації світоустрою, 2023, № 25-01, с. 183–194. DOI: 10.30890/2709-2313.2023-25-00-024

32. Котляров, В.О. Принципи управління безпекою організацій. Mechanism of an Economic Regulation, 2023, 4 (102), 25-28. DOI: 10.32782/mer.2023.102.04

Тези конференцій:

33. Kotliarov V.O. Strategic Security of the Enterprise. 3rd International Conference on Corporation Management (ICCM-2023). 29.06.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICCM/ICCM-2023/paper/view/547

34. Reznik N.P., Kotliarov V.O. Information Security: Challenges to the Global Information Society. ICEAF-2023. 15.12.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICEAF/ICEAF-2023/paper/view/696.

Особистий внесок: класифіковано глобальні виклики інформаційній безпеці та

формуванні аналітичної моделі оцінки їх впливу на міжнародні інститути.

35. Reznik N.P., Kotliarov V.O. Особливості системи забезпечення стратегічної безпеки компанії. II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology». 15–17.11.2023. Варшава, Польща. URL: https://isu-conference.com/en/archive/modern-approaches-to-problem-solving-in-science-and-technology; PDF. *Особистий внесок: розроблено структурну модель корпоративної інформаційної безпеки з урахуванням репутаційних ризиків.*

36. Reznik N.P., Kotliarov V.O. Аспекти державної системи стратегічного планування національної безпеки України. III International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research». 29.11–01.12.2023. Амстердам, Нідерланди. URL: https://isu-conference.com/en/archive/collective-thinking-unifying-scientific-approaches-in-multifaceted-research; PDF. *Особистий внесок: змодельовано інформаційний компонент державної системи стратегічного планування та обґрунтуванні його ролі в національній безпеці.*

АНОТАЦІЯ

Котляров В.О. Механізми реалізації інформаційної безпеки у системі публічного управління. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Національний аерокосмічний університет «Харківський авіаційний інститут» – Харків, 2026.

Обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури та інформаційної політики); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства.

Поглиблено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів. Розроблено підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб'єктів – Служби безпеки України (СБУ), Ради національної безпеки та оборони України

(РНБО) та Міністерства цифрової трансформації України (Мінцифри) – виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб'єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція).

Систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики.

Концептуалізовано сутнісне призначення механізму правового регулювання ІБ. Систематизовано та науково обґрунтовано методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft.

Розроблено концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію нової системної логіки та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування).

Розвинуто теоретичні засади стратегічного управління інформаційною безпекою шляхом систематизації та компаративного аналізу міжнародних моделей. Узагальнено та систематизовано сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави. Обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки. Розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством.

Ключові слова : інформаційна безпека, національна безпека, державне управління, інформаційні загрози, правове регулювання, кібербезпека, комунікаційна стратегія, глобалізація, механізми захисту, суб’єкти безпеки.

ABSTRACT

Kotliarov Valerii. Mechanisms for the Implementation of Information Security in the System of Public Administration. – Qualified Scientific Work on the Rights of a Manuscript.

Dissertation for the Degree of Doctor of Sciences in Public Administration, specialty 25.00.02 – Mechanisms of Public Administration. – National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, 2026.

The integrative model of mechanisms for the implementation of information security in the system of public administration in Ukraine is substantiated and developed. This model, in contrast to existing ones, is based on intersectoral and communication-strategic approaches and includes: an improved institutional and legal structure for the key subjects of ensuring information resilience (NSDC, Center for Countering Disinformation; Ministry of Culture and Information Policy); criteria for the functional diagnostics of managerial limitations under martial law; a comprehensive concept of strategic management of information security that ensures synergy between the protection of critical infrastructure and the maintenance of information hygiene in civil society.

The theoretical and methodological foundations for studying information security in the system of public administration are deepened through a systemic analysis of its dual nature and the author's structuring of its key elements:

Information security as a system of social relations: A comprehensive

differentiation and structuring of its elements are carried out (subjects: state, civil society, business; object: information environment; regulation; institutions; goals), and its key features are identified (subject interdependence, civil participation, information literacy, ethics, and responsibility), which allows for a shift from static description to dynamic process management.

Information security as an object of legal protection: Domestic and foreign scientific paradigms are analyzed and systematized (criminal law, digital, administrative law), and scientifically grounded recommendations for its effective legal protection are proposed, which include the necessity of legally equating the terms "state information security" and "citizen information security" as de facto objects of legal protection.

Approaches to the institutional mechanism for ensuring information security in the system of public administration. The methodological foundations for studying information security in the system of public administration are systematized and conceptualized. The essential purpose of the mechanism of legal regulation of IS is conceptualize.

Methodological approaches to counteracting threats to Ukraine's information security under military aggression are systematized and scientifically substantiated, which is expressed in the clustering of methodological approaches to counteracting information security threats in the public administration system, highlighting five complementary clusters.

A conceptual model for transitioning to an adaptive IS architecture is developed (based on the concept of adaptive security governance), which provides for the formalization of a new systemic logic and the implementation of a three-level management structure: strategic level (creation of an analytical center for IS forecasting (focus on foresight and scenario planning)); operational level (creation of joint interagency response centers (ensuring a synchronized response)); tactical level (development of local action scenarios at the level of agencies and territorial communities (flexible response)).

The theoretical foundations of strategic information security management are developed by systematizing and comparatively analyzing international models. Contemporary challenges and trends in the development of state information security mechanisms are summarized and systematized.

The theoretical and methodological foundations for the formation of information security mechanisms are substantiated through: the systematization and critical analysis of three main managerial models (centralized, decentralized, and public-private partnership) in the context of counteracting hybrid threats, with the isolation of their advantages and limitations for Ukraine: centralized model (USA, Israel): identified as effective for rapid response and standardization, but risks of bureaucratization and duplication of powers in the Ukrainian context (SSU, NSDC) are noted; decentralized model (Germany, Japan): its advantages in flexibility and accounting for sectoral specifics (Mincifra, NBU, SSSCIP) are justified, but a key drawback is identified – the risk of disparate standards and low coordination without

proper mechanisms; public-private partnership (USA – CISA, Great Britain – CiSP): justified as a critically important mechanism for the operational exchange of threat information and the integration of private sector technological expertise, which is necessary to counteract modern information and cyber threats.

The strategy-model of national digital resilience of Ukraine is developed and scientifically substantiated. It is an integral three-level system (strategic, tactical, and operational levels) that ensures synergy between public administration, the private sector, and civil society in counteracting hybrid threats. It includes four key principles (proactivity, multi-level coordination, flexibility, democratic control) that form the methodological framework of the strategy-model, ensuring the transition from reactive to prognostic-preventive information security management, and provides for institutional and instrumental support (creation of a Unified National Center for Strategic Communications as a key coordinating institution that integrates threat monitoring, inter-level coordination, and strategic communications).

Keywords: information security, national security, public administration, information threats, legal regulation, cybersecurity, communication strategy, globalization, protection mechanisms, security subjects.

Відповідальна за друк Котляров В.О.

Підписано до друку 08.05.2026 р.
Формат 60х84 $^{1}/_{16}$. Обл.-вид. арк. 0,9.
Гарнітура Таймс. Тираж 100 прим.

Віддруковано з оригінал-макета в друкарні ФОП Леонов Д.С.
61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80