

**Хряпинський А.П., Хмиров І.М.,
Хмирова А.О., Пархоменко-Куцевіл О.І.**

МОНОГРАФІЯ

**ДЕРЖАВНА ІНФОРМАЦІЙНА
ПОЛІТИКА УКРАЇНИ В УМОВАХ
ГІБРИДНИХ ЗАГРОЗ: ТЕОРЕТИЧНІ
ОСНОВИ, ВИКЛИКИ ТА МЕХАНІЗМИ
ПРОТИДІЇ**

Переяслав – 2026

УДК 323:004-049.5(477):]355.01-0.25.26

Д 36

*Монографію розглянуто та рекомендовано до друку Вченою Радою
Університету Григорія Сковороди в Переяславі
Протокол № 5 від 24 грудня 2025 року*

Авторський колектив:

Хряпинський А.П., д.держ.упр. (передмова, розділ 1, висновки); Хмиров І.М., д.держ.упр., доцент (передмова, розділ 2, висновки), Хмирова А.О., к.держ.упр. (розділ 3, підрозділ 3.1, підрозділ 3.2), Пархоменко-Куцевіл О.І., д.держ.упр., проф. (розділ 3, підрозділ 3.3, підрозділ 3.4)

Рецензенти:

Сурай І.Г. – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника;

Яровой Т.С. – доктор наук з державного управління, доцент, професор кафедри бізнесу, адміністрування та права, ЗВО «Університет трансформації майбутнього» (УТМ), м. Чернігів

Антонова О. В. – доктор наук з державного управління, професор, завідувач кафедри публічного управління та митного адміністрування Університету митної справи та фінансів.

Д 36 Державна інформаційна політика України в умовах гібридних загроз: теоретичні основи, виклики та механізми протидії [Текст] : монографія / А.П. Хряпинський, І.М. Хмиров, А.О. Хмирова, О.І. Пархоменко-Куцевіл. Переяслав (Київська обл.): Домбровська Я.М., УГСП, 2026. 234 с. ISBN 978-617-8562-04-5

У монографії обґрунтована модель адаптивної державної інформаційної політики та комплексна протидія гібридним впливам, що враховують часовий вимір, взаємодію акторів та динаміку інформаційного протистояння. Застосування концепції «м'який як сильний» дозволяє впроваджувати гнучкі та всеохопні стратегії реагування на гібридні загрози, враховуючи їх невизначеність та складність.

Практична значущість монографії полягає у можливості використання її результатів органами державної влади для підвищення ефективності формування та реалізації інформаційної політики, а також у наданні рекомендацій щодо удосконалення національної системи інформаційної безпеки. Запропоновані підходи та моделі сприяють розвитку стійкості держави та суспільства до деструктивних інформаційних впливів, створюючи науково-методологічну базу для формування адаптивної, комплексної та ефективної державної політики у сфері інформаційної безпеки.

УДК 323:004-049.5(477):]355.01-0.25.26

ISBN 978-617-8562-04-5

© Хряпинський А.П., Хмиров І.М., Хмирова А.О.,
Пархоменко-Куцевіл О.І.
© УГСП України, 2026

ЗМІСТ

ПЕРЕДМОВА

4

**РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ
ПОЛІТИКИ В УМОВАХ ГІБРИДНОГО СЕРЕДОВИЩА**

1.1.	Сутність та еволюція державної інформаційної політики в умовах цифровізації	7
1.2.	Влада, суспільство і комунікація в інформаційну добу	15
1.3.	Концепт гібридності: природа, структура та інформаційний вимір гібридних загроз	45
1.4.	Актори гібридного впливу та інформаційні інструменти дестабілізації	68

**РОЗДІЛ 2.
СОЦІАЛЬНО-ПОЛІТИЧНИЙ ВИМІР ГІБРИДНИХ ЗАГРОЗ
ТА ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ**

2.1.	Стан інформаційної сфери та виклики гібридних впливів у публічній комунікації	86
2.2.	Рівень та механізми захисту інформаційного простору на національному і організаційному рівнях	103
2.3.	Особистісний вимір інформаційної безпеки та захисту персональних даних	122

**РОЗДІЛ 3.
СТРАТЕГІЧНІ НАПРЯМИ УДОСКОНАЛЕННЯ
ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ**

3.1.	Протидія гібридним методам впливу: принципи, підходи, моделі	138
3.2.	Національна стратегія інформаційної безпеки: цілі, пріоритети, інструменти	152
3.3.	Розвиток системи стратегічних комунікацій	162
3.4.	Концепція комплексної моделі протидії гібридним загрозам	176

ВИСНОВКИ

191

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

200

ПЕРЕДМОВА

У сучасну епоху цифровізації інформаційний простір виступає ключовим фактором розвитку державних інституцій та формування суспільної свідомості. Швидко зростання ролі інформації у всіх сферах суспільного життя супроводжується появою нових форм загроз, здатних підривати стабільність державних систем та загрожувати національній безпеці. Особливої значущості набуває проблема протидії гібридним загрозам, які поєднують традиційні методи впливу з сучасними інформаційними технологіями, створюючи складні виклики для державної інформаційної політики.

Трансформація характеру сучасних конфліктів, де інформаційне протистояння часто визначає перебіг подій, вимагає переосмислення підходів до формування державної інформаційної політики. Традиційні механізми захисту інформаційного простору виявляються недостатньо ефективними перед обличчям гібридних загроз, що постійно еволюціонують і набувають нових форм. Це створює потребу в розробці адаптивних стратегій протидії, здатних оперативно реагувати на зміни в характері та інтенсивності інформаційних атак.

Особливу увагу привертає інтеграція технологічних рішень у систему державного управління інформаційною безпекою. Наявний розрив між технічними фахівцями та управлінцями призводить до фрагментарності та зниження ефективності заходів захисту. Подолання цього розриву вимагає створення координаційної системи, яка б забезпечувала взаємодію всіх зацікавлених сторін та прийняття обґрунтованих рішень на всіх рівнях управління.

Глобальний характер сучасних інформаційних загроз підкреслює важливість міжнародної співпраці та обміну досвідом. Розвиток ефективних механізмів взаємодії між державними структурами, приватним сектором та

громадянським суспільством стає критично важливим для формування стійкої системи захисту від гібридних загроз. Водночас підвищення інформаційної культури та медіаграмотності населення розглядається як ключовий фактор національної стійкості.

Постійний розвиток інформаційно-комунікаційних технологій створює нові можливості для підвищення ефективності державного управління, але водночас породжує нові вразливості. Зростання складності та масштабності інформаційних атак, використання штучного інтелекту для генерації дезінформації та розвиток технологій глибинних фейків формують новий ландшафт загроз, що потребує постійного вдосконалення системи інформаційної безпеки.

Комплексний підхід до протидії гібридним загрозам передбачає врахування як глобального контексту, так і специфіки національного середовища. Пріоритетними завданнями державної політики стають захист критичної інформаційної інфраструктури, забезпечення інформаційного суверенітету та протидія деструктивним інформаційним впливам. Успішність цих заходів залежить від здатності держави координувати ресурси всіх зацікавлених сторін та створювати ефективну екосистему інформаційної безпеки.

Наукова новизна представленої роботи полягає у розробці моделей адаптивної державної інформаційної політики та комплексної протидії гібридним впливам, що враховують часовий вимір, взаємодію акторів та динаміку інформаційного протиборства. Застосування концепції «м'який як сильний» дозволяє впроваджувати гнучкі та всеохопні стратегії реагування на гібридні загрози, враховуючи їх невизначеність та складність.

Практична значущість монографії полягає у можливості використання її результатів органами державної влади для підвищення ефективності формування та реалізації інформаційної політики, а також у наданні

рекомендацій щодо удосконалення національної системи інформаційної безпеки.

Запропоновані підходи та моделі сприяють розвитку стійкості держави та суспільства до деструктивних інформаційних впливів, створюючи науково-методологічну базу для формування адаптивної, комплексної та ефективної державної політики у сфері інформаційної безпеки.

