МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут захисту інформації
Кафедра публічного управління та адміністрування

галузь знань 28 «Публічне управління та адміністрування» спеціальність 281 «Публічне управління та адміністрування»
освітня програма «Публічне управління та адміністрування»
рівень освіти другий «Магістр»

Форма навчання: денна

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: Інформаційно-психологічна війна в Україні: стан проблеми і шляхи подолання наслідків

Виконав: студент 6 курсу,
групи ПУДМ-61
Юрій ЧЕРЕДНІЧЕНКО

Керівник, доктор наук з державного управління, доктор медичних наук, почесний академік НАПН України, професор ДУІКТ
Олег ПАНЧЕНКО

Рецензент
(*прізвище та ініціали)*

Київ – 2025

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ВІЙНИ 7

1.1. Поняття та еволюція ІПВ 7

1.2. Механізми психологічного впливу 13

1.3. Нормативно-правові засади та методологія дослідження 18

РОЗДІЛ 2. АНАЛІЗ УПРАВЛІНСЬКИХ АСПЕКТІВ У СФЕРІ ІПВ 27

2.1. Український контекст управління 27

2.2. Ключові ворожі наративи в Україні 37

2.3. Інституційна спроможність протистояння ІПВ в Україні 45

РОЗДІЛ 3. ШЛЯХИ ПОДОЛАННЯ НАСЛІДКІВ ІПВ В УКРАЇНІ: ПОЛІТИКА, ІНТЕРВЕНЦІЇ, ОЦІНЮВАННЯ 54

3.1. Цільова модель протидії ІПВ 54

3.2. План впровадження політики подолання наслідків ІПВ 62

3.3. Прогноз наслідків ІПВ (2025–2027) 70

ВИСНОВКИ 77

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 81

ВСТУП

Повномасштабна війна Російської Федерації в Україні, що розгортається у форматі гібридної війни, актуалізувала якісно новий рівень загроз у сфері національної безпеки. Серед них особливе місце посідає інформаційно-психологічна війна (далі – ІПВ) як комплекс цілеспрямованих впливів на масову свідомість, індивідуальні установки, соціальні практики та інституційну довіру. У сучасних умовах ІПВ в Україні є не епізодичним явищем, а сталою реальністю, що супроводжує воєнні, політичні, економічні та соціальні процеси. З точки зору публічного управління вона формує особливе середовище ризику, в якому державні рішення можуть бути дискредитовані, суспільна згуртованість – підірвана, а психоемоційна стійкість громадян – істотно послаблена.

Актуальність дослідження зумовлена трьома взаємопов'язаними факторами. По-перше, ІПВ системно впливає на ключові показники державної керованості: довіру до інститутів влади, легітимність політик, готовність громадян до виконання рішень та участі в обороні країни. По-друге, посилюється технологічний вимір ІПВ: соціальні мережі, цифрові платформи, алгоритмічні механізми рекомендацій, а також інструменти штучного інтелекту збільшують швидкість і масштаб поширення дезінформації та маніпуляцій. По-третє, ІПВ має виразні довгострокові наслідки для людського капіталу держави: виснаження, тривожність, зниження критичного мислення, формування інформаційної залежності або апатії. Відтак протидія ІПВ та подолання її наслідків потребують не лише безпекових, а й управлінських рішень – комплексної державної політики, здатної поєднати правові, організаційні, комунікаційні та соціально-реабілітаційні інструменти.

Водночас наукова та практична дискусія нерідко зосереджується на описі психологічних ефектів або медіатехнологічних механізмів,

залишаючи поза увагою питання державної спроможності: інституційної координації, стратегічного планування, управління ризиками, моніторингу та оцінювання ефективності політики. Саме цей управлінський фокус відповідає змісту спеціальності «Публічне управління та адміністрування» та дозволяє розглядати ІПВ як об’єкт державної політики у сфері інформаційної та інформаційно-психологічної безпеки. Наукові підходи, запропоновані О. А. Панченком у дослідженнях про державне управління інформаційною безпекою в умовах турбулентності [1], роль масових комунікацій у державній інформаційній політиці, а також системний підхід до ментальної стійкості суспільства, є важливою теоретико-методологічною основою цієї роботи. Додатково людиноцентричний вимір державної політики інформаційної безпеки доцільно підсилювати положеннями І. В. Кукіна щодо державного управління інформаційною безпекою особистості, а також напрацюваннями І. П. Коваля, присвяченими аналізу каналів поширення дезінформації в Україні, та М. В. Сидоренка, який розглядає приклади інформаційних операцій проти нашої держави та їхні наслідки.

Мета дослідження – здійснити комплексний аналіз інформаційно-психологічної війни в Україні як сучасної реальності, оцінити стан проблеми з позицій публічного управління та обґрунтувати шляхи удосконалення державної політики подолання наслідків ІПВ.

Для досягнення зазначеної мети поставлено такі завдання:

1) уточнити сутність і еволюцію ІПВ у контексті гібридної війни та визначити ключові механізми психологічного впливу і соціальні індикатори наслідків;

2) проаналізувати нормативно-правові засади України у сфері протидії ІПВ і визначити методологічні підходи до управлінського аналізу проблеми;

3) оцінити український контекст управління у сфері ІПВ, виокремити ключові ворожі наративи, вразливі групи та ризики для національної безпеки;

4) визначити рівень інституційної спроможності держави протистояти ІПВ, встановити основні розриви у координації, ресурсах та процедурах;

5) розробити цільову модель протидії ІПВ і запропонувати комплекс управлінських інтервенцій;

6) сформувати план упровадження державної політики подолання наслідків ІПВ та обґрунтувати прогноз розвитку ситуації на 2025–2027 роки.

Об’єктом дослідження є державна політика та система публічного управління у сфері забезпечення інформаційної й інформаційно-психологічної безпеки України в умовах гібридної війни.

Предметом дослідження є управлінські механізми, інституційні інструменти та практики протидії ІПВ в Україні, а також підходи до подолання її соціально-психологічних і комунікаційних наслідків на державному та суспільному рівнях.

Методологія дослідження базується на поєднанні загальнонаукових і спеціальних методів публічного управління: аналізу та синтезу, системного і інституційного підходів, порівняльного аналізу, контент-аналізу інформаційних матеріалів, а також прикладних аналітичних інструментів (PESTLE, SWOT, GAP). Для обґрунтування управлінських пропозицій застосовано елементи сценарного прогнозування та підходи до моніторингу й оцінювання ефективності державної політики.

Наукова новизна роботи полягає у формуванні комплексного управлінського бачення ІПВ в Україні як багаторівневої загрози, що потребує інтегрованої державної відповіді; у визначенні ключових інституційних розривів у системі протидії ІПВ; а також у розробленні

цільової моделі та практичного плану державних інтервенцій із урахуванням посилення медійної гігієни, інформаційної стійкості та ментального здоров'я населення.

Практичне значення отриманих результатів полягає в можливості використання запропонованих рекомендацій органами державної влади та місцевого самоврядування, профільними структурами сектору безпеки і оборони, освітніми та комунікаційними інституціями для підвищення ефективності координації та реалізації політики інформаційно-психологічної безпеки. Результати можуть бути застосовані також у навчальних програмах із публічного управління, стратегічних комунікацій та національної стійкості.

Таким чином, дослідження теми «Інформаційно-психологічна війна в Україні: стан проблеми і шляхи подолання наслідків» є своєчасним і практично значущим для розвитку теорії та практики публічного управління в умовах воєнної турбулентності, оскільки спрямоване на посилення державної спроможності захищати особистість, суспільство та інституційну стабільність держави від деструктивних інформаційно-психологічних впливів [1].

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ВІЙНИ

1.1. Поняття та еволюція ІПВ

Інформаційно-психологічний вплив (ІПВ) – це цілеспрямований процес впливу на свідомість, емоції та поведінку людей за допомогою інформаційних засобів і психологічних механізмів. Його сутність полягає у формуванні певних установок, переконань або дій, що відповідають інтересам суб'єкта впливу. Основною метою ІПВ є зміна або коригування поглядів, емоційного стану та поведінки аудиторії таким чином, щоб досягти бажаного результату – від підтримки певних рішень до формування лояльності чи мотивації до дії [1, с. 112].

Характерними ознаками інформаційно-психологічного впливу є його цілеспрямованість, тобто орієнтація на конкретну групу або особу з чітко визначеними цілями. Він реалізується через різноманітні інформаційні канали – засоби масової інформації, соціальні мережі, рекламу, комунікаційні платформи – і використовує психологічні механізми, такі як емоційне зараження, навіювання, маніпуляція, створення когнітивних дисонансів. Завдяки цьому ІПВ здатний впливати не лише на раціональне мислення, а й на підсвідомі реакції людини. Узагальнені характерні ознаки ІПВ наведено в таблиці 1.1, а основні сфери його застосування – у таблиці 1.2.

Таблиця 1.1 систематизує ключові властивості ІПВ: від прихованості та адаптивності до комплексності методів, що поєднують інформаційні й психологічні технології. З точки зору публічного управління ці ознаки важливі тим, що визначають складність державної відповіді: органи влади мають діяти не лише реактивно, а й превентивно, вибудовуючи системи

раннього виявлення впливів, кризових комунікацій та стійкості до маніпуляцій.

Таблиця 1.1

Характерні ознаки інформаційно-психологічного впливу

Ознака	Пояснення ознаки
Цілеспрямованість	Орієнтація на конкретну аудиторію або особу з чітко визначеними цілями.
Використання інформаційних каналів	Застосування ЗМІ, соціальних мереж, реклами, комунікаційних платформ для поширення впливу.
Психологічні механізми	Використання навіювання, маніпуляції, емоційного зараження, когнітивних дисонансів.
Комплексність	Поєднання інформаційних та психологічних методів для досягнення ефекту.
Прихованість	Часто здійснюється непомітно для об’єкта впливу, щоб уникнути опору.
Адаптивність	Здатність змінювати форми та методи залежно від реакції аудиторії.

Таблиця 1.2

Сфери застосування інформаційно-психологічного впливу

Сфера застосування	Особливості використання ІПВ
Політика	Формування громадської думки, створення іміджу лідерів, дискредитація опонентів, вплив на електорат.
Бізнес	Просування товарів і послуг, створення позитивного бренду, стимулювання попиту через рекламу та маркетинг.
Соціальні мережі	Швидке поширення інформації, формування трендів, вплив на поведінку користувачів через контент і алгоритми.
Військова сфера	Деморалізація противника, підвищення бойового духу власних сил, управління інформаційним простором під час конфліктів.

Водночас таблиця 1.2 демонструє, що ІПВ не обмежується виключно воєнним контекстом. У політиці він використовується для

формування громадської думки, підтримки іміджу лідерів або дискредитації опонентів. У бізнесі ІПВ допомагає просувати товари та послуги, створювати позитивний бренд-образ і стимулювати споживчий попит. Соціальні мережі стали одним із найпотужніших інструментів такого впливу, адже дозволяють швидко поширювати інформацію, формувати тренди і створювати стійкі інформаційні «бульбашки», що підсилюють емоційні реакції аудиторії.

Особливо значущим ІПВ є у військовій сфері та в умовах гібридної війни, де інформаційний простір перетворюється на повноцінний театр протиборства. У такому середовищі ІПВ застосовується для деморалізації противника, підриву довіри до державних інституцій, розхитування соціальної згуртованості, нав'язування вигідної противнику картини реальності. Прикладами є масове розповсюдження фейкових повідомлень про нібито великі втрати або відступи військ, створення постановочних відео «здачі в полон» чи «знищення техніки», а також цілеспрямовані кампанії із поширення панічних настроїв серед цивільного населення через соціальні мережі та месенджери [2]. Такі практики одночасно б'ють по моральному стану війська й по довірі громадян до офіційної інформації, ускладнюючи реалізацію державної політики в умовах воєнного часу.

Еволюція інформаційно-психологічного впливу відображає глибокі зміни у способах комунікації та технологічних можливостях суспільства. На ранніх етапах розвитку людства основними методами впливу були усна пропаганда та друковані засоби масової інформації. Вони дозволяли поширювати ідеї та формувати громадську думку, однак мали обмежене охоплення і залежали від фізичних каналів комунікації. З появою радіо та телебачення масштаби впливу значно зросли, адже ці технології дали змогу одночасно звертатися до мільйонів людей, використовуючи силу образів і звуку для емоційного впливу [2].

Подальший розвиток технологій радикально змінив характер ІПВ. Інтернет став ключовим інструментом, що забезпечив глобальну доступність інформації та інтерактивність комунікації. Соціальні мережі відкрили нові можливості для таргетованого впливу, адже дозволяють не лише поширювати контент, а й аналізувати поведінку користувачів. Алгоритми персоналізації стали важливим елементом сучасного інформаційного простору: вони формують стрічку новин кожного користувача, підбираючи контент відповідно до його інтересів, що значно підсилює ефективність психологічного впливу. Узагальнені етапи еволюції ІПВ наведено у таблиці 1.3.

Як видно з таблиці 1.3, сучасний технологічний етап характеризується використанням Big Data, штучного інтелекту, психологічного таргетингу та автоматизації впливу. Збирання і аналіз великих масивів даних про поведінку людей, їхні уподобання та емоційні реакції дозволяє максимально точно формувати «пакети» повідомлень для різних соціальних груп. Штучний інтелект використовують для створення персоналізованих текстів, зображень, відео, а також для автоматизації комунікацій через чат-боти. Психологічний таргетинг, що базується на аналізі особистісних характеристик, дозволяє впливати на людей максимально точково, використовуючи їхні емоційні тригери [3, с. 76].

Усе це робить сучасний інформаційно-психологічний вплив більш технологічним, масштабним і водночас менш помітним для об’єкта впливу.

Таблиця 1.3

Етапи еволюції ІПВ

Етап	Характеристика	Приклади
Класичний (до XX ст.)	Усна пропаганда, друковані ЗМІ; обмежене охоплення, прямий вплив через слово та текст.	Проповіді, політичні мітинги, газети, листівки.
Мас-медіа (XX ст.)	Радіо, телебачення; масштабне охоплення аудиторії, використання образів і звуку для емоційного впливу.	Радіопередачі часів Другої світової війни, телевізійні політичні дебати, рекламні ролики.
Інтернет-епоха (кінець XX – початок XXI ст.)	Глобальна доступність інформації, інтерактивність, перші онлайн-комунікації.	Веб-сайти новин, електронна пошта, перші форуми та чати.
Соціальні мережі (XXI ст.)	Таргетований вплив, алгоритми персоналізації, формування інформаційних «бульбашок».	Facebook, Twitter, Instagram, вірусні меми, таргетована реклама.
Сучасний технологічний етап	Використання Big Data, штучного інтелекту, психологічного таргетингу, автоматизація впливу.	Chatbots, deepfake-відео, алгоритми TikTok, політичні кампанії з AI-аналітикою.

В умовах гібридної війни ІПВ перетворюється на комплексну систему засобів тиску, де інформаційні та психологічні технології взаємодіють із силовими, економічними та політичними інструментами. У цьому контексті доцільно розглядати не «відмінності» ІПВ від суміжних явищ, а основні засоби інформаційно-психологічного впливу, які застосовуються противником для досягнення стратегічних цілей. Серед таких засобів у гібридній війні виділимо насилля/тероризм, пропаганду та дезінформацію (відповідно до підходів, представлених у сучасних дослідженнях проблематики турбулентного часу). Саме ці інструменти створюють системний ефект залякування, дезорієнтації, підриву довіри і фрагментації суспільства.

Інформаційно-психологічна операція є одним із практичних проявів ІПВ у воєнному середовищі. Її можна визначити як сплановану кампанію з поширення спеціально підібраної інформації з метою впливу на емоції, думки та поведінку цільової аудиторії. Вона орієнтована на породження конкретних управлінськи значущих наслідків: паніки, страху, соціальної апатії, протестної мобілізації або підриву довіри до органів влади. У державницькому вимірі ІПСО слід розглядати як інструмент гібридної війни, що діє поряд із пропагандою та дезінформацією і спрямований на отримання політичних, військових чи соціальних переваг.

З огляду на це логічно змінити зміст табл. 1.4 і подати її як узагальнення засобів ІПВ у гібридній війні, а не як «відмінності». Така логіка краще відповідає предмету дослідження і управлінському підходу: державі важливо не стільки формально розділити терміни, скільки розуміти набір інструментів противника і вибудовувати відповідні контрзаходи. У запропонованій логіці таблиця 1.4 містить: пропаганду (як інструмент формування лояльності/ ворожості), дезінформацію (як інструмент дезорієнтації та хаотизації), ІПСО (як комплексні кампанії з чіткими оперативними цілями).

Таблиця 1.4

Основні засоби інформаційно-психологічного впливу в умовах гібридної війни

Поняття	Мета	Роль у структурі ІПВ	Приклад
Пропаганда	Формування потрібних ідеологічних/ціннісних установок, легітимація власних дій і делегітимація противника	Використовується як інструмент довготривалого впливу на масову свідомість: створює потрібні образи “свій/чужий”, підсилює лояльність або ворожість, готує ґрунт для інших впливів	Меседжі про “нелегітимність влади”, “зраду союзників”, “невідворотність поразки”

Дезінфор-мація	Навмисне введення в оману, дезорієнтація та хаотизація сприйняття подій	Використовується як тактичний інструмент ІПВ: провокує паніку, сумніви, недовіру до офіційних джерел, розколює суспільство, зміщує фокус уваги	Фейкові новини про “масові втрати”, “відступи”, “катастрофи”, “розкол у керівництві”
ІПСО	Досягнення конкретних оперативно-стратегічних цілей через комплексний психологічний і інформаційний тиск	Є організованою формою реалізації ІПВ у воєнній/гібридній площині: поєднує пропаганду, дезінформацію, маніпуляції, інформаційні вкиди, роботу з емоціями та поведінковими моделями	Кампанії з деморалізації військ, дискредитації командування, підриву довіри до державних рішень

Таким чином, ІПВ як соціально-комунікаційне явище пройшов шлях від класичних форм впливу через слово і друк до високотехнологічних інструментів, які спираються на алгоритми, великі дані та штучний інтелект. Для України, що протистоїть гібридній війні, ІПВ є не лише психологічним або медійним феноменом, а й предметом публічного управління. Його ознаки, канали та засоби визначають характер державної політики у сфері інформаційної та інформаційно-психологічної безпеки. Відповідно, теоретичне осмислення поняття та еволюції ІПВ створює основу для подальшого управлінського аналізу українського контексту, ключових ворожих наративів і оцінки інституційної спроможності держави протистояти цим впливам, що буде розкрито в наступних підрозділах роботи.

1.2. Механізми психологічного впливу

Психологічні механізми інформаційно-психологічного впливу ґрунтуються на глибинних особливостях людського сприйняття,

когнітивних процесів та емоційних реакцій (табл. 1.5). Вони використовують природні схильності людини до спрощення інформації, емоційного реагування та соціальної взаємодії, що робить їх надзвичайно ефективними у сучасному інформаційному середовищі.

Таблиця 1.5

Механізми інформаційно-психологічного впливу

Механізм	Значення	Приклад
Навіювання	Передача інформації без критичного осмислення, створення установок.	Використання авторитетних джерел для формування довіри.
Маніпуляція	Прихований вплив через викривлення фактів або емоційні акценти.	Реклама, що перебільшує переваги товару.
Емоційне зараження	Поширення емоцій через контент, що викликає страх, паніку чи ентузіазм.	Панічні повідомлення у соцмережах під час кризи.
Когнітивний дисонанс	Використання суперечливих повідомлень для зміни поведінки.	Поширення інформації, що суперечить усталеним переконанням.
Фреймінг	Вплив через формулювання проблеми та акценти в подачі інформації.	Подання економічної кризи як «виклику» або «катастрофи».
Праймінг	Підготовка свідомості до певного способу інтерпретації інформації.	Використання ключових слів перед основним повідомленням.
Ефект повторення	Часте повторення повідомлення для закріплення у свідомості.	Слогани у політичних кампаніях або рекламі.

Одним із ключових механізмів є навіювання та маніпуляція. Навіювання передбачає створення умов, за яких людина некритично сприймає інформацію, особливо якщо вона подається авторитетним джерелом або в умовах емоційного напруження. Маніпуляція, у свою чергу, полягає у прихованому впливі на свідомість через викривлення фактів, використання емоційно забарвлених слів, створення асоціативних зв’язків [11, с. 34]. Наприклад, у політичних кампаніях часто застосовують

маніпулятивні техніки, щоб сформувати позитивний образ кандидата або дискредитувати опонента.

Механізми інформаційно-психологічного впливу Емоційне зараження є ще одним потужним інструментом, що полягає у швидкому поширенні емоцій через інформаційний контент. Повідомлення, які викликають страх, паніку або ентузіазм, здатні охоплювати великі групи людей, формуючи колективні настрої. Це особливо помітно у кризових ситуаціях або під час воєнних конфліктів, коли емоційні повідомлення можуть призвести до масової паніки або, навпаки, мобілізації населення.

Когнітивний дисонанс використовується для зміни поведінки шляхом створення суперечливих повідомлень, що змушують людину переглядати свої погляди, аби зняти внутрішнє напруження. Наприклад, коли людина стикається з інформацією, яка суперечить її переконанням, вона може змінити свою позицію, щоб уникнути психологічного дискомфорту [11, с. 41].

Фреймінг та праймінг є одними з найважливіших психологічних механізмів інформаційно-психологічного впливу, оскільки вони формують не лише те, що людина бачить, але й те, як вона це інтерпретує. Фреймінг (від англ. *framing*) полягає у виборі певного «рамкового» контексту для подання інформації. Це означає, що одна й та сама подія може бути представлена під різними кутами зору, що суттєво впливає на емоційну реакцію та поведінку аудиторії. Наприклад, повідомлення про економічну кризу може бути подане як «тимчасові труднощі, які стимулюють інновації» або як «катастрофа, що призведе до масового безробіття». У першому випадку формується оптимістичний настрій і готовність до дій, у другому — страх і пасивність [12, с. 103].

Праймінг (від англ. *priming*) працює більш тонко: він готує свідомість до певного способу сприйняття інформації ще до того, як основне повідомлення буде отримане. Це може бути досягнуто через

використання ключових слів, образів або попередніх сигналів, які активують у пам’яті певні асоціації. Наприклад, якщо перед новиною про економічну ситуацію показати сюжет про успішні стартапи, аудиторія буде схильна сприймати кризу як можливість для розвитку. Якщо ж попередньо продемонструвати кадри закритих підприємств і черг на біржі праці, реакція буде зовсім іншою — домінуватиме відчуття загрози та безнадії [12, с. 105].

Ці механізми активно використовуються у політичних кампаніях, рекламі та медіа для формування потрібних установок. Вони не змінюють фактичний зміст інформації, але впливають на її інтерпретацію, що робить їх надзвичайно ефективними і водночас малопомітними для пересічного споживача. У сучасних умовах алгоритми соціальних мереж підсилюють ефект фреймінгу та праймінгу, підбираючи контент відповідно до попередніх уподобань користувача, що створює інформаційні «бульбашки» і ще більше закріплює задані рамки сприйняття.

Ефект повторення також відіграє важливу роль. Чим частіше повідомлення повторюється, тим більше воно сприймається як істина, навіть якщо його зміст є сумнівним. Цей механізм активно використовується у пропаганді та рекламі, де повторювані слогани закріплюють у свідомості певні асоціації.

Операціоналізація індикаторів наслідків інформаційно-психологічного впливу (див. табл. 1.6) є ключовим етапом у дослідженні його ефективності, адже вона дозволяє перевести абстрактні поняття на рівень вимірюваних показників. Це важливо для того, щоб зрозуміти, наскільки глибоко інформаційні кампанії або психологічні операції впливають на суспільство, його емоційний стан, поведінку та соціальні зв’язки [12, с. 110].

Таблиця 1.6

Основні індикатори наслідків інформаційно-психологічного впливу

Індикатор	Суть	Методи вимірювання	Приклади даних
Рівень стресу та тривоги	Емоційний стан населення під впливом інформаційних атак	Психометричні шкали (Бека, Гамільтона), соціологічні опитування, аналіз пошукових запитів	Зростання запитів «паніка», «депресія», «тривога»
Довіра до інституцій	Ставлення до влади, армії, медіа, міжнародних організацій	Соціологічні дослідження, індекси довіри	Зниження рейтингу довіри до уряду або ЗСУ
Медіагігієна	Здатність критично сприймати інформацію	Опитування про перевірку джерел, використання фактчекінгу, тести на медіаграмотність	Низький відсоток перевірки новин перед поширенням
Соціальна згуртованість	Рівень єдності та готовності до колективних дій	Аналіз активності в громадах, участь у волонтерських рухах, моніторинг соцмереж	Зростання поляризації, конфліктів у коментарях

Одним із найважливіших індикаторів є рівень стресу та тривоги в населення. Він може бути оцінений за допомогою психометричних методів, таких як шкала тривожності Бека або шкала депресії Гамільтона, а також через масові соціологічні опитування. У сучасних умовах додатковим джерелом даних є аналіз цифрових слідів — наприклад, частота пошукових запитів у мережі, пов’язаних із симптомами тривожності, паніки чи депресії. Зростання таких запитів часто корелює з інформаційними атаками або кризовими подіями.

Другим важливим показником є рівень довіри до інституцій — державних органів, армії, медіа, міжнародних організацій. Його вимірюють чеірез регулярні соціологічні дослідження та індекси довіри.

Зниження цього показника може свідчити про успішність інформаційно-психологічних операцій, спрямованих на дискредитацію влади або підрив легітимності державних структур [13].

Медіагігієна є ще одним критичним індикатором, що відображає здатність населення критично сприймати інформацію. Вона оцінюється за частотою перевірки джерел, використанням фактчекінгових ресурсів, рівнем медіаграмотності та критичного мислення. Низький рівень медіагігієни робить суспільство більш вразливим до маніпуляцій, фейків та пропаганди.

Соціальна згуртованість показує, наскільки суспільство готове до колективних дій і взаємодії. Її можна оцінити за показниками активності в громадах, участі у волонтерських рухах, рівнем поляризації в соціальних мережах та готовністю до спільних ініціатив [13]. Зниження згуртованості часто є наслідком інформаційних атак, спрямованих на розкол суспільства, створення конфліктів між групами та підрив єдності.

Таким чином, операціоналізація індикаторів дозволяє не лише фіксувати наслідки інформаційно-психологічного впливу, а й прогнозувати ризики для національної безпеки та розробляти стратегії протидії.

1.3. Нормативно-правові засади та методологія дослідження

В Україні питання інформаційної та інформаційно-психологічної безпеки, а також протидії інформаційно-психологічним впливам регулюються комплексом законодавчих актів, стратегічних документів і підзаконних нормативів. Саме вони створюють рамку для формування державної політики у сфері протидії ІПВ, визначають повноваження суб’єктів публічного управління та встановлюють базові стандарти захисту інформаційного простору. Такий підхід загалом корелює з

науковими підходами О. А. Панченка, який розглядає інформаційно-психологічну безпеку як складову національної безпеки та як об’єкт цілеспрямованого державного управління в умовах турбулентності [1].

Методологія дослідження

Методологія дослідження інформаційно-психологічної війни в Україні ґрунтується на поєднанні загальнонаукових і спеціальних методів публічного управління, психології та комунікаційних студій. В основі лежить системний підхід, який відповідає позиції О. А. Панченка щодо розгляду інформаційно-психологічної безпеки як складної багаторівневої системи, де взаємодіють державні інституції, суспільство, медіа, міжнародні актори та індивідуальні суб’єкти.

Дослідницький дизайн передбачає уточнення об’єкта та предмета, формулювання дослідницьких питань і гіпотез, а також операціоналізацію індикаторів, які відображають як управлінські, так і соціально-психологічні аспекти ІПВ (рівень довіри до інститутів, поширеність ворожих наративів, індикатори стресу й тривоги, показники медіагігієни тощо). Для цього застосовується поєднання кількісних та якісних методів, що дозволяє отримати цілісну картину явища.

Кількісний вимір реалізується через аналіз статистичних даних, соціологічні опитування, а також контент-аналіз медіа-матеріалів і повідомлень у соціальних мережах. Контент-аналіз дає змогу виявляти маніпулятивні техніки, домінуючі наративи, темпи поширення пропагандистських і дезінформаційних матеріалів. Соціологічні опитування дозволяють оцінити суб’єктивні показники – рівень довіри, відчуття небезпеки, стресу, згуртованості – серед різних груп населення. Узагальнення основних методів, що застосовуються в дослідженні, подано в табл. 1.7.

Таблиця 1.7

Методи дослідження інформаційно-психологічного впливу

Метод дослідження	Характеристика методу	Приклади застосування
Контент-аналіз	Аналіз змісту інформаційних матеріалів для виявлення маніпулятивних технік.	Дослідження новинних статей, постів у соцмережах.
Соціологічні опитування	Вимірювання ставлення, рівня довіри, стресу та тривоги серед населення.	Опитування щодо довіри до медіа або державних інституцій.
Психометричні тести	Оцінка психологічного стану (тривожність, стрес, депресія).	Використання шкали Бека або Гамільтона.
Аналіз Big Data	Вивчення цифрових слідів: пошукові запити, активність у соцмережах.	Аналіз трендів у Google, Twitter, Facebook.
Експертні інтерв'ю	Отримання оцінок від фахівців у сфері інформаційної безпеки та психології.	Інтерв'ю з аналітиками, психологами, кіберекспертами.
Мережевий аналіз	Виявлення бот-мереж, інформаційних кластерів та каналів поширення фейків.	Аналіз структури поширення контенту у Telegram чи Twitter.
Експериментальні методи	Перевірка реакцій на різні типи інформаційних повідомлень у контрольних групах.	Лабораторні експерименти з впливом емоційних тригерів.

Для поглибленого розуміння контексту явищ і управлінських рішень використовуються якісні методи: експертні інтерв'ю з фахівцями у сфері інформаційної безпеки, стратегічних комунікацій, психології, а також кейс-стаді конкретних інформаційних операцій в Україні. Мережевий аналіз дає змогу виявляти бот-мережі, інформаційні кластери та канали поширення фейків, що особливо важливо при вивченні ІПСО. Аналіз Big Data і цифрових слідів (пошукові запити, активність у соцмережах,

відкриті дані платформ) використовується для виявлення трендів, патернів поведінки й реакцій населення.

Джерелами даних виступають офіційна статистика (Державна служба статистики, профільні міністерства та відомства), результати соціологічних опитувань провідних дослідницьких центрів (КМІС, Центр Разумкова, Rating Group), звіти організацій медіа-моніторингу (Інститут масової інформації, StopFake тощо), а також відкриті дані міжнародних організацій і технологічних компаній. Для підвищення валідності висновків використовується принцип триангуляції: поєднання різних методів і джерел даних, що дозволяє мінімізувати похибки й упередження.

Етичні засади дослідження ґрунтуються на національному законодавстві у сфері захисту персональних даних, а також на міжнародних стандартах інформаційної безпеки й конфіденційності. Особлива увага приділяється добровільності участі респондентів, інформованій згоді, анонімності та недопущенню шкоди для учасників дослідження. Основні міжнародні стандарти, що стосуються управління інформаційною безпекою та захистом даних, систематизовано в табл. 1.8.

Таблиця 1.8

Основні міжнародні стандарти інформаційної безпеки та захисту даних

GDPR (General Data Protection Regulation)	Європейський Союз	Захист персональних даних та конфіденційності.	2018
Стандарт / Документ	Організація	Сфера застосування	Рік прийняття / актуалізації
ISO/IEC 27001	ISO / IEC	Система управління інформаційною безпекою (ISMS).	2013 (оновлено у 2022)
ISO/IEC 27002	ISO / IEC	Практичні правила для управління інформаційною безпекою.	2022

ISO/IEC 27701	ISO / IEC	Розширення ISO 27001 для управління конфіденційністю (Privacy).	2019
ENISA Guidelines	ЄС (ENISA)	Рекомендації з кібербезпеки для державних і приватних структур.	Постійно оновлюються
Budapest Convention on Cybercrime	Рада Європи	Міжнародне співробітництво у боротьбі з кіберзлочинністю.	2001

Загалом обрана методологія дозволяє поєднати аналіз нормативно-правових засад, управлінських практик та реальних інформаційно-психологічних впливів на українське суспільство. Це відповідає завданням спеціальності «Публічне управління та адміністрування» та забезпечує наукову й практичну цінність отриманих результатів.

Базовим нормативним актом є Закон України «Про інформацію» (перша редакція – 1992 р., чинна редакція – 2011 р.), який визначає принципи інформаційної діяльності, права громадян на доступ до достовірної інформації, гарантії свободи слова та відповідальність за зловживання інформацією. Цей закон задає фундаментальні рамки для функціонування інформаційного простору й одночасно окреслює межі втручання держави, що є критично важливим у контексті балансування між безпекою та свободою вираження поглядів.

Ключову роль відіграють також акти у сфері національної безпеки. Сучасна редакція законодавства у цій сфері закріплює інформаційну безпеку як один із пріоритетних напрямів державної політики безпеки й оборони, підкреслюючи необхідність протидії інформаційним та інформаційно-психологічним загрозам. У цьому контексті понятійні та управлінські підходи, запропоновані О. А. Панченком у монографії про інформаційно-психологічну безпеку в епоху турбулентності, дають

можливість розглядати українське законодавство не лише як набір норм, а як інструмент побудови цілісної політики стійкості держави та суспільства до деструктивних впливів [1].

Важливим елементом правової бази є Закон України «Про захист персональних даних» (2010 р.), який встановлює правила обробки інформації про громадян, права суб'єктів персональних даних та обов'язки розпорядників. У контексті ІПВ це має подвійне значення. З одного боку, закон захищає громадян від зловживань при збиранні й використанні їхніх персональних даних (що особливо актуально в умовах Big Data і психологічного таргетингу). З іншого боку, він задає етичні й правові рамки для наукових досліджень, у тому числі тих, що аналізують психологічні наслідки інформаційних впливів.

У сфері регулювання медіапростору важливу роль відіграє Закон України «Про медіа», а також нормативні акти Національної ради з питань телебачення і радіомовлення. Вони спрямовані на забезпечення прозорості структури власності медіа, дотримання стандартів поширення достовірної інформації та протидію маніпуляціям і дезінформації. У практичній площині це створює механізми для обмеження діяльності медіа-ресурсів, що системно поширюють пропаганду ворожої держави або дезінформаційні кампанії, та для стимулювання саморегуляції медіасектору.

Стратегічний вимір забезпечує Доктрина інформаційної безпеки України (2017 р.), яка визначає основні загрози в інформаційній сфері, пріоритети державної політики, а також завдання для органів публічного управління у сфері протидії пропаганді, інформаційним операціям і кібератакам. У Доктрині, зокрема, наголошено на необхідності розвитку системи стратегічних комунікацій, підвищення рівня медіаграмотності населення, захисту критичної інформаційної інфраструктури. Ці напрями співзвучні науковій позиції О. А. Панченка щодо потрібності

комплексного, міжсекторального підходу до інформаційно-психологічної безпеки, який поєднує правові, організаційні та медико-психологічні заходи.

Окреме місце займають нормативні акти у сфері кібербезпеки та цифрової трансформації. До них належать закони щодо базових засад кібербезпеки, підзаконні акти Державної служби спеціального зв'язку та захисту інформації, а також стратегічні документи Міністерства цифрової трансформації. Ці акти забезпечують технічну складову захисту інформаційних систем, що, у свою чергу, є необхідною умовою протидії ІПВ, які реалізуються через кіберпростір (злам ресурсів, вкидання фейкових матеріалів, маніпуляції цифровими платформами).

Узагальнення ключових законодавчих актів і стратегічних документів, що формують правову основу інформаційної та інформаційно-психологічної безпеки України, подано в табл. 1.9.

Важливу роль у реалізації цих норм відіграють державні інституції. Державна служба спеціального зв'язку та захисту інформації координує заходи кіберзахисту, впроваджує стандарти безпеки й відповідає за захист урядових інформаційних систем. Підрозділи кіберполіції здійснюють розслідування кіберзлочинів та взаємодіють із міжнародними партнерами. Міністерство цифрової трансформації розвиває національні системи кіберзахисту, цифрові сервіси та підвищує рівень цифрової грамотності населення. Центр стратегічних комунікацій та інформаційної безпеки, інші профільні структури сектору безпеки і оборони працюють над протидією дезінформації, аналізом наративів та проведенням роз'яснювальних кампаній для громадян. Така інституційна архітектура загалом відповідає підходу, окресленому О. А. Панченком, щодо необхідності поєднання інформаційно-аналітичних, комунікаційних та реабілітаційних компонентів у системі державного управління інформаційно-психологічною безпекою.

Таблиця 1.9

Законодавчі акти та їх роль у сфері інформаційної безпеки та протидії інформаційно-психологічним впливам

Нормативний акт	Основний зміст
Закон України «Про інформацію»	Визначає принципи інформаційної діяльності, права громадян на доступ до достовірної інформації.
Закон «Про основи національної безпеки України»	Розглядає інформаційну безпеку як ключовий елемент державної політики у сфері національної безпеки.
Закон «Про захист персональних даних»	Встановлює правила обробки та захисту персональних даних громадян, що важливо для досліджень і безпеки.
Закон «Про медіа»	Містить положення щодо протидії дезінформації, регулює діяльність медіа та стандарти контенту.
Нормативи Нацради з питань телебачення і радіомовлення	Забезпечують контроль за дотриманням стандартів інформаційного контенту та протидію фейкам.
Доктрина інформаційної безпеки України	Визначає стратегічні підходи до захисту інформаційного простору та протидії інформаційним загрозам.

Не менш важливим є міжнародний вимір правового забезпечення інформаційної безпеки. Україна є учасницею Будапештської конвенції про кіберзлочинність, співпрацює з НАТО, ЄС та профільними агенціями (зокрема ENISA) у сфері кіберзахисту та протидії інформаційним загрозам. Великі технологічні компанії підтримують Україну у відбитті кібератак і наданні хмарної інфраструктури для збереження даних. Це означає, що національна нормативна база поступово інтегрується в ширший європейський і євроатлантичний правовий простір, де питання інформаційної та інформаційно-психологічної безпеки розглядаються як елемент колективної безпеки.

Таким чином, нормативно-правові засади протидії ІПВ в Україні мають багаторівневий характер: від загальних законів про інформацію та

національну безпеку до спеціальних актів у сфері медіа, персональних даних, кіберзахисту й стратегічних комунікацій. Ця правова рамка створює підґрунтя для формування комплексної державної політики, спрямованої на запобігання, виявлення та подолання наслідків інформаційно- психологічних впливів, а також дає можливість узгоджувати практику публічного управління з науковими підходами до інформаційно- психологічної безпеки.

РОЗДІЛ 2. АНАЛІЗ УПРАВЛІНСЬКИХ АСПЕКТІВ У СФЕРІ ІПВ

2.1. Український контекст управління

Інформаційно-психологічна війна проти України є не епізодичним явищем, а постійною складовою гібридної війни, що ведеться проти нашої держави. Вона являє собою цілеспрямований і систематичний комплекс дій, спрямованих на вплив на свідомість, емоції та поведінку громадян, а також на суспільні настрої загалом. Її головне завдання — дестабілізувати державу, підірвати її єдність, знизити здатність суспільства до опору та поставити під сумнів легітимність публічної влади [19, с. 46]. Для цього використовуються різні механізми дезорієнтації та деморалізації населення, підриву довіри до державних інституцій, армії та медіа, а також створення розколу за мовними, культурними, політичними чи релігійними ознаками. Важливе місце займає формування вигідних агресору наративів, зокрема тверджень про «неспроможність України як держави», «зраду західних партнерів» тощо.

Методи ведення цієї війни різноманітні: від пропаганди та поширення фейкової інформації через соціальні мережі, засоби масової інформації та ботоферми — до кібероперацій, психологічних атак і використання псевдоекспертів. Активно застосовується маніпуляція емоціями: страх, паніка та ненависть використовуються як інструменти тиску на суспільство [19, с. 47]. Імітуються авторитетні джерела — створюються фейкові сторінки медіа, акаунти «аналітиків» чи «військових експертів», які поширюють керований дезінформаційний контент. До цього додаються злам акаунтів, цілеспрямоване поширення компрометуючих матеріалів, нагнітання тем втрат, економічної кризи та «зради» керівництва.

Канали впливу охоплюють практично всі сучасні інформаційні платформи: соціальні мережі (Facebook, Instagram, TikTok), месенджери (Telegram, Viber), телебачення та радіо, онлайн-медіа й блогосферу. Значну роль відіграють лідери думок та інфлюенсери, які свідомо або несвідомо ретранслюють дезінформаційні наративи. Як показують дослідження І. П. Коваля, критичними є саме канали поширення дезінформації, через які одночасно атакуються різні сегменти української аудиторії, а інформаційні операції, описані М. В. Сидоренком, демонструють довгострокові наслідки подібних кампаній для довіри та соціальної згуртованості.

Наслідки інформаційно-психологічної війни проявляються у зростанні тривожності та недовіри, поширенні міфів і конспірологічних теорій, поляризації громадської думки, зниженні готовності до спротиву й підтримки держави [20, с. 49]. Такий стан створює сприятливі умови для дестабілізації країни та реалізації стратегічних цілей агресора. У працях О. А. Панченка ці процеси розглядаються як прояви турбулентності інформаційного середовища, що вимагають від держави цілісної системи управління інформаційно-психологічною безпекою, а не лише ситуативних реакцій [1].

PESTLE-аналіз інформаційно-психологічної війни в Україні

Для комплексної оцінки середовища, у якому розгортається ІПВ, доцільно застосовувати PESTLE-аналіз. PESTLE (від англ. Political, Economic, Social, Technological, Legal, Environmental) – це інструмент стратегічного аналізу, що дозволяє розглянути політичні, економічні, соціальні, технологічні, правові та екологічні чинники, які формують зовнішнє середовище функціонування державної політики. У контексті публічного управління протидією ІПВ PESTLE-аналіз дає змогу виявити ключові вразливості та точки прикладання управлінських зусиль.

Узагальнені результати PESTLE-аналізу інформаційно-психологічної війни в Україні наведено в таблиці 2.1.

Таблиця 2.1

PESTLE-аналіз інформаційно-психологічної війни в Україні

Фактор	Ключові аспекти	Вплив на середовище
P – Політичні	- Війна та гібридні атаки - Поляризація політичних сил - Міжнародна підтримка	Розкол суспільства, підрив довіри до влади
E – Економічні	- Економічна нестабільність - Залежність від зовнішніх ринків - Кіберзагрози	Паніка, зниження довіри до фінансової системи
S – Соціальні	- Стрес і тривожність - Міграція, демографічні зміни - Соцмережі як канал впливу	Поширення фейків, радикалізація, зростання конфліктів
T – Технологічні	- Соцмережі та месенджери - ШІ у пропаганді (deepfake) - Кіберзахист	Масове поширення дезінформації, атаки на критичну інфраструктуру
L – Правові	- Закони про медіа - Міжнародні санкції - Захист персональних даних	Недостатня регуляція, складність контролю контенту
E – Екологічні	- Фейки про катастрофи - Паніка через екологічні загрози	Створення страху, дестабілізація суспільства

Як показує табл. 2.1, політичні фактори пов’язані насамперед із триваючою повномасштабною війною та гібридними атаками, високим рівнем політичної поляризації, а також залежністю від міжнародної підтримки. Інформаційно-психологічні операції активно експлуатують будь-які політичні суперечності всередині країни, намагаючись посилити розкол та підірвати довіру до влади, парламенту, сил безпеки.

Економічні чинники включають загальну нестабільність, інфляційні процеси, руйнування інфраструктури, залежність від зовнішніх ринків і фінансової підтримки. Ці теми стають ґрунтом для дезінформаційних кампаній про «неминучий економічний колапс», «зупинку допомоги»,

«неплатоспроможність держави», що посилює панічні настрої та недовіру до фінансової системи.

Соціальні фактори характеризуються високим рівнем стресу й тривожності населення через бойові дії, втрати, внутрішнє переміщення, роз'єднані сім'ї. Демографічні зміни, зокрема міграція та зниження народжуваності, створюють додаткові вразливості. Соціальні мережі стають основним каналом поширення фейків, емоційно забарвлених наративів і мови ворожнечі, що призводить до радикалізації та конфліктів.

Технологічний вимір пов'язаний із стрімким розвитком цифрових платформ, месенджерів, технологій штучного інтелекту (зокрема deepfake) та одночасною недостатністю кіберзахисту. Це створює передумови для масового поширення дезінформації, атак на критичну інфраструктуру та кібершантажу. Дослідження І. П. Коваля показують, що саме технологічна інфраструктура каналів поширення дезінформації є одним із ключових викликів для української моделі інформаційної безпеки.

Правові фактори охоплюють стан національного законодавства у сфері медіа, персональних даних, кібербезпеки, а також застосування міжнародних санкцій проти агресора й пов'язаних з ним структур. Правові прогалини, повільна адаптація норм до нових форматів онлайн-комунікації та складність контролю контенту у глобальних платформах посилюють уразливість інформаційного простору.

Екологічний вимір проявляється через використання тем техногенних і екологічних катастроф (ядерна загроза, руйнування гідроспоруд, забруднення води тощо) для нагнітання страху та паніки. Фейки про «неминучі катастрофи» підривають довіру до офіційних джерел і ускладнюють управління кризовими ситуаціями.

Таким чином, PESTLE-аналіз демонструє багатовимірний характер ІПВ і показує, що агресор системно використовує політичні, економічні,

соціальні, технологічні, правові та екологічні слабкі місця України. Такий контекст потребує цілісної, міжсекторальної державної політики, що відповідає управлінським підходам, запропонованим О. А. Панченком у дослідженнях державного управління інформаційною безпекою в умовах турбулентності [1].

Роль соціальних мереж у українському контексті ІПВ

Особливої уваги заслуговує роль соціальних мереж як ключового середовища реалізації ІПВ. Вони перетворилися на головний канал поширення дезінформації, пропаганди та маніпуляцій, оскільки забезпечують миттєве розповсюдження контенту та дозволяють охоплювати мільйони людей протягом лічених годин. Механізми таргетингу та персоналізації дають можливість налаштовувати повідомлення під конкретні групи населення, використовуючи дані про їхні інтереси, емоційний стан та поведінку, що робить вплив максимально ефективним [21, с. 13].

Соціальні мережі створюють потужний емоційний ефект: візуальний контент, меми, короткі відео та коментарі викликають сильні реакції, які маніпулятори використовують для формування страху, гніву або безсилля. Алгоритми платформ сприяють формуванню інформаційних «бульбашок», коли користувачі отримують переважно той контент, який відповідає їхнім попереднім поглядам; це ізолює їх від альтернативних точок зору й посилює поляризацію. Анонімність і легкість створення фейкових акаунтів та бот-мереж дають змогу організовувати масштабні інформаційні атаки й імітувати «суспільну думку» [21, с. 15]. У такому середовищі державні органи вимушені адаптувати свої інструменти публічних комунікацій і стратегічних комунікацій до нових реалій цифрової екосистеми.

Карта українських стейкхолдерів у сфері ІПВ

Для розуміння управлінського контексту важливо окреслити коло основних стейкхолдерів, залучених до протидії інформаційно-психологічній війні. Під стейкхолдером (англ. stakeholder) у публічному управлінні розуміють заінтересовану сторону – суб'єкта, на якого впливає відповідна політика і який, своєю чергою, впливає на її реалізацію (органи влади, інституції, організації, групи громадян, міжнародні партнери тощо). Мапування стейкхолдерів дозволяє визначити їхні ролі, ресурси, ризики та можливості взаємодії.

До ключових українських стейкхолдерів у сфері протидії ІПВ належать:

- Центральні органи влади (Кабінет Міністрів, Ради національної безпеки і оборони, Міністерство оборони, Міністерство цифрової трансформації, Служба безпеки України, Центр стратегічних комунікацій та інформаційної безпеки тощо) – формують державну політику інформаційної та інформаційно-психологічної безпеки, організовують кіберзахист, координують стратегічні комунікації у кризових ситуаціях.

- Місцеві органи влади – забезпечують комунікацію з населенням на локальному рівні, поширюють достовірну інформацію, організовують інформаційні кампанії в громадах, але часто стикаються з обмеженими ресурсами та низьким рівнем цифрових компетенцій.

- Освітні та медичні заклади – формують медіаграмотність, інформаційну гігієну, довіру до системи освіти й охорони здоров'я, але водночас стають мішенню фейкових кампаній (наприклад, щодо вакцинації, дистанційної освіти) [23, с. 101].

- Цифрові платформи (соціальні мережі, месенджери, державні сервіси на кшталт «Дія») – є основними каналами поширення інформації, мають значний вплив на громадську думку, але залишаються вразливими до використання бот-мереж, ворожої реклами та маніпулятивних алгоритмів.

- НУО та громадські організації – неурядові організації (НУО) зосереджуються на моніторингу інформаційного простору, фактчекінгу, освітніх програмах з медіаграмотності, аналітичній підтримці держави (StopFake, Інститут масової інформації, VoxCheck тощо) [23, с. 103].

- Медіа – національні та регіональні ЗМІ залишаються для значної частини населення основним джерелом інформації; вони можуть як протидіяти дезінформації, так і, навпаки, ретранслювати маніпулятивні матеріали.

Міжнародні партнери (ЄС, НАТО, США, міжнародні НУО, технологічні компанії) – надають допомогу у сфері кіберзахисту, фінансування просвітницьких кампаній, технологічні рішення для боротьби з пропагандою.

- Ворожі актори – насамперед Російська Федерація та пов'язані з нею державні й недержавні структури, які системно використовують державні медіа, бот-мережі, кіберзброю, проксі-ресурси для реалізації ІПВ [23, с. 104].

Узагальнений аналіз українських стейкхолдерів в інформаційно-психологічній війні наведено в табл. 2.2.

Таблиця 2.2

Аналіз українських стейкхолдерів в інформаційно-психологічній війні

Стейкхолдер	Роль	Ризики	Можливості
Центральні органи влади	Координація інформаційної політики, кіберзахист, стратегічні комунікації	Недостатня швидкість реагування, бюрократія, ризик витоку даних	Розробка єдиної стратегії, посилення кіберзахисту, міжнародна співпраця
Місцеві органи влади	Локальна комунікація з населенням, поширення достовірної інформації	Низька цифрова компетентність, обмежені ресурси	Партнерство з НУО, впровадження локальних інформаційних кампаній

Освітні та медичні заклади	Формування медіаграмотності, поширення правдивої інформації про освіту та медицину	Атаки через фейки про вакцинацію, освіту, паніка серед населення	Освітні програми з інформаційної гігієни, співпраця з медіа та державними органами
Цифрові платформи	Канали комунікації, поширення контенту, захист даних	Використання для пропаганди, бот-мережі, витік персональних даних	Впровадження алгоритмів протидії фейкам, партнерство з державою
НУО та громадські організації	Моніторинг фейків, просвітницькі кампанії, аналітика	Обмежене фінансування, ризик атак на репутацію	Розширення програм медіаграмотності, міжнародні гранти
Медіа	Інформування населення, протидія дезінформації	Вразливість до маніпуляцій, залежність від фінансування	Підвищення стандартів журналістики, фактчекінг, партнерство з міжнародними організаціями
Міжнародні партнери	Підтримка кіберзахисту, фінансування, технологічні рішення	Залежність від зовнішньої допомоги, політичні ризики	Технологічна допомога, навчання персоналу, спільні інформаційні кампанії
Ворожі актори	Поширення пропаганди, дезінформації, кіберзагрози	Масовані інформаційні атаки, використання ботів, підрив довіри до держави	Виявлення та блокування каналів впливу, міжнародні санкції

Роль НУО у протидії ІПВ: український та міжнародний вимір

Окремої уваги заслуговує діяльність неурядових організацій. Ефективність українських НУО у протидії інформаційно-психологічній війні доцільно оцінювати за кількома ключовими критеріями [23, с. 107].

По-перше, це вплив на медіаграмотність населення. Організації, такі як StopFake, Інститут масової інформації, VoxCheck, реалізують масштабні освітні кампанії, тренінги, створюють пояснювальний контент,

спрямований на викриття фейків. Вони суттєво підвищують рівень критичного мислення, особливо серед молоді та активних користувачів інтернету.

По-друге, це моніторинг та фактчекінг. НУО активно відстежують інформаційний простір, оперативно реагують на дезінформаційні вкиди, публікують спростування, готують аналітичні огляди. Це допомагає зменшити вплив фейків, хоча охоплення їхньої аудиторії часто поступається масштабам атак.

По-третє, важлива співпраця з державою та міжнародними партнерами. Багато організацій отримують гранти від ЄС, USAID, НАТО та інших донорів, що дозволяє реалізовувати проєкти з кіберзахисту, медіаграмотності та інформаційної безпеки. Водночас координація з державними структурами іноді є недостатньою, що знижує синергетичний ефект.

Серед ключових викликів для НУО — обмежене фінансування, нестача кадрів, інформаційні атаки на їхню репутацію, а також нерівномірне територіальне охоплення: активність зосереджена переважно у великих містах, тоді як у сільських регіонах рівень медіаграмотності залишається низьким. Для порівняння діяльності українських та міжнародних НУО доцільно звернутися до табл. 2.3.

Таблиця 2.3

Діяльність українських та міжнародних НУО у сфері протидії інформаційно-психологічній війні

Критерій	Українські НУО	Міжнародні НУО
Сильні сторони	Глибоке знання локального контексту, швидка реакція на внутрішні атаки, освітні програми для населення	Потужні фінансові ресурси, доступ до технологій, глобальні мережі, вплив на міжнародну політику
Слабкі сторони	Обмежене фінансування, невелике охоплення, слабка присутність у сільських регіонах	Менше знання локальних нюансів, залежність від партнерства з місцевими організаціями

Роль	Просвіта населення, фактчекінг, моніторинг локальних фейків	Глобальний моніторинг, аналітика, тиск на платформи та уряди, підтримка місцевих НУО
Ресурси	Обмежені бюджети, гранти від міжнародних донорів	Великі бюджети, доступ до передових технологій, аналітичних інструментів
Охоплення	Локальне (переважно Україна, іноді регіональні проєкти)	Глобальне, багатонаціональні кампанії

Як видно з табл. 2.3, українські НУО мають сильні сторони у вигляді глибокого знання локального контексту, швидкої реакції на внутрішні інформаційні атаки та тісної взаємодії із населенням. Натомість їхні слабкі сторони пов’язані з обмеженими ресурсами, невеликим охопленням та слабкою присутністю в сільських регіонах. Міжнародні НУО володіють значними фінансовими та технологічними ресурсами, глобальними мережами і впливом на міжнародну політику, однак потребують партнерства з місцевими організаціями для точного врахування культурних і соціальних особливостей України [24, с. 41].

Оптимальна стратегія, що відповідає управлінській логіці, полягає у поглибленні співпраці між українськими та міжнародними НУО, а також у кращій інтеграції НУО в систему публічного управління інформаційною безпекою. Це дозволяє поєднати локальну експертизу з глобальними ресурсами та технологіями, створюючи більш стійку й гнучку систему протидії інформаційно-психологічній війні.

Узагальнюючи, український контекст ІПВ характеризується високою інтенсивністю та багаторівневістю загроз, що діють у політичному, економічному, соціальному, технологічному, правовому та екологічному вимірах. Мережа стейкхолдерів – від центральних органів влади до НУО та міжнародних партнерів – формує потенціал для комплексної відповіді. Водночас виявлені PESTLE-аналізом вразливості та обмеження стейкхолдерів вказують на необхідність подальшого посилення

інституційної спроможності держави, що стане предметом детальнішого аналізу в наступних підрозділах.

2.2. Ключові ворожі наративи в Україні

Інформаційно-психологічна війна проти України базується на системному використанні ворожих наративів, які слід розглядати, за підходом Панченко О.І., як структуровані смислові конструкції, спрямовані на підрив ментальної стійкості суспільства та довіри до інститутів держави. Ці наративи не існують ізольовано: вони утворюють цілісну систему, що працює на делегітимацію української державності, деморалізацію населення та руйнування горизонтальних і вертикальних зв'язків довіри.

До ядра ворожих наративів належить твердження «Україна – держава, що не відбулася». Воно експлуатує теми корупції, бюрократії, управлінської неефективності, формуючи відчуття безнадії та марності будь-яких реформаторських зусиль. Такий наратив підриває легітимність публічної влади, демотивує громадян брати участь у політичному житті та підтримувати державні ініціативи.

Надзвичайно потужним є наратив «Захід зрадить Україну», який маніпулює страхами щодо надійності міжнародних партнерів. Він активізується у періоди складних переговорів, затримок військової або фінансової допомоги, формуючи сумніви у доцільності стратегічного курсу на євроатлантичну інтеграцію [25, с. 9]. У практичній площині цей наратив підживлює радикальні настрої – від вимог «негайного миру будь-якою ціною» до зневіри у спроможності союзників дотримуватися зобов'язань.

Один із найнебезпечніших наративів – «Війна – марна, треба капітулювати». Він спрямований безпосередньо на бойовий дух, волю до

опору та готовність суспільства витримувати тривалу боротьбу. Під виглядом гасел про «мир» просувається ідея відмови від спротиву, що де-факто означає капітуляцію та втрату суверенітету. Наратив підкріплюється емоційно насиченими історіями про втрати, руйнування, втому від війни, що особливо болісно сприймається сім'ями військових та внутрішньо переміщеними особами.

Наратив «Українці та росіяни – один народ» спрямований на розмивання української національної ідентичності. Він апелює до спільної історії, мовної та культурної близькості, родинних зв'язків, намагаючись виправдати агресію й окупацію, подати їх як «внутрішній конфлікт» чи «цивілізаційну єдність» [26, с. 191]. Особливу вразливість до цього наративу демонструють групи з радянським світоглядом, а також ті, хто має тісні родинні зв'язки з РФ.

Окремий напрямок інформаційного тиску – безпековий. Наратив «Мобілізація = смерть» експлуатує страхи, пов'язані з військовою службою: поширюються фейки про «масове знищення мобілізованих», «кидання без підготовки», «повну байдужість командування». Це провокує відмови від призову, посилює тривогу родин військових і знижує обороноздатність держави.

Економічний вимір представлений наративом «Економіка зруйнована, майбутнього немає». Він б'є по базовому відчуттю безпеки: розганяються чутки про «неминучий дефолт», «припинення виплат пенсій», «колапс енергосистеми», що створює паніку, викликає ажіотаж у банках, посилює недовіру до уряду та фінансових інституцій.

Нарешті, важливе місце посідає наратив «Влада переслідує інакодумців», який експлуатує тему свободи слова. Законні дії держави щодо проросійських медіа або колаборантів подаються як прояв «авторитаризму» і «цензури», що сприяє делегітимації публічної влади,

посиленню конфліктів і зростанню популярності анонімних каналів, де домінує неконтрольована дезінформація [26, с. 196].

Ці наративи взаємодіють між собою, створюючи комплексний інформаційно-психологічний тиск на суспільство. Одні й ті ж групи можуть одночасно підпадати під вплив політичних, економічних, ідентифікаційних та безпекових меседжів. Для цілей подальшого управлінського аналізу доцільно систематизувати їх з урахуванням вразливих груп і базових метрик моніторингу. Узагальнення ключових наративів, цільових аудиторій та можливих індикаторів спостереження за їхнім впливом наведено в табл. 2.4.

Таблиця 2.4

Наративи та метрики їх моніторингу

Наратив	Вразливі групи	Метрики моніторингу
Україна – держава, що не відбулася	Люди похилого віку, регіони з низьким доходом	Медіаграмотність (% розпізнавання фейків), довіра до інституцій
Захід зрадить Україну	Молодь, ВПО, особи з високим рівнем стресу	Довіра до партнерів, аналіз тональності соцмереж
Війна – марна, треба капітулювати	Військові родини, молодь	Психоемоційні маркери (тривожність, депресія), інциденти онлайн
Українці та росіяни – один народ	Люди похилого віку, особи з низьким рівнем освіти	Аналіз тональності, рівень ідентичності
Мобілізація = смерть	Військові родини, молодь	Інциденти офлайн/онлайн, психоемоційні маркери
Економіка зруйнована, майбутнього немає	Регіони з низьким доходом, ВПО	Динаміка довіри до ЗМІ, економічні страхи
Влада переслідує інакодумців	Молодь, активні користувачі соцмереж	Кількість випадків дезінформації, конфлікти, довіра

Вразливі групи та індивідуальна інформаційна безпека

Питання вразливості окремих груп населення до інформаційно-психологічних впливів тісно пов'язане з людиноцентричним підходом до інформаційної безпеки, розробленим, зокрема, І. В. Кукіним у контексті державного управління інформаційною безпекою особистості [5]. Вразливість у цьому контексті означає підвищену ймовірність прийняття дезінформаційних послань, емоційної дестабілізації та поведінкових реакцій під впливом ІПВ.

До найбільш вразливих груп належать:

Люди похилого віку, які через низьку цифрову грамотність та орієнтацію переважно на телевізійний контент часто отримують інформацію з обмеженого кола джерел, серед яких можуть домінувати маніпулятивні або проросійські медіа. Вони особливо чутливі до наративів про «зруйновану економіку», «державу, що не відбулася», а також до фейків про соціальні виплати.

Молодь, яка активно користується соціальними мережами (TikTok, Instagram, Telegram) і характеризується високою емоційною реактивністю. Вона стає мішенню для наративів про «марність війни», «мобілізацію як смертний вирок», «тотальну корумпованість влади», а також для культурно-ідентифікаційних меседжів.

Внутрішньо переміщені особи (ВПО), що перебувають у стані хронічного стресу та невизначеності. Вони особливо вразливі до наративів про «зраду з боку держави та партнерів», «відсутність перспектив», «безглуздість продовження спротиву» [2].

Жителі регіонів з низьким рівнем доходів, які гостро реагують на економічні страхи та інформацію про можливі соціальні потрясіння. Для них небезпека становлять наративи про «економічний колапс», «зупинку соціальних виплат», «непотрібність реформ».

Родини військових і люди з високим рівнем стресу чи травматичного досвіду, які болісно реагують на повідомлення про втрати, «знищення мобілізованих», «байдужість командування». Для них надзвичайно небезпечні наративи «Мобілізація = смерть» та «Війна – марна».

У працях Панченка і Кукіна наголошується, що державна політика у сфері інформаційної безпеки має враховувати саме людиноцентричний вимір – не лише захищати інформаційні системи, а й підтримувати психологічну стійкість конкретних груп населення. Це вимагає таргетованих комунікаційних стратегій, програм підтримки ментального здоров'я, просвітницьких ініціатив з медіаграмотності [5].

Метрики та інструменти моніторингу наслідків ІПВ

Для ефективного управління протидією ІПВ необхідно не лише ідентифікувати наративи й вразливі групи, а й мати систему метрик, що дозволяють відстежувати динаміку їхнього впливу. На основі підходів О. А. Панченка до оцінювання стану інформаційно-психологічної безпеки та сучасних практик OSINT-аналізу можна виділити кілька груп індикаторів.

Когнітивно-довірові метрики:

1) індекси довіри до державних інституцій, Збройних сил, органів місцевого самоврядування, міжнародних партнерів;

2) показники довіри до різних типів медіа (офіційні ЗМІ, анонімні канали, соціальні мережі);

3) рівень медіаграмотності (частка населення, здатного розпізнавати фейки, участь у програмах цифрової освіти тощо).

2. Психоемоційні маркери:

1) результати опитувань і психометричних досліджень щодо рівня тривожності, депресивних симптомів, почуття безнадії;

2) аналіз тональності контенту в соціальних мережах (Sentiment Analysis): частота використання лексики, пов’язаної зі страхом, агресією, зневірою;

3) статистика звернень до психологічних служб, гарячих ліній, волонтерських ініціатив підтримки.

3. Поведенкові індикатори:

1) кількість інцидентів, пов’язаних із дезінформацією (конфлікти, протести, відмови від мобілізації, ажіотажні закупівлі);

2) динаміка участі в громадських ініціативах підтримки ЗСУ, волонтерстві, благодійності;

3) зміни у виборчій поведінці, рівні політичної участі як реакція на інформаційні кампанії.

4. Цифрово-комунікаційні метрики:

1) охоплення, частота та інтенсивність поширення ворожих наративів у соцмережах;

2) структура мережі поширення (бот-мережі, ключові хаби впливу);

3) динаміка появи та зникнення каналів, що системно поширюють дезінформацію.

Для збору та аналізу цих даних використовується широкий спектр інструментів відкритої розвідки (OSINT) та аналітики соціальних мереж. Платформа Molfar спеціалізується на аналізі контенту в Telegram та інших соцмережах, дозволяючи виявляти джерела та маршрути розповсюдження фейків. Bellingcat Toolkit акумулює інструменти для верифікації джерел і геолокації матеріалів, тоді як Maltego використовується для побудови графів зв’язків між акаунтами, сайтами та іншими цифровими об’єктами. Hoaxy дає змогу візуалізувати поширення фейкових повідомлень у Twitter [32].

Для аналізу соціальних мереж використовуються CrowdTangle (Facebook, Instagram), TGStat (Telegram), а також системи моніторингу згадок і тональності, такі як Brandwatch та Talkwalker. Методи автоматичного аналізу емоційного забарвлення контенту реалізуються за допомогою інструментів Sentiment Analysis на основі Python та технологій обробки природної мови (NLP) [35].

Важливу роль відіграють фактчекінгові проєкти StopFake та VoxCheck, які здійснюють систематичну перевірку інформації, публікують спростування фейків і надають суспільству верифікований контент. Для перевірки візуальних матеріалів використовуються сервіси InVID (аналіз відео) та TinEye (зворотній пошук зображень), що дозволяє встановити первинне походження візуального контенту [30; 31].

Практичну реалізацію поєднання наративів, вразливих груп, метрик та інструментів моніторингу ілюструють конкретні кейси інформаційно-психологічних атак, зафіксовані в Україні у 2022–2024 рр. Один із показових прикладів – кампанія навколо наративу «Захід зрадить Україну», коли після чергових зустрічей у форматі «Рамштайн» у соціальних мережах масово поширювалися повідомлення про «припинення постачання зброї».

Аналогічно працював наратив «Мобілізація = смерть»: телеграм-канали поширювали постановочні відео з «могилами мобілізованих», що спричиняло страх і відмови від призову. У випадку з наративом «Економіка зруйнована, майбутнього немає» фейки про «дефолт» та «зупинку виплат пенсій» призводили до панічних настроїв серед пенсіонерів та черг у банках; контрзаходи включали офіційні заяви НБУ й уряду, а також роз’яснювальні кампанії у соцмережах. Наратив «Влада переслідує інакодумців» особливо активно використовувався для інтерпретації блокування проросійських медіа як «цензури», що сприяло міграції аудиторії в анонімні канали.

Зведену таблицю ключових кейсів ІПВ, пов’язаних із зазначеними наративами, вразливих груп, базових метрик та інструментів їхнього моніторингу наведено в табл. 2.5.

Таблиця 2.5

Ключові кейси ІПВ

Наратив	Кейс	Вразливі групи	Метрики	Інструменти
Захід зрадить Україну	Чутки про припинення постачання зброї після зустрічей у Рамштайні, масове поширення у соцмережах	Молодь, ВПО, особи з високим рівнем стресу	Довіра до партнерів, аналіз тональності соцмереж	Molfar, Bellingcat Toolkit, CrowdTangle, TGStat, StopFake
Мобілізація = смерть	Відео з фейковими могилами мобілізованих у Telegram, що викликало страх і відмови від призову	Військові родини, молодь	Інциденти офлайн/онлайн, психоемоційні маркери	TGStat, Sentiment Analysis (Python NLP), Maltego, InVID
Економіка зруйнована, майбутнього немає	Фейки про дефолт України та зупинку виплат пенсій, що спричинили паніку серед пенсіонерів і черги в банках	Регіони з низьким доходом, пенсіо-нери	Динаміка довіри до ЗМІ, економічні страхи	CrowdTangle, Brandwatch, Talkwalker, TinEye
Влада переслідує інакодумців	Інтерпретація блокування проросійських медіа як цензури, що призвело до зростання популярності анонімних каналів	Молодь, активні користувачі соцмереж	Кількість випадків дезінформації, конфлікти, довіра	Molfar, Maltego, Hoaxy, VoxCheck

Узагальнюючи, можна відзначити, що інформаційно-психологічна війна проти України має системний і багатовимірний характер. Ворожі наративи цілеспрямовано б'ють по політичній, економічній, соціальній та ідентифікаційній сферах, використовуючи страхи, невизначеність та емоційну вразливість населення [2]. Найбільш уразливими залишаються групи з низьким рівнем цифрової грамотності, люди в стані стресу, молодь та родини військових. Реальні кейси демонструють, що дезінформаційні кампанії мають конкретні наслідки – від панічних настроїв і падіння довіри до партнерів до локальних конфліктів і психологічного виснаження.

Ефективна протидія, у руслі підходів О. А. Панченка, потребує системного моніторингу, заснованого на чітких метриках, а також використання сучасних OSINT-інструментів, аналітики соціальних мереж і потужної системи фактчекінгу. У поєднанні з людиноцентричними політиками підтримки ментального здоров'я та розвитку медіаграмотності це створює передумови для формування стійкого до ІПВ суспільства та збереження довіри до держави й міжнародних партнерів.

2.3. Інституційна спроможність протистояння ІПВ в Україні

Під інституційною спроможністю протидії інформаційно-психологічній війні в Україні у контексті публічного управління доцільно розуміти інтегральну здатність системи державних і недержавних інституцій *формулювати, реалізовувати та коригувати* державну політику в сфері інформаційної безпеки, забезпечуючи стійкість суспільства до дезінформації, пропаганди та цілеспрямованого психологічного впливу. У працях О. А. Панченка інституційна спроможність розглядається як ключовий компонент державного управління інформаційною безпекою в умовах турбулентності, де важливо

не лише мати формальні структури, а й забезпечити їхню узгоджену, проактивну та людиноцентричну діяльність [1].

Узагальнюючи підходи сучасної науки публічного управління та напрацювання О. А. Панченка й І. В. Кукіна, інституційну спроможність протидії ІПВ можна розкласти на кілька взаємопов'язаних блоків [5].

Нормативно-правова база. Йдеться про наявність законів, доктрин, стратегій та підзаконних актів, які визначають напрями, принципи й механізми протидії інформаційним загрозам, захисту інформаційного простору, персональних даних і кібербезпеки. Для ефективного публічного управління важливо, щоб ця база була не фрагментарним набором норм, а узгодженою *політикою* (policy), що задає інституційний каркас системи інформаційної безпеки.

Організаційна структура. Це сукупність органів публічної влади та спеціалізованих центрів (Центр стратегічних комунікацій, підрозділи кібербезпеки, служби моніторингу, урядові офіси цифрової трансформації), а також механізми координації між ними. У термінах публічного управління йдеться про інституційний дизайн системи – розподіл повноважень, функцій, каналів взаємодії та підзвітності.

Кадровий потенціал. Йдеться не лише про чисельність персоналу, а передусім про *компетентності* фахівців: розвідка на основі відкритих джерел (Open Source Intelligence, OSINT), стратегічні комунікації, кіберпсихологія, аналіз великих даних, кризові та ризик-комунікації. Для магістерської спеціальності «публічне управління» це безпосередньо пов'язано з підготовкою нової генерації управлінців, здатних працювати в умовах гібридної війни [4].

Технологічні ресурси. Це доступ до сучасних систем моніторингу соціальних мереж, платформ аналізу інформаційних потоків, засобів кіберзахисту, інструментів штучного інтелекту (Artificial Intelligence, AI) та обробки природної мови (Natural Language Processing, NLP), сервісів

фактчекінгу й верифікації контенту. У публічному управлінні йдеться про спроможність держави й партнерських організацій застосовувати ці технології системно, а не точково.

Комунікаційна спроможність. Це здатність органів влади та партнерських структур *швидко, послідовно й прозоро* інформувати громадян, спростовувати фейки, пояснювати управлінські рішення та формувати власні позитивні наративи. У підходах О. А. Панченка стратегічні комунікації розглядаються як ключовий елемент державної політики інформаційної безпеки, що безпосередньо впливає на ментальну стійкість населення.

Міжнародна співпраця. Інституційна спроможність у сфері інформаційної безпеки неможлива без інтеграції в євроатлантичні безпекові структури, участі у спільних програмах НАТО, ЄС, ОБСЄ, обміну аналітичними ресурсами та технологіями. З позицій публічного управління це вимір *зовнішньої* спроможності держави – здатність залучати зовнішні ресурси та включатися в глобальні режими співпраці.

Таким чином, інституційна спроможність – це не лише наявність певних органів чи законів, а *їх ефективність у взаємодії*, швидкість реагування, здатність прогнозувати загрози та системно формувати стійкість суспільства. Для її оцінки доцільно застосовувати інструменти стратегічного аналізу, які активно використовуються в публічному управлінні, зокрема SWOT- і GAP-аналіз.

SWOT-аналіз інституційної спроможності України протидії ІПВ

SWOT-аналіз (Strengths, Weaknesses, Opportunities, Threats) – класичний інструмент стратегічного управління, який дозволяє оцінити внутрішні (сильні та слабкі сторони) і зовнішні (можливості та загрози) фактори, що впливають на певну політику або інституційну систему [38, с. 127]. У публічному управлінні його застосування дає змогу поєднати оцінку поточного стану з формуванням варіантів управлінських рішень.

У контексті протидії ІПВ об’єктом SWOT-аналізу виступає **інституційна спроможність України у сфері інформаційної безпеки**. Відповідно до логіки стратегічного аналізу спочатку здійснюється збирання даних щодо:

1) стану нормативно-правової бази (закони, доктрини, стратегії);

2) ефективності організаційної структури (координація між органами влади, Центр стратегічних комунікацій, кіберпідрозділи);

3) кадрового потенціалу (фахівці з OSINT, кіберпсихології, стратегічних комунікацій);

4) технологічних ресурсів (системи моніторингу, AI-платформи, інструменти аналізу соцмереж);

5) комунікаційної спроможності (оперативність та прозорість офіційних повідомлень);

6) рівня міжнародної співпраці.

На основі цих даних фактори розподіляються за чотирма категоріями. До **сильних сторін** віднесено розвинену мережу фактчекінгових організацій (StopFake, VoxCheck), активну громадянську позицію та волонтерські ініціативи у сфері кібербезпеки, наявність державних комунікаційних платформ і міжнародну підтримку у вигляді OSINT-інструментів та навчальних програм. До слабких сторін – нерівномірний рівень медіаграмотності населення, обмежені ресурси для масштабного моніторингу соцмереж, фрагментарність координації між державними та громадськими структурами, нестача спеціалістів з OSINT, кіберпсихології та аналізу великих даних [27].

Можливості пов’язані з розширенням міжнародного партнерства, впровадженням систем автоматичного моніторингу дезінформації на основі AI та NLP, запуском масових освітніх програм з медіаграмотності, розвитком кіберрезерву й центрів психологічної стійкості. Серед загроз – еволюція методів дезінформації (deepfake, генеративні моделі), висока

швидкість поширення контенту в соцмережах, використання внутрішніх соціальних конфліктів для підриву єдності, кібератаки на критичну інформаційну інфраструктуру. Узагальнення результатів наведено в табл. 2.6.

Таблиця 2.6

SWOT-аналіз інституційної спроможності України протидії ІПВ

Strengths	Weaknesses	Opportunities	Threats
Розвинена мережа фактчекінгових організацій (StopFake, VoxCheck)	Нерівномірний рівень медіаграмотності населення	Розширення міжнародного партнерства для доступу до технологій	Еволюція методів дезінформації (deepfake, генеративні моделі)
Активна громадянська позиція та волонтерські ініціативи у сфері кібербезпеки	Обмежені ресурси для масштабного моніторингу соцмереж	Впровадження системи автоматичного моніторингу дезінформації на основі AI	Висока швидкість поширення контенту в соцмережах
Державні комунікаційні платформи для оперативного інформування	Фрагментарність координації між державними та громадськими структурами	Масові освітні програми з медіаграмотності	Використання внутрішніх соціальних конфліктів для підриву єдності
Міжнародна підтримка у вигляді OSINT-інструментів та навчальних програм	Недостатня кількість спеціалістів з OSINT та кіберпсихології	Розвиток кіберрезерву та центрів психологічної стійкості	Кібератаки на критичну інформаційну інфраструктуру

Отримані результати свідчать, що з точки зору публічного управління Україна має низку суттєвих *інституційних активів*: активне громадянське суспільство, сильні фактчекінгові команди, базові державні комунікаційні платформи та міжнародну підтримку. Водночас слабкі сторони – низький рівень медіаграмотності значної частини населення,

нестача фахових кадрів, фрагментарна координація – обмежують ефективність цих активів.

Стратегічно важливим є використання **можливостей**: інтеграція AI-рішень у моніторинг, системні програми медіаграмотності, розвиток кіберрезерву та психологічної підтримки населення й військових. **Загрози** вимагають переходу від реактивної до проактивної моделі управління – від відповіді на вже здійснені атаки до прогнозування та випереджального блокування.

З погляду науки публічного управління SWOT-аналіз дає підґрунтя для формування *інституційної дорожньої карти*: які сильні сторони слід посилювати, які слабкості – мінімізувати, які можливості – конвертувати в конкретні програми, а які загрози – закривати через нормативні, організаційні та технологічні рішення.

GAP-аналіз координації, спроможностей і ресурсів.

Як наступний крок інституційної діагностики доцільно застосувати **GAP-аналіз**, який у стратегічному управлінні використовується для визначення розриву між *поточним* і *бажаним* станом системи та формування плану дій для його подолання [39]. Для публічного управління це особливо важливо, оскільки GAP-аналіз дозволяє перевести загальні цілі державної політики в конкретні управлінські завдання.

У сфері протидії ІПВ GAP-аналіз охоплює такі ключові аспекти:

1) **координація** між державними органами, НУО, медіа та приватним сектором;

2) **кадровий потенціал** (спеціалісти з OSINT, кіберпсихології, стратегічних комунікацій, data-science);

3) **технологічні ресурси** (системи моніторингу, AI/NLP-платформи, кіберзахист);

4) **нормативно-правова база** (наявність цілісної стратегії інформаційної та психологічної безпеки);

5) **комунікаційна спроможність** (швидкість і прозорість офіційних комунікацій, робота в соцмережах);

6) **міжнародна співпраця** (системність інтеграції до міжнародних мереж і платформ). Для кожного аспекту визначаються: 1) поточний стан; 2) бажаний (цільовий) стан; 3) власне «розрив» (Gap); 4) управлінські рекомендації. Результати узагальнено в табл. 2.7.

Таблиця 2.7

GAP-аналіз координації, спроможностей і ресурсів України у протидії інформаційно-психологічній війні

Аспект	Поточний стан	Бажаний стан	Розрив (Gap)	Рекомендації
Координація	Фрагментарність між державними та громадськими структурами	Єдиний координаційний центр, інтегрована система взаємодії	Відсутність єдиної структури та механізмів координації	Створити національний центр координації та кризових комунікацій
Кадровий потенціал	Недостатня кількість спеціалістів з OSINT та кіберпсихології	Високий рівень підготовки кадрів, наявність кіберрезерву	Брак кваліфікованих кадрів та навчальних програм	Інвестувати в навчання OSINT, кіберпсихології та аналітики
Технологічні ресурси	Обмежені системи моніторингу, відсутність автоматизації	Автоматизовані системи моніторингу на основі AI та NLP	Низький рівень технологічної оснащеності	Впровадити AI-системи для моніторингу та аналізу дезінформації
Нормативно-правова база	Є окремі закони, але немає комплексної стратегії	Комплексна стратегія інформаційної безпеки та психологічної стійкості	Немає узгодженої стратегії та стандартів	Розробити комплексну стратегію та нормативні стандарти
Комунікаційна спроможність	Низька швидкість реагування, слабка прозорість комунікацій	Оперативні та прозорі комунікації, активне використання соцмереж	Недостатня швидкість реагування та комунікаційна прозорість	Запустити систему швидкого реагування та прозорих комунікацій

Міжнародна співпраця	Співпраця існує, але не систематизована	Системна міжнародна інтеграція, доступ до аналітичних платформ	Обмежена інтеграція з міжнародними партнерами	Розширити міжнародні партнерства та обмін технологіями

Інтерпретація таблиці 2.7 показує, що з позицій публічного управління найбільші *розриви* спостерігаються у трьох площинах.

Координація та управлінська архітектура. На сьогодні система протидії ІПВ характеризується фрагментарністю: окремі органи влади, НУО та волонтерські ініціативи працюють ефективно, але *розрізнено*. Відсутність єдиного координаційного центру стратегічних комунікацій і кризового реагування знижує швидкість та узгодженість відповідей на інформаційні атаки.

Кадровий та технологічний потенціал. Брак фахівців з OSINT, кіберпсихології, аналізу великих даних, а також обмежені технологічні ресурси (автоматизовані AI/NLP-системи моніторингу) не дозволяють повною мірою реалізувати проактивну модель інформаційної безпеки, про яку пише О. А. Панченко в контексті управління в умовах турбулентності [1].

Стратегічна та нормативна цілісність. Попри наявність окремих законів і доктрин, відсутня єдина *комплексна* стратегія інформаційної та психологічної безпеки, яка б інтегрувала інституційні, технологічні й людиноцентричні компоненти, включно з захистом інформаційної безпеки особистості, про що наголошує І. В. Кукін [5].

З огляду на результати GAP-аналізу можна сформулювати низку управлінських рекомендацій, спрямованих на подолання виявлених розривів:

Створення національного центру координації та кризових комунікацій, який би об’єднав державні органи, НУО й експертні спільноти, забезпечував цілодобовий моніторинг інформаційного простору та швидкі погоджені реакції на інформаційні кризи.

Розбудова кадрового потенціалу через спеціалізовані освітні програми з OSINT, кіберпсихології, аналізу даних та стратегічних комунікацій у закладах, що готують фахівців з публічного управління. Це відповідає завданню формування нової генерації управлінців, здатних діяти в умовах гібридних загроз.

Впровадження автоматизованих AI/NLP-систем моніторингу соціальних мереж і медіапростору в реальному часі, інтегрованих з аналітичними платформами міжнародних партнерів. Це дасть змогу перейти до проактивного виявлення й блокування дезінформаційних кампаній.

Розробка комплексної стратегії інформаційної та психологічної безпеки, що враховуватиме як державний, так і людиноцентричний вимір (захист інформаційної безпеки особистості, ментальна стійкість, підтримка вразливих груп).

Посилення комунікаційної спроможності: створення протоколів швидкого реагування, систематичне використання соціальних мереж для пояснення рішень влади, прозорі механізми спростування фейків, партнерство з медіа та НУО у сфері фактчекінгу.

Систематизація міжнародної співпраці: укладання довгострокових програм обміну даними, спільних навчань і досліджень, використання передових аналітичних платформ партнерів [24, с. 38].

Таким чином, інституційна спроможність протистояння ІПВ в Україні з точки зору публічного управління перебуває у стані *частково сформованої*, але такої, що потребує глибокої структурної модернізації. Поєднання результатів SWOT- і GAP-аналізу дозволяє перейти від констатації проблем до формування цілісної політики зміцнення інформаційної стійкості держави, що є ключовою передумовою успішної протидії інформаційно-психологічній війні.

РОЗДІЛ 3. ШЛЯХИ ПОДОЛАННЯ НАСЛІДКІВ ІПВ В УКРАЇНІ: ПОЛІТИКА, ІНТЕРВЕНЦІЇ, ОЦІНЮВАННЯ

3.1. Цільова модель протидії ІПВ

Цільова модель протидії інформаційно-психологічній війні (ІПВ) в Україні у площині публічного управління доцільно розуміти як бажаний, нормативно окреслений та організаційно забезпечений стан системи державної політики, інститутів та інструментів, які спільно забезпечують стійкість держави, суспільства та особистості до дезінформації, пропаганди, насильницько-терористичних акцій із інформаційним компонентом та інших засобів ІПВ. У наукових підходах О. А. Панченка така модель розглядається як відповідь держави на «епоху турбулентності», коли інформаційні загрози є постійними та багатовимірними, а отже, протидія їм повинна бути не епізодичною, а системною та проактивною [1].

Вихідною передумовою для формування цільової моделі є розуміння ІПВ як комплексного явища, де використовуються взаємопов’язані засоби: насильство/тероризм, пропаганда, дезінформація (Кабанцева А. В.), а також складні інформаційно-психологічні операції, у контексті гібридних війн описані О. А. Панченком [4]. Тому йдеться не лише про боротьбу з фейками або окремими інформаційними кампаніями, а про побудову цілісної архітектури публічного управління, здатної захищати ментальну, інформаційну та інституційну стійкість держави.

Принципи цільової моделі протидії ІПВ

Цільова модель має спиратися на низку принципів, які відображають як вимоги демократичного публічного управління, так і специфіку гібридної війни:

1. Людиноцентричність. У працях І. В. Кукіна підкреслюється, що державна політика інформаційної безпеки має починатися з безпеки особистості [5]. Отже, захист ментального здоров'я, індивідуальної інформаційної безпеки, прав людини і свобод слова має поєднуватися з активною протидією дезінформації та пропаганді.

2. Системність і міжсекторальність. Протидія ІПВ не може бути лише функцією силового блоку або окремого міністерства. Цільова модель передбачає взаємодію органів державної влади, місцевого самоврядування, сил безпеки й оборони, освітніх та медичних закладів, медіа, цифрових платформ, громадських організацій і міжнародних партнерів.

3. Проактивність і випереджальний характер. Панченко О.А. у підході до управління в умовах турбулентності ключовим є перехід від реактивних дій до прогнозування загроз та їх випереджального нейтралізування. Це означає розвиток систем раннього виявлення дезінформаційних кампаній та інформаційно-психологічних операцій [1].

4. Прозорість і демократична підзвітність. Оскільки в боротьбі з пропагандою легко перейти до надмірних обмежень і цензури, цільова модель повинна бути заснована на прозорих процедурах, судовому контролі й дотриманні стандартів прав людини. Це є принциповою умовою довіри до інституцій публічної влади.

5. Інклюзивність та участь громадян. Громадянське суспільство, волонтерські ініціативи, професійні спільноти (журналісти, психологи, освітяни) мають бути не лише «реципієнтами» державної політики, а активними суб'єктами формування та реалізації заходів протидії ІПВ.

6. Наукова обґрунтованість та орієнтація на дані. З огляду на складність психологічних механізмів ІПВ, державна політика має спиратися на емпіричні дослідження, психометричні вимірювання, аналіз

великих масивів даних (Big Data) та рекомендації фахівців з психіатрії, психології та інформаційної безпеки.

Структура цільової моделі: рівні та компоненти

З урахуванням зазначених принципів цільову модель протидії ІПВ доцільно представити як багаторівневу систему, у якій виокремлюються стратегічний, оперативно-тактичний та індивідуально-соціальний рівні.

1. Стратегічний (макрорівень публічного управління).

На цьому рівні формуються:

1. державна стратегія інформаційної та психологічної безпеки, яка інтегрує положення Доктрини інформаційної безпеки, воєнної доктрини, стратегій кібербезпеки та національної стійкості;

2. інституційна архітектура: визначення провідних органів (РНБО, профільні міністерства, Центр стратегічних комунікацій, Держспецзв'язку, СБУ тощо) та механізмів їх координації;

3. нормативно-правове забезпечення, що унормовує протидію пропаганді, дезінформації, терористичним актам із потужним інформаційним компонентом, а також захист персональних даних і свободу слова;

4. міжнародно-правові та інституційні рамки співпраці (ЄС, НАТО, ОБСЄ, окремі партнерські держави, міжнародні НУО).

На стратегічному рівні визначаються цілі державної політики: захист суверенітету та територіальної цілісності, збереження національної ідентичності, підвищення ментальної стійкості населення, зміцнення довіри до інститутів публічної влади.

2. Оперативно-тактичний (мезорівень).

Цей рівень охоплює практичну реалізацію політики через програми, інтервенції та механізми управління ризиками, зокрема:

1. створення та функціонування оперативних центрів моніторингу інформаційного простору (OSINT, аналітика соцмереж, виявлення бот-мереж, кластерів дезінформації);

2. системи стратегічних комунікацій: урядові брифінги, офіційні канали у соцмережах, комунікація у кризових ситуаціях, роз'яснення рішень влади, контрнаративи;

3. програми підготовки кадрів у сфері OSINT, кіберпсихології, кризових комунікацій, психосоціальної підтримки;

4. цільові програми медіаграмотності, орієнтовані на різні групи населення (люди похилого віку, молодь, ВПО, родини військових);

5. психологічні й соціальні інтервенції: центри психологічної підтримки, програми профілактики посттравматичних розладів, робота з вразливими групами;

6. взаємодія з цифровими платформами (Telegram, Meta, TikTok, Google): механізми повідомлення про ворожий контент, узгодження політик модерації, спільні інформаційні кампанії.

Саме на цьому рівні розгортається практичне втілення наукових підходів О. А. Панченка щодо управління інформаційною безпекою в умовах турбулентності [1] та ідей І. В. Кукіна щодо захисту інформаційної безпеки особистості [5].

3. Індивідуально-соціальний (мікрорівень).

Цей рівень репрезентує поведінку та стан конкретних людей і спільнот. До цільової моделі тут належать:

1. індивідуальна медіагігієна та критичне мислення громадян;
2. ментальна стійкість як здатність зберігати психологічну рівновагу під впливом інформаційних атак;
3. діяльність громадських організацій та НУО, що здійснюють фактчекінг, освітні програми, локальні інформаційні кампанії;
4. професійні стандарти журналістики та етичні кодекси медіа;

5. локальні спільноти (громади, освітні заклади, ветеранські організації), що стають середовищем взаємної підтримки і джерелом достовірної інформації.

У термінах публічного управління цільова модель передбачає, що держава не намагається «контролювати» поведінку громадян, а створює умови та інституційні стимули для розвитку стійкості, медіаграмотності та самозахисту від ІПВ.

Функціональні блоки цільової моделі

Для практичного опису цільову модель протидії ІПВ доцільно структурувати за чотирма функціональними блоками: управлінсько-координаційний, аналітико-технологічний, комунікаційно-психологічний та освітньо-профілактичний.

1. Управлінсько-координаційний блок

Управлінсько-координаційний блок визначає, *хто і як* у державі відповідає за протидію ІПВ. У межах цільової моделі йдеться не просто про наявність окремих документів чи відомств, а про узгоджену систему публічної політики.

По-перше, держава має **формувати й регулярно актуалізувати стратегію протидії ІПВ**, яка логічно поєднує воєнну доктрину, стратегію національної безпеки, доктрину інформаційної безпеки та політику цифрової трансформації. Це не «паперовий» документ, а рамка, яка задає спільний вектор для всіх інституцій.

По-друге, необхідна **координація дій органів виконавчої влади, сектору безпеки й оборони та органів місцевого самоврядування**. Ті самі наративи та інформаційні атаки мають бути розпізнані і враховані на центральному рівні, у регіонах і в громадах — без суперечливих меседжів «з Києва» і «на місцях».

По-третє, важливою складовою є **системна взаємодія з міжнародними партнерами та неурядовими організаціями**.

Міжнародні структури, українські й зарубіжні НУО, аналітичні центри, фактчекінгові проєкти — це не «сторонні спостерігачі», а повноцінні учасники інституційної мережі протидії ІПВ.

Нарешті, цей блок забезпечує **правову визначеність і дотримання прав людини**. Будь-які заходи протидії пропаганді чи дезінформації мають спиратися на закон, проходити через прозорі процедури та не перетворюватися на інструмент політичних переслідувань. Саме тут балансуються безпека і свобода слова.

2. Аналітико-технологічний блок

Аналітико-технологічний блок — це «очі й нервова система» цільової моделі. Він відповідає за те, щоб держава не діяла навмання, а спиралася на дані, аналіз і сучасні технології.

Ключовою функцією є **безперервний моніторинг інформаційного простору**: від національних телеканалів і онлайн-медіа до соціальних мереж, месенджерів та локальних спільнот. Йдеться не про хаотичне «читання стрічок», а про структурований збір даних, у тому числі в режимі реального часу.

На основі цього моніторингу використовуються **OSINT-інструменти, платформи штучного інтелекту та мережевий аналіз**. Вони дозволяють виявляти аномальні інформаційні сплески, координовані кампанії, бот-мережі, «міграцію» ворожих наративів між різними майданчиками.

Важливою функцією блоку є **фіксація та документування інформаційних операцій, кампаній пропаганди й дезінформації**. Це потрібно не лише для поточної протидії, а й для подальших правових, дипломатичних чи військово-політичних рішень.

Окремий вимір — **підтримка кібербезпеки критичної інформаційної інфраструктури**: державних реєстрів, систем зв’язку, платформ електронного урядування. У сучасних умовах кібератака й

інформаційно-психологічна операція часто йдуть у парі, тому захист «заліза» і захист свідомості громадян мають розглядатися разом.

3. Комунікаційно-психологічний блок

Комунікаційно-психологічний блок відповідає за те, *що і як* держава говорить своїм громадянам і світові, а також — як вона враховує психологічні наслідки ІПВ.

У центрі — **система стратегічних комунікацій**. Це не лише пресрелізи й брифінги, а цілісна здатність держави *пояснювати свої рішення*, *швидко спростовувати фейки*, пропонувати *власні контрнаративи*, які підтримують віру в перемогу, довіру до інститутів та відчуття суб'єктності громадян.

Другий важливий напрям — **психологічна підтримка населення й військових**. Інформаційні атаки завжди б'ють по емоціях — страх, безнадія, агресія, вина. Тому необхідні програми профілактики паніки, кризове консультування, підтримка родин військових, робота з травмою. Тут особливо корисними є підходи, напрацьовані в медицині й психіатрії, зокрема досвід реабілітації учасників ліквідації наслідків Чорнобильської аварії, який досліджував О. А. Панченко.

Третій вимір — **інтеграція психологічних знань у дизайн комунікацій**. Йдеться про те, щоб державні повідомлення враховували механізми тривоги, заперечення, групової ідентичності, впливу травматичного досвіду. Це дозволяє не просто «передавати інформацію», а працювати зі станом суспільства, підтримувати його стійкість, а не посилювати вразливість.

4. Освітньо-профілактичний блок

Освітньо-профілактичний блок — це «довга гра» цільової моделі. Його завдання — зробити так, щоб через кілька років суспільство в цілому стало менш вразливим до маніпуляцій, навіть якщо конкретні інформаційні атаки змінюються.

Базовим елементом тут є **інтеграція медіаграмотності в систему освіти**: від школи до університетів та післядипломного навчання. Йдеться не тільки про технічні навички користування інтернетом, а про вміння критично оцінювати джерела, розпізнавати маніпуляції, відстежувати емоційний вплив контенту.

Окрема лінія — **спеціальні програми для держслужбовців, військових, журналістів, лідерів громадської думки**. Це ті групи, які одночасно є цілями ІПВ і каналами впливу на інших. Їхня стійкість і компетентність прямо визначає успіх або провал публічної політики.

Важливо також **підтримувати дослідження у сфері ІПВ, інформаційної безпеки, кіберпсихології**. Наукова база дозволяє не діяти інтуїтивно, а розробляти інтервенції, які спираються на емпіричні дані та сучасні теорії.

І, нарешті, освітньо-профілактичний блок включає **цільові просвітницькі кампанії для вразливих груп** — людей похилого віку, внутрішньо переміщених осіб, родин військових тощо. Для кожної з цих груп потрібні свої формати, мова й канали комунікації, щоб не лише попереджати про загрози, а й давати відчуття підтримки та включеності.

Схематично взаємодію блоків цільової моделі можна подати у вигляді концептуальної схеми, де показано циклічний зв’язок: моніторинг → аналіз → управлінське рішення → комунікація та інтервенції → оцінювання → корекція політики.

Місце публічного управління в реалізації цільової моделі

Цільова модель протидії ІПВ є, по суті, моделлю публічного управління в умовах гібридної війни [4].. Саме органи публічної влади:

1. ініціюють і затверджують стратегічні документи;

2. визначають інституційні ролі й відповідальність;

3. забезпечують ресурсне (кадрове, фінансове, технологічне) наповнення політики;

4. встановлюють механізми підзвітності, контролю та оцінювання.

У цьому контексті підходи О. А. Панченка до державного управління інформаційною безпекою в епоху турбулентності та ідеї І. В. Кукіна щодо державного управління інформаційною безпекою особистості задають теоретико-методологічні орієнтири для побудови такої цільової моделі. Вони наголошують на необхідності поєднання інституційної, технологічної та психологічної складових, а також на пріоритеті захисту людини й суспільства як основних суб'єктів інформаційної безпеки.

Таким чином, цільова модель протидії ІПВ в Україні у площині публічного управління може бути визначена як багаторівнева, людиноцентрична та науково обґрунтована система стратегій, інститутів, інструментів і практик, спрямованих на зниження вразливості держави, суспільства та особистості до інформаційно-психологічних атак та на забезпечення їхньої стійкості в умовах тривалої гібридної війни [4]. У наступних підрозділах ця модель конкретизуватиметься через план впровадження політики подолання наслідків ІПВ та прогноз її ефективності у середньостроковій перспективі.

3.2. План впровадження політики подолання наслідків ІПВ

План впровадження політики подолання наслідків інформаційно-психологічної війни в Україні передбачає комплексний підхід, спрямований на зміцнення інформаційної стійкості держави та суспільства. Насамперед необхідно оновити законодавство у сфері інформаційної безпеки, кіберзахисту та протидії дезінформації, а також впровадити стандарти медіаграмотності у державні програми. Це створить правову основу для подальших дій.

Важливим етапом є формування інституційної та технологічної інфраструктури. План передбачає створення Центру інформаційної

стійкості, який здійснюватиме моніторинг та аналіз інформаційних атак, а також розробку національної платформи фактчекінгу для перевірки достовірності інформації. Одночасно необхідно посилити кіберзахист критичної інфраструктури, щоб запобігти кібератакам та витоку даних [47.].

Особливу увагу освітнім та просвітницьким програмам слід приділити через їхню ключову роль у формуванні інформаційної стійкості суспільства. Медіаграмотність має бути інтегрована у навчальні програми на всіх рівнях освіти — від початкової школи до університетів. Це передбачає розробку сучасних навчальних матеріалів, включення тем про розпізнавання фейків, критичне мислення, безпечне використання цифрових ресурсів та аналіз джерел інформації. Для вчителів необхідно створити методичні рекомендації та провести курси підвищення кваліфікації, щоб вони могли ефективно викладати ці теми.

Для державних службовців, журналістів та освітян слід організувати спеціалізовані тренінги, спрямовані на розпізнавання маніпуляцій, протидію пропаганді та використання інструментів фактчекінгу. Такі тренінги мають бути практичними, з реальними кейсами та симуляціями інформаційних атак.

Паралельно необхідно реалізувати масштабні інформаційні кампанії для населення. Вони можуть включати соціальну рекламу, відеоролики, інтерактивні онлайн-курси, мобільні додатки для перевірки новин, а також активність у соціальних мережах [47]. Основна мета — підвищити рівень критичного мислення, навчити громадян перевіряти джерела інформації та розуміти механізми маніпуляцій. Особливий акцент слід зробити на молодь та людей похилого віку, які є найбільш вразливими до дезінформації.

Не менш важливим є напрям психологічної реабілітації та підтримки. План передбачає створення програм психологічної допомоги

для груп, що зазнали впливу пропаганди, а також розвиток сервісів кризової психологічної підтримки, які допоможуть знизити негативні наслідки інформаційного тиску.

Важливим компонентом є міжнародна співпраця. Україна має активно обмінюватися досвідом з країнами ЄС та НАТО, а також залучати гранти та технічну допомогу для розвитку кіберзахисту та інформаційної безпеки. Це дозволить інтегрувати найкращі практики та отримати доступ до сучасних технологій [48].

Завершальним етапом є моніторинг та оцінка ефективності реалізованих заходів. Для цього необхідно регулярно готувати звіти про інформаційні загрози, визначати ключові показники ефективності (KPI) для програм медіаграмотності та кіберзахисту, а також проводити аудит інформаційної безпеки. Такий комплексний підхід забезпечить системну протидію наслідкам інформаційно-психологічної війни та підвищить стійкість українського суспільства до зовнішніх інформаційних впливів (див. таблицю 3.1).

Таблиця 3.1

П’ятирічний план протидії інформаційно-психологічній війні

Рік	Основні заходи
Рік 1: Підготовчий етап	Аналіз ситуації, розробка нормативної бази, створення Національного центру інформаційної стійкості, запуск пілотних програм медіаграмотності
Рік 2: Інституційне зміцнення	Розгортання системи моніторингу, запуск платформи фактчекінгу, навчання держслужбовців та журналістів, початок масових інформаційних кампаній
Рік 3: Масштабування програм	Впровадження медіаграмотності у всі освітні рівні, розширення кіберзахисту, запуск психологічних програм реабілітації, співпраця з міжнародними партнерами
Рік 4: Інтеграція та автоматизація	Впровадження AI-рішень для виявлення фейків, створення реєстру інформаційних атак, розширення цифрових сервісів, аудит ефективності програм

Рік 5: Стійкість та контроль	Інтеграція інформаційної безпеки у державну політику, регулярні звіти та контроль, оцінка результатів, закріплення міжнародних партнерств

Запропонований п’ятирічний план є комплексною стратегією, яка поєднує правові, технологічні, освітні та психологічні заходи. Його реалізація дозволить Україні підвищити стійкість до інформаційно-психологічних атак, забезпечити захист критичної інфраструктури, сформувати культуру медіаграмотності та зміцнити міжнародне співробітництво. Системний підхід і поетапне впровадження гарантують довготривалий ефект та зниження ризиків дестабілізації суспільства.

В період реалізації плану доцільним буде врахувати всі можливі ризики та попередити їх. Серед ризиків варто виокремити наступні [47].

1. *Недостатнє фінансування.*

Ризик полягає у можливості браку коштів для реалізації запланованих програм. Впровадження комплексної політики потребує значних фінансових ресурсів для створення інфраструктури, навчання кадрів, запуску інформаційних кампаній та розробки технологічних рішень. Якщо бюджет буде обмеженим або фінансування нестабільним, це призведе до скорочення обсягів робіт, затримок у реалізації та зниження ефективності заходів.

2. *Опір суспільства.*

Низький рівень довіри до державних інституцій може стати серйозною перешкодою. Громадяни можуть сприймати інформаційні кампанії як пропаганду, а освітні програми — як нав’язування певних поглядів. Це знижує ефективність просвітницьких заходів і може викликати негативну реакцію, що ускладнить формування інформаційної стійкості.

3. *Технологічне відставання.*

Відсутність сучасних інструментів для боротьби з фейками, аналізу інформаційних потоків та кіберзахисту створює вразливість перед інформаційними атаками. Якщо Україна не зможе впровадити штучний інтелект, автоматизовані системи моніторингу та цифрові платформи, ефективність протидії дезінформації буде низькою.

4. *Посилення атак з боку агресора.*

У відповідь на заходи з протидії ІПВ агресор може збільшити масштаби інформаційних атак, використовуючи нові технології, бот-мережі та психологічні операції. Це може призвести до дестабілізації суспільства, зростання паніки та недовіри до держави, а також до підриву міжнародного іміджу України.

5. *Кадровий дефіцит.*

Реалізація програми потребує висококваліфікованих спеціалістів у сфері кіберзахисту, психології, медіаграмотності та комунікацій. Нестача таких кадрів може призвести до низької якості програм, затримок у впровадженні та обмеження масштабів роботи.

6. *Політична нестабільність.*

Зміна уряду або політичних пріоритетів може призвести до зупинки або перегляду програми. Якщо інформаційна безпека перестане бути пріоритетом, фінансування та підтримка заходів знизяться, що поставить під загрозу досягнення стратегічних цілей.

7. *Міжнародні ризики.*

Геополітичні фактори можуть обмежити доступ до сучасних технологій, програмного забезпечення або фінансування з боку міжнародних партнерів. Санкції, конфлікти або зміна зовнішньополітичних умов можуть знизити рівень співпраці, що вплине на темпи реалізації програми та її ефективність. Наявні ризики, ймовірності та статегії мінімізації відображені в тиблиці 3.2.

Таблиця 3.2

Матриця ризиків

Ризик	Ймовірність	Вплив	Стратегія мінімізації
Недостатнє фінансування	Висока	Високий	Залучення міжнародних грантів, оптимізація витрат, створення резервного фонду
Опір суспільства	Середня	Середній	Прозора комунікація, залучення громадських організацій, інформаційні кампанії для підвищення довіри
Технологічне відставання	Середня	Високий	Інвестиції в інновації, партнерство з технологічними компаніями, навчання персоналу
Посилення ат агресора	Висока	Високий	Постійний моніторинг, розвиток кіберзахисту, міжнародна співпраця у сфері безпеки
Кадровий дефіци	Середня	Середній	Програми підготовки кадрів, залучення експертів з-за кордону, підвищення мотивації персоналу
Політична нестабільність	Середня	Високий	Закріплення політики на законодавчому рівні, створення незалежних інституцій, міжнародні гарантії підтримки
Міжнародні ризики	Низька	Середній	Диверсифікація партнерів, розвиток власних технологій, укладання довгострокових угод

Аналіз показує, що найбільш критичними є ризики з високою ймовірністю та високим впливом — недостатнє фінансування та посилення атак агресора. Їх мінімізація потребує комплексних заходів: залучення додаткових ресурсів, міжнародної підтримки та розвитку кіберзахисту. Ризики середнього рівня, такі як опір суспільства, кадровий дефіцит і політична нестабільність, можна знизити через прозору комунікацію, освітні програми та закріплення політики на законодавчому

рівні. Міжнародні ризики мають нижчу ймовірність, але потребують стратегічного підходу — диверсифікації партнерів та розвитку власних технологій [48]. Системне управління ризиками забезпечить стабільність реалізації плану та підвищить його ефективність. З метою запобігання ризикам та їх мінімалізації наведемо план реагування на ризики, що відображається в таблиці 3.3

Таблиця 3.3

План реагування на ризики

Ризик	План реагування
Недостатнє фінансування	Перегляд пріоритетів програми, скорочення другорядних заходів, термінове залучення донорських коштів через міжнародні гранти та партнерські проєкти
Опір суспільства	Запуск додаткових роз'яснювальних кампаній, організація відкритих дискусій, залучення лідерів думок для підвищення довіри до державних ініціатив
Технологічне відставання	Термінове укладання угод з міжнародними постачальниками технологій, закупівля готових рішень, прискорене навчання персоналу для швидкої адаптації до сучасних інструментів
Посилення атак агресора	Активація кризового штабу, посилення кіберзахисту, залучення міжнародних експертів для оперативного реагування
Кадровий дефіцит	Терміновий набір персоналу на контрактній основі, залучення фрілансерів та міжнародних консультантів для виконання критичних завдань
Політична нестабільність	Залучення міжнародних організацій для підтримки програм, перенесення ключових функцій на незалежні структури для забезпечення безперервності роботи
Міжнародні ризики	Активізація внутрішніх ресурсів, пошук альтернативних партнерів, розробка локальних технологічних рішень для збереження темпів впровадження стратегії

У випадку виникнення ризику недостатнього фінансування першочерговим кроком стане перегляд пріоритетів програми, скорочення другорядних заходів та термінове залучення донорських коштів через

міжнародні гранти та партнерські проєкти. Якщо спостерігатиметься опір суспільства, необхідно негайно запустити додаткові роз'яснювальні кампанії, організувати відкриті дискусії та залучити лідерів думок для підвищення довіри до державних ініціатив.

У разі технологічного відставання план передбачає термінове укладання угод з міжнародними постачальниками технологій, закупівлю готових рішень та прискорене навчання персоналу для швидкої адаптації до сучасних інструментів. Якщо агресор посилить інформаційні атаки, буде активовано кризовий штаб, посилено кіберзахист та залучено міжнародних експертів для оперативного реагування.

При виникненні кадрового дефіциту необхідно терміново набрати персонал на контрактній основі, залучити фрілансерів та міжнародних консультантів для виконання критичних завдань. У випадку політичної нестабільності план передбачає залучення міжнародних організацій для підтримки програм та перенесення ключових функцій на незалежні структури, щоб забезпечити безперервність роботи [48]. Якщо реалізуються міжнародні ризики, слід активізувати внутрішні ресурси, шукати альтернативних партнерів та розробляти локальні технологічні рішення для збереження темпів впровадження стратегії.

Аналіз п'ятирічного плану впровадження політики подолання наслідків інформаційно-психологічної війни в Україні показує, що стратегія є комплексною та системною, охоплюючи правові, технологічні, освітні, психологічні та міжнародні аспекти. Її реалізація спрямована на підвищення інформаційної стійкості держави, захист критичної інфраструктури, формування культури медіаграмотності та забезпечення психологічної підтримки населення.

Важливим елементом є поетапність впровадження: від підготовчого етапу з розробкою нормативної бази та створенням інституцій до інтеграції сучасних технологій і закріплення результатів у державній

політиці. Такий підхід дозволяє поступово нарощувати потенціал та адаптуватися до змін у зовнішньому середовищі.

Аналіз ризиків показав, що найбільшу загрозу становлять недостатнє фінансування та посилення атак агресора, які мають високу ймовірність і значний вплив. Інші ризики, такі як технологічне відставання, кадровий дефіцит та політична нестабільність, також потребують уваги, але можуть бути мінімізовані через гнучкі управлінські рішення та міжнародну підтримку. Розроблений план реагування забезпечує можливість швидкої адаптації до негативних сценаріїв, що підвищує стійкість програми.

Загалом, реалізація запропонованої стратегії дозволить Україні не лише нейтралізувати наслідки інформаційно-психологічної війни, а й створити фундамент для довгострокової інформаційної безпеки, зміцнити міжнародні позиції та підвищити рівень довіри суспільства до державних інституцій.

3.3. Прогноз наслідків ІПВ (2025–2027)

У період 2025–2027 років інформаційно-психологічна війна проти України, за логікою «епохи турбулентності» [1], яку описує О. А. Панченко, й надалі матиме системний, довготривалий та багатовимірний характер. Йдеться не про окремі інформаційні кампанії, а про стійке, хвилеподібне навантаження на суспільство, інститути публічної влади та інформаційну інфраструктуру держави, що поєднує дезінформацію, кібероперації, психологічний тиск і політичні маніпуляції. У цьому контексті прогноз наслідків ІПВ повинен розглядатися як інструмент державного управління ризиками в інформаційно-безпековій сфері, а не як суто академічна вправа. Саме так підходить до проблеми Панченко, коли розглядає інформаційно-психологічну безпеку як предмет цілеспрямованої

управлінської діяльності держави в умовах невизначеності та багатоканальних загроз.

Спираючись на ідеї О. А. Панченка щодо сценарного аналізу, державної інформаційної політики та ментальної стійкості суспільства, доцільно прогнозувати наслідки ІПВ у форматі трьох базових сценаріїв – оптимістичного, базового та песимістичного – із виокремленням чотирьох ключових вимірів: соціального, економічного, політичного та технологічного. Узагальнений сценарний прогноз подано у таблиці 3.10.

У соціальному вимірі оптимістичний сценарій передбачає, що завдяки системним заходам публічного управління – розвитку стратегічних комунікацій, підтримці психологічної стійкості, масовим програмам медіаграмотності – рівень поляризації суспільства поступово знижується, а довіра до базових інститутів (армії, органів влади, місцевого самоврядування) утримується на прийнятному рівні. У базовому сценарії очікується помірне зростання поляризації, коли інформаційні атаки регулярно створюють хвилі напруги, але держава здатна втримувати ситуацію в полі керованості. Песимістичний сценарій, який особливо детально аналізується в роботах Панченка про інформаційний тиск у кризових умовах, передбачає глибоку соціальну фрагментацію, коли недовіра, втома від війни та накопичений стрес стають живильним середовищем для радикалізації й масової апатії.

В економічному вимірі оптимістичний сценарій пов’язаний із тим, що держава вчасно вибудовує прозору комунікацію з бізнесом і громадянами, оперативно спростовує фейки про «дефолт», «зупинку виплат» чи «колапс енергетики», а регулятори (НБУ, профільні міністерства) працюють у логіці проактивної інформаційної політики. У такій моделі ІПВ не призводить до критичних збоїв в інвестиційних рішеннях. Базовий сценарій передбачає періодичні інформаційні кризи – локальні панічні закупівлі, епізодичні «набіги» на банки, підвищену

чутливість до чуток, – але без системного обвалу. Песимістичний сценарій означає, що інформаційні атаки на фінансову й енергетичну системи збігаються з реальними економічними труднощами, викликаючи ланцюгові реакції – від відтоку депозитів до гальмування інвестицій та загострення соціально-економічної напруги.

Політичний вимір у 2025–2027 роках залишатиметься одним із головних полів, на яких концентруватимуться інформаційні атаки, що повністю відповідає логіці «цільових аудиторій» інформаційно-психологічних війн, описаній О. А. Панченком. В оптимістичному сценарії виборчі процеси проходять під посиленим захистом: дієвий моніторинг дезінформації, прозорість підрахунку голосів, системна участь міжнародних спостерігачів, злагоджена робота органів публічної влади в кризових ситуаціях. Базовий сценарій означає, що спроби дестабілізації виборів відбуватимуться, але не досягатимуть критичного ефекту: може падати довіра до окремих інститутів, однак загальна легітимність влади зберігається. Песимістичний сценарій передбачає глибоку кризу довіри, масове поширення наративів про «фальсифікації», «змову еліт», делегітимізацію ключових інститутів і перехід частини протестного потенціалу в деструктивні форми – що зовнішні актори можуть використати як «вікно можливостей» для політичного впливу.

У технологічному вимірі Панченко акцентує на взаємопов’язаності кіберзагроз і ІПВ як єдиного поля гібридної війни. В оптимістичному сценарії держава нарощує потенціал CERT-структур, впроваджує сучасні SIEM-системи, використовує штучний інтелект для аналізу аномалій у трафіку, а також для виявлення deepfake-контенту. У базовому сценарії бот-мережі, генеративні моделі та deepfake активно використовуються противником, але завдяки інституційній спроможності критичні інфраструктури залишаються функціональними. Песимістичний сценарій передбачає масові кібератаки на енергетику, транспорт, фінансовий

сектор, які супроводжуються хвилями дезінформації – це створює відчуття «тотальної нестабільності» й підриває віру громадян у здатність держави їх захистити.

Рекомендації щодо реагування на кожен із трьох сценаріїв також слід розглядати в логіці публічного управління, а не лише технічних заходів. В оптимістичному сценарії ключове завдання – інституціоналізувати успіх: закріпити ефективні практики стратегічних комунікацій, інтегрувати медіаграмотність у системи освіти та підготовки держслужбовців, посилити програми психологічної підтримки й реабілітації, про необхідність яких ідеться в працях О.А. Панченка, присвячених реабілітації учасників екстремальних подій.

У базовому сценарії акцент зміщується на превентивне управління ризиками. Потрібні: стабільні канали комунікації між урядом, регуляторами, бізнесом і громадськістю; стандартизовані протоколи кризових комунікацій; кіберзахист виборчих процесів і електронних реєстрів; систематичні кампанії, спрямовані на підвищення довіри до офіційних джерел.

У песимістичному сценарії держава повинна мати заздалегідь розроблені надзвичайні плани інформаційно-психологічної реакції, про що прямо говорить О. А. Панченко, розглядаючи управління інформаційною безпекою в умовах «турбулентних потрясінь» [1]. Йдеться про розгортання кризових інформаційних центрів, залучення міжнародних партнерів до забезпечення прозорості процесів, оперативну реалізацію антикризових економічних і соціальних заходів, а також інтенсивні програми психологічної підтримки для населення і військових.

Для того, щоб прогноз не залишався декларативним, він має бути інтегрований у систему моніторингу та оцінки (M&E), яка виступає інструментом публічного управління у сфері інформаційної безпеки. На ідеї Панченка О.А. про необхідність постійного вимірювання стану

інформаційно-психологічної сфери спирається формування набору індикаторів, що дозволяють оцінювати як масштаб загроз, так і ефективність управлінських рішень.

У таблиці 3.4 наведено узагальнену M&E-рамку для відстеження наслідків ІПВ у 2025–2027 роках. Вона включає чотири групи індикаторів: соціальні, інформаційні, економічні та технологічні, а також окремий блок методів збору й аналізу даних. Соціальні індикатори (рівень довіри до інститутів, індекс поляризації, рівень тривожності) дозволяють оцінити ментальну стійкість суспільства, яку Панченко розглядає як один із ключових елементів інформаційної безпеки. Інформаційні індикатори (кількість і охоплення фейків, виявлені бот-мережі) показують інтенсивність атак і здатність держави та НУО їх фіксувати. Економічні й технологічні індикатори (коливання інвестиційної довіри, кількість кібератак, використання deepfake) відображають вплив ІПВ на матеріальні й інфраструктурні основи функціонування держави.

Таблиця 3.4

Узагальнені M&E-рамки для відстеження наслідків ІПВ

Компонент	Деталі	Методи/Інструменти	Періодичність
Індикатори Соціальні	Рівень довіри до державних інституцій, індекс поляризації суспільства, рівень тривожності	Опитування, аналіз соцмереж	Щокварталу
Індикатори Інформаційні	Кількість фейкових новин, охоплення дезінформаційних кампаній, кількість виявлених бот-мереж	Моніторинг соцмереж, AI-інструменти	Щоденно
Індикатори Економічні	Коливання інвестиційного індексу, вплив на курс гривні, зміни у ВВП	Економетричні моделі, статистичний аналіз	Щомісяця
Індикатори Технологічні	Кількість кібератак на критичну інфраструктуру, частота використання deepfake	Системи кіберзахисту, AI-аналіз	У реальному
Методи збору аналізу	NLP-аналіз тональності, виявлення ботів і deepfake, економетричні моделі	OSINT-платформи, AI-інструменти	Постійно

Джерела даних	Maltego, Social Bearing, SIEM, Threat Intelligence, НБУ, соціологічні служби	Інтегровані системи збору даних	Відповідно пу даних

Більш деталізовані приклади індикаторів подано в таблиці 3.5. На рівні impact-індикаторів доцільно відстежувати, зокрема, індекс довіри до органів державної влади й місцевого самоврядування, а також рівень соціальної поляризації, який може оцінюватися за допомогою інструментів аналізу тональності дискурсу в соціальних мережах. На рівні outcome-індикаторів важливо вимірювати частку фейкових новин, які були оперативно спростовані офіційними або авторитетними джерелами, і кількість виявлених та нейтралізованих бот-мереж. Output-індикатори відображають управлінські зусилля: середній час реакції на інформаційну атаку, кількість проведених контркампаній, масштаб освітніх та просвітницьких заходів.

Таблиця 3.5

Приклади індикаторі наслідків ІПВ

Рівень	Індикатор	Джерело/Метод	Цільове значення
Impact	Індекс довіри до державних інституцій	Національні опитування, соціологічні служби	≥50%
Impact	Рівень соціальної поляризації	Аналіз тональності дискурсу в соцмережах (Sentiment Analysis)	% негативних/ агресивних постів
Outcome	Частка фейкових новин, що були спростовані офіційно	Медіа-моніторинг, OSINT	>70% протягом 48 годин
Outcome	Кількість виявлених бот-мереж	AI-аналіз соцмереж, кіберзахист	Кількість заблокованих акаунтів
Output	Середній час реакції на інформаційну атаку	Внутрішні звіти центрів кіберзахисту	<24 години
Output	Кількість проведених інформаційних кампаній для протидії	Звіти комунікаційних служб	Кількість кампаній на місяць
Економічні	Індекс інвестиційної довіри	Дані фондового ринку, НБУ	-
Економічні	Коливання курсу гривн під час інформаційних атак	Порівняння з базовим трендом	-

Технологічні	Кількість кібератак на критичну інфраструктуру	CERT-UA, звіти кібербезпеки	
Технологічні	Рівень використання deepfake у пропаганді	AI-аналіз відео та фото	

Такий підхід повністю корелює з логікою державного управління інформаційною безпекою, запропонованою О. А. Панченком: від констатації загроз – до їхнього вимірювання і включення в цикл управлінських рішень. Іншими словами, прогноз наслідків ІПВ на 2025–2027 роки має слугувати не тільки описом можливих негативних сценаріїв, але й основою для формування системи цілей, завдань і показників результативності публічної політики у сфері інформаційної безпеки.

Отже, у 2025–2027 роках інформаційно-психологічна війна залишатиметься однією з ключових загроз публічному управлінню в Україні. Ризики поглиблення соціальної поляризації, зниження довіри до інституцій, дестабілізації виборчих процесів, економічних коливань та технологічних атак будуть безпосередньо залежати від того, наскільки держава зможе реалізувати цільову модель протидії ІПВ, посилити інституційну спроможність та впровадити дієву систему моніторингу й оцінки. Спираючись на наукові підходи О. А. Панченка та інших дослідників інформаційної безпеки, можна стверджувати, що поєднання сценарного прогнозування і M&E-підходів створює основу для переходу від реактивної до проактивної моделі державного управління в умовах інформаційно-психологічної війни.

ВИСНОВКИ

Проведене дослідження дозволило комплексно розглянути інформаційно-психологічну війну (ІПВ) проти України як сталу складову гібридної війни, що безпосередньо впливає на публічне управління, ментальну стійкість населення та інституційну спроможність держави. Поставлена мета роботи — проаналізувати стан проблеми ІПВ та обґрунтувати шляхи подолання її наслідків — досягнута шляхом послідовного виконання визначених завдань.

За результатами виконання завдань дослідження отримано такі висновки:

1) Уточнено сутність і еволюцію ІПВ у контексті гібридної війни та визначено ключові механізми психологічного впливу й соціальні індикатори наслідків. Встановлено, що сучасний інформаційно-психологічний вплив поєднує класичні механізми (навіювання, маніпуляцію, емоційне зараження, фреймінг і праймінг) із високотехнологічними інструментами (Big Data, ШІ, психологічний таргетинг, deepfake-технології). Для управлінського виміру операціоналізовано базові індикатори наслідків ІПВ (рівень стресу і тривоги, довіра до інституцій, медіагігієна, соціальна згуртованість), що формує основу для моніторингу та оцінювання ефективності державної політики.

2) Проаналізовано нормативно-правові засади України у сфері протидії ІПВ і визначено методологічні підходи до управлінського аналізу проблеми. Обґрунтовано, що правове забезпечення протидії ІПВ має багаторівневий характер — від загальних законів у сфері інформації та національної безпеки до спеціальних актів у медіасфері, захисті персональних даних, кіберзахисті й стратегічних комунікаціях — та

поступово інтегрується у ширший європейський і євроатлантичний безпековий контекст.

Методологічно доведено доцільність управлінського аналізу ІПВ на основі інструментів PESTLE, SWOT і GAP, а також використання OSINT-підходів і аналітики соціальних мереж як джерела даних для ухвалення рішень.

3) Оцінено український контекст управління у сфері ІПВ, виокремлено ключові ворожі наративи, вразливі групи та ризики для національної безпеки. PESTLE-аналіз підтвердив, що агресор системно експлуатує політичні, економічні, соціальні, технологічні, правові та інші вразливості держави; виокремлено ключові ворожі наративи та запропоновано метрики їх моніторингу з використанням OSINT-інструментів.

Найбільш уразливими групами визначено населення з низьким рівнем цифрової грамотності, осіб у стані хронічного стресу, молодь та родини військових; це напряму підсилює ризики для суспільної згуртованості та керованості державних рішень.

4) Визначено рівень інституційної спроможності держави протистояти ІПВ та встановлено основні розриви у координації, ресурсах і процедурах. SWOT- і GAP-аналізи засвідчили наявність значущих активів (активне громадянське суспільство, мережі фактчекінгу, міжнародна підтримка), однак водночас виявили системні розриви: фрагментарну міжвідомчу координацію, кадровий і технологічний дефіцит, а також відсутність цілісної стратегії інформаційної та психологічної безпеки як управлінської рамки.

5) Розроблено цільову модель протидії ІПВ та запропоновано комплекс управлінських інтервенцій. Цільову модель визначено як бажаний, нормативно окреслений і організаційно забезпечений стан системи державної політики, інститутів та інструментів, що забезпечують

стійкість держави, суспільства й особистості до дезінформації, пропаганди та інших засобів ІПВ; модель має бути системною та проактивною.

Практичні інтервенції конкретизовано через створення/посилення інституційної та технологічної інфраструктури (зокрема Центру інформаційної стійкості, національної платформи фактчекінгу, посилення кіберзахисту критичної інфраструктури), а також через освітні, комунікаційні та психологічні програми як інструменти зниження вразливості.

6) Сформовано план упровадження державної політики подолання наслідків ІПВ та обґрунтовано прогноз розвитку ситуації на 2025–2027 роки. Запропоновано поетапний план реалізації політики (з логікою: підготовка → інституційне зміцнення → масштабування → інтеграція й автоматизація → стійкість і контроль), що включає оновлення нормативної бази, запуск моніторингу та фактчекінгу, масові програми медіаграмотності, розвиток психологічної підтримки й використання AI-рішень для виявлення фейків та ведення реєстру інформаційних атак.

Прогноз на 2025–2027 роки обґрунтовано як інструмент управління ризиками: визначено, що ІПВ матиме системний хвилеподібний характер і концентруватиметься, зокрема, у політичному та економічному вимірах; описано сценарії (оптимістичний/базовий/песимістичний) із різними наслідками для довіри, легітимності та стійкості, а ключовою умовою кращого сценарію є проактивні комунікації та спроможність держави швидко нейтралізувати фейки.

Узагальнюючи результати дослідження, встановлено, що інформаційно-психологічна війна є системним інструментом гібридної агресії, який одночасно впливає на державу (керованість і легітимність рішень), суспільство (згуртованість і довіру) та особистість (психологічну стійкість і поведінкові реакції). Сучасна ІПВ поєднує класичні механізми маніпуляції з технологізованими засобами поширення контенту,

таргетингом та автоматизацією впливу, тому протидія їй має розглядатися не як разове реагування, а як стала функція публічного управління і складова управління ризиками для національної безпеки.

Дослідження показало, що Україна має нормативно-правові засади та практику реагування на інформаційні загрози, однак ключова проблема полягає в узгодженості та спроможності системи: фрагментарність координації і процедур, нерівномірність ресурсів і компетенцій, недостатність єдиного моніторингу та вимірювання результативності. Це створює вразливості, які противник використовує через адаптивні наративи, спрямовані на соціальні "больові точки" та вразливі групи.

Практичний висновок роботи полягає в тому, що ефективна протидія ІПВ потребує комплексної державної політики, яка інтегрує: правові інструменти, інституційну координацію, аналітику й моніторинг (зокрема OSINT та метрики впливу), стратегічні комунікації, а також освітні й соціально-психологічні програми. Запропоновані цільова модель і план упровадження переводять протидію ІПВ у керований цикл політики (виявлення → оцінка → інтервенції → вимірювання → коригування), а прогноз на 2025–2027 роки виступає управлінським інструментом для сценарного планування та підготовки рішень в умовах тривалої гібридної загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Панченко О. А. Інформаційно-психологічна безпека в епоху турбулентності. Київ: КВІЦ, 2020. 472 с.

2. Панченко О. А. Психологічні механізми масової паніки в умовах криз і катастроф // Медична психологія. 2017. № 3. С. 5–15.

3. Панченко О. А. Засоби масової комунікації як платформа державної інформаційної політики // Державне управління: теорія та практика. 2019. № 2. С. 45–56.

4. Панченко О. А. Ментальна стійкість суспільства як об’єкт державного управління в умовах гібридних загроз // Вісник НАДУ. 2021. № 1. С. 30–41.

5. Кукін І. В. Державне управління інформаційною безпекою особистості. Київ: НАДУ, 2018. 256 с.

6. Бондаренко С. І. Маніпулятивні технології в медіа: психологічні аспекти. Харків: ХНУ ім. В. Каразіна, 2020. 256 с.

7. Брижко В. М. Інформаційна безпека держави: правові та організаційні аспекти. Київ: Юрінком Інтер, 2020. 312 с.

8. Герасимчук В. Г. Інформаційно-психологічна безпека: теорія та практика. Київ: НАДУ, 2018. 320 с.

9. Дергачов О. В. Інформаційні війни та психологічні операції. Харків: Право, 2019. 280 с.

10. Ліпкан В. А. Національна безпека України: теорія і практика. Київ: Кондор, 2019. 400 с.

11. Олійник О. М. Кібербезпека та інформаційні загрози: сучасні виклики. Київ: Ліра-К, 2021. 210 с.

12. Шевченко О. В. Інформаційні війни: методи та засоби протидії. Київ: НАДУ, 2021. 280 с.

13. Castells M. The Power of Communication. Oxford: Oxford University Press, 2013. 456 p.

14. European Union Agency for Cybersecurity (ENISA). Cybersecurity Threat Landscape Report. Brussels: ENISA, 2022. 88 p.

15. NATO StratCom COE. Social Media as a Tool of Hybrid Warfare. Riga: NATO Centre of Excellence, 2020. 95 p.

16. RAND Corporation. Countering Russian Information Operations in the Digital Sphere. Santa Monica: RAND, 2021. 120 p.

17. Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. Boston: Houghton Mifflin Harcourt, 2018. 320 p.

18. UNESCO. Journalism, ‘Fake News’ and Disinformation: Handbook for Journalism Education and Training. Paris: UNESCO, 2018. 128 p.

19. Буряк, В. Г. Інформаційно-психологічна війна: сутність та основні напрями впливу // Науковий вісник Академії муніципального управління. 2023. № 2. С. 45–52.

20. Державна служба спеціального зв’язку та захисту інформації України. Інформаційна безпека: аналітичний звіт. – Київ: ДССЗЗІ, 2024. 78 с.

21. Коваль, І. П. Канали поширення дезінформації в Україні: аналіз та протидія // Український журнал інформаційної безпеки. 2023. № 3. С. 12–19.

22. Міністерство оборони України. Доктрина інформаційної безпеки України. Київ: МОУ, 2023. С. 56

23. Петренко, Л. С. Роль неурядових організацій у забезпеченні інформаційної безпеки держави // Держава та право. 2022. № 4. С. 101–108.

24. Рада національної безпеки і оборони України. Стратегія кібербезпеки України на 2025–2030 роки. Київ: РНБО, 2025. 64 с.

25. Сидоренко, М. В. Інформаційні операції в Україні: приклади та наслідки // Аналітичні записки Інституту стратегічних досліджень. 2023. № 5. С. 7–15.

26. Ващенко Н. Головні наративи сучасної російської пропаганди як впливогенна проблематика. Scientific Notes of Institute of Journalism. 2020. Т. 1 (76). С. 180–202.

27. Зозуля О. Фейк як інструмент інформаційної війни. Юридична газета онлайн: сайт. URL: https://yur-gazeta.com/publications/practice/inshe/feyk-yak-instrument-informaciynoyi-viyni.html.

28. Іваницька Б. Основні методи пропаганди в російському інтернет-ЗМІ Pravda.ru. Вісник Національного університету «Львівська політехніка». Серія: Журналістські науки. 2018. № 896. С. 54–58. URL: http://science.lpnu.ua/uk/sjs/vsi-vypusky/zhurnalists

29. Юськів О. Наративи російської пропаганди в Україні. Вісник Львівського університету. Серія: Філософсько-політологічні студії. 2020. Вип. 30. С. 226–232.

30. StopFake. Проект з перевірки фактів та боротьби з дезінформацією URL: https://www.stopfake.org.

31. VoxCheck. Фактчекінг та аналітика URL: https://voxukraine.org/voxcheck

32. Bellingcat. OSINT Toolkit URL: https://www.bellingcat.com/resources/how-tos/2021/10/14/bellingcats-online-investigation-toolkit.

33. Maltego. Інструмент для розслідувань URL: https://www.maltego.com

34. Hoaxy. Візуалізація поширення дезінформації URL: https://hoaxy.osome.iu.edu

35. CrowdTangle. Аналіз контенту в соцмережах URL: https://www.crowdtangle.com

36. TGStat. Аналітика Telegram-каналів URL: https://tgstat.com Brandwatch.

37. Моніторинг соціальних медіа URL: https://www.brandwatch.com

38. Герасимчук В. Г. *Стратегічний менеджмент*. Київ: КНЕУ, 2017. 512 с.

39. Jurevicius, O. *Gap Analysis: The Definitive Guide* URL: https://strategicmanagementinsight.com/tools/gap-analysis/

40. Горбулін В. П., Ланде Д. В. Інформаційні операції та безпека суспільства. Київ: НІСД, 2019. 284 с.

41. Ліпкан В. А. Національна безпека України: навч. посіб. Київ: Кондор, 2018. 368 с.

42. Чернявська О. П. Протидія інформаційним загрозам: аналітичні матеріали. Харків: Право, 2021. 198 с.

43. Ланде Д. В., Снігуров О. В. Інформаційні війни та кібербезпека: монографія. Київ: Інститут кібернетики НАН України, 2022. 256 с.

44. Стратегія інформаційної безпеки України: Указ Президента України від 28.12.2021 № 685/2021. Офіційний вісник Президента України. 2022. № 1.

45. Центр стратегічних комунікацій та інформаційної безпеки URL: https://spravdi.gov.ua (дата звернення: 27.11.2025).

46. Медіаграмотність та протидія дезінформації: Інститут масової інформації. Медіаграмотність в Україні: аналітичний звіт. Київ: IMI, 2023. 45 с. URL: https://imi.org.ua

47. Кіберзахист та інформаційна стійкість: Державна служба спеціального зв’язку та захисту інформації України. Звіт про стан кіберзахисту в Україні у 2023 році. Київ: ДССЗЗІ, 2024. 32 с. URL: https://cip.gov.ua

48. Міжнародні стандарти протидії інформаційним атакам: NATO StratCom COE. Countering Disinformation: Best Practices and Lessons Learned. Riga: NATO Strategic Communications Centre of Excellence, 2022. 60 p. URL: https://stratcomcoe.org

49. CERT-UA. Державна служба спеціального зв’язку та захисту інформації України URL: https://cert.gov.ua

50. NATO StratCom Centre of Excellence URL: https://stratcomcoe.org

51. Hybrid CoE. European Centre of Excellence for Countering Hybrid Threats URL: https://www.hybridcoe.fi (дата звернення: 27.11.2025).