

Харківський національний університет імені В. Н. Каразіна

Філософський факультет

Кафедра політології

**Пояснювальна записка**

до кваліфікаційної роботи бакалавра

на тему «**Вплив інформаційних війн на політичну стабільність  
держав**»

Виконав: здобувач вищої освіти  
4 курсу групи ОП-41 денного відділення  
напряму підготовки 05 - "Соціальні та  
поведінкові науки"  
спеціальності 052 «Політологія»

ОПП «Політичні технології  
та аналіз політики»

Ємельянов Іван Олександрович

Керівник: д. політ. н., професор

Комарова Тетяна Геннадіївна

Рецензент: д. політ. н., проф., професор

Романюк Олександр Іванович

Харків – 2025 року

Харківський національний університет ім. В.Н. Каразіна

Філософський факультет

Кафедра політології

Спеціальність 052 Політологія

Освітньо-професійна програма «Політичні технології та аналіз політик»

Рівень вищої освіти: перший (бакалаврський)

**ЗАТВЕРДЖУЮ:**  
**Завідувач кафедри**

**О.А. ФІСУН**  
(ініціали, прізвище)

\_\_\_\_\_ (підпис)

« \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_  
року

### **ЗАВДАННЯ**

#### **На кваліфікаційну роботу бакалавра**

Ємельянова Івана Олександровича

1. Тема роботи: «Вплив інформаційних війн на політичну стабільність держав»

керівник роботи Комарова Тетяна Геннадіївна, д. політ. н., проф. кафедри політології

затверджені наказом по університету від «22» березня 2024 року № 3801-5/795

2. Строк подання студентом роботи 30.04.2025

3. Перелік питань, які потрібно розробити:

1. Дослідити сутність, ознаки та типологію інформаційних війн як феномену сучасного політичного протистояння.
2. Встановити основні стратегії, методи та засоби реалізації інформаційних війн у політичній сфері.
3. Проаналізувати поняття політичної стабільності, її критерії, чинники забезпечення та загрози в умовах інформаційного впливу.
4. Дослідити механізми впливу інформаційних атак на політичні інститути, рівень довіри до влади та громадську згуртованість.
5. Визначити взаємозв'язок між розвитком інформаційних технологій та зростанням вразливості політичних систем до інформаційного тиску.

## 4. План роботи

№ з/п	Назва етапу роботи	Термін виконання етапу
1	Консультація з керівником щодо обрання теми роботи	30.09.2024
2	Затвердження теми роботи	12.10.2024
3	Аналіз та підбір літературних джерел для написання роботи	30.11.2024
4	Написання змісту до кваліфікаційної роботи	30.12.2024
5	Написання першого розділу та висновків до нього	30.01.2025
6	Написання другого розділу та висновків до нього	28.02.2025
7	Написання вступу до роботи	15.03.2025
8	Написання висновків до роботи	31.03.2025
9	Оформлення списку використаних джерел	15.04.2025
10	Написання анотації	30.04.2025
11	Фінальні коригування та доопрацювання	12.05.2025
12	Переддипломна практика	19.05.2025- 08.06.2025
13	Підготовка доповіді до виступу на захисті кваліфікаційної роботи	20.05.2025
14	Підготовка презентації до виступу на захисті кваліфікаційної роботи	21.05.2025
15	Підготовка до виступу на захисті кваліфікаційної роботи	22.05.2025
16	Передзахист кваліфікаційної роботи	26.05.2025
17	Фінальні коригування та доопрацювання після зауважень на передзахисті	26-29.05.2025
18	Перевірка кваліфікаційної роботи через систему антиплагіат	30.05.2025
19	Захист кваліфікаційної роботи	12.06.2025

5. Дата видачі завдання 30.09.2024

Здобувач вищої освіти



І.О.Ємельянов

Керівник роботи

Т.Г.Комарова

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н.  
КАРАЗІНА  
ПОДАННЯ  
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ  
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ**

Направляється студент *Ємельянов І.О.* до захисту бакалаврської роботи за спеціальністю 052 – політологія на тему: *«Вплив інформаційних війн на політичну стабільність держав»*

Бакалаврська робота і рецензія додаються.

Декан філософського факультету \_\_\_\_\_ Карпенко І. В.

**Довідка про успішність**

Студент *Ємельянов І.О.* за період навчання на філософському факультеті з 2021 року по 2025 рік повністю виконала навчальний план за спеціальністю з таким розподілом оцінок за національною шкалою:

відмінно – \_\_\_\_\_%, добре – \_\_\_\_\_%, задовільно – \_\_\_\_\_%.

Фахівець 1 категорії  
навчального центру організації

освітнього процесу філософського факультету \_\_\_\_\_ Ревкова Н. Є.

**Висновок керівника бакалаврської роботи**

Студент *Ємельянов І.О.* виконав бакалаврську роботу на тему *«Вплив інформаційних війн на політичну стабільність держав»* яка присвячена дослідженню того, як інформаційні війни впливають на політичну стабільність держав через підриг довіри до інститутів влади, маніпулювання громадською думкою та дестабілізацію суспільства.

Керівник бакалаврської роботи:  
професор кафедри політології  
Харківського національного  
університету імені В. Н. Каразіна,  
доктор політичних наук



\_\_\_\_\_ Комарова Т. Г.

\_\_\_\_\_20\_\_\_\_ року

**Висновок кафедри про бакалаврську роботу**

Бакалаврська робота розглянута. Студент *Ємельянов І.О.* допускається до захисту роботи в Екзаменаційній комісії.

Зав. кафедри політології \_\_\_\_\_

\_\_\_\_\_ Фісун О.А

## ЗМІСТ

<u>Зміст</u>	4
<u>Вступ</u>	5
<u>Розділ 1: Теоретико-методологічні засади дослідження інформаційних війн та політичної стабільності</u>	10
<u>1.1. Сутність і типологія інформаційних війн: поняття, ознаки та основні стратегії</u>	10
<u>1.2. Політична стабільність держави: критерії, чинники забезпечення та загрози в умовах інформаційного впливу</u>	
Висновки до розділу 1	20
<u>Розділ 2: Аналіз впливу інформаційних війн на політичну стабільність: приклади, наслідки, протидія</u>	34
<u>2.1. Інформаційні війни в сучасному світі: кейси України, Грузії, США та інших країн</u>	34
<u>2.2. Протидія інформаційним загрозам як чинник забезпечення політичної стабільності: практичні інструменти та державна політика</u>	
Висновки до розділу 2	43
<u>Висновки</u>	58
<u>Список використаних джерел</u>	60

## ВСТУП

Проблематика впливу інформаційних війн на політичну стабільність держави, яка розглядається у цій роботі, набуває особливої актуальності у сучасних умовах, коли інформаційний простір перетворюється на арену глобального протистояння, а інформаційні технології стають не лише інструментом комунікації, а й засобом маніпуляції масовою свідомістю, що, у свою чергу, породжує нові виклики для забезпечення політичної стабільності, оскільки держави стикаються з необхідністю реагувати на багатовимірні загрози, які виникають у традиційних сферах, і, відповідно, у сфері інформаційної безпеки, де інформаційні війни здатні підривати довіру до інститутів влади, провокувати соціальну напругу, а також впливати на формування громадської думки, що підтверджується сучасними тенденціями розвитку інформаційного суспільства, де інформаційні атаки стають дедалі складнішими, а їх наслідки – більш масштабними та непередбачуваними. Актуальність дослідження визначається тим, що у сучасних умовах інформаційні війни стають не лише інструментом досягнення політичних цілей, а й чинником, який безпосередньо впливає на функціонування політичних інститутів, змінює характер політичної взаємодії, створює нові виклики для забезпечення політичної стабільності, що підтверджується зростанням кількості інформаційних атак, спрямованих на дестабілізацію внутрішньополітичної ситуації, маніпулювання громадською думкою, посилення соціальної напруги, а також появою нових форм інформаційного впливу, які потребують глибокого теоретичного осмислення та практичного вирішення.

Ступінь вивченості обраної теми є високою, завдяки значній кількості досліджень, у яких розглядаються окремі аспекти цієї проблематики, зокрема визначення сутності інформаційних війн, їх типології, основних

ознак і стратегій, а також аналізуються механізми впливу інформаційних атак на політичні процеси, однак у більшості робіт відсутній комплексний підхід до вивчення взаємозв'язку між інформаційними війнами та політичною стабільністю, що обумовлює необхідність подальшого дослідження цієї проблеми з урахуванням сучасних тенденцій розвитку інформаційного простору, а також зосередження уваги на виявленні нерозв'язаних питань, пов'язаних із забезпеченням політичної стійкості в умовах інформаційного протистояння.

Метою даної роботи є теоретичне обґрунтування та емпіричний аналіз впливу інформаційних війн на політичну стабільність держави, що передбачає дослідження сутності та типології інформаційних війн, визначення їх основних ознак і стратегій, а також виявлення механізмів, за допомогою яких інформаційні війни здатні впливати на політичну стабільність, з урахуванням сучасних тенденцій розвитку інформаційного простору.

Для досягнення поставленої мети треба виконати наступні завдання: планується з'ясувати сутність інформаційних війн як явища, що впливає на політичні процеси, визначити їхні характерні риси, типи та етапи розвитку, зокрема в контексті сучасних міжнародних конфліктів. Особливу увагу буде приділено вивченню методів та стратегій ведення інформаційної війни — від класичних пропагандистських інструментів до новітніх цифрових технологій, включно з використанням соціальних мереж, бот-мереж і фейкових новин. Аналіз стосуватиметься також політичної стабільності як категорії, її індикаторів, умов підтримання та факторів загроз в умовах цілеспрямованого інформаційного впливу.

Окремо досліджуватимуться механізми, за допомогою яких інформаційні атаки підривають довіру до інститутів влади, провокують соціальну напругу та знижують рівень громадянської згуртованості, що, у свою чергу,

призводить до політичної дестабілізації. Увага буде приділена і аналізу залежності між технологічним розвитком і зростанням вразливості політичних систем: чим більше цифрових інструментів використовується в публічному управлінні та політичній комунікації, тим більшими є ризики маніпуляцій. Завершальним етапом стане вивчення ролі інституцій інформаційної безпеки, їхньої здатності протистояти інформаційним загрозам і забезпечувати стабільність держави в умовах гібридного протистояння.

Об'єктом дослідження виступають процеси, пов'язані з виникненням, розвитком та реалізацією інформаційних війн у сучасному суспільстві.

Предметом дослідження є сукупність властивостей, структурних характеристик, механізмів і зв'язків, що виникають у межах взаємодії інформаційних війн та політичної стабільності а саме – особливості впливу інформаційних атак на політичні інститути, трансформацію громадської думки, динаміку соціальної згуртованості, а також специфіку стратегій, інструментів і технологій.

У процесі дослідження застосовано комплекс загальнонаукових і спеціальних методів, що дозволяє забезпечити всебічний аналіз проблеми. Серед загальнонаукових методів використовувався аналіз, який дав змогу розчленувати складне явище інформаційних війн на окремі складові, виявити їх сутність, типологію, ознаки та стратегії, а також синтез, що забезпечив можливість поєднати отримані результати у цілісну систему знань про вплив інформаційних війн на політичну стабільність. Застосування індукції дозволило на основі окремих фактів і прикладів сформулювати загальні висновки щодо закономірностей впливу інформаційних атак на політичні процеси, а дедукція дала змогу перевірити ці закономірності на конкретних прикладах, що ілюструють взаємозв'язок між інформаційними війнами та політичною стабільністю. Метод порівняння використовувався для зіставлення різних підходів до визначення

сутності інформаційних війн, їх типології та стратегій, а також для аналізу відмінностей у впливі інформаційних атак на політичну стабільність у різних державах. Системний підхід дозволив розглядати інформаційні війни як складне багаторівневе явище, що охоплює різні сфери суспільного життя, а також виявити взаємозв'язки між окремими елементами цього явища та їх вплив на політичну стабільність. Моделювання, як універсальний метод наукового пізнання, дозволило створити теоретичні моделі взаємодії інформаційних війн і політичної стабільності, що дало змогу виявити основні чинники, які визначають ефективність інформаційного впливу, а також сприяло формуванню нових гіпотез щодо механізмів дестабілізації політичної системи під впливом інформаційних атак.

Серед спеціальних методів дослідження застосовувалися морфологічний аналіз, що дав змогу систематизувати всі можливі варіанти впливу інформаційних війн на політичну стабільність, а також визначити структурні та функціональні ознаки інформаційних атак, методи асоціацій і контрольних питань, які сприяли активізації творчого мислення під час аналізу складних ситуацій, пов'язаних із інформаційними війнами, метод мозкового штурму, що дозволив генерувати нові ідеї щодо шляхів протидії інформаційним загрозам, синектика, яка забезпечила поєднання різнорідних елементів у процесі пошуку оптимальних рішень, а також узагальнений евристичний метод, що дозволив формалізувати процедури пошуку нових підходів до забезпечення політичної стабільності в умовах інформаційних війн. Використання цих методів дозволило розкрити сутність і типологію інформаційних війн і обґрунтувати необхідність подальшого вивчення їх впливу на політичну стабільність, розробити рекомендації щодо підвищення рівня інформаційної безпеки. Особливу увагу у дослідженні приділено системно-структурному та синергетичному

підходам, які дозволяють розглядати інформаційні війни як складні відкриті системи, що взаємодіють із зовнішнім середовищем, мають ієрархічну структуру з наявністю емерджентних властивостей та здатністю до самоорганізації, що особливо важливо для аналізу процесів дестабілізації політичної системи під впливом інформаційних атак. Системно-структурний підхід забезпечує інтеграцію знань про різні елементи інформаційних війн, дозволяє виявити стійкі зв'язки між ними, визначити основні механізми впливу на політичну стабільність, а синергетичний підхід дає змогу аналізувати процеси самоорганізації, флуктуації, біфуркації та переходу від хаосу до порядку, що є характерним для сучасних політичних систем, які перебувають під впливом інформаційних загроз.

Основна частина роботи складається з двох блоків: у першому блоці розкриваються теоретико-методологічні засади дослідження інформаційних війн та політичної стабільності, аналізується сутність і типологія інформаційних війн, визначаються їх поняття, ознаки та основні стратегії, у другому блоці здійснюється аналіз впливу інформаційних війн на політичну стабільність держави, розглядаються механізми впливу, а також наводяться приклади конкретних ситуацій, що ілюструють взаємозв'язок між інформаційними війнами та політичною стабільністю. Структура роботи передбачає наявність вступу, двох розділів, висновків, списку використаних джерел, який налічує 52 найменування, загальний обсяг роботи становить 65 сторінок, з яких основного тексту – 55 сторінок.

## **РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН ТА ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ**

### **1.1. Сутність і типологія інформаційних війн: поняття, ознаки та основні стратегії**

Інформаційне протиборство, яке знаходить своє втілення у концепті інформаційної війни, є невід'ємною складовою сучасних геополітичних реалій та суспільних процесів, адже воно виходить далеко за межі традиційного розуміння воєнного конфлікту, охоплюючи значно ширший спектр впливів, спрямованих на деформацію свідомості, зміну поведінкових патернів та нав'язування певних ціннісних орієнтирів цілим суспільствам або окремим соціальним групам і цей феномен, він активно досліджується представниками різних наукових дисциплін, та вимагає комплексного підходу до свого вивчення, оскільки його прояви спостерігаються в політичній, економічній, військовій, культурній та соціальній сферах, причому особливої гостроти набуває питання його впливу в умовах стрімкого розвитку інформаційно-комунікаційних технологій, які надають безпрецедентні можливості для маніпулювання інформаційними потоками та формування громадської думки в глобальному масштабі. Трансформація інформаційної війни з інструментального засобу забезпечення бойових дій у самостійний та повноцінний вид протистояння свідчить про фундаментальні зміни у природі сучасних конфліктів, де перемога може бути досягнута не лише шляхом фізичного знищення

супротивника, але й через підкорення його волі та свідомості, що робить інформаційну війну особливо небезпечною та підступною формою агресії(Проноза, 2018: 117; Грицай, 2023: 26).

Витоки інформаційного протиборства можна простежити ще з давніх часів, коли правителі та полководці вдавалися до різноманітних хитрощів, дезінформації та психологічного тиску для досягнення переваги над ворогом, однак саме в ХХ та на початку ХХІ століття, з появою масових комунікацій, таких як радіо, телебачення, а згодом і Інтернет, інформаційна війна набула рис глобального явища, здатного впливати на долі мільйонів людей та змінювати хід історії. Розвиток теоретичних основ інформаційної війни пов'язаний з іменами багатьох дослідників, які намагалися осмислити нові реалії інформаційної епохи та запропонувати моделі для розуміння цього складного явища, і, як влучно зауважив Маршалл Маклюен, інформація стає ключовим ресурсом, контроль над яким визначає владу та вплив у сучасному світі, перетворюючи інформаційну війну на тотальне протистояння, що охоплює всі сфери суспільного життя, це твердження підкреслює масштаб й глибину проникнення інформаційних впливів, які можуть непомітно, але наполегливо формувати суспільні настрої, політичні уподобання та навіть фундаментальні світоглядні позиції(Яковчук, Малець, Борзов, б.р.: 1).

Визначаючи сутність інформаційної війни, необхідно звернути увагу на її багатоаспектність, оскільки різні наукові школи та дослідницькі підходи акцентують увагу на різних її вимірах, що іноді призводить до певної термінологічної плутанини, проте загальним знаменником є розуміння її як цілеспрямованої діяльності, спрямованої на досягнення інформаційної переваги над супротивником шляхом маніпулювання інформацією (Проноза, 2018). Деякі дослідники, а саме - О.В. Курбан, наголошує на комплексному характері заходів, що включають вплив на

інформаційні ресурси, інформаційні процеси, а також на свідомість населення та особового складу збройних сил, підкреслюючи, що метою таких дій є не лише дезорганізація управління та підірив морального духу, але й нав'язування вигідних наративів, які спотворюють реальну картину світу і це свідчить про те, що інформаційна війна ведеться не лише в технічній площині, але й у ментальному просторі, де відбувається боротьба за інтерпретацію подій та смислів(Курбан, 2016: 10).

Інформаційна війна, як інтелектуальний вид протиборства, висуває на перший план не матеріально-технічні ресурси, хоча вони й залишаються важливими, а здатність генерувати переконливі інформаційні повідомлення, які можуть ефективно впливати на свідомість та поведінку цільових аудиторій, що вимагає глибоких знань у галузі психології, соціології, культурології та комунікаційних технологій (Пашенко, 2023: 125). Використання інформаційної зброї, що включає широкий арсенал методів, таких як дезінформація, пропаганда, маніпуляція фактами, поширення чуток, створення фейкових новин та використання ботоферм у соціальних мережах, стає ключовим інструментом для досягнення цілей інформаційної війни, дозволяючи сіяти паніку, розпалювати ворожнечу, підіривати довіру до державних інститутів та дестабілізувати суспільство зсередини. Причому, на відміну від традиційних воєн, інформаційна війна може вестися приховано, без офіційного оголошення, поступово руйнуючи основи державності та суспільної злагоди, що робить її особливо небезпечною для країн, які не приділяють належної уваги питанням інформаційної безпеки. Ключовими ознаками, що дозволяють ідентифікувати інформаційну війну, є, по-перше, чітко визначені суб'єкти та об'єкти впливу, де в ролі суб'єктів можуть виступати не лише державні структури та спецслужби, а й різноманітні недержавні актори, включаючи медіа-корпорації, громадські організації, хакерські угруповання та навіть

окремі впливові особи, тоді як об'єктами стають як окремі індивіди, так і цілі соціальні групи, державні інститути, економічні системи та інформаційна інфраструктура. По-друге, це цілеспрямованість інформаційного впливу, який завжди підпорядкований досягненню конкретних стратегічних або тактичних цілей, будь то дискредитація політичного керівництва, зміна зовнішньополітичного курсу, провокування внутрішніх конфліктів чи отримання економічних дивідендів. По-третє, це використання специфічних методів та технологій інформаційно-психологічного впливу, які базуються на глибокому розумінні механізмів людського сприйняття, мотивації та поведінки, а також на використанні вразливостей у системі масової комунікації і ці методи постійно еволюціонують, адаптуючись до нових технологічних можливостей та змін у соціально-культурному середовищі, що вимагає від дослідників та практиків постійного оновлення знань та навичок (Ухаль, 2023: 21-23).

Важливою характеристикою інформаційних війн є їх системність та тривалість, оскільки для досягнення стійких змін у свідомості та поведінці цільових аудиторій зазвичай недостатньо одноразових інформаційних атак; натомість потрібні довготривалі, скоординовані кампанії, які поступово, крок за кроком, формують необхідні уявлення та стереотипи. Масштабність інформаційних війн також є їхньою невід'ємною рисою, особливо в епоху Інтернету, коли інформація може миттєво поширюватися по всьому світу, долаючи державні кордони та мовні бар'єри, що дозволяє агресорам впливати на глобальну громадську думку та створювати міжнародний резонанс. Прихованість багатьох операцій інформаційної війни, особливо тих, що проводяться в кіберпросторі, створює значні труднощі для їх виявлення, атрибуції та вироблення адекватних заходів протидії, оскільки агресор часто діє анонімно, використовуючи проксі-сервери, ботнети та

інші засоби маскуванню, що ускладнює притягнення його до відповідальності та застосування міжнародних санкцій. Ця асиметричність та складність атрибуції є одними з визначальних викликів сучасної інформаційної безпеки(Жадько, 2018: 65-66).

Типологізація інформаційних війн є важливим кроком на шляху до їх глибшого розуміння та розробки ефективних стратегій протидії і цієї класифікації, як правило, базуються на таких критеріях: об'єкти впливу, цілі, використовувані інструменти та характер протиборства. Мартін Лібікі, один із піонерів дослідження інформаційної війни, запропонував детальну класифікацію, що включає сім основних форм: командно-управлінську війну, спрямовану на дезорганізацію системи управління супротивника; розвідувальну війну, що ґрунтується на отриманні та використанні розвідувальної інформації, електронну війну, що передбачає вплив на електронні системи; психологічну війну, метою якої є вплив на свідомість та емоції; хакерську війну, що полягає в атаках на комп'ютерні системи; економічну інформаційну війну, спрямовану на підрив економіки; та кібервійну, що охоплює весь спектр ворожих дій у віртуальному просторі. Ця класифікація, незважаючи на свій вік, продовжує залишатися актуальною, оскільки вона відображає ключові напрямки інформаційного протиборства, хоча й потребує певних доповнень з урахуванням нових технологій та форм ведення війни. Інші підходи до типології можуть базуватися на цілях, які переслідує агресор, що дозволяє виділити інформаційні війни, спрямовані на досягнення політичних, економічних, військових чи ідеологічних переваг, або на характері впливу, розрізняючи, наприклад, деструктивні інформаційні війни, метою яких є руйнування інформаційної інфраструктури та дезорганізація суспільства, та конструктивні інформаційні операції, спрямовані на формування позитивного іміджу або просування певних ідей. Розмежування,

запропоноване Дж. Арквіллою та Д. Ронфельдтом, між кібервійною, яка пов'язана з військовими операціями в кіберпросторі, та мережевою війною, що стосується суспільних конфліктів, де використовуються мережеві форми організації та комунікації, також є важливим для розуміння різноманіття форм інформаційного протистояння, оскільки воно вказує на те, що інформаційні війни можуть вестися не лише між державами, але й за участю недержавних акторів, таких як терористичні організації, кримінальні угруповання або громадські рухи. Сучасні реалії демонструють, що інформаційні війни все частіше набувають гібридного характеру, поєднуючи елементи різних типів та використовуючи широкий спектр інструментів, що робить їх аналіз та протидію ще складнішими завданнями(Ухаль, 2023: 25 - 27).

Стратегії, що застосовуються в інформаційних війнах, є надзвичайно різноманітними та адаптивними, оскільки вони повинні враховувати специфіку цільової аудиторії, особливості інформаційного простору та конкретні цілі, які ставить перед собою агресор, однак можна виділити кілька ключових напрямків, які є характерними для більшості сучасних інформаційних конфліктів. Стратегія інформаційного домінування, як одна з найбільш важливих, передбачає встановлення контролю над основними каналами поширення інформації, що дозволяє нав'язувати власні наративи, формувати громадську думку та ефективно придушувати будь-які альтернативні точки зору, створюючи таким чином спотворену інформаційну реальність, в якій супротивник позбавлений можливості об'єктивно оцінювати ситуацію та приймати адекватні рішення. Реалізація цієї стратегії може включати як створення потужних пропагандистських медіа-ресурсів, так і використання більш прихованих методів, як фінансування лояльних ЗМІ, підкуп журналістів, поширення дезінформації через соціальні мережі за допомогою ботоферм та тролів, а також

здійснення кібератак на незалежні інформаційні ресурси. Стратегія дезінформації та пропаганди є однією з найдавніших та найпоширеніших стратегій інформаційної війни, яка полягає у цілеспрямованому поширенні неправдивої, спотвореної або неповної інформації з метою введення супротивника в оману, підриву його довіри до власних джерел інформації, формування негативного образу ворога та мобілізації власних прихильників (Грицай, 2023: 28). Дезінформаційні кампанії часто мають складну, багат шарову структуру, використовуючи різноманітні канали поширення та адаптуючи повідомлення до особливостей різних цільових аудиторій, причому особлива увага приділяється створенню правдоподібних фейкових новин, маніпулюванню фото- та відеоматеріалами, а також використанню так званих агентів впливу, які свідомо чи несвідомо поширюють дезінформацію, користуючись своїм авторитетом або популярністю. Пропаганда, як зазначає О.В. Курбан, є невід'ємною складовою інформаційної війни, яка використовує емоційний вплив, апеляцію до стереотипів та ідеологічних кліше для формування певних установок та мобілізації мас на підтримку дій агресора (Курбан, 2016: 55-58). Стратегія психологічного виснаження та деморалізації спрямована на підрив морально-психологічного стану населення та збройних сил супротивника, створення атмосфери страху, невпевненості, апатії, недовіри до влади та розколу в суспільстві, що може суттєво знизити його здатність до опору та полегшити досягнення цілей агресора (Пашенко, 2023: 128). Ця стратегія може реалізовуватися шляхом поширення панічних чуток, залякування населення терористичними актами або демонстрацією військової сили, проведенням цілеспрямованих атак на культурні та історичні символи, що мають важливе значення для національної ідентичності, а також шляхом дискредитації лідерів та розпалювання внутрішніх конфліктів. Наративи, як смислові конструкції, що формують уявлення про реальність та впливають на поведінку людей, відіграють ключову роль у цій стратегії, оскільки

створення та поширення деструктивних наративів, які підривають основи суспільної злагоди та національної єдності, є надзвичайно ефективним механізмом психологічного впливу (Грицай, 2023: 28).

Кібернетичні стратегії в інформаційній війні набувають все більшого значення в умовах цифровізації суспільства та зростаючої залежності від інформаційних технологій, оскільки вони дозволяють здійснювати прямий вплив на інформаційні системи та мережі супротивника, викрадати конфіденційну інформацію, порушувати роботу критично важливих об'єктів інфраструктури, проводити шпигунські операції та дезорганізувати систему державного та військового управління (Borden, 1999: 3-5). Арсенал методів кібервпливу є надзвичайно широким і включає хакерські атаки, поширення шкідливого програмного забезпечення, таке як віруси, трояни, програми-шпигуни та програми-вимагачі, здійснення DDoS-атак для блокування доступу до веб-ресурсів, фішинг для отримання облікових даних користувачів, а також більш складні операції, спрямовані на проникнення в закриті мережі та отримання контролю над системами управління. Наслідки успішних кібератак можуть бути катастрофічними, спричиняючи значні економічні збитки, порушуючи функціонування державних служб, створюючи загрозу для національної безпеки та навіть призводячи до людських жертв. Стратегія інформаційної блокади є складною для реалізації в повному обсязі в сучасному глобалізованому світі, але є актуальним інструментом інформаційної війни, який передбачає обмеження або повне припинення доступу супротивника до важливих інформаційних ресурсів та каналів комунікації з метою його ізоляції, позбавлення можливості отримувати об'єктивну інформацію та поширювати власні повідомлення. Ця стратегія може включати як технічні заходи, такі як глушіння радіо- та телесигналів, блокування інтернет-ресурсів, фільтрація трафіку, так і фізичне знищення об'єктів

інформаційної інфраструктури, а також адміністративні заходи, такі як введення цензури, обмеження діяльності іноземних ЗМІ та переслідування незалежних журналістів. Створення інформаційного вакууму або суттєве спотворення інформаційного поля на території супротивника створює сприятливі умови для проведення інших інформаційних операцій, таких як пропаганда та дезінформація, оскільки позбавляє населення можливості критично оцінювати отримувану інформацію та порівнювати її з альтернативними джерелами(Ухаль, 2023: 55).

Ефективність будь-якої стратегії інформаційної війни значною мірою залежить від глибокого розуміння особливостей цільової аудиторії, її культурних, психологічних, соціальних та політичних характеристик, а також від здатності адаптувати інформаційний вплив до конкретних умов та обставин, що вимагає не лише технічних знань, але й гуманітарної експертизи. Джеймс Фарвелл у своїх працях наголошує на необхідності розробки комплексних комунікаційних стратегій, які б враховували не лише канали поширення інформації, але й глибинні механізми її сприйняття, інтерпретації та впливу на свідомість та поведінку людей, що передбачає проведення ретельних досліджень цільових аудиторій, аналіз їхніх інформаційних потреб, цінностей, страхів та очікувань. Тільки такий комплексний підхід дозволяє створювати справді ефективні інформаційні повідомлення, які здатні досягати поставлених цілей та забезпечувати перевагу в інформаційному протиборстві(Farwell, 2020: 15-19).

Невід'ємною складовою інформаційної війни є й заходи з інформаційної безпеки, які спрямовані на захист власного інформаційного простору, ресурсів, інфраструктури та суспільства від ворожих інформаційних впливів, а також на виявлення, аналіз та нейтралізацію інформаційних атак супротивника. Ці заходи мають комплексний характер і включають технічний захист інформаційних систем та мереж, розробку та

впровадження стандартів інформаційної безпеки, контрпропаганду та спростування дезінформації, розвиток медіаграмотності населення та формування критичного мислення, а також правове регулювання інформаційної сфери та створення ефективних механізмів реагування на інформаційні загрози. Як зазначено в Доктрині інформаційної безпеки України, захист українського суспільства від деструктивної пропаганди та агресивного інформаційного впливу, спрямованого на підрив суверенітету та територіальної цілісності, є одним із ключових національних інтересів та пріоритетів державної політики, що підкреслює, що інформаційна війна є двостороннім процесом, де успіх залежить не лише від здатності ефективно атакувати, але й від спроможності надійно захищати власний інформаційний простір (Zhadko, 2018: 64 - 65).

Перехід інформаційного протиборства на новий етап, де воно стає самостійним і часто домінуючим фактором у міжнародних відносинах та внутрішньополітичних процесах, вимагає від науковців, політиків та військових розробки більш досконаlih методів аналізу, прогнозування та протидії інформаційним загрозам, а також переосмислення традиційних підходів до забезпечення національної та міжнародної безпеки. Зростаюча роль соціальних мереж як основного каналу комунікації, поширення інформації та дезінформації, а також як інструменту мобілізації та координації дій, створює нові виклики, оскільки вони дозволяють здійснювати швидкий, масштабний та часто анонімний вплив на суспільну свідомість, обходячи традиційні медіа та державний контроль. Це вимагає постійного моніторингу інформаційного простору, розробки гнучких та адаптивних стратегій реагування, а також міжнародної співпраці у боротьбі з транскордонними інформаційними загрозами. Подальше концептуальне осмислення інформаційної війни, уточнення її термінології, розробка уніфікованих класифікаційних систем та створення онтологічної основи

для майбутніх теорій, як пропонує Джастін Волтерман, є надзвичайно важливим завданням, яке сприятиме глибшому розумінню природи цього складного феномену та розробці ефективніших засобів забезпечення інформаційної стійкості в сучасному світі (Wolterman, 2019: 2).

## **1.2. Політична стабільність держави: критерії, чинники забезпечення та загрози в умовах інформаційного впливу**

Політична стабільність держави, як якісна характеристика політичної системи суспільства, що відображає її стійкість, здатність ефективно функціонувати та розвиватися в умовах внутрішніх і зовнішніх змін, а також забезпечувати правопорядок і громадянський мир, виступає одним з ключових об'єктів політологічного аналізу, особливо в контексті глобалізаційних процесів та системних трансформацій, що характерні, зокрема, для пострадянських суспільств, де вона зазнає значних викликів, пов'язаних із соціально-економічними кризами перехідної доби. Сама сутність політичної стабільності охоплює не лише збереження існуючого політичного режиму чи уряду, але й передбачає такий стан політичного життя, за якого забезпечується підтримка легітимності влади, ефективність її діяльності у виконанні суспільно значущих функцій та її здатність політичної системи до самовідтворення та адаптації до змінюваних умов без руйнівних конфліктів, що підкреслює динамічний, а не статичний характер цього феномену. У цьому контексті, дослідження інститутів інформаційної безпеки сучасної держави набуває особливої ваги, оскільки вони виступають як вагомий чинник суспільно-політичної стабільності, покликаний забезпечувати захищеність життєво важливих інтересів особистості, суспільства та держави від інформаційних загроз, що можуть мати деструктивний вплив на політичні процеси та інститути (Яворський 2017, Міненко 2024: 1, 3).

Критерії політичної стабільності є багатограними і включають оцінку рівня довіри громадян до політичних інститутів, ефективність механізмів прийняття та реалізації політичних рішень, стан правопорядку та рівень політичного насильства, а також здатність політичної еліти до консенсусу та консолідації навколо національних інтересів, що всебічно впливає на загальну атмосферу в суспільстві та його спроможність до поступального розвитку. Розглядаючи політичну стабільність як динамічну рівновагу політичної системи, важливо враховувати її здатність не лише зберігати свою цілісність під тиском дестабілізуючих чинників, але й здійснювати необхідні перетворення, що відповідають суспільним очікуванням та викликам часу, уникаючи при цьому глибоких соціальних потрясінь. В умовах інформаційного суспільства, де інформація стає стратегічним ресурсом і водночас потенційним джерелом загроз, критерієм стабільності також виступає стійкість держави до зовнішніх та внутрішніх інформаційних впливів, спрямованих на підрив її суверенітету, територіальної цілісності чи конституційного ладу. Наприклад, функціонування інститутів інформаційної безпеки, що забезпечують захист інформаційного простору, є не просто технічним завданням, а важливою складовою забезпечення політичної стабільності, адже неконтрольоване поширення дезінформації чи ворожої пропаганди може суттєво дестабілізувати суспільно-політичну ситуацію, провокуючи конфлікти та підриваючи довіру до влади. Тому вивчення ключових елементів інформаційної безпеки держави — таких як регулювання доступу до інформації, захист інформаційної інфраструктури, забезпечення безпечного розвитку інформаційного простору, охорона національного інформаційного ринку, а також протидія інформаційному тероризму та війні — становить невід’ємну складову аналізу чинників, що впливають на політичну стабільність. (Степко 2015: 75).

Забезпечення політичної стабільності держави в сучасному світі нерозривно пов'язане з ефективністю державної інформаційної політики та функціонуванням системи інформаційної безпеки, оскільки інформаційний простір перетворився на арену не лише конкуренції, але й прямого протиборства, де застосовуються технології маніпулювання суспільною свідомістю та підриву державних інститутів. Одним з ключових чинників забезпечення стабільності є формування національної системи протидії інформаційним загрозам, яка б включала технічні засоби захисту інформації та інформаційної інфраструктури та комплекс заходів, спрямованих на підвищення медіаграмотності населення, розвиток критичного мислення та утвердження національних цінностей в інформаційному просторі, що сприяло б зменшенню вразливості суспільства до деструктивних інформаційних впливів. Ефективне функціонування такої системи передбачає чітку координацію зусиль державних органів, громадянського суспільства та приватного сектору, а також наявність сучасної нормативно-правової бази, що регулює відносини в інформаційній сфері та встановлює відповідальність за поширення шкідливого контенту. Дослідження показують, що рівень політичної стабільності безпосередньо корелює з рівнем інформаційної безпеки країни, адже недостатній захист інформаційних ресурсів та інфраструктури може призвести до серйозних економічних втрат, порушення функціонування систем державного управління та оборони, а також до соціальної напруженості, викликані поширенням панічних настроїв чи недостовірної інформації. Розвиток інститутів інформаційної безпеки, таким чином, стає стратегічним пріоритетом для будь-якої держави, яка прагне забезпечити свій сталий розвиток та політичну стабільність в умовах глобальної інформаційної конкуренції та гібридних загроз (Міненко 2024: 76-78). Здатність держави ефективно реагувати на інформаційні атаки, які можуть мати різноманітний характер, від поширення фейкових

новин та пропаганди до складних кібератак на об'єкти критичної інфраструктури, є важливим чинником підтримки політичної стабільності, що потребує постійного вдосконалення як технічних, так і організаційно-правових механізмів захисту. Інформаційна взаємодія у політико-владному полі, особливо у великих містах, які є центрами концентрації інформаційних потоків та соціально-політичної активності, демонструє складність управління інформаційними процесами та необхідність налагодження ефективних каналів комунікації між владою та суспільством для запобігання інформаційним кризам та маніпуляціям (Ковалевський 2010: 15-17). Важливим аспектом забезпечення стабільності є також формування суспільної стійкості до інформаційно-психологічних впливів, що досягається через освітні програми, розвиток незалежних медіа та підтримку громадських ініціатив, спрямованих на боротьбу з дезінформацією. Не менш значущим є міжнародне співробітництво у сфері інформаційної безпеки, оскільки багато інформаційних загроз мають транскордонний характер і потребують спільних зусиль для їх нейтралізації, що особливо актуально для країн, які стикаються з цілеспрямованими інформаційними кампаніями з боку інших держав. Створення комплексної системи моніторингу та реагування на комп'ютерні атаки, якою є діяльність FinCERT у Російській Федерації, каже нам про усвідомлення державами важливості захисту фінансово-кредитної сфери, яка є однією з пріоритетних цілей для кіберзлочинців та суб'єктів інформаційної війни (Nguyen 2021: 14).

Загрози політичній стабільності в умовах інформаційного впливу є надзвичайно різноманітними та динамічними, що зумовлено швидким розвитком інформаційно-комунікаційних технологій та їх активним використанням різними акторами, включаючи державні спецслужби, терористичні організації, кримінальні угруповання та політичні сили, для

досягнення своїх цілей. Однією з найсерйозніших загроз є інформаційна війна, яка передбачає цілеспрямоване використання інформації для завдання шкоди іншій державі шляхом маніпулювання суспільною думкою, дискредитації органів влади, провокування соціальних конфліктів та підризу національної єдності. Технології мікротаргетингу, що дозволяють доставляти специфічні повідомлення вузьким групам населення на основі їхніх психологічних профілів та поведінкових даних, значно посилюють ефективність таких впливів, роблячи їх менш помітними та складнішими для виявлення та нейтралізації. Поширення дезінформації та фейкових новин через соціальні мережі та інші онлайн-платформи стало повсякденним явищем, що здатне швидко дестабілізувати ситуацію, викликаючи паніку, недовіру до офіційних джерел інформації та розпалюючи ворожнечу між різними соціальними групами. Такі інформаційні операції часто спрямовані на ерозію довіри до демократичних інститутів, зокрема виборчих процесів, що може призвести до політичної кризи та втрати легітимності влади (Albert 2023: 16-17, 21).

У внутрішньополітичному розрізі, інформаційний вплив може використовуватися для посилення існуючих суспільних розколів, маніпулювання протестними настроями та дискредитації політичних опонентів, що створює сприятливе підґрунтя для дестабілізації. Наприклад, російські спецслужби та пропагандистські структури активно використовують інформаційні кампанії для інспірування вертикальної напруженості між суспільством та владою в Україні, зокрема, шляхом поширення наративів про нелегітимність влади або необхідність проведення виборів в умовах воєнного стану, розраховуючи на посилення внутрішніх суперечностей та ослаблення держави. Корупційні скандали, навіть якщо вони мають реальне підґрунтя, можуть бути використані та багатократно посилені за допомогою інформаційних технологій для

дискредитації політичного керівництва та зниження рівня суспільної довіри, що, у свою чергу, є значною загрозою для політичної стабільності. Таким чином, падіння довіри суспільства до політичного керівництва, часто підживлюване цілеспрямованими інформаційними атаками, розглядається як одна з ключових загроз внутрішньополітичній стабільності (Павленко та ін. 2024: 29). Посилення інформаційної присутності держави, яке не супроводжується адекватною стратегією комунікації та забезпеченням доступу до правдивої інформації, може призвести до зворотного ефекту, поглиблюючи кризу довіри та створюючи умови для поширення чуток і маніпуляцій. Ще одним виміром є кіберзагрози інформаційного впливу на політичну стабільність, оскільки атаки на критично важливі об'єкти інфраструктури, такі як енергетичні системи, транспортні мережі, фінансові установи та системи державного управління, можуть мати катастрофічні наслідки, викликаючи економічні збитки, хаос та соціальну дестабілізацію. Сучасні інформаційні технології надають широкий спектр інструментів для здійснення таких атак, починаючи від розподілених атак на відмову в обслуговуванні, це таке звані DDoS, і закінчуючи складними операціями з проникнення в закриті мережі та викрадення або знищення даних. Захист інформаційної інфраструктури держави вимагає не лише значних фінансових та технологічних ресурсів, але й високого рівня координації між державними та приватними структурами, а також постійного оновлення знань та навичок фахівців у сфері кібербезпеки. Інформаційний тероризм, що передбачає використання інформаційних технологій для здійснення терористичних актів або їх інформаційної підтримки, також є серйозною загрозою, яка може призвести до значних людських жертв, руйнувань та поширення страху в суспільстві, тим самим підриваючи політичну стабільність. Усвідомлення цих загроз спонукає держави до розробки комплексних стратегій інформаційної безпеки, які б охоплювали всі аспекти захисту від інформаційних впливів, від технічного

захисту до контрпропаганди та розвитку інформаційної культури суспільства(Степко 2015: 75).

Проблема визначення самої політичної стабільності є предметом тривалих наукових дискусій, і різні дослідники пропонують власні підходи до її класифікації та вимірювання, що ускладнює формування універсальних критеріїв та механізмів її забезпечення. Деякі автори розглядають політичну стабільність переважно з точки зору збереження існуючого політичного порядку та відсутності насильницьких конфліктів, тоді як інші наголошують на важливості динамічного розвитку, адаптивності політичної системи та її здатності забезпечувати суспільний прогрес (Яворський 2017: 131-132). У дисертаційних дослідженнях, присвячених цій проблематиці, політична стабільність часто аналізується у зв'язку з питаннями політичної безпеки, етнічними та релігійними факторами, що впливають на суспільну злагоду, проте аспекти інформаційного забезпечення політичної стабільності нерідко розглядаються лише побіжно або фрагментарно, що свідчить про актуальність подальшого вивчення механізмів впливу інформаційного середовища на стійкість політичних систем і це акцентує на необхідності комплексного підходу до розуміння політичної стабільності, який би враховував взаємодію політичних, економічних, соціальних, культурних та інформаційних чинників. В контексті інформаційного впливу, забезпечення політичної стабільності вимагає від держави не лише реактивних заходів, спрямованих на нейтралізацію вже існуючих загроз, але й проактивної стратегії, що передбачає формування стійкого та безпечного інформаційного простору, що включає розвиток національного інформаційного контенту, підтримку незалежних та відповідальних ЗМІ, підвищення рівня медіаграмотності громадян, створення ефективних механізмів виявлення та спростування дезінформації (Міненко 2024:

145-147). Важливу роль у цьому процесі відіграють інститути громадянського суспільства, які можуть сприяти моніторингу інформаційного простору, викриттю маніпулятивних кампаній та поширенню достовірної інформації. Ефективна інформаційна політика держави повинна базуватися на принципах прозорості, підзвітності та діалогу з суспільством, оскільки саме довіра є ключовим ресурсом у боротьбі з інформаційними загрозами. Відсутність такої довіри створює вакуум, який швидко заповнюється чутками, дезінформацією та пропагандою, що може мати руйнівні наслідки для політичної стабільності. Створення системи стратегічних комунікацій, здатної не лише інформувати населення про діяльність органів влади, але й формувати позитивний імідж держави на міжнародній арені та протидіяти ворожим наративам, є одним із пріоритетних завдань у забезпеченні інформаційної складової національної безпеки і, відповідно, політичної стабільності(Ковалевський 2010: 55-58).

Розглядаючи чинники, що сприяють політичній стабільності, неможливо оминати роль правової держави та ефективного врядування, оскільки саме вони створюють підґрунтя для суспільної злагоди, економічного розвитку та довіри громадян до влади. Політична стабільність не є самоціллю, а скоріше умовою для ефективного функціонування та розвитку політичної системи суспільства, що дозволяє вирішувати нагальні проблеми та досягати суспільно значущих цілей (Яворський 2017: 134). В умовах інформаційного суспільства, прозорість діяльності органів влади, доступ громадян до інформації про їхню діяльність та можливість участі у процесах прийняття рішень стають важливими факторами легітимації влади та зміцнення політичної стабільності. Навпаки, закритість, корупція та ігнорування суспільних інтересів створюють сприятливі умови для поширення негативних інформаційних впливів та підриву довіри до

державних інститутів. З огляду на це, розвиток електронного урядування та запровадження сучасних інформаційно-комунікаційних технологій у сфері публічного адміністрування можуть сприяти підвищенню ефективності та прозорості державного управління, що, в свою чергу, позитивно впливатиме на політичну стабільність, але, цифровізація несе в собі нові ризики, пов'язані з можливістю витоку даних, кібератаками на державні інформаційні системи та поширенням цифрової нерівності, що потребує комплексного підходу до управління цими процесами(Міненко 2024: 88-90).

Сферою що впливає на стабільність держави є, безумовно сфера міжнародних відносин, особливо в умовах глобалізації та зростаючої взаємозалежності держав, це включає в себе зовнішні інформаційні впливи, спрямовані на дестабілізацію внутрішньополітичної ситуації, можуть бути частиною гібридних війн або стратегій окремих держав, спрямованих на досягнення геополітичних цілей. Забезпечення стійкості до таких впливів вимагає не лише сильної національної системи інформаційної безпеки, але й активної зовнішньої політики, спрямованої на формування сприятливого міжнародного середовища, розвиток союзницьких відносин та участь у міжнародних ініціативах з протидії інформаційним загрозам. Ефективність боротьби з транскордонними інформаційними загрозами, такими як кіберзлочинність та міжнародний тероризм, значною мірою залежить від рівня міжнародного співробітництва та обміну інформацією між правоохоронними органами та спецслужбами різних країн. З іншого боку, надмірна залежність від зовнішніх інформаційних джерел або технологій може створювати додаткові вразливості для політичної стабільності, тому розвиток власного інформаційного потенціалу та диверсифікація інформаційних зв'язків є важливими завданнями для будь-якої держави(Albert 2023: 18-19).

Психологічний вимір інформаційного впливу на політичну стабільність заслуговує на окрему увагу, оскільки маніпулятивні технології часто спрямовані на емоційну сферу людини, її страхи, упередження та стереотипи. Поширення панічних настроїв, розпалювання соціальної ворожнечі, формування синдрому недовіри та апатії – все це може бути результатом цілеспрямованих інформаційно-психологічних операцій, що підривають основи суспільної згуртованості та створюють умови для політичної дестабілізації (Міненко 2024: 11, 105-107). У цьому контексті, підвищення психологічної стійкості населення до маніпулятивних впливів, розвиток навичок критичного аналізу інформації та формування культури відповідального споживання інформаційного контенту стають важливими чинниками забезпечення політичної стабільності. Освітні програми з медіаграмотності, спрямовані на різні вікові та соціальні групи, можуть відіграти значну роль у підвищенні рівня інформаційної культури суспільства та його здатності протистояти деструктивним інформаційним впливам. Важливо також, щоб держава та суспільні інститути забезпечували доступ до якісної психологічної допомоги для осіб, які постраждали від інформаційних атак або зазнали негативного психологічного впливу внаслідок поширення шкідливого контенту.

На останок варто сказати, що політична стабільність не є статичним станом, а динамічним процесом, що вимагає постійних зусиль з боку держави та суспільства для її підтримки та зміцнення, особливо в умовах швидких змін та зростаючих інформаційних загроз. Адаптивність політичної системи, її здатність своєчасно реагувати на нові виклики та ефективно управляти кризовими ситуаціями є ключовими критеріями її стійкості. В інформаційну епоху це означає, зокрема, здатність держави швидко адаптувати свої стратегії інформаційної безпеки до нових технологій та методів інформаційного впливу, а також гнучко реагувати на

зміни в інформаційному середовищі. Розвиток аналітичних центрів, що займаються моніторингом інформаційних загроз та розробкою рекомендацій для органів влади, а також залучення наукової спільноти до вирішення проблем інформаційної безпеки, можуть сприяти підвищенню адаптивності держави у цій сфері. Політична воля керівництва держави та наявність необхідних ресурсів для реалізації заходів із забезпечення інформаційної безпеки є вирішальними факторами успіху в цій справі, адже без них будь-які стратегії та концепції залишаться лише на папері, а забезпечення балансу між свободою слова та необхідністю захисту інформаційного простору від шкідливих впливів є одним із найскладніших завдань для демократичних держав, яке потребує постійного пошуку оптимальних рішень та врахування як національних інтересів, так і міжнародних стандартів у сфері прав людини (Міненко 2024: 187-189).

Отже, у процесі аналізу теоретико-методологічних засад, що стосуються інформаційних війн і політичної стабільності, у першому розділі було досліджено, що інформаційне протиборство, яке набуло форми концепту інформаційної війни, стало невід'ємною складовою сучасних геополітичних реалій і суспільних процесів, виходячи далеко за межі класичного розуміння воєнного конфлікту та охоплюючи широкий спектр впливів, спрямованих на трансформацію свідомості, зміну моделей поведінки та нав'язування певних ціннісних орієнтирів як цілим суспільствам, так і окремим соціальним групам. Цей феномен, що перебуває у фокусі наукових досліджень, вимагає комплексного підходу до вивчення, оскільки його прояви фіксуються у політичній, економічній, військовій, культурній та соціальній сферах, набуваючи особливої гостроти в умовах стрімкого розвитку інформаційно-комунікаційних технологій, які відкривають безпрецедентні можливості для маніпулювання інформаційними потоками та формування громадської думки на

глобальному рівні. Трансформація інформаційної війни з допоміжного інструменту забезпечення бойових дій у самостійний і повноцінний вид протистояння свідчить про фундаментальні зміни у природі сучасних конфліктів, де перемога досягається не лише фізичним знищенням супротивника, а й підкоренням його волі та свідомості, що робить інформаційну війну особливо небезпечною та підступною формою агресії. Визначаючи сутність інформаційної війни, слід враховувати її багатовимірність, оскільки різні наукові школи та дослідницькі підходи акцентують увагу на різних аспектах, проте спільним є розуміння її як цілеспрямованої діяльності, спрямованої на досягнення інформаційної переваги шляхом маніпулювання інформацією, причому комплексний характер заходів охоплює вплив на інформаційні ресурси, інформаційні процеси, а також на свідомість населення та особового складу збройних сил, маючи на меті не лише дезорганізацію управління та підрив морального духу, а й нав'язування вигідних наративів, що спотворюють реальну картину світу. Інформаційна війна, як інтелектуальний різновид протиборства, висуває на перший план здатність створювати переконливі інформаційні повідомлення, які ефективно впливають на свідомість і поведінку цільових аудиторій, що вимагає глибоких знань у сфері психології, соціології, культурології та комунікаційних технологій, а використання інформаційної зброї, що включає широкий арсенал методів – дезінформацію, пропаганду, маніпуляцію фактами, поширення чуток, створення фейкових новин, використання ботоферм у соціальних мережах – стає ключовим інструментом досягнення цілей інформаційної війни, дозволяючи сіяти паніку, розпалювати ворожнечу, підривати довіру до державних інститутів і дестабілізувати суспільство зсередини.

Серед основних ознак інформаційної війни виділяються чітко визначені суб'єкти та об'єкти впливу, цілеспрямованість інформаційного

впливу, підпорядкованого досягненню конкретних стратегічних або тактичних цілей, а також використання специфічних методів і технологій інформаційно-психологічного впливу, що базуються на глибокому розумінні механізмів людського сприйняття та вразливостей у системі масової комунікації. Системність і тривалість інформаційних війн є важливою характеристикою, оскільки для досягнення стійких змін у свідомості потрібні довготривалі, скоординовані кампанії, а масштабність, особливо в умовах Інтернету, дозволяє впливати на глобальну громадську думку. Прихований характер багатьох операцій створює значні труднощі для їх виявлення та атрибуції, що є визначальним викликом сучасної інформаційної безпеки. Типологізація інформаційних війн, наприклад, класифікація Мартіна Лібікі, яка охоплює командно-управлінську, розвідувальну, електронну, психологічну, хакерську, економічну інформаційну та кібервійну, сприяє глибшому розумінню цього явища, хоча сучасні інформаційні війни дедалі частіше набувають гібридного характеру, поєднуючи елементи різних типів. Стратегії інформаційних війн різноманітні: стратегія інформаційного домінування передбачає контроль над каналами поширення інформації та нав'язування власних наративів, стратегія дезінформації та пропаганди спрямована на введення супротивника в оману та формування негативного образу ворога, стратегія психологічного виснаження та деморалізації має на меті підрив морально-психологічного стану населення та збройних сил супротивника, кібернетичні стратегії передбачають прямий вплив на інформаційні системи та мережі, а стратегія інформаційної блокади обмежує доступ супротивника до важливих інформаційних ресурсів. Ефективність будь-якої стратегії залежить від глибокого розуміння цільової аудиторії та розробки комплексних комунікаційних стратегій, а невід'ємною складовою є заходи з інформаційної безпеки, спрямовані на захист власного інформаційного простору та нейтралізацію інформаційних атак. Перехід інформаційного

протиборства на новий рівень, де воно стає домінуючим фактором, вимагає розробки досконаліших методів аналізу та протидії, особливо з урахуванням зростаючої ролі соціальних мереж.

Політична стабільність держави, як характеристика політичної системи, що відображає її стійкість і здатність ефективно функціонувати та розвиватися, забезпечуючи правопорядок і громадянський мир, є ключовим об'єктом аналізу, особливо в умовах глобалізаційних процесів і системних трансформацій. Сутність політичної стабільності охоплює не лише збереження існуючого режиму, а й підтримку легітимності влади, ефективність її діяльності, здатність системи до самовідтворення та адаптації без руйнівних конфліктів, підкреслюючи динамічний характер цього явища. У цьому контексті інститути інформаційної безпеки набувають особливої ваги як чинник суспільно-політичної стабільності, покликаний забезпечувати захищеність від інформаційних загроз. Критерії політичної стабільності багатогранні: рівень довіри громадян до політичних інститутів, ефективність механізмів прийняття рішень, стан правопорядку, рівень політичного насильства, здатність еліти до консенсусу, а також стійкість держави до інформаційних впливів, спрямованих на підрив її суверенітету. Функціонування інститутів інформаційної безпеки, що забезпечують захист інформаційного простору, є важливою складовою підтримки політичної стабільності, оскільки неконтрольоване поширення дезінформації може дестабілізувати суспільно-політичну ситуацію. Забезпечення політичної стабільності нерозривно пов'язане з ефективністю державної інформаційної політики та функціонуванням системи інформаційної безпеки, що вимагає формування національної системи протидії інформаційним загрозам, яка включає технічні засоби захисту, підвищення медіаграмотності населення та утвердження національних цінностей. Рівень політичної стабільності безпосередньо корелює з рівнем

інформаційної безпеки країни, оскільки недостатній захист інформаційних ресурсів може призвести до серйозних економічних втрат і соціальної напруженості. Здатність держави ефективно реагувати на інформаційні атаки – від фейкових новин до кібератак – є важливим чинником підтримки політичної стабільності, що потребує вдосконалення технічних і організаційно-правових механізмів захисту, а також налагодження ефективних каналів комунікації між владою та суспільством для запобігання інформаційним кризам. Формування суспільної стійкості до інформаційно-психологічних впливів через освітні програми та підтримку незалежних медіа, поряд із міжнародною співпрацею у сфері інформаційної безпеки, є важливими аспектами забезпечення стабільності.

## **Висновки до розділу 1**

У результаті проведеного дослідження встановлено, що інформаційна війна є самостійною формою сучасного протистояння, що виходить за межі класичних воєнних дій і здійснюється в інформаційно-психологічному просторі. Визначено, що вона охоплює комплекс цілеспрямованих впливів на свідомість та поведінку масової аудиторії шляхом маніпуляцій інформаційними потоками, використання фейків, дезінформації, пропаганди, кібератак тощо. Типологізація інформаційних війн (зокрема за М. Лібікі) дозволяє класифікувати їх за цілями, методами й об'єктами впливу, що є підґрунтям для розробки ефективних стратегій протидії. Проаналізовано основні стратегії, серед яких домінування в інформаційному полі, психологічне виснаження, блокада доступу до правдивої інформації тощо. Особливу увагу приділено ролі соціальних мереж, які стали головним інструментом масштабного поширення інформаційного впливу.

Отже, інформаційна війна суттєво впливає на політичну стабільність держави, яка в умовах цифрової епохи залежить не лише від легітимності

інститутів влади чи ефективності управління, але й від здатності захищати інформаційний простір. Доведено, що політична стабільність є динамічним станом, що включає як збереження громадянського миру й порядку, так і стійкість до інформаційних загроз. Функціонування інститутів інформаційної безпеки, медіаграмотність громадян, ефективна державна комунікація та міжнародна кооперація у сфері кібербезпеки визначено як ключові фактори, що забезпечують здатність держави зберігати політичну рівновагу та протистояти дестабілізуючим впливам у сучасному світі.

## **РОЗДІЛ 2. АНАЛІЗ ВПЛИВУ ІНФОРМАЦІЙНИХ ВІЙН НА ПОЛІТИЧНУ СТАБІЛЬНІСТЬ: ПРИКЛАДИ, НАСЛІДКИ, ПРОТИДІЯ**

### **2.1. Інформаційні війни в сучасному світі: кейси України, Грузії, США та інших країн**

Слід почати з інформаційної війни України та РФ, цей вплив є системним та багатоаспектним підходом, спрямованим на дестабілізацію внутрішньополітичної ситуації та підрив її міжнародного іміджу, що знаходить своє відображення у використанні широкого спектру засобів та методів, починаючи від традиційних медіа і завершуючи новітніми цифровими платформами. Специфіка російських

інформаційно-психологічних операцій полягає у їх спрямованості на свідомість та підсвідомість об'єкта впливу, з метою формування вигідних для агресора моделей поведінки та реакцій, що досягається через маніпулювання інформацією, поширення дезінформації та створення фейкових новин, які активно тиражуються через контрольовані або лояльні медіа-ресурси . Успішність таких операцій значною мірою залежить від уразливості цільової аудиторії, зокрема від рівня її медіаграмотності, критичного мислення та здатності розрізняти достовірну інформацію від маніпулятивної, що робить освітні та просвітницькі програми у сфері медіаграмотності важливим елементом протидії інформаційним загрозам(Худолій 2022: 15-17). Використання соціальних мереж як інструментів для проведення інформаційних операцій стало однією з ключових особливостей сучасних конфліктів, і російсько-українська війна після 24 лютого 2022 року не є винятком, адже саме через платформи по типу Telegram, Facebook, Instagram та інші відбувається швидке поширення як правдивої, так і фейкової інформації, що дозволяє оперативно впливати на настрої великих мас людей. Російська Федерація активно використовує соціальні мережі для поширення власних наративів, дискредитації української влади та збройних сил, а також для мобілізації проросійських настроїв серед населення як в Україні, так і за її межами, причому ефективність такого впливу посилюється можливістю таргетування повідомлень на конкретні групи населення з урахуванням їхніх психологічних та соціально-демографічних характеристик. Мобілізаційна функція соціальних мереж проявилася у стимулюванні благодійності та волонтерського руху як в Україні, де вони стали важливим інструментом координації зусиль громадянського суспільства для допомоги армії та постраждалим, так і в Російській Федерації, де державні структури та громадські організації використовували їх для збору коштів на підтримку

власної армії та для просування патріотичних наративів(Амелічева 2023: 25-27).

У контексті російської агресії проти Грузії у 2008 році інформаційна складова також відігравала значну роль, оскільки Росія активно використовувала медіа для формування негативного образу Грузії та виправдання власних дій, представляючи операцію як примус до миру та захист своїх громадян та миротворців. Інтенсивність російських пропагандистських атак проти Грузії визначалася низкою факторів, серед яких були поляризоване політичне середовище в Грузії, відкритий ринок мас-медіа, який дозволяв російським наративам проникати в інформаційний простір країни, а також недостатня готовність грузинської сторони до ефективної протидії таким атакам. Російська стратегія інформаційного впливу в Грузії мала на меті виправдати військові дії та посіяти сумніви щодо суверенітету та територіальної цілісності Грузії, а також дискредитувати її прагнення до євроатлантичної інтеграції, що свідчить про довгостроковий характер російських інформаційних операцій, спрямованих на досягнення геополітичних цілей й аналогічні підходи до ведення інформаційної війни Росія продемонструвала і під час анексії Криму та розпалювання конфлікту на Донбасі у 2014 році, де інформаційні операції передували та супроводжували військові дії, створюючи сприятливе підґрунтя для реалізації російських планів. Російські ЗМІ активно поширювали дезінформацію про нібито загрозу російськомовному населенню з боку нової української влади, про утиски прав та свобод, а також про так званий державний переворот у Києві, що мало на меті легітимізувати в очах власного населення та міжнародної спільноти анексію Криму та підтримку сепаратистських рухів на сході України. Успіху російської інформаційної кампанії 2014 року сприяла низка факторів, зокрема раптовість нападу, слабкість українських державних інституцій на

той момент, а також багаторічна присутність російського інформаційного продукту в українському медіа-просторі, що сформувало певну лояльність частини населення до російських наративів (Худолій 2022: 50-55). Стратегічні цілі російської інформаційної війни часто включають підрив національної єдності в цільових країнах, що особливо помітно на прикладі країн Балтії, де Росія намагається використовувати наявні етнічні, мовні та соціальні розбіжності для посилення напруженості та зменшення суспільної стійкості. Поширення наративів про нібито дискримінацію російськомовного населення, спотворення історичних фактів, зокрема щодо періоду радянської окупації, та підтримка проросійських політичних сил та громадських організацій є одними з ключових інструментів російського впливу в Латвії, Литві та Естонії. Створення альтернативної реальності через контрольовані Кремлем ЗМІ, по типу Sputnik та RT, які транслюють програми місцевими мовами, спрямоване на формування у частини населення країн Балтії лояльності до Росії та недовіри до власних урядів та західних інституцій, що створює довгострокові виклики для національної безпеки цих країн(Чакарс, Екманіс 2025: 45-50).

У відповідь на російську інформаційну агресію Україна розробляє та впроваджує власні стратегії протидії, які включають як технічні засоби захисту інформаційного простору та контрпропагандистські заходи, спрямовані на розвінчування російських фейків та поширення правдивої інформації про події в країні. Важливу роль у цьому процесі відіграють державні органи, такі як Центр протидії дезінформації при РНБО України, а також громадські ініціативи та незалежні медіа, які займаються фактчекінгом та підвищенням медіаграмотності громадян (Амелічева 2023: 45-48). Культурна дипломатія та спортивні досягнення також використовуються Україною для просування позитивного іміджу країни на міжнародній арені та для протидії російським наративам, що є частиною

ширшої стратегії інформаційного спротиву, спрямованого на витіснення Росії з публічного простору та зміцнення міжнародної підтримки України. Російська концепція гібридної війни, яскраво продемонстрована на прикладах України та Грузії, передбачає комплексне використання військових, політичних, економічних, інформаційних та кібернетичних інструментів для досягнення стратегічних цілей, причому інформаційна складова часто відіграє ключову роль на початкових етапах конфлікту, готуючи підґрунтя для подальших дій. Дестабілізація внутрішньої ситуації в країні-жертві, створення хаосу та невпевненості, дискредитація влади та силових структур, а також формування міжнародної громадської думки, сприятливої для агресора, є типовими завданнями інформаційних операцій у рамках гібридної війни. Важливим елементом російської гібридної тактики є використання так званих проксі-сил, тобто недержавних акторів, які діють в інтересах Росії, але формально не є частиною її збройних сил, що дозволяє Росії заперечувати свою пряму участь у конфлікті та уникати міжнародної відповідальності (Muradov 2022: 170-172).

Поняття інформаційної війни включає поширення дезінформації та проведення відповідних психологічних операцій, спрямованих на зміну емоційного стану, мотивації та поведінки цільової аудиторії, що може мати далекосяжні наслідки для суспільної стабільності та національної безпеки. Російські інформаційно-психологічні операції проти України часто апелюють до таких емоцій: страх, ненависть, зневіра та почуття несправедливості, з метою деморалізації українського суспільства та підриву його здатності до опору (Худолій 2022: 22-25). Ефективність таких операцій посилюється використанням маніпулятивних технік, таких як створення хибних дилем, перебільшення загроз, використання емоційно забарвленої лексики та посилення на авторитети, які насправді можуть бути фейковими або контрольованими агресором. Одним із вимірів

інформаційного протистояння є боротьба наративів, де кожна зі сторін намагається нав'язати власне бачення подій та інтерпретацію реальності, що є особливо актуальним у контексті російсько-української війни, де історична пам'ять та національна ідентичність стали об'єктами інформаційних атак. Росія активно просуває наратив про Україну як про штучне державне утворення, про братні народи, яких роз'єднав Захід, та про необхідність відновлення історичної справедливості шляхом повернення України до сфери російського впливу, тоді як Україна наголошує на своїй тисячолітній історії державності, на праві самостійно обирати власний шлях розвитку та на тому, що російська агресія є неспровокованим актом порушення міжнародного права. Ця боротьба наративів відбувається не лише в медіа-просторі, але й у сфері культури, освіти та науки, де кожна зі сторін намагається утвердити власну версію минулого та сьогодення(Амелічева 2023: 15-18).

Уразливість цільової держави до інформаційних атак є ключовим фактором, що визначає їхню потенційну ефективність, і ця уразливість може бути зумовлена різними чинниками, як наявність глибоких суспільних розколів, низький рівень довіри до державних інституцій, недостатній розвиток незалежних медіа та високий рівень корупції. Росія часто використовує ці вразливості у своїх інформаційних кампаніях, намагаючись поглибити існуючі проблеми та представити себе як єдину силу, здатну навести лад або захистити інтереси певних груп населення. У випадку України, Росія активно експлуатувала мовне питання, регіональні відмінності та різні погляди на історичне минуле для розпалювання внутрішніх конфліктів та просування сепаратистських настроїв, що свідчить про глибоке розуміння російськими стратегами внутрішніх проблем цільових країн. Довготривалі інформаційні кампанії, які Росія веде проти країн Балтії, мають на меті не лише дискредитувати їхні уряди та

західний вектор розвитку, але й вплинути на формування ідентичності молодого покоління, яке не має особистого досвіду життя в Радянському Союзі. Через соціальні мережі, розважальний контент та освітні програми, що фінансуються Росією, робляться спроби романтизувати радянське минуле, применшити злочини радянського режиму та сформувати у молоді позитивне ставлення до сучасної Росії та її політики. Це створює серйозні виклики для систем освіти та національно-патріотичного виховання в країнах Балтії, які змушені шукати ефективні способи протидії такому впливу та формування у молоді критичного мислення та стійкості до маніпуляцій. Мікротаргетинг як інструмент інформаційної війни, що передбачає доставку спеціально підготовлених повідомлень вузьким сегментам аудиторії на основі їхніх персональних даних, інтересів та поведінкових характеристик, становить особливу загрозу, оскільки дозволяє здійснювати прихований та персоніфікований вплив. Російські операції з використанням мікротаргетингу були зафіксовані під час виборчих кампаній у США та інших країнах, де вони були спрямовані на посилення поляризації суспільства, маніпулювання електоральними настроями та підірив довіри до демократичних процесів (Mullaney 2022: 75-76). Використання ботів та фейкових акаунтів у соціальних мережах для поширення таких таргетованих повідомлень та створення ілюзії масової підтримки певних ідей чи кандидатів є поширеною тактикою, яка ускладнює виявлення та протидію інформаційним впливам(Чакарс, Екманіс 2025: 150-155).

Застосування Росією кібернетичних засобів у поєднанні з інформаційними операціями створює синергетичний ефект, посилюючи загальний вплив на цільову аудиторію та ускладнюючи атрибуцію атак і однією із таких атак є злам серверів політичних організацій з подальшою публікацією викраденої інформації, яка може бути як правдивою, так і

сфальсифікованою або вирваною з контексту, використовується для дискредитації політичних опонентів та впливу на громадську думку, як це було під час виборів у США у 2016 році. Подібні операції вимагають високого рівня координації між різними державними структурами та спецслужбами, що свідчить про централізований характер російських інформаційних та кібернетичних атак, в свою чергу, недооцінка російських кібернетичних та інформаційних можливостей може призвести до серйозних наслідків для національної безпеки, тому важливим є постійний аналіз тактик противника та адаптація власних стратегій захисту (Kerr 2023: 10-12).

Операції впливу, здійснювані Росією, часто спрямовані не на пряме переконання аудиторії, а на створення сумнівів, поширення хаосу та підірив довіри до будь-яких джерел інформації, що призводить до так званого інформаційного нігілізму, коли люди перестають вірити будь-кому і стають більш вразливими до маніпуляцій. Ця тактика, відома як створення інформаційного шуму або затуманення інформаційного простору, ускладнює для громадян можливість орієнтуватися в потоці інформації та приймати усвідомлені рішення. У таких умовах зростає роль незалежних та професійних медіа, які дотримуються стандартів журналістської етики та надають перевірену та збалансовану інформацію, допомагаючи громадянам формувати власну об'єктивну картину світу. Приклади інформаційного впливу Росії на виборчі процеси в Сполучених Штатах Америки демонструють, що навіть потужні демократії не є невразливими до таких атак, і що інформаційна війна може вестися не лише проти країн, які перебувають у стані прямого конфлікту з Росією, але й проти тих, кого Росія розглядає як своїх геополітичних суперників. Використання викрадених даних, поширення фейкових новин через соціальні мережі, діяльність фабрик тролів та фінансування політичної реклами з прихованих

джерел – все це елементи комплексної стратегії, спрямованої на дестабілізацію політичної системи США та підрив її міжнародного авторитету. Наслідки таких операцій можуть бути довготривалими, оскільки вони посилюють політичну поляризацію, знижують рівень суспільної довіри та створюють прецеденти для майбутніх втручань. У контексті інформаційної війни, яку Росія веде проти України, особливе значення має використання історичних наративів та маніпулювання історичною пам'яттю, оскільки це дозволяє агресору обґрунтовувати свої територіальні претензії та заперечувати право українського народу на самовизначення. Поширення міфів про спільне походження, про штучність української державності, про нацистський характер української влади – все це спрямовано на дегуманізацію українців та легітимізацію агресії в очах власного населення та міжнародної спільноти. Протидія таким наративам вимагає не лише спростування конкретних фейків, але й системної роботи з відновлення та популяризації правдивої української історії, а також формування стійкої національної ідентичності, здатної протистояти зовнішнім маніпуляціям (Худолій 2022: 85-90).

Інформаційна війна є невід'ємною складовою російської стратегії так званої війни нового покоління, яка характеризується нелінійністю, асиметричністю та комплексним використанням різноманітних засобів впливу, де інформаційні операції часто відіграють важливішу роль, ніж традиційні військові дії, особливо на початкових етапах конфлікту. Метою таких операцій є створення сприятливих умов для досягнення політичних цілей без прямого широкомасштабного застосування військової сили або з мінімальним її використанням, шляхом маніпулювання громадською думкою, дестабілізації внутрішньої ситуації в країні-жертві та підриву її здатності до опору (Muradov 2022: 175-178). Ця концепція передбачає активне використання інформаційного простору як поля бою, де ведеться

боротьба за уми та серця людей, а перемога в цій боротьбі може мати вирішальне значення для загального успіху кампанії.

Естонський досвід протистояння російським інформаційним впливам, особливо після бронзової ночі 2007 року, коли країна зазнала масштабних кібератак та інформаційних нападів, є цінним прикладом того, як невелика держава може розробити ефективну систему захисту від гібридних загроз. Цей досвід включає створення спеціалізованих державних структур, таких як Центр передового досвіду НАТО з питань спільної кібероборони, розвиток співпраці між державним та приватним сектором, підвищення медіаграмотності населення та активну комунікаційну політику, спрямовану на розвінчування дезінформації. Естонія також приділяє значну увагу підтримці незалежних російськомовних ЗМІ, які можуть стати альтернативним джерелом інформації для російськомовного населення країни та протидіяти кремлівській пропаганді. Складність протидії російським інформаційним операціям полягає також у тому, що вони часто використовують тактику віддзеркалення, звинувачуючи протилежну сторону у тому, що роблять самі, наприклад, у поширенні фейків, втручанні у внутрішні справи чи розпалюванні ненависті. Це створює додаткові труднощі для виявлення та спростування дезінформації, оскільки звинувачення звучать з обох сторін, і пересічному громадянину буває складно розібратися, де правда, а де брехня. У таких умовах зростає важливість розвитку навичок критичного мислення та медіаграмотності, які б дозволяли людям самостійно аналізувати інформацію, перевіряти її джерела та розпізнавати маніпулятивні техніки (Чакарс, Екманіс 2025: 90-95).

## **2.2. Протидія інформаційним загрозам як чинник забезпечення політичної стабільності: практичні інструменти та державна політика**

Сьогоднішній інформаційний простір фактично перетворився на арену гібридного протистояння, що зумовлює особливу значущість питань, пов'язаних із протидією інформаційним загрозам. Адже саме через інформаційно-психологічні операції, які активно застосовуються противником, здійснюється вплив на внутрішню ситуацію в державі: провокується паніка, поширюються дезінформація та фейки, підривається довіра до державних інституцій. Усе це безпосередньо позначається на рівні політичної стабільності в країні. Водночас ефективна державна політика у сфері інформаційної безпеки здатна протидіяти таким загрозам, зміцнюючи суспільну стійкість, відновлюючи довіру до органів влади й забезпечуючи стабільність навіть у періоди глибокої кризи. Це особливо важливо в умовах війни, коли інформаційне середовище перетворюється на поле бою, рівнозначне воєнному фронту. У цьому контексті інформаційна політика держави має бути спрямована на формування єдиного інформаційного простору, розвиток і адаптацію нормативно-правової бази, яка регулює суспільні відносини відповідно до актуальних викликів, а також на забезпечення інформаційної безпеки як основи політичної стабільності. Крім того, така політика повинна гарантувати технологічну підтримку інформаційних ресурсів, забезпечувати відкритий доступ до них, а також створювати умови для ефективного пошуку, обробки та передачі інформації. (Ржевська, 2024: 69–70).

У воєнний період інформаційна політика держави набуває особливої важливості, виступаючи як комплекс заходів, що реалізуються спільно з інститутами громадянського суспільства й спрямовані на регулювання інформаційних потоків, розвиток інформаційного суспільства та забезпечення національної безпеки. В умовах збройного конфлікту першочергове значення надається саме оборонним аспектам інформаційної політики, що зумовлено необхідністю захисту прав і свобод людини, моральних засад суспільства, а

також гарантуванням інформаційної безпеки особистості, суспільства і держави в цілому. Військова агресія актуалізує потребу в обмеженні поширення певної інформації, зокрема щодо стратегічних операцій Збройних сил України чи об'єктів військової інфраструктури. У цьому контексті діяльність представників медіа регламентується спеціальними нормами, які встановлюють чіткі обмеження на час воєнного стану. Журналісти зобов'язані дотримуватись вимог щодо недопущення витоку даних, що потенційно можуть завдати шкоди обороноздатності держави та безпеці громадян. Значну роль у регулюванні інформаційної політики відіграє Закон України «Про медіа», який покликаний забезпечити баланс між правом на свободу слова та необхідністю захисту національних інтересів. Документ гарантує доступ до достовірної та оперативної інформації, захист прав споживачів медіа-сервісів, а також визначає правові засади функціонування медіа у воєнний час. Попри це, чинна нормативно-правова база досі не охоплює в повному обсязі питання журналістських розслідувань, які за умов війни набувають особливої ваги, оскільки можуть виявляти як внутрішні проблеми, так і загрози зовнішнього впливу. (Ржевська, 2024: 73).

Досягнення балансу між свободою слова та захистом національної безпеки в умовах війни можливе шляхом запровадження чітко визначених нормативно-правових механізмів на рівні підзаконних актів, чинність яких обмежується періодом воєнного стану. Попри те, що в демократичному суспільстві заборона на проведення журналістських розслідувань є неприйнятною, в умовах збройного конфлікту виникає обґрунтована необхідність у впровадженні обмежень, насамперед щодо процедури оприлюднення результатів таких розслідувань. Інформація, отримана під час журналістського розслідування, може слугувати орієнтовним матеріалом, однак для підтвердження її достовірності та визначення можливості публічного розголошення вона має бути передана до компетентних правоохоронних органів. Саме ці структури повинні здійснити фахову

перевірку й визначити допустимий обсяг інформації, який не загрожує суспільній безпеці. Усі дії в цьому напрямі повинні бути підпорядковані головному принципу — забезпеченню інтересів держави, безпеки громадян, захисту їхніх прав і свобод в умовах війни. (Ржевська, 2024: 73).

Особливої уваги заслуговує той факт, що Указом Президента України від 25 лютого 2017 року було затверджено «Доктрину інформаційної безпеки України», яка заклала основи державної політики у сфері інформаційного захисту. З початком повномасштабної агресії проти України питання інформаційної безпеки набуло критичної ваги, що знайшло своє відображення в рішенні Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». У цьому документі підкреслюється, що забезпечення єдиної інформаційної політики є стратегічним пріоритетом національної безпеки в умовах війни. У межах цього підходу було створено Центр протидії дезінформації при РНБО України — платформу для інформування громадськості щодо актуальних загроз у сфері інформаційної безпеки. Захист інформаційного простору сьогодні постає одним із ключових напрямів державної безпеки, що вимагає високої професійної підготовки фахівців, зокрема в галузі інформаційної безпеки. Ці фахівці повинні вміти керувати інформаційними потоками, виявляти потенційні загрози та ефективно застосовувати механізми протидії деструктивному інформаційному впливу. Особливе значення має стратегічне планування та реалізація інформаційної роботи з військовослужбовцями, яка потребує спеціальної підготовки, навичок виявлення загроз і точного інструментарію впливу. Найбільшою небезпекою в інформаційній сфері нині виступає необережне чи неконтрольоване поширення чутливої інформації через соціальні мережі, що відкриває доступ до неї широкому колу користувачів — включаючи потенційного противника. (Ржевська, 2024: 74–75).

Аналізуючи практичні інструменти протидії інформаційним загрозам, можна виокремити дві основні категорії заходів, що забезпечують інформаційну безпеку. Першу групу становлять технічні й технологічні засоби захисту інформаційних систем від пошкоджень, витоку чи несанкціонованого доступу. До них належать заходи з охорони військових об'єктів та комп'ютерного обладнання, протидії дистанційному втручанню, захисту інформації, що має гриф державної або військової таємниці, а також засоби радіоелектронного захисту. У цьому контексті застосування сертифікованих захищених апаратно-програмних комплексів та надійних засобів зв'язку є критично важливим компонентом забезпечення інформаційної безпеки. Друга група заходів зосереджена на протидії цілеспрямованому інформаційно-психологічному впливу, який здійснюється противником з метою дестабілізації емоційного стану військовослужбовців. Це вимагає розробки методик психологічного впливу, організації спеціалізованої просвітницької роботи, створення структур з фахівців у сфері інформаційно-психологічної безпеки, а також впровадження найсучасніших технологій і аналітичних програм. Ефективність таких заходів забезпечується через міжвідомчу взаємодію, зокрема співпрацю між військовими структурами, аналітичними центрами та спеціальними службами. Особливе значення має захист інформаційного середовища всередині військових формувань, оскільки інформаційна деморалізація особового складу безпосередньо впливає на зниження бойового духу та рівня готовності до виконання бойових завдань. Потенційно небезпечними є спроби вплинути на військових через спотворення інформації, нагнітання соціальної напруги або втягування у внутрішньополітичні процеси. Для нейтралізації таких загроз проводиться систематична психологічно-просвітницька робота з особовим складом, а також вибудовується комунікація з органами місцевого самоврядування з метою запобігання провокаціям і блокування

деструктивного впливу з боку ЗМІ та інших джерел інформаційних атак. (Ржевська, 2024: 75).

Функціонування інформаційних систем, що використовуються у військовій сфері, зокрема систем управління та збереження конфіденційних даних, передбачає ризики виникнення технічних проблем, які можуть бути наслідком як внутрішніх збоїв у роботі обладнання, навмисного втручання чи пошкодження, так і недбалості окремих працівників. Особливої уваги потребує захист інформації, яка передається через військові канали, адже її компрометація може призвести до критичних наслідків для обороноздатності країни. У зв'язку з цим заходи з підвищення безпеки охоплюють удосконалення автоматизованих систем управління, а також професійну підготовку персоналу відповідно до актуальних вимог захисту інформації. На державному рівні забезпечення належного рівня інформаційної безпеки передбачає дотримання затверджених стандартів і впровадження ефективних технічних та організаційних рішень. Однак на практиці часто спостерігається затримка у впровадженні нових програмно-технічних засобів, необхідних для протидії сучасним загрозам. Подібне зволікання створює потенційні ризики для загальної безпеки військових підрозділів і може бути використане противником для отримання стратегічно важливої інформації. Серед ключових проблем залишається й недостатня розвиненість законодавчої бази у сфері інформаційної безпеки та боротьби з новітніми викликами в інформаційному просторі. Деякі форми загроз і потенційних наслідків їх реалізації все ще не мають достатнього нормативного відображення, що ускладнює притягнення до відповідальності за дії або бездіяльність, які можуть завдати шкоди інформаційній безпеці Збройних сил України та їх особовому складу. (Ржевська, 2024: 75).

Ефективне управління суспільними процесами з боку держави є неможливим без доступу до різноманітних джерел та інформаційних потоків, що

відображають соціальні запити, інтереси та потреби різних суб'єктів політичного процесу. Саме ця інформація забезпечує підвищення результативності діяльності органів влади. Водночас характер взаємодії між державними інституціями та медіа значною мірою визначається поточною політичною ситуацією, а також рівнем розвитку і специфікою громадянського суспільства в конкретний історичний період. У період дії воєнного стану зростає інтенсивність загроз в інформаційному середовищі, що вимагає постійного оновлення засобів їх виявлення та нейтралізації, а також ефективної протидії їх негативним наслідкам. Це особливо актуально з огляду на потребу гарантувати надійний рівень інформаційної безпеки Збройних сил України. Від початку повномасштабного вторгнення держава продемонструвала здатність до оперативного реагування в інформаційній сфері: зокрема, було створено офіційні сторінки державних установ у соціальних мережах, які забезпечують швидке та достовірне інформування громадян. Крім того, важливим кроком у напрямі інформаційного розвитку стало створення цифрового порталу державних послуг у межах мобільного застосунку «Дія». Цей сервіс дозволив забезпечити доступ населення до ключових адміністративних послуг, документів і цифрових інструментів безпосередньо через смартфон. (Ржевська, 2024: 76).

Розглядаючи державну політику у сфері інформаційної безпеки, слід наголосити, що ефективна протидія інформаційним загрозам не може обмежуватись лише тактичними рішеннями чи технічними засобами. Її результативність значною мірою залежить від глибини та якості системних демократичних реформ, спрямованих на підвищення рівня інклюзивності, прозорості й підзвітності управлінських процесів. Лише гармонійне поєднання стратегічного бачення інформаційної політики з практичними заходами, які укріплюють національну ідентичність, сприяють суспільній консолідації та стимулюють громадянську активність, здатне створити

необхідний рівень стійкості до когнітивних атак та інформаційних операцій з боку агресора. У сучасному протистоянні ключовим полем битви стає інформаційний простір та сфера свідомості — боротьба за уми і серця людей. Перемогу в цій війні отримає той, хто зуміє ефективно мобілізувати суспільство навколо чіткого ціннісного й ідеологічного проєкту, здатного об'єднати людей навколо спільної мети й переконати у реальності спільного майбутнього. В умовах гібридної війни противник використовує синергетичне поєднання класичних інструментів пропаганди та дезінформації з сучасними маніпулятивними технологіями, кіберзасобами та прихованими каналами впливу, що дозволяє йому здійснювати масове психологічне маніпулювання, провокувати соціальні конфлікти та підривати довіру до державних інституцій. Особливо вразливими до таких впливів є країни пострадянського простору з транзитивною демократією, які проходять складний шлях політичної, соціальної та культурної трансформації. В умовах слабкості демократичних інститутів, відсутності традицій відповідальної політичної культури, а також за наявності значних внутрішніх соціальних розколів, ці держави стають мішенню для зовнішніх деструктивних стратегій. Україна, попри поступ у сфері цифровізації та зміцнення інформаційної політики, залишається вразливою через низький рівень медіаграмотності значної частини населення, обмежені інституційні можливості держави щодо ефективного контролю цифрового середовища, відсутність прозорості у сфері медіавласності та редакційної політики. Особливою проблемою є нестача системної практики фактчекінгу й верифікації інформації. Усе це створює умови для безперешкодного поширення дезінформації, маніпулятивного контенту не лише в соціальних мережах, а й у професійних засобах масової інформації, які, навпаки, мали б гарантувати об'єктивність і достовірність даних для широкого загалу. (Хряпинський, 2024: 323 - 325).

У цьому контексті одним із ключових напрямів удосконалення інформаційної політики України має стати системна розбудова медіаосвіти та підвищення рівня цифрової грамотності громадян. Це повинно здійснюватися з урахуванням найкращих європейських практик, зокрема досвіду Фінляндії, де медіаграмотність інтегрована в освітній процес на всіх рівнях — від дошкільної до вищої освіти. Крім того, там функціонують спеціалізовані програми для дорослого населення, спрямовані на розвиток критичного мислення та підвищення стійкості до дезінформації. Такий підхід сприяє формуванню відповідальних і свідомих споживачів інформації, які здатні розпізнавати фейкові повідомлення, маніпуляції та приховані впливи. Другим пріоритетом має стати зміцнення інституційного потенціалу в галузі стратегічних комунікацій. Це передбачає створення спеціалізованих структур, що займаються моніторингом інформаційного простору, аналізом ворожих дезінформаційних кампаній і системним спростуванням фейків. Важливим напрямом є також розвиток партнерства державних органів з глобальними цифровими платформами та соціальними мережами з метою протидії поширенню деструктивного контенту. У цьому контексті варто враховувати досвід Європейського Союзу, де діє Кодекс практики з протидії дезінформації. До цього документа приєдналися ключові гравці цифрового ринку — Facebook, Google, Twitter, Microsoft та інші, які взяли на себе зобов'язання з видалення фейкових акаунтів, маркування політичної реклами, блокування джерел прибутку для дезінформаційних ресурсів. Ще одним важливим кроком має стати реалізація проактивної інформаційної політики, що передбачає не лише реагування на ворожі інформаційні впливи, а й формування позитивного, ціннісно зорієнтованого порядку денного. (Хряпинський, 2024: 327).

Сучасна державна політика у сфері протидії інформаційним загрозам дедалі більше орієнтується на інвестиції в технологічні рішення, здатні забезпечити

як оперативне виявлення та нейтралізацію дезінформації, так і захист критичної інфраструктури. Яскравим прикладом такої практики є ініціатива Європейського Союзу — платформа EUvsDisinfo, яка в автоматичному режимі відстежує дезінформаційні наративи, зокрема ті, що стосуються європейської інтеграції, і надає перевірену, спростовану інформацію. Паралельно в ЄС активно впроваджуються алгоритми штучного інтелекту, які здатні здійснювати верифікацію контенту в соціальних мережах, і ці технології можуть бути адаптовані до українських умов, зокрема у сфері стратегічних комунікацій. Водночас в Україні одним із ключових напрямів зміцнення інформаційної безпеки є розвиток інформаційної культури та підвищення загального рівня обізнаності населення щодо природи гібридних загроз. Особливої актуальності це питання набуває в умовах широкого використання маніпулятивних технологій у медіа та соціальних мережах. Низький рівень медіаграмотності, відсутність навичок критичного аналізу інформації та довіра до неперевічених джерел створюють сприятливе середовище для поширення фейків та реалізації масштабних інформаційно-психологічних операцій противника. Саме тому важливо впроваджувати системний підхід до медіаосвіти, який охоплює всі вікові групи та рівні навчання — від початкової школи до освітніх програм для дорослих. Формування навичок критичного мислення, вміння перевіряти інформацію, розпізнавати маніпуляції та розуміти механізми інформаційного впливу мають стати пріоритетами державної освітньої та інформаційної політики. (Хряпинський, 2024: 327).

Поряд із розвитком медіаграмотності серед населення важливим напрямом державної інформаційної політики є зміцнення стійкості національного медійного середовища до впливу дезінформації та поширення шкідливого контенту. Це передбачає впровадження ефективних механізмів саморегулювання в медіасфері, що ґрунтуються на засадах професійної

журналістської етики, забезпеченні редакційної незалежності та дотриманні стандартів якісної журналістики. Визначальна роль у цьому процесі має належати громадським медійним організаціям та професійним об'єднанням, які можуть виробити спільні, узгоджені правила і процедури з метою захисту інформаційного простору від маніпуляцій та деструктивного впливу. Держава, у свою чергу, повинна створювати сприятливі регуляторні умови для функціонування відповідальних медіа, забезпечувати рівний доступ до інформації, а також підтримувати ініціативи, спрямовані на покращення якості контенту та дотримання етичних норм у роботі журналістів. Така політика сприятиме підвищенню довіри до медіа та посилить стійкість суспільства до інформаційних атак. Критично важливим чинником протидії сучасним гібридним загрозам є активна співпраця держави з глобальними технологічними компаніями та соціальними платформами, які нині фактично контролюють основну частину віртуального медіапростору. Хоча ці компанії часто позиціонують себе як нейтральні інфраструктурні майданчики, що не несуть відповідальності за контент, створений користувачами, у нинішніх умовах зростаючих ризиків вони мають проявляти більшу відповідальність і проактивність у питанні захисту інформаційного суверенітету держав. У цьому контексті важливо стимулювати цифрові корпорації до посилення прозорості своїх алгоритмів, удосконалення системи контролю за політичною рекламою та забезпечення відкритості щодо обробки та використання персональних даних користувачів. (Хряпинський, 2024: 328).

Важливим ресурсом для підвищення суспільної стійкості до гібридних загроз є розвиток незалежних аналітичних центрів та експертних мереж, які спроможні оперативно реагувати на інформаційні виклики. Такі організації відіграють ключову роль у виявленні та спростуванні дезінформації, проведенні стратегічного аналізу загроз, а також у напрацюванні практичних рекомендацій для державної політики у сфері інформаційної безпеки. Їхня

діяльність сприяє формуванню обґрунтованих рішень у сфері протидії маніпулятивним кампаніям і формує доказову базу для інформування громадськості. В Україні вже накопичено значний позитивний досвід функціонування таких організацій, як «StopFake», «Інститут масової інформації», «Детектор медіа», «Інтерньюз-Україна». Ці інституції спеціалізуються на системному моніторингу медіапростору, фактчекінгу, викритті фейкових повідомлень та дослідженні динаміки поширення дезінформації. Їхні аналітичні звіти, методичні матеріали та навчальні програми є цінним інструментом як для професійної спільноти, так і для широкого загалу. У цьому контексті держава повинна активніше інтегрувати експертний потенціал таких центрів у процеси формування та реалізації інформаційної політики. Зокрема, йдеться про залучення фахівців до розробки стратегічних документів, реалізації державних інформаційних кампаній, цільових програм, а також проведення тренінгів і навчальних заходів для представників органів державної влади та публічної служби. (Хряпинський, 2024: 328).

Наступним є посилення інституційної спроможності у сфері стратегічних комунікацій, що передбачає розбудову цілісної та скоординованої системи взаємодії органів влади з цільовими аудиторіями, і йдеться не лише про формування у структурі ключових міністерств і відомств спеціалізованих підрозділів, відповідальних за аналіз інформаційного середовища, планування та реалізацію узгоджених комунікативних кампаній, спрямованих на роз'яснення та просування офіційної позиції, а й про стимулювання горизонтальної взаємодії між різними державними інституціями, місцевим самоврядуванням, бізнесом, громадськістю навколо вирішення спільних безпекових завдань, де особливу роль відіграє синхронізація меседжів та координація зусиль усіх комунікаторів у протидії ворожим інформаційним кампаніям. Зміцнення

кібербезпеки як невід'ємного компоненту інформаційної стійкості держави є критично важливим, оскільки в умовах гібридної війни деструктивні інформаційні впливи часто супроводжуються кібератаками на об'єкти критичної інфраструктури, державні реєстри, бази даних, і здатність своєчасно виявляти та нейтралізувати кіберзагрози набуває ключового значення для захисту суверенітету та обороноздатності країни, що вимагає розробки проактивних стратегій кібероборони, інвестування у сучасні технології захисту інформації, посилення координації між профільними відомствами, а також налагодження тісного партнерства з приватним сектором у форматі обміну даними про загрози та кращими практиками реагування на інциденти (Хряпинський, 2024: 329).

Не менш напрямом діяльності є й розвінчування фейків та дезінформації, які становлять основу гібридних інформаційних атак, і окрім зусиль державних органів та громадських ініціатив, спрямованих на викриття маніпулятивних меседжів, необхідно розбудовувати культуру критичного споживання інформації серед широких верств населення, коли користувачі медіа повинні мати базові навички перевірки даних, вміти розпізнавати ознаки фейкових повідомлень, розуміти природу маніпулятивних технологій, і лише поєднання інституційної роботи з фактчекінгом та розвитком медіаграмотності громадян здатне мінімізувати руйнівний вплив дезінформації на суспільну свідомість та процеси вироблення політичних рішень. Значну увагу слід приділяти розробці позитивного стратегічного нарративу України, який би чітко артикулював національні цінності, пріоритети розвитку та принципи взаємодії з зовнішнім світом, і в умовах інформаційної війни вкрай важливо формувати власний порядок денний, що ґрунтується на ствердженні української ідентичності, просуванні європейського та євроатлантичного вибору, захисті національних інтересів на міжнародній арені, адже послідовне

обстоювання власних смислів та інтерпретацій є запорукою збереження стратегічної суб'єктності держави в гібридному протистоянні (Хряпинський, 2024: 329).

Протидія деструктивним інформаційним впливам вимагає зміцнення механізмів демократичної участі та розширення можливостей громадянського суспільства, і що більш інклюзивними та підзвітними є процеси вироблення державної політики, то важче маніпулювати громадською думкою та дестабілізувати ситуацію ззовні, тому розвиток електронної демократії, забезпечення доступу до публічної інформації, налагодження системних комунікацій влади з населенням не лише сприяють ефективному урядуванню, але й виступають дієвими запобіжниками проти гібридних атак, а потужним інструментом протидії ворожим інформаційним кампаніям є розвиток якісної журналістики, орієнтованої на відстоювання суспільних інтересів та цінностей демократії, де професійні та етичні ЗМІ здатні чинити опір поширенню фейків та маніпуляцій, забезпечувати громадян збалансованою та достовірною інформацією, викривати приховані впливи та зловживання з боку можновладців. Успішність протидії гібридній агресії значною мірою залежить від здатності мобілізувати суспільство навколо спільних цінностей та змістів, і особливо важливу роль у цих процесах відіграє національна еліта – інтелектуальні та моральні авторитети країни, які через власну активну громадянську позицію задають тренди суспільного дискурсу, а їхні голоси мають бути добре чутними в медіапросторі, а меседжі – спрямованими на консолідацію соціуму, зміцнення державницьких засад, просування реформ та цивілізаційного вибору України (Хряпинський, 2024: 330).

Отже, до розділу 2 можна зробити наступні висновки. В результаті дослідження у другому розділі можна сказати, що Російський вплив на

Україну має системний і багатовимірний характер, спрямований на дестабілізацію внутрішньополітичної ситуації та підрив міжнародного іміджу держави через використання широкого спектра інструментів – від традиційних медіа до сучасних цифрових платформ, причому особливість російських інформаційно-психологічних операцій полягає у цілеспрямованому впливі на свідомість і підсвідомість цільової аудиторії з метою формування вигідних моделей поведінки, а ефективність таких операцій значною мірою визначається рівнем медіаграмотності та критичного мислення населення. Використання соціальних мереж як інструменту інформаційних операцій стало однією з ключових рис сучасних конфліктів, і російсько-українська війна після 24 лютого 2022 року це підтверджує, оскільки через цифрові платформи здійснюється швидке поширення інформації, що дозволяє оперативно впливати на масові настрої, при цьому Росія активно використовує соціальні мережі для просування власних наративів і дискредитації української влади, а мобілізаційна функція цих платформ проявляється у стимулюванні волонтерства та збору коштів з обох сторін. У випадку російської агресії проти Грузії у 2008 році інформаційна складова також відіграла значну роль, оскільки Росія активно використовувала медіа для формування негативного образу Грузії та легітимації власних дій, експлуатуючи поляризоване політичне середовище та відкритий ринок мас-медіа, що свідчить про довготривалий характер російських інформаційних операцій, аналогічні підходи до яких були застосовані під час анексії Криму та розпалювання конфлікту на Донбасі у 2014 році, де інформаційні операції супроводжували військові дії. Стратегічні цілі російської інформаційної війни часто полягають у підриві національної єдності цільових країн, що особливо помітно на прикладі країн Балтії, де Росія намагається використовувати етнічні, мовні та соціальні розбіжності для посилення напруженості шляхом поширення наративів про дискримінацію

російськомовного населення та спотворення історичних фактів через контрольовані Кремлем ЗМІ.

У відповідь на російську інформаційну агресію Україна впроваджує власні стратегії протидії, які включають технічні засоби захисту інформаційного простору, контрпропагандистські заходи, діяльність державних органів, таких як Центр протидії дезінформації, громадські ініціативи, незалежні медіа та культурну дипломатію. Російська концепція гібридної війни передбачає комплексне використання військових, політичних, економічних, інформаційних і кібернетичних інструментів, де інформаційна складова часто відіграє ключову роль на початкових етапах конфлікту для дестабілізації внутрішньої ситуації та формування сприятливої міжнародної громадської думки, часто із залученням проксі-сил. Поняття інформаційної війни охоплює поширення дезінформації та проведення психологічних операцій, спрямованих на зміну емоційного стану та поведінки цільової аудиторії, як це видно з російських операцій проти України, що апелюють до страху, ненависті та зневіри. Одним із вимірів інформаційного протистояння є боротьба наративів, де кожна зі сторін намагається нав'язати власне бачення подій, що особливо актуально у контексті російсько-української війни, де Росія просуває наратив про Україну як штучне державне утворення, а Україна наголошує на своїй історії державності та праві на самовизначення. Уразливість цільової держави до інформаційних атак, зумовлена суспільними розколами, низьким рівнем довіри до інституцій чи слабкістю медіа, є ключовим фактором їхньої ефективності, і Росія часто використовує ці вразливості, експлуатуючи мовні питання чи регіональні відмінності в Україні. Довготривалі інформаційні кампанії Росії проти країн Балтії спрямовані на вплив на формування ідентичності молодого покоління через романтизацію радянського минулого та формування позитивного ставлення

до сучасної Росії, що створює серйозні виклики для систем освіти цих країн. Мікротаргетинг як інструмент інформаційної війни, що передбачає доставку спеціально підготовлених повідомлень вузьким сегментам аудиторії, становить особливу загрозу через можливість прихованого та персоніфікованого впливу, як це було зафіксовано під час виборчих кампаній у США та інших країнах із використанням ботів і фейкових акаунтів.

Застосування Росією кібернетичних засобів у поєднанні з інформаційними операціями створює синергетичний ефект, посилюючи загальний вплив, прикладом чого є злам серверів політичних організацій із подальшою публікацією викраденої інформації для дискредитації опонентів, що свідчить про централізований характер російських атак. Операції впливу, здійснювані Росією, часто спрямовані не на пряме переконання, а на створення сумнівів і підрив довіри до будь-яких джерел інформації, що призводить до інформаційного нігілізму та ускладнює громадянам орієнтацію в інформаційному потоці. Приклади інформаційного впливу Росії на виборчі процеси в США демонструють, що навіть розвинені демократії не є невразливими до таких атак, які спрямовані на дестабілізацію політичної системи та підрив міжнародного авторитету, маючи довготривалі наслідки у вигляді політичної поляризації та зниження суспільної довіри. У контексті інформаційної війни проти України Росія активно використовує історичні наративи та маніпулює історичною пам'яттю для обґрунтування своїх територіальних претензій і заперечення права українського народу на самовизначення, що вимагає системної роботи з відновлення та популяризації правдивої української історії. Інформаційна війна є невід'ємною складовою російської стратегії війни нового покоління, яка характеризується нелінійністю та комплексним використанням різноманітних засобів впливу, де інформаційні операції

часто відіграють важливішу роль, ніж традиційні військові дії, для досягнення політичних цілей із мінімальним застосуванням сили. Естонський досвід протидії російським інформаційним впливам, особливо після 2007 року, є прикладом розробки ефективної системи захисту від гібридних загроз, що включає створення спеціалізованих державних структур, співпрацю державного та приватного сектору, підвищення медіаграмотності та активну комунікаційну політику. Складність протидії російським інформаційним операціям полягає також у використанні тактики віддзеркалення, коли Росія звинувачує опонентів у тих самих діях, які здійснює сама, що підкреслює важливість розвитку критичного мислення та медіаграмотності.

## **Висновки до розділу 2**

У другому розділі стало очевидно, що інформаційна війна — це не просто про фейки чи пропаганду, а про цілеспрямований і системний вплив на свідомість, довіру, ідентичність і політичну стабільність цілих держав. Росія, як головний ініціатор такого типу агресії, використовує максимально гнучкі й підступні методи — від розпалювання страху і ненависті через соціальні мережі до формування паралельної реальності за допомогою історичних фальсифікацій. І хоча основна увага була зосереджена на прикладі України, важливо, що аналогічні інструменти застосовувалися і в Грузії, країнах Балтії та навіть у США, що лише підтверджує глобальний характер цієї загрози. Разом з тим, ми бачимо, що протидія можлива — і вона починається з усвідомлення проблеми. Медіаграмотність, сильна інституційна комунікація, національна ідентичність і незалежна журналістика стають ключовими щитами у цій новій війні. Україна, хоч і стала мішенню, водночас стала й прикладом стійкості: від дій Центру протидії дезінформації до культурної дипломатії та цифрових ініціатив. Усе це — не лише реакція на загрозу, а й стратегія боротьби за власну реальність, суб'єктність і майбутнє.

## **ВИСНОВКИ**

Отже, результатом даної роботи є здійснення комплексного аналізу теоретико-методологічних засад, що дозволило розкрити сутність і типологію інформаційних війн і, найголовніше, виявити ті глибинні

механізми, які визначають характер і масштаби деструктивного впливу інформаційних атак на політичні інститути, громадську думку, соціальну згуртованість та загальний рівень політичної стійкості держави, причому особливу увагу було приділено аналізу тих стратегій і технологій, які використовуються у сучасних інформаційних війнах для досягнення цілей, що виходять далеко за межі традиційного політичного протистояння, оскільки інформаційний простір перетворюється на багатовимірну арену, де взаємодіють різноманітні суб'єкти, а інформаційні потоки стають інструментом не лише для формування, а й для руйнування політичної стабільності. Було доведено, що інформаційні війни здатні провокувати виникнення кризових явищ у політичній системі, сприяти формуванню атмосфери недовіри, розколу в суспільстві, а також створювати умови для дестабілізації політичної влади, що підтверджується аналізом конкретних ситуацій, які були розглянуті у межах основної частини роботи, де простежується чіткий взаємозв'язок між інтенсивністю інформаційних атак і рівнем політичної напруги, а також зниженням ефективності функціонування політичних інститутів. Іншим є той факт, що інформаційні війни, використовуючи сучасні інформаційно-комунікаційні технології, здатні впливати на масову свідомість, формувати альтернативні реальності, створювати ілюзію консенсусу або, навпаки, розпалювати конфлікти, що ускладнює процес прийняття політичних рішень, підвищує ризики для політичної стабільності та вимагає розробки нових підходів до забезпечення інформаційної безпеки.

Досягнення поставленої мети та виконання завдань дослідження дало можливість систематизувати існуючі наукові підходи до аналізу інформаційних війн і обґрунтувати необхідність подальшого розвитку теоретичних і практичних засад протидії інформаційним загрозам, тому що сучасний стан інформаційного простору є дуже динамічним, зі зростанням

кількості та складності інформаційних атак, появою нових форм і методів впливу, що вимагає від держави, суспільства та політичних інститутів формування ефективних механізмів реагування, які базуються на системному аналізі, використанні сучасних технологій моніторингу, прогнозування та нейтралізації інформаційних загроз.

В ході цієї роботи також було доведено, що для забезпечення політичної стабільності в умовах інформаційних війн необхідно формувати культуру критичного мислення, підвищувати рівень інформаційної грамотності населення, удосконалювати законодавчу та інституційну базу, а також забезпечувати ефективну взаємодію між державними органами, громадянським суспільством і засобами масової інформації, оскільки лише за умови комплексного підходу до вирішення проблеми можна досягти стійкості політичної системи, мінімізувати ризики дестабілізації та забезпечити ефективне функціонування політичних інститутів у довгостроковій перспективі. Результатом роботи є доведення, що інформаційні війни є нестандартним та невидимим явищем, яке потребує постійного моніторингу, аналізу та вдосконалення підходів до забезпечення політичної стабільності, причому особливу увагу слід приділяти розвитку системи раннього попередження, підвищенню рівня координації між різними суб'єктами інформаційної безпеки та формуванню ефективної системи комунікації між владою і суспільством.

## **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Амелічева А. С. Окремі аспекти російсько-української інформаційної війни після 24 лютого 2022. Київ, 2023. 87 с.
2. Аналіз загроз національній безпеці у сфері внутрішньої політики : аналітична доповідь. Київ : НІСД, 2024. 31 с.
3. Васюк Н. О., Гаєвська Л. А. Реалізація державної політики протидії дезінформації в Україні: організаційно-правові засади. Інвестиції: практика та досвід. 2023. № 16. С. 172–178.
4. Гошовська В., Гандзюк А., Даниленко Л., Шемчук А., Гачков А. Проблеми інформаційного забезпечення української політичної безпеки. AD ALTA: Journal of Interdisciplinary Research. 2023. Vol. 13, Iss. 1. P. 200–204.
5. Грицай Р. О. Інформаційні війни: пошук стратегій протидії. Публічне управління і адміністрування в Україні. 2023. Вип. 33. С. 18–23.
6. Жадько Т. В. Інформаційні війни в історії та сучасності: характерні ознаки новітніх протистоянь. 64–95 с.
7. Інформаційна агресія в сучасному світі: правовий аналіз та протидія: Матеріали всеукраїнського науково-практичного круглого столу (2024). Харків: НДІ вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України.
8. Ковалевський, В. О. (2010). Інформаційна взаємодія у політико-владному полі великого міста. ІПіЕНД ім. І.Ф. Кураса НАН України.
9. «Коли слова стали зброєю»: безпрецедентні ризики для цивільного населення через поширення дезінформації в Україні. Center for Civilians in Conflict. 2023. 100 с.

10. Ломака, І. (2024). Війна як чинник нестабільності в сучасній Україні та її вплив на сфери національної безпеки. Вісник Прикарпатського університету. Серія: Політологія, (17), 84–89.
11. Міненко, Є. С. (2024). Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності. Український державний університет імені Михайла Драгоманова.
12. Пащенко А. Методи та складові сучасної інформаційної війни, вивчення її впливу на свідомість та поведінку людей. Збірник наукових праць. Психолого-педагогічні проблеми сучасної школи. 2023. Вип. 2(10). С. 83–90.
13. Проноза І. І. Інформаційна війна: сутність та особливості прояву. Актуальні проблеми політики. 2018. Вип. 61. С. 76–84.
14. Ржевська Н. Сучасна інформаційна політика: досвід США для України. Політична культура та ідеологія. 2024. № 1. С. 4–15.
15. Семченко, О. Р. (2015). Політична стабільність: огляд дисертаційних досліджень (2003-2014 рр.). Науковий часопис НПУ імені М. П. Драгоманова, (16), 193–200.
16. Скочиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2024. № 2 (42). С. 151–158.
17. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. Науковий вісник Ужгородського національного університету. Серія: Право. 2018. Вип. 52. Т. 3. С. 96–99.
18. Ухаль П. О. Інформаційні війни: причини та технології ведення : дипломна робота на здобуття освітнього ступеня магістра. Ужгород : Ужгородський національний університет, 2023. 76 с.

19. Худолій А. О. Інформаційна війна 2014–2022 рр. : монографія. Острого : Видавництво Національного університету «Острозька академія», 2022. 208 с.
20. Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії: довга тінь Росії / пер. з англ. І. Ємельянової. Бостон : Academic Studies Press, 2025. 306 с.
21. Яворський, М. (2017). Політична стабільність: сутність та основні підходи до класифікації. *Political sciences*, 3(1), 1–6.
22. Яковчук Я. С., Малець Б. І., Борзов Ю. О. Інформаційні війни в сучасному світі. Львівський державний університет безпеки життєдіяльності. Львів. 4 с.
23. Adefolurin T. Analytical study of national security linkages in Nigeria and solutions to the problematics of Boko Haram terrorist activities 2009–2014 : Master's thesis. Lafia : National Open University of Nigeria, 2014. 88 с.
24. Albert, C. D., Mullaney, S., Huitt, J., Hunter, L. Y., & Snider, L. (2023). Weaponizing Words: Using Technology to Proliferate Information Warfare. *The Cyber Defense Review*, 8(3), 1–25.
25. Baezner M. Cyber and Information warfare in the Ukrainian conflict. Version 2. Zürich : Center for Security Studies (CSS), ETH Zürich, 2018. 55 p.
26. Baranovsky-Dewey A. Determinants of the timing and intensity of propaganda attacks: Russia's information offensives in Georgia and Ukraine. *STAIR*. 2018. Vol. 14, no. 2. P. 120–146.

27. Baranovsky-Dewey A. Determinants of the timing and intensity of propaganda attacks: Russia's information offensives in Georgia and Ukraine. *Stair*. 2019. Vol. 14, No. 2. P. 120–141.
28. Brantly, A. Battling the bear: Ukraine's approach to national cyber and information security. In *Ukraine's approach to national cyber and information security*.
29. Farah M. B. Internal and external challenges of federalism in Somalia : Master of Public Administration (MPA) Program. Bangladesh : Stamford University Bangladesh, 2018. 53 c.
30. Farwell J. P. *Information Warfare: Forging Communication Strategies for Twenty-first Century Operational Environments*. Quantico, Virginia : Marine Corps University Press, 2020. 198 p.
31. Fedoniuk S., Karpchuk N., Yuskiv B. Ukraine's Information Security Policy: at the Crossroads between Russia and the West. *Czech Journal of Political Science/Politologický Časopis*. 2023. Vol. 30, Issue 3. P. 184–198.
32. Helmus T. C., Holynska K. *Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict*. Santa Monica : RAND Corporation, 2024. 96 c.
33. Hryshchenko, S., Savchenko, V., Kumeiko, A., Patsuriia, N., & Rieznikova, V. (n.d.). *Current State of Information Security in Ukraine*. *Danube*, 16(1), 16–29.
34. Iasiello E. J. Russia's Improved Information Operations: From Georgia to Crimea. *Parameters*. 2017. Vol. 47, No. 2. P. 7–15.
35. Kerr J. A. *Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons*. Arlington, VA : CNA, 2023. 52 p.

36. Khryapynskiy A. Promising directions of information policy for countering hybrid threats. *State Formation*. 2024. No. 2 (36). P. 165–173.
37. Kurban O. V. Сучасні інформаційні війни у мережевому он-лайн просторі: навчальний посібник. Київ, 2016. 286 с.
38. Lange-Ionatamishvili E. Analysis of Russia's information campaign against Ukraine: Examining non-military aspects of the crisis in Ukraine from a strategic communications perspectives. Riga : NATO StratCom Centre of Excellence, 2015. 40 с.
39. Legenkyi M., Piankivska L., Tolbatov A. Legal basis for cybersecurity in Ukraine under martial law. *CEUR Workshop Proceedings*. 2023. P. 1–10.
40. Mirzoyan A. Theoretical Approaches to Political Stability: How Do Theories Interpret the Factors Influencing It? *Journal of Political Science: Bulletin of Yerevan University*. 2024. Vol. 3, No. 2 (8). P. 65–80.
41. Mullaney, S. (2020). *Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020*. [Неопублікована робота].
42. Mullaney, S. (2021). *Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020*.
43. Muradov I. The Russian hybrid warfare: the cases of Ukraine and Georgia. *Defence Studies*. 2022. Vol. 22, no. 2. P. 168–191.
44. Nguyen T. A. [та ін.]. Effects of ‘Digital’ Country’s Information Security on Political Stability. 2021. 23 p.
45. Nguyen, T. A., Koblandin, K., Suleymanova, S., & Volokh, V. (2021). Effects of ‘Digital’ Country’s Information Security on Political Stability. *International Journal of Digital Economy*, 2(4), 31–51.

46. Pierri, F., & Jindal, N. (2023). Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine.
47. The Russia-Ukraine War's Implications for Global Security: A First Multi-issue Analysis / edited by T. Greminger and T. Vestner. Geneva : Geneva Centre for Security Policy, 2022. 54 с.
48. Sadik G. (ed.). The effects of the Russia-Ukraine war on countering terrorism. Ankara: Centre of Excellence Defence Against Terrorism (COE-DAT), 2025. 138 p.
49. Savchuk, V. R. (2024). Від умиротворення до консолідації: підтримка України як відповідь Заходу на початок російського вторгнення. Науковий журнал «Політикус», (6), 174. DOI: <https://doi.org/10.24195/2414-9616.2024-6.25>
50. Shih, V., Zhang, P., & Liu, M. (2018). Threats and Political Instability in Authoritarian Regimes: A Dynamic Theoretical Analysis. [Неопублікована робота].
51. Sirinyok-Dolgaryova, K., Yurtayeva, K., & Taranenko, A. (n.d.). Countering Disinformation Among Hybrid Threats in the Russia-Ukraine War: Building Resilience Through Government and Civil Society Cooperation. Retrieved from <https://ssrn.com/abstract=4882578>
52. Wolterman J. Mapping Information Warfare: Creating a Coherent Typology of Informational Coercion. 2019. 30 p.

## АНОТАЦІЯ

Ємельянов І. О. Вплив інформаційних війн на політичну стабільність держав (бакалаврська робота). Харків: Харківський національний університет імені В. Н. Каразіна, 2025. 55 с. (рукопис).

У роботі досліджено теоретико-методологічні засади та практичні аспекти впливу інформаційних війн на політичну стабільність держави. Обґрунтовано актуальність вивчення інформаційного протистояння як фактора, що суттєво трансформує політичні інститути, громадську думку та соціальну згуртованість. Розкрито поняття, типологію, ознаки та стратегії інформаційних війн. У другому блоці проаналізовано механізми їх впливу на політичну стабільність, включаючи емпіричні приклади дестабілізації. Застосовано комплекс загальнонаукових та спеціальних методів дослідження, включаючи системний та синергетичний підходи.

Ключові слова: інформаційна війна, політична стабільність, інформаційна безпека, дезінформація, вплив на громадську думку.

## ANNOTATION

Yemelianov I. O. The Impact of Information Wars on the Political Stability of the State (Bachelor's Thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 55 p. (manuscript).

This thesis explores the theoretical and methodological foundations, as well as the practical aspects, of how information wars influence political stability. The work substantiates the relevance of studying information confrontation as a factor that significantly transforms political institutions, public opinion, and social cohesion. It defines the concept, typology, characteristics, and strategies of information wars. The second section examines their mechanisms of influence, including empirical examples of destabilization. A comprehensive set of general scientific and special research methods is employed, notably systemic and synergetic approaches.

Keywords: information warfare, political stability, information security, disinformation, influence on public opinion.

**ВІДГУК**  
**на кваліфікаційну роботу бакалавра**  
**4-го курсу групи ОП-41 денної форми навчання**  
**спеціальності 052 «Політологія»**  
**освітньо-професійної програми «Політичні технології та аналіз**  
**політики»**  
**філософського факультету**  
**Харківського національного університету імені В. Н. Каразіна**  
**Ємельянова Івана Олександровича**  
**на тему: «Вплив інформаційних війн на політичну стабільність держав»**

Актуальність теми роботи **Ємельянова Івана Олександровича** обумовлена кількома факторами: інформаційний простір перетворюється на арену глобального протистояння; інформаційні технології стають не лише інструментом комунікації, а й засобом маніпуляції масовою свідомістю; інформаційні війни здатні підривати довіру до інститутів влади, провокувати соціальну напругу, а також впливати на формування громадської думки. Основним фактором є необхідність швидкого реагування на зміни, забезпечення безпеки та стабільності у політичній сфері. Тематика політичної стабільності була актуальною від початку української незалежності, але не менш важливим фактором є й надзвичайно пришвидшене посилення значення завдань протистояння інформаційній війні від початку російської агресії. Автор сконцентрував увагу практичної частини дослідження саме на аналізі сучасних кейсів щодо інформаційних війн, на практичних питаннях забезпечення протидії викликам інформаційної війни на рівні інструментів та державної політики. Такий фокус є виправданим та вдалим, оскільки роль практичних заходів у цій сфері збільшується, натомість ці питання залишається недостатньо вивченим та недостатньо висвітленим у публічній площині особливо через швидкість змін..

Позитивні аспекти роботи, на нашу думку, такі: значний обсяг сучасних джерел та опрацьованої літератури, велика частина з якої західних авторів; достатня емпірична база; логічність структури роботи, самостійність та обґрунтованість основних позицій, рекомендацій та висновків. Зміст роботи розкриває мету та завдання, що були визначені. Автор вірно звертається до визначення теоретичних засад проблематики, надає критичний погляд на практику реалізації різних кейсів, доцільно використовує обрані методи дослідження, розробляє власні підходи до оцінки практичних інструментів та державної політики протидії інформаційним загрозам. Наприклад, у другому розділі здійснюється аналіз впливу інформаційних

війн на політичну стабільність держави, розглядаються механізми впливу, а також наводяться приклади конкретних ситуацій, що ілюструють взаємозв'язок між інформаційними війнами та політичною стабільністю. Автор доцільно виокремлює стратегії ведення інформаційних війн, вірно визначає їхню типологію. Автор досліджує досвід інших країн, наприклад, Грузії, Сполучених Штатів Америки, вміло використовує порівняльний метод, адаптує цей досвід для використання у рекомендаціях відповідних до українського контексту.

Відповідно, запропоновані автором висновки та рекомендації заслуговують на схвальну оцінку, виявляють високий рівень фахової підготовки та здатність автора до наукових розвідок. Слід зазначити, що висновки та пропозиції Івана Ємельянова мають практичну цінність для організації ефективних заходів протидії інформаційним війнам, практична цінність роботи для застосування у політичній сфері щодо розробки політичних технологій та політичного аналізу підсилюється обраним вектором дослідження, який поєднує вимір інформаційних загроз та політичної стабільності.

Питання, визначені в роботі, розкрито, але вона не позбавлена окремих недоліків. Автору слід було б звернути більшу увагу на характеристику стану нестабільності, провести кореляцію інформаційних загроз, впливів інформаційної війни та особливостей продукування нестабільності. У першому розділі слід було б приділити більшу увагу факторам актуалізації інформаційних війн в інформаційну епоху, що відповідає системному підходу до розгляду обраної проблематики.

У цілому кваліфікаційна робота бакалавра «Вплив інформаційних війн на політичну стабільність держав» за всіма формальними та змістовними критеріями відповідає встановленим вимогам та заслуговує на високу оцінку (91 бал за 100-бальною шкалою), а її автор, Ємельянов Іван Олександрович, гідний присвоєння кваліфікації бакалавра зі спеціальності 052 «Політологія» (ОПП «Політичні технології та аналіз політики»).

**Керівник кваліфікаційної роботи:**

д. політ. н., доц., професор  
кафедри політології  
Харківського національного

університету імені В. Н. Каразіна  
КОМАРОВА



Тетяна

## РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра  
4-го курсу групи ОП-41 денної форми навчання  
спеціальності 052 «Політологія»

освітньо-професійної програми «Політичні технології та аналіз політики»  
філософського факультету

Харківського національного університету імені В. Н. Каразіна  
Ємельянова Івана Олександровича

на тему: «Вплив інформаційних війн на політичну стабільність держав»

Кваліфікаційна робота І. О. Ємельянова є актуальним дослідженням, присвяченим проблемі впливу інформаційних війн на політичну стабільність держав. У контексті сучасної міжнародної ситуації, зокрема російсько-української війни, тема роботи набуває особливої ваги. Під час дослідження студент продемонстрував глибоке розуміння природи інформаційного протиборства та його системного впливу на політичну сферу.

Робота має раціональну структуру. У першому розділі автор ґрунтовно розглядає сутність, ознаки та типологію інформаційних війн, окреслює їхні основні стратегії, засоби впливу, цілі, інструменти та суб'єкти. У другому розділі акцент зроблено на прикладному аспекті: проаналізовано кейси України, Грузії, США та інших країн.

Теоретична база роботи охоплює широкий спектр джерел – від класичних концепцій до сучасних напрацювань у сфері інформаційної безпеки. У роботі вдало поєднано загальнонаукові й спеціальні методи, що забезпечує комплексний підхід до розкриття теми.

Окрему увагу приділено механізмам протидії інформаційним загрозам, зокрема ролі державної політики, стратегічних комунікацій, інститутів інформаційної безпеки, розвитку медіаграмотності. Автор виявляє зв'язок між цифровізацією та зростанням вразливості політичної системи, детально описує інформаційні атаки на інститути влади та соціальну згуртованість.

Робота характеризується високим рівнем наукового аналізу, використанням сучасних емпіричних прикладів, добре структурованими розділами. Особливо варто відзначити спробу концептуалізувати інформаційну війну як багатовимірне явище, що проникає у всі рівні політичного процесу. Студент демонструє вміння працювати з теорією, робити порівняльний аналіз, узагальнювати та формулювати обґрунтовані висновки.

Попри високий рівень роботи, є деякі зауваження. Наприклад, у розділі 2.1 було б доречно більш чітко розмежувати політичні, психологічні й технічні

наслідки інформаційних атак. У висновках варто було б стисло окреслити рекомендації для державної політики у сфері протидії гібридним загрозам. Також у деяких місцях стилістика потребує більшої академічної точності.

У цілому треба констатувати, що робота має велику актуальність, наукову новизну, теоретико-практичну цінність й відповідає вимогам, що ставляться до кваліфікаційної роботи бакалавра, а її автор, Смелянов Іван Олександрович, заслуговує на присвоєння кваліфікації бакалавра зі спеціальності 052 «Політологія».

**Рецензент:**

доктор політичних наук, професор,  
професор кафедри міжнародних відносин і  
політичної філософії  
Харківського національного економічного  
університету імені Семена Кузнеця



О. І. Романюк