**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ФАКУЛЬТЕТ СОЦІОЛОГІЇ ТА УПРАВЛІННЯ**

**КАФЕДРА ПОЛІТОЛОГІЇ**

**Кваліфікаційна робота**

**бакалавра**

**ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВІЙНИ**

Виконав: студент групи 6.0520-п

спеціальності 052 Політологія

освітньо-професійної програми «Політологія»

О. В. Стасик

Керівник доцент кафедри політології, доцент,

к.політ.н. А. О. Руднєва

Рецензент доцент кафедри політології,

доцент, к.політ.н. Мальована Ю.Г.

Запоріжжя – 2024

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

Факультет соціології та управління

Кафедра політології

Рівень вищої освіти бакалавр

Спеціальність 052 Політологія

Освітньо-професійна програма «Політологія»

**ЗАТВЕРДЖУЮ**

Завідувач кафедри Є.Г. Цокур\_\_\_\_\_

«12» червня\_2024 року

**З А В Д А Н Н Я**

**НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Стасику Олександру Віталійовичу

1. Тема роботи (проєкту) Особливості інформаційної політики в Україні в умовах війни

керівник роботи Руднєва Анна Олегівна, к.політ.н., доцент

затверджені наказом ЗНУ від «18»\_січня\_\_2024\_року № 77-с

1. Строк подання студентом роботи 12 червня 2024 року

Вихідні дані до роботи Абрамов В.І. Гібридна війна як нова форма міждержавного протиборства: стратегія перемоги. *Виклики і загрози національній безпеці в умовах гібридної війни* : матеріали наук.-практ. семінару, м. Київ, 27 квіт. 2017 р. Київ, 2017. С. 17–22. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні. Київ : «Юстиніан», 2006. 176 с. Глушко О.К. Журналістське розслідування: Історія, теорія, практика : навчальний посібник для студентів вищих навчальних закладів. Київ : Арістей, 2006. 144 с. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті : монографія. Київ : Генеза, 2004. 208 с.

1. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1.Розкрити стан наукового дослідження питання інформаційної політики в умовах війни. 2.Проаналізувати понятійно-категоріальний апарат дослідження. 3.Визначити методи та принципи дослідження інформаційної політики в умовах війни. 4.Визначити сутність інформаційної політики. 5.Висвітлити інструменти та методи інформаційної боротьби в умовах конфлікту. 6.Охарактеризувати виклики та загрози в інформаційній сфері в умовах війни. 7.Описати сучасний стан реалізації інформаційної політики України в умовах війни. 8.Дослідити міжнародний досвід формування інформаційної політики в умовах війни. 9.Надати рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах війни.
2. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) таблиць 0
3. Консультанти розділів роботи

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  Консультанта | Підпис, дата | |
| завдання  видав | завдання  прийняв |
| Розділ 1 | Руднєва А.О., доцент кафедри політології | 05.12.23 | 05.12.23 |
| Розділ 2 | Руднєва А.О., доцент кафедри політології | 24.01.24 | 24.01.24 |
| Розділ 3 | Руднєва А.О., доцент кафедри політології | 22.02.24 | 22.02.24 |

1. Дата видачі завдання 5 грудня 2023

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
| 1. | Вибір та формулювання теми роботи | Жовтень 2023 | *виконано* |
| 2. | Опрацювання наукових джерел | Листопад 2023 | *виконано* |
| 3. | Робота над вступом | Грудень 2023 | *виконано* |
| 4. | Робота над першим розділом | Січень 2024 | *виконано* |
| 5. | Робота над другим розділом | Лютий 2024 | *виконано* |
| 6. | Проведення дослідження | Березень 2024 | *виконано* |
| 7. | Робота над третім розділом | Квітень 2024 | *виконано* |
| 8. | Систематизація висновків | Травень 2024 | *виконано* |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О. В. Стасик

Керівник роботи (проєкту) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. О. Руднєва

**Нормоконтроль пройдено**

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_ Ю. Г. Мальована

**РЕФЕРАТ**

Кваліфікаційна робота складається з 59 сторінок, без ілюстрацій, перелік літератури з 80 позицій.

ІНФОРМАЦІЯ, ВІЙНА, ІНФОРМАЦІЙНА ПОЛІТИКА, БЕЗПЕКА, ТЕХНОЛОГІЇ

*Мета роботи* дослідити особливості інформаційної політики України в умовах війни, розробити рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах військового конфлікту.

*Об’єктом дослідження* є інформаційна політика України.

*Предметом дослідження* є особливості інформаційної політики України в умовах війни.

*Методи дослідження:* дедукція, індукція, аналіз, спостереження, порівняння та узагальнення.

*Гіпотеза дослідження:* умови війни суттєво впливають на інформаційну політику України, що проявляється у підвищенні рівня державного контролю над медіа, збільшенні кількості інформаційних кампаній, спрямованих на підтримку морального духу населення, та активізації заходів протидії ворожій пропаганді.

*Висновки:*

1. Інформаційна політика України в умовах війни спрямована на захист інформаційного простору та підвищення інформаційної безпеки
2. Україна використовує різноманітні інструменти для інформаційної боротьби, включаючи медіа, соціальні мережі, психологічні впливи, кіберзаходи та дипломатичні канали.

**ABSTRACT**

The qualification work consists of 59 pages, without illustrations, a list of literature of 80 items.

INFORMATION, WAR, INFORMATION POLICY, SECURITY, TECHNOLOGY

*The purpose of the work* is to investigate the peculiarities of the information policy of Ukraine in the conditions of war, to develop recommendations for improving the information policy of Ukraine in order to counter information aggression in the conditions of a military conflict.

*The object* of the study is the information policy of Ukraine.

*The subject* of the study is the peculiarities of the information policy of Ukraine in the conditions of war.

*Research methods*: deduction, induction, analysis, observation, comparison and generalization.

*The hypothesis of the study*: the conditions of war significantly affect the information policy of Ukraine, which is manifested in the increase in the level of state control over the media, the increase in the number of information campaigns aimed at supporting the morale of the population, and the activation of measures to counter enemy propaganda.

*Conclusions*:

1. The information policy of Ukraine in the conditions of war is aimed at protecting the information space and increasing information security

2. Ukraine uses various tools for information warfare, including media, social networks, psychological influences, cyber measures and diplomatic channels.

ЗМІСТ

[ВСТУП 7](#_Toc168736636)

РОЗДІЛ 1. [ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВІЙНИ](#_Toc168736638)

[1.1. Стан наукового дослідження питання інформаційної політики в умовах війни 10](#_Toc168736639)

[1.2. Аналіз понятійно-категоріального апарату дослідження 16](#_Toc168736640)

[1.3. Методи та принципи дослідження інформаційної політики в умовах війни…………………………………………………………………………………19](#_Toc168736641)

РОЗДІЛ 2. [ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ В УМОВАХ ВІЙНИ](#_Toc168736643)

[2.1. Сутність інформаційної політики 24](#_Toc168736644)

[2.2. Інструменти та методи інформаційної боротьби в умовах конфлікту 29](#_Toc168736645)

[2.3. Виклики та загрози в інформаційній сфері в умовах війни 35](#_Toc168736646)

РОЗДІЛ 3. [ПРАКСЕОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВІЙНИ](#_Toc168736648)

[3.1. Сучасний стан реалізації інформаційної політики України в умовах війни 43](#_Toc168736649)

[3.2. Міжнародний досвід реалізації інформаційної політики в умовах військових конфліктів 50](#_Toc168736650)

[3.3. Рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах війни 58](#_Toc168736651)

[ВИСНОВКИ 65](#_Toc168736652)

[СПИСОК ЛІТЕРАТУРИ 68](#_Toc168736653)

# ВСТУП

Розвиток новітніх технологій та зростання ролі інформаційного простору впливають на всі сфери суспільства, включаючи освіту, бізнес, виробництво, науку та політику. Сучасна епоха характеризується інтенсивним розвитком і використанням різноманітних інформаційних ресурсів, які впливають на процеси управління та суспільний розвиток. Зокрема, введення новітніх технологій створює нові виклики у політичній сфері, де стабільність та функціонування залежать від якості та оперативності інформації, яку отримує політична еліта, а також від реакції управлінської системи на цю інформацію. Це підтверджує тезу про те, що політична діяльність сьогодні – це боротьба за вплив на свідомість політичної еліти та систему управління, особливо в умовах інформаційного суспільства.

Інформація проникає у будь-які сфери існування держави, зокрема в політичну, соціальну та економічну. Щоб мати змогу конкурувати на міжнародній арені та вигідно представляти себе, держава повинна адаптуватися під зростаючий рівень цифровізації у світі. Дуже важливим елементом існування будь-якої держави є безпека, інформаційну складову якої неможливо переоцінити. Події сьогодення вказують на актуальність проблеми пов’язаної з реалізацією інформаційної політики, зокрема створення іміджевої складової держави на міжнародній арені. Реальність вказує на певний парадокс у загальній поінформованості світу : чим більше джерел інформації існує , тим менше інформації може дійти до споживача. Цей тренд яскраво прослідковується в умовах гібридної війни росії проти України. Враховуючи лавину пропаганди з боку росії та великої кількості маніпулятивних впливів слід адекватно реагувати на ці виклики та гідно давати їм відсіч. Тому для України є життєво необхідним правильно формувати інформаційну політику як внутрішню так і зовнішню, позаяк наразі стоїть питання існування держави як суверенного та незалежного утворення.

Мета кваліфікаційної роботи: дослідити особливості інформаційної політики України в умовах війни, розробити рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах військового конфлікту.

Для досягнення заданої мети визначені такі завдання:

– розкрити стан наукового дослідження питання інформаційної політики в умовах війни;

– проаналізувати понятійно-категоріальний апарат дослідження;

– визначити методи та принципи дослідження інформаційної політики в умовах війни;

– визначити сутність інформаційної політики;

– висвітлити інструменти та методи інформаційної боротьби в умовах конфлікту;

– охарактеризувати виклики та загрози в інформаційній сфері в умовах війни;

– описати сучасний стан реалізації інформаційної політики України в умовах війни;

– дослідити міжнародний досвід формування інформаційної політики в умовах війни;

– надати рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах війни.

Об’єкт дослідження – інформаційна політика України.

Предмет дослідження – особливості інформаційної політики України в умовах війни.

Гіпотеза: умови війни суттєво впливають на інформаційну політику України, що проявляється у підвищенні рівня державного контролю над медіа, збільшенні кількості інформаційних кампаній, спрямованих на підтримку морального духу населення, та активізації заходів протидії ворожій пропаганді. Така трансформація інформаційної політики сприяє консолідації суспільства, покращенню міжнародного іміджу України та забезпеченню національної безпеки в умовах агресії.

Структура роботи: кваліфікаційна робота складається зі вступу, трьох розділів, поділених на підрозділи, висновків та списку використаних джерел. Загальний обсяг роботи – 59 сторінок. Список використаних джерел та літератури містить 80 найменувань.

# РОЗДІЛ 1

# ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВІЙНИ

## 1.1. Стан наукового дослідження питання інформаційної політики в умовах війни

Процеси глобалізації та трансформації, які відбуваються у всьому світі, пов’язані з поширенням нового інформаційного суспільства та його впливом на розвиток громадянських інститутів. Розвиток інформаційно-комунікаційних технологій відіграє ключову роль у функціонуванні громадянського суспільства і держави, стаючи важливим компонентом їхньої діяльності. У такому глобальному суспільстві важливо для людини адаптуватися до нового інформаційного середовища, вирішуючи завдання, пов’язані з освоєнням цього інформаційного простору. Це вимагає зміни звичайного способу життя та адаптації до нового інформаційного світу з усіма його глобальними, економічними, соціальними і культурними взаємозв’язками. Отже, інформаційна культура стає все більш значущою для населення і суттєво впливає на їхнє повсякденне життя [13, с. 122].

Видатні зарубіжні дослідники, такі як Д. Бел, Е. Бредлі, П. Бурдьє, М. Кастельс, П. Лазарсфельд, Т. Парсонс, М. Порат та інші, у своїх дослідженнях про інформаційне суспільство філософськи обґрунтовують розвиток і використання інформаційно-комунікаційних технологій. Вони підкреслюють, що засоби масової комунікації є важливим інструментом контролю за владою і повинні задовольняти потреби суспільства в інформації та комунікації [3].

Серед численних наукових праць про державну інформаційну політику України в контексті євроінтеграції особливо виділяються роботи В. Антонюка, І. Арістової [2], Л. Губерського, Ю. Нестеряка та монографія Національного інституту стратегічних досліджень. Ці дослідження мають важливе значення для розгляду даної теми.

Монографія Ю. Нестеряка «Державна інформаційна політика: теоретико-методологічні засади» досліджує основи державної інформаційної політики та пропонує методику створення комплексних механізмів її впровадження в Україні, враховуючи національні та культурні особливості і глобальні тенденції фрагментації традиційної ідентичності [32, с. 3].

У монографії «Державна інформаційна політика: організаційно-правові аспекти» І. Арістова досліджує головну мету державної інформаційної політики – створення відкритого інформаційного простору та його інтеграцію у світовий інформаційний простір. Вона аналізує організаційні та правові аспекти цього процесу, враховуючи державні пріоритети та особливості країни в забезпеченні інформаційної безпеки на внутрішньому і міжнародному рівнях [2].

С. Демський і С. Павлюк проаналізували понад 240 законодавчих актів, виданих органами державної влади України для регулювання інформаційних відносин [12, с. 8].

Медіа-експерти Д. Проценко і Д. Тупчієнко проаналізували світовий досвід правового регулювання нових засобів масової інформації [52, с. 4].

У повсякденному розумінні термін «інформаційна політика» часто пов’язують із засобами масової інформації та їх впливом на сприйняття публікованої інформації.

Суспільство трактує «інформаційну політику» в широкому і вузькому сенсі. У широкому сенсі це політика, пов’язана з інформаційною сферою, яка охоплює суспільні відносини, пов’язані з інформацією та інформаційною інфраструктурою як об’єктами інтересів індивіда, суспільства і держави [58].

За таким підходом, «інформаційна політика» означає використання ресурсів публічної влади для розв’язання ключових проблем розвитку інформаційної сфери. Ці проблеми включають підвищення якості життя, зміцнення гарантій прав і свобод, прискорення переходу до інформаційної фази розвитку, розвиток конкурентоспроможної інформаційної індустрії, забезпечення безпеки інформаційних систем та збереження культурних і моральних цінностей [20].

В узагальненому вигляді, «інформаційна політика» визначається як сукупність стратегій і методів, що використовуються для збору, використання, розповсюдження та зберігання інформації в соціальних системах, зокрема тих, які є чутливими до внутрішніх і зовнішніх інформаційних потоків. Такі процеси управління інформацією організовані і контролюються різними суспільними структурами [6].

Для формування особистого світогляду важливо мати доступ до різноманітних новин і подій, а також до професійних аналітиків, які можуть аналізувати не лише власне події, а й інформацію з інших джерел, перетворюючи її у новини. Це допомагає нам краще розуміти, куди направляти свої погляди і на що звертати увагу.

Основні стратегії і методи інформаційної політики включають такі аспекти [18, с. 12]:

1. забезпечення доступу громадян до інформації;

2. створення систем і мереж інформації для ефективного обміну даними;

3. підвищення матеріально-технічних, фінансових, організаційних, правових та наукових засад інформаційної діяльності;

4. забезпечення ефективного використання інформації через навчання аналізу та критичного мислення;

5. підтримка постійного оновлення, збагачення та збереження інформаційних ресурсів;

6. створення системи охорони інформації для захисту від несанкціонованого доступу та поширення інформації.

Держава має ключове значення серед учасників інформаційної політики завдяки своїй особливій ролі у забезпеченні функціонування політичної системи суспільства [15].

Важливо відзначити, що однією з основних функцій держави як органу публічної влади є легітимізація політики через відкрите визначення пріоритетів суспільного розвитку шляхом публічної політичної боротьби, в якій беруть участь різні суспільні сили. Ця функція передбачає правове регулювання політичної діяльності і забезпечення всіма учасниками дотримання законів. Якщо держава не здійснює цю функцію, політична боротьба може вийти за межі правового поля і призвести до використання соціальної сили або навіть насильства.

Держава виступає як активний учасник політичної боротьби, встановлюючи правила, форми і обмеження цієї боротьби, забезпечуючи дотримання законодавства, ініціюючи законодавчі та організаційні зміни, а також беручи участь у політичних процесах як суб’єкт з публічною владою [29].

Так, держава в суспільному контексті сприяє об'єднанню громадян для досягнення загального блага, забезпечує цілісність та ефективний розвиток суспільства. На індивідуальному рівні, вона реалізує свої ідеологічні погляди та концепції для раціонального вирішення найактуальніших суперечностей у суспільному розвитку.

Державна політика – це управлінська діяльність органів влади, яка базується на законодавчих нормах, легітимному застосуванні сили та належному забезпеченні ресурсами. Основні завдання включають підтримку функціонування суспільних та державних інституцій, забезпечення безпеки території та населення, а також реалізацію ідеологічних програм суб’єкта, що має публічну владу.

Сутність державної політики у суспільному контексті полягає у використанні ресурсів публічної влади для об’єднання громадян, для досягнення загального благополуччя, збереження цілісності суспільства та забезпечення його ефективного розвитку [26].

У суб’єктному вимірі, суть державної політики полягає у використанні правових та організаційних засобів публічної влади для втілення ідеологічних концепцій суб’єкта політики, що має публічну владу, у вирішенні актуальних проблем у суспільному розвитку.

Державна інформаційна політика – це термін, що вже визнаний і використовується в законодавстві. Він відображає спеціальну сферу діяльності державних органів та посадових осіб у сфері інформації, що ґрунтується на виконанні основних функцій держави.

Державна інформаційна політика може бути розглянута в двох аспектах: громадському і суб’єктному. У громадському аспекті ця політика спрямована на досягнення загального блага, включаючи підтримку конкурентоспроможності суспільства та соціальної стабільності. У суб’єктному аспекті вона зорієнтована на запобігання діям суб’єктів політики, що можуть шкодити конкурентоспроможності та стабільності суспільства [30].

Державна інформаційна політика у суспільному аспекті служить як механізм визначення та втілення суспільних пріоритетів у сфері інформації. Вона спрямована на виконання основних функцій держави та забезпечення законності використання цієї сфери, щоб запобігти недозволеним діям суб’єктів політики у боротьбі за владу.

У суб’єктному аспекті, державна інформаційна політика відображає інтереси суб’єкта політики, який має публічну владу, і спрямована на задоволення його політичних цілей. Ці цілі включають реалізацію ідеологічної програми суб'єкта політики та вирішення актуальних суспільних проблем.

Суб’єкт політики, після конкурентної боротьби, отримує можливість використовувати публічну владу. Його ідеологічна програма відображає потреби частини суспільства у розвитку культурних та моральних цінностей і протидії нелегітимним суб’єктам політики. Таким чином, держава зобов’язана сприяти суб’єкту політики у вирішенні цих завдань в рамках законодавчих параметрів і обмежень [33, с. 42].

Так, в суб’єктному аспекті, державна інформаційна політика може бути визначена як діяльність державних органів і посадових осіб у сфері інформації, спрямована на втілення ідеологічної програми суб’єкта з публічною владою. Ця діяльність спрямована на розвиток політичної свідомості суспільства і залучення суб’єктів політики до вирішення суспільних протиріч.

Отже, суть державної інформаційної політики в суб’єктному вимірі полягає в застосуванні правових та організаційних інструментів публічної влади для впливу на інформаційну сферу суспільства та залучення суб’єктів політики до вирішення найактуальніших соціально-економічних та політичних проблем, керуючись ідеологічною програмою суб'єкта з публічною владою.

Так, державна інформаційна політика служить засобом встановлення та досягнення цілей розвитку інформаційної сфери, сприяє стабільності управління країною і збереженню її культурних цінностей.

Державна інформаційна політика впливає на політичну свідомість та громадську думку, використовуючи різноманітні методи і засоби для мобілізації громадян на підтримку державної політики та їх участь у ній. Також, вона включає методи та засоби протидії «інформаційному тиску» на державу та суспільство з боку нелегітимних політичних сил та інших держав [38, с. 67].

Суть державної інформаційної політики визначається її метою, завданнями, принципами, пріоритетами та умовами діяльності державних органів і посадових осіб, які беруть участь у формуванні та реалізації цієї політики.

Форма державної інформаційної політики виявляється через механізми регулювання, які визначаються законодавчими актами та заходами управління, які впроваджуються державними органами та посадовими особами з метою реалізації цієї політики.

Як висновок можна зазначити, що досить велика кількість як зарубіжних так і українських науковців досліджували питання інформаційної політики держави. Серед них можна виділити В. Ю. Баскакова, І. А. Кисарець, В.А. Ліпкан, К.Г. Татарникова, О. В. Чуприна.

Отже, інформаційна політика стає важливим інструментом для формування політичної свідомості та впливу на громадську думку, а також для захисту державних інтересів у сфері інформації.

## 1.2. Аналіз понятійно-категоріального апарату дослідження

Сучасні наукові дослідження зосереджуються на різних аспектах створення, розвитку та функціонування державної інформаційної політики. Вони ґрунтуються на різноманітних наукових школах і теоріях, які розглядають інформацію та інформаційні системи як об’єкти управління державою. У сучасних умовах, включаючи часи воєнних конфліктів, методологія дослідження державної інформаційної політики має ґрунтуватися на сучасних уявленнях про неї як систему ідей, методів і засобів, які використовуються для нормативного регулювання взаємин між державною інформаційною системою, що впливає на суспільні процеси, та громадянським суспільством.

Спершу слід з’ясувати поняття інформації як такої. Інформація (від лат. informatio – роз’яснення) – відомості, які передають усним, писемним та іншими шляхами за допомогою умовних сигналів і технічних засобів [14].

Також в рамках нашого дослідження дуже важливо зрозуміти сутність поняття «війна». Війна це соціально-політичне явище, крайня форма розв’язання соціально-політичних, ідеологічних, економічних, територіальних, етнонаціональних, релігійних чи інших суперечностей між державами, народами, націями, урядами, спільнотами або воєнізованими групами, що відбувається за допомогою організованої збройної боротьби [8].

У процесі даного дослідження нам також потрібно встановити значення поняття «інформаційна війна» через важливість та актуальність цього поняття в сучасних реаліях російсько-української війни.Інформаційна війна – форма протиборства між різними суб’єктами (державами, неурядовими, економічними або іншими структурами), яка передбачає проведення комплексу заходів із завдання шкоди інформаційній сфері протилежної сторони та захисту власної інформаційної безпеки [19].

Методологія, згідно з визначенням Сурміна та Надолішного, є формою раціональної та рефлексивної свідомості, яка спрямована на вивчення, удосконалення та створення методів у різних сферах діяльності [61, с. 9]. Для систематизації методологічних підходів, які відповідають предмету дослідження, важливо спочатку чітко визначити такі поняття, як політика, інформаційна політика та державна інформаційна політика.

У вивченні політичної сфери українські дослідники стикаються з двозначністю терміну «політика», оскільки він може мати два різні концепти. У політології вживається термін «politics» для позначення «сфери взаємодії різних соціальних груп та індивідів у зв’язку з використанням інститутів державної влади для реалізації своїх суспільно значущих інтересів і потреб» [41, с. 13]. У контексті державної політики, «політика» тлумачиться як «policy», описуючи стратегію або план дій, що приймається та втілюється владою чи політичною партією [80, с. 984]. У відповідності з цим, «політика» в даному контексті означає сукупність намірів та засобів реалізації, які формуються суб’єктом управління для конкретної сфери суспільного життя, включаючи державну інформаційну політику.

Ураховуючи значний вплив недержавних акторів, таких як бізнес, ЗМІ, наукові установи, міжнародні організації та інститути громадянського суспільства на інформаційну політику, важливо розрізняти державну інформаційну політику від державної політики в інформаційній сфері. За словами Олександра Дем’янчука, державна політика охоплює ширший спектр суб’єктів, об’єктів і дій, ніж державна політика, оскільки не всі вони перебувають безпосередньо під впливом органів державного управління і самостійно формують свою політику, що неминуче впливає на державну політику [53, с. 11]. Ці розміри ускладнюють розуміння концепту «державна інформаційна політика» у сучасній політичній науці.

На сьогодні існують два основних підходи до тлумачення інформаційної політики: вузький та широкий. У вузькому підході державну інформаційну політику розглядають як «сукупність напрямів та методів, що використовуються державою для отримання, використання, поширення та збереження інформації». Проте таке обмеження значно скорочує її зміст та область застосування в науці державного управління [7, с. 78]. Ураховуючи важливість інформаційних технологій у всіх сферах життя сучасного суспільства, ми вважаємо за доцільне перейти від управління інформаційною безпекою до більш широкого управління інформаційною політикою, детально визначивши її пріоритети і принципи діяльності.

За вузьким підходом до інформаційної політики, вона розглядається як метод управління інформаційними потоками і ресурсами, який здійснюють інституціоналізовані суб’єкти управління, такі як держава, державні органи та організації. Для них інформація виконує виключно технічну функцію і розглядається як один із багатьох ресурсів. У такому розумінні, інформаційна політика зводиться до контролю за рухом інформаційних потоків і їх розподілом для досягнення запланованого ефекту [27, с. 16].

Прихильники широкого підходу розглядають інформаційну політику як складну та багатокомпонентну категорію в рамках науки державного управління. Згідно з їх поглядами, інформаційна політика визначає правила функціонування інформаційної сфери держави, зокрема, системи ЗМІ та взаємодії влади і суспільства. Крім того, вона повинна забезпечувати інформаційну безпеку держави. Додатково, державна інформаційна політика має сприяти взаємодії влади та суспільства через ЗМІ та громадські зв’язки, забезпечувати прозорість діяльності державних органів та публічного управління, а також захищати свободу слова та задовольняти інформаційні потреби громадян. Такий підхід ставить інформаційну політику на три рівні структури: держава, суспільство та індивідуальна особа [13, с. 54].

Державна інформаційна політика, за розумінням Олександра Юдіна та Володимира Богуша, орієнтується на створення умов для якісного та ефективного інформаційного забезпечення стратегічних та оперативних завдань соціального та економічного розвитку країни [70, с. 36]. За В. Карпенком, державна інформаційна політика спрямована на створення, збереження та розвиток об'єктів національного інформаційного простору для забезпечення безпеки та економічного розвитку України. Вона також має захищати національного виробника інформаційного продукту, сприяти впровадженню новітніх інформаційних технологій, розвивати інформаційну систему та інфраструктуру. Внутрішня інформаційна політика спрямована на задоволення інформаційних потреб суспільства, тоді як зовнішня інформаційна політика має на меті формування позитивного образу держави за кордоном, інформування світової громадськості про політичний, економічний, культурний та інвестиційний клімат в Україні, а також експорт українського продукту на світовий інформаційний ринок [23].

Олександр Соснін розглядає державну інформаційну політику як важливу складову державної політики інформатизації, яка сприяє формуванню інформаційного суспільства. Інформатизація є глобальним процесом, який впливає на економічний та соціальний розвиток, змінюючи характер і структуру світової діяльності. Проте державна інформаційна політика охоплює ширший спектр проблем, ніж лише інформатизація, і включає в себе регулювання інших аспектів інформаційного простору. Також важливо розуміти, що політика інформатизації є лише однією зі складових державної інформаційної політики [60, с. 213].

Отже, основними поняттями дослідження є інформація, війна, інформаційна війна, політика та інформаційна політика. Розуміння цих понять дає можливість більш глибоко дослідити тему інформаційної політики в умовах війни.

## 1.3. Методи та принципи дослідження інформаційної політики в умовах війни

Під час роботи над обраною темою нами були використані дві групи методів, а саме емпіричні та теоретичні. Серед емпіричних можна вказати на індукцію та дедукцію, які допомогли скласти висновки до кожного з підрозділів окремо та підсумувати результати дослідження. Також під час викладу основного матеріалу неодноразово використовувався метод аналізу, який мав на меті пошук необхідної інформації та відокремлення важливих фактів від загального масиву тексту. Використання методу синтезу було задіяно для того, щоб створити цільну доповідь з відомостей, що містяться у різних джерелах. Для систематизації інформації про, наприклад, поширювані росією наративи , ми звертались до методу класифікації. Ще один теоретичний метод – це узагальнення. Цей метод знадобився нам для формування висновків щодо ролі інформації у соціально-політичних та геополітичних процесах сучасності.

Нормативний підхід дозволяє розглянути інформаційну політику крізь призму законів, нормативних актів і доктринальних положень, що регулюють процеси створення, обробки, передавання, зберігання та використання інформації. Це розуміння інформаційної політики спрямовує нас на визначення методології системного підходу як основи нашого дослідження.

Основні аспекти системності в цій сфері включають:

– системність мислення, системність пізнання через збір та обробку інформації;

– системність результатів пізнання у структуруванні отриманої інформації;

– системність вивчення середовища політичної сфери;

– системність суспільства у взаємодії з системою політичної сфери;

– системність взаємодії людини з середовищем, що передбачає врахування всіх факторів, що впливають на зовнішнє середовище [73].

В. Бакуменко та С. Кравченко розглядають системний підхід у контексті дослідження державного управління як методологічний напрямок наукового пізнання та соціальної практики, що ґрунтується на аналізі об’єктів як систем. О. Богданов розробив базові принципи системного підходу, який охоплює не лише статичний аспект структур системи, а й вивчає їх динаміку, розвиток організаційної структури та значення зворотного зв’язку. Його підхід підкреслює важливість урахування власних цілей системи і визначає місце системного підходу як організаційної методологічної позиції у вивченні будь-якого управлінського явища, зокрема аналіз відносин між усіма складовими системи та її взаємодію з оточуючим середовищем [75]. Ці концепції розгортаються В. Волковою та О. Денисовим, що описують системний підхід як методологічний шлях пізнання [41, с. 12].

Згідно з Ю. Латигіним, системний підхід вплітається у структуру діалектики, де об’єкти розглядаються як цілісні системи. Загалом, системний підхід можна розглядати як метод мислення, що стосується державного управління та інформаційної політики [75]. В. Попов розглядає системний підхід як методологію дослідження об’єктів систем, що складаються з зовнішнього середовища та внутрішньої структури. Він вважає державну інформаційну політику системою, що містить взаємопов’язані елементи, які забезпечують вплив суб’єкта управління на об’єкт управління. Ця політика розглядається як система, що інтегрується в управлінські практики та взаємодіє з зовнішнім середовищем. Такий підхід дозволяє розглядати державну інформаційну політику як складну систему, що взаємодіє не лише на внутрішньому рівні країни, а й у контексті міжнародних відносин, враховуючи вплив інших державних інформаційних політик.

Для вивчення інформаційної політики важливим є системний аналіз, що представляє собою комплекс методів та інструментів для розробки ефективних управлінських рішень. Він виник як відповідь на потребу дослідження та моделювання складних соціальних систем. Інструменти системного аналізу дозволяють вирішувати різноманітні завдання в дослідженні державної інформаційної політики, такі як вивчення взаємодії з зовнішнім середовищем, розроблення альтернативних моделей розвитку, побудова імітаційних моделей, розробка моделей прийняття рішень, а також прогнозування та планування розвитку системи [71].

У контексті сфери державного управління, використання системного аналізу передбачає:

– визначення компонентів системних об’єктів;

– аналіз якісних і кількісних параметрів цих компонентів;

– опис структури, взаємозв’язків та способів внутрішньої і зовнішньої взаємодії.

Використання системного підходу у дослідженні інформаційної політики дозволить детально описати її характеристики, такі як склад, структура, організація, функціонування, взаємодія з навколишнім середовищем та розвиток [59, с. 12].

Таким чином, аналіз феноменологічного аспекту інформаційної політики дозволяє наблизитися до розуміння оптимальних методів взаємодії між державними та приватними інституціями, політики в сфері інформації та процесу пізнання. Це випливає з того, що основною метою державної інформаційної політики є сприяння переходу до нового етапу розвитку країни, формування інформаційного суспільства та інтеграція в систему світового інформаційного простору з урахуванням національних інформаційних інтересів.

Підвищення значення методології змішаного типу у дослідженні політичної сфери, сприяє розгляду різноманітних підходів та концепцій. Використання системного підходу в аналізі державної інформаційної політики акцентує увагу на її структурі та завданнях.

Отже, використання як теоретичних так і емпіричних методів допомогає нам досліджувати сутність основних понять, усвідомити їх взаємозв’язок, всебічно розглянути складові частини формування та реалізації інформаційної політики в умовах війни та розкрити основну суть досліджуваної проблеми.

Проведений аналіз наукових джерел підтверджує, що в галузі політичної науки існує група дослідників, які досліджують аспекти інформаційної політики у сфері управління інформаційними ресурсами. Вони розглядають основні напрямки та характеристики цієї політики. Це вимагає подальшого розвитку у рамках визначених цілей та завдань, з урахуванням методологічних принципів. Крім того, необхідність вивчення особливостей та тенденцій розвитку інформаційної політики у цій сфері, а також урахування світового досвіду свідчать про важливість та актуальність дослідження цієї проблематики в Україні. Тим паче спираючись на вже, на жаль, багаторічний досвід перебування України в умовах інформаційної війни з росією вказує на необхідність розвивати саме цю складову державної діяльності по забезпеченню інформаційної, а відтак і національної безпеки.

Різні дослідники розуміють термін «інформаційна політика» по-різному: одні вважають його сукупністю державної політики, яка стосується отримання, використання, поширення та зберігання інформації, або як заходи з захисту від кіберзагроз; інші розглядають його як комплекс стратегічних завдань держави з метою переходу до інформаційного суспільства. Реалії сьогодення вказують на дуже широке коло як об’єктів так і суб’єктів інформаційної політики.

Серед дослідників існує розбіжність у визначенні основних завдань інформаційної політики держави. Проте в умовах інформаційної революції більшість з них погоджуються, що побудова інформаційного суспільства та забезпечення інформаційної безпеки є ключовими напрямами інформаційної політики.

Основними поняттями дослідження інформаційної політики України в умовах війни є інформація, війна, інформаційна війна, політика та інформаційна політика.

Основними методами дослідження нашої роботи є дедукція, індукція, аналіз, спостереження, порівняння та узагальнення.

Серед підходів ми використали системний, історичний, нормативний, та комунікативний.

# РОЗДІЛ 2

# ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ В УМОВАХ ВІЙНИ

## 2.1. Сутність інформаційної політики

Актуальність дослідження інформаційної політики пояснюється декількома причинами. Серед них можна виділити зростання ролі інформації як такої в сучасному суспільстві та її вплив на економічну, соціальну політичну та культурну складову існування держави. Також в умовах становлення інформаційного суспільства особлива роль відводиться саме інформації як провідній складовій існування такого суспільства. На фоні цифровізації суспільств різко підвищуються глобалізаційні процеси, посилюються міжнаціональні та міжкультурні зв’язки, а відтак і формується імідж держави. На основі існуючої інформації сама держава формує своє місце на міжнародній арені та комунікує з іншими акторами. Тому наразі є дуже важливим саме формування та реалізація інформаційної політики, яка могла б вигідно представити державу як на міжнародній арені так і всередині самої країни. Також сформувати необхідний рівень інформаційної безпеки, адже наразі інформація стала певним чином зброєю, якою слід навчитися правильно користуватись та використовувати задля безпеки держави.

Сучасні науковці в своїх дослідженнях різним чином трактують визначення поняття «державна інформаційна політика». Деякі дослідники, зокрема, посилаючись на Закон України «Про інформацію», визначають її як «сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації» [63]. В електронній версії Закону станом на жовтень 2023 року стаття 6 не містить визначення «державна інформаційна політика». Замість цього, стаття регулює гарантії права на інформацію, зокрема, її забезпечення, доступ і контроль за дотриманням законодавства. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, для запобігання розголошенню конфіденційної інформації або в інших випадках, коли це необхідно для захисту прав та інтересів інших осіб, а також для підтримання авторитету і неупередженості правосуддя [46].

Дослідники, що визначають поняття «державна інформаційна політика», звертаються до статті 3 того самого Закону. Однак, вона не надає чіткого визначення цього терміну, лише встановлює основні напрями державної інформаційної політики. Серед цих напрямків є:

– забезпечення доступу кожного до інформації;

– створення рівних можливостей у сфері створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації;

– створення умов для формування інформаційного суспільства в Україні;

– забезпечення відкритості та прозорості діяльності суб’єктів владних повноважень;

– розвиток інформаційних систем і мереж, електронного урядування;

– постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

– забезпечення інформаційної безпеки України;

– сприяння міжнародній співпраці в інформаційній сфері та включенню України до світового інформаційного простору [46].

Тому в контексті цих суперечностей варто звернути увагу на те, що у національному законодавстві розлоге визначення поняття «державна інформаційна політика» відсутнє, а більшість визначень цього поняття є авторськими тлумаченнями науковців, а не таким поняттям, що прописане в законодавстві. В сучасному науковому просторі дослідниками запропоновано низку розлогих понять, які розкривають сутність поняття «інформаційна політика».

Достатньо влучно, на нашу думку, розкриває поняття інформаційної політики дослідник О. Токар, який розглядає державну інформаційну політику як сукупність напрямів діяльності держави в сфері інформації, що базується на певних нормативних принципах і спрямована передусім на зміцнення інформаційної безпеки держави, суспільства та особи, маючи внутрішнє і зовнішнє спрямування [64]. Також важливо навести думку В. Негодченка, який визначає державну інформаційну політику як сукупність напрямів та заходів, спрямованих на отримання, використання, поширення та зберігання інформації, що передбачає вплив уповноважених суб’єктів, зокрема, відповідних органів державної влади, на об’єкт управління з метою досягнення потрібного результату [31].

Визначення державної інформаційної політики в законодавстві набуває важливого значення під час воєнного стану. У законодавстві про воєнний стан 2023 року визначено особливий правовий режим, який передбачає введення унікальних заходів для забезпечення національної безпеки. На жаль, цей закон не містить конкретного визначення державної інформаційної політики в умовах воєнного стану, але все ж він встановлює правила, які дозволяють державі регулювати діяльність з поширення інформації з метою забезпечення безпеки. Наприклад, стаття 8 цього закону надає право владі регулювати роботу постачальників електронних комунікаційних мереж та послуг, поліграфічних підприємств, видавництв, телерадіоорганізацій тощо з метою використання їх для військових потреб та роз’яснювальної роботи серед військ і населення. Таким чином, державна інформаційна політика у воєнний час стає основним інструментом для забезпечення безпеки і захисту інтересів держави [50].

Так, державна інформаційна політика стає дуже гнучкою у воєнний час, з важливим акцентом на забезпечення інформаційної та кібербезпеки. Українське законодавство передбачає спеціальний підхід до координації єдиної інформаційної політики під час дії воєнного стану, включаючи об’єднання телеканалів та інформаційних ресурсів на єдиній платформі для стратегічної комунікації. Після тривалого періоду війни, українські науковці вже здійснили перші кроки у розумінні та формулюванні поняття «державна інформаційна політика в умовах воєнного стану», що допомагає наблизитися до розуміння її сутності.

Інформаційна політика в умовах війни – це комплекс заходів, який здійснюється державою спільно з громадськими інститутами для регулювання інформаційних процесів, створення та розвитку інформаційного суспільства. Її головна мета – захист національних інтересів країни у сфері оборони, а також прав і інтересів людини, моральних цінностей та інформаційної безпеки [28].

В сучасних умовах інформація відіграє ключову роль у формуванні суспільних процесів, визначаючи напрямки розвитку держав та їх взаємодію на міжнародній арені. Інформаційна політика, як складова державної політики, спрямована на регулювання інформаційних потоків, забезпечення інформаційної безпеки та формування позитивного іміджу країни. Вона стає невід’ємною частиною національної безпеки, особливо в умовах глобалізації та зростання інформаційних загроз.

Інформаційна політика – це сукупність заходів і стратегій, що застосовуються державою для управління інформаційним простором, забезпечення права громадян на доступ до інформації, захисту національних інтересів та створення умов для розвитку інформаційного суспільства. Основні цілі інформаційної політики включають:

1. Забезпечення інформаційної безпеки: захист інформаційного простору від внутрішніх та зовнішніх загроз, включаючи кібератаки, дезінформацію та пропаганду. Як приклад можна навести деякі елементи російської пропаганди які покликані підірвати довіру до України з боку світової спільноти. Наративи які провадить росія наступні: «Україні – це агресор у сучасному протистоянні», «США руками України намагаються воювати з росією та знищити її».
2. Гарантування свободи слова: забезпечення права громадян на отримання та поширення інформації, підтримка свободи медіа та протидія цензурі. В рамках Ради національної безпеки та оборони існує Центр протидії дезінформації, який власне забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [67].
3. Формування позитивного іміджу країни: використання інформаційних ресурсів для створення та підтримки позитивного міжнародного іміджу, сприяння культурному обміну та дипломатії. Прикладом може слугувати кампанія Bravery яка була запущена в квітні 2022 року після повномасштабного вторгнення росії в Україну. Ця кампанія мала на меті повідомити світу про події в Україні, стійкість та сміливість українського народу та потребу в допомозі зокрема зброєю для захисту власного суверенітету та незалежності [57].
4. Підтримка розвитку інформаційного суспільства: стимулювання інновацій у сфері інформаційних технологій, розширення доступу до інтернету та забезпечення цифрової грамотності населення.

Інформаційна політика охоплює кілька ключових напрямків, які визначають її сутність та функціонування:

1. Правове регулювання інформаційної діяльності: створення законодавчої бази, що регламентує інформаційні відносини, права та обов’язки суб’єктів інформаційного простору. Це включає закони про захист персональних даних, свободу інформації, захист інтелектуальної власності тощо.

2. Інформаційна безпека: розробка та впровадження стратегій і технологій захисту інформаційних систем від несанкціонованого доступу, кібератак та інших форм інформаційного впливу. Це також включає моніторинг і аналіз інформаційних загроз, розвиток кібербезпекових структур та навчання фахівців.

3. Інформаційна підтримка державного управління: забезпечення ефективного функціонування державних органів за допомогою сучасних інформаційних технологій, автоматизація управлінських процесів та покращення взаємодії між державними структурами та громадянами.

4. Медіа політика: підтримка незалежних медіа, забезпечення плюралізму думок, боротьба з пропагандою та дезінформацією. Це також включає розвиток медіа грамотності серед населення та підтримку якісної журналістики.

5. Культурна та освітня політика: сприяння розвитку інформаційної культури та освіти, підтримка наукових досліджень у сфері інформаційних технологій, інтеграція інформаційних ресурсів у навчальні процеси та культурні заходи.

Інформаційна політика є невід’ємною частиною сучасної державної стратегії, спрямованої на захист національних інтересів, забезпечення інформаційної безпеки та підтримку розвитку інформаційного суспільства. В умовах швидкого розвитку технологій та зростання інформаційних загроз, ефективна інформаційна політика стає ключовим елементом стабільності та процвітання держави. Важливо, щоб вона була гнучкою, адаптивною та орієнтованою на довгострокові перспективи, враховуючи як внутрішні потреби, так і зовнішні виклики.

Отже, інформаційна політика є багатогранною складовою процесу існування держави, яка через свої функції формує інформаційне забезпечення вектору розвитку держави, пояснює процеси, які в ній відбуваються, та за потреби може мобілізувати населення задля забезпечення свого існування.

## 2.2. Інструменти та методи інформаційної боротьби в умовах конфлікту

Інформаційна боротьба стала невід’ємною частиною сучасних конфліктів, де інформація використовується як стратегічний ресурс для досягнення політичних, військових та економічних цілей. В умовах збройної агресії рф Україна зіштовхується зі значними викликами та загрозами, у тому числі в інформаційній сфері.

Розглянемо основні інструменти та методи інформаційної боротьби в умовах конфлікту, зокрема в умовах гібридної війни, де традиційні бойові дії поєднуються з інформаційними та психологічними операціями.

Основні інструменти інформаційної боротьби:

1. Мас-медіа: традиційні засоби масової інформації (телебачення, радіо, преса) використовуються для поширення офіційної інформації, пропаганди, а також для формування громадської думки. В умовах конфлікту мас-медіа можуть виступати як інструмент маніпуляції свідомістю населення, поширюючи односторонню або викривлену інформацію. Прикладом існування подібних мас-медіа може слугувати телемарафон «Єдині новини» який розпочав свою трансляцію з початку повномасштабного вторгнення росії в Україну і не припиняв мовлення ні на хвилину. Така «монополія» на донесення інформації до громадян якраз і спричинила спотворене бачення реальності в українців в умовах війни.

2. Інтернет та соціальні мережі: соціальні платформи (Facebook, Twitter, Instagram, Telegram) є потужними інструментами для поширення інформації швидко та на великі аудиторії. Вони використовуються для інформаційних атак, дезінформації, а також для мобілізації підтримки серед населення. Вищевказані платформи дуже стали в нагоді від початку війни, через те, що саме через різноманітні канали та чат-боти передавалась інформація українським захисникам про переміщення російських окупантів, які потім були знищені. Також на цих платформах почали існувати і продовжують реалізовуватись різноманітні фандрайзингові та краудфандингові проекти на допомогу Україні, загальних обсяг яких вже перевищив декілька мільярдів доларів.

3. Кібероперації: включають атаки на інформаційні системи, сайти урядових та приватних організацій з метою отримання даних, порушення роботи критичної інфраструктури, а також для поширення шкідливого програмного забезпечення. Кібероперації часто супроводжуються інформаційними кампаніями для посилення їхнього впливу. Українські хакери неодноразову зламували інтернет сайти різноманітних російських державних установ та отримували всю інформацію, яка знаходилась в тих реєстрах. До більш психологічних кібератак можна віднести злами російського кабельного мовлення та запуск в ефір гімну України [5].

4. Психологічні операції (PSYOP): Використовують методи психологічного впливу для деморалізації супротивника, зниження його бойового духу, а також для впливу на громадську думку. Ці операції включають поширення чуток, дезінформації та інших форм психологічного тиску.

До методів інформаційної боротьби в інформаційному просторі можна віднести наступні:

1. Пропаганда: використовується для поширення політично спрямованої інформації з метою впливу на громадську думку. Пропаганда може бути білою (правдивою), сірою (частково правдивою) та чорною (повністю неправдивою). Прикладом багаторічної пропагандистської діяльності можна віднести загалом практичну всю роботу російських федеральних каналів, які намагаються сплюндрувати образ України в очах світової спільноти використовуючи різноманітні абсолютно неправдиві наративи. Наприклад, «Україна разом із США порушує конвенції та застосовує хімічну зброю», «росія захищає "пригнічених" російськомовних», «росія прагне переговорів» [65].
2. Дезінформація: цілеспрямоване поширення неправдивої інформації для введення в оману супротивника або населення. Дезінформація може бути спрямована на підрив довіри до уряду, військових структур або інших важливих інституцій. Одним із найяскравіших прикладів такої дезінформації є меседжі російської пропаганди у перші години та дні повномасштабного вторгнення , серед них «президент Зеленський втік у Польщу», «Всі літаки і ППО України знищене», «українці радо будуть зустрічати російську армію».
3. Фейки: створення та поширення фальшивих новин, фотографій, відео з метою маніпуляції свідомістю людей. Фейки часто використовуються для розпалювання конфліктів, паніки та недовіри. Новий етап у фейковиробництві з’явився з технологією «deepfake», тобто коли зображення людини та її голос, а також міміка створюється нейромережами та може бути використано у злочинних цілях. Одним із свіжих прикладів діпфейку є так зване «звернення Залужного» після його звільнення, де колишній очільник Збройних Сил України закликав до збройного перевороту та зміни президента України військовим шляхом. Наразі нейромережі не є такими професійними та майстерними , щоб повністю зімітувати голос, міміку та зображення людини, проте тенденція, на жаль, невтішна для безпекової ситуації загалом і це кидає великий виклик передусім фахівцям з кібербезпеки [55].
4. Меметика: використання мемів для поширення ідеологічних меседжів. Меметика стала потужним інструментом в умовах інформаційної боротьби, оскільки меми легко поширюються та запам'ятовуються. Серед них можна виділити «Доброго вечора, ми з України», «рускій воєнний корабель, іди…» «нє хочу уєзжать із крима» та «а я сєйчас покажу откуда готовілось нападєніє».
5. Спрямовані атаки на лідерів думок: використання інформаційних кампаній для дискредитації лідерів думок, журналістів, політичних діячів, які мають вплив на громадську думку.
6. Інформаційні кампанії: комплекс заходів, спрямованих на досягнення стратегічних цілей. Кампанії можуть включати серію повідомлень, статей, виступів, спрямованих на формування певної думки або поведінки серед населення.

Інформаційна боротьба в умовах конфлікту створює низку викликів для держав, зокрема необхідність захисту інформаційного простору, забезпечення кібербезпеки, а також протидії пропаганді та дезінформації. Основними стратегіями протидії є:

* підвищення інформаційної грамотності населення: освіта громадян щодо методів розпізнавання фейків, критичного мислення та аналізу джерел інформації;
* розвиток кібербезпеки: впровадження сучасних технологій захисту інформаційних систем, проведення регулярних кібернавчань та створення спеціалізованих підрозділів для протидії кіберзагрозам;
* сприяння свободі слова та незалежній журналістиці: підтримка незалежних медіа, забезпечення прозорості та доступу до правдивої інформації;
* міжнародне співробітництво: співпраця з міжнародними організаціями, обмін досвідом та інформацією щодо методів протидії інформаційним загрозам.

Інформаційна боротьба в умовах конфлікту є складним та багатогранним явищем, яке вимагає комплексного підходу до протидії. Використання сучасних інструментів та методів інформаційної боротьби дозволяє державам ефективно захищати свій інформаційний простір, а також формувати стійкість суспільства до інформаційних загроз.

Враховуючи необхідність захисту держави в умовах війни , зокрема її інформаційної складової Україна утворила кілька центральних органів державної виконавчої влади, які відповідають за впровадження державної інформаційної політики. Серед них [28]:

1. Державний комітет інформаційної політики, телебачення і радіомовлення України (Держкомінформ) здійснює керівництво у сферах інформації та видавництва, а також координує виконання державної політики в цих галузях. Він працює відповідно до законів та актів Президента і Кабінету Міністрів України, сприяючи вдосконаленню відповідного законодавства.

2. Державний комітет зв’язку та інформатизації України відповідає за регулювання сфери зв’язку та інформатизації, спрямовуючи свою діяльність на розвиток цих сфер та визначення стратегії та політики у цих напрямках.

3. Національна рада з питань телебачення та радіомовлення контролює видачу ліцензій для мовлення та встановлює правила для телевізійних і радіостанцій, виконуючи важливі функції у сфері регулювання телебачення та радіомовлення в Україні.

Всі ці органи співпрацюють з метою втілення державної інформаційної політики в Україні [56].

Концепція державної інформаційної політики України включає наступні секції [4, с. 154]: державна політика щодо засобів масової інформації; державна політика у сфері розвитку телерадіоінформаційної структури; державна політика щодо комп’ютерних технологій та систем телекомунікацій; державна політика у видавничій справі; державна політика в музейній справі; державна політика в архівній галузі; державна політика у бібліотечній справі; державна політика в кінематографії; державна політика щодо реклами як носія інформації; державна політика у сфері етнокультури як носія інформації; державна політика щодо інформаційної безпеки.

На нашу думку, деякі з розділів у Концепції потребують подальшого уточнення та поліпшення.

Основні принципи для розробки Концепції ґрунтуються на нормах Конституції та ряді законодавчих актів, включаючи закони про інформацію, засоби масової інформації, участь у міжнародному інформаційному обміні, зв’язок, інформаційне забезпечення органів державної влади, а також інші відповідні правові документи. Крім того, враховуються результати аналітичних та прогностичних досліджень щодо процесів інформатизації.

Формування адекватної інформатизації та загальної державної інформаційної політики суттєво впливає процес становлення та розвитку світового інформаційного співтовариства і перехід розвинених країн до постіндустріального (інформаційного) суспільства. Цей напрямок базується на найновіших досягненнях інформаційних та телекомунікаційних технологій, а також засобів зв’язку. Сучасні технології та інструменти обміну інформацією, включаючи Інтернет, розкривають нові можливості для міжнародного інформаційного обміну. Ці процеси концептуально та практично визначають формування світового інформаційного простору.

Загалом метою державної інформаційної політики є сприяння розвитку виробництва засобів інформатизації, телекомунікацій, інформаційних продуктів і послуг, одночасно забезпечуючи попит на них. Проте практична реалізація цієї політики потребує широкої публічної підтримки її основних принципів, пояснень щодо її соціальної важливості та обґрунтованості.

Отже, з огляду на розглянутий матеріал слід зазначити, що існує велика кількість інструментів та методів інформаційної боротьби в умовах конфлікту, які покликані нівелювати шкідливий вплив наративів країни-агресора, розкрити та пояснити реальний стан речей, та за потреби реалізувати контрпропаганду задля захисту національної інформаційної безпеки.

## 2.3. Виклики та загрози в інформаційній сфері в умовах війни

Інформаційна сфера часто розглядається як допоміжний інструмент для обслуговування корпоративних інтересів держави, а засоби масової інформації, незалежно від статусу, розглядаються як посередники між державою і громадянським суспільством, не враховуючи їхньої власної інформаційної влади.

Сьогодні відбувається формування нової інформаційної реальності через глобальну інформаційну інфраструктуру. Лідери держав прагнуть створити інформаційне суспільство та досягти інформаційного господарства, що створює нові виклики. Однією з найважливіших проблем є сфера інформаційної безпеки та інформаційних війн, спровокованих глобальними змінами [2].

Інформаційні війни включають не лише заборонені методи поширення, але й використання неправдивої інформації для маніпуляції свідомістю. Вони стали важливою частиною ідеологічної боротьби [24].

Суть війни змінилася: інформаційна перевага тепер важливіша, ніж будь-коли. Інформаційна війна охоплює не лише військову, а й політичну та інші сфери, вимагаючи нового підходу до регулювання відносин між суспільними групами та державами [54, с. 62].

Ідеологія інформаційної політики під час війни має ґрунтуватися на сучасних концепціях державної інформаційної політики. Це система ідей, цілей, методів і засобів, через які держава регулює відносини між громадянським суспільством та інформаційною системою, впливаючи на суспільні процеси [24].

Засоби масової інформації мають задовольняти потреби особистості в доступі до необхідної інформації, сприяючи її участі в суспільних змінах. Держава повинна створити нормативно-правову базу для регулювання інформаційної політики, забезпечуючи доступ до інформації та захист державних інтересів від зловживань через законодавче регулювання [11, с. 138].

З теоретичної точки зору, інформаційна політика – це використання ресурсів державної влади для ефективного вирішення ключових завдань розвитку інформаційної сфери. Вона охоплює організацію створення, поширення та зберігання інформації в соціальних системах, що реагують на внутрішні та зовнішні інформаційні потоки. Управління та контроль цих процесів є важливим завданням для всіх суспільств [66, с. 8].

Державна інформаційна політика під час війни відіграє ключову роль у розвитку суспільства. Основні завдання включають створення єдиного інформаційного простору України, інтеграцію у світовий інформаційний простір та гарантування інформаційної безпеки особистості, суспільства і держави. Сучасна інформаційна політика є інструментом забезпечення безпеки на всіх рівнях [11, с. 136].

У багатьох країнах та міжнародних об'єднаннях є структури, відповідальні за інформаційну діяльність. Вищі посадові особи беруть участь у формуванні та реалізації інтересів у сфері національної та міжнародної безпеки. Це характерно як для авторитарних, так і для демократичних держав.

Інформаційна політика є важливим інструментом для вирішення національних і міжнародних завдань під час війни. Вона забезпечує баланс інтересів суспільства, доступ до об’єктивної інформації та безпеку під час бойових дій. Державне управління суспільними процесами неможливе без інформаційних потоків, що відображають соціальні потреби. Ефективність взаємодії між державою та ЗМІ залежить від політичної ситуації та специфіки взаємодії громадянського суспільства і влади [16, с. 59].

У демократичній системі засоби масової інформації стають автономними і важливими для зворотного зв’язку в політичних процесах. Інформаційне середовище саморегулюється, і завданням демократичної держави є обмеження фінансового та політичного тиску на ЗМІ. Відносини між ЗМІ та державою відображають характер суспільних відносин та політичну ситуацію [17].

Інформаційна політика в умовах війни – це система заходів держави та громадянського суспільства для регулювання інформаційних процесів, розвитку інформаційного суспільства з пріоритетом національних інтересів у сфері оборони, захисту прав людини, моральних цінностей і забезпечення інформаційної безпеки особистості, суспільства і держави [17].

Стійкість соціальної системи залежить від узгодженості дій державних органів та медіа, що забезпечує прямий зв’язок між громадянським суспільством і державою. Воєнна ситуація та агресивна інформаційна політика агресора спрямовані на створення враження нестабільності та погіршення економічної ситуації, активізуючи деструктивні політико-ідеологічні чинники. Це загрожує національним цінностям, руйнує структури соціалізації особистості та створює загрозу для безпеки життя людини, суспільства і держави [17].

Сьогодні зростає загроза від застосування інформаційних методів стратегічними противниками та глобальними терористичними організаціями. Це включає не лише окремі військово-політичні операції, але й розвиток їхнього стратегічного потенціалу загалом. Захист від таких загроз стає важливим завданням для Збройних Сил та їхнього особового складу, який стає головною мішенню для методів гібридної війни.

Захист інформаційних ресурсів визнається пріоритетним завданням, що вимагає від фахівців з безпеки ефективного управління інформаційними потоками для захисту держави. Важливо ідентифікувати та класифікувати загрози за їхнім походженням, впливом та ступенем небезпеки. Ці загрози можуть бути як внутрішні, так і зовнішні, а іноді в одному явищі можна виявити обидві ці категорії [35, с. 20].

Інформаційна безпека військових формувань набуває великого значення через загрозу негативного впливу на моральний стан військ, що може призвести до зниження їх бойового духу та готовності до дій. Важливо також запобігти спрямованому впливу на особовий склад шляхом фальсифікації інформації, що може призвести до підвищення соціальної напруги та спроб втягнути їх у політичні конфлікти. Для цього ведеться психолого-просвітницька робота з особовим складом, а також співпраця з місцевими владами з метою запобігання провокаційній діяльності засобів масової інформації та інших джерел інформаційних атак [35, с. 22].

Інколи вплив на військовослужбовців може вийти за межі психологічного тиску, що може призвести до психологічних розладів, що сприяють вчиненню військових злочинів або дезертирству. Крім того, це може призвести до формування у військах груп, спрямованих на свідомий підрив обороноздатності країни.

Технічні загрози інформаційного характеру можуть впливати на функціонування інформаційних систем, які використовуються військами, а також на збереження конфіденційної інформації, що передається через військові зв’язки. Ці загрози можуть включати навмисне пошкодження систем, крадіжку інформації та недбалість окремих співробітників. Для захисту передбачені заходи, такі як підвищення рівня безпеки автоматизованих систем управління і навчання персоналу відповідно до вимог захисту інформації. Однак зволікання з впровадженням нових програмно-технічних засобів може стати загрозою для загальної безпеки [36].

Технічні загрози можуть включати навмисне пошкодження техніки та комунікаційних ліній через недбалість особового складу або дії противника. Для прикладу порушення систем життєзабезпечення військових кораблів, викликане необачністю або спеціальними атаками, може мати трагічні наслідки для екіпажу. Контроль за збереженням військової техніки стає найважливішим завданням для військовослужбовців. Ризик атак на інформаційні системи повітряних сил або ядерних об’єктів, а також введення неправдивої інформації в системи виявлення можливих атак, може створити серйозні загрози. Необхідно вживати заходів для запобігання цим загрозам та забезпечення інформаційної безпеки військових частин.

На сьогоднішній день законодавча база, яка має регулювати захист інформації та боротьбу з новими загрозами в інформаційному просторі, є недостатньою розвиненою. Багато аспектів цих явищ і їх можливі наслідки ще не враховані в нормативних актах, що ускладнює введення заходів щодо відповідальності за дії або організацію діяльності, які можуть шкодити інформаційній безпеці Збройних Сил та їх військовослужбовців. Проте ситуація поступово змінюється за рахунок прийняття нормативно-правових актів, які регулюють використання військової техніки та інших технологій, особливо іноземного походження [37].

Зовнішні загрози включають різноманітні форми інформаційно-психологічного впливу, які розробляються та використовуються противниками.

Нові форми інформаційної зброї можуть спрямовуватися на паралізацію інформаційних систем або вплив на психологічний стан військовослужбовців. Використання ультразвуку, електромагнітних полів та інших технологій для маніпулювання поведінкою стає все більш реальною загрозою. Також можливе використання медичних та хімічних засобів для впливу на військовослужбовців, особливо в регіонах, де тривають конфлікти [68, с. 313].

Боротьба з новими інформаційними загрозами постійно еволюціонує, і вживаються відповідні правові та організаційні заходи для забезпечення інформаційної безпеки Збройних Сил.

Планування та здійснення цілеспрямованого інформаційного впливу на військовослужбовців вимагає попередньої підготовки та навичок ідентифікації загроз. Однією з найбільш серйозних проблем безпеки є використання соціальних мереж, через які важлива інформація може випадково стати доступною широкому колу осіб. Головне завдання – вчасно виявляти такі загрози та припиняти їх дію.

Заходи для забезпечення безпеки можна розділити на дві групи. Перша група включає захист інформаційних систем від пошкоджень, запобігання витоку та перехопленню інформації, захист об’єктів військової дислокації та комп’ютерної техніки, забезпечення безпеки інформації, що становить державну або військову таємницю, радіоелектронний захист і використання захищених моделей комп’ютерів і програмного забезпечення, а також захист систем зв’язку. Друга група заходів передбачає запобігання цілеспрямованому інформаційно-психологічному впливу на психіку військовослужбовців та корекцію інформації, що транслюється потенційними супротивниками, включаючи проведення досліджень методів впливу на психіку та використання психологічної роботи з військовослужбовцями [69, с. 25].

Для ефективної реалізації цих заходів необхідно створити спеціалізовані підрозділи та використовувати нові наукові розробки та програмне забезпечення. Ця робота передбачає комплексний підхід і співпрацю різних спеціалізованих служб та аналітичних центрів.

В умовах сучасної війни, інформаційна сфера стає однією з ключових арен протистояння. Інформаційні війни, дезінформація, кібератаки, пропаганда – всі ці інструменти використовуються для маніпулювання свідомістю громадян, підриву морального духу населення та впливу на політичні процеси. Сучасні конфлікти демонструють, що ефективне управління інформаційним простором може бути вирішальним чинником у досягненні стратегічних цілей. Розглянемо основні виклики та загрози в інформаційній сфері в умовах війни:

1. Дезінформація та пропаганда. Дезінформація – це навмисне поширення неправдивої або викривленої інформації з метою введення в оману. Пропаганда спрямована на формування громадської думки та маніпуляцію свідомістю населення. В умовах війни ці інструменти використовуються для деморалізації супротивника, створення хаосу та паніки серед мирного населення, а також для підриву довіри до влади та військових сил. Приклади включають фальшиві новини, маніпулятивні соціальні медіа кампанії та використання ботів і тролів для поширення неправдивої інформації.

2. Кібератаки та інформаційні операції. Кібератаки на інфраструктуру, засоби масової інформації та соціальні мережі стають дедалі частішими. Метою таких атак є знищення або викрадення інформації, порушення роботи критичних систем, а також розповсюдження паніки серед населення. Інформаційні операції включають у себе не тільки хакерські атаки, але й більш витончені методи, такі як фішинг, соціальна інженерія та шкідливе програмне забезпечення.

3. Поляризація суспільства. Інформаційна війна сприяє загостренню соціальної поляризації. В умовах війни відбувається розкол суспільства за ідеологічними, політичними та етнічними ознаками. Цей процес підживлюється інформаційними кампаніями, що створюють ілюзію значного розриву між різними групами населення. Така поляризація може призвести до внутрішніх конфліктів і послаблення державної цілісності.

4. Психологічний тиск і моральна деморалізація. Психологічні операції спрямовані на зниження морального духу як військових, так і цивільного населення. Це досягається через постійний інформаційний тиск, поширення страху та безнадії, а також через підрив довіри до власних сил та керівництва. В результаті, навіть найсильніші армії та нації можуть стати вразливими до психологічного впливу.

5. Інформаційні бар’єри та цензура. В умовах війни держава може вдаватися до інформаційної цензури та обмеження доступу до певних ресурсів з метою захисту національної безпеки. Це створює виклики для вільного обміну інформацією та може призвести до обмеження громадянських свобод. Проте, в умовах активних бойових дій, такі заходи можуть бути виправданими для запобігання поширенню дезінформації та підтримки морального духу населення.

6. Міжнародний інформаційний контекст. Сучасні конфлікти мають глобальний вимір, і інформаційна війна виходить далеко за межі національних кордонів. Інформація про конфлікт поширюється по всьому світу, формуючи міжнародну громадську думку та впливаючи на рішення світових лідерів. Відтак, держава повинна не тільки захищати свій внутрішній інформаційний простір, але й активно працювати на міжнародній арені для формування сприятливого інформаційного контексту.

В умовах війни інформаційна сфера стає критично важливою для досягнення військових та політичних цілей. Держава повинна бути готова до нових викликів та загроз, розробляти ефективні стратегії протидії дезінформації, кібератакам та психологічному тиску. Водночас, важливо зберігати баланс між національною безпекою та свободою інформації, забезпечуючи доступ громадян до правдивих та об’єктивних даних. Тільки комплексний підхід до інформаційної безпеки дозволить ефективно протистояти сучасним викликам та загрозам в умовах війни.

Отже, як ми бачимо на ряду з бойовими діями реалізується інформаційна боротьба. Загалом інформаційна підтримка необхідна для пояснення потреби у цих бойових діях. Адже, як відомо, вбиває людина, а не зброя. Війна починається задовго до першого вибуху, вона починається з інформаційної підготовки населення, актуалізації потреби в бойових діях та розповсюдження ненависті до іншого народу, щоб виправдовувати свої криваві рішення.

Інформаційна політика України в умовах війни спрямована на захист інформаційного простору та підвищення інформаційної безпеки. Вона включає в себе стратегічне планування, розробку та впровадження заходів з контролю, моніторингу та реагування на інформаційні загрози.

Україна використовує різноманітні інструменти для інформаційної боротьби, включаючи медіа, соціальні мережі, психологічні впливи, кіберзаходи та дипломатичні канали. Методи включають розкриття дезінформації, аналіз загроз та розробку стратегій протидії.

Умови війни створюють серйозні виклики для інформаційної сфери, такі як дезінформація, маніпуляція, кібератаки, терористичні загрози та втручання в політичні процеси. Ці загрози вимагають комплексного підходу та ефективної координації зусиль для захисту національної інформаційної безпеки.

# РОЗДІЛ 3

# ПРАКСЕОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВІЙНИ

## 3.1. Сучасний стан реалізації інформаційної політики України в умовах війни

У демократичній політичній системі засоби масової інформації набувають автономності і стають важливим елементом системи зворотного зв’язку у складних політичних умовах. Забезпечення умов для незалежності ЗМІ від фінансового або політичного тиску стає завданням демократичної держави. Взаємодія держави та ЗМІ відображає характер суспільних відносин та політичну обстановку в суспільстві.

Інформаційна політика в умовах конфлікту – це комплекс заходів, які здійснюються державою спільно з громадськими організаціями для регулювання інформаційних процесів та формування інформаційного суспільства. Її мета полягає в захисті прав і інтересів громадян, моральних цінностей та інформаційної безпеки держави, зокрема в сфері оборони [54, с.61].

Стабільність соціальної системи визначається узгодженістю між діями владних структур та медіа, що забезпечує ефективний зв’язок між громадськістю та державою. Військові конфлікти та агресивна інформаційна кампанія спрямовані на формування переконання у нестабільності та погіршенні економічної ситуації, активізацію деструктивних політичних та ідеологічних факторів. Це загрожує національним цінностям, ідеалам, традиціям та структурам соціалізації, а також створює небезпеку для безпеки особистості, суспільства та держави.

До ключових нормативно-правових актів, що регулюють державну інформаційну політику, належать такі: Закон України «Про доступ до публічної інформації», який стосується оприлюднення та поширення інформації в Інтернеті, прав користувачів на доступ до неї і таке інше [45]; Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи захисту інтересів громадян, суспільства та держави у кіберпросторі [49]; Закон України «Про боротьбу з тероризмом», який обмежує поширення інформації, що має на меті пропаганду або виправдання тероризму [43]. Нормативно-правові акти, що встановлюють принципи державної інформаційної політики, включають:

1. Закон України «Про доступ до публічної інформації», який регулює розповсюдження та доступ до інформації в Інтернеті і права користувачів на доступ до неї [45];

2. Закон України «Про основні засади забезпечення кібербезпеки», що визначає правові та організаційні аспекти захисту інтересів у кіберпросторі [49];

3. Закон України «Про боротьбу з тероризмом», який регулює обмеження поширення інформації, зокрема, заборону пропаганди тероризму та висловлювання осіб, що закликають до опору антитерористичним операціям [43];

Ці закони встановлюють основні принципи та правила для державної інформаційної політики, що стосуються доступу до інформації, кібербезпеки та обмежень у поширенні інформації в ключових сферах.

Законодавчі акти, що регулюють державну інформаційну політику в умовах війни, включають:

1. Указ Президента України про введення воєнного стану, який встановлює правовий режим воєнного стану [44].

2. Указ Президента України щодо реалізації єдиної інформаційної політики в умовах воєнного стану, який визначає пріоритетну роль цієї політики в національній безпеці та об’єднання телеканалів для забезпечення єдиної інформаційної платформи [51].

3. Наказ Головнокомандувача Збройних Сил України про організацію взаємодії з представниками ЗМІ на час дії воєнного стану, включає в себе правила роботи журналістів у районах ведення бойових дій [48].

Алгоритм роботи представників ЗМІ в умовах воєнного стану обмежує розголошення стратегічних даних про дії Збройних Сил України та інших військових об’єктів. Також встановлені правила для журналістів у цей період, щоб уникнути розголошення інформації, яка може загрожувати національній безпеці.

Закон України «Про медіа» від 13 грудня 2022 року №2849-IX є важним кроком у формуванні організаційно-правових засад державної інформаційної політики в умовах війни [47]. Цей закон спрямований на забезпечення права на свободу висловлювання думок, доступу до різноманітної, достовірної та оперативної інформації, а також захисту національних інтересів України та прав користувачів медіасервісів. Він регулює діяльність у сфері медіа на основі принципів прозорості, справедливості та неупередженості.

Україна прийняла «Доктрину інформаційної безпеки» з метою забезпечення інформаційної безпеки в країні, яка стала актуальною особливо в умовах війни [48]. Рішення Ради національної безпеки і оборони України щодо реалізації єдиної інформаційної політики в умовах воєнного стану визначає цю реалізацію як пріоритетне завдання національної безпеки. Також в Україні був створений Центр протидії дезінформації при Раді національної безпеки і оборони України, де можна отримати актуальну інформацію та події в цій сфері [47].

З ініціативи введення воєнного стану в Україні було внесено зміни до законодавства, спрямовані на врахування потреб у воєнному часі. Ці зміни стосуються регулювання різних аспектів інформаційної діяльності, включаючи обмеження поширення конкретних типів інформації через її потенційно небезпечний вплив на суспільство, встановлення процедур технічного запису інформації під час воєнного стану, збільшення відповідальності за розповсюдження певних видів інформації, а також вдосконалення процедур здобуття інформації. Наприклад, був ухвалений закон, що збільшує кримінальну відповідальність за незаконне фото- та відеофіксацію руху Збройних Сил та міжнародної військової допомоги під час воєнного стану.

Додатково, зміни до Кримінально-процесуального кодексу спрощують проведення слідчих дій та надають слідчим можливість фіксувати комп’ютерні дані на місці обшуку навіть без зазначення цього у дозволі. Також збільшено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції [39].

Нормативно-правове регулювання державної інформаційної політики в умовах війни включає такі законодавчі акти: Указ Президента України від 24 лютого 2022 року №64/2022 «Про введення воєнного стану в Україні» [44], Указ Президента України «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [51]. Згідно з цими документами, реалізація єдиної інформаційної політики стає пріоритетним завданням національної безпеки. Відповідно до цього, Рада національної безпеки і оборони України вирішила об’єднати усі загальнонаціональні телеканали на єдиній інформаційній платформі, а саме – цілодобовому інформаційному марафоні «Єдині новини #UАразом» [51]. Крім того, наказом Головнокомандувача Збройних Сил України від 03 березня 2022 року №73 «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» затверджено Алгоритм роботи з акредитованими представниками засобів масової інформації під час дії правового режиму воєнного стану [48].

Закон України «Про медіа» від 13 грудня 2022 року №2849-IX визначає права та обов’язки у сфері медіа з метою захисту свободи вираження поглядів, доступу до об’єктивної інформації та забезпечення плюралізму думок. Згідно з цим законом, забороняється поширення недостовірних матеріалів, які можуть спричинити ворожнечу або закликати до насильницьких дій проти конституційного ладу чи територіальної цілісності України. Такі дії вважаються порушенням інформаційного законодавства [47].

Сьогодні законодавство не врегульовує журналістське розслідування, що стає проблемою, особливо в контексті війни та інформаційного протистояння [62]. Журналістське розслідування – це аналітичний жанр, який має на меті виявлення суспільних проблем та прихованих причин за ними. У процесі розслідування використовуються різні стилі та прийоми, спрямовані на створення образу події та залучення уваги громадськості [10, с. 4]. Головним принципом у роботі журналіста, який проводить розслідування, є створення відповідної атмосфери та формування громадської думки [34].

У воєнний час питання щодо публічного оприлюднення результатів журналістського розслідування та їх обговорення може бути обтяжливим. Це може спричинити конфлікт інтересів між державними органами та засобами масової інформації, що потенційно може викликати деструктивний вплив на соціалізацію особистості та психологічний стан суспільства. Такі ситуації можуть підірвати цілісність громадянського суспільства та держави.

Необхідність збалансування інтересів вимагає розгляду питання про регулювання журналістських розслідувань на рівні підзаконного акту, спеціально розробленого для періоду воєнного стану. У демократичному суспільстві заборонити такі розслідування неможливо, однак в умовах військового конфлікту потрібно чітко визначити правила їх проведення та оприлюднення результатів. Отримана інформація повинна розглядатися як вказівка, яка потребує перевірки компетентними правоохоронними органами. Рішення про можливість та обсяг оприлюднення даних повинно прийматися відповідними органами з урахуванням інтересів суспільства, держави та прав громадян у часи війни.

Додатковий нормативний акт може доповнити Указ Президента України про єдину інформаційну політику в умовах воєнного стану таким чином: інформація, яка отримана в результаті журналістського розслідування і стосується національної безпеки, оборони, територіальної цілісності та суверенітету України, може бути опублікована лише після перевірки відповідними владними органами та їхнього дозволу, з урахуванням принципів свободи медіа, інтересів національної безпеки та інших важливих аспектів, таких як громадський порядок та охорона здоров'я населення.

Україна переживає тривале реформування своєї соціально-політичної системи, що ставить перед політиками, науковцями та державними діячами завдання ефективної державної інформаційної політики. Ця політика є ключовим інструментом регулювання взаємодії між державою, громадянським суспільством та медіа. Вона залежить від рівня політичної культури, свідомості суспільства та адекватності політичної ідеології. Російсько-українська війна прискорила ці процеси, змушуючи розвивати державну інформаційну політику в кризових умовах. Вона включає комплекс заходів, спрямованих на дотримання принципів свободи медіа та забезпечення балансу інтересів суспільства та держави під час відбиття збройної агресії.

Підвищення достовірності та ефективного використання інформаційних ресурсів у військовий період допомагає удосконалити управлінські рішення, зміцнити стійкість політичної та військової системи та забезпечити стабільність у соціально-політичному розвитку в умовах кризи. Це сприяє успішній обороні України на полі бою.

Інформаційна політика є важливим інструментом державного управління, особливо в умовах війни, коли питання національної безпеки та захисту державного суверенітету виходять на перший план. Україна, зіштовхнувшись із російською агресією, змушена адаптувати свою інформаційну політику для забезпечення ефективної комунікації як всередині країни, так і на міжнародній арені. Розглянемо сучасний стан реалізації інформаційної політики України в умовах війни, її основні напрями та виклики.

Розглянемо основні напрями інформаційної політики України в умовах війни:

1. Протидія дезінформації та пропаганді. Російська агресія супроводжується масштабною інформаційною війною, яка включає розповсюдження фейкових новин, дезінформації та пропаганди. Для протидії цим загрозам Україна активно співпрацює з міжнародними партнерами, запроваджує санкції проти медіаресурсів, що поширюють дезінформацію, та розвиває власні платформи для перевірки фактів.
2. Підтримка національної єдності. Інформаційна політика спрямована на зміцнення національної єдності та підтримку морального духу населення. Це включає розробку і поширення патріотичних матеріалів, висвітлення героїчних дій українських військових та волонтерів, а також наголошення на важливості єдності у протистоянні агресору.
3. Міжнародна комунікація. Україна активно інформує міжнародну спільноту про події на фронті та наслідки російської агресії, залучаючи до цього дипломатичні канали, міжнародні організації та медіа. Це сприяє формуванню позитивного іміджу України на міжнародній арені та мобілізації міжнародної підтримки.
4. Розвиток цифрових комунікацій. З розвитком технологій цифрові платформи стали ключовим інструментом у реалізації інформаційної політики. Використання соціальних мереж, офіційних вебсайтів та мобільних додатків дозволяє швидко поширювати інформацію, реагувати на дезінформацію та підтримувати зв’язок із громадянами.

Виклики в реалізації інформаційної політики України в умовах війни наступні:

1. Інформаційні атаки. Росія систематично проводить інформаційні атаки, спрямовані на дестабілізацію ситуації в Україні, розкол суспільства та підрив довіри до державних інституцій. Протидія цим атакам вимагає значних ресурсів та координації зусиль різних державних та недержавних структур.

2. Обмеженість ресурсів. В умовах війни Україна стикається з обмеженістю фінансових та людських ресурсів для реалізації ефективної інформаційної політики. Це вимагає оптимізації витрат та залучення міжнародної допомоги.

3. Внутрішні розбіжності. Внутрішньополітичні розбіжності та відсутність єдиної стратегії можуть ускладнювати реалізацію інформаційної політики. Важливо забезпечити координацію дій між різними гілками влади та суспільними інститутами.

4. Швидка адаптація до змін. Інформаційне середовище швидко змінюється, що вимагає оперативної адаптації стратегій та підходів. Це включає як технологічні інновації, так і нові методи комунікації та реагування на виклики.

5. Перспективи розвитку. Україна продовжує розвивати свою інформаційну політику, впроваджуючи нові технології та методики для протидії дезінформації та підтримки національної єдності. Важливу роль у цьому процесі відіграє міжнародна співпраця, яка дозволяє залучити додаткові ресурси та досвід.

В умовах війни інформаційна політика стає не лише засобом комунікації, але й важливим інструментом захисту національних інтересів. Подальший розвиток цієї сфери залежатиме від здатності України оперативно реагувати на нові виклики, залучати сучасні технології та забезпечувати ефективну координацію між усіма учасниками інформаційного процесу.

Таким чином, реалізація інформаційної політики України в умовах війни є ключовим елементом у забезпеченні національної безпеки та суверенітету держави. В Україні формується як і нормативно-правова база і безпосередньо реалізується сама інформаційна політика покликана на захист держави в умовах війни. На жаль, не завжди вона є ефективною, проте вона розвивається та намагається гідно протистояти викликам сьогодення.

## 3.2. Міжнародний досвід реалізації інформаційної політики в умовах військових конфліктів

Сучасні нормативні документи, такі як Доктрина інформаційної безпеки та Стратегічний оборонний бюлетень, визнають значення співпраці з міжнародними цивільними і військовими організаціями для підвищення обороноздатності та зміцнення національної безпеки, зокрема інформаційної [40].

Вивчення зарубіжних моделей інформаційної безпеки, зокрема досвіду Сполучених Штатів Америки (США), є важливим для українських фахівців у процесі оптимізації системи державного управління в цій сфері. США відомі своїм передовим досвідом у цьому напрямку, будучи першою державою, яка впровадила електронне урядування та систему захисту національного інформаційного суверенітету та безпеки [74].

У Сполучених Штатах Америки (США) існують різні державні інституції, що відповідають за забезпечення інформаційної безпеки. Вони включають Агентство національної безпеки (АНБ), Національне управління кібербезпеки при Міністерстві внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР) та Центральне розвідувальне управління (ЦРУ). АНБ активно співпрацює з приватним сектором і науковими установами для боротьби з загрозами у неурядових комп’ютерних мережах, зокрема, захищаючи приватні телекомунікаційні, електричні та банківські мережі та беручи участь у антитерористичних заходах разом з приватними та громадськими організаціями [42].

У США понад 150 державних організацій та численні приватні структури забезпечують інформаційну безпеку, координуючись з АНБ. Основне регулювання інформаційної безпеки здійснює Президент США.

Організаційно-правові засади інформаційної безпеки в США виникли після Другої світової війни для захисту інформаційних та оборонних систем від радянської пропаганди. Ця основа включає федеральні та штатові закони, що забезпечують загальне розуміння важливості інформаційної безпеки для кожного громадянина [52, с. 76].

Правова основа інформаційної безпеки в США включає федеральні закони, такі як «Про охорону особистих таємниць» (1974), «Про таємницю» (1974), «Про висвітлення діяльності уряду», «Про право на фінансову таємницю» (1978), «Про доступ до інформації про діяльність ЦРУ» (1984), «Про безпеку комп’ютерних систем» (1987), «Про комп'ютерне шахрайство та зловживання» (1986) та інші. Важливими є також президентські директиви, що визначають політику інформаційної безпеки, наприклад, PD/NSC-24 (1977) і SDD-145 (1984), які встановлюють національну політику захисту систем зв’язку та автоматизованих інформаційних систем [52, с. 89].

У 1990-х роках, з активізацією та глобалізацією інформаційних відносин, у США прийняли федеральні закони «Про інформаційну безпеку» та «Про удосконалення інформаційної безпеки» (1997) [25]. Зростання ролі інформаційних технологій у військовій сфері збільшило військовий вплив на інформаційну безпеку.

У 1992 році Міністерство оборони США запровадило Директиву «Інформаційна війна», яка визначала політику захисту інформаційних ресурсів. Директива охоплювала аспекти, такі як психологічний вплив на супротивника, оперативна безпека, електронне втручання, інформаційна розвідка та захист.

У США значна увага приділяється управлінню інформаційними ресурсами для забезпечення власної інформаційної безпеки та впливу на системи інформаційної безпеки потенційних супротивників. Це дозволяє вести інформаційні війни, включаючи активні інформаційно-психологічні операції як інструмент зовнішньої політики, що може напружити військові відносини і вплинути на збереження мирних відносин з іншими країнами [52, с. 70].

З 2001 року, після заяви президента Джорджа Буша про важливість інформаційної безпеки як пріоритету національної безпеки, у США були запроваджені федеральні програми для захисту національного інформаційного середовища в комп’ютерних мережах. Метою цих програм було створення умов для розвідувальних органів збору та обробки інформації щодо загроз від інших країн та осіб, що призвело до розвитку нормативно-правової бази для протидії кіберзлочинності.

У 2003 році була введена Національна стратегія безпечного кіберпростору, а згодом ухвалені різні законодавчі акти і директиви з кібербезпеки. Особливу увагу приділяють співпраці між державними установами у сфері кібербезпеки та розробці стандартів електронної аутентифікації [52, с. 74].

У 2009 році в Конгресі був представлений законопроект «Акт про кібербезпеку» (The Cybersecurity Act of 2009), що надавав президентові США повноваження обмежувати доступ до Інтернету в разі загрози національній безпеці. Цей закон підкреслив ключову роль президента в управлінні кібербезпекою та захисті інформаційних проектів на федеральному, регіональному та місцевому рівнях.

Під час президентства Барака Обами цифрову інфраструктуру США було визнано «стратегічною національною цінністю», а її захист став національним пріоритетом. Ця концепція, заснована на ідеї Маршалла Макклюена про ключову роль обміну знаннями та інформацією, підкреслила, що боротьба за доступ до інформаційних ресурсів стає головною проблемою національної безпеки.

Президент США визначив основні завдання в інформаційній сфері, такі як постійне вдосконалення стратегії забезпечення безпеки мереж і комунікацій, розробка систем попередження та реагування на кібератаки, збільшення співпраці між державою та приватним сектором у кібербезпеці, приваблення інвестицій у новітні технології та підвищення громадської свідомості про необхідність боротьби з кіберзагрозами.

У 2010 році була впроваджена «Ініціатива зі всебічної національної кібербезпеки», яка передбачала створення загальнофедеральної мережі захищених зв’язків та спеціальних підрозділів кіберконтррозвідки для виявлення та запобігання загрозам інформаційним мережам країни. Також була розроблена система управління ризиками для прогнозування можливих наслідків несанкціонованого втручання в інформаційні мережі державних установ. Крім того, була запроваджена програма «Ейнштейн» для виявлення втручань у державні інформаційні мережі.

З початку 2012 року хакерські атаки в США розглядаються як форма збройної агресії, що вимагає відповідного реагування. Щоб захистити себе від цих загроз, значна частина фінансування науково-дослідних проектів в країні спрямовується на розробку систем захисту інформації [42].

Канада, подібно до своїх сусідів у США, активно працює над регулюванням та забезпеченням інформаційної безпеки, впроваджуючи комплексну політику в цій сфері. У країні держава відіграє ключову роль у керуванні інформаційними потоками та забезпеченні безпеки інформації. Важливо зауважити, що у порівнянні з іншими країнами участь громадянського суспільства в цих процесах у Канаді досить обмежена, оскільки громадяни високо довіряють державі [52, с. 90].

Сьогодні політика регулювання інформаційної безпеки в Канаді вважається багатьма країнами і міжнародними організаціями прикладом позитивного підходу. Інформаційна безпека стала важливою складовою розвитку інформаційного суспільства в Канаді. Ключовим моментом стало прийняття «Канадських критеріїв безпеки комп’ютерних систем» у 1993 році, що сприяло створенню єдиної шкали критеріїв безпеки для порівняння різних систем обробки інформації.

Канада відзначається в галузі інформаційної безпеки завдяки створенню «Інформаційної магістралі», що є стратегічним документом, регламентуючим адміністративно-правові та технічні заходи для забезпечення автентичності інформації у мережах. Крім того, слід зазначити роль Консультативної Ради з інформаційної магістралі, яка активно сприяє удосконаленню нормативної бази інформаційної безпеки в країні [52, с. 92].

Головним об’єктом захисту в системі інформаційної безпеки Канади є електронний уряд, який забезпечує доступ громадян до публічних послуг та сприяє їхній рівності.

У 1997 році Канада ухвалила федеральні закони, які гарантували позитивний доступ до Інтернету та збереження конфіденційності в онлайн просторі. Ці закони стали основною правовою підставою для захисту користувачів мережі, зокрема, щодо забезпечення конфіденційності їхніх персональних даних.

У 2001 році у Канаді було засновано Групу інформаційних операцій Канадських збройних сил в Міністерстві оборони. Цей підрозділ був створений з метою розробки канадської стратегії інформаційного протиборства для забезпечення національної інформаційної безпеки.

У 2005 році Канада утворила Центр по кіберінцидентам, який діє при уряді країни. Цей центр координує боротьбу з кіберзлочинами та моніторить загрози для критичної інфраструктури. Він також надає технічні консультації з безпеки інформаційних технологій і сприяє підвищенню рівня інформаційної грамотності серед населення.

У 2010 році Канада запровадила Канадську стратегію кібербезпеки, яка охоплює широкий спектр заходів для захисту урядових інформаційних систем, забезпечення безпеки громадян у онлайн-середовищі, обміну інформацією між федеральними органами, укладення міжнародних угод та захисту приватного сектора від кіберзагроз. Країна продовжує активно розвивати свої організаційно-правові та технічні засоби для забезпечення інформаційної безпеки.

У Європі історія забезпечення інформаційної безпеки налічує декілька століть. Вже у XVIII столітті відбулися перші кроки у цьому напрямку. Наприклад, 2 грудня 1766 року король Швеції видав Милостивий указ про свободу письма і друку, який регламентував поняття відкритої та таємної інформації, визначаючи їхню роль в інтересах держави [21].

Федеративна Республіка Німеччина володіє значним досвідом у сфері забезпечення інформаційної безпеки. У цій країні дотримання принципу конфіденційності інформації особи має високий ступінь важливості в адміністративно-правовому порядку. Зокрема, починаючи з 1977 року, діє Закон ФРН «Про захист персональних даних», що регулює використання таких даних у федеральних і земельних органах влади, ЗМІ та приватному секторі, а також встановлює процедури автоматизованої обробки цієї інформації [70, с. 322].

У 1997 році в Федеративній Республіці Німеччина був ухвалений Закон «Про основи надання інформаційних та комунікаційних послуг», що визначає адміністративно-правові принципи захисту інформації у сфері інформаційних та телекомунікаційних мереж. Відповідно до цього закону, збір, обробка та використання інформації можливі лише за наявності відповідних законодавчих норм або згоди користувача.

Крім того, інформація може бути збирана, оброблятися та використовуватися окремо для різних послуг, і користувач не може бути примушений надавати згоду на отримання послуг. Інформація також може бути оброблена в обсязі, необхідному для виконання угоди, якщо це передбачено угодою [70, с. 317].

У Німеччині Федеральне управління з інформаційної безпеки, зі штаб-квартирою у Бонні, відповідає за забезпечення інформаційної безпеки на федеральному рівні та співпрацює з Федеральною розвідувальною службою. Це управління було засноване в 2009 році відповідно до Закону ФРН «Про посилення безпеки інформаційних систем». Далі, у 2011 році була ухвалена федеральна Стратегія забезпечення кібернетичної безпеки Німеччини, яка визначає основні напрямки заходів у галузі захисту від кібернетичних загроз [70, с. 320].

Стратегія визначає кіберпростір як віртуальний простір, що включає інформаційні мережі, такі як Інтернет, та є відкритим для підключення інших мереж передачі даних. Для покращення співпраці та координації заходів у галузі захисту інформації було утворено Національний центр кіберзахисту, який діє під керівництвом федерального Міністерства внутрішніх справ.

Згідно зі стратегією, планується створення Національної ради кібербезпеки, яка буде відповідальна за розроблення стратегічних основ державної політики з інформаційної безпеки та боротьби з кіберзагрозами.

Федеральна розвідувальна служба відповідає за забезпечення кібербезпеки державних інформаційних ресурсів та здійснює дії для запобігання, припинення та ліквідації наслідків кібернетичних загроз.

Федеральне управління має підрозділ «BSI», який взаємодіє з приватними ІТ-компаніями та комерційними користувачами, щоб узгоджувати заходи з інформаційної безпеки та надавати консультації з питань інформаційних технологій.

У Франції система державного регулювання інформаційної безпеки має схожі риси з моделлю, що існує у Німеччині. Основний акцент робиться на захисті кібернетичної безпеки та конфіденційності даних у Інтернеті. Французька правова система не має спеціальних законів, що регулювали б діяльність фахівців з захисту різних видів інформації. Безпека державної таємниці забезпечується за допомогою кримінального законодавства, а захист персональних даних і комерційних таємниць – за допомогою кримінального, трудового і цивільного законодавства [52, с. 55].

Французька модель інформаційної безпеки наголошує на готовності до ведення інформаційних війн як у цивільній, так і військовій сферах. У військовому аспекті це передбачає обмежену роль інформаційних операцій, переважно в контексті конфліктів невеликої інтенсивності або миротворчих операцій. У цивільній сфері використовуються широкі адміністративні інформаційні заходи для запобігання втручанню в бази даних державних установ, підприємств і організацій, а також для захисту персональних даних. Франція також активно досліджує конфлікти в економічній сфері з точки зору інформаційної безпеки та розробляє стратегії для протидії інформаційним загрозам у цьому секторі.

У Франції боротьба з інформаційними загрозами, як правило, здійснюється на місцях через регіональні поліцейські управління, кожне з яких має спеціальний відділ для боротьби зі злочинами в сфері інформаційних технологій. У цьому підході важлива участь фахівців з різних галузей, таких як фінанси, право, аудит і т. д. Це обумовлено зростанням електронної комерції у країні. Цей комплексний підхід призвів до позитивних результатів, зокрема, у запобіганні шахрайству з банківськими картками [40].

Важливу роль у Франції відіграє Центр електроніки і озброєнь (CELAR), який займається різноманітними аспектами, включаючи електронну війну, телекомунікації, інформаційну безпеку та інформаційні системи.

Огляд регулювання інформаційної безпеки в іноземних країнах допомагає вирішити важливі завдання у галузі науки та практики. Це надає нові можливості вітчизняним експертам для розробки та вдосконалення практичних інструментів для управління інформаційною безпекою. Крім того, вони можуть використовувати наявний емпіричний досвід для створення та впровадження нових нормативних актів у цій сфері [40].

Розглянуті вище приклади забезпечення існування та реалізації інформаційної політики, зокрема її безпеки вказують на її важливість для інформаційного суспільства. В епоху повальної діджиталізації питання безпеки інформації постає чи не найпершому місці через важливість існування безпечних комунікацій та інтеракцій як між глобальними гравцями так і всередині будь-якої держави. Досвід інших держав є важливим для України, яка наразі тільки формує сталі та ефективні механізми з захисту інформаційної політики. На противагу цьому Україна є безпосереднім автором створення різноманітних методів, засобів та способів захисту інформаційної політики «в полі » позаяк вона, Україна, знаходиться у стані війни.

Отже, це дозволяє створювати нові структури для забезпечення інформаційної безпеки та удосконалювати законодавчу базу для сектору безпеки та оборони в Україні.

## 3.3. Рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах війни

Державна інформаційна політика має сприяти створенню єдиного інформаційного простору України, її інтеграції у світовий інформаційний простір та гарантуванню безпеки інформації для особистості, суспільства й держави. Ця політика виступає ключовим інструментом у забезпеченні безпеки індивіда, соціуму, держави і світової спільноти [9].

Важливими аспектами інформаційної політики у воєнний час є забезпечення балансу між інтересами суспільства, здобуття об’єктивної та своєчасної інформації і дотримання вимог щодо збереження конфіденційності під час активних воєнних дій. Це включає в себе вирішення завдань, пов’язаних із захистом від агресії ворожих сил за допомогою різноманітних військових та мілітаризованих формувань.

Інформаційна політика в умовах війни – це система заходів, що проводяться державою та громадськими організаціями для регулювання інформаційних процесів та розвитку інформаційного суспільства. Її головна мета – захист прав індивідуумів, моральних цінностей та національних інтересів у сфері оборони та інформаційної безпеки [1, с. 19].

Стійкість соціальної системи залежить від гармонії між органами влади та медіа, що забезпечує взаємодію між громадянами та державою. Війна та агресивна інформаційна кампанія агресора спрямовані на поширення переконання про нестабільність та загрозу для соціально-економічного благополуччя. Вони активізують деструктивні ідеологічні чинники, що підірвують національні цінності та створюють загрозу для безпеки людей, суспільства та держави.

Закон України «Про медіа» прийнятий для забезпечення свободи слова та доступу до достовірної інформації, а також для захисту національних інтересів. Він визначає правовий статус та функції Національної ради України з питань телебачення і радіомовлення. Закон забороняє поширення інформації, що неправдиво представляє збройну агресію проти України та дії держави-агресора, яка може призвести до порушення конституційного ладу чи територіальної цілісності [47].

Порушення законодавства про медіа можуть включати неправдиву інформацію, невиконання журналістських стандартів, обмеження свободи преси, використання необ’єктивних джерел, розсекречування конфіденційної інформації, політичний тиск на медіа, створення матеріалів, що загрожують громадському порядку або національній безпеці, та зловживання рекламою.

Визначення порушень може варіюватися залежно від конкретного законодавства та правил, що діють у кожній країні. Громадські та професійні організації часто грають роль у визначенні та нагляді за дотриманням етичних та законодавчих стандартів у медіаіндустрії.

У воєнний час виникає потреба у єдиній інформаційній стратегії. Президент України підписав Указ №152/2022, який стосується введення в дію рішення Ради національної безпеки і оборони України щодо реалізації єдиної інформаційної політики під час воєнного стану.

Ураховуючи пряму військову агресію Російської Федерації та активне поширення дезінформації, Рада національної безпеки і оборони України прийняла рішення про встановлення єдиної інформаційної політики під час дії в Україні воєнного стану. Це визначається як пріоритетне питання національної безпеки, що забезпечується шляхом об’єднання загальнонаціональних телеканалів на єдиній інформаційній платформі під назвою «Єдині новини #UАразом» [51].

Удосконалення інформаційної політики України під час воєнних дій потребує всебічного та гнучкого підходу. Пропонуємо наступні практичні рекомендації для досягнення цієї мети:

1. Необхідно переглянути систему спеціального зв’язку та підвищити кваліфікацію персоналу в сфері інформаційної та кібербезпеки для ефективного керування інформаційними заходами та комунікаційною стратегією під час воєнних конфліктів. Основні напрями включають криптографічний захист, технічний захист, авторизацію безпеки, аналітику вразливостей та тестування систем захисту інформації.

2. Співпраця з демократичними країнами для зміцнення кібербезпеки та критичної інфраструктури є важливою. Це включає такі кроки, як обмін досвідом та партнерство у виявленні та протидії кіберзагрозам, проведення спільних тренувань, створення систем обміну інформацією, розвиток міжнародних стандартів та протоколів, захист критичних об'єктів та навчання персоналу. Важливо також проводити інформаційні кампанії для свідомого громадянства, підготовку кадрів у сфері кібербезпеки та удосконалення механізмів реагування на кібератаки.

3. Розбудова Центру протидії дезінформації включає створення ефективної системи моніторингу та реагування на дезінформацію, розвиток фактчекінгових ініціатив для перевірки правдивості інформації, використання спеціалізованих інструментів для виявлення поширення дезінформації та проведення інформаційних кампаній щодо роз’яснення шкідливих наслідків дезінформації. Зокрема, до цього може включатися залучення громадськості та міжнародних експертів.

4. Міністерство цифрової трансформації України працює над підвищенням рівня цифрової грамотності громадян через оновлену Рамку цифрової компетентності. Це включає запуск освітніх кампаній та врахування новітніх технологій, таких як штучний інтелект, доповнена та віртуальна реальність, інтернет речей. Зокрема, оновлена версія Рамки враховує виклики, пов’язані з введенням воєнного стану, такі як збільшення кількості внутрішньо переміщених осіб та інформаційна війна. Розвиток цифрових технологій є важливим для зміцнення національної економіки та підвищення якості життя громадян.

5. Створення медіаорганізацій, таких як Hromadske TV, Texty.org.ua, Detector Media, Interfax-Ukraine і Ukrayinska Pravda, сприяє забезпеченню прозорості та незалежності в медіа. Ці організації відзначаються об’єктивністю та відкритістю власності та джерел фінансування. Наприклад, Hromadske TV та Ukrayinska Pravda активно прагнуть до фінансової прозорості та взаємодії з аудиторією, а Texty.org.ua спеціалізується на журналістських розслідуваннях. Interfax-Ukraine відоме своєю об’єктивністю та лідерством в інформаційному просторі.

6. Розвиток ефективної зовнішньої комунікації потребує стратегічного підходу та уваги до потреб різних груп зацікавлених сторін. Це означає розробку стратегій комунікацій для висвітлення ситуації в Україні та залучення підтримки міжнародної громадськості, забезпечення чіткості та зрозумілості усіх комунікаційних повідомлень, сприяння взаємодії з громадськістю та механізмів для отримання зворотного зв’язку, використання різних каналів зв’язку, відкритості та доступності інформації, а також підсилення позитивного бренду органів публічного управління. До цього також входить розробка плану реагування на кризові ситуації, визначення цільової аудиторії та організація заходів для взаємодії з громадськістю та ЗМІ. Гнучкість та здатність адаптуватися до змін є ключовими в комунікаційних стратегіях.

7. Створення кампаній проти дезінформації: проведення заходів для пояснення та висвітлення фактів з метою зменшення впливу дезінформації.

8. Розвиток медійної грамотності: запуск освітніх програм для усвідомлення громадянами роботи медіа та виявлення дезінформації. Використання найкращих практик, таких як американська Стратегічна освітня ініціатива та європейська рамка кваліфікацій, включаючи National initiative for cybersecurity education (NICE), Cyber security and infrastructure security agency (CISA), National initiative for cybersecurity careers and studies (NICCS), Federal Virtual Training Environment (FedVTE) та National Centers of Academic Excellence (CAE).

9. Забезпечення ефективної кібербезпеки для захисту інформаційної інфраструктури від кібератак включає проведення регулярних аудитів та оцінок ризиків для виявлення вразливостей, розробку та впровадження докладного плану кіберзахисту, вимагання складних паролів та використання двоетапної аутентифікації. Також важливі заходи, такі як встановлення програм антивірусного захисту, регулярне оновлення програмного забезпечення, застосування мережевих заходів безпеки та створення резервних копій даних. Співпраця з іншими організаціями та урядовими установами також є ключовим аспектом для обміну інформацією та взаємодопомоги в питаннях кібербезпеки.

10. Розвиток гібридної війни включає в себе комбінацію різних методів, таких як військові, політичні, економічні та інформаційні, для досягнення стратегічних цілей без прямого зіткнення. Це передбачає розробку стратегій, які використовують інформаційні, кібернетичні та психологічні інструменти, а також застосування різноманітних методів, таких як дезінформація, комп’ютерні атаки, економічні санкції, дипломатичні тиски та втручання в політичні процеси. Гібридна війна вимагає комплексного підходу та адаптивних стратегій для ефективного протидії у постійно змінному середовищі.

11. Залучення громадськості включає активну участь у формуванні та виконанні інформаційної політики, сприяючи ініціативам та співпрацю з активістами та журналістами.

12. Міжнародна співпраця включає взаємодію з міжнародними партнерами для обміну досвідом та отримання підтримки у сфері інформаційної політики.

Отже, запропоновані рекомендації можуть допомогти українському уряду створити ефективну інформаційну політику, придатну для умов війни, що спрямована на захист інформаційного простору та підтримку громадян. Вони можуть також служити основою для подальшого вдосконалення стратегій інформаційної політики в умовах війни в Україні, включаючи заходи зі зміцнення внутрішньої та зовнішньої інформаційної безпеки, підвищення громадської свідомості та покращення комунікації.

Україна активно працює над зміцненням своєї інформаційної політики в умовах війни. Зусилля спрямовані на захист інформаційного простору від зовнішньої агресії, підвищення інформаційної безпеки та підтримку громадян у відсіюванні дезінформації.

Україна досліджує та адаптує кращі практики формування інформаційної політики зі світового досвіду. Вивчаються досвід країн, що також переживають воєнні конфлікти, а також успішні приклади захисту інформаційного простору.

Рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах війни:

1) проведення систематичних аналізів і підготовка стратегій з протидії інформаційній агресії;

2) підвищення рівня медійної грамотності населення;

3) розвиток механізмів контролю та виявлення дезінформації;

4) зміцнення співпраці з міжнародними партнерами у сфері інформаційної безпеки.

# 

# ВИСНОВКИ

У процесі дослідження особливостей інформаційної політики України в умовах війни було вирішено всі завдання, що вимагала реалізація поставленої мети роботи.

Так, з’ясовано стан наукового дослідження проблематики інформаційної політики в умовах війни. Також була визначена сутність інформаційної політики як процесу пояснення, цілепокладання та реалізації певного вектору розвитку держави, зокрема в процесі військового протистояння, де питання існування держави стоїть на першому місці. Нами був описаний сучасний стан реалізації інформаційної політики України в умовах війни. Тут слід зазначити, що сам процес цілепокладання та реалізації інформаційної політики існує на досить високому рівні, адже за майже два з половиною роки повномасшабного вторгнення та неймовірно великої кількості пропаганди з боку росії, Україні вдається гідно захищати свій народ, залучати допомогу з усього світу та проводити контрпропагандні заходи проти країни-окупанта. На жаль, все ще існують певні слабкі сторони інформаційної політики України, які мають під собою історичне, культурне або навіть управлінське підгрунтя.

Проведений аналіз наукових джерел підтверджує, що існує група дослідників, які розглядають аспекти державної політики у сфері управління інформаційними ресурсами. Вони розглядають основні напрямки та характеристики цієї політики. На жаль, недостатня розробленість цієї теми, необхідність вивчення особливостей та тенденцій розвитку державної політики у сфері інформаційної політики, а також урахування світового досвіду свідчать про важливість та актуальність дослідження цієї проблематики в Україні.

Різні дослідники розуміють термін «інформаційна політика» по-різному: одні вважають його сукупністю державної політики, яка стосується отримання, використання, поширення та зберігання інформації, або як заходи з захисту від кіберзагроз; інші розглядають його як комплекс стратегічних завдань держави з метою переходу до інформаційного суспільства. На мою думку, більшість цих визначень охоплюють лише певні аспекти інформаційної діяльності уряду.

Серед дослідників існує розбіжність у визначенні основних завдань інформаційної політики держави. Проте в умовах інформаційної революції більшість з них погоджуються, що побудова інформаційного суспільства та забезпечення інформаційної безпеки є ключовими напрямами інформаційної політики.

З вищесказаного можна зробити висновок, що одна з ключових характеристик інформаційної політики – узгодженість – є дуже слабкою, оскільки існують значні відмінності в розумінні її природи, цілей і завдань. Це значно підриває ефективність і результативність цієї політики та вимагає швидкої розробки і правового закріплення єдиної загальної концепції чи кодексу інформаційної політики в Україні.

Інформаційна політика України в умовах війни спрямована на захист інформаційного простору та підвищення інформаційної безпеки. Вона включає в себе стратегічне планування, розробку та впровадження заходів з контролю, моніторингу та реагування на інформаційні загрози.

Україна використовує різноманітні інструменти для інформаційної боротьби, включаючи медіа, соціальні мережі, психологічні впливи, кіберзаходи та дипломатичні канали. Методи включають розкриття дезінформації, аналіз загроз та розробку стратегій протидії.

Умови війни створюють серйозні виклики для інформаційної сфери, такі як дезінформація, маніпуляція, кібератаки, терористичні загрози та втручання в політичні процеси. Ці загрози вимагають комплексного підходу та ефективної координації зусиль для захисту національної інформаційної безпеки.

Україна активно працює над зміцненням своєї інформаційної політики в умовах війни. Зусилля спрямовані на захист інформаційного простору від зовнішньої агресії, підвищення інформаційної безпеки та підтримку громадян у відсіюванні дезінформації. Україна досліджує та адаптує кращі практики формування інформаційної політики зі світового досвіду. Вивчаються досвід країн, що також переживають воєнні конфлікти, а також успішні приклади захисту інформаційного простору.

Рекомендації щодо вдосконалення інформаційної політики України з метою протидії інформаційній агресії в умовах війни:

1) проведення систематичних аналізів і підготовка стратегій з протидії інформаційній агресії;

2) підвищення рівня медійної грамотності населення;

3) розвиток механізмів контролю та виявлення дезінформації;

4) зміцнення співпраці з міжнародними партнерами у сфері інформаційної безпеки.

Гіпотеза нашого дослідження підтвердилась лиш частково, позаяк державою був обраний правильний інформаційно-політичний дискурс, як основа для реалізації інформаційної політики, проте , очевидно, його не є достатньо. Враховуючи третій рік повномасштабної війни , цілком природньо, що питання виживання стоїть не так гостро для багатьох українців, як це було на початку війни. Тому перед державою з’являються нові питання як тримати питання обороноздатності на першому місці з-поміж інших та як проводити інформаційно-іміджеву політику на міжнародній арені задля залучення військової допомоги з інших країн.

# СПИСОК ЛІТЕРАТУРИ

1. Абрамов В.І. Гібридна війна як нова форма міждержавного протиборства: стратегія перемоги. *Виклики і загрози національній безпеці в умовах гібридної війни* : матеріали наук.-практ. семінару, м. Київ, 27 квіт. 2017 р. Київ, 2017. С. 17–22.
2. Арістова І. Державна інформаційна політика: організаційно-правові аспекти / за заг. ред. О.М. Бандурки. Харків : видавництво університету внутрішніх справ, 2000. 368 c. URL: https://salo.li/025a3c0 (дата звернення: 17.05.2024)
3. Банах С. Поняття та особливості інформації як теоретичної категорії. *Актуальні проблеми правознавства*. 2019. №4. C. 226–231. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/907?articlesBySimilarityPage=2 (дата звернення: 01.04.2024)
4. Башук А.І. Підходи до інформаційної політики у контексті переходу до інформаційного суспільства. *Наукові записки Інституту журналістики: науковий збірник*. Київ, 2010. Т.38. С. 152–157.
5. Бесараб Т. Українські хакери та ГУР зламали російські держпослуги та сайти міністерств – ЗМІ. *Informator.ua*. URL: https://informator.ua/uk/ukrajinski-hakeri-ta-gur-zlamali-rosiyski-derzhposlugi-ta-sayti-ministerstv-zmi (дата звернення: 06.06.2024)
6. Брижко В.М. До гносеології категорії «інформація». *Інформація і право*. 2011. №2(2). С. 13–20. DOI: https://doi.org/10.37750/2616-6798.2011.2(2).271511 (дата звернення: 11.04.2024)
7. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні. Київ : «Юстиніан», 2006. 176 с.
8. Війна. *Велика Українська Енциклопедія*. URL: https://vue.gov.ua/Війна (дата звернення: 06.06.2024)
9. Воронкова В.Г. Технології інформаційного менеджменту в державному управлінні. *Вісник Національного університету цивільного захисту України: збірник наукових праць*. Харків, 2021. №. 2(15). С. 70–79. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/14917/1/Zb%D1%96rnik%20NUCZU\_2021\_2\_15.pdf (дата звернення: 17.05.2024)
10. Глушко О.К. Журналістське розслідування: Історія, теорія, практика : навчальний посібник для студентів вищих навчальних закладів. Київ : Арістей, 2006. 144 с.
11. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ при Президентові України*. 2015. №1. С. 136–141.
12. Демський С.Е., Павлюк С. П. Правове регулювання інформаційної діяльності в Україні: станом на 1 січня 2001 року. Київ : Юрінком Інтер, 2001. 687 с.
13. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті : монографія. Київ : Генеза, 2004. 208 с.
14. Енциклопедична стаття. Інформація. *Енциклопедія сучасної України*. URL: https://esu.com.ua/article-12485 (дата звернення: 06.06.2024)
15. Заніздра Н.О. Державна інформаційна політика на сучасному етапі та шляхи вдосконалення. *Вісник КрНУ імені Михайла Остроградського*. 2012. №4(75). С. 193–196. URL: https://visnikkrnu.kdu.edu.ua/statti/2012-4-1(75)/193.pdf (дата звернення: 01.04.2024)
16. Захаренко К.В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. Київ : Український державний університет імені Михайла Драгоманова, 2021. 423 с.
17. Іванченко Ю.М. Сутність, головні напрями та способи державної інформаційної політики в Україні. *Державне управління: теорія і практика*. 2005. №2.
18. Інформаційна безпека : підручник / за заг. ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.
19. Інформаційна війна. *Велика Українська Енциклопедія*. URL: https://vue.gov.ua/Інформаційна\_війна (дата звернення: 06.06.2024)
20. Інформаційна політика. *Державне підприємство «Волинський науково-виробничий центр стандартизації, метрології та сертифікації»*. URL: http://volynstandart.com.ua/information-policy/ (дата звернення: 10.04.2024)
21. Історія доступу по-шведськи: королівський указ про свободу друку року 1766 року. *Доступ до правди*. URL: https://dostup.org.ua/stories/publications/istoriia-dostupu-po-shvedsky-korolivskyi-ukaz-pro-svobodu-druku-1766-roku (дата звернення: 15.05.2024)
22. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека : навчальний посібник. Харків : ХНЕУ, 2018. 196 с.
23. Карпенко В.О. Інформаційна політика та безпека : підручник. Київ : Нора-Друк, 2006. 320 с. URL: https://studfile.net/preview/10004788/ (дата звернення: 18.04.2024)
24. Кобільник Б.Ю., Гізун А.І. Роль інформаційно-психологічниx впливів у інформаційній війні. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали всеукр. наук-практ. конф., м. Кропивницький, 23-25 листопад. 2016 р. Кропивницький, 2016. С. 28–29. URL: https://core.ac.uk/download/pdf/84825493.pdf (дата звернення: 04.04.2024)
25. Конституція України : офіц. текст. Київ : ВАІТЕ, 2021. 324 с. URL: https://ccu.gov.ua/sites/default/files/commemorative\_constitution\_2021.pdf (дата звернення: 15.05.2024)
26. Лизанчук В.В. Інформаційна безпека України: теорія і практика : підручник. Львів : ЛНУ імені Івана Франка, 2017. 728 с. URL: https://journ.lnu.edu.ua/wp-content/uploads/2020/11/Lyzanchuk-Informatsiyna-bezpeka-Ukrainy-2017.pdf (дата звернення: 04.04.2024)
27. Макаренко Є.А. Європейська інформаційна політика : монографія. Київ : Наша культура і наука, 2000. 368 с.
28. Мирошниченко А.І. Щодо інформаційної політики в умовах воєнного стану. *Організаційно-правові аспекти публічного управління в Україні* : матеріали Х міжнар. наук-практ. інтернет-конф., м. Полтава, 27 квіт. 2023 р. Полтава, 2022. С. 37–39. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/14338/1/2.pdf (дата звернення: 21.04.2024)
29. Мохова Ю.Л., Луцька А.І. Сутність та головні напрямки державної інформаційної політики України. *Державне управління: удосконалення та розвиток*. 2018. №12. URL: http://www.dy.nayka.com.ua/pdf/12\_2018/27.pdf (дата звернення: 04.04.2024)
30. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с. URL: https://elibrary.kubg.edu.ua/id/eprint/18860/1/A\_Nashinets-Naumova\_monografia\_1\_FPMV.pdf (дата звернення: 17.05.2024)
31. Негодченко В. Основні напрями державної інформаційної політики в Україні. *Підприємництво, господарство і право*. 2016. №4. С.77–81. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/25b4c17b-1b45-47ea-abf6-5adcf2749ee9/content (дата звернення: 15.05.2024)
32. Нестеряк Ю.В. Державна інформаційна політика України: теоретико-методологічні засади : монографія. Київ : НАДУ, 2014. 592 с.
33. Нестеряк Ю.В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. *Вісник НАДУ*. 2013. № 3. С. 40–45.
34. Нікітіна Н. В. Специфіка журналістського розслідування: основи жанру й методу. *Електронна бібліотека* *Інституту журналістики*. URL: http://journlib.univ.kiev.ua/index.php/index.php?act=article&article=2326 (дата звернення: 15.05.2024)
35. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. №1. С. 17–23.
36. Новицький А. Щодо питання структуризації інформаційного права як наукової категорії. *Актуальні проблеми правознавства*. 2017. №4. С. 34–38. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/94?articlesBySimilarityPage=2 (дата звернення: 18.04.2024)
37. Олійник О. Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи*. 2012. №4(1). С. 65–68. URL: [http://nbuv.gov.ua/UJRN/evpe\_2012\_4%281%29\_\_13](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=evpe_2012_4%281%29__13) (дата звернення: 18.04.2024)
38. Олійник О.В. Державна політика інформаційної безпеки України. *Юридичний вісник*. 2012. №4(25). С.65–69.
39. Онищенко С.В., Глушко А.Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. *Соціальна економіка*. 2020. №59. C. 14–24. DOI: https://doi.org/10.26565/2524-2547-2020-59-02 (дата звернення: 18.04.2024)
40. Пєвцов Г.В., Гордієнко А.М., Залкін С.В., Сідченко С.О., Хударковський К.І. Досвід і концепції веденян інформаційної боротьби у провідних країнах світу. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. №1(18). С. 12–16. URL: http://nbuv.gov.ua/UJRN/Nitps\_2015\_1\_4 (дата звернення: 18.04.2024)
41. Пилипишин В.П. Поняття та основні риси державного управління. *Юридична наука і практика*. 2011. №2. С.10–14.
42. Пирожик О. Про необхідність використання Україною позитивного досвіду США з питань розбудови системи інформаційної безпеки. *Вісник Пенітенціарної асоціації України*. 2021. №2(16). С. 64–73. DOI: https://doi.org/10.34015/2523-4552.2021.2.07 (дата звернення: 11.04.2024)
43. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. №638-IV. Дата оновлення: 28.04.2023. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 10.05.2024)
44. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. №64/2022 URL: https://www.president. gov.ua/documents/642022-41397 (дата звернення: 10.05.2024)
45. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 08.10.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 14.04.2024)
46. Про інформацію : Закон України від 02.10.1992 р. №2657-XII. Дата оновлення: 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 14.04.2024)
47. Про медіа : Закон України від 13.12.2022 р. №2849-IX. Дата оновлення: 11.02.2024. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text/ (дата звернення: 14.04.2024)
48. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану : Наказ Головнокомандувача Збройних Сил України від 03.03.2022 р. №73. Дата оновлення: 03.02.2024. URL: https://ips.ligazakon.net/document/MUS36785 (дата звернення: 14.04.2024)
49. Про основні засади забезпечення кібербезпеки України : Закон України від 09.05.2018 р. №2163-VIII. Дата оновлення: 04.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19/#Text (дата звернення: 14.04.2024)
50. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. №389-VIII. Дата оновлення: 18.05.2024. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 14.04.2024)
51. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» : Указ Президента України від 19.03.2022 р. №152/2022. URL: https://www.president.gov.ua/documents/1522022-41761 (дата звернення: 14.04.2024)
52. Проценко Д., Тупчієнко Д. Огляд підходів до регулювання нових конвергентних аудіовізуальних засобів масової інформації: міжнародний досвід. Київ : Національний університет «Києво-Могилянська Академія», 2012. 108 с.
53. Публічна політика в системі управління суспільним життям. Система розробки та здійснення публічних політик в Україні / за заг. ред. О.П. Дем’янчука. Київ : Факт, 2004. С. 5–21.
54. Пунда О.О., Добрянська О.Д., Новицька Н.Б. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. *Екологічне право*. 2022. №1-2. С. 60–65.
55. Російські пропагандисти вигадали новий фейк про Залужного: деталі. *Слово і діло. Аналітичний портал*. URL: https://www.slovoidilo.ua/2024/02/03/novyna/suspilstvo/rosijski-propahandysty-vyhadaly-novyj-fejk-pro-zaluzhnoho-detali (дата звернення: 06.06.2024)
56. Рябоконь О. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2016. №43. С. 97–114. URL: http://nbuv.gov.ua/UJRN/npnbuimviv\_2016\_43\_9 (дата звернення: 18.05.2024)
57. Сміливість бути Україною. *Brave.ua*. URL: https://www.brave.ua (дата звернення: 06.06.2024)
58. Солодка, О. М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право*. 2020. №4(35). С. 39–46. DOI: https://doi.org/10.37750/2616-6798.2020.4(35).221216 (дата звернення: 11.05.2024)
59. Сорока К. О. Основи теорії систем і системного аналізу. Харків : ХНАМГ, 2004. 291 с.
60. Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України : монографія. Київ : Інститут держави і права ім. В.М. Корецького НАН України, 2003. 572 с.
61. Сурмін Ю.П., Надолішній П.І. Методологія як інструмент ефективної реалізації можливостей державного управління. *Енциклопедія державного управління* : у 8 т. Київ : НАДУ, 2011. Т. 2. С. 7–11.
62. Сущенко В.М. Журналістське розслідування правопорушень: загальна характеристика та поняття з точки зору правознавства. *Наукові записки НаУКМА*. 2011. Т. 116. С. 26–29. URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/2614/Sushchenko\_Zhurnalistske\_rozsliduvannia\_pravoporushen.pdf?sequence=1&isAllowed=y/ (дата звернення: 12.05.2024)
63. Терещенко В. Особливості державної інформаційної політики в умовах війни. *Юридичний науковий електронний журнал*. 2023. №2. С. 391–395. URL: http://www.lsej.org.ua/2\_2023/92.pdf (дата звернення: 27.05.2024)
64. Токар О. Державна інформаційна політика: проблеми визначення концепту. *Політичний менеджмент*. 2009. №5. С. 131–141. URL: http://nbuv.gov.ua/UJRN/PoMe\_2009\_5\_16 (дата звернення: 27.05.2024)
65. Топ абсурдних російських фейків про Україну за час повномасштабної війни. *Слово і діло. Аналітичний портал*. URL: https://www.slovoidilo.ua/2023/05/12/infografika/bezpeka/top-absurdnyx-rosijskyx-fejkiv-pro-ukrayinu-chas-povnomasshtabnoyi-vijny (дата звернення: 06.06.2024)
66. Фурашев В.М. Правові аспекти інформаційної безпеки. Київ : КПІ ім. Ігоря Сікорського, 2018. 67 с.
67. Центр протидії дезінформації. *Cpd.gov.ua*. URL: https://cpd.gov.ua (дата звернення: 06.06.2024)
68. Цимбалюк В. Інформаційне право (основи теорії і практики) : монографія. Київ : Освіта України, 2010. 388 с.
69. Цимбалюк В.С., Бабінська А.В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес*. 2014. №2(8). С. 22–30.
70. Юдін О.К, Богуш В.М. Інформаційна безпека. Нормативно-правове-забезпечення : підручник. Київ : Видавництво Національного авіаційного університету «НАУдрук», 2011. 640 с.
71. An Introductory Toolkit for Civil Servants. *Government Office for Science*. URL: https://www.gov.uk/government/publications/systems-thinking-for-civil-servants/toolkit (дата звернення: 12.04.2024)
72. Braman S. Change of State: Information, Policy, and Power. London : University of Cambridge, 2006. P. 313–330. DOI: https://doi.org/10.7551/mitpress/1783.001.0001(дата звернення: 02.06.2024)
73. Checkland P., Winter M. Process and content: two ways of using SSM. *Journal of the Operational Research Society*. 2006. №57(12). URL: https://www.researchgate.net/publication/31942282\_Process\_and\_content\_Two\_ways\_of\_using\_SSM (дата звернення: 02.06.2024)
74. National Cybersecurity Strategy. *The White House*. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 12.04.2024)
75. Ramakrishnan.T.K., Raimol Ravi K. Theories and Concepts of Public Administration : study material. Kerala : University of Calicut, 2019. 59 p. URL: https://sde.uoc.ac.in/sites/default/files/sde\_videos/POL1C04%20-%20Theories%20&%20Concepts.pdf (дата звернення: 11.05.2024)
76. Thomson G., Crowther S. Attuning to trustworthiness and final reflections. *Hermeneutic phenomenology in health and social care research*. Routledge, 2022. P. 213–227. URL: https://www.researchgate.net/publication/361631426\_Attuning\_to\_trustworthiness\_and\_final\_reflections (дата звернення: 11.05.2024)
77. Titchen A., Hobson D. Understanding phenomenology through reverse perspectives. *Theory and methods in social research*. London, 2011. №2. P. 121–128. URL: https://www.researchgate.net/publication/290392665\_Understanding\_phenomenology\_through\_reverse\_perspectives (дата звернення: 11.05.2024)
78. Vagle M.D. Crafting Phenomenological Research : a book. New York : Routledge, 2014. 171 p. DOI: https://doi.org/10.4324/9781315431451 (дата звернення: 11.05.2024)
79. Vorotin V.Ye., Romanenko Ye.A., Shchokin R.G., Pivovarov K.V. Improving the organizational and legal mechanism of state economic management: the European experience for Ukraine. *Financial and credit activity: problems of theory and practice*. 2018. №3(26). P. 368–376. URL: https://pdfs.semanticscholar.org/4b5c/559acca128826dc112b14012f1842970d929.pdf (дата звернення: 28.05.2024)
80. Webster’s new universal unabridged Dictionary. New-York : Barnes & Noble books, 1996. 2230 p.