**ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ**
**Факультет обліку та фінансів**
**Кафедра політології, історії і філософії**

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти
бакалавр

на тему: «Проблеми забезпечення інформаційної безпеки України»

Виконала: здобувачка вищої освіти
за освітньою програмою Політологія
спеціальності 052 Політологія
ступеня вищої освіти бакалавр
групи 052ПОЛІТбд_41
Пахомій О. М.
Керівник: Некряч О. М.
Рецензент: Перепелиця М. П.

**Полтава 2025 року**

**ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ**
**Факультет обліку та фінансів**
**Кафедра гуманітарних і соціальних дисциплін**

Освітня програма Політологія
Спеціальність 052 Політологія
Рівень вищої освіти бакалаврський

**ЗАТВЕРДЖУЮ**
**Завідувач кафедри**
_____ Наталія СИЗОНЕНКО
16 травня 2024 року

# З А В Д А Н Н Я
## НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
## Пахомій Олександри Михайлівни

1. Тема кваліфікаційної роботи: «Проблеми забезпечення інформаційної безпеки України»

керівник роботи: доктор політичних наук, професор, професор кафедри гуманітарних і соціальних дисциплін Некряч Анастасія Іванівна

Затверджено засіданням кафедри протокол № 20 від 21 травня 2024 р.

2. Строк подання здобувачем вищої освіти роботи 15 травня 2025 р.

3. Вихідні дані до роботи: інформаційні джерела та наукові дослідження відповідно до тематики кваліфікаційної роботи
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
Розділ 1. Теоретичні основи інформаційної безпеки.
Розділ 2. Аналіз сучасного стану інформаційної безпеки в Україні.
Розділ 3. Шляхи підвищення рівня інформаційної безпеки України.

5. Перелік графічного матеріалу: схеми, рисунки, графіки, діаграми за темою та об’єктом дослідження.

6. Дата видачі завдання: 16 травня 2024 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Вибір і затвердження теми роботи. | 02.04.2024 р. – 30.04.2024 р. | |
| 2 | Складання та погодження розгорнутого плану та завдання на кваліфікаційну роботу | 01.05.2024 р. – 15.05.2024 р. | |
| 3 | Опрацювання літературних джерел | 16.05.2024 р. – 30.06.2024 р. | |
| 4 | Збір, вивчення і обробка інформації, необхідної для виконання роботи | 16.05.2024 р. – 26.04.2025 р. | |
| 5 | Виконання теоретичних розділів роботи | 16.05.2024 р. – 20.03.2025 р. | |
| 6 | Виконання дослідницького розділу роботи | 01.02.2025 р. – 20.03.2025 р. | |
| 7 | Оформлення тексту роботи | 09.05.2025 р. – 16.05.2025 р. | |
| 8 | Попередній захист роботи на кафедрі | 16.05.2025 р. | |
| 9 | Доопрацювання роботи з урахуванням зауважень і пропозицій | 17.05.2025 р. – 26.05.2025 р. | |
| 10 | Нормо-контроль | 27.05.2025 р. – 28.05.2025 р. | |
| 11 | Захист кваліфікаційної роботи | 16.06.2025 р. – 18.06.2025 р. | |

Здобувач вищої освіти _____ Олександра ПАХОМІЙ
(підпис)

Керівник роботи _____ Анастасія НЕКРЯЧ
(підпис)

**ЗМІСТ**

# ВСТУП

**Актуальність теми.** В умовах сучасного геополітичного протистояння, інформація набуває стратегічного значення, трансформуючись у дієвий інструмент впливу. Її роль у врегулюванні конфліктів та подоланні суспільно-політичних криз є надзвичайно вагомою, особливо в контексті гібридних війн, де інформаційний компонент відіграє ключову роль.

Низький рівень медіаграмотності суспільства створює сприятливі умови для маніпуляцій громадською думкою, що ускладнює критичний аналіз інформації та прийняття обґрунтованих рішень. У такому контексті, формування ефективної державної політики інформаційної безпеки є нагальною необхідністю. Вона має включати такі складові:

- підвищення рівня інформаційної освіти, що забезпечує всебічний захист інформаційного простору та сприяє збалансованому розвитку інформаційного суспільства;

- створення умов для забезпечення інформаційних потреб громадян, незалежно від потенційних загроз;

- розвиток та використання інформаційного середовища для задоволення потреб суспільства;

- протидія інформаційним загрозам, як потенційним, так і реальним.

Отже, розробка та реалізація ефективної державної політики інформаційної безпеки є критично важливим завданням, особливо в умовах агресії, з якою стикається Україна. Інформаційна сфера є одним з ключових напрямків протистояння, що вимагає пильної уваги та системного підходу.

**Метою роботи** є вивчення способів, механізмів та інструментів інформаційної безпеки України.

Для досягнення поставленої мети поставлено **такі завдання:**

- розкрити поняття «інформаційна безпека», дослідивши його ключові аспекти;

- окреслити головні завдання, що стоять перед інформаційною безпекою;

- проаналізувати сучасний стан державної політики у сфері інформаційної безпеки;

- розкрити політичні засади, на яких формується державна політика у сфері інформаційної безпеки;

- проаналізувати форми забезпечення інформаційної безпеки Української держави в умовах війни;

- розкрити інформаційну війну та дезінформацію як основні загрози національній безпеці України;

- розкрити роль контрпропаганди як важливого інструменту в забезпеченні інформаційної безпеки України.

**Об'єктом дослідження** є процес формування інформаційної безпеки України.

**Предметом дослідження** є способи та механізми, за допомогою яких Україна впроваджує свою державну політику в галузі інформаційної безпеки.

**Огляд використаних джерел.** Питання, що розглядається, привернуло увагу широкого кола науковців та експертів, серед яких: П.Д. Біленчук, С.С. Білько, С.Л. Гнатюк, Ю.П. Горбань, О.П. Дзьобань, О.Д. Довгань, О.О. Золотар, О.І. Косілова, С.В. Кудін, В.А. Ліпкан, О.В. Логінов, Н.Б. Новицька, Т.Ю. Ткачук, О.О. Тихомиров, А.Й. Француз, В.С. Цимбалюк, А.Є. Шевченко, О.Г. Ярема та інші.

Особливості формування інформаційної політики в умовах збройного конфлікту були предметом дослідження О. Пунди, О. Добрянської та Н. Новицької. І. Залєвська та Г. Удренас у своїх працях висунули гіпотезу про те, що ефективне управління інформаційним простором з боку держави може значно підвищити її здатність до подолання кризових ситуацій.

**Методи дослідження** були визначені відповідно до мети, завдань, об'єкту та предмету дослідження: сукупність загальнофілософських, загальнонаукових (аналіз, синтез, індукція, дедукція, абстрагування та узагальнення) та емпіричних методів, що дозволив систематизувати та узагальнити отримані результати з різних аспектів дослідження.

Для аналізу нормативної бази та наукових джерел був використаний метод системного та структурного дослідження.

**Наукова новизна отриманих результатів.** У кваліфікаційній роботі запропоновано низку інструментів щодо зміцнення інформаційної безпеки в Україні.

**Практична значущість**. Дане дослідження має широкий спектр практичного застосування, включаючи науково-дослідницьку діяльність. Ці матеріали можуть бути використані у ході освітнього процесу, при підготовці проведення науково практичних процесів та інших політичних дискусійних форм.

**Структура та обсяг кваліфікаційної роботи.** Кваліфікаційна робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. Загальний обсяг: 60 сторінок, кількість джерел – 33.

# РОЗДІЛ 1.
# ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 1.1. Поняття інформаційної безпеки: сутність та складові

В епоху цифрової трансформації, коли інформаційні технології пронизують усі сфери суспільного життя, забезпечення інформаційної безпеки набуває критичного значення для національних інтересів. Формування стійкого та захищеного інформаційного простору є не просто бажаним, а необхідним елементом розвитку сучасної держави.

Інтенсивне впровадження інформаційних технологій у систему державного управління, хоч і підвищує ефективність, водночас відкриває нові вектори загроз. Ризики несанкціонованого доступу до критичної інфраструктури та витоку конфіденційної інформації зростають експоненціально, а потенційні наслідки таких інцидентів стають дедалі масштабнішими. У зв’язку з цим, питання захисту інформації виходить на перший план у стратегіях національної безпеки багатьох країн.

Держави, які не здатні забезпечити належний рівень інформаційної безпеки, ризикують втратити конкурентоспроможність на світовій арені. Історичний досвід свідчить, що неспроможність адаптуватися до змін в інформаційному просторі та забезпечити ефективне управління інформаційними потоками може призвести до втрати державного суверенітету [12].

Отже, формування комплексної системи інформаційної безпеки, закріпленої на законодавчому рівні, є нагальною потребою для будь-якої сучасної держави. Ця система повинна включати чітко визначені функції та повноваження державних органів, відповідальних за забезпечення інформаційної безпеки.

Інформаційна безпека – це складне, багатоаспектне явище, що балансує між забезпеченням вільного доступу громадян до інформації та необхідністю захисту державних таємниць, збереженням цілісності суспільства та протидією

деструктивним інформаційним впливам. Ефективне вирішення цієї проблеми є запорукою захисту національних інтересів та реалізації права громадян на отримання достовірної інформації.

Для забезпечення інформаційної безпеки держави необхідно вирішити низку масштабних завдань, серед яких:

- розробка теоретичних засад інформаційної безпеки;
- формування системи органів, відповідальних за інформаційну безпеку;
- удосконалення механізмів управління захистом інформації та їх автоматизація;
- створення комплексної нормативно-правової бази;
- розвиток вітчизняного виробництва засобів захисту інформації;
- підготовка кваліфікованих фахівців у галузі інформаційної безпеки.

Комплекс питань інформаційної безпеки держави охоплює такі ключові сфери:

- захист та регулювання обігу інформації;
- захист критичної інформаційної інфраструктури;
- забезпечення безпечного розвитку інформаційного простору;
- захист національного інформаційного ринку;
- протидія інформаційному тероризму та інформаційним війнам [1, с. 68].

Інформаційна безпека розглядається в контексті національної безпеки з двох точок зору. З одного боку, вона є самостійним елементом національної безпеки, а з іншого – інтегрованою складовою інших її видів, таких як військова, економічна та політична безпека.

У контексті сучасних викликів, інформаційна безпека постає як багатогранний феномен, що охоплює захист життєво важливих інтересів особистості, суспільства та держави. Її сутність полягає у мінімізації ризиків, пов’язаних з недостовірністю, неповнотою або несвоєчасністю інформації, негативним інформаційним впливом, а також несанкціонованим поширенням даних та наслідками функціонування інформаційних технологій [1, с. 86]. Це

визначення, хоч і не позбавлене певної абстрактності, відображає комплексний характер інформаційної взаємодії в державі.

Захист інформаційного суверенітету тісно пов’язаний з інформаційною безпекою, що передбачає захист внутрішньої інформації, її якості, надійності та конфіденційності. Водночас, це включає контроль над інформаційними потоками, обмеження поширення провокаційної або ворожої інформації, а також захист національного інформаційного простору від зовнішньої експансії.

Ключовими компонентами інформаційної безпеки держави є обсяг виробництва інформаційного продукту, стійкість мереж до інформаційного навантаження, здатність держави регулювати інформаційні потоки, доступність інформаційних джерел для населення та відкритість інформаційного простору [4, с. 53].

Аналіз праць вітчизняних дослідників дозволяє сформулювати ключові цілі політики інформаційної безпеки України. Насамперед, це реалізація конституційних прав громадян на інформацію, захист інформаційного суверенітету, забезпечення інформаційної достатності для прийняття рішень та гідна присутність країни у світовому інформаційному просторі.

Експерти також наголошують на необхідності зміцнення національної безпеки через ефективне використання інформаційного потенціалу, підвищення рівня вітчизняного інформаційного продукту, розвиток інформаційної інфраструктури та підтримку національних суб’єктів інформаційного простору. Важливим є й упорядкування інформаційних відносин, особливо зміна співвідношення вітчизняної та зарубіжної інформаційної продукції на користь першої.

Забезпечення інформаційної безпеки зумовлене потребою в національній безпеці, існуванням загроз в інформаційній сфері та можливістю впливу на свідомість людей. Стратегічним завданням є створення потужного національного інформаційного простору, що включає протидію загрозам та захист інформаційних ресурсів.

Завданнями забезпечення інформаційної безпеки є виявлення та прогнозування загроз, розробка та координація державної політики, створення систем інформаційної безпеки та формування позитивного іміджу держави у міжнародних інформаційних відносинах [2].

Забезпечення захисту та контролю національного інформаційного простору, а також формування позитивного іміджу країни у світовому інформаційному середовищі, є ключовим викликом інформаційної безпеки. Інформаційний простір, що визначається як середовище, де відбувається створення, збір, зберігання, обробка та поширення інформації, підпадає під юрисдикцію держави.

Будь-яка інформаційна технологія складається з етапів створення, обробки, зберігання та споживання інформації. Для забезпечення безпеки необхідно гарантувати надійність функціонування кожного з цих елементів. Зважаючи на це, основною метою інформаційної діяльності є побудова повноцінного та відкритого інформаційного простору.

Засоби масової інформації (ЗМІ) відіграють важливу роль в інформаційному просторі. Умови їхньої діяльності, законодавче регулювання та захист журналістів є критично важливими факторами. У країнах, що розвиваються, ЗМІ можуть мати вирішальний вплив на суспільство, оскільки за відсутності належного законодавства вони можуть маніпулювати громадською думкою та поширювати недостовірну інформацію, що становить загрозу національній інформаційній безпеці. В умовах сучасних конфліктів інформація, що формує суспільну думку, набуває все більшого значення в системі національної оборони. Як зазначав Г. Почепцов, «для тоталітарного, як і для будь-якого іншого сучасного суспільства інформаційна картина світу (уявлення про світ) важливіша, ніж сам реальний світ» [20]. Довготривалий вплив ЗМІ, що формують соціально-політичні установки та стереотипи, також має велике значення.

Ключове завдання заходів з інформаційної безпеки полягає в тому, щоб мінімізувати потенційну шкоду, яка може виникнути через неповну, запізнілу

або неправдиву інформацію, а також через негативний вплив, спричинений інформаційними технологіями, включаючи несанкціоноване поширення даних.

Загалом, діяльність у сфері інформаційної безпеки держави охоплює широкий спектр заходів. Це включає в себе:

- розвиток науково-практичних основ інформаційної безпеки;
- удосконалення законодавчої та нормативно-правової бази;
- розробку нормативно-правових та організаційно-методичних документів;
- створення концепції інформаційної безпеки та спеціальних правових і організаційних заходів для захисту та розвитку інформаційних ресурсів;
- визначення правового статусу суб'єктів системи інформаційної безпеки;
- розробку законів та нормативних актів для врегулювання ліквідації наслідків загроз інформаційній безпеці;
- відновлення порушених прав та ресурсів, а також реалізацію компенсаційних заходів;
- вдосконалення організації, форм та методів запобігання та нейтралізації загроз;
- розвиток сучасних методів забезпечення інформаційної безпеки.

Отже, осмислення проблем, пов'язаних з державною інформаційною політикою, є критично важливим для розвитку інформаційного суспільства в Україні. Їх вирішення сприяє не лише прогресу, а й забезпеченню національної та інформаційної безпеки.

## 1.2. Політико-правове регулювання інформаційної безпеки в Україні

Досліджуючи еволюцію політико-правових основ інформаційної безпеки України у період 2014–2024 рр., не можна не відзначити, що з моменту проголошення незалежності в Україні було сформовано певний законодавчий фундамент у сфері національної інформаційної безпеки, який функціонував до початку повномасштабного вторгнення росії. Ключовим концептуальним

документом, що поклав початок нормативно-правовій базі інформаційної безпеки, стала Конституція України, яка визначила інформаційну безпеку як одну з найважливіших функцій держави, поряд із захистом суверенітету та територіальної цілісності. Конституція України [14].

Ці пріоритети знайшли своє відображення в низці нормативно-правових актів, зокрема, Законах України «Про інформацію» (1992), «Про друковані засоби масової інформації (пресу в Україні)» (1992), «Про телебачення і радіомовлення» (1993), «Про інформаційні агенції» (1995), «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (1997), «Про телекомунікації» (2003) та інших, які відображали розуміння українською владою розвитку інформаційного простору в умовах демократичних перетворень суспільства та усвідомлення потенційних загроз, що можуть виникнути в інформаційній сфері для стабільності суспільства в умовах глобалізації інформаційних процесів. Варто також згадати Доктрину інформаційної безпеки України 2009 року, що свідчило про зростання уваги з боку державного керівництва до питань інформаційної безпеки. Однак, загалом, підходи до інформаційної безпеки не набули системного характеру в контексті цілісної стратегії, здатної регулювати державну інформаційну політику у всіх сферах суспільних відносин та ефективно протидіяти можливим загрозам у цій галузі [2].

Інформаційна інфраструктура, як ключовий елемент реалізації державної політики в інформаційній сфері, виступає невід'ємною складовою стратегічних інформаційних ресурсів. Її роль у забезпеченні обороноздатності держави та розвитку інформаційного ринку є надзвичайно вагомою. Згідно з Законом України «Про Концепцію національної програми інформатизації», інформаційна інфраструктура охоплює широкий спектр компонентів, включаючи міжнародні та міжміські телекомунікаційні та комп'ютерні мережі, системи інформаційно-аналітичних центрів, інформаційні ресурси та технології, науково-дослідні установи, виробництво та обслуговування технічних засобів інформації, а також систему підготовки кваліфікованих фахівців. [24] Інформаційна інфраструктура

являє собою складну систему, що об’єднує виробництво інформаційних продуктів, їх доставку до споживача, виробництво засобів виробництва та доставки, інформаційні технології, накопичення та збереження інформаційних ресурсів, сервісне обслуговування та підготовку кадрів.

Формування сприятливого середовища для підготовки та початку агресії російської федерації проти України у 2014 році відбувалося в умовах гібридної війни, де інформаційна та психологічна складові відігравали як допоміжну, так і самостійну роль. У відповідь на цю загрозу, Україна об’єктивно потребувала залучення ресурсів як військового, так і інформаційного характеру. При цьому інформаційний чинник набував ключового значення як інструмент мобілізації суспільної свідомості та готовності до протистояння агресору [5].

Конкретними кроками у цьому напрямку стали зміни до чинного законодавства, спрямовані на його актуалізацію, а також розробка низки нових законодавчих та нормативно-правових актів, що регулюють інформаційну сферу. Серед них, зокрема, Стратегії національної безпеки України (2015 та 2020 років), Закон України «Про національну безпеку України», Доктрина інформаційної безпеки України, Стратегія кібербезпеки України, Воєнна доктрина України, Закони України «Про інформацію», «Про доступ до публічної інформації», «Про Раду національної безпеки і оборони України», Стратегія інформаційної безпеки та інші акти.

Реакцією на радикальні зміни у безпековому ландшафті України, спричинені агресією рф, стало ухвалення Стратегії національної безпеки 2015 року. Цей документ ознаменував перехід до якісно нової державної політики, націленої на ефективний захист національних інтересів у всіх сферах. Ключовими напрямами визначено комплексну реформу сектору безпеки та оборони, з акцентом на готовність до відбиття зовнішньої агресії, зокрема гібридних загроз [6, с. 138].

Наступним кроком стало прийняття Закону «Про національну безпеку України» (2018), що конкретизував положення Стратегії та визначив правові засади забезпечення національної безпеки в умовах російської агресії.

Закон України «Про національну безпеку України» від 2018 року є ключовим документом, що визначає основні поняття та принципи державної політики у цій сфері. Зокрема, у ньому:

- надано дефініції національної безпеки, національних інтересів, Стратегії національної безпеки та Стратегії кібербезпеки;

- закріплено правову основу державної політики, що базується на Конституції України, зазначеному законі, інших законодавчих актах та міжнародних договорах;

- визначено принципи державної політики та фундаментальні національні інтереси України [26].

Доктрина окреслює різноманітні пріоритети державної політики в інформаційному просторі, зосереджуючись на кількох ключових аспектах. По-перше, акцент робиться на зміцненні інформаційної безпеки шляхом створення комплексної системи для оцінки та реагування на загрози. Це передбачає розширення повноважень регуляторних органів для ефективного протистояння як поточним, так і майбутнім викликам. По-друге, доктрина націлена на захист та розвиток національного інформаційного простору, а також на забезпечення права громадян на доступ до інформації. Крім того, підкреслюється важливість відкритості та прозорості державного управління, а також формування позитивного міжнародного іміджу України.

Особлива увага приділяється визначенню структури та функцій державних органів, відповідальних за інформаційну безпеку. Доктрина також передбачає науково-аналітичну підтримку державної інформаційної політики, покладаючи цю функцію на Національний інститут стратегічних досліджень при Президентові України.

Важливо відзначити, що реалізація доктрини відбувається в контексті інших політико-правових документів, таких як Воєнна доктрина України, Стратегія кібербезпеки України та відповідне законодавство, що регулює діяльність виконавчої влади в інформаційній сфері [13, с. 67].

Важливим підґрунтям для цього закону стала Доктрина інформаційної безпеки, затверджена Президентом України у 2017 році. Її метою було уточнення засад державної інформаційної політики, особливо в контексті протидії інформаційній агресії ворога. Доктрина ґрунтується на принципах дотримання прав і свобод людини, захисту її інтересів, а також забезпечення суверенітету та територіальної цілісності України.

У 2016 році, в умовах російської агресії, Рада національної безпеки і оборони України ухвалила рішення, яке стало фундаментом для формування національної системи кібербезпеки. Цей крок не лише визначив необхідність негайного створення такої системи, але й заклав правові основи для державної політики у цій сфері [16, с. 48]. Важливим аспектом стало врахування міжнародних стандартів, зокрема Конвенції про кіберзлочинність, та національного законодавства, що регулює питання національної безпеки, інформаційних ресурсів та електронних комунікацій.

Подальший розвиток нормативно-правової бази відбувся у 2020 році з прийняттям нової Стратегії національної безпеки України. Цей документ, що з’явився після президентських виборів 2019 року, підтвердив гібридний характер ворога, де інформаційна війна є невід’ємною складовою. Стратегія визначила пріоритетність активної протидії розвідувально-підривній діяльності, кібератакам та пропаганді.

Особлива увага приділяється створенню національної системи стійкості, здатної реагувати на широкий спектр загроз. Цей підхід поєднується з необхідністю ефективного стратегічного планування та кризового менеджменту в усіх сферах державної політики, включаючи інформаційну безпеку.

В умовах повномасштабної агресії рф, концентрація інформаційних ресурсів під державним контролем стала ключовим елементом стратегії інформаційної безпеки України [5, с. 59]. Резонансним кроком у цьому напрямку стало рішення РНБО від 19.03.2022, що імплементувало єдину інформаційну політику шляхом створення цілодобового марафону «Єдині новини #UAразом».

Цей захід, хоч і викликав дискусії щодо свободи слова, був обґрунтований необхідністю оперативного протистояння інформаційним загрозам.

Паралельно, законодавче поле інформаційної безпеки було доповнено Законом України «Про медіа» (№ 2849-IX), який набув чинності 31.03.2023. Закон розширив повноваження Національної ради з питань телебачення і радіомовлення, надавши їй інструменти для регулювання медійного простору, включаючи реєстрацію ЗМІ та застосування санкцій. Ці зміни, хоч і викликають занепокоєння щодо можливого обмеження свободи слова, відображають прагнення держави до ефективного контролю за інформаційним простором в умовах війни [25].

Отже, у контексті поточних викликів, першочерговим завданням є не лише створення комплексної нормативно-правової бази для протидії інформаційній агресії, але й адаптація чинного законодавства до реалій воєнного стану. Оптимізована система нормативно-правового забезпечення інформаційної безпеки має не тільки вдосконалити механізми протидії інформаційним атакам з боку рф, але й закласти основу для нейтралізації інформаційних загроз, що виникають в процесі післявоєнної відбудови та розвитку держави.

# РОЗДІЛ 2
# АНАЛІЗ СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

## 2.1. Інформаційне поле України в умовах сучасних викликів і загроз

Наприкінці лютого 2022-го, після невдалих спроб інтегрувати Україну в орбіту «русского міра» у попередні роки, розпочалася повномасштабна фаза російсько-української війни. Ця ескалація виявила не лише стійкість українського опору, але й прогалини в інформаційній безпеці, зокрема, наявність колаборантів, що підривали національну єдність. У цих умовах, інформаційна політика держави мала на меті не лише викрити згубність колабораціонізму, але й зміцнити віру в перемогу, протидіючи ворожій пропаганді.

Ключовим завданням стало налагодження ефективної комунікації між владою та суспільством, що сприяло б збереженню довіри та розумінню необхідності непопулярних рішень, зумовлених воєнним станом. Водночас, виникла потреба в обмеженні доступу до інформації, яка могла б сприяти ворожим діям [1, с. 196].

Діджиталізація медіа, що сталася до початку повномасштабного вторгнення, виявилася важливим фактором у забезпеченні інформаційної стійкості. Перехід на цифрові технології зробив неефективними спроби ворога зруйнувати інформаційну інфраструктуру через атаки на телевежі. Крім того, це дозволило державі ефективніше контролювати інформаційний простір, зокрема, через можливість відключення певних телеканалів.

Однак, швидке поширення інформації, яке стало можливим завдяки цифровим технологіям, також створило нові виклики, зокрема, ризик поширення фейків та дезінформації.

На початку повномасштабної агресії рф в Україні, Telegram-канали стали ключовим інструментом для оперативного інформування населення. Була

швидко розгорнута система сповіщення про повітряні тривоги з візуалізацією на інтерактивній карті.

Місцеві органи влади, освітні та медичні заклади, поліція – всі активно використовували Telegram для поширення життєво важливої інформації: від розташування пунктів незламності до графіків евакуаційних потягів та наявності пального. Простота та швидкість платформи забезпечили широке охоплення аудиторії в умовах воєнного часу [33].

Певний час, військові без цензури ділилися відео з передової, демонструючи хід бойових дій та знищення техніки противника. Ці матеріали, хоч і мали психологічний вплив, піднімаючи бойовий дух, могли містити інформацію, що становить стратегічну цінність для ворога. Слова захисників острова Зміїний стали символом опору, а знищення крейсера «Москва» – демонстрацією військової спроможності України.

Президент України Володимир Зеленський регулярно звертався до нації, використовуючи відеозвернення з київських локацій, що мало на меті підтвердити його присутність в країні. Однак, прагнучи підтримати моральний дух, він неодноразово висловлював оптимістичні прогнози щодо термінів завершення війни, зокрема, називаючи травень 2022 року як можливу дату.

В українському медіапросторі спостерігалася тенденція до формування завищених очікувань щодо швидкого розпаду російської федерації та переможного завершення воєнних дій восени 2022 року, що ґрунтувалися на серії успішних контрнаступів ЗСУ. Водночас, стрімкий наступ ворога на південному напрямку викликав нерозуміння та критику щодо дій високопосадовців, які напередодні повномасштабного вторгнення заперечували його можливість.

З метою централізації інформаційного потоку та забезпечення оперативного інформування населення було запроваджено цілодобовий телемарафон «Єдині новини #UAразом». Національна рада з питань телебачення і радіомовлення надала дозвіл на відступ від програмних концепцій телеканалів на період воєнного стану. Міністерство культури та інформаційної політики

ініціювало створення загальнонаціонального телемарафону, до якого долучилися провідні українські телеканали, такі як «1+1», СТБ/ICTV, «Інтер», «Рада», «Україна», «Україна 24» та «Суспільне». Проте, низка рейтингових телеканалів, зокрема «5-й канал», «Прямий» та «Еспресо», на початковому етапі повномасштабного вторгнення продовжували власне мовлення, згодом інтегруючи вставки з телемарафону [33].

Ініціатива створення телемарафону передбачала формування універсального інформаційного майданчика, доступного для громадян у цілодобовому режимі, з метою оперативного інформування про ключові події національного та міжнародного значення. Однак, реалізація цього проєкту зіткнулася з низкою організаційних викликів. Зокрема, спостерігалася тенденція до надмірного використання повторного контенту, що включав як матеріали попередніх періодів, так і поточні виступи, що негативно вплинуло на сприйняття телемарафону як джерела актуальної інформації. Крім того, відсутність чіткого графіку виходу новинних блоків ускладнювала сприйняття інформаційного потоку. Спроби забезпечення півгодинних випусків новин не завжди були успішними через дефіцит відповідного матеріалу, а нічні інформаційні блоки часто характеризувалися затримками в оприлюдненні інформації.

У період повномасштабного воєнного конфлікту спостерігалося стрімке зростання популярності Telegram-каналів, таких як «Інсайдер-UA», «Лачен пише», «Доброго вечора, ми з України» та «Інсайдер ЗСУ», що свідчить про зміну інформаційних переваг аудиторії. Факт акредитації представників Telegram-каналів на пресконференцію Президента України В. Зеленського у грудні 2023 року відображає визнання їхньої ролі як ключового джерела інформації, що було підтверджено результатами соціологічних досліджень [21].

В умовах воєнного стану та енергетичної кризи, зокрема регулярних відключень електропостачання восени 2022 – взимку 2023 років, держава тимчасово утрималася від внесення змін до нормативно-правових актів, що регулюють діяльність блогерів. Ця ситуація сприяла переорієнтації споживання

медіа-контенту, з акцентом на мобільні платформи, здатні функціонувати в умовах обмеженого доступу до електроенергії.

Феномен поширення суб'єктивних оцінок подій російсько-української війни блогерами на цифрових платформах, таких як соціальні мережі, відеохостинги та месенджери, набув особливої актуальності. Сприйняття цих оцінок як «незалежних» та їхня різноманітність стимулювали активний пошук інформації з метою формування індивідуального комфортного інформаційного простору. В умовах зростання інформаційних потоків, пріоритетними стали персоналізація інформаційного поля та оперативність отримання життєво важливих даних.

Повномасштабна військова агресія спричинила активізацію горизонтальних зв'язків між громадянами, що було зумовлено нагальною потребою у швидкому обміні актуальною інформацією, яка не могла бути оперативно надана традиційними засобами масової інформації [33]. Зокрема, у перші дні вторгнення критично важливими стали повідомлення про наявність пального, можливості тимчасового розміщення та ремонту транспортних засобів, а також інформація про стан транспортних магістралей та волонтерську допомогу.

При цьому спостерігалася тенденція до переважного використання інформації, отриманої від близьких осіб. У цифровому просторі швидко сформувалися тематичні групи для обговорення проблем, пов'язаних з евакуацією та пошуком притулку. В умовах воєнних дій також набули поширення локальні групи, об'єднуючі мешканців конкретних населених пунктів, вулиць та навіть будинків. Ці групи відігравали важливу роль у вирішенні соціально-побутових проблем, забезпеченні продуктами харчування, водою та медикаментами, особливо в умовах тривалої комендантської години. Крім того, соціальні мережі стали важливим інструментом для психологічної підтримки, забезпечуючи можливість постійного спілкування.

Аналіз даних Київського міжнародного інституту соціології, отриманих у травні 2022 року, демонструє домінуючу роль соціальних мереж як джерела

інформації для українського суспільства (76,6%). Порівняно з телебаченням (66,7%) та інтернет-простором (61,2%), соціальні мережі, попри дещо нижчий рівень довіри (54% проти 60,5% у телебачення), забезпечують оперативне поширення інформації. Однак, паралельно з цим, спостерігається інтенсифікація використання соціальних мереж та месенджерів для трансляції ворожих пропагандистських наративів та дезінформації [9].

Комерціалізація блогерської діяльності сприяє поширенню неперевіреної інформації, що претендує на сенсаційність, а також суб'єктивних коментарів та упереджених висновків. Ключовим фактором при оприлюдненні контенту стає потенційна можливість залучення максимальної кількості користувачів. В умовах повномасштабної війни, окремі блогери продовжують просувати ідею «поглиблення дружніх відносин з росією», критикуючи дії українського керівництва, спрямовані на організацію опору агресору. При цьому, як правило, такі блогери уникають обговорення територіальних претензій рф, наслідків ворожих обстрілів та перспектив існування незалежної України.

Суспільна думка щодо необхідності законодавчого регулювання діяльності блогерів розділилася: 34% респондентів виступають проти, 30% підтримують цю ідею [9]. Противники регулювання наголошують на необхідності збереження свободи вираження думок в Інтернеті та сумніваються в ефективності державного втручання. Прихильники регулювання, у свою чергу, виступають за його універсальне застосування до всіх блогерів без винятків.

Дискусії щодо доцільності державного контролю за діяльністю блогерів в Україні набули гострого характеру. Практика блокування окремих YouTube- чи Telegram-каналів виявилася неефективною через швидке виникнення нових. Такий підхід призвів би лише до розпорошення державних ресурсів. Тому в березні 2022 року Верховна Рада внесла зміни до Кримінального кодексу, додавши статті 435-1 та 436-2 [15]. Ці статті передбачають кримінальну відповідальність за виправдання, визнання правомірною або заперечення збройної агресії рф проти України, а також за глорифікацію її учасників [18, с. 174].

Кримінальний кодекс України також передбачає відповідальність за образу честі та гідності військовослужбовців, а також за виготовлення та розповсюдження відповідних матеріалів. Поширення інформації, що заперечує збройну агресію рф проти України, також карається кримінально. Зрозуміло, що посилення відповідальності за розповсюдження недостовірної інформації в умовах війни є логічним кроком. Однак, цей крок був би значно ефективнішим, якби відповідні заходи були вжиті на початку російсько-української війни, а держава ще в 1990-х роках сформувала б систему захисту інформаційного простору та протидії ворожим ІПСО [3, с. 124]. Відсутність досвіду формування українського інформаційного поля стала очевидною під час повномасштабного вторгнення рф. Однією з особливостей цієї війни стало те, що медіа не лише висвітлюють події, але й активно впливають на їх формування.

На початку 2024 року оцінка ефективності державної інформаційної політики України в умовах повномасштабного вторгнення рф є неоднозначною. З одного боку, успішним виявилося висвітлення характеру конфлікту та розвінчання міфу про «другу армію світу», що сприяло розширенню міжнародної підтримки. З іншого боку, агресор, усвідомивши неможливість швидкої перемоги, перейшов до тактики тотального руйнування цивільної інфраструктури, що засвідчили події в Бучі, Ірпені, Маріуполі та інших містах.

Українські медіа оперативно реагували на ці злочини, поширюючи інформацію про обстріли та жертви серед мирного населення, що дозволило світовій спільноті оцінити реальний масштаб трагедії. Важливим фактором стало не лише висвітлення злочинів з боку журналістів, але й самодокументування агресора, який публікував відео знущань та вбивств у мережі Інтернет.

Окремо варто відзначити проєкт журналістів В. Золкіна та Д. Карпенка, який за підтримки держави показав реальні мотиви російських військовополонених, більшість з яких керувалися меркантильними інтересами. Цей проєкт дозволив українському суспільству провести паралель між власним прагненням до заробітку та мотивацією окупантів.

Аналіз інформаційного простору виявив неоднозначну роль колаборантів, які, керуючись різними мотивами, брали участь у коригуванні ворожих обстрілів українських міст. Паралельно, спостерігалася тенденція до співпраці окремих блогерів з державними органами, що сприяло частковому спрощенню процесу обміну військовополоненими та, певною мірою, підірвало наратив про невідмовність росії від своїх громадян [12, с. 115].

Посилення впливу цифрових платформ зумовило значний зсув у споживанні медійного контенту, з традиційного телебачення на соціальні мережі, відеохостинги та месенджери. Домінуючу позицію в інформаційному просторі України зайняли Telegram-канали, що, ймовірно, було посилено підтримкою з боку владних структур. Водночас, використання інфлюенсерів як джерела інсайдерської інформації виявилося неоднозначним, оскільки їх коментарі часто відображали провладну позицію. Якщо на початковому етапі конфлікту така позиція сприймалася як виправдана, то з часом зростання недовіри до офіційних джерел інформації призвело до зміни ставлення. Це було зумовлено нездатністю деяких експертів адекватно оцінити ситуацію на фронті, масштаби та умови надання міжнародної допомоги, зокрема, її зв’язок з антикорупційними заходами української влади [30].

В умовах повномасштабного вторгнення, Telegram-канали продемонстрували відсутність відповідальності за достовірність інформації, виступаючи скоріше як інструмент економічної діяльності, де швидкість поширення інформації є ключовим фактором. У випадках поширення недостовірної інформації, її спростування часто подається як чергова сенсація.

Отже, у початковий період повномасштабного вторгнення російської федерації в Україну, централізація інформаційного потоку виявилася дієвим інструментом, що запобіг панічним настроям та сприяв консолідації сил для опору на ключових напрямках. Просування україноцентричних наративів стало вагомим чинником у формуванні сприятливого інформаційного простору для патріотично налаштованих громадян.

Наразі, одним із ключових завдань державної інформаційної політики є підтримка єдності українського суспільства у протистоянні агресору. В Україні назріла потреба у відкритому обговоренні актуальної ситуації на фронті, проте дефіцит політичного діалогу компенсується надмірною присутністю так званих «експертів». Викривлення дійсності цими «експертами» підриває довіру до влади та знижує мотивацію громадян до захисту держави. Влада не може ігнорувати нагальні питання, зокрема щодо причин швидкої окупації південних територій та щодо впливу корупційних дій на ефективність оборони.

Для підвищення мобілізаційного потенціалу державної інформаційної політики необхідно активно поширювати інформацію про перспективи та стратегії післявоєнної відбудови, зосереджуючись на інноваційних проєктах, модернізації економіки та налагодженні ефективної взаємодії між бізнесом та владою, а також на зміцненні міжрегіональних зв'язків [11, с. 43].

В умовах цифрової трансформації медіа, блокування окремих інформаційних ресурсів має обмежену ефективність, оскільки автори заблокованих каналів можуть використовувати альтернативні цифрові платформи. Тому, назріла необхідність у модернізації формату загальнонаціонального телемарафону, шляхом залучення до створення його контенту усіх рейтингових телеканалів.

Сучасна інформаційна політика держави стикається з низкою викликів, що потребують негайного вирішення. Нерівномірний розподіл інформаційних ресурсів, коли перевага надається наближеним до влади блогерам та Telegram-каналам, призводить до ситуації, в якій навіть журналісти, що працюють над створенням контенту для загальнонаціонального телемарафону, змушені використовувати вже оприлюднену в цих джерелах інформацію. Така практика не лише знижує оперативність та якість інформаційного потоку, але й підриває довіру до офіційних джерел.

Окремої уваги заслуговує проблема непрозорого фінансування виробників контенту. Недостатня прозорість у розподілі коштів між великими медіа-

холдингами та окремими проєктами створює умови для зловживань та непродуктивного використання державних ресурсів.

Для подолання цих проблем необхідно переорієнтувати державну інформаційну політику на створення сприятливих умов для розвитку якісних медіа. Це передбачає відмову від вузькоплатформних проєктів та перехід до мультимедійного контенту, який би охоплював візуальні, аудіо- та цифрові формати з використанням можливостей штучного інтелекту.

Ставка на Telegram як основний канал поширення інформації є необґрунтованою. Анонімність та відсутність відповідальності за поширення контенту сприяють поширенню дезінформації та знижують рівень довіри до інформаційних повідомлень. У цьому контексті необхідно активізувати роботу з підвищення рівня медіаграмотності населення, формуючи критичне ставлення до анонімних джерел інформації.

В умовах зниження довіри до офіційних джерел інформації, мережа якісних регіональних та національних ЗМІ, що функціонують за підтримки західних партнерів, може стати ефективною альтернативою загальнонаціональному телемарафону [22].

Спроби держави консолідувати інформаційний простір через телемарафон та підтримку окремих Telegram-каналів не демонструють очікуваної ефективності. Відсутність стабільного та збалансованого діалогу між владою та суспільством стимулює громадян до пошуку альтернативних джерел інформації, що сприяє розширенню горизонтальних зв’язків.

Зростання горизонтальних зв’язків в умовах інформаційного вакууму з офіційних джерел не лише підриває довіру до влади, але й створює сприятливий ґрунт для ворожих інформаційно-психологічних операцій.

Отже, в умовах воєнного стану, самоцензура стає критично важливим інструментом для медійників, запобігаючи поширенню забороненої інформації та надмірному акценту на негативних аспектах життя в Україні. Українські медіа мають прагнути до збалансованого висвітлення корупційних випадків, реформ та бойових дій.

Важливо наголошувати на успішному досвіді ЗСУ у війні, що є найбільшою з часів Другої світової, та на їхніх досягненнях у знищенні значної частини Чорноморського флоту ворога.

## 2.2. Інформаційна війна та дезінформація як загрози національній безпеці

Дезінформація, як явище, являє собою складний конструкт, що охоплює навмисне поширення неправдивих або спотворених відомостей з метою введення в оману. Її застосування варіюється від тактичних військових операцій, де вона слугує для дезорієнтації противника, до стратегічних політичних кампаній, спрямованих на формування громадської думки.

Згідно з визначенням Кембриджського словника, дезінформація – це неправдива інформація, що поширюється з метою обману. Проте, важливо розрізняти дезінформацію та інші форми неправдивої інформації, такі як місінформація, яка може поширюватися без злого наміру [7, с. 47].

Військова дезінформація, зокрема, передбачає створення ілюзії щодо стану власних збройних сил, їхнього озброєння та планів, що може включати імітацію військової активності або створення фіктивних об’єктів.

Історично, дезінформація відігравала значну роль у політичних стратегіях. Прикладом може слугувати радянська пропаганда, яка систематично використовувала дезінформацію для формування викривленого сприйняття реальності, що мало довготривалі наслідки для суспільства.

Згідно з міжнародними документами, зокрема Спільною декларацією представників ООН, ОБСЄ та інших організацій, а також доповіддю Спеціального доповідача ООН від 13 квітня 2021 року, дезінформація визначається як навмисне поширення неправдивої інформації з метою завдання шкоди суспільству, політичним опонентам або отримання економічної вигоди.

Цей підхід підтверджується також Кодексом практики ЄС щодо протидії дезінформації [17].

Ключовою відмінністю дезінформації від звичайної недостовірної інформації є наявність умислу. Тобто, дезінформація – це не просто помилкова інформація, а свідомо створена маніпуляція з метою досягнення конкретних цілей.

Попри те, що в українському законодавстві, зокрема в Законах України «Про інформацію» та «Про медіа», закріплено принцип достовірності інформації, чітке визначення поняття «дезінформація» досі відсутнє. Водночас, законодавство України досить детально регламентує способи державного втручання в інформаційну діяльність, включаючи заходи щодо запобігання поширенню дезінформації.

У контексті забезпечення національної безпеки, згідно з правовими нормами, зокрема Законом України «Про національну безпеку України», ключовим аспектом є захист суверенітету держави, її територіальної цілісності та конституційного ладу від різноманітних загроз [26].

Важливим елементом правового регулювання інформаційного простору є Закон України «Про інформацію», який у статті 28 встановлює обмеження на використання інформації, забороняючи її застосування для закликів до повалення конституційного ладу, порушення територіальної цілісності, пропаганди війни, насильства, розпалювання ворожнечі та інших протиправних дій [23].

Для протидії дезінформації та забезпечення інформаційної безпеки України було створено Центр протидії дезінформації при Раді національної безпеки і оборони України. Його діяльність, визначена Указом Президента України № 187/2021, спрямована на виявлення та нейтралізацію інформаційних загроз, протидію пропаганді та маніпуляціям громадською думкою.

Стратегія інформаційної безпеки України, затверджена Указом Президента України № 685/2021, визначає стратегічні цілі та завдання у сфері інформаційної безпеки, включаючи захист прав громадян на інформацію та

персональні дані, а також протидію актуальним викликам та загрозам в інформаційному просторі. Її реалізація розрахована на період до 2025 року [30].

У контексті сучасного інформаційного простору, особливо в умовах збройного конфлікту, питання регулювання медіаконтенту набуває особливої актуальності. Згідно з положеннями статті 119 Закону, на суб'єктів аудіовізуальних, друкованих та онлайн-медіа накладається заборона на поширення інформації, що інтерпретує збройну агресію проти України як внутрішній конфлікт, громадянський конфлікт чи громадянську війну. Таке обмеження спрямоване на запобігання розпалюванню ворожнечі, ненависті, а також закликам до насильницької зміни конституційного ладу чи порушення територіальної цілісності [12]. Аналогічно, забороняється поширення недостовірних матеріалів, що стосуються збройної агресії та дій держави-агресора (держави-окупанта), її посадових осіб, осіб та організацій, що контролюються державою-агресором (державою-окупантом), якщо це призводить до аналогічних наслідків.

Водночас, в Україні активно розробляються та впроваджуються стратегії з використання штучного інтелекту для забезпечення інформаційної безпеки. Відповідно до Концепції розвитку штучного інтелекту в Україні, затвердженої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р, одним із пріоритетних напрямів є виявлення, запобігання та нейтралізація наслідків поширення недостовірної, неповної або упередженої інформації. Передбачається, що системи штучного інтелекту можуть бути використані для виявлення потенційно небезпечної інформації, аналізу авторства та джерела походження [27].

Інформаційні технології, безсумнівно, відкривають нові горизонти для державного управління, інформування громадськості та залучення громадян до участі в житті країни. Однак, паралельно з цим, зростає ризик поширення дезінформації. Алгоритмічні системи та штучний інтелект дозволяють створювати фейкові новини, які важко відрізнити від правдивих, і націлювати їх на конкретні аудиторії, що робить їх особливо небезпечними.

На сьогоднішній день Інтернет є основним джерелом інформації для українців. Згідно з опитуванням, проведеним у 2023 році, 62% респондентів черпають інформацію з соціальних мереж, а 48% – з новинних сайтів. Соціальні мережі особливо вразливі до поширення дезінформації через відсутність редакційного контролю, можливість вільно публікувати матеріали та швидкість і безкоштовність поширення інформації. Користувачі можуть легко поширювати вірусний контент, який швидко розлітається по різних платформах [8].

Соціальні мережі набули величезної популярності, оскільки кожен може створювати контент. В умовах інформаційного перенасичення критично важливо вміти відрізняти надійні джерела від тих, що вводять в оману.

Методологія дезінформаційних заходів варіюється залежно від оперативної ситуації, цілей та завдань, що стоять перед суб'єктом, який їх застосовує. Кожен метод має свої переваги та недоліки, що визначають його ефективність у конкретному контексті [6, с. 138].

Основні принципи побудови дезінформаційних кампаній включають:

1. Систематизацію повідомлень, а саме використання «класифікаторів» – ключових слів або маркерів, що дозволяють групувати дезінформаційні наративи за певними ознаками.

2. Мережеву організацію, тобто, формування «сіток» – скоординованих груп Telegram-каналів з єдиним центром управління та концепцією. Структура таких сіток включає власників, кураторів, редакторів, PR-менеджерів, дизайнерів, авторів контенту та технічний персонал, що забезпечує комплексний підхід до поширення дезінформації.

3. Маніпулювання інформаційним простором, активне використання анонімних Telegram-каналів для поширення неперевірених політичних та військових «інсайдів», суб'єктивних інтерпретацій геополітичних подій, з акцентом на репости та дезінформаційну тональність.

4. Застосування «риторичних запитань» – формулювання псевдо-фактів з подальшим підведенням до питань, що не потребують відповіді, з метою створення ілюзії логічної аргументації.

5. Використання «принципу психологічного шоку» – поширення сенсаційних новин, що викликають сильні емоційні реакції, руйнуючи психологічний захист аудиторії та створюючи умови для нав’язування потрібних наративів.

6. Маніпуляція контекстом, а саме, застосування «принципу контрасту» – відволікання уваги від негативних подій шляхом акцентування на інших, більш резонансних, що дозволяє затьмарити невдачі.

7. Використання механізму «перекладання відповідальності» – ухилення від негативних наслідків шляхом звинувачення інших суб’єктів, що є типовим для пропагандистських кампаній [19].

Ці методи, у різних комбінаціях, використовуються для досягнення конкретних цілей дезінформаційних кампаній, таких як маніпулювання громадською думкою, створення хаосу та дестабілізація ситуації.

У контексті сучасних інформаційних війн, ворог активно застосовує різноманітні механізми дезінформації, спрямовані на маніпуляцію суспільною свідомістю. Аналіз цих методів дозволяє краще зрозуміти їхню природу та розробити ефективні стратегії протидії.

Одним із поширених прийомів є «заговорювання», що має на меті викликати інформаційну втому та знизити інтерес до певних тем. «Ефект первинності» використовує психологічну схильність до довіри першій отриманій інформації, що особливо ефективно в умовах інформаційного хаосу. «Буденна розповідь» полягає у систематичному впровадженні дезінформації про насильство, що з часом притуплює реакцію аудиторії.

«Удар на випередження» передбачає поширення дезінформації з метою спровокувати реакцію противника та використати її у власних інтересах. «Хибна аналогія» маніпулює логічними зв’язками, створюючи штучні паралелі між подіями. «Констатація факту» подає бажану інформацію як беззаперечну істину, часто з використанням авторитетних джерел.

«Обхід з флангу» полягає у поєднанні правдивої інформації з дезінформацією, що дозволяє непомітно впроваджувати потрібні наративи.

«Створення проблеми» маніпулює інформаційним простором, надаючи одним подіям надмірної важливості, а іншим – занижуючи їхнє значення. «Керований коментар» спрямовує думки аудиторії у потрібному напрямку, пропонуючи заздалегідь визначені інтерпретації подій.

«Ефект ореолу» використовує стереотипи та упередження, переносячи позитивні якості з однієї сфери на іншу. «Відволікання уваги» полягає у створенні інформаційного шуму, що відволікає від важливих тем. «Переконання» – це метод впливу на критичне мислення, що використовує логічні аргументи та емоційні звернення [31].

З метою підвищення ефективності протидії інформаційним загрозам, детального аналізу їхньої структури та вивчення тактик, що використовуються противником, Центром протидії дезінформації було розроблено «Посібник з протидії дезінформації» (2023), реалізований за підтримки Консультативної місії ЄС в Україні [12].

Окрім цього, у вересні 2021 року на платформі «Prometheus» було запущено онлайн-курс «Дезінформація: види, інструменти та способи захисту». Цей курс, розроблений Українським кризовим медіа-центром за підтримки USAID, спрямований на широке коло аудиторії: від студентів, що вивчають журналістику та суміжні спеціальності, до державних службовців і громадських діячів. Програма курсу охоплює п’ять модулів, що детально розглядають дезінформацію як систему, її структурні елементи, основні інструменти та тактики, а також практичні загрози в контексті України. Лекції містять аналіз реальних кейсів та актуальні дані досліджень, а кожен модуль завершується практичними рекомендаціями та додатковими матеріалами.

Отже, дезінформація в епоху цифрових технологій набула не просто глобального, а, екзистенційного характеру. Здається,  всі ми, від студентів до політиків, відчуваємо її вплив на собі. І це не просто питання «фейкових новин», це виклик, що пронизує всі аспекти нашого життя: від політичних виборів до здоров’я.

Зрозуміло, що міжнародна спільнота намагається знайти баланс між свободою слова та необхідністю протидії дезінформації. В Україні, як і в багатьох інших країнах, назріла гостра потреба в розробці чітких правових механізмів. Потрібне законодавство, яке не тільки визначить, що таке дезінформація, але й встановить відповідальність за її поширення. І, звичайно, не можна забувати про медіаграмотність – без неї всі наші зусилля будуть марними.

Але тут є ще один важливий момент: міжнародні практики також потребують постійного оновлення. Технології змінюються з неймовірною швидкістю, і те, що працювало вчора, може бути абсолютно неефективним завтра. Потрібно навчитися не просто реагувати на загрози, а й передбачати їх.

## 2.3. Російсько-українська війна в контексті інформаційного протистояння

У сучасних політичних конфліктах інформаційна загроза набуває форми активного використання ресурсів мас-медіа та соціальних мереж протидіючими сторонами. Цей феномен виступає як елемент міжнародного тиску, так і інструмент соціально-психологічного впливу на державу або окремих індивідів в умовах політичного протистояння, причому активізація конфлікту супроводжується інтенсифікацією агресивних інформаційних кампаній.

Основною метою інформаційної війни є досягнення та утримання інформаційної переваги однією зі сторін шляхом цілеспрямованого інформаційно-психологічного та інформаційно-технічного впливу на систему державного прийняття рішень. Сучасні дослідники виділяють кілька етапів інформаційних війн. На початковому етапі спостерігається збільшення обсягу інформаційних матеріалів та активності з метою актуалізації «проблемної ситуації». Другий етап характеризується пошуком, завоюванням та консолідацією аудиторії навколо ключового протиріччя. На третьому етапі відбувається масова інформаційна обробка аудиторії, насичення інформаційного

простору матеріалами, що сприяють залученню широкої аудиторії на бік однієї з протидіючих сторін. Завершальним етапом є реакція аудиторії, що визначає домінування конкретної сторони в інформаційному просторі [2].

Аналіз інформаційного поля вказує на систематичну пропагандистську діяльність ворога проти України, що бере свій початок з моменту проголошення незалежності. Ескалація цієї діяльності спостерігалася в період правління В. Януковича. З початком російської агресії, зокрема під час операції з анексії Криму, експерти Національного інституту стратегічних досліджень зафіксували проведення ворогом масштабної інформаційно-психологічної кампанії. Ця кампанія була спрямована на дестабілізацію українського суспільства, деморалізацію силових структур та формування викривленого сприйняття подій серед російської та західної аудиторій.

Ключовими завданнями цієї інформаційної операції були:

- підрив бойового духу українських військових та правоохоронців;

- провокування суспільних заворушень;

- створення ілюзії масової підтримки російських дій серед населення південних та східних регіонів України;

- фальсифікація історичних подій [5, с. 63].

Для досягнення цих цілей використовувалися різноманітні комунікаційні канали, включаючи традиційні та електронні ЗМІ, інтернет-платформи та соціальні мережі.

З повномасштабним вторгненням росії 24 лютого 2022 року, інтенсивність пропагандистської діяльності значно зросла. Провідні російські телеканали активно поширюють фейкові новини та пропагандистські матеріали, спрямовані на виправдання агресії.

Одним із ключових наративів ворожої пропаганди є звинувачення України в «нацизмі». Це використовується для делегітимізації України на міжнародній арені. Крім того, ворожа пропаганда намагається представити конфлікт як боротьбу з окремими «нацистами» та «бандерівцями», які нібито утискають російськомовне населення України.

Аналіз інформаційного простору, що супроводжує російську агресію проти України, виявляє систематичне використання дезінформації та маніпулятивних технік. Зокрема, російські медіа уникають терміну «війна», замінюючи його на «спеціальна військова операція», що є прямим наслідком законодавчих обмежень, які передбачають кримінальну відповідальність за використання коректної термінології. Така підміна понять має на меті не лише приховати реальний характер конфлікту, але й сформувати у російського суспільства викривлене сприйняття подій, мінімізуючи негативне ставлення до агресії [10, с. 20].

Окрім цього, ворожа пропаганда активно поширює наративи, спрямовані на дискредитацію українського керівництва, зокрема, через створення міфу про «президента-втікача», що не відповідає дійсності. Також, систематично розповсюджуються фейкові повідомлення про «звірства українських націоналістів», такі як легенда про «розп’ятого хлопчика», що має на меті розпалювання міжнаціональної ворожнечі.

Додатково, російські ЗМІ намагаються виправдати вторгнення в Україну, стверджуючи про загрозу з боку НАТО, що є безпідставним. Звинувачення українських сил в обстрілах цивільних об’єктів, зокрема, у Маріуполі, також не витримують критики, оскільки міжнародні організації мають докази причетності російських військ до цих злочинів.

Отже, ворожа інформаційна війна характеризується використанням широкого спектру маніпулятивних технік, спрямованих на дезінформацію суспільства та виправдання агресивних дій.

З перших днів повномасштабного вторгнення ворожої армії в Україну, інформаційний простір вибухнув свідченнями воєнних злочинів. Вже в перший тиждень конфлікту було зафіксовано тисячі фактів, що підтверджують злочинні дії російських військ.

Аналізуючи інформаційну політику ворога, можна припустити, що значна частина пропагандистських зусиль спрямована на внутрішню аудиторію. В умовах потенційного розриву зв’язків із Заходом, російська еліта, ймовірно,

прагне посилити контроль над суспільною думкою для збереження стабільності режиму. Однак, в епоху цифрових технологій, повна інформаційна ізоляція є малоймовірною, і частина об’єктивної інформації неминуче просочується в загальний інформаційний простір.

Україна, у свою чергу, активно протидіє ворожій пропаганді. Зокрема, реалізується програма інформування населення про можливі фейкові повідомлення з боку противника. З кінця лютого 2022 року українські інформаційні ресурси зосередилися на донесенні до громадян достовірної інформації, наголошуючи на важливості довіри лише офіційним джерелам. Це дозволило ефективно протистояти традиційній російській тактиці дезінформації, яка передбачає масове поширення фейкових новин через соціальні мережі та інші канали [22].

Важливу роль у формуванні об’єктивного сприйняття подій відіграла оперативна робота українських журналістів та військового командування. З перших днів конфлікту вони регулярно інформували суспільство про ситуацію на фронті, включаючи як успіхи, так і невдачі. Така відкритість нейтралізувала ключову перевагу ворожої пропаганди – можливість маніпулювання інформацією в умовах інформаційного вакууму, що сприяло запобіганню поширенню панічних настроїв.

Безперечно, перехід до відкритості джерел у світовій журналістиці став каталізатором для об’єктивнішого висвітлення подій. Це ускладнило поширення російської дезінформації, зокрема фейків про бомбардування мирних міст «націоналістичними батальйонами». Водночас, варто врахувати, що загальна репутація ворожих державних ЗМІ, позначена систематичною брехнею, пропагандою та сумнівними «експертними» висновками, підірвала довіру до їхньої версії подій у міжнародному інформаційному просторі.

Українська інформаційна стратегія виявилася ефективною завдяки відкритості щодо злочинів окупантів. Це сприяло формуванню в українському суспільстві чіткого усвідомлення жорстокості ворожої агресії. З іншого боку, російське керівництво, очевидно, розраховувало на швидку «перемогу», що не

передбачало розробки ефективної інформаційної стратегії. «Шокова тактика» ведення війни не потребувала додаткових пояснень, зокрема щодо втрат. Ключовою помилкою ворожої інформаційної політики стало поширення наративу про «очікування визволителів» українським населенням. Неочікуваний опір українців та жорстокість війни призвели до деморалізації російських військ.

Аналіз поточного стану інформаційної політики України демонструє відносну ефективність у протидії ворожій пропаганді та іншим інформаційним загрозам. Внутрішня інформаційна діяльність українських ЗМІ сприяла підвищенню медіаграмотності населення, що, у свою чергу, зміцнило стійкість до дезінформаційних кампаній. Попри спроби російської влади дестабілізувати суспільну думку за допомогою інформаційних операцій, основні наративи українського суспільства залишаються відносно стабільними. Одним із яскравих прикладів успішного протистояння інформаційній агресії є високий рівень довіри до Збройних Сил України. Цей показник, що залишається найвищим серед державних інституцій, демонструє позитивну динаміку навіть в умовах постійних інформаційних викликів, пов’язаних з російсько-українською війною.

Отже, інформаційна війна, що розгорнулася в рамках російсько-українського конфлікту, є складовою ширшого військового протистояння. Ключовим вектором ворожої пропаганди стала дискредитація українських державних інституцій, збройних сил та суспільства загалом. Особливий акцент робився на поширенні дезінформації щодо «неонацистів» в Україні, що мало на меті підірвати міжнародну суб’єктність України. Крім того, ворожа пропаганда прагнула звузити конфлікт до боротьби з «нацистами» та «бандерівцями», які нібито утискають російськомовне населення.

Варто зазначити, що з 2014 року Україна значно зміцнила свою інформаційну оборону: були налагоджені ефективні канали комунікації з суспільством, запобігнуто поширенню паніки, а також встановлено співпрацю із західними партнерами для забезпечення їх об’єктивною інформацією про хід бойових дій. Це дозволило досягти успіху у висвітленні подій, де чітко визначено агресора та його наміри. Активна робота українських ЗМІ, незалежних експертів

та військових змусила російську пропаганду зосередитися на внутрішній аудиторії, де, на жаль, вона має певні успіхи.

Перспективним напрямом для подальших досліджень є аналіз трансформації ворожого суспільства, що призвела до підтримки війни та поширення ксенофобських настроїв. Очевидно, що цей процес «зомбування» має глибоке коріння, що сягає не лише 2014 року. Вивчення цього явища дозволить глибше зрозуміти механізми російської пропаганди та викрити роль ворожої держави в її поширенні.

# РОЗДІЛ 3
# ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

## 3.1. Державна політика в галузі інформаційної безпеки: основні напрями

Згідно з положеннями Закону України «Про інформацію», державна інформаційна політика визначається як комплекс стратегічних напрямків та тактичних методів, що застосовуються державою для забезпечення процесів отримання, обробки, поширення та збереження інформаційних ресурсів. Ключові аспекти цієї політики включають:

- гарантування доступу громадян до інформації, що є критично важливим для демократичного суспільства;
- розбудова національних інформаційних систем та мереж, що забезпечують ефективний обмін інформацією;
- підтримка матеріально-технічної, фінансової, організаційної, правової та наукової інфраструктури, необхідної для інформаційної діяльності;
- оптимізація використання інформаційних ресурсів для досягнення суспільно значущих цілей;
- стимулювання постійного оновлення, збагачення та надійного збереження національних інформаційних ресурсів;
- формування загальнодержавної системи захисту інформації від несанкціонованого доступу та інших загроз;
- розвиток міжнародного співробітництва у сфері інформації та забезпечення інформаційного суверенітету України [23].

Реалізація державної інформаційної політики покладається на органи державної влади загальної та спеціальної компетенції. Право на інформацію, що гарантується громадянам України, юридичним особам та державним органам, передбачає можливість вільного отримання, використання, поширення та

зберігання інформації, необхідної для реалізації їхніх прав, свобод та законних інтересів. Важливо підкреслити, що реалізація права на інформацію не повинна порушувати права та інтереси інших суб'єктів. Кожному громадянину гарантується доступ до інформації, що стосується його особисто, за винятком випадків, передбачених законодавством.

З метою оптимізації державної інформаційної політики в Україні, згідно з Указом Президента «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України"», передбачається розробка проекту Стратегії впровадження національної інформаційної політики [30]. Цей проект має акцентувати увагу на наступних ключових аспектах:

- гарантування інформаційних прав та свобод (створення та впровадження ефективних механізмів реалізації інформаційних прав і свобод громадян, суспільства та держави, які закріплені в Конституції та законах України);

- удосконалення законодавчої бази (подальша модернізація законодавства України в інформаційній сфері з урахуванням сучасних викликів);

- розвиток інформаційної інфраструктури (розбудова національної інформаційної інфраструктури на основі сучасних інформаційних технологій, оптимізація системи інформаційно-аналітичного забезпечення органів державної влади, підвищення конкурентоспроможності вітчизняних виробників інформаційного продукту);

- регулювання інформаційних потоків (визначення чіткого порядку функціонування та механізмів державного контролю за супутниковими, кабельними та комп'ютерними системами передачі інформації);

- формування системи зв'язків з громадськістю (створення єдиної державної системи зв'язків з громадськістю для забезпечення ефективної комунікації між владою та суспільством);

- лібералізація ринку телекомунікацій (подальша лібералізація українського ринку телекомунікацій з урахуванням національних інтересів та запобігання монополізації інформаційних ринків);

- розвиток науково-технічного та кадрового потенціалу (забезпечення науково-технічного та кадрового розвитку інформаційної галузі);

- забезпечення інформаційного суверенітету (зміцнення інформаційного суверенітету України та вдосконалення системи захисту національних інформаційних ресурсів) [30].

До першочергових завдань державної інформаційної політики належать:

- розгляд проекту Концепції роздержавлення засобів масової інформації в Україні;

- забезпечення законодавчої бази для запровадження системи Суспільного телебачення і радіомовлення;

- законодавче врегулювання питань забезпечення конституційних прав громадян на інформацію та захисту журналістів;

- розробка Концепції розвитку телерадіоінформаційного простору України;

- розробка Концепції розвитку глобальних інформаційних мереж в Україні;

- розробка Концепції інформаційної безпеки України;

- розробка Інформаційного кодексу України.

Ці напрямки та завдання відображають стратегічну необхідність у комплексній реформі інформаційної політики України, спрямованої на забезпечення інформаційної безпеки, захист прав громадян та розвиток інформаційного суспільства.

Державна політика в галузі інформаційно-телекомунікаційної інфраструктури зосереджується на кількох ключових напрямках. Насамперед, це стимулювання швидкого розвитку зв’язку, залучення інвестицій в IT-сектор, модернізація телекомунікацій та пошти з акцентом на вітчизняні технології. Важливо інтегрувати їх у глобальні мережі, зокрема Інтернет, та забезпечити широкий доступ до інформаційних ресурсів.

Для ефективної інтеграції України в світовий інформаційний простір необхідно прискорити комп'ютеризацію, особливо в освітніх установах, та розширити доступ до інформаційних ресурсів.

Міжнародне співробітництво в інформаційній сфері, як зазначає Сергій Перепьолкін, базується на низці принципів, що формують правову основу для взаємодії держав. Ці принципи, виражені в нормах міжнародного права, забезпечують цілісність та єдність правового регулювання [12, с. 86].

Серед основних принципів, спільних для міжнародного права, виділяють повагу до державного суверенітету, суверенну рівність держав, співробітництво та сумлінне виконання міжнародних зобов'язань. Окрім того, існують спеціальні принципи, що регулюють конкретні аспекти співпраці, такі як взаємність, добровільність, законність та захист прав та інтересів третіх сторін.

Інформаційна сфера тісно пов'язана з іншими важливими суспільними процесами, що впливають на реалізацію свобод та інтересів громадян. Тому здатність держави ефективно діяти на міжнародній арені як рівноправний суб'єкт є критично важливою. Зовнішній аспект державного суверенітету визначає можливість реалізації національних інтересів, зокрема в інформаційній сфері, в рамках встановлених міжнародних норм.

Україна, володіючи розвиненим інформаційним простором та структурованою інформаційною сферою, використовує ресурси для реалізації своїх національних інтересів як на внутрішній, так і на зовнішній арені. Однак, як слушно зауважує Ярослав Лелет, інформаційний простір відіграє ключову роль у сучасних військово-політичних конфліктах. Інформація, незалежно від її характеру, є стратегічним активом у формуванні національної безпекової доктрини будь-якої держави [1, с. 96].

Згідно з цим дослідником, інформаційна політика України спрямована на забезпечення та функціонування системи інформаційної безпеки. Це особливо актуально в умовах ворожої агресії, де інформація використовується як зброя. Враховуючи можливість маніпуляцій, держави, що стикаються з

інформаційними загрозами, повинні ідентифікувати ці загрози та вживати заходів для їх нейтралізації.

Ефективна реалізація національних цілей в інформаційній сфері можлива лише за умови міжнародної співпраці, обміну досвідом та отримання аналітичної та консультативної допомоги від країн з розвиненими механізмами забезпечення національних інтересів в інформаційному просторі. Інтеграція національного інформаційного простору у світовий є не лише засобом підвищення ефективності міжнародної взаємодії, але й предметом та способом співпраці.

Сучасна міжнародна співпраця в інформаційній сфері базується на договірних засадах або, за їх відсутності, на принципах взаємності, здійснюється в рамках міжнародних організацій, через представників державних органів та на регіональному рівні. Ця діяльність регулюється системою правових норм, що поєднує міжнародне та національне право.

Отже, слід активізувати інформатизацію державних органів, фінансового сектору, впровадження електронного документообігу, комп'ютеризацію архівів та статистики, а також покращити комунікацію між державою та громадянами через онлайн-платформи. Крім того, важливо узгодити українське законодавство у сфері зв'язку з правовими нормами, які прийняті в ЄС.

## 3.2. Контрпропаганда як важливий напрям в забезпеченні інформаційної безпеки України

В умовах інформаційної війни, розв'язаної рф, одним із першочергових завдань є розробка та впровадження ефективних стратегій контрпропаганди. Це зумовлено тим, що тривалий вплив пропагандистських наративів спричиняє деформацію системи цінностей та оцінок, що, своєю чергою, негативно впливає на психічне здоров'я [7].

Пропаганда використовує маніпулятивні методи, такі як селективне подання інформації та сугестивні психологічні техніки, що знижують критичне

мислення. В результаті формується викривлена картина реальності, яка стає фільтром для сприйняття подальшої інформації. Це призводить до накопичення негативних емоційних станів, відчуття безпорадності та втрати сенсу життя, що руйнує психічне здоров'я.

Для вирішення цієї проблеми необхідні системні зміни в соціально-економічній сфері. Стабільність суспільства, що базується на чіткій програмі дій, є запорукою психічного здоров'я громадян. Здорова особистість може розвиватися лише в здоровому суспільстві.

Психічне здоров'я є інтегративним фактором, що визначає збалансованість когнітивних, мотиваційних та емоційно-вольових аспектів особистості. Воно також сприяє підвищенню стресостійкості, мобілізації захисних механізмів організму та формуванню суб'єктивного відчуття благополуччя. Останнє, зокрема, корелює з наявністю стійкої мотивації до подолання наслідків російської агресії, відновлення національної інфраструктури та розробки ефективних стратегій протидії ворожій пропаганді [10].

Термін «контрпропаганда» визначається як сукупність заходів, спрямованих на протидію пропагандистській діяльності. Контрпропаганда, як правило, є реактивною стратегією, що використовує специфічні методи, такі як моніторинг, аналіз, деконструкція джерел та цілей пропаганди, а також виявлення логічних помилок.

Ефективність контрпропаганди, подібно до пропаганди, залежить від її здатності резонувати з емоційними реакціями цільової аудиторії. Цей аспект викликає занепокоєння, оскільки використання емоційного впливу може розглядатися як форма маніпуляції, що приховує справжні наміри суб'єкта впливу.

Зв'язок контрпропаганди з пропагандою є очевидним, адже перша виникає як реакція на другу. Контрпропаганда активізується, коли виявляються ознаки пропагандистського впливу, діючи у захисному режимі. Зазвичай, для ефективного протистояння, контрпропаганда використовує схожі методи та канали поширення інформації, орієнтуючись на ту ж саму цільову аудиторію.

Ефективність контрпропаганди визначається її здатністю:

- застосовувати аналогічні пропагандистським підходи;

- зосереджуватися на тій же аудиторії, що й пропаганда;

- діяти оперативно, щоб нейтралізувати пропагандистський вплив.

Контрпропаганда, хоч і має спільні риси з пропагандою, все ж відрізняється суттєвими характеристиками. Перш за все, вона базується на правді. Це дозволяє завоювати довіру аудиторії, дотримуючись етичних норм у поширенні інформації. Використання неправдивих повідомлень у контрпропаганді може призвести до хаосу та підірвати довіру до опозиції, що вигідно пропагандистам.

Друга важлива характеристика – зрозумілість. Контрпропаганда має бути максимально простою, щоб її могли зрозуміти всі. Складні повідомлення можуть бути проігноровані, особливо людьми, чиє мислення вже зазнало впливу пропаганди. Простота забезпечує однозначне сприйняття інформації та її запам’ятовування.

І, нарешті, швидкість реагування. Контрпропаганда – це відповідь, тому вона має бути оперативною, щоб не дати пропаганді закріпитися в свідомості людей. Своєчасна реакція дозволяє збити хвилю дезінформації. При цьому відповіді мають бути коректними, пропорційними та простими за формою [6, с. 138].

Контрпропаганда не обмежується лише формуванням альтернативних поглядів на пропагандистський контент. Її сутність полягає у цілеспрямованому донесенні інформації, що розкриває брехливість пропагандистських повідомлень та сприяє розвитку критичного мислення в аудиторії, формуючи обережне ставлення до певного типу контенту. Цей процес нівелює довіру до джерел пропаганди, створюючи упереджене негативне ставлення до їхніх повідомлень.

Наприклад, на деокупованих територіях контрпропаганда має на меті надання достовірної інформації про реальні дії окупантів. Таким чином, контрпропаганда – це не лише створення контенту, що протистоїть пропаганді

противника, а й комплекс заходів, спрямованих на інформаційну протидію. Стратегія контрпропаганди повинна бути не лише оборонною, але й мати активний наступальний характер, що сприятиме запобіганню розвитку негативних психоемоційних станів та зневіри в майбутнє серед населення.

З огляду на викладене, для підтримки психологічного здоров'я громадян доцільно виокремити декілька напрямків протидії пропаганді.

Перший напрямок – формування стійкості українського суспільства, зокрема мешканців звільнених територій, до впливу ворожої пропаганди. Цей підхід базується на тому, що інформація, яка суперечить особистим переконанням, часто відкидається [3, с. 122]. Наприклад, складно миттєво змінити релігійні погляди людини або перетворити брехуна на чесну особистість. Крім того, зіткнення з інформацією, що кардинально відрізняється від усталеної системи цінностей, може призвести до фрустрації – емоційного стану, що характеризується відчуттям безвиході та дезорганізацією свідомості. Тому людина часто намагається уникнути такої інформації для збереження психологічного балансу.

Цим явищем можна пояснити складнощі у спілкуванні з людьми, які довгий час перебували під впливом російської пропаганди. Вони відкидають логічні аргументи та повторюють завчені пропагандистські тези. Зміна таких усталених поглядів вимагає тривалого та системного переконання.

Важливо зазначити, що формування спільних моральних цінностей, які визначають критерії оцінки дійсності, є завданням суспільства, до якого людина відчуває приналежність. Хоча формування стійкості до ворожої пропаганди на базовому рівні доцільно також для громадян інших країн.

З метою протидії дезінформації та пропаганді, необхідно зосередитися на комплексі заходів, спрямованих на формування стійкого інформаційного простору. Важливо забезпечити населення достовірною інформацією, яка не лише відображає реальний стан речей, але й сприяє усвідомленню спільних цінностей та пріоритетів. Це дозволить зміцнити відчуття приналежності до спільноти, де кожен відчуває себе частиною цілого.

Окрім цього, необхідно активно транслювати цінності, що об’єднують українське суспільство. Пошук та популяризація таких цінностей, як гідність, свобода, повага та толерантність, сприятимуть формуванню позитивного образу українця, який викликає повагу та довіру.

Важливим аспектом є формування громадянської ідентичності, що базується на активній громадянській позиції, свободі та повазі до прав інших. Йдеться не про вседозволеність, а про усвідомлення відповідальності за власні дії та повагу до потреб і прагнень інших членів суспільства. Такий підхід сприятиме побудові гармонійного суспільства, де кожен відчуває себе повноцінним громадянином [13, с. 68].

Стратегія протидії ворожій інформаційній агресії передбачає не лише активне поширення власних наративів, але й ретельний аналіз та нейтралізацію пропаганди противника. Цей підхід, що часто називають контрпропагандою, зосереджується на виявленні та спростуванні дезінформації, спрямованої на дестабілізацію суспільної думки.

На практиці це означає, що ми реагуємо на інформаційні атаки, намагаючись:

-досягти тих самих аудиторій, які стали об’єктом ворожої пропаганди;

- викликати емоційні реакції, достатні для нейтралізації негативного впливу;

- конкретно відповідати на питання та теми, підняті пропагандистами.

В Україні цей напрям роботи набув значного поширення, охоплюючи широкий спектр діяльності:

- спростування викривлених інтерпретацій історичних подій;

- деконструкція міфів про переваги колишнього радянського союзу;

- критика завищеної оцінки ролі ворожої культури;

- викриття дезінформації щодо поточних подій;

- аналіз справжніх мотивів проросійських публічних діячів.

Ці дії спрямовані на захист інформаційного простору України та формування стійкого імунітету до ворожої пропаганди.

У контексті протидії інформаційним маніпуляціям, що поширюються ворожими силами, ефективними виявилися підходи, які дозволяють розкрити абсурдність та маніпулятивність пропаганди [3, с. 125]. Зокрема, використання сатири та іронії дає змогу висміяти нелогічність та суперечливість наративів, що поширюються. Аналогії з відомими історичними подіями або ситуаціями допомагають продемонструвати шаблонність та передбачуваність дій противника, виявляючи їхні справжні наміри. Важливим аспектом є аналіз причин та мотивів, що лежать в основі створення та поширення пропагандистських повідомлень. Розуміння контексту та цілей, які переслідує ворог, дає змогу ефективно протидіяти їхньому впливу. Нарешті, виявлення методів та каналів, які використовуються для розповсюдження дезінформації, дозволяє блокувати їхнє поширення та захистити інформаційний простір від ворожих маніпуляцій [17].

Одним із перспективних напрямів протидії ворожій пропаганді є проактивна контрпропаганда. Цей підхід передбачає не лише реагування на вже поширені дезінформаційні наративи, але й попередження їх появи. Зокрема, йдеться про прогнозування можливих векторів пропаганди противника, особливо на деокупованих територіях, та завчасну підготовку відповідного інформаційного контенту для населення.

Алгоритм реалізації проактивної контрпропаганди:

- моніторинг: систематичне відстеження інформаційного простору з метою виявлення потенційних «точок напруги», сигналів активності ворога та аналіз вразливих, неочевидних аспектів;

- аналіз та прогнозування: на основі виявлених тенденцій здійснюється комплексний аналіз ситуації з виокремленням критичних сфер, що потребують першочергової уваги. Також визначаються необхідні експерти для розробки сценаріїв протидії;

- розробка сценарію: формування кількох варіантів реагування на прогнозовані загрози та вибір оптимальної стратегії протидії;

- реалізація плану: впровадження обраного сценарію з урахуванням наявних ресурсів та забезпечення оперативного реагування на можливі зміни ситуації;

- рефлексія: критичний аналіз результатів реалізації плану, оцінка ефективності застосованих заходів та їх відповідності поставленим цілям [7].

Такий підхід дозволяє не лише мінімізувати негативний вплив ворожої пропаганди, але й активно формувати інформаційний порядок денний, сприяючи зміцненню інформаційної стійкості суспільства.

Отже, проблема протидії ворожій пропаганді вимагає комплексного підходу, що охоплює не лише боротьбу з самим пропагандистським контентом, але й вплив на тих, хто його створює, та канали його поширення.

Психологічні технології контрпропаганди, спрямовані на протидію багаторічному деструктивному пропагандистському апарату рф, можуть включати:

1. Систематичне розвінчування ворожих інформаційних маніпуляцій.

2. Активне поширення достовірної інформації.

3. Розробка та впровадження інформаційних стратегій, що сприяють формуванню позитивного інформаційного простору, який підтримує психічне здоров’я громадян.

4. Комплексне застосування різних напрямів контрпропаганди, таких як формування стійкості українського суспільства, традиційна контрпропаганда та проактивна контрпропаганда, для створення ефективної системи запобігання та протидії ворожій пропаганді.

Ці заходи, в сукупності, мають сприяти розробці та впровадженню оптимізованої системи запобігання та протидії поширенню ворожої пропаганди, яка негативно впливає на психічний стан населення.

### 3.3. Інформаційна безпека майбутнього: напрями, інструменти, методи

В епоху стрімкої інформатизації суспільства забезпечення інформаційного суверенітету особистості стає ключовим завданням держави. Інформаційна безпека особистості розглядається як стан захищеності її психіки та свідомості від деструктивних інформаційних впливів, таких як маніпуляція, дезінформація та спонукання до самогубства.

Інформаційно-психологічна безпека особистості визначається через:

- здатність особистості, завдяки належній теоретичній та практичній підготовці, забезпечувати захист та реалізацію своїх життєво важливих інтересів, а також гармонійний розвиток, незалежно від інформаційних загроз;

- можливість держави створювати умови для гармонійного розвитку та задоволення інформаційних потреб особистості, незалежно від наявності інформаційних загроз;

- гарантування, розвиток та використання інформаційного середовища в інтересах особистості;

- захищеність від різноманітних інформаційних небезпек.

Аналізуючи сучасні тенденції, можна констатувати, що розвиток технологій та методик впливу на свідомість та підсвідомість людини випереджає темпи формування ефективних механізмів протидії цим деструктивним впливам. Це створює серйозну загрозу для інформаційно-психологічної безпеки особистості [33].

Аналіз вибірковості сприйняття інформації показує, що індивід, як правило, обробляє лише ту частину даних, яка узгоджується з його особистими переконаннями, психологічними установками та перевагами. З огляду на це, суб’єкти інформаційного впливу прагнуть враховувати ступінь готовності аудиторії до сприйняття конкретної інформації, щоб максимізувати ефективність впливу на індивідуальну та суспільну свідомість.

Об’єкти маніпулятивного впливу можна класифікувати за такими категоріями:

- мотиваційна сфера (потреби, інтереси, схильності, що стимулюють активність);

- регулятивна сфера (групові норми, самооцінка (почуття власної гідності, самоповага, гордість), суб’єктивні відносини, світогляд, переконання, вірування, ціннісні та операційні установки);

- когнітивна сфера (інформаційні структури, зокрема інформаційно-орієнтовна основа поведінки);

- операційна сфера (способи мислення, стилі поведінки та спілкування, звички, вміння та навички);

- психічна сфера (фонові, функціональні та емоційні стани) [3, с. 125].

Таким чином, динамічний розвиток інформаційно-комунікаційних технологій створює потенційну загрозу їх використання для реалізації різноманітних форм та методів маніпуляції, а також для здійснення негативного психологічного впливу на окремих осіб з метою досягнення недоброчесних цілей. Це обумовлює необхідність для держави та громадянського суспільства вдосконалення стратегій та інструментів забезпечення інформаційної безпеки громадян в умовах сучасного інформаційного простору.

У сучасних умовах глобалізації інформаційного простору, боротьба з деструктивним інформаційним впливом вимагає комплексного підходу. Міжнародний досвід демонструє, що ефективне протистояння маніпулятивним технологіям включає не лише обмеження агресивної реклами та політичної пропаганди, але й формування особистої інформаційної гігієни.

В контексті державної інформаційної політики, пріоритетним завданням є інтеграція національних інформаційних систем у міжнародні структури, що спеціалізуються на протидії негативному інформаційному впливу. Паралельно, необхідна адаптація законодавчої бази до міжнародних стандартів та створення дієвих механізмів правового регулювання інформаційних процесів. Важливим аспектом є налагодження ефективної взаємодії між державними органами та

інститутами громадянського суспільства у процесі формування та реалізації інформаційної політики.

Інформаційні структури органів державної влади повинні зосередитися на моніторингу інформаційних потоків, забезпеченні суспільства об'єктивною та вичерпною інформацією, а також на наданні фахових коментарів щодо актуальних подій. Систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів є необхідним для формування довіри до державних інституцій.

Окрім правових та регуляторних механізмів, важливим елементом протидії шкідливому інформаційному впливу є розвиток критичного мислення та медіаграмотності в суспільстві. Здатність до аналізу інформації та виявлення маніпуляцій стає ключовим фактором в умовах інформаційного перенасичення. Держава повинна активно сприяти розвитку освіти та культури, створюючи умови для формування інформаційно компетентних громадян [4, с. 53].

Ефективний захист інформаційних систем вимагає застосування комплексного підходу, що охоплює всі аспекти безпеки. Абсолютно невразливих систем не існує, тому метою є створення механізмів, вартість обходу яких перевищує цінність захищеної інформації. Впровадження програмних засобів безпеки, інтегрованих у структуру програмного забезпечення, є необхідним для реалізації функцій захисту.

Основні принципи забезпечення інформаційної безпеки:

1. Законність: Дотримання законодавчих норм, зокрема захист персональних даних, забезпечення правомірного доступу та обробки інформації, а також відповідність чинному законодавству України у сфері інформаційної безпеки.

2. Баланс інтересів: Узгодження інтересів особи, суспільства та держави, включаючи державне управління інформаційною сферою, захист від інформаційних загроз та забезпечення інформаційних прав і свобод.

3. Комплексність: Застосування сукупності організаційних, технічних та програмних заходів захисту, з урахуванням усіх аспектів інформаційної безпеки,

таких як конфіденційність, цілісність, доступність, незаперечність та підзвітність.

4. Системність: Постійне вдосконалення системи інформаційної безпеки, створення багаторівневого захисту та забезпечення єдності й взаємозв'язку всіх компонентів системи.

Дотримання цих принципів та впровадження комплексної стратегії захисту дозволяє мінімізувати ризики, пов'язані з кібератаками, забезпечити безперебійну роботу та зберегти конфіденційність інформації.

Окрім технічних заходів, важливим є розвиток «інформаційного імунітету» в суспільстві, що передбачає здатність ігнорувати непотрібну інформацію та встановлювати психологічні бар'єри проти маніпулятивних повідомлень.

У сучасному інформаційному просторі здатність до ефективного відбору даних стає ключовою навичкою для кожної людини. Цей підхід до регулювання інформаційного впливу є більш продуктивним, ніж пряме втручання держави з метою обмеження або блокування певних інформаційних потоків. Він дозволяє індивіду самостійно визначати пріоритетність інформації та свідомо контролювати її обсяг [17]. Це сприяє трансформації людини з пасивного об'єкта маніпуляцій у активного суб'єкта, що формує власне інформаційне середовище. У такому контексті вже не ЗМІ нав'язують свою думку, а людина сама фільтрує інформацію, ігноруючи непотрібний контент, наприклад, відмовляючись від купівлі упередженої преси, перегляду політичних новин або відвідування певних веб-сайтів.

Цей феномен можна назвати «контрманіпуляцією», що означає свідоме обмеження доступу до інформаційних та рекламних повідомлень. Контрманіпуляція є соціальним явищем, яке потребує індивідуального розвитку у кожної людини, і може розглядатися як елемент виховання.

Теоретичною основою для такого виховання є медіапедагогіка – наука та навчальна дисципліна, спрямована на формування критичного ставлення до ЗМІ, компетентного та відповідального їх використання. Її мета – ознайомити

громадян з роллю ЗМІ в демократичному суспільстві, їх позитивним та негативним впливом, а також навчити орієнтуватися у складному інформаційному потоці та протистояти маніпуляціям. Як зазначив Елвін Тоффлер у своїй праці «Шок майбутнього», для захисту від інформаційного перевантаження необхідно навчитися створювати «зони стабільності» у постійно мінливому середовищі.

Отже, сучасна інформаційна епоха відкриває перед суспільством та кожним з нас безліч можливостей для використання інформації з метою покращення особистого добробуту. Проте, разом з цим виникають і ризики неправомірного, а іноді й шкідливого застосування інформації, що може порушувати інформаційний суверенітет як окремої особистості, так і суспільства в цілому. Тому, на мою думку, захист інформаційного суверенітету, побудова ефективної системи інформаційної безпеки та розробка дієвих стратегій протидії медіазагрозам повинні стати першочерговими завданнями для державних органів та громадських організацій.

# ВИСНОВКИ

Вивчивши та проаналізувавши форми та інструменти забезпечення інформаційної політики України автор прийшов до таких висновків:

Перше, інформаційна безпека – це, по суті, комплекс заходів, спрямованих на захист інформаційних ресурсів від різних загроз, починаючи від банального несанкціонованого доступу і закінчуючи повним знищенням даних. Це не просто набір інструментів, а ціла система, що охоплює технологічні, організаційні та навіть правові аспекти.

Інформаційно безпека полягає в стані захищеності інтересів держави, її суверенітету та територіальної цілісності в інформаційному просторі. Йдеться про комплекс заходів або здатність системи ефективно протистояти різного роду загрозам – як тим, що пов’язані з технічними чинниками, так і тим, що мають психологічний вплив. Головна мета такого захисту – не допустити дестабілізації.

Тому інформаційна безпека – це не просто модне слово, а необхідність. Вона вимагає не лише використання сучасних технологій, але й формування культури безпеки серед користувачів та фахівців. Кожен, хто працює з інформацією, повинен розуміти свою відповідальність і дотримуватися правил безпеки. Це складна, але надзвичайно важлива задача, яка вимагає постійного вдосконалення та адаптації до нових викликів.

Друге, державна політика в галузі інформаційної безпеки являє собою комплексний підхід, що включає стратегії, законодавчі акти, програми та регуляторні заходи. Їхня мета – захист інформації, критично важливої для національних інтересів, суспільства та громадян. Ця політика спрямована на забезпечення стабільності інформаційного простору, захист прав та свобод громадян, гарантування конфіденційності та цілісності даних, а також на підтримку економічного розвитку та стимулювання інноваційного потенціалу країни.

Третє, в умовах триваючого збройного конфлікту та агресивних дій з боку російської федерації, забезпечення інформаційної безпеки України набуває

критичного значення для збереження національного суверенітету. До ключових викликів, що потребують, на нашу думку, негайного вирішення, є кібернетичні атаки, дезінформаційні кампанії, технологічна вразливість та психологічний тиск на населення.

Для ефективного протистояння цим загрозам необхідний комплексний підхід, що включає в себе модернізацію систем кіберзахисту, розробку стратегій протидії дезінформації, оновлення технічної інфраструктури та зміцнення психологічної стійкості громадян. Успішне забезпечення інформаційної безпеки України можливе лише за умови скоординованих дій держави, громадянського суспільства та міжнародних партнерів, що є необхідною умовою для збереження національної безпеки та суверенітету.

Четверте, на сьогоднішній день інформаційна війна є невід'ємною складовою військового конфлікту росії проти України, що ведеться цілеспрямовано та інтенсивно. Унікальність інформаційної війни полягає не лише у використанні передових технологій, а й в тому, що це непідконтрольний ресурс, який важко піддати правовій регламентації. Ворожі медіа використовують різноманітні методи пропаганди для маніпуляції населенням України, викривлення правдивої інформації, дискредитації української влади та збройних сил, зокрема: містифікацію, міфотворчість, фільтрацію інформації, маніпулювання традиційними символами та стереотипами, засоби гіперболізації. Головною умовою протистояння таким ворожим атакам є формування ефективної системи української контрпропаганди, забезпечення інформаційної безпеки населення, а також розвиток критичного мислення у кожного громадянина України.

П'яте, важливою складовою є забезпечення стабільності інформаційної структури. Цифрова трансформація виступає адекватною відповіддю на актуальні інформаційні та кіберзагрози, як на глобальному рівні, так і в Україні. Інтеграція цифрової трансформації в міжнародні процеси спрямована на посилення інформаційних комунікацій, розробку стратегій і концепцій, а також

на забезпечення безпеки та адаптацію політичних рішень в умовах воєнного стану в Україні.

Тому очевидною потребою на сучасному етапі є необхідність прийняття та ухвалення політичних рішень і трансформації, яка повинна стати ефективним способом протидії інформаційним загрозам з боку ворога. Україна, в подальшому, повинна постійно вдосконалювати законодавство в сфері інформаційної безпеки, такий підхід обумовлений європейським вибором нашої країни та побудови стійкого цифрового суспільства, орієнтованого на людину.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біленчук П. Д. Правові засади інформаційної безпеки України : монографія. Харків, 2018. 289 с.

2. Білько С. Формування інформаційної безпеки національної економіки : дис. … д-ра філософії в галузі економіки : 051. Полтава, 2023. 211 с.

3. Войтко О., Кацалап В., Рахімов В. Аналіз особливостей маніпуляції як інструмент психологічного впливу на свідомість. *Сучасні інформаційні технології у сфері безпеки та оборони* . 2019. Т. 2, № 35. С. 121–126.

4. Гнатюк С.Л. Особливості захисту персональних даних у сучасному кіберпросторі : правові та техніко-технологічні аспекти : аналітична доповідь. Київ, 2014. С. 52-55. URL: //www.niss.gou.ua/content/articles/druk_Gnatuk 1/indd-8b6f2pdf.

5. Голованова Н. Інформаційна політика України в умовах війни (архетипний підхід). Наукові перспективи. 2022. № 6. С. 57–70.

6. Горбань Ю. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. № 1. С. 136–141

7. Денисюк Ж. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В.І. Вернадського. Серія «Державне управління»* . 2021. Т. 32 (71), № 2. С. 46–51.

8. Джерела інформації українців у 2023 році. *Uchoose*. URL: https://surl.lu/yfjznd (дата звернення: 29.04.2025).

9. Динаміка довіри соціальним інституціям у 2021-2024 роках. *Київський міжнародний інститут соціології.* URL: https://surli.cc/sfibmm (дата звернення: 12.04.2025).

10. Драпушко Р. Г., Горінов П. В. Сучасні виклики і загрози правової культури молоді. *Аналітично-порівняльне правознавство*. 2021. № 4. С. 18–22.

11. Золотар О. О. Інформаційні революції: соціально-правове значення. *Публічне право*. 2017. № 2. С. 40–46.

12. Інформаційна безпека держави : Конспект лекцій / уклад.: Ю. Ткач, С. Семендяй. Чернігів : НУ «Черніг. політехніка», 2022. 133 с.

13. Калініченко Б. Визначальні напрями формування стратегії протистояння інформаційній війні. *Держава і право. Серія : Політичні науки*. 2019. № 83. С. 61–73.

14. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 05.03.2025).

15. Ліга закон. Важливе судове рішення ухвалене під час воєнного стану. URL: https://surl.li/brhrvn (дата звернення: 04.04.2025).

16. Меренюк С., Меренюк Х. Україно-російська гібридна війна. *Україна в умовах трансформації міжнародної системи*. Львів, 2019. С. 47–51.

17. Неправда законна й незаконна. Межі боротьби проти дезінформації за версією ОБСЄ. *Детектор Медіа*. URL: https://surl.lu/urytlf (дата звернення: 31.03.2025).

18. Нечипорук Я. Правовий статус блогера. *Юридичний науковий електронний журнал.* 2022. № 9. С. 172–176. URL: http://lsej.org.ua/9_2022/41.pdf (дата звернення: 26.03.2025).

19. Парфенюк І. Інструментарій інформаційних війн: традиційні та новітні засоби. *Вісник Книжкової палати*. 2019. № 1. С. 7–10.

20. Почепцов Г. Пропаганда будує світ, водночас руйнуючи його. *StopFake*. URL: https://surl.li/xbkwkn (дата звернення: 20.03.2025).

21. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах : Наказ Департаменту спец. телекомунікац. систем та зах. інформації Служби безпеки України від 24.12.2001 № 76 : станом на 8 лип. 2006 р. URL: https://zakon.rada.gov.ua/laws/show/z0027-02#Text (дата звернення: 26.03.2025).

22. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 12.04.2025).

23. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 15 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 16.05.2025).

24. Про Концепцію Національної програми інформатизації : Закон України від 04.02.1998 № 75/98-ВР : станом на 1 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/75/98-вр#Text (дата звернення: 17.04.2025).

25. Про медіа : Закон України від 13.12.2022 № 2849-IX. URL: https://ips.ligazakon.net/document/T222849 (дата звернення: 09.04.2025).

26. Про національну безпеку України : Закон України. URL: https://ips.ligazakon.net/document/JH6841AA (дата звернення: 09.04.2025).

27. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядж. Каб. Міністрів України від 02.12.2020 № 1556-р : станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 17.04.2025).

28. Стратегія інформаційної безпеки : Указ Президента України від 28.12.2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 12.04.2025).

29. Указ президента України №1193/2001. *Президент України*. URL: https://www.president.gov.ua/documents/11932001-231.

30. Українські медіа, ставлення та довіра у 2023 році. *Детектор медіа*. URL: https://detector.media/infospace/article/218819/2023-11-01-ukrainski-media-stavlennya-ta-dovira-u-2023-rotsi/ (дата звернення: 18.02.2025).

31. Фещенко І. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. 2021. Вип. 13 (1). С. 96–103.

32. Frizell J. War and modern taxation. *Global Taxation*, 2022. Vol. 1. P. 43–66

33. Oporaua. Медіаспоживання українців в умовах повномасштабної війни. Опитування ОПОРИ. URL: https://surl.li/hqlicv.