МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний педагогічний університет імені М.П. Драгоманова

Історичний факультет

Кафедра міжнародних відносин та регіональних студій

Дудник Ярослав Васильович

СУЧАСНІ ІНФОРМАЦІЙНІ ВІЙНИ НА ЄВРОПЕЙСЬКОМУ ГЕОПРОСТОРІ

Кваліфікаційна робота

на здобуття освітнього рівня «бакалавр»

за спеціальністю 291 – Міжнародні відносини, суспільні комунікації та регіональні студії

Науковий керівник:

_____

Київ – 2025

ЗМІСТ

ВСТУП

У сучасному світі інформаційні війни перетворилися на одну з провідних форм ведення конфліктів, що мають значний вплив не лише на окремі держави, а й на міжнародну безпеку в цілому. З розвитком цифрових технологій інформація стала потужним інструментом, здатним формувати громадську думку, впливати на політичні процеси, а також змінювати баланс сил на глобальній арені. Особливу актуальність ця проблема набуває в європейському геопросторі — регіоні з багатою історією взаємодії численних народів, культур і політичних систем, де перетинаються інтереси як західних демократичних країн, так і східних геополітичних гравців. Ця різноманітність створює сприятливі умови для виникнення та ескалації інформаційних конфліктів.

Інформаційні війни у Європі характеризуються використанням широкого спектру технологічних засобів — від традиційних медіа до сучасних цифрових платформ, таких як соціальні мережі, месенджери, блоги і відеохостинги. Завдяки цьому з’явилась можливість здійснювати цілеспрямовані маніпуляції суспільною свідомістю, поширювати дезінформацію та пропаганду, розпалювати політичні та соціальні протистояння, а також впливати на виборчі процеси. Додатково, активна участь недержавних акторів — хакерських груп, інформаційних агентств, а також приватних компаній з розробки цифрових технологій — ускладнює ситуацію, роблячи інформаційний простір більш непередбачуваним та вразливим.

Ці процеси призводять до значного послаблення традиційних державних інституцій, підриву довіри до органів влади, розколу суспільства на внутрішньополітичному рівні та дестабілізації міждержавних відносин. Геополітичне загострення, зокрема у контексті конфліктів на Сході Європи, додатково підсилює загрози, пов’язані з інформаційними війнами. Саме тому

вивчення сучасних інформаційних війн стає надзвичайно важливим для науки, яка покликана не лише описувати і аналізувати ці процеси, але й розробляти ефективні механізми протидії загрозам. Практичне значення таких досліджень проявляється у формуванні національної та міжнародної політики безпеки, удосконаленні систем захисту інформаційного простору та підвищенні рівня медіаграмотності суспільства.

Об’єктом дослідження є сучасні інформаційні війни як форма геополітичної боротьби у цифровому просторі, що охоплюють механізми, інструменти та наслідки інформаційних операцій на території європейського геопростору.

Предметом дослідження виступають інформаційні конфлікти, їхні технології, стратегії та тактики ведення на прикладі основних учасників і зон конфронтації в Європі, а також вплив цих процесів на безпекову ситуацію та суспільно-політичні процеси.

Метою дослідження є комплексний аналіз сучасних інформаційних війн на європейському геопросторі, виявлення їхніх особливостей, загроз та механізмів протидії, а також формулювання рекомендацій для забезпечення інформаційної безпеки в регіоні.

Для досягнення поставленої мети необхідно розв’язати такі завдання:

- Охарактеризувати поняття, сутність і види інформаційних війн.
- Проаналізувати геополітичний контекст та основних учасників інформаційних конфліктів у Європі.
- Вивчити методи та технології інформаційних операцій, що застосовуються на європейському континенті.
- Дослідити наслідки інформаційних війн для безпеки, політики і суспільства в регіоні.

- Розробити рекомендації щодо ефективних заходів протидії інформаційним загрозам.

Методологічною основою дослідження є комплексний підхід, який поєднує в собі методи системного аналізу, порівняльного аналізу, контент-аналізу, а також елементи геополітичного та соціологічного дослідження. Особливе значення має використання методів інформаційного моніторингу та аналізу цифрових медіа, що дозволяє оцінити вплив інформаційних операцій у реальному часі.

Наукова новизна дослідження полягає у всебічному комплексному аналізі сучасних інформаційних війн, що враховує їхню специфіку саме в європейському геопросторі. Вперше узагальнено методи та інструменти інформаційних конфліктів з урахуванням новітніх технологій та цифрових платформ. Запропоновано нові підходи до класифікації інформаційних загроз і механізмів протидії, що відповідають викликам сучасності.

Практична цінність роботи полягає у розробці рекомендацій для державних органів, аналітичних центрів і спецслужб щодо підвищення ефективності боротьби з інформаційними загрозами. Отримані результати можуть бути використані при формуванні державної політики інформаційної безпеки, розробці систем протидії дезінформації, а також у сфері освіти та підвищення медіаграмотності населення.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНИХ ВІЙН У СИСТЕМІ МІЖНАРОДНИХ ВІДНОСИН

1.1. Поняття та сутність інформаційної війни

Інформаційна війна є одним із найактуальніших і найскладніших явищ сучасної міжнародної політики, що значною мірою трансформує традиційні підходи до безпеки, конфліктів і взаємодії держав. Сутність інформаційної війни полягає у цілеспрямованому використанні інформаційних ресурсів і комунікаційних технологій для впливу на політичні, соціальні, економічні процеси в цільовому середовищі з метою досягнення стратегічних або тактичних цілей. Поняття інформаційної війни виникло у другій половині XX століття на фоні стрімкого розвитку інформаційних технологій, поширення глобальних мереж та посилення ролі інформації як ключового фактора впливу в системі міжнародних відносин. Інформація, яка раніше розглядалася як допоміжний або другорядний ресурс, сьогодні стала одним із найважливіших стратегічних ресурсів держав і недержавних акторів, що безпосередньо впливає на баланс сил у світовій політиці.

Інформаційна війна відрізняється від традиційних форм воєнної діяльності тим, що вона не передбачає прямого застосування збройних сил, а орієнтована на досягнення цілей через зміни у свідомості та поведінці населення, політичних еліт, військових структур і суспільства загалом. Основна мета таких дій полягає у створенні вигідного інформаційного середовища, в якому противник втрачає можливість адекватно сприймати реальність, приймати виважені рішення та реалізовувати власні стратегічні інтереси. Таким чином, інформаційна війна — це інструмент досягнення влади і контролю, що працює у сфері ідей, свідомості та інтелектуального простору.

Вивчення феномену інформаційної війни у науковій українській літературі набуло значного розвитку в останні десятиліття, що пов’язано з посиленням інформаційних викликів у контексті сучасних міжнародних відносин та безпеки України. Значний внесок у теоретичне осмислення інформаційної війни зробили такі українські вчені, як В. І. Нестуля, О. М. Савченко, І. В. Таран, А. П. Тараненко та інші, які розглядають це явище як складну багатовимірну систему впливу на інформаційне поле держави та суспільства[1,2,3].

В. І. Нестуля у своїх роботах акцентує увагу на тому, що інформаційна війна є не лише засобом політичного впливу, але й формою гібридного конфлікту, де інформація і маніпуляції з нею стають ключовими елементами боротьби за владу і контроль. Автор підкреслює важливість розуміння інформаційної війни як окремої складової сучасної безпеки, що потребує спеціалізованих підходів для її виявлення, оцінки та протидії. Нестуля виділяє інформаційний вплив як комплекс дій, спрямованих на зміну поведінкових моделей та свідомості населення, що створює додаткові загрози національній стабільності[4].

О. М. Савченко у своїх дослідженнях звертає увагу на роль медіа і комунікаційних технологій у формуванні інформаційного простору. Він детально аналізує механізми пропаганди, дезінформації та психологічних операцій, які використовуються в інформаційній війні, та їхній вплив на громадську думку і суспільну свідомість. Особливо важливим у роботах Савченка є висвітлення специфіки інформаційної війни в умовах сучасних технологій, зокрема, соціальних мереж, які кардинально змінили способи поширення інформації та методи маніпулювання нею.

І. В. Таран у низці публікацій розглядає інформаційну війну в контексті національної безпеки України, підкреслюючи необхідність системного підходу до її вивчення і протидії. Автор аналізує інформаційні загрози як компонент

гібридної агресії, спрямованої на дестабілізацію політичної системи, розкол суспільства та послаблення державного суверенітету. Таран наголошує на важливості інтеграції інформаційної безпеки в загальну систему національної безпеки та міжнародних стандартів, що є ключовим фактором збереження державної цілісності[5].

А. П. Тараненко, розглядаючи інформаційну війну з позиції соціально-психологічних аспектів, вказує на маніпулятивний характер інформаційного впливу, спрямованого на зміну ціннісних орієнтацій, поведінкових моделей та соціальних установок у різних верствах населення. Автор наголошує на необхідності підвищення інформаційної грамотності громадян як одного з найважливіших чинників протидії інформаційним загрозам[6].

Загалом, внесок українських дослідників у теорію інформаційної війни сприяє не лише кращому розумінню сутності та механізмів цього явища, але й розробці практичних рекомендацій щодо формування ефективної інформаційної політики держави. Ці наукові доробки є особливо актуальними в умовах посилення інформаційної агресії, з якою сьогодні стикається Україна на міжнародній арені, що вимагає комплексного і системного підходу до забезпечення інформаційної безпеки на всіх рівнях.

Важливо підкреслити, що інформаційна війна включає комплекс методів і прийомів, серед яких ключовими є пропаганда, дезінформація, психологічні операції, кібернапади, медіаманіпуляції, а також використання соціальних мереж і цифрових платформ для поширення контрольованої інформації. Пропаганда, як складова інформаційної війни, спрямована на формування у населення певної системи цінностей, переконань та емоційного ставлення, що сприяє підтримці політики агресора або послаблює опір. Дезінформація полягає у свідомому поширенні неправдивих або спотворених даних з метою заплутати

опонента, посіяти недовіру і розділити суспільство. Психологічні операції спрямовані на вплив на моральний стан військових, політичних лідерів і громадськості, знижуючи їх бойовий дух, впевненість у власних силах та волю до опору.

Суттєвим елементом інформаційної війни є кіберпростір, який сьогодні виступає як окреме поле битви. Кібероперації включають атаки на інформаційні системи, мережі комунікацій, бази даних, що дозволяє порушувати роботу критичної інфраструктури, зірвати комунікації і контролювати потоки інформації. Таким чином, технічний аспект інформаційної війни стає не менш важливим, ніж ідеологічний або психологічний. Застосування сучасних цифрових технологій, штучного інтелекту, автоматизованих систем поширення інформації значно підвищує ефективність таких дій і робить їх важкозахисними.

Інформаційна війна у системі міжнародних відносин є частиною ширшого явища — гібридної війни, яка поєднує традиційні військові дії з нетрадиційними методами впливу, серед яких інформаційні операції мають центральне місце. Гібридний характер таких конфліктів полягає в одночасному застосуванні збройної сили, економічного тиску, політичного шантажу та інформаційної агресії, що дозволяє державам і недержавним акторам діяти ефективно та асиметрично, уникаючи прямого військового протистояння, яке може призвести до масштабних втрат і міжнародного засудження[15].

Особливістю сучасних інформаційних війн є їх глобалізація і мультиплатформенність, що полягає у можливості оперативного поширення інформації у будь-якій точці світу через інтернет і соціальні мережі. Територіальні межі перестають відігравати визначальну роль, оскільки інформаційний простір охоплює всі сфери суспільного життя і міжнародного діалогу. Це породжує значні виклики для національних систем безпеки, які

змушені адаптуватися до нових умов і розробляти ефективні механізми захисту інформаційного простору.

Інформаційна війна також має глибокі соціально-політичні наслідки. Вона підриває довіру громадян до державних інститутів, розколює суспільство, сприяє поширенню радикалізму і екстремізму. Внаслідок поширення дезінформації відбувається спотворення суспільної свідомості, що ускладнює прийняття об'єктивних політичних рішень і підриває легітимність політичної влади. На міжнародному рівні це призводить до ескалації конфліктів, підвищення напруженості у відносинах між державами, порушення норм міжнародного права і послаблення системи колективної безпеки[2].

З огляду на викладене, визнання інформаційної війни як окремого виду збройного конфлікту є важливим кроком для формування міжнародно-правового регулювання і розробки відповідних політик безпеки. Однак відсутність чітких та загальноприйнятих норм створює прогалини у системі міжнародного права, що ускладнює відповідальність за інформаційні агресії та ускладнює співпрацю між державами у протидії цим загрозам[6].

Отже, інформаційна війна є складним багатовимірним процесом, що поєднує технологічні, психологічні та політичні аспекти впливу і вимагає від держав нових підходів до забезпечення безпеки. Вона суттєво змінює парадигму сучасних міжнародних відносин, встановлюючи нові правила гри у сфері влади, контролю і конфліктів. Усвідомлення її сутності і механізмів є необхідною умовою для розробки ефективних стратегій захисту на національному та міжнародному рівнях.

1.2. Основні інструменти та методи інформаційного впливу

Інформаційна війна неможлива без застосування різноманітних інструментів та методів інформаційного впливу, які спрямовані на формування, зміну або послаблення суспільної думки, політичних рішень і стратегічної поведінки держав, організацій та окремих індивідів. Важливо зазначити, що інструменти інформаційного впливу охоплюють широкий спектр засобів і технологій, які за допомогою маніпуляції інформацією створюють у свідомості цільової аудиторії бажаний образ реальності або дезорієнтують її, послаблюючи спроможність приймати адекватні рішення.

Серед основних інструментів інформаційного впливу виділяються медіа ресурси — засоби масової інформації (телебачення, радіо, друковані видання), цифрові платформи (соціальні мережі, блоги, форуми) та спеціалізовані інформаційні агенції, які здатні формувати масову свідомість. Важливо, що в сучасних умовах цифровізація інформаційного простору суттєво розширила можливості поширення інформації, зокрема, завдяки соціальним мережам, що надають миттєвий доступ до аудиторії мільйонів користувачів та дозволяють створювати так звані «інформаційні бульбашки» із спрямованою дезінформацією або пропагандою.

Ось приклад таблиці 1.1. що узагальнює наведений текст про методи інформаційного впливу, поділені на прямі та непрямі

Таблиця 1.1. Методи інформаційного впливу

Категорія методів	Опис	Приклади
Прямі методи	Відкрите поширення інформації з чіткою метою впливу на аудиторію.	Офіційна пропаганда, публічні заяви, інформаційні кампанії.
Непрямі методи	Маніпулятивні технології, що використовують приховані або непрямі способи впливу.	Фейкові новини, дезінформація, поширення чуток, психологічні операції, створення страху і недовіри.

Психологічний вплив	Формування емоційних станів і настроїв для зміни сприйняття і поведінки аудиторії.	Однобічне подання фактів, перебільшення, замовчування інформації, використання символіки і риторики.
Технічні засоби	Використання цифрових технологій для порушення роботи інформаційних систем і підриву довіри.	Кібератаки, віруси, злом баз даних, дестабілізація через цифрові атаки.
Психологічні операції	Інфільтрація в структури опонента для збору інформації та посіву дезінформації зсередини.	Маніпулювання процесами прийняття рішень, підрив авторитету лідерів, зниження ефективності управління.

Джерело на основі [3]

Отже, аналіз основних інструментів та методів інформаційного впливу свідчить про їхню складність і багатогранність, що поєднує традиційні форми комунікації з сучасними цифровими технологіями. Розподіл на прямі та непрямі методи підкреслює різні підходи до маніпуляції інформацією — від відкритої пропаганди до прихованих психологічних операцій. Особливу увагу слід приділяти психологічним і технічним засобам, які посилюють ефективність інформаційних атак і створюють значні виклики для безпеки держави та суспільства. Це вимагає постійного розвитку протидіючих стратегій, підвищення інформаційної грамотності та впровадження новітніх технологій захисту інформаційного простору.

Методи інформаційного впливу поділяються на прямі та непрямі. Прямі методи передбачають відкриту трансляцію інформації з визначеною метою, зокрема, офіційну пропаганду, публічні заяви, інформаційні кампанії. Непрямі ж методи включають застосування маніпулятивних технологій — використання фейкових новин, дезінформації, психологічних операцій (псівдоопераций), створення і поширення чуток, а також вплив через соціально-психологічні чинники, такі як формування страху, недовіри або ворожнечі серед населення.

Значну роль у системі методів відіграє психологічний вплив, який використовується для створення певних емоційних станів і настроїв у суспільстві. Маніпулювання свідомістю через інформаційний простір

спрямоване на зміну сприйняття подій, формування ворожості до певних соціальних груп або інституцій, а також дестабілізацію суспільного порядку. В цьому контексті важливими є методи пропаганди, які базуються на однобічному поданні фактів, перебільшенні або замовчуванні певної інформації, а також активному використанні символіки і риторики для впливу на свідомість аудиторії.

Технічні засоби інформаційного впливу включають також кібератаки на інформаційні системи, розповсюдження вірусів, злом баз даних та інші форми цифрової агресії, які мають на меті не лише зірвати роботу державних та комерційних структур, а й підривати довіру до офіційних джерел інформації. Таким чином, сучасна інформаційна війна поєднує традиційні засоби комунікації з новітніми технологіями кіберпростору, що створює комплексну систему впливу.

Не менш важливими є також методи психологічних операцій, які використовують інфільтрацію у соціальні та політичні структури опонента з метою збору інформації та посіву дезінформації зсередини. Застосування таких методів дозволяє маніпулювати ключовими процесами прийняття рішень, підривати авторитет лідерів і знижувати ефективність управлінських структур.

У наукових працях українських дослідників, таких як В. І. Нестуля, О. М. Савченко та І. В. Таран, наголошується на необхідності системного підходу до виявлення та нейтралізації цих інструментів та методів. Автори підкреслюють, що тільки через координацію державних структур, підвищення рівня інформаційної грамотності громадян та розвиток сучасних технологій захисту інформаційного простору можливо ефективно протистояти інформаційним загрозам.

Отже, аналіз основних інструментів та методів інформаційного впливу свідчить про їхню різноманітність, динамічність і високий рівень

технологічного розвитку, що вимагає від суб'єктів міжнародних відносин постійного удосконалення механізмів захисту інформаційного простору та формування стійкості до інформаційних атак.

РОЗДІЛ 2. СУЧАСНІ ІНФОРМАЦІЙНІ ВІЙНИ НА ЄВРОПЕЙСЬКОМУ ГЕОПРОСТОРІ В КОНТЕКСТІ МІЖНАРОДНОЇ БЕЗПЕКИ

2.1. Геополітичний контекст та учасники інформаційних конфліктів

У XXI столітті інформаційний простір став ключовим полем геополітичного протистояння, особливо в умовах трансформації міжнародної безпекової системи. Європейський геопростір у цьому контексті є одним із найбільш вразливих і водночас активних регіонів, де зіштовхуються інтереси як традиційних світових гравців, так і новітніх акторів — недержавних структур, транснаціональних корпорацій, мережевих спільнот тощо. Сучасні інформаційні війни, що ведуться на цьому просторі, мають не лише медійний або пропагандистський вимір, але й стратегічне значення для формування політичних альянсів, підриву легітимності інститутів, впливу на виборчі процеси та зміну міжнародного порядку.

В умовах глобалізації та гібридизації конфліктів інформаційна сфера стала головною ареною для реалізації як державних, так і недержавних стратегій впливу, спрямованих на зміну політичного ландшафту, підрив стабільності та легітимності владних інститутів.

Першим ключовим чинником є перехід від традиційних форм ведення війни до гібридних стратегій, у яких поєднуються класичні військові, економічні, дипломатичні та інформаційно-психологічні методи. Інформаційні операції у такому контексті виконують роль каталізатора політичних змін, інструменту дестабілізації та засобу формування суспільної думки. Прикладом цього є події, пов’язані з анексією Криму у 2014 році, коли інформаційна кампанія, підтримана масовим поширенням дезінформації, створила передумови для збройного захоплення частини української території. Російські медіа-ресурси цілеспрямовано транслювали меседжі про “захист російськомовного населення”, маніпулювали історичними фактами та підсилювали наративи про “фашистську загрозу” з боку Києва.

Другим фактором виступає посилення конкуренції за вплив у регіоні Центрально-Східної Європи, що є зоною стратегічного протистояння між Заходом (НАТО, ЄС, США) та Російською Федерацією. Такі держави, як Польща, країни Балтії, Румунія, Україна, стають мішенями інформаційних атак, спрямованих на дискредитацію євроатлантичної інтеграції, поширення антизахідних наративів, підрив внутрішньої єдності. Прикладом є операція "Ghostwriter", в рамках якої було здійснено серію хакерських атак з подальшим поширенням фейкових повідомлень від імені політиків та офіційних органів Польщі, Литви, Латвії та Німеччини. Ця кампанія мала на меті скомпрометувати позиції НАТО та знизити довіру громадськості до власних урядів.

Третім аспектом є розвиток цифрових технологій і стрімке поширення соціальних мереж, які стали потужним каналом для інформаційного впливу. Такі платформи, як Facebook, Twitter, Telegram, YouTube, відіграють роль не лише у розповсюдженні інформації, але й у мобілізації політичних рухів, створенні альтернативної реальності, спрямованої на підрив національної ідентичності та демократичних цінностей. Розслідування, проведені зокрема у Великій Британії та Франції, показали, що російські тролі з "фабрики ботів" у Санкт-Петербурзі активно впливали на хід виборчих кампаній, зокрема Brexit та президентські вибори 2017 року у Франції, розповсюджуючи маніпулятивні новини та підбурюючи до поляризації суспільства.

Крім цього, важливим чинником є відсутність чітко врегульованого міжнародного правового механізму протидії інформаційним війнам. Незважаючи на наявність базових положень міжнародного гуманітарного права, таких як Женевські конвенції, більшість форм інформаційної агресії залишаються поза правовим регулюванням, що створює простір для безкарного використання інформації як зброї. Це спонукає держави до активної розробки національних стратегій кібербезпеки, кібероборони та інформаційного захисту,

однак ефективність таких ініціатив залишається обмеженою без координації на міжнародному рівні.

Не менш важливою є проблема участі недержавних акторів — приватних компаній, хакерських груп, псевдожурналістських організацій — які часто діють у сірій зоні міжнародного права. Такі структури, як “CyberBerkut” або “APT28” (Fancy Bear), використовують кібершпигунство, злам систем державного управління, викрадення персональних даних, і поширення їх з метою дестабілізації політичних процесів. У 2015 році в результаті кібератаки на електромережу України було частково паралізовано роботу енергетичної системи західного регіону — вперше у світі кібератака мала прямий вплив на критичну інфраструктуру держави.

Участь у інформаційних конфліктах беруть і традиційні медіа, які можуть як протидіяти, так і сприяти поширенню дезінформації. У ряді країн Східної Європи (Угорщина, Сербія, Болгарія) спостерігається контроль певних ЗМІ проросійськими бізнес-структурами, що формує спотворене уявлення про події в Україні, на Заході, щодо міграційної політики, НАТО, тощо. Таким чином, медіа виступають не лише інструментом, а й активним учасником у формуванні геополітичного порядку денного.

Окремо варто наголосити на тому, що геополітичні інформаційні конфлікти все частіше набувають транскордонного характеру та мають довготривалі наслідки. У зв’язку з цим країни Європи посилюють співпрацю в межах таких структур, як Європейська служба зовнішніх дій (EEAS), Центр стратегічних комунікацій НАТО, Європейський центр протидії гібридним загрозам у Гельсінкі. Їхньою метою є моніторинг інформаційного простору, виявлення деструктивних впливів, просування правдивої інформації та зміцнення стійкості суспільств до зовнішніх інформаційних втручань.

Серед основних учасників інформаційних війн на європейському геопросторі варто виокремити декілька категорій. Першу групу складають державні актори, які використовують інформаційні операції як інструмент реалізації своїх зовнішньополітичних інтересів. У цьому контексті одним з найактивніших учасників є Російська Федерація, яка системно застосовує інформаційно-психологічні впливи для просування власного наративу, дискредитації західних інституцій, посилення розколів у європейських суспільствах та підтримки проросійських сил. Приклади таких дій включають втручання у вибори у Франції та Німеччині, поширення фейкової інформації про український конфлікт, а також кампанії проти НАТО й ЄС.

У контексті сучасних геополітичних викликів Захід виступає не лише об’єктом інформаційної агресії, але й активним суб’єктом формування інформаційної безпеки в глобальному масштабі. Західні держави, а також міжурядові структури, такі як Європейський Союз, НАТО, ОБСЄ, стали ключовими гравцями у сфері протидії дезінформації, кібератакам та маніпулятивним наративам, що поширюються ззовні, насамперед із боку Російської Федерації, а також Китаю, Ірану та інших авторитарних режимів. Водночас вони активно формують власні стратегічні інформаційні платформи, які мають на меті як захист внутрішнього інформаційного середовища, так і підтримку союзників, зокрема на східному фланзі Європи.

Одним із ключових інституційних відповідей на інформаційні загрози з боку Європейського Союзу стало створення у 2015 році спеціального підрозділу — East StratCom Task Force, який діє в межах Європейської служби зовнішніх справ (European External Action Service). Основне завдання цього підрозділу — виявлення, аналіз та спростування дезінформаційних кампаній, зокрема з боку Росії, а також зміцнення стратегічної комунікації між ЄС та країнами Східного партнерства (Україна, Грузія, Молдова, Вірменія, Азербайджан, Білорусь). У

рамках ініціативи була запущена платформа EUvsDisinfo, яка фіксує приклади дезінформації та надає систематизовані аналізи поширених наративів.

За роки існування EUvsDisinfo задокументовано понад 15 000 випадків дезінформації, серед яких особливу увагу приділяють російським медіа-ресурсам RT (Russia Today) та Sputnik. Наприклад, наратив про те, що Євросоюз є нібито «деградуючим альянсом», який втрачає цінності та ідентичність через підтримку України або санкційну політику щодо Росії, активно поширювався у країнах Балкан, Центральної та Східної Європи. У відповідь на це ЄС розширює присутність у стратегічних комунікаціях, зокрема фінансує незалежні медіа, підтримує фактчекінгові платформи (наприклад, StopFake в Україні, Demagog у Польщі, EU DisinfoLab у Бельгії), а також розробляє освітні ініціативи для підвищення медіаграмотності.

У 2022 році, у зв’язку з повномасштабним вторгненням РФ в Україну, Європейський Союз прийняв рішення про заборону трансляції державних російських каналів RT та Sputnik у межах європейського інформаційного простору, визнавши їх інструментами державної пропаганди. Це рішення було підтримано всіма державами-членами ЄС, попри критику з боку окремих організацій щодо обмеження свободи слова. Проте в умовах гібридної війни ЄС наголосив на праві держав захищати свою інформаційну безпеку та запобігати поширенню неправдивих повідомлень, які можуть сприяти дестабілізації.

Західна протидія інформаційним загрозам включає також розвиток оборонних механізмів у межах НАТО. Альянс визнав інформаційні та кібератаки як потенційний привід для застосування Статті 5 Північноатлантичного договору, що розглядає напад на одного члена як напад на всіх. НАТО створив Центр стратегічних комунікацій у Ризі (STRATCOM COE), який розробляє доктрини протидії дезінформації, тренінги для військових, журналістів, аналітиків і співробітників безпекових структур країн-членів.

Також функціонує Центр кібербезпеки в Естонії (CCDCOE), який координує заходи з протидії кібератакам та проводить симуляційні навчання (наприклад, Locked Shields) для підвищення готовності до інформаційно-кіберзагроз.

Особливо показовою є стратегія Сполучених Штатів Америки у сфері інформаційної безпеки. У 2020 році було ухвалено Cybersecurity and Infrastructure Security Agency (CISA) Act, який передбачає координацію захисту критичних інфраструктур, у тому числі в інформаційному полі. Додатково, в рамках Державного департаменту США функціонує Global Engagement Center (GEC), що спеціалізується на виявленні та нейтралізації іноземної пропаганди, у першу чергу з боку авторитарних режимів. GEC активно підтримує незалежні медіа, надає гранти на розвиток аналітичних центрів, співпрацює з журналістами-розслідувачами (наприклад, Bellingcat, The Dossier Center), а також веде інформаційні кампанії у соціальних мережах, спрямовані на спростування фейків.

США також надають значну допомогу союзним країнам у галузі цифрової безпеки. Наприклад, після масштабних кібератак на урядові інституції в Україні у 2022–2023 роках, американські фахівці допомогли впровадити нові протоколи захисту вітчизняних систем, провели спільні навчання, надали інфраструктурну підтримку для резервного збереження критичних даних. Крім того, у 2021 році було створено U.S.–EU Trade and Technology Council, що серед іншого розглядає питання боротьби з дезінформацією, розробки етичних норм штучного інтелекту та спільного регулювання цифрових платформ.

Варто також відзначити роль ОБСЄ, яка, попри обмежений мандат, регулярно публікує аналітичні звіти про стан свободи слова, зловживання інформацією, випадки маніпуляції в медіа та соціальних мережах. Представник ОБСЄ з питань свободи ЗМІ неодноразово звертав увагу на небезпеку

використання пропаганди як зброї та закликав держави дотримуватись принципів прозорості, правдивості й плюралізму в інформаційному просторі.

Додатковим напрямом західної інформаційної протидії є інвестування в медіаграмотність населення. Наприклад, у Фінляндії впроваджено обов'язкові курси з критичного мислення у школах, а також програми з виявлення фейків на рівні муніципальних центрів освіти. Подібні ініціативи діють у Швеції, Литві, Чехії. У межах проекту UNESCO з медіаосвіти підтримується публікація навчальних посібників, які використовуються в університетах Європи та Центральної Азії.

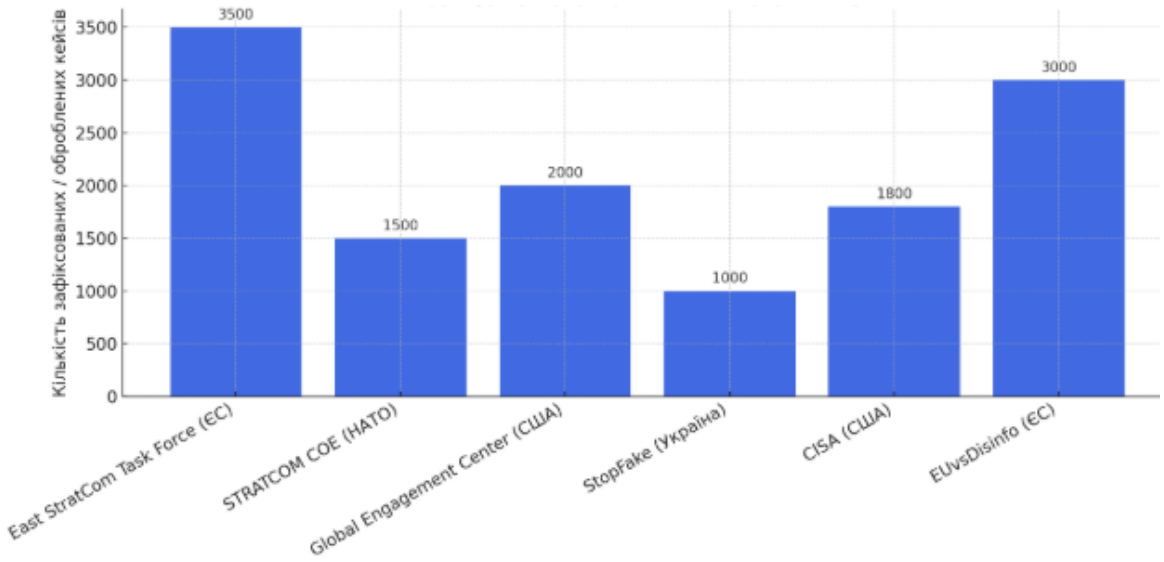

Рис.2.1. Основні західні структури у сфері протидії дезінформації

Особливу роль у сучасних інформаційних війнах відіграють недержавні актори. Це, зокрема, приватні медіакомпанії, соціальні платформи (Facebook, Twitter, TikTok), які, навіть не беручи прямої участі в геополітичному протистоянні, часто стають каналами поширення деструктивної інформації або, навпаки, майданчиками для контрдезінформаційних ініціатив. Іншою групою недержавних суб'єктів є хакерські об'єднання (наприклад, Anonymous або проросійські угруповання, як-от Killnet), які здійснюють кібератаки, викрадення

даних, публікацію компрометуючих матеріалів (leaks) з метою впливу на громадську думку чи підриву довіри до державних інституцій.

Варто звернути увагу також на роль національних меншин, міграційних спільнот та етнічних діаспор, які можуть як стати жертвами, так і об'єктами маніпулятивного впливу. Застосування інформаційних операцій щодо таких груп дозволяє з одного боку сіяти соціальну напругу, а з іншого — створювати віртуальні платформи для просування певних політичних ідеологій чи навіть сепаратистських настроїв.

Інформаційні війни в Європі тісно пов'язані з конкретними конфліктами. Найяскравішим прикладом є російсько-українська війна, що з 2014 року супроводжується масштабними інформаційними кампаніями з боку РФ. У цьому конфлікті інформаційна війна є не просто доповненням до збройного протистояння, а його невід’ємним компонентом. Російські ЗМІ, мережі ботів, псевдоаналітичні ресурси активно використовуються для створення паралельної реальності щодо подій в Україні, легітимації анексії Криму, делегітимації української влади та Збройних Сил. У відповідь, Україна активізувала зусилля щодо формування стійкої системи стратегічних комунікацій, реформування медіапростору, підвищення цифрової стійкості суспільства.

Не менш важливою є інформаційна компонента у контексті військової присутності НАТО у Східній Європі. Пропагандистські наративи про «загрозу від НАТО» активно просуваються в країнах Балтії, Польщі, Словаччині, використовуючи історичні, соціальні та економічні маркери. Уряди цих країн у відповідь розгортають стратегії інформаційної протидії, зокрема, шляхом впровадження програм медіаграмотності, зміцнення незалежних медіа та протидії ворожим впливам на вибори.

Суттєвим викликом для європейського безпекового середовища є й використання інформаційних технологій у терористичній діяльності.

Інформаційні платформи часто стають каналами вербування, радикалізації та координації дій екстремістських груп, зокрема, ісламістських угруповань, що використовують соціальні мережі для просування радикальних ідей. Це вимагає від урядів країн ЄС та міжнародних організацій створення систем моніторингу та протидії цифровому тероризму.

Таким чином, сучасний геополітичний контекст Європи формує сприятливі умови для масштабного використання інформаційних засобів як у міждержавному, так і внутрішньополітичному протистоянні. Інформаційні війни стали ключовим інструментом досягнення стратегічних цілей, дестабілізації опонентів, маніпулювання громадською думкою та створення нових точок напруги. Ефективна протидія таким загрозам можлива лише за умови координації зусиль держав, міжурядових організацій, приватного сектору та громадянського суспільства.

2.2. Основні напрями та тактики інформаційних атак у Європі

У сучасному геополітичному контексті інформаційні атаки стали невід'ємною складовою гібридної війни та інструментом впливу на внутрішньополітичну стабільність, громадську думку, міждержавні відносини та міжнародну безпеку. Особливу активність таких впливів спостерігаємо на європейському геопросторі, де цифрова взаємозалежність, політична плюралістичність і високий рівень медіаспоживання роблять країни Європи вразливими до інформаційних маніпуляцій.

Одним із провідних напрямів інформаційних атак у Європі є дестабілізація політичних процесів, зокрема вплив на вибори, референдуми, урядові кризи та суспільні протестні рухи. Найяскравішим прикладом є

втручання у виборчі кампанії у Франції (2017), Німеччині (2017, 2021), Італії (2018), а також кампанія навколо референдуму щодо Brexit у Великій Британії. Атаки передбачали масове поширення дезінформації, злом електронної кореспонденції політиків, створення фальшивих новин та використання бот-мереж. У випадку з Францією йдеться, зокрема, про злам електронної пошти штабу Еммануеля Макрона, що супроводжувався публікацією підроблених і маніпулятивних документів напередодні виборів.

Ще одним ключовим напрямом є посилення розколів у суспільстві через нагнітання конфліктів на етнічному, релігійному, ідеологічному чи соціальному ґрунті. Інформаційні кампанії націлені на розпалювання ксенофобії, антимігрантських настроїв, ворожості до представників ЛГБТ-спільноти або до Європейського Союзу як інституції. У 2015–2016 роках, на піку міграційної кризи, дезінформаційні атаки в Німеччині, Австрії та Швеції використовували емоційно заряджені наративи про злочини мігрантів, які часто були сфабрикованими або викривленими. Це сприяло зростанню впливу праворадикальних сил і зниженню довіри до державних структур та медіа.

Гібридна війна проти України, яка супроводжується масштабними інформаційно-психологічними кампаніями Російської Федерації, стала полігоном для відпрацювання деструктивних інформаційних технологій, які згодом застосовуються в інших регіонах Європи. Зокрема, кампанії, спрямовані на дискредитацію європейської підтримки України, спотворення фактів війни, поширення фейків про «українських нацистів» або «біолабораторії США» мали на меті вплинути на громадську думку в країнах ЄС і зменшити готовність урядів підтримувати Україну фінансово та військово.

Важливою тактикою сучасних інформаційних атак є використання соціальних мереж як каналів впливу. Створення фейкових акаунтів, ботів і тролів, автоматизоване поширення меседжів (astroturfing), організація

онлайн-флешмобів, коментування новин з маніпулятивною метою – усе це забезпечує ефективну деструкцію інформаційного середовища. Прикладом є операція Secondary Infektion – багаторічна кампанія поширення дезінформації через підставні акаунти у Facebook, Reddit, Medium та інших платформах. У ній фіксувалися публікації підроблених листів, звітів та інтерв'ю, які згодом репостилися через фейкові профілі в соцмережах.

Особливо небезпечними є атаки на критичну інфраструктуру інформаційного простору – атаки на медіаресурси, інформаційні агентства, сайти урядових установ. У 2021–2022 роках були зафіксовані серії кібератак на міністерства та ЗМІ в Польщі, Литві та Україні, які супроводжувалися розміщенням фейкових новин, зломами облікових записів і маніпулятивними повідомленнями. Це поєднання технічного втручання з психологічним впливом свідчить про синергію кібероперацій і інформаційної війни як цілісної стратегії.

Значна частина атак орієнтована на дискредитацію міжнародних інституцій, таких як НАТО, Європейський Союз, ООН, з метою зменшення довіри до спільних зусиль у сфері безпеки та правопорядку. Зокрема, під час пандемії COVID-19 було поширено численні теорії змови щодо «біологічної зброї НАТО», «контролю населення через вакцини» або «світової змови фармацевтичних корпорацій», що підривали зусилля держав ЄС у боротьбі з пандемією.

До поширених тактик також відноситься створення альтернативної інформаційної реальності, що включає формування паралельних медіасистем із псевдонезалежними сайтами, YouTube-каналами, Telegram-ресурсами, які систематично поширюють викривлену або вигадану інформацію. Їхнє завдання – посіяти сумніви, поляризувати суспільство, підважити авторитет традиційних медіа і наукових джерел. Деякі з таких ресурсів ретельно маскуються під

професійні ЗМІ, мають візуально привабливий дизайн, використовують мову фактів і експертних думок, але в реальності є частиною скоординованих інформаційних кампаній.

Окремим тактичним елементом інформаційної війни в Європі є вплив через культурну дипломатію та «м'яку силу», який у деструктивному контексті набуває форми культурної інфільтрації, нав'язування альтернативної історичної інтерпретації, просування антидемократичних наративів через мистецтво, літературу, медіа. Такі кампанії часто мають кумулятивний ефект, поступово змінюючи ідеологічний ландшафт аудиторії.

Таким чином, спектр напрямів та тактик інформаційних атак у Європі надзвичайно широкий. Вони охоплюють як пряме втручання в політичні процеси, так і довготривалі деструктивні стратегії зі зміни культурного і когнітивного фону суспільств. Спільним знаменником усіх форм є прагнення вплинути на прийняття рішень, дестабілізувати інституції, підірвати міждержавну довіру і трансформувати сприйняття реальності на користь стратегічного опонента. Розуміння цих процесів є необхідним для формування ефективних механізмів захисту, стійкості та просування демократичних цінностей в умовах інформаційної турбулентності сучасного міжнародного середовища.

РОЗДІЛ 3. ВПЛИВ ТА ПРОТИДІЯ ІНФОРМАЦІЙНИМ ВІЙНАМ НА ЄВРОПЕЙСЬКОМУ РІВНІ В МІЖНАРОДНИХ ВІДНОСИНАХ

3.1. Наслідки інформаційних війн для безпеки та суспільства

У контексті сучасного європейського геополітичного простору інформаційні війни перетворилися з побічного елемента зовнішньополітичної

боротьби на повноцінну складову системних викликів безпеці та соціальній стабільності. Їхній вплив виявляється не лише на державному рівні, але й у повсякденному житті громадян, формуючи нові виклики для суспільного консенсусу, національного суверенітету, довіри до інституцій і функціонування демократичних структур. Аналіз наслідків інформаційних війн в Європі вимагає міждисциплінарного підходу, який охоплює політичну, соціологічну, психологічну та безпекову площини.

Одним із найпомітніших наслідків інформаційних війн є ерозія суспільної довіри до традиційних джерел інформації та демократичних інституцій. У багатьох країнах ЄС спостерігається зростання недовіри до національних урядів, парламентів, правоохоронних органів і засобів масової інформації. Цей процес підживлюється систематичним поширенням фейкових новин, теорій змови, дезінформаційних наративів, зокрема про «корумповану владу», «зовнішнє управління» або «змова еліт». Прикладом є кампанії, що супроводжували пандемію COVID-19, коли тисячі користувачів соціальних мереж у Європі втратили довіру до офіційної інформації щодо вакцин, заходів безпеки та рішень урядів. Таке інформаційне середовище створює сприятливий ґрунт для зростання радикальних рухів, антисистемних партій і соціальних протестів.

Інформаційні війни також спричиняють політичну поляризацію, особливо в умовах виборчих процесів. Маніпулятивні стратегії поділу суспільства на «нас» і «їх», культивація образу ворога, емоційне нагнітання через соціальні мережі та алгоритми платформ призводять до радикалізації позицій виборців і втрати політичної поміркованості. Такі тенденції були помітні під час виборів у Франції, Італії, Іспанії та Німеччині, де крайні політичні сили (праві чи ліві)

посилили свої позиції, зокрема за рахунок активного використання соціальних мереж, підтриманих іноземними інформаційними впливами.

Ще одним серйозним наслідком є підрив національної безпеки, зокрема у сфері кібербезпеки, оборони, внутрішнього правопорядку. Інформаційні атаки часто супроводжуються або передують кібератакам, які паралізують роботу державних установ, стратегічних об'єктів інфраструктури (електромереж, водопостачання, банківських систем), а також військових структур. Наприклад, у 2022 році Литва, Латвія та Естонія зазнали масових DDoS-атак та хакерських вторгнень, які супроводжувалися інформаційними кампаніями про «зовнішнє управління країнами Балтії з боку НАТО» або «зміну історичної пам'яті».

Крім безпекових ризиків, інформаційні війни мають значний вплив на психологічний стан населення та суспільну згуртованість. Постійна експозиція до негативного, страхітливого або спотвореного контенту, тривожні наративи та напівправда сприяють виникненню масової тривоги, депресивних настроїв, відчуття безсилля, а також втрати віри в колективні зусилля суспільства. Це особливо небезпечно в умовах кризових ситуацій, як-от пандемія, військовий конфлікт чи економічна рецесія. У таких умовах легко активізуються конспірологічні спільноти, зростає популярність авторитарних лідерів і зменшується здатність суспільства до солідарної мобілізації.

Також варто згадати про економічні наслідки інформаційних атак, які проявляються у вигляді втрати інвестиційної привабливості, падіння курсу національної валюти, коливань фондового ринку внаслідок чуток або штучно згенерованих повідомлень. У сучасних умовах, коли економіка багато в чому залежить від інформаційних потоків і репутаційних ризиків, навіть короткотермінова кампанія дезінформації може призвести до довготривалих фінансових наслідків.

Інформаційні війни також впливають на зовнішньополітичну орієнтацію держав, змінюючи уявлення суспільства про союзників і ворогів, маніпулюючи історичними фактами, підміняючи поняття міжнародного права. Зокрема, зусилля РФ щодо розповсюдження наративів про «занепад Заходу», «двійні стандарти НАТО», «невигідність членства в ЄС» мають на меті розхитати єдність Європейського Союзу та зруйнувати трансатлантичну єдність. У деяких країнах, наприклад, в Угорщині, Болгарії чи Словаччині, ці наративи частково знаходять політичне відображення у вигляді антиєвропейських ініціатив або проросійських симпатій окремих партій.

Важливим наслідком також є деформація інформаційного простору та криза журналістики, яка втрачає монополію на формування суспільного дискурсу. Розмивання межі між журналістикою, пропагандою та контентом соціальних мереж ускладнює перевірку фактів і унеможливлює ефективне функціонування публічної сфери як простору раціональної дискусії. Особливо гостро це сприймається серед молоді, яка в значній мірі отримує новини через TikTok, Instagram або Telegram, де кількість переглядів часто замінює достовірність джерела.

Таблиця 3.1. Основні наслідки інформаційних війн у Європі

Сфера впливу	**Характер наслідків**	**Приклади**	**Наслідки для суспільства / держави**
Політична	Поляризація, зниження довіри до інституцій, зростання підтримки радикальних сил	Вибори у Франції (2017, 2022), підтримка антисистемних партій у Німеччині, Італії	Послаблення демократичної легітимності, нестабільність політичної системи

Соціальна	Розкол суспільства, зростання протестних настроїв, агресія між групами	Протести антивакцинаторів у Нідерландах, Бельгії, Іспанії	Деградація громадянського діалогу, ризики масових заворушень
Безпекова (кібер)	Кібератаки, витік даних, зниження готовності до надзвичайних ситуацій	DDoS-атаки на урядові сайти Литви, Польщі, кібератаки проти Чехії	Паралізація державних функцій, ризик саботажу
Інформаційна / медійна	Дезінформація, фейки, втрата орієнтації в інформаційному полі	Пропаганда про «загниваючий Захід», поширення фейків про Україну та НАТО	Зниження критичного мислення, сприйнятливість до зовнішніх впливів
Психологічна	Масова тривожність, втома, втрата довіри до реальності	Кампанії страху під час COVID-19, війни в Україні	Зниження стійкості суспільства, депресивні тенденції
Економічна	Репутаційні втрати, коливання ринку, зниження інвестиційної привабливості	Чутки про банківську кризу в Італії, антипольські кампанії в аграрному секторі	Економічна нестабільність, втрати інвесторів
Зовнішньополітична	Зміна уявлень про союзників/ворогів, підрив єдності ЄС і НАТО	Проросійські кампанії в Болгарії, Угорщині, поширення наративу «ЄС як диктат»	Дестабілізація зовнішньої політики, посилення впливу авторитарних країн

У підсумку, наслідки інформаційних війн у Європі є системними, довготривалими та багатовимірними. Вони не лише порушують поточну безпеку, але й трансформують уявлення про суспільну норму, підривають демократичні процедури, створюють нові лінії конфлікту та змінюють архітектуру міжнародних відносин. В умовах, коли інформація стає зброєю, здатною паралізувати не гірше за танки чи ракети, захист від неї має бути не лише технічним, а передусім соціальним, культурним і освітнім.

Європейські країни вже сьогодні повинні інвестувати у підвищення медійної грамотності, розвиток незалежної журналістики, створення інституційної спроможності до реагування на загрози інформаційної війни,

формування спільної інформаційної політики ЄС, а також трансатлантичної взаємодії з партнерами. Без цього будь-які заходи з безпеки залишатимуться вразливими до однієї з найнебезпечніших зброї XXI століття — зброї інформаційного впливу.

3.2. Стратегії та механізми протидії інформаційним загрозам на європейському рівні

Сучасні виклики в інформаційному просторі вимагають скоординованої та багаторівневої реакції з боку європейських інституцій та національних урядів. Поширення фейкових новин, кібератак, кампаній дезінформації та маніпулювання громадською думкою становлять пряму загрозу для безпеки демократичних процесів, економічної стабільності та суспільної єдності. У відповідь на зростання масштабів інформаційних загроз, Європейський Союз (ЄС), НАТО, а також окремі країни-члени почали формувати стратегії та механізми, спрямовані на забезпечення інформаційної стійкості. Ці механізми охоплюють як нормативно-правові аспекти, так і технологічні інструменти, освітні програми та міжнародне співробітництво.

Однією з ключових стратегічних ініціатив ЄС стала створена у 2015 році East StratCom Task Force, що функціонує в межах Європейської служби зовнішніх справ (EEAS). Основним завданням цього підрозділу є моніторинг дезінформаційних кампаній, зокрема з боку Російської Федерації, а також підвищення обізнаності громадян про засоби маніпулювання у ЗМІ. Продуктом діяльності цієї групи став портал EUvsDisinfo, який збирає, аналізує та публікує приклади фейкових повідомлень, одночасно надаючи аналітичні роз’яснення та

контраргументи. Цей інструмент став важливою ланкою у стратегії «доказової протидії» — надання перевіреної, прозорої та логічно побудованої інформації як відповідь на пропагандистські меседжі.

Ще одним важливим механізмом протидії стала Європейська цифрова служба (European Digital Media Observatory, EDMO), яка об'єднує університети, наукові інститути, незалежні фактчекінгові платформи та журналістські організації з метою забезпечення комплексного аналізу інформаційних потоків. EDMO реалізує як наукові дослідження, так і практичну взаємодію між стейкхолдерами задля протидії дезінформації на національному та транснаціональному рівнях. Національні хаби EDMO створені у більшості країн-членів ЄС, зокрема у Франції, Німеччині, Італії, Польщі та країнах Балтії.

Значну увагу ЄС приділяє також розбудові медіаграмотності. Розуміння принципів функціонування медіа, вміння ідентифікувати фейки та маніпуляції, критичне мислення — ці компетентності є основою для формування інформаційно захищеного суспільства. Програми, спрямовані на розвиток цифрової освіти, включено до рамкової стратегії Digital Education Action Plan (2021–2027), а також до ініціативи EU Code of Practice on Disinformation, що залучає цифрові платформи до співрегулювання контенту.

Не менш важливою є співпраця з соціальними мережами. У 2018 році Європейська Комісія ухвалила Кодекс належної практики (Code of Practice on Disinformation), який підписали такі гіганти як Facebook (Meta), Google, Twitter, Microsoft та TikTok. Згідно з кодексом, платформи зобов'язалися демонструвати прозорість алгоритмів, маркувати політичну рекламу, блокувати боти та системи автоматизованої дезінформації. У 2022 році Кодекс був оновлений, додавши більш жорсткі вимоги, зокрема щодо прозорості джерел інформації та щомісячного моніторингу звітів.

У рамках NATO активно розвивається напрям Strategic Communications (StratCom), який включає Центр досконалості у Ризі (StratCom COE). Його завдання — формування стратегічних наративів Альянсу, виявлення ворожої пропаганди та аналіз інформаційної поведінки супротивників. StratCom COE тісно співпрацює з національними структурами безпеки, розвідкою, а також медіаорганізаціями ля забезпечення скоординованої протидії.

Особливу увагу приділяють кіберзахисту, який є невід'ємною складовою інформаційної безпеки. Європейська агенція з кібербезпеки (ENISA) розробляє та координує реалізацію стандартів у сфері кіберстійкості, зокрема згідно з директивою NIS2 (Network and Information Security). В рамках реалізації Єдиного цифрового ринку (Digital Single Market) формується інфраструктура швидкого реагування на кібератаки, обміну інформацією між країнами-членами, а також стандартизація протоколів реагування.

На національному рівні окремі держави також створюють власні аналітичні та моніторингові центри. Наприклад, у Фінляндії діє Центр компетенцій з гібридних загроз (Hybrid CoE), який аналізує поведінку державних і недержавних акторів у сфері гібридних конфліктів, зокрема у кібер- та інформаційному вимірах. Польща, Литва та Чехія впровадили державні програми фактчекінгу та просування національної цифрової безпеки через шкільні програми та підтримку незалежних медіа.

Варто також зазначити важливість міжнародної кооперації, зокрема в рамках Групи семи (G7), Організації з безпеки і співробітництва в Європі (ОБСЄ) та Ради Європи, які розглядають інформаційні загрози як загальноєвропейську безпекову проблему. Приймаються рекомендації щодо прозорості державних комунікацій, відповідальності платформ та захисту свободи слова в умовах новітніх загроз.

У підсумку, стратегії ЄС та міжнародних організацій демонструють поступовий перехід від реактивного підходу до проактивного управління інформаційною сферою. Інституалізація протидії дезінформації, розвиток цифрової грамотності, кіберзахист і міжсекторальна співпраця є ключовими елементами сталого механізму безпеки. Однак, інформаційні загрози постійно еволюціонують, що вимагає не лише адаптації політик, а й постійного інноваційного пошуку нових форм захисту європейського інформаційного простору.

ВИСНОВОК

У результаті дослідження теми «Сучасні інформаційні війни на європейському геопросторі» було з’ясовано, що інформаційна сфера у XXI столітті набула стратегічного значення в системі міжнародної безпеки та геополітичного протистояння. На тлі розвитку цифрових технологій, глобалізації комунікаційних мереж і зростання ролі інформації як ресурсу влади,

інформаційні війни стали однією з основних форм конфліктної взаємодії між державами, а також між державними і недержавними суб’єктами.

Особливо це стосується європейського геопростору — регіону, де традиційно перетинаються геополітичні інтереси провідних світових гравців, таких як Європейський Союз, Сполучені Штати Америки, Російська Федерація, а також КНР і Туреччина. Європа, з її високим рівнем цифровізації, відкритими демократичними інститутами, плюралізмом думок і свободою слова, є вразливою мішенню для зовнішнього впливу, зокрема в інформаційній сфері.

Різноманітні методи інформаційної війни, включаючи поширення фейкових новин, дезінформації, маніпулятивного контенту, використання ботів і тролів у соціальних мережах, мають на меті впливати на громадську думку, змінювати політичні пріоритети, дискредитувати демократичні процеси, сприяти зростанню недовіри до державних інституцій та розколювати суспільство зсередини. Усі ці процеси відбуваються без застосування фізичної сили, але здатні викликати наслідки, порівнювані з воєнними конфліктами, — політичну дестабілізацію, зміну урядів, порушення територіальної цілісності та суверенітету держав.

Одним з ключових висновків проведеного дослідження є усвідомлення того, що інформаційні війни мають багаторівневий і гібридний характер. Їхня ефективність значною мірою залежить від здатності противника приховати джерело впливу, маскувати його під внутрішні соціальні процеси або легітимну журналістику. Саме ця властивість робить інформаційні операції складними для ідентифікації та нейтралізації. Найчастіше їхня мета полягає не лише у поширенні неправдивої інформації, а й у формуванні викривленого світогляду, дезорієнтації аудиторії, створенні атмосфери тотальної недовіри до будь-яких джерел інформації. Особливо небезпечним виявився вплив таких кампаній на виборчі процеси, референдуми, міжетнічні та міжконфесійні відносини,

інформаційну безпеку під час надзвичайних ситуацій (пандемії, міграційні кризи, енергетичні загрози тощо).

Досвід окремих європейських країн, зокрема України, країн Балтії, Польщі, Німеччини, Франції, Великої Британії, свідчить, що протидія інформаційним війнам потребує не лише оперативного реагування, а й довгострокової стратегії. Вона повинна включати розвиток медіаграмотності громадян, створення стійкої інформаційної інфраструктури, підтримку незалежних медіа, моніторинг цифрового середовища, а також формування прозорих правил функціонування соціальних платформ. Одним з перспективних напрямів є розвиток спеціалізованих центрів інформаційної безпеки, які здійснюють аналітичне опрацювання загроз, виявляють джерела атак та забезпечують державне реагування у випадках цілеспрямованих інформаційних кампаній. Водночас, протидія інформаційним загрозам має здійснюватися з дотриманням стандартів прав людини, уникненням цензури, збереженням свободи вираження поглядів, що становить значний виклик для демократичних суспільств.

Окремої уваги заслуговує важливість міжнародної кооперації у сфері інформаційної безпеки. На рівні Європейського Союзу та НАТО вже створені перші інституційні механізми координації дій у сфері протидії дезінформації (наприклад, EUvsDisinfo, East StratCom Task Force, Hybrid CoE тощо), проте вони потребують подальшого розвитку та інтеграції з національними системами реагування. Важливим є також вироблення єдиних європейських стандартів щодо протидії фейкам, прозорості цифрової реклами, маркування політичного контенту, підзвітності цифрових платформ, що сприяє гармонізації інформаційної політики країн-членів ЄС. Необхідно також поглиблювати співпрацю з провідними цифровими компаніями (Google, Meta, X, TikTok),

забезпечуючи їхню відповідальність у сфері модерації шкідливого контенту та запобігання маніпуляціям у цифровому середовищі.

Підсумовуючи викладене, можна зробити висновок, що інформаційні війни на європейському геопросторі є надзвичайно складним і динамічним явищем, яке має потенціал до подальшої ескалації. Умови відкритого інформаційного простору, висока політична чутливість європейських суспільств, поширення цифрових технологій і відсутність ефективного міжнародного правового механізму роблять Європу вразливою до таких форм агресії.

Успішна протидія вимагає комплексного підходу, що об’єднує інституційні, технологічні, правові, освітні та дипломатичні інструменти. Зміцнення інформаційної стійкості має стати пріоритетом не лише окремих країн, а й усієї європейської спільноти як гарантія збереження демократії, стабільності та суверенітету в сучасному цифровому світі. Подальше наукове дослідження цих процесів має велике значення для формування адекватної політики інформаційної безпеки, ефективної побудови комунікаційних стратегій та запобігання новим формам інформаційного впливу в майбутньому.

СПИСОК ЛІТЕРАТУРИ

1. Нестуля, В. І. (2018). Інформаційна війна: теоретичні основи та сучасні виклики. Київ: Видавництво Національного університету оборони України імені Івана Черняховського.

2. Савченко, О. М. (2019). Механізми інформаційного впливу в умовах гібридної війни. Вісник Національного університету «Києво-Могилянська академія», № 23, с. 45–59.
3. Таран, І. В. (2020). Інформаційна безпека України в умовах сучасних викликів. Журнал міжнародного права і міжнародних відносин, № 1, с. 88–102.
4. Тараненко, А. П. (2017). Соціально-психологічні аспекти інформаційної війни. Психологія і суспільство, Том 9, № 2, с. 112–125.
5. Бєлінська, Я. В. (2022). Інформаційна війна як загроза національній безпеці: український вимір. К.: НАДУ при Президентові України.
6. Ковальов, А. І. (2023). Гібридні війни: інформаційна зброя в новій реальності. Харків: Право.
7. Гудима, А. М. (2021). Інформаційна боротьба: історія, теорія, практика. Львів: Видавництво ЛНУ ім. Івана Франка.
8. Клименко, А. В. (2020). Пропаганда як інструмент інформаційної війни. Одеса: Юридична література.
9. Пархоменко, Т. В. (2022). Маніпуляції в медіа в умовах гібридної війни. Київ: Академія медіаосвіти.
10. Шевченко, О. В. (2023). Інформаційна політика держави у протидії дезінформації в умовах війни. К.: Держуправління.
11.
12. Лапкіна, О. І. (2021). Медіаосвітні інструменти протидії інформаційним впливам. Харків: Основа.
13. Марущак, І. В. (2020). Інформаційна безпека як складова національної безпеки України. Львів: Світ.

14. Савенко, О. П. (2022). Дезінформація та її вплив на суспільну свідомість. Чернігів: ЧНТУ.
15. Андрусів, С. (2023). «Інформаційна війна як інструмент реалізації зовнішньої політики РФ». Інформаційне право України, №2, с. 18–25.
16. Поліщук, І. (2022). «Гібридна війна в Україні: роль соціальних медіа в дезінформаційних кампаніях». Державне управління: теорія та практика, №1.
17. Копчак, В. (2023). «Інформаційна безпека в умовах повномасштабної війни Росії проти України». Національна безпека і оборона, №3.
18. Таран, О. (2022). «Кібер- та інформаційні загрози в умовах російської агресії». Військово-науковий вісник, №2.
19. Паламарчук, С. (2023). «Європейський досвід протидії інформаційним загрозам». Вісник Київського національного університету імені Тараса Шевченка. Міжнародні відносини.
20. Демченко, І. (2022). «Механізми протидії фейкам та дезінформації в Україні». Журнал східноєвропейського права, №4.
21. Снігур, В. (2021). «Державна політика протидії інформаційним операціям у воєнний період». Збірник наукових праць НАДУ, №5.
22. Мусієнко, М. (2023). «Становлення стратегічних комунікацій в Україні». Security and Defence Quarterly (UA).

23. Горбулін, В. П. (2020). «Гібридна агресія Росії: інформаційний вимір». Стратегічні пріоритети, №1.
24. Тимчук, Д. (посмертно). (2021). Інформаційний спротив: досвід інформаційної оборони України 2014–2019 років. Київ: ІС Груп.

25. Pomerantsev, P. (2019). This is Not Propaganda: Adventures in the War Against Reality. London: Faber & Faber.
26. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
27. Lucas, E., & Pomerantsev, P. (2016). Winning the Information War: Techniques and Counter-strategies Against Russian Propaganda in Central and Eastern Europe. CEPA Report.
28. Oates, S. (2020). Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere. Oxford University Press.
29. Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, 33(2), 122–139.
30. Barrett, D., et al. (2021). Disinformation and Democracy: The Internet's Influence on Political Systems. RAND Corporation.
31. Nissen, T. E. (2015). The Weaponization of Social Media. Royal Danish Defence College
32. European External Action Service (EEAS). (2023). Disinformation Review [EUvsDisinfo platform]. https://euvsdisinfo.eu
33. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats). (2024). Strategic Communication and Countering Disinformation in Europe. https://www.hybridcoe.f
34. NATO StratCom COE. (2022). Russia’s Strategy in the Information Environment: Analysis of Tactics and Narratives. Riga: NATO Strategic Communications Centre of Excellence.
35. Freedom House. (2023). Freedom on the Net: Countering an Authoritarian Overhaul of the Internet. https://freedomhouse.org

36. Council of Europe. (2023). Addressing Disinformation in the Context of Elections: Policy Toolkit. Strasbourg.
37. Ukrainian Crisis Media Center. (2022). Information Warfare: How Russia Weaponizes Media Against Ukraine and Europe. https://uacrisis.org
38. StopFake.org. (2023). Annual Report on Russian Disinformation Campaigns Targeting Ukraine and the EU. https://www.stopfake.org
39. Oxford Internet Institute. (2022). The Global Disinformation Order: 2021 Report on Organised Social Media Manipulation. University of Oxford.
40. Atlantic Council's Digital Forensic Research Lab (DFRLab). (2023). Weaponized Information: Influence Operations in the Digital Age. https://www.atlanticcouncil.org
41. Carnegie Europe. (2024). How Democracies Can Defend Against Disinformation. https://carnegieeurope.eu