

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

ННІ інститут бізнес-освіти імені Анатолія Поручника

Кафедра політичних технологій

Освітньо-професійна програма	«Публічна політика та лідерство»
Галузь знань	05 «Соціальні та поведінкові науки»
Спеціальність	052 «Політологія»

Форма здобуття освіти: заочна

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему **«Гібридні війни у сучасному міжнародному середовищі»**

здобувача **Юсипенка Кирила Олеговича**_____

Науковий керівник: к.і.н., доцент, доцент кафедри
політичних технологій Погорєлова І.С.

(підпис)

**Робота допущена до захисту перед екзаменаційною
комісією з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.політ.н., проф., Гапоненко В.А.

(підпис)

Київ 2026

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНЕ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН.....	11
1.1 Поняття та еволюція гібридної війни у науковому дискурсі.....	11
1.2 Основні компоненти гібридного впливу: військові, інформаційні, економічні, кібернетичні	14
1.3 Методологічні підходи до аналізу гібридних війн у сучасному міжнародному середовищі.....	17
РОЗДІЛ 2. ГІБРИДНІ АСПЕКТИ ВІЙН У СУЧАСНОМУ МІЖНАРОДНОМУ СЕРЕДОВИЩІ НА ПРИКЛАДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ	20
2.1. Етапи та особливості розгортання гібридної російсько-української війни	20
2.2. Інформаційні, кібернетичні та економічні інструменти гібридного впливу РФ.....	26
2.3. Вплив гібридних загроз на політичну систему України в умовах російсько-української війни.....	36
2.4. Міжнародні заходи протидії гібридним загрозам	46
РОЗДІЛ 3. УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ ПРОТИДІЇ ГІБРИДНИМ ВІЙНАМ.....	53
3.1. Механізми підвищення національної стійкості України до гібридних загроз.....	53
3.2. Вдосконалення інформаційної стійкості українського суспільства ...	62
3.3. Міжнародна співпраця і колективні заходи протидії гібридним загрозам	69
ВИСНОВКИ.....	76
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	79

ВСТУП

У сучасному світі міжнародні відносини та безпекове середовище зазнають докорінної трансформації. Класичні моделі ведення війни, засновані на прямому військовому зіткненні, дедалі частіше поступаються місцем складним, багатовимірним конфліктам, відомими як «гібридні війни». Цей феномен, що поєднує військові, політичні, економічні, інформаційні, кібернетичні та інші невійськові засоби тиску, став одним із головних викликів для глобальної стабільності у XXI столітті.

Актуальність теми дослідження зумовлена тим, що гібридні загрози руйнують традиційні уявлення про війну та мир, розмиваючи межі між ними і ставлячи під сумнів ефективність існуючих механізмів міжнародного права та безпеки. Для України ця тема має не лише теоретичне, але й гостро практичне значення, оскільки наша держава стала безпосереднім об'єктом тривалої гібридної агресії з боку Російської Федерації, що вимагає наукового осмислення цього явища. Критичний аналіз інструментів та методів гібридної війни є нагальним завданням для розробки дієвих стратегій протидії та захисту національних інтересів в умовах сучасного міжнародного середовища.

Ступінь наукової розробленості проблеми. Проблематика гібридних війн активно досліджується як вітчизняними, так і зарубіжними науковцями. Значний внесок у розробку теоретичних засад гібридної війни зробили Френк Хоффман [88], який запропонував концепцію гібридної війни як поєднання регулярних і нерегулярних методів ведення бойових дій, Томас Рід [71], що аналізує сучасні інформаційні та кібероперації у гібридних конфліктах, Стівен Мец [53], який досліджує стратегії асиметричних та гібридних конфліктів, а також Джон Дж. МакКвін [54], що концентрується на військових інноваціях та адаптації армій до нових загроз. В українському науковому дискурсі важливими є праці Олександра Литвиненка [50], який аналізує загрози національній безпеці в контексті гібридних конфліктів, Володимира Горбуліна [18], який займається стратегічними аспектами безпеки та інформаційної протидії, та Миколи Сунгуровського [76], що

досліджує політичні та соціальні механізми протидії гібридним загрозам. Так, дослідження Авер'янової Н. М. (2017), Магди Є.В. та Гетьманчука М. П. (2017) розкривають особливості російсько-української гібридної війни та інформаційного аспекту конфлікту, Галіпчак В. (2023) досліджує інформаційну складову гібридних операцій, а Воронков О. С. (2021) та Комарчук О. (2018) пропонують методологічні підходи до вивчення гібридних війн. Для аналізу інформаційної протидії та стратегічних комунікацій використані роботи Войтенкова Р. М. (2024), Денисюк Ж. З. (2021, 2025), Кондратюк-Антонової Т. В. та Тучака В. Р. (2023), а також сучасні дослідження Ульяненка К. В. (2025) та Христової А. О. і Кулінської А. В. (2023). Джерела вивчення кібербезпеки включають праці Гнатюка С. О. (2020), Дубова Д. В. (2014).

Проте, незважаючи на наявність фундаментальних досліджень, залишається недостатньо опрацьованим питання систематизації інструментів гібридного впливу, їхнього застосування та адаптації міжнародних механізмів реагування. Бракує й комплексних досліджень, які б систематизували механізми адаптації міжнародних інституцій до гібридних загроз та аналізували довгострокові наслідки гібридних воєн для світового порядку.

Мета і завдання дослідження. Метою кваліфікованої роботи є аналіз гібридних війн у сучасному міжнародному середовищі на прикладі гібридної агресії Російської Федерації проти України та розробці рекомендацій щодо підвищення ефективності публічної політики та міжнародного співробітництва у сфері протидії гібридним загрозам.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. визначити поняття гібридної війни та дослідити її еволюцію;
2. проаналізувати основні компоненти гібридного впливу: військові, інформаційні, економічні та кібернетичні;
3. розглянути методологічні підходи до аналізу гібридних війн у сучасному міжнародному середовищі;
4. оцінити аспекти й еволюцію гібридної агресії Російської Федерації проти України та її вплив на політичну систему держави;

5. розробити рекомендації щодо вдосконалення публічної політики України та міжнародного співробітництва у сфері протидії гібридним загрозам.

Об'єкт і предмет дослідження. Об'єктом дослідження кваліфікаційної магістерської роботи є гібридні війни та механізми гібридного впливу у сучасному міжнародному середовищі. Предметом дослідження постає сутність, інструменти, форми та наслідки гібридних воєн у сучасному міжнародному середовищі на прикладі війни РФ проти України.

Для розв'язання поставлених завдань у роботі використано комплекс загальнонаукових та спеціальних **методів**, а саме:

1. аналіз та синтез - для систематизації наукових підходів до вивчення гібридних війн;
2. порівняльний метод - для зіставлення різних проявів гібридних загроз у міжнародній практиці;
3. історичний метод - для дослідження еволюції гібридних війн та їх проявів на прикладі російсько-української війни;
4. системний підхід - для комплексного вивчення взаємозв'язків між компонентами гібридного впливу;
5. методи експертних оцінок та аналізу стратегічних документів - для визначення ефективності заходів протидії гібридним загрозам і розробки рекомендацій щодо публічної політики.

Теоретична значущість отриманих результатів полягає у розширенні наукового розуміння сутності, механізмів та форм гібридних воєн у сучасному міжнародному середовищі, а також у систематизації знань про способи протидії гібридним загрозам на прикладі війни РФ проти України.

Практична значущість роботи полягає у тому, що отримані результати можуть бути використані для вдосконалення публічної політики України, підвищення національної стійкості та інформаційної безпеки українського суспільства, а також для розвитку міжнародного співробітництва у сфері протидії гібридним загрозам. Матеріали дослідження можуть бути використані у

діяльності органів державної влади, аналітичних центрів, а також у навчальному процесі.

Інформаційна база дослідження включає наукові праці вітчизняних та зарубіжних авторів у галузі гібридних війн, міжнародних відносин, політології та безпекових студій. Використано матеріали державних установ (СІР, НАБУ, Держспецзв'язку). Важливу роль відіграють аналітичні публікації міжнародних дослідницьких центрів, таких як Center for European Policy Analysis (CEPA, 2025), збірники доповідей наукових конференцій (Acta de Historia & Politica, 2021; Мальський М. та ін., 2025), а також статті й матеріали українських та міжнародних медіа (Радіо Свобода, 2021; Ukrinform, 2025; Detektor Media, 2018). Крім того, були використані правові акти та закони України для контексту дослідження національної безпеки (Закон України «Про національну безпеку», 2018; Указ Президента України № 392/2020).

Структура роботи. Магістерська кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 95 найменувань. Основний зміст роботи викладено на 72 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНЕ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН

1.1. Поняття та еволюція гібридної війни у науковому дискурсі

Сучасне міжнародне безпекове середовище характеризується стрімкою трансформацією характеру міждержавних конфліктів. На початку XXI століття класична війна, заснована на прямому зіткненні збройних сил, дедалі частіше поступається місцем складним, багатовимірним формам агресії. У цьому контексті поняття «гібридна війна» (*hybrid warfare*) стало одним із найбільш обговорюваних, але водночас і найбільш суперечливих термінів у сучасному науковому та політичному дискурсі [79, с. 72]. Аналіз сучасного стану наукової думки засвідчує відсутність єдиного, універсально визнаного визначення цього феномену. Ця концептуальна невизначеність частково зумовлена самою природою гібридної війни, яка полягає у розмиванні меж - між станом війни та миру, між військовими та цивільними цілями, між комбатантами та некомбатантами, а також між різними сферами протиборства (політичною, економічною, інформаційною та військовою). Еволюція концепції гібридної війни має глибоке коріння, адже поєднання військових та невійськових методів боротьби є давнім, як і сама війна. Ще давньокитайський стратег Сунь-цзи наголошував на перевазі перемоги без битви, використовуючи обман, шпигунство та маніпуляції [72]. Проте, як науковий термін, «гібридна війна» набула поширення на початку 2000-х років.

Важливою фігурою в популяризації терміну вважається американський військовий аналітик Френк Хоффман. У своїх працях він визначив гібридну війну як поєднання конвенційних збройних сил, нерегулярних (партизанських, терористичних) тактик, злочинної діяльності та інформаційного впливу, що синхронно застосовуються одним актором для досягнення стратегічних цілей [19]. Поштовхом для його аналізу стала, зокрема, війна в Лівані 2006 року, де «Хезболла» продемонструвала здатність поєднувати партизанські методи з використанням сучасних озброєнь та потужною інформаційною кампанією. Проте

справжньої гостроти та практичного значення термін набув після агресії Російської Федерації проти України у 2014 році. Ці події стали класичним прикладом гібридної війни нового покоління. Росія продемонструвала комплексне застосування:

1. політичного тиску (дипломатичний шантаж, підтримка маріонеткових режимів);
2. економічного впливу (торговельні війни, енергетичний шантаж);
3. інформаційно-психологічних операцій (масштабна дезінформація, пропаганда, розпалювання ворожнечі);
4. кібернетичних атак (втручання в роботу державних установ, об'єктів інфраструктури).

Нова реальність стимулювала активну дискусію щодо природи російської стратегії. Часто згадується так звана «доктрина Герасимова», хоча, як справедливо зазначає британський дослідник Марк Галеотті (Mark Galeotti), це радше інтерпретація Заходом статті начальника ГШ РФ, а не офіційна доктрина. Галеотті пропонує термін «нелінійна війна», підкреслюючи, що в російському баченні невійськові методи (політичні, інформаційні, економічні) за своєю ефективністю часто перевищують військову силу.

Огляд вітчизняних наукових джерел показує значне опрацювання теми гібридної війни крізь призму національної безпеки України. Праці Володимира Горбуліна, Георгія Почепцова, Євгена Магди та інших українських фахівців детально аналізують інструментарій та наслідки гібридної агресії РФ. Зокрема, Георгій Почепцов акцентує увагу на домінуванні інформаційно-сміслової складової, де боротьба ведеться не стільки за території, скільки за контроль над свідомістю та сприйняттям реальності. Володимир Горбулін розглядає гібридну війну як екзистенційний виклик для державності України [15]. Різні автори визначають гібридну війну по-своєму. Френк Хоффман (2009) описує її як поєднання регулярних та нерегулярних форм війни, у тому числі асиметричних дій та інструментів інформаційного впливу [97]. Олександр Литвиненко (2017) визначає гібридну війну як системну комбінацію військових, політичних,

економічних та інформаційних заходів, спрямованих на дестабілізацію держави [73]. Євген Магда (2015) підкреслює, що гібридна війна - це форма конфлікту, де традиційні військові методи доповнюються психологічним, медіа- та кібервпливом для досягнення політичних цілей [51]. Микола Плакида (2025) розглядає її як комплексну взаємодію військових, економічних, інформаційних та культурних інструментів у режимі постійного тиску на державу та суспільство [39]. Незважаючи на широке вживання, термін «гібридна війна» залишається предметом наукової критики. Деякі дослідники вважають його надто широким, стверджуючи, що будь-яка війна в історії була певною мірою «гібридною». Критики вказують, що новизна полягає не в самих методах, а в інтенсивності, синхронізації та глобальному охопленні цих методів, зумовлених технологічним розвитком (інтернет, соціальні мережі, глобальні фінансові системи). Головне проблемне питання полягає не в тому, чи є феномен гібридної війни новим, а в тому, як саме технологізація та глобалізація змінили його характер, зробивши його ключовим інструментом ревізіоністських держав у сучасному міжнародному середовищі.

Виходячи з аналізу наявних концепцій, у магістерській роботі під гібридною війною розуміється стратегія досягнення політичних цілей, що передбачає скоординоване, адаптивне та синхронізоване застосування державним або недержавним актором конвенційних військових засобів, нерегулярних збройних формувань, а також невійськових інструментів тиску (політичних, економічних, енергетичних, інформаційно-психологічних та кібернетичних) з метою дестабілізації супротивника, підриву його інституційної спроможності та легітимності, уникаючи при цьому порогу повномасштабної конвенційної війни та розмиваючи юридичну відповідальність за агресію [94, с. 12]. Гібридна війна є не просто новою формою конфлікту, а системним викликом для міжнародної безпеки, який потребує комплексного міждисциплінарного аналізу. Її дослідження має спиратися на поєднання політичної науки, безпекових студій, комунікацій, кібернетики та міжнародного права.

1.2. Основні компоненти гібридного впливу: військові, інформаційні, економічні, кібернетичні

Гібридна війна як форма сучасного конфлікту базується на синергії різних інструментів впливу, які застосовуються одночасно або послідовно, залежно від стратегічних цілей. Її багатовимірність дозволяє агресору уникати прямої відповідальності, зберігаючи видимість мирного співіснування. Наведемо основні компоненти гібридного впливу:

1. Військовий. У гібридній війні військова складова часто відіграє непряму, приховану, але критично важливу роль. На відміну від класичної війни, її мета полягає не стільки у повному розгромі збройних сил противника, скільки у створенні контрольованого хаосу, дестабілізації, виснаженні та примусі супротивника до політичних поступок. Важливим елементом є використання проксі-сил - нерегулярних збройних формувань, найманців, приватних військових компаній та місцевих колабораціоністських угруповань, які фінансуються, озброюються та скеровуються державою-агресором. Такий підхід дозволяє формально залишатися «осторонь» конфлікту й зберігати можливість «правдоподібного заперечення» (plausible deniability) своєї участі на міжнародній арені [51, с. 2]. Значну роль відіграють і операції сил спеціального призначення, спрямовані на розвідку, диверсії, саботаж, а також організацію та підготовку місцевих повстанських рухів.

У межах гібридної агресії часто застосовуються й регулярні війська, але у обмежених та маскованих формі - під виглядом «миротворців», «добровольців» або під час раптових «навчань» біля кордонів, як це, зокрема, продемонструвала РФ у 2014 році із застосуванням «зелених чоловічків» у Криму. Завдання таких підрозділів полягає в отриманні переваги у ключових точках і швидкому захопленні територій, поки противник дезорієнтований. Водночас важливим інструментом стає створення зон A2/AD (Anti-Access/Area Denial), що передбачає розгортання сучасних систем протиповітряної оборони та протикорабельних комплексів із метою блокування доступу третіх сторін, зокрема НАТО, до території конфлікту.

2. Інформаційно-психологічний компонент (Information Component). Цей аспект є одним із центральних компонентів гібридної війни, який часто передує військовій фазі та супроводжує її на всіх етапах. Як зазначав Георгій Почепцов, сучасні війни ведуться за «контроль над свідомістю», тоді як територія стає лише похідною ціллю [122]. Інструментарій інформаційного впливу надзвичайно широкий і включає стратегічну пропаганду та дезінформацію, які реалізуються через державні ЗМІ, такі як RT або Sputnik, соціальні мережі та мережі ботів для створення системних неправдивих наративів, спрямованих на дискредитацію уряду країни-цілі, її союзників і демократичних цінностей. Значну роль відіграють інформаційно-психологічні операції (ІПСО), що передбачають цілеспрямовані дії з деморалізації населення та збройних сил противника, розпалювання внутрішніх конфліктів на етнічному, релігійному або політичному ґрунті, а також поширення паніки та недовіри до влади. Одночасно активно використовується маніпуляція суспільною думкою через створення та швидке поширення фейкових новин, що впливає на прийняття рішень, зокрема на виборчі процеси в інших державах. Додатково застосовується так звана «дипломатія хаосу», коли офіційні дипломатичні канали використовуються для поширення дезінформації та висування свідомо неприйнятних ультиматумів, що фактично продовжує інформаційну війну.

3. Економічний компонент (Economic Component). Економічний тиск є одним із ключових інструментів гібридної агресії, що використовується для підриву соціально-економічної стабільності країни-цілі, виснаження її ресурсів і створення у населення відчуття безвиході, яке підсилює ефективність інформаційних операцій. Серед основних методів економічної війни вирізняється енергетичний шантаж, що полягає у використанні домінуючого становища на ринку енергоносіїв - газу та нафти - для політичного тиску, маніпуляції цінами або прямого припинення постачання. Важливу роль відіграють також торговельні війни та ембарго, коли агресор запроваджує заборону на імпорт ключових товарів із країни-цілі, як це було у випадку блокування українських товарів у РФ, що завдає удару цілим секторам економіки. До цього додається інструмент

економічної корупції: підтримка й фінансування лояльних політичних та бізнесових еліт усередині країни-цілі з метою просування власних економічних інтересів і саботажу рішень, які суперечать стратегії агресора. Нарешті, ще одним напрямом впливу є штучне створення економічної нестабільності, що може проявлятися у атаках на фінансову систему, провокуванні відтоку капіталу та девальвації національної валюти.

4. Кібернетичний компонент (Cyber Component). Кіберпростір перетворився на повноцінне поле бою, де операції здатні завдати шкоди, співставної з наслідками військового удару. Цей компонент тісно пов'язаний з інформаційною сферою, проте має і самостійне значення. Кібервійна охоплює кілька напрямів, серед яких атаки на критичну інфраструктуру, що передбачають виведення з ладу енергетичних систем, транспортних вузлів, банківських мереж чи урядових комунікацій; показовими прикладами є атака BlackEnergy на Прикарпаттяобленерго у 2015 році та кібератака NotPetya у 2017 році. Важливим інструментом є кібершпигунство, спрямоване на злам урядових і військових баз даних з метою отримання конфіденційної інформації. До цього додаються онлайн-дезінформаційні кампанії, у межах яких використовуються «фабрики тролів» та ботоферми для маніпуляції громадською думкою в соціальних мережах, що доповнює традиційні інформаційно-психологічні операції. Ще одним засобом впливу є псування та блокування веб-ресурсів, коли здійснюються атаки на сайти державних інституцій та провідних ЗМІ з метою підризу довіри та поширення паніки.

Узагальнюючи, зазначимо, що сила гібридної війни полягає не в окремих її компонентах, а у їхній комплексній інтеграції. Економічний тиск посилюється інформаційною панікою, яку, у свою чергу, підживлюють кібератаки, тоді як військова загроза на кордоні створює тло, що робить усі невійськові інструменти впливу значно дієвішими. Розуміння цієї взаємодії є ключовим для аналізу сучасних конфліктів і формування ефективних механізмів протидії.

1.3. Методологічні підходи до аналізу гібридних війн у сучасному міжнародному середовищі

У сучасному міжнародному середовищі феномен гібридна війна має комплексний, багатовимірний характер, що поєднує військові, інформаційні, кібернетичні, економічні та психологічні засоби впливу. Це вимагає від дослідників застосування відповідної методології, яка б змогла охопити всю багатофакторність, швидку трансформацію та невизначеність. Методологічні підходи до аналізу гібридних війн становлять надзвичайно важливу складову наукових досліджень у сфері безпеки, політики та міжнародних відносин. Гібридна війна - це не лише поєднання різних форм і методів ведення збройної боротьби, а й явище, що відображає новий тип глобальної конфронтації, де стираються межі між війною і миром, між внутрішніми та зовнішніми загрозами, між фізичним і віртуальним простором. Саме тому для її аналізу потрібна гнучка, інтегративна й багатовимірна методологія, що дозволяє всебічно оцінювати політичні, економічні, інформаційні, соціальні та психологічні чинники, які формують характер і динаміку гібридного протистояння.

Одним із базових підходів є системний підхід, який дає змогу розглядати гібридну війну як цілісну систему, що складається з взаємопов'язаних елементів - політичних рішень, військових дій, дипломатичних кроків, економічного тиску, інформаційних кампаній, кібератак, соціальних протестів тощо. Кожен з цих елементів має власну логіку функціонування, проте лише у взаємодії вони створюють комплексний вплив, спрямований на досягнення стратегічних цілей агресора. Системний підхід дозволяє ідентифікувати ключові ланки цієї системи, визначити взаємозв'язки між різними типами впливів і зрозуміти, як вони посилюють один одного.

Важливе значення має міждисциплінарний підхід, який поєднує інструменти політичної науки, військової стратегії, міжнародного права, психології, соціології, інформаційних технологій, медіазнавства та економіки. Такий підхід допомагає побачити гібридну війну не лише як воєнну операцію, а як довготривалий процес підриву стійкості держави, дестабілізації її інституцій та

суспільної свідомості. Наприклад, аналіз пропагандистських кампаній вимагає медіалінгвістичних методів, вивчення впливу соціальних мереж - цифрової аналітики, а дослідження соціальних настроїв - соціологічних опитувань і психологічних тестів. Міждисциплінарність дозволяє створити багаторівневу картину гібридного конфлікту, що охоплює як матеріальні, так і нематеріальні аспекти [68, с. 23]. Значну роль у дослідженні гібридних воєн відіграє конфліктологічний підхід, який орієнтований на виявлення причин, динаміки, фаз і наслідків гібридних конфліктів. Цей підхід розглядає гібридну війну як особливу форму соціально-політичного конфлікту, де класичні воєнні дії поєднуються з маніпуляціями суспільною думкою, підривною діяльністю та внутрішньополітичними кризами. Він допомагає зрозуміти, як гібридна стратегія формує «контрольований хаос» - стан, у якому суспільство втрачає орієнтири, а зовнішній агресор отримує можливість впливати на політичні процеси з мінімальними витратами. Окрему увагу заслуговує інформаційно-комунікативний підхід, який досліджує роль інформації як інструмента зброї. Сучасні гібридні війни дедалі частіше ведуться у сфері комунікацій - через медіа, соціальні мережі, інтернет-платформи, блогосферу. Інформаційні атаки, фейки, дезінформація, «інформаційні вкиди», маніпуляції історичною пам'яттю чи емоціями - все це використовується для зміни сприйняття реальності, створення ворожих наративів і підриву довіри до влади. Цей підхід передбачає застосування методів контент-аналізу, дискурс-аналізу, когнітивного моделювання, що дозволяє оцінити ефективність інформаційного впливу та розробити контрстратегії.

Важливим напрямом є кібернетичний підхід, який аналізує використання кіберпростору як поля бою. Гібридна війна активно використовує інструменти кіберагресії - від атак на критичну інфраструктуру до кібершпигунства, викрадення даних, зламу банківських систем, втручання у виборчі процеси. Цей підхід поєднує технічний аналіз із політичним і правовим, оскільки кібератаки часто маскуються під діяльність «невідомих хакерів», що ускладнює їхнє відстеження і відповідь з боку міжнародної спільноти. Важливою складовою є

геополітичний і цивілізаційний підхід, який розглядає гібридні війни як інструмент боротьби за вплив у глобальному світі. З цієї перспективи, гібридна агресія є не лише військовою чи інформаційною операцією, а формою геостратегічного суперництва між державами або блоками держав. Вона відображає зіткнення різних моделей розвитку, систем цінностей, політичних культур і способів мислення. Такий підхід дозволяє виявити, як гібридні війни змінюють структуру міжнародних відносин, формують нові центри сили й дестабілізують старі системи безпеки. Не менш важливим є соціально-психологічний підхід, який зосереджується на дослідженні впливу гібридної війни на суспільну свідомість, моральний стан населення, поведінку мас і рівень довіри до інститутів влади. Гібридна агресія часто спрямована на посилення страху, розколу, апатії чи агресії в суспільстві. Психологічні операції (PSYOPS) стають ефективним інструментом управління поведінкою людей без фізичного насильства.

Отже, методологія дослідження гібридних воєн у сучасному міжнародному середовищі є комплексною і динамічною системою, що поєднує різні наукові підходи та інструменти. Вона вимагає не лише аналізу фактів, а й глибокого розуміння закономірностей взаємодії між політичними, інформаційними, військовими, економічними й культурними чинниками. У добу цифрових технологій і глобальної взаємозалежності гібридні війни стають однією з головних загроз міжнародній стабільності. Саме тому розроблення сучасних методологічних підходів до їх аналізу є ключовою умовою формування дієвих стратегій національної безпеки, інформаційної стійкості та колективної оборони у світі, що перебуває у постійному стані «гібридного миру» [58, с. 14].

РОЗДІЛ 2. ГІБРИДНІ АСПЕКТИ ВІЙН У СУЧАСНОМУ МІЖНАРОДНОМУ СЕРЕДОВИЩІ НА ПРИКЛАДІ РОСІЙСЬКО- УКРАЇНСЬКОЇ ВІЙНИ

2.1. Етапи та особливості розгортання гібридної російсько-української війни

Російсько-українська гібридна війна розпочалася задовго до 2014 року, коли Москва систематично використовувала комплекс невійськових засобів для дестабілізації України. Перший етап характеризувався активним інформаційно-пропагандистським впливом через російські медіа, які формували негативний образ української державності та європейського вибору країни. Кремль послідовно впроваджував наратив про «штучність» української нації та необхідність повернення до «російського світу» [59]. Цей період супроводжувався економічним тиском через енергетичні важелі, коли Газпром регулярно маніпулював цінами на природний газ залежно від геополітичної позиції Києва. Дипломатичні канали використовувалися для блокування євроінтеграційних прагнень України через залучення механізмів Митного союзу та Євразійського економічного простору. РФ методично створювала передумови для майбутньої воєнної агресії, формуючи агентурні мережі та підтримуючи проросійські політичні сили в Україні.

Другий етап розгорнувся після Революції Гідності наприкінці 2013 - на початку 2014 року, коли Росія перейшла до активної фази гібридної агресії проти України. Анексія Автономної Республіки Крим відбулася за класичним сценарієм гібридної операції з використанням «зелених чоловічків» - російських військовослужбовців без розпізнавальних знаків. Кремль застосував комбінацію військової сили, інформаційних операцій та псевдолегітимних політичних процедур для захоплення українського півострова. Блокування українських військових частин здійснювалося одночасно з масованою пропагандистською кампанією про «захист російськомовного населення» та «повернення до історичної батьківщини». Швидкість операції та відсутність офіційного визнання участі російських збройних сил стали взірцем гібридної тактики, що дозволила

Москві уникнути міжнародної ізоляції на початковому етапі. Незаконний «референдум» 16 березня 2014 року завершив формальне закріплення окупації Криму, продемонструвавши ефективність поєднання військових та політико-дипломатичних інструментів гібридної війни [64, с. 194].

Третій етап характеризувався поширенням гібридної агресії на Донецьку та Луганську області, де Росія застосувала дещо відмінну модель дестабілізації порівняно з кримським сценарієм. Москва активізувала місцеві сепаратистські рухи, забезпечуючи їх озброєнням, фінансуванням та військовими інструкторами під виглядом «добровольців» та «ополченців». Створення псевдодержавних утворень «ДНР» та «ЛНР» супроводжувалося захопленням адміністративних будівель, правоохоронних органів та об'єктів критичної інфраструктури. Російські регулярні війська безпосередньо брали участь у бойових діях, приховуючи свою присутність через відсутність розпізнавальних знаків та офіційні заперечення Кремля. Інформаційна складова конфлікту полягала у створенні образу «громадянської війни» та «боротьби народу Донбасу проти київської хунти», що дозволяло Москві уникати прямої відповідальності за агресію. Підписання Мінських угод у 2014-2015 роках не припинило конфлікт, а лише зафіксувало статус-кво, який влаштовував Росію для подальшого тиску на Україну.

Четвертий етап охопив період 2015-2021 років, коли Росія підтримувала стан «контрольованої нестабільності» на Донбасі паралельно з посиленням гібридного тиску на інших напрямках. Кремль систематично порушував режим припинення вогню, здійснював терористичні акти на підконтрольній Україні території та проводив масштабні кібератаки на критичну інфраструктуру. Економічна блокада окупованих територій поглиблювала їхню залежність від Росії, перетворюючи ці регіони на інструмент шантажу української влади. Дипломатичні зусилля Москви концентрувалися на легітимізації окупаційних адміністрацій через Мінські домовленості та блокування ініціатив щодо розміщення миротворчого контингенту ООН. Інформаційні операції еволюціонували у бік використання соціальних мереж та альтернативних медіа для поширення дезінформації та поглиблення суспільних розколів в Україні. Росія

послідовно нарощувала військову присутність біля українського кордону, проводячи регулярні навчання та демонструючи готовність до ескалації конфлікту [36, с. 190].

П'ятий етап розпочався у 2022 році з повномасштабного вторгнення російських військ на територію України, що ознаменувало трансформацію гібридної війни у відкриту збройну агресію з елементами гібридних операцій. Кремль застосував класичні військові операції, поєднуючи їх з масованими кібератаками, інформаційно-психологічними операціями та економічною війною. Спроби швидкого захоплення Києва та інших обласних центрів провалилися через ефективний опір українських збройних сил та добровольчих формувань. Росія адаптувала тактику, переходячи до затяжної війни на виснаження з систематичними обстрілами цивільної інфраструктури та енергетичних об'єктів. Інформаційна складова конфлікту набула глобального масштабу, коли Москва намагалася виправдати агресію через конструювання наративів про «денацифікацію» та «демлітаризацію» України. Гібридний характер війни проявлявся у використанні енергетичної зброї проти європейських партнерів України, організації міграційних криз та проведенні операцій впливу на міжнародну громадську думку.

Шостий етап характеризується закріпленням довгострокового протистояння з елементами позиційної війни та продовженням гібридних операцій на всіх рівнях міжнародної системи. Росія намагається легітимізувати окупацію захоплених територій через організацію псевдореферендумів та інкорпорацію цих регіонів до складу Російської Федерації всупереч нормам міжнародного права. Економічна складова гібридної війни трансформувалася у глобальне протистояння між Заходом та Росією з санкціями, контрсанкціями та боротьбою за енергетичні ринки. Інформаційні операції Кремля спрямовані на підірив міжнародної підтримки України через поширення наративів про «втому від війни» та необхідність компромісу з агресором. Кібернетичний простір залишається ареною постійного протиборства, де російські хакерські групи атакують критичну інфраструктуру України та країн-союзників. Дипломатична

діяльність Москви концентрується на блокуванні ініціатив щодо притягнення Росії до відповідальності за воєнні злочини та порушення міжнародного гуманітарного права [52, с. 112].

Особливості російсько-українського гібридного конфлікту полягають у безпрецедентній тривалості та інтенсивності застосування невійськових засобів паралельно з військовою агресією. Кремль демонструє здатність швидко адаптувати тактику залежно від ефективності українського опору та реакції міжнародної спільноти. Використання енергетичної залежності європейських країн як інструменту тиску на Україну стало характерною рисою цього конфлікту. Інформаційні операції Росії відрізняються масштабністю охоплення аудиторії та координацією між державними пропагандистськими каналами, агентами впливу та мережевими структурами. Кібернетична складова конфлікту еволюціонувала від точкових атак до системних кампаній, спрямованих на паралізацію критичної інфраструктури та державного управління.

Стратегічна мета російської гібридної агресії полягає не лише у територіальних захопленнях, а й у демонтажі української державності та перешкодженні її євроатлантичній інтеграції. Москва прагне створити модель «керованого хаосу», де Україна постійно перебуватиме у стані нестабільності та залежності від російських рішень. Гібридна війна дозволяє Кремлю уникати прямої відповідальності за агресію, приховуючи військову присутність за маскою «добровольців» та «повстанців». Комбінація різноманітних інструментів впливу створює синергетичний ефект, коли економічний тиск підсилюється інформаційними операціями, а військові дії супроводжуються дипломатичним шантажем. Російська модель гібридної війни стала викликом для традиційних механізмів міжнародної безпеки, які виявилися неефективними у протидії такому типу агресії [42, с. 48].

Українська відповідь на гібридну агресію еволюціонувала від несистемних заходів до комплексної стратегії національної стійкості та оборони. Київ розробив механізми протидії інформаційним операціям через створення системи стратегічних комунікацій та спростування російської пропаганди. Посилення

кібербезпеки стало пріоритетом після серії успішних російських атак на енергетичну інфраструктуру та державні інформаційні системи. Економічна політика України спрямована на диверсифікацію енергетичних джерел та зменшення залежності від російських поставок. Дипломатичні зусилля концентруються на залученні міжнародної підтримки через багатосторонні механізми та двосторонні партнерства з демократичними державами. Досвід протистояння російській гібридній агресії демонструє необхідність цілісного підходу до національної безпеки, що охоплює військові, інформаційні, економічні та соціальні виміри. Україна розробила унікальну модель реагування на гібридні загрози, яка базується на залученні громадянського суспільства, волонтерського руху та міжнародних партнерів. Створення Сил територіальної оборони та кіберволонтерських груп стало відповіддю на асиметричну природу російської агресії [69]. Економічна реформа системи управління та боротьба з корупцією зміцнили інституційну спроможність держави протистояти зовнішнім викликам [63, с. 187].

Регіональний вимір російсько-українського конфлікту проявляється у різній інтенсивності гібридного впливу на окремі області України залежно від етнічного складу, економічної структури та історичної спадщини. Схід та Південь країни зазнали найбільшого тиску через традиційні зв'язки з Росією та присутність російськомовного населення [32]. Центральні та Західні регіони демонстрували вищу стійкість до російської пропаганди, що пояснюється сильнішою національною ідентичністю та проєвропейськими настроями населення. За даними Київського міжнародного інституту соціології (КМІС, 2021), у Західному регіоні 70 % опитаних підтримували приєднання України до ЄС, у Центральному - 57,6 %, тоді як на Півдні лише 37 %, а на Сході - 25,9 % [61]. Подібна тенденція простежується і щодо орієнтації на НАТО, де Захід та Центр відзначаються вищим рівнем підтримки, ніж Схід та Південь. Фонд Демократичні Ініціативи ім. Ілька Кучеріва спільно з Центром Разумкова (2016) також вказує на те, що на Сході і Півдні частіше підтримували компроміси з проросійськими політичними рішеннями, тоді як Захід і Центр більш однозначно виступали проти таких кроків

[92]. Кримський півострів вважається особливо уразливим до гібридної агресії РФ через специфічну демографічну ситуацію, присутність Чорноморського флоту Росії та обмежену територіальну зв'язність з материковою Україною. Донбас став об'єктом гібридної операції через поєднання економічних проблем, російського інформаційного домінування та наявності сепаратистського потенціалу серед частини населення. Проте слід зазначити, що немає відкритих репрезентативних соціологічних даних для Криму та окупованих районів Донбасу, оскільки доступ до цих територій обмежений [61]. Тому висновки щодо «найуразливіших» регіонів слід розглядати як гіпотезу, підкріплену історичними, демографічними та геополітичними обставинами.

Міжнародна реакція на російську гібридну агресію проти України пройшла шлях від обережних заяв до комплексних санкцій та військової допомоги Києву. НАТО посилило східний фланг альянсу та розгорнуло додаткові сили у країнах Балтії та Польщі як відповідь на російську загрозу. Європейський Союз запровадив секторальні санкції проти російської економіки, хоча їхня ефективність залишається предметом дискусій. США надали Україні летальну зброю та фінансову допомогу для зміцнення обороноздатності. Організація Об'єднаних Націй засудила російську агресію через резолюції Генеральної Асамблеї, проте Рада Безпеки залишилася паралізованою через право вето Москви [16]. Міжнародне кримінальне право активізувалося через розслідування воєнних злочинів та злочинів проти людяності, скоєних російськими військами на території України [66, с. 34].

Трансформація російсько-українського конфлікту від локальної гібридної операції до повномасштабної війни засвідчила обмеженість гібридних стратегій у досягненні стратегічних цілей без застосування прямої військової сили. Кремль змушений був відмовитися від маскування агресії та перейти до відкритого вторгнення через неефективність попередніх гібридних інструментів у поваленні української влади. Стійкість українського суспільства та держави спростувала розрахунки Москви на швидку перемогу через внутрішню дестабілізацію та інформаційно-психологічний тиск. Консолідація української нації перед

обличчям агресії стала несподіваним результатом російської політики, що мала на меті розколоти та послабити Україну. Міжнародна підтримка України зросла після початку повномасштабного вторгнення, демонструючи, що відкрита агресія мобілізує глобальну спільноту ефективніше, ніж гібридні операції.

2.2. Інформаційні, кібернетичні та економічні інструменти гібридного впливу РФ

Інформаційна війна Росії проти України базується на системному використанні пропаганди, дезінформації та маніпуляції громадською думкою через контрольовані державою медіа та мережеві ресурси. Кремль створив потужну інфраструктуру впливу, що включає телевізійні канали, радіостанції, інтернет-видання та акаунти в соціальних мережах, які транслюють узгоджені наративи про Україну та російсько-український конфлікт. Центральним елементом російської інформаційної стратегії є конструювання альтернативної реальності, де Україна постає як «нацистська держава», «колонія Заходу» або «штучне утворення без історичного права на існування». Ці наративи систематично повторюються через різноманітні канали комунікації, створюючи ефект правдоподібності завдяки багаторазовій рециркуляції однієї інформації. Російські пропагандисти вправно поєднують елементи правди з вигадками, роблячи дезінформацію складнішою для виявлення та спростування. Цільовими аудиторіями виступають як внутрішні споживачі в Росії, так і міжнародна спільнота, зокрема населення європейських країн та глобального Півдня.

Технології інформаційного впливу еволюціонували від традиційної пропаганди через телебачення до складних операцій в цифровому просторі з використанням ботів, тролів та алгоритмічного підсилення потрібних меседжів. Фабрики тролів, найвідомішою з яких є петербурзьке «Агентство інтернет-досліджень», координують масовані кампанії з поширення дезінформації та розпалювання дискусій у соціальних мережах. Ці структури створюють тисячі фейкових акаунтів, які імітують справжніх користувачів та генерують контент,

спрямований на дискредитацію України, посилення суспільних розколів та підрив довіри до державних інституцій. Автоматизовані боти підсилюють охоплення деструктивних меседжів, штучно формуючи враження масової підтримки певних позицій чи поширеності певних думок. Російські інформаційні операції характеризуються високим рівнем координації між різними акторами - державними медіа, псевдонезалежними виданнями, блогерами та агентами впливу у західних країнах. Використання емоційних тригерів, страху, обурення та недовіри дозволяє російським пропагандистам ефективно впливати на психологічний стан аудиторії [74, с. 46].

Тематичні напрямки російської інформаційної агресії охоплюють широкий спектр питань від історичної легітимності української державності до поточних політичних та економічних процесів в країні. Кремль систематично намагається переписати історію, применшуючи український внесок у перемогу над нацизмом, заперечуючи Голодомор як геноцид українського народу та конструюючи наратив про «єдиний російський народ» [17]. Дискредитація української влади здійснюється через постійні звинувачення у корупції, некомпетентності та залежності від західних покровителів. Російська пропаганда активно експлуатує реальні проблеми українського суспільства - економічні труднощі, соціальну нерівність, міграцію, перебільшуючи їх масштаб та приписуючи їх виключно діям київської влади. Євроатлантичний вибір України представляється як «зрада національних інтересів» та втрата суверенітету на користь Брюсселя та Вашингтона. Етнічні та мовні питання інструменталізуються для розпалювання конфліктів між різними групами українського населення.

Дезінформаційні кампанії Росії під час активної фази війни набули особливої інтенсивності та цинічності, коли Кремль систематично заперечував скоєння воєнних злочинів, приписував їх українській стороні або називав постановками та фейками. Масові вбивства цивільних у Бучі, Ірпені, Маріуполі та інших населених пунктах російські пропагандисти намагалися дискредитувати через десятки суперечливих версій від повного заперечення до звинувачень української армії у самострілянині [95]. Обстріли цивільної інфраструктури,

лікарень, шкіл та пологових будинків представляються як «звільнення від нацистів» або звинувачується українська сторона у розміщенні військових об'єктів у житлових кварталах. Інформація про катування, сексуальне насильство та депортацію українських дітей заперечується або виправдовується необхідністю «захисту» від української влади. Російські медіа конструюють паралельну реальність, де агресор постає жертвою, а справжні жертви звинувачуються у провокаціях [13, с. 26].

Кібернетична складова гібридної агресії Росії проти України розпочалася ще до 2014 року та послідовно нарощувалася за масштабом і складністю атак на критичну інфраструктуру держави. Перші масштабні кібератаки зафіксовані ще у 2013-2014 роках, коли хакерські групи, пов'язані з російськими спецслужбами, намагалися паралізувати урядові веб-сайти під час Революції Гідності. Енергетична система України стала головною мішенню російських кібероператорів, коли у грудні 2015 року відбулася перша в історії успішна кібератака на енергомережу, що призвела до відключення електропостачання для понад 200 тисяч споживачів. Атака продемонструвала спроможність російських хакерів проникати у промислові системи управління та маніпулювати ними для досягнення фізичних наслідків. Наступна хвиля кібератак у 2016-2017 роках підтвердила системний характер російських дій та їхню координацію з іншими компонентами гібридної війни [40, с. 78].

Шкідливе програмне забезпечення NotPetya, випущене у червні 2017 року, стало найруйнівнішою кібератакою в історії з глобальними наслідками, хоча первинною мішенню була саме Україна [55]. Вірус-шифрувальник паралізував роботу українських банків, урядових установ, телекомунікаційних компаній, транспортної інфраструктури та приватних підприємств. Атака здійснювалася через компрометацію програмного забезпечення для бухгалтерського обліку, яке використовувала більшість українських компаній для взаємодії з податковою службою. Економічні збитки від NotPetya в Україні оцінюються у сотні мільйонів доларів, а глобальні втрати перевищили 10 мільярдів доларів. Міжнародне співтовариство офіційно визнало причетність російських спецслужб до розробки

та поширення цього зловмисного коду. Атака продемонструвала готовність Кремля використовувати кіберпростір для завдання економічної шкоди та дестабілізації України незалежно від побічних наслідків для інших країн [91].

Кібершпиунство становить окремий напрямок російської кіберагресії, спрямований на викрадення конфіденційної інформації, державних секретів та персональних даних українських громадян. Хакерські групи APT28 (Fancy Bear) та APT29 (Cozy Bear), які атрибутуються до російських військових розвідувальних служб, систематично проникають у мережі українських урядових установ, оборонних відомств та критичних підприємств. Фішингові кампанії спрямовані на українських чиновників, військовослужбовців та активістів з метою отримання доступу до їхніх акаунтів та комунікацій. Викрадена інформація використовується для розвідувальних цілей, шантажу, компрометації державних діячів або організації цільових кібератак на основі отриманих даних про мережеву інфраструктуру. Масштабні витоки персональних даних українських виборців використовувалися для мікротаргетування дезінформації під час виборчих кампаній. Компрометація телекомунікаційних мереж дозволяла російським спецслужбам відстежувати пересування та комунікації українських військових і політиків [80, с. 134].

DDoS-атаки стали постійним інструментом тиску на українські державні та приватні веб-ресурси, особливо під час критичних подій чи воєнних операцій. Розподілені атаки на відмову в обслуговуванні паралізують роботу урядових порталів, банківських систем, медіа-сайтів та телекомунікаційних сервісів шляхом перевантаження їхніх серверів величезною кількістю запитів. Напередодні повномасштабного вторгнення у лютому 2022 року Україна зазнала масованих DDoS-атак на банківський сектор та державні веб-ресурси, що стало частиною загальної стратегії дестабілізації. Ботмережі, контрольовані російськими операторами, генерують мільйони запитів, роблячи веб-сервіси недоступними для легітимних користувачів. Це створює паніку серед населення, підриває довіру до державних інституцій та ускладнює координацію під час

кризових ситуацій. Одночасність кібератак з військовими операціями демонструє інтегрованість кіберкомпоненту у загальну стратегію гібридної війни [22, с. 4].

Економічні інструменти гібридного впливу Росії на Україну базуються на історичній економічній інтеграції двох країн часів радянського періоду та пострадянських десятиліть взаємозалежності. Енергетична зброя стала головним важелем економічного шантажу, коли Газпром регулярно маніпулював цінами на природний газ, обсягами поставок та транзитними маршрутами залежно від політичної позиції української влади. Російська сторона використовувала «газові війни» 2006 та 2009 років для демонстрації вразливості України та європейських споживачів від російських енергоресурсів. Ціноутворення на газ відбувалося не за ринковими принципами, а як інструмент політичного тиску - проросійські уряди отримували знижки, проєвропейські стикалися з підвищенням тарифів. Загроза припинення газопостачання використовувалася для примушування Києва до політичних поступок, зокрема відмови від євроінтеграції на користь Митного союзу з Росією [11, с. 78].

Торговельні війни та економічні санкції Росії проти українських товарів також почалися задовго до 2014 року та систематично застосовувалися для покарання України за небажані геополітичні кроки. Кремль запроваджував заборони на імпорт української продукції, посиляючись на нібито санітарні, фітосанітарні або технічні проблеми, хоча справжні причини були суто політичними. Особливо постраждали українські виробники кондитерських виробів, молочної продукції, м'яса та машинобудівної продукції, для яких російський ринок традиційно був одним з найбільших. Після Революції Гідності Росія запровадила масштабні торговельні обмеження, що завдали мільярдних збитків українській економіці. Блокування експорту змусило українських виробників терміново шукати альтернативні ринки збуту в Європі, Азії та на Близькому Сході [9, с. 89].

Фінансовий тиск здійснювався через кредитні механізми, коли Росія пропонувала Україні вигідні позики за умови відмови від європейського вибору або вимагала дострокового повернення боргів у разі небажаної політичної

поведінки. Грудень 2013 року ознаменувався російським кредитом у 15 мільярдів доларів для режиму Януковича після відмови підписати Асоціацію з ЄС, що продемонструвало використання фінансових інструментів для геополітичних цілей. Після зміни влади Москва почала вимагати негайного повернення боргів та відмовилася від подальшого фінансування, створюючи додатковий тиск на новий український уряд [93]. Російські банки та фінансові установи в Україні використовувалися для виведення капіталу, дестабілізації банківської системи та фінансування сепаратистських рухів на Донбасі. Економічна блокада окупованих територій з української сторони призвела до їхньої повної залежності від російського фінансування, що перетворило ці регіони на економічний тягар для Кремля, але водночас на інструмент шантажу України.

Інфраструктурна залежність України від Росії використовувалася як довгостроковий важіль економічного впливу через контроль над транспортними коридорами, трубопровідними системами та енергетичними мережами. Російські залізничні та морські маршрути були критично необхідними для українського експорту до країн Азії, а їхнє блокування завдавало шкоди торговельним зв'язкам. Транзит російського газу через українську територію до Європи давав Москві можливість шантажувати як Київ, так і європейських партнерів, загрожуючи перекриттям поставок [70]. Будівництво обхідних газопроводів «Північний потік» та «Турецький потік» було спрямоване на позбавлення України транзитного статусу та доходів від перекачування газу. Енергетична інфраструктура України залишалася технологічно інтегрованою з російською системою, що створювало вразливості для диверсій та маніпуляцій [24, с. 145].

Промислова кооперація радянського періоду створила складні ланцюги постачання між українськими та російськими підприємствами, розрив яких завдав економічних втрат обом сторонам, але використовувався Москвою як інструмент тиску. Українські виробники літаків, ракетних двигунів, турбін та військової техніки залежали від російських комплектуючих, а російські корпорації потребували українських технологій та компонентів. Після 2014 року Росія припинила військово-технічну співпрацю з Україною, змусивши українську

оборонну промисловість шукати альтернативних партнерів та розвивати власне виробництво. Деякі російські підприємства зазнали серйозних проблем через втрату українських постачальників критичних компонентів, зокрема у космічній та авіаційній галузях. Економічна війна виявилася дорогою для обох країн, але для України вона стала каталізатором структурних реформ та диверсифікації економіки.

Інвестиційні механізми використовувалися Росією для встановлення контролю над стратегічними активами української економіки та створення проросійських груп впливу серед бізнес-еліти. Додатковим важелем впливу Росії на Україну був її економічний капітал. У банківському секторі російські установи мали помітну частку - у середині 2010-х сім російських банків володіли приблизно 15% активів української банківської системи: зокрема, Prominvestbank мав близько \$5 млрд активів, Sberbank - приблизно \$4 млрд, а VTB - близько \$3 млрд. У телекомунікаціях російська група МТС, що працювала в Україні через MTS Ukraine (пізніше - Vodafone Ukraine), контролювала близько 35–38% ринку мобільного зв'язку та обслуговувала орієнтовно 22–23 мільйони абонентів у 2014 році, що робило її одним із ключових гравців на ринку та створювало простір для потенційних інформаційних впливів [1]. В енергетиці критичним фактором залишалася залежність від російського газу: у 2014 році «Газпром» поставив Україні близько 14,5 млрд кубометрів газу, а до 2013 року імпортні потреби сягали 30–33 млрд кубометрів. На відміну від банківської сфери, телекомунікацій та енергетики, у роздрібній торгівлі домінування російського капіталу не підтверджується: основними операторами ринку були європейські мережі на кшталт METRO, Auchan та Rewe, а також великі українські ритейлери - АТБ та Fozzy Group. Хоча окремі російські інвестори були присутні у секторі, їхня роль була фрагментарною й не визначала структуру ринку.

Є підозри, що окремі олігархи з проросійською орієнтацією отримували фінансування та підтримку від Кремля в обмін на лобіювання російських інтересів у київських коридорах влади [72]. Після анексії Криму та початку війни на Донбасі українська влада почала процес санації банків з російським капіталом та

обмеження діяльності компаній, пов'язаних з агресором. Націоналізація Приватбанку та виведення з ринку російських банків зменшили фінансові важелі Москви, але економічні зв'язки через офшорні схеми та неформальні канали зберігалися [56, с. 41].

Контрабанда та тіньова економіка на окупованих територіях стали джерелом фінансування російської агресії та корупційних схем, що підривали економічну безпеку України. Незаконне видобування вугілля, металу та інших ресурсів на непідконтрольних територіях Донбасу давало прибутки окупаційним адміністраціям та російським кураторам. Контрабандні маршрути через лінію розмежування дозволяли переміщення товарів, валюти та зброї в обидва напрямки, створюючи можливості для фінансування сепаратистів. Київ запровадив економічну блокаду окупованих територій у 2017 році, припинивши офіційну торгівлю та пенсійні виплати на цих територіях. Ця політика мала суперечливі наслідки - з одного боку обмежила фінансові потоки до бойовиків, з іншого - посилила гуманітарну кризу серед цивільного населення та збільшила їхню залежність від Росії.

Соціально-економічні маніпуляції через субсидіювання окремих регіонів або груп населення використовувалися Росією для створення лояльних анклавів та дестабілізації української державності. На цьому тлі Кремль системно фінансував і підтримував проросійські політичні структури та пов'язані медіа-ресурси, що дозволяло просувати потрібні повідомлення і перешкоджати демократичним реформам. Одним із ключових прикладів була діяльність «Партії регіонів» у 2006–2014 роках, яку численні аналітичні центри - зокрема Freedom House, Transparency International та OSW - характеризували як політичну силу, інтегровану у мережі російського впливу, з непрозорими фінансовими потоками та тісними зв'язками з російським бізнесом, особливо у сфері енергетики [86].

Після 2014 року її місце у просуванні проросійських інтересів зайняла «Опозиційна платформа - За життя», лідери якої, включно з Віктором Медведчуком і Тарасом Козаком, підтримували публічні та неформальні контакти з російським політичним істеблішментом, що підтверджувалося аналітичними

звітами CEPA та Atlantic Council. У лютому 2021 року РНБО та Президент України запровадили санкції проти Козака та медіа-структур 112, NewsOne і ZIK, які перебували під фактичним контролем групи Медведчука й системно транслиували російські наративи [83]. Крім політичних партій і медіа, Росія використовувала мережу культурно-освітніх організацій, таких як «Русский мир» і Россотрудничество, які до 2014 року систематично фінансували діяльність лояльних громадських та освітніх центрів в Україні. Кейс-дослідження європейських та українських дослідницьких інститутів підтверджують, що ці структури були елементами «м'якої сили» Кремля, спрямованої на формування проросійських ідентичностей і поширення меседжів, які зменшували суспільну підтримку інтеграції України до європейських інституцій. Сукупність діяльності політичних партій із проросійською орієнтацією, контрольованих медіа та фінансованих проросійських громадських організацій поєднувалася Росією з економічним важелем впливу, що дозволяло формувати стійкі канали впливу на внутрішньополітичні процеси та створювати соціальні групи й регіони, більш схильні до сприйняття російської політичної та інформаційної повістки.

Пенсіонери окупованих територій отримували виплати з російського бюджету, що формувало економічну залежність та лояльність до окупаційної влади. Гуманітарні «конвої» з Росії на Донбас використовувалися для поставок військового спорядження під виглядом допомоги цивільному населенню. Економічна інтеграція окупованих територій до російського економічного простору здійснювалася через запровадження рубля, підключення до російських банківських систем та інтеграцію підприємств до російських холдингів [74, с. 198]. Кібернетичні атаки на фінансову систему України були спрямовані на підрив довіри до банківського сектору та створення економічної паніки серед населення. Масовані DDoS-атаки на сайти українських банків у 2022 році спричинили тимчасову недоступність онлайн-банкінгу та платіжних систем [23]. Спроби злому банківських серверів та викрадення коштів клієнтів здійснювалися російськими хакерськими групами з метою завдання фінансових збитків та дискредитації банківської безпеки. Фішингові кампанії проти клієнтів

українських банків намагалися отримати доступ до рахунків та викрасти заощадження. Національний банк України та комерційні банки змушені були значно посилити кібербезпеку, запровадивши додаткові протоколи автентифікації та моніторингу підозрілих транзакцій. Міжнародна технічна допомога від західних партнерів дозволила українській фінансовій системі витримати кібернетичний тиск та зберегти стабільність [87].

Енергетична війна 2022 року набула нових форм через систематичні ракетні та дроніві удари по українській енергетичній інфраструктурі з метою залишити населення без електрики, опалення та води в зимовий період. Російські збройні сили цілеспрямовано атакували й атакують теплові електростанції, гідроелектростанції, трансформаторні підстанції та лінії електропередач, намагаючись зламати волю українців до опору. Економічні наслідки цих атак включали не лише прямі збитки від знищення обладнання, а й втрати від зупинки промислового виробництва, комерційної діяльності та погіршення умов життя населення. Україна отримала термінову міжнародну допомогу у вигляді генераторів, трансформаторів та обладнання для відновлення енергосистеми. Диверсифікація енергетичних джерел через розвиток відновлюваної енергетики та інтеграцію до європейської енергосистеми ENTSO-E зменшила вразливість України до російського енергетичного шантажу [62, с. 121].

Продовольча безпека стала об'єктом російської економічної агресії через блокаду українських портів на Чорному морі та перешкоджання експорту зерна до світових ринків. Росія намагалася використати глобальну продовольчу кризу як інструмент шантажу міжнародної спільноти, вимагаючи зняття санкцій в обмін на відкриття зернового коридору. Захоплення та знищення українських сільськогосподарських земель, техніки та інфраструктури завдало мільярдних збитків аграрному сектору країни. Мінування полів та викрадення врожаїв на окупованих територіях додатково погіршили продовольчу ситуацію. Міжнародна ініціатива щодо зернового коридору дозволила частково відновити українських експорт, але Росія систематично порушувала домовленості та зрештою вийшла з угоди. Альтернативні маршрути експорту через Дунай та країни Балтії частково

компенсували втрати, але залишалися менш ефективними за чорноморський коридор.

Економічні санкції західних країн проти Росії стали відповіддю на агресію, але їхня ефективність обмежувалася через лазівки, обхідні схеми та повільність запровадження. Початкові секторальні санкції 2014 року не змогли змінити політику Кремля через їхню обмеженість та можливість адаптації російської економіки. Посилення санкційного тиску після 2022 року включало заморожування активів російських олігархів, відключення банків від системи SWIFT, ембарго на російську нафту та газ. Росія відповіла контрсанкціями та орієнтацією на азійські ринки, зокрема Китай та Індію, що частково компенсувало втрати від західних обмежень. Економічна війна між Росією та Заходом завдала збитків обом сторонам, але не призвела до припинення агресії проти України [6, с. 740].

2.3. Вплив гібридних загроз на політичну систему України в умовах російсько-української війни

Гібридні загрози сьогодні є одним із найскладніших викликів для регіональної та глобальної безпеки. Вони поєднують військові, економічні, політичні, інформаційні та кібернетичні інструменти впливу, що дозволяє державам або недержавним акторам досягати стратегічних цілей без формального оголошення війни. Такі загрози здатні підірвати інституційні механізми державної влади, створювати внутрішню політичну нестабільність, послаблювати економічні системи та маніпулювати громадською думкою. На регіональному рівні це проявляється через підтримку сепаратистських рухів, кібератаки на критичну інфраструктуру, політичну дестабілізацію та поширення дезінформації серед населення. На глобальному рівні гібридні дії можуть впливати на міжнародні альянси, економічні ринки та роботу організацій, таких як ООН, НАТО або ЄС, змінюючи баланс сил без відкритого військового конфлікту. Прикладами є кібератаки на енергетичні та фінансові системи у США та країнах Європи, масштабні дезінформаційні кампанії у соціальних мережах, а також

використання фінансових і політичних важелів для просування вигідних агресору політичних сил [26].

На національному рівні ефективність гібридних загроз залежить від стійкості політичних та соціальних інститутів. Вразливість держав до таких дій зростає при слабких інститутах, низькому рівні медіаграмотності населення та недостатньому контролі над критичною інфраструктурою. Економічний тиск, включаючи санкції, маніпуляції енергетичними ресурсами та втручання у фінансові ринки, часто поєднується з інформаційними кампаніями для посилення соціальної напруженості та зниження довіри до влади. Класичним прикладом глобального впливу є діяльність хакерських груп, пов'язаних із державами, які здійснюють атаки на урядові та корпоративні системи для збору даних, саботажу або залякування населення [48, с. 15]. Подібні дії показують, що гібридні загрози не обмежуються традиційними фронтами і можуть мати довгостроковий вплив на політичну та економічну стабільність держав. Україна є прикладом того, як держави можуть зіткнутися з комплексною гібридною агресією і водночас виробити стратегії протидії. Тут гібридні методи проявилися через інформаційні кампанії, дезінформацію, кібератаки на державні системи та спроби політичного впливу на вибори. У відповідь країна посилила механізми кібербезпеки, створила структури стратегічних комунікацій, зміцнила контррозвідку та розвинула волонтерські та громадські ініціативи для протидії пропаганді та підтримки критично важливих функцій держави [47].

Політична система України зазнала безпрецедентного тиску від російської гібридної агресії, що виявило як структурні вразливості, так і потенціал стійкості демократичних інституцій. Кремль систематично втручався у виборчі процеси в Україні через фінансування проросійських кандидатів, дезінформаційні кампанії та кібератаки на виборчу інфраструктуру. Президентські вибори 2014 та 2019 років супроводжувалися спробами підриву довіри до виборчого процесу через поширення фейків про фальсифікації, дискредитацію окремих кандидатів та маніпуляції громадською думкою. Парламентські вибори ставали об'єктом інформаційних операцій, спрямованих на просування сил, що виступають за

федералізацію України, відмову від євроатлантичної інтеграції та відновлення тісних зв'язків з Росією. Центральна виборча комісія та правоохоронні органи розробили механізми протидії виборчим маніпуляціям, включаючи моніторинг іноземного втручання, спростування дезінформації та захист електронних систем підрахунку голосів [75, с. 168].

Державні інституції виявилися недостатньо підготовленими до гібридної агресії на початковому етапі конфлікту через корупцію, слабкість спецслужб та відсутність координації між різними відомствами. Силові структури, включаючи Службу безпеки України та Міністерство внутрішніх справ, були інфільтровані російською агентурою, що полегшило окупацію Криму та розгортання сепаратистських рухів на Донбасі [10]. Реформування сектору безпеки стало пріоритетом після 2014 року з метою очищення від зрадників, посилення контррозвідки та розвитку спроможностей протидії гібридним загрозам. Створення нових структур, таких як Департамент кіберполіції та Центр стратегічних комунікацій, відображало усвідомлення необхідності адаптації державних інституцій до нових викликів. Судова система залишалася слабкою ланкою через корупцію та неефективність, що ускладнювало притягнення до відповідальності осіб, причетних до підриву національної безпеки [60, с. 133].

Регіональна політика України стала об'єктом активних російських маніпуляцій через експлуатацію регіональних відмінностей, мовних питань та історичної пам'яті для розколу країни. Кремль просував ідеї федералізації, автономізації окремих областей та надання особливого статусу російській мові, використовуючи це як інструмент послаблення центральної влади. Значну роль у цьому процесі відігравала Партія регіонів, яка особливо активно діяла на Сході та Півдні України, фінансувалася з Росії і просувала проросійську повістку, зокрема питання федералізації та протистояння Києву [81]. Паралельно Комуністична партія України зберігала тісні зв'язки з російськими структурами та виступала проти євроінтеграції, використовуючи історичні наративи та радянську символіку для формування проросійських настроїв у регіонах. Після 2014 року, у контексті окупації частини територій та відкритої збройної агресії, більшість цих

політичних сил втратили підтримку серед населення через дискредитацію їхніх проросійських позицій, а децентралізаційна реформа посилила єдність держави, надавши реальні повноваження місцевому самоврядуванню без створення сепаратистських анклавів [27].

Після початку війни більшість цих партій втратили підтримку через дискредитацію проросійської позиції серед населення. Децентралізаційна реформа, започаткована у 2014 році, парадоксально зміцнила єдність країни через надання реальних повноважень місцевому самоврядуванню без створення сепаратистських анклавів. Окуповані території перетворилися на антиприклад для решти України, демонструючи економічну деградацію та порушення прав людини під російським контролем [57, с. 163].

Партійна система України пройшла трансформацію під впливом гібридної війни, коли відкрито проросійські сили втратили електоральну підтримку, а провідні партії консолідувалися навколо порядку денного національної оборони та європейської інтеграції. Заборона Комуністичної партії України та інших проросійських політичних сил відбулася на основі їхньої підтримки агресії та сепаратизму. Опозиційні платформи, що мали зв'язки з Росією, змушені були переформатувати риторику та дистанціюватися від Кремля для збереження політичної суб'єктності. Парламентські дебати зосередилися на питаннях національної безпеки, обороноздатності та протидії російському впливу, витісняючи на другий план традиційні соціально-економічні теми. Консолідація політичного класу навколо національних інтересів не виключила внутрішньої конкуренції та критики уряду, але встановила червоні лінії щодо сепаратизму та капітуляції перед агресором [14, с. 30].

Громадянське суспільство виявилось найстійкішим елементом української політичної системи, демонструючи здатність до самоорганізації, волонтерської діяльності та протидії російським наративам. Майдан 2013-2014 років засвідчив силу низової мобілізації у захисті демократичних цінностей та європейського вибору України. Волонтерський рух став критичним фактором підтримки української армії на початковому етапі війни, коли держава не могла забезпечити

військових необхідним спорядженням та матеріалами. Правозахисні організації, незалежні медіа та аналітичні центри розробили ефективні методи моніторингу російської пропаганди, документування воєнних злочинів та адвокації українських інтересів на міжнародній арені. Кіберактивісти та IT-волонтери створили інструменти для спростування дезінформації, захисту від кібератак та підтримки цифрової інфраструктури держави [90, с. 87].

Національна ідентичність українців зміцнилася під впливом російської агресії, спростувавши кремлівські розрахунки на внутрішній розкол та відсутність єдиної української нації. Війна стала каталізатором формування громадянської ідентичності, що об'єднала різні етнічні, мовні та регіональні групи навколо спільних цінностей свободи, суверенітету та демократії. Російськомовні українці масово підтримали опір агресору, демонструючи, що мова не визначає політичну лояльність та національну приналежність. Кримські татари стали однією з найактивніших груп у протидії окупації півострова, зберігаючи українську ідентичність території попри репресії. Історична пам'ять про Голодомор, радянські репресії та боротьбу за незалежність актуалізувалася у контексті протистояння російському імперіалізму. Мовне питання втратило політичну гостроту, коли російськомовні та україномовні громадяни об'єдналися у захисті держави [31, с. 163].

Інституційна стійкість української держави проявилася у збереженні конституційного порядку, демократичних процедур та цивільного контролю над силовими структурами попри воєнний стан. Передача влади між президентами Порошенком та Зеленським у 2019 році відбулася демократичним шляхом всупереч російським прогнозам про неминучий авторитаризм чи хаос. Парламент продовжував функціонувати навіть під час найгарячіших фаз конфлікту, приймаючи необхідне законодавство для зміцнення обороноздатності та реформування держави. Судова влада, попри слабкості, зберегла незалежність від виконавчої гілки та продовжила розгляд справ, включаючи політично чутливі. Місцеве самоврядування на підконтрольних Україні територіях функціонувало навіть у прифронтових містах, забезпечуючи комунальні послуги та соціальну

підтримку населення. Бюрократичний апарат адаптувався до воєнних умов, зберігаючи базову функціональність держави [7, с. 41].

Економічна стійкість України виявилася недостатньою для повної автономії від зовнішньої фінансової підтримки, але достатньою для уникнення колапсу під тиском російської агресії. Міжнародні фінансові організації, передусім МВФ та Світовий банк, надали критичну підтримку для стабілізації економіки та фінансування оборонних потреб. Національний банк України запровадив жорстку монетарну політику для підтримки стабільності гривні та контролю інфляції попри воєнні витрати. Бізнес-сектор продемонстрував гнучкість через релокацію виробництв з прифронтових регіонів, диверсифікацію ринків збуту та адаптацію до воєнних умов. Податкова система зберегла функціональність, забезпечуючи державні доходи для фінансування армії та соціальних програм. Зовнішній борг зріс через необхідність фінансування військових витрат, створюючи виклики для довгострокової фінансової стійкості [79, с. 4].

Соціальна стійкість українського суспільства базувалася на патріотичній мобілізації, солідарності та готовності до жертв заради збереження незалежності держави. Масова мобілізація до лав збройних сил та добровольчих батальйонів засвідчила готовність громадян захищати країну зі зброєю в руках. Внутрішньо переміщені особи, кількість яких перевищила півтора мільйона після 2014 року та кілька мільйонів після 2022 року, інтегрувалися у приймаючі громади попри соціально-економічні труднощі. Родини військовослужбовців та цивільне населення демонстрували витримку перед обличчям постійної загрози, втрат близьких та погіршення умов життя. Психологічна стійкість підтримувалася через патріотичні наративи, віру у перемогу та міжнародну солідарність. Соціальні програми підтримки ветеранів, поранених та родин загиблих військових стали пріоритетом державної політики.

Культурна стійкість проявилася у розквіті української мови, культури та мистецтва як форми опору російській агресії та утвердження національної ідентичності. Український кінематограф, література, музика та візуальне мистецтво пережили ренесанс, відображаючи тему війни, опору та національного

відродження. Перехід українськомовних авторів, артистів та медіа на українську мову став масовим трендом, спростовуючи російські наративи про штучність та нежиттєвість української культури. Декомунізація та демонтаж символів радянської та російської імперської спадщини символізували розрив з колоніальним минулим та утвердження нової національної ідентичності. Культурна дипломатія України на міжнародній арені посилювалася через промоцію української культури, історії та сучасних досягнень. Захист культурної спадщини від російських обстрілів та розграбувань став частиною загальнонаціонального опору.

Інформаційна стійкість українського суспільства зросла через розвиток медіаграмотності, критичного мислення та спроможності розпізнавати російську пропаганду. Незалежні українські медіа відіграли ключову роль у спростуванні дезінформації, висвітленні правди про війну та мобілізації суспільства. Фактчекінгові організації створили ефективні механізми перевірки інформації та публічного викриття фейків. Обмеження діяльності російських медіа в Україні та блокування проросійських інтернет-ресурсів зменшили канали поширення ворожої пропаганди. Соціальні мережі стали полем битви за наративи, де українські користувачі активно протистояли російським ботам та троям. Державна система стратегічних комунікацій координувала інформаційну політику різних відомств та забезпечувала послідовність меседжів [67, с. 141].

Міжнародна підтримка стала критичним фактором стійкості України, компенсуючи обмеженість власних ресурсів через фінансову, військову, гуманітарну та дипломатичну допомогу. Західні партнери надали Україні десятки мільярдів доларів у вигляді кредитів, грантів та гуманітарної допомоги для підтримки економіки та держави [85]. Постачання зброї, включаючи сучасні системи протиповітряної оборони, артилерію та бронетехніку, посилювало обороноздатність України. Дипломатична підтримка у міжнародних організаціях, передусім ООН та ОБСЄ, забезпечила ізоляцію Росії та визнання її агресором. Прийняття мільйонів українських біженців європейськими країнами продемонструвало солідарність зі страждаючим населенням. Євroatлантична

перспектива України, включаючи надання статусу кандидата до ЄС, посилила стратегічну мотивацію суспільства до продовження боротьби.

Адаптивність української політичної системи проявилася у здатності швидко реагувати на нові виклики, проводити необхідні реформи та інтегрувати уроки гібридної війни у державну політику. Законодавство у сфері національної безпеки було суттєво оновлено для врахування гібридних загроз, кіберзагроз та необхідності стратегічних комунікацій. Наприклад, було прийнято нове законодавство, яке встановило систему стратегічних комунікацій та посилення координації між силовими структурами та органами влади. Реформа Збройних Сил України перетворила армію з радянської моделі на сучасну оборонну силу, здатну протистояти агресору, а розвиток системи територіальної оборони дозволив залучити цивільне населення до захисту держави [37]. Створення Департаменту кіберполіції та Центру протидії дезінформації дозволило ефективно реагувати на кібератаки та російську пропаганду, а реформа Служби безпеки України посилила здатність держави протидіяти агентурній діяльності та зовнішньому впливу. Реформа збройних сил перетворила українську армію з радянської моделі на сучасну силу, здатну протистояти російській агресії. Система цивільної оборони та територіальної оборони розвинулася для залучення широких верств населення до національної оборони. Антикорупційна реформа, хоча й повільна, зменшила вразливості держави до російського впливу через корупційні схеми.

Політична система України поступово виробила концепцію національної стійкості як здатності держави та суспільства підтримувати функціонування під час тривалого зовнішнього тиску. Під національною стійкістю розуміють спроможність інститутів влади, економіки та громадянського суспільства діяти узгоджено для запобігання руйнівним наслідкам гібридних атак, швидко відновлювати функції після криз і забезпечувати довіру громадян до держави. Цей підхід охоплює як політичну, так і інформаційну, економічну та психологічну складові. Україна в процесі війни перейшла від пасивного реагування до активної моделі управління ризиками, коли рішення ухвалюються на основі оцінки загроз,

а не постфактум. Сформована система кризового управління при Раді національної безпеки і оборони координує діяльність державних органів, інтегруючи військову, дипломатичну й комунікаційну політику. Це забезпечує швидкість рішень та підвищує передбачуваність дій влади [78, с. 112].

Інтеграція концепції демократичної стійкості в політичне життя стала логічним продовженням національної стійкості. Демократична стійкість трактується як здатність політичної системи зберігати демократичні механізми навіть за умов воєнної загрози. Вона проявляється через підтримку плюралізму, свободи слова та політичної конкуренції без порушення безпекових інтересів держави. Українські медіа, партії та громадські організації пристосувалися до воєнного контексту, не втрачаючи критичного голосу. Це забезпечило баланс між демократичною відкритістю та національною безпекою, що стало ключовою перевагою перед авторитарними моделями управління, схильними до репресій під час війни. Розвиток демократичної стійкості також зміцнив легітимність державних рішень, оскільки суспільство визнає їх результатом колективної участі, а не нав'язаних зверху директив.

Впровадження принципів інституційної адаптивності дозволило уникнути колапсу політичного управління навіть під час найгостріших фаз бойових дій. Інституційна адаптивність означає здатність державних структур змінювати свої процедури, структуру та методи управління відповідно до нових викликів без втрати керованості. Наприклад, Верховна Рада перейшла на дистанційний режим ухвалення рішень, уряд запровадив цифрові платформи для безперервного адміністрування послуг, а військово-цивільні адміністрації забезпечили виконання функцій місцевої влади на прифронтових територіях. Цей процес довів, що українська політична система може діяти ефективно не лише в умовах стабільності, а й під постійним тиском агресора.

Формування національної єдності стало ключовим чинником підтримання політичної стійкості держави. Єдність розглядається не як відсутність політичних відмінностей, а як готовність громадян і політичних еліт узгоджувати дії задля спільної мети - збереження суверенітету. Після 2014 року суспільство пододало

пострадянську фрагментацію, що базувалася на регіональних, мовних і культурних протиріччях. Символи та наративи української державності - від тризуба до пісень спротиву - набули консолідуючого змісту, сприяючи самоідентифікації громадян як частини політичної нації. Цей процес зменшив ефективність російських спроб провокувати внутрішні конфлікти через «захист російськомовних» або апеляції до «спільної історії».

Поступово відбулося й осмислення поняття стратегічної автономії - спроможності держави ухвалювати ключові політичні рішення незалежно від зовнішнього тиску, водночас зберігаючи союзницькі зобов'язання. Україна прагне поєднати глибоку інтеграцію з Європейським Союзом та НАТО із внутрішнім розвитком оборонного, енергетичного й технологічного потенціалу. Зміцнення стратегічної автономії в умовах гібридної війни означає зниження вразливості до енергетичного шантажу, інформаційних маніпуляцій та політичного впливу іноземних гравців. Цей курс спрямований на формування самодостатньої моделі державності, що здатна утримувати рівновагу між зовнішньою підтримкою і власною спроможністю до відновлення [25, с. 207].

2.4. Міжнародні заходи протидії гібридним загрозам

Міжнародна система безпеки за останнє десятиліття поступово перейшла від реактивного підходу до системного осмислення природи гібридних загроз. Гібридна форма агресії не має чітких кордонів між війною і миром, між державним і недержавним насильством. Держави, що опинилися під впливом таких дій, потребують не лише оборонних засобів, а й комплексної системи стратегічного управління ризиками. Термін «comprehensive defense» у документах НАТО та ЄС означає підхід, за якого безпека досягається шляхом координації дипломатичних, економічних, інформаційних і військових зусиль [24]. Таким чином, боротьба з гібридними загрозами розглядається не як суто військове завдання, а як функція державної і міждержавної взаємодії. Цей перехід до комплексності визначив нову логіку безпеки - від ізольованих відомчих дій до інтегрованої стратегічної відповіді.

Гібридна агресія Росії проти України стала каталізатором для формування спеціальних підрозділів, здатних діяти в умовах інформаційних і кібернетичних атак. З 2018 року у Брюсселі функціонує NATO Hybrid Analysis Branch, який здійснює моніторинг гібридної активності противників і надає аналітичну підтримку країнам-членам. З'явилося поняття Hybrid Deterrence - стримування гібридних дій через поєднання військової готовності, кіберзахисту та дипломатичних заходів. НАТО розглядає гібридну війну як зону, де противник прагне уникнути порогу колективної оборони, тому головне завдання полягає у зменшенні «сірих зон» невизначеності. Україна, співпрацюючи з Альянсом, бере участь у навчаннях і програмах оцінки вразливостей, формуючи спільні механізми протидії [28, с. 59].

Європейський Союз розробив власну рамкову політику реагування на гібридні загрози, що спирається на інтеграцію дипломатичних і цивільних інструментів. У 2016 році ЄС створив Hybrid Fusion Cell- аналітичний центр при Європейській службі зовнішніх дій, який акумулює інформацію з держав-членів щодо ознак гібридної активності. Європейська стратегія базується на концепції «resilience» - здатності суспільств витримувати тиск через дезінформацію, кібератаки, енергетичні маніпуляції чи політичне втручання. Важливою ініціативою стало створення European Centre of Excellence for Countering Hybrid Threats у Гельсінкі, де об'єднано експертів з НАТО та ЄС [30]. Центр досліджує практики інформаційної безпеки, критичної інфраструктури та стратегічних комунікацій. Європейський підхід акцентує увагу на превенції: замість реагування після атаки, держави розробляють плани протидії завчасно. Такий механізм дозволяє зменшити політичні втрати та посилити координацію на рівні Єврокомісії й національних урядів.

Міжнародне право також адаптується до нових умов, у яких гібридна агресія не завжди має класичні ознаки збройного конфлікту. Поняття «невійськової агресії» починає набувати юридичного змісту через практику міжнародних судів і рішень ООН. У документах Міжнародного кримінального суду розглядається можливість кваліфікації кібератак як актів агресії, якщо вони призводять до

суттєвої шкоди цивільним чи інфраструктурі [44]. Розробляються норми, які дозволять притягати до відповідальності не лише держави, а й приватні групи, що діють під державним контролем. Така інтерпретація змінює уявлення про суб'єктність у міжнародному праві, адже визнання «групової відповідальності» створює прецедент для розгляду діяльності російських хакерських формувань. Українська дипломатія бере активну участь у просуванні цих ідей, намагаючись юридично закріпити поняття гібридної агресії як порушення Статуту ООН. Велика Британія стала однією з перших держав, що розробила національну стратегію протидії гібридним впливам у глобальному вимірі. Її концепція базується на доктрині «Integrated Security», яка передбачає синхронізацію дій уряду, армії, розвідки, бізнесу й громадянського суспільства. Одночасно розвивається система стратегічних комунікацій, що координує роботу медіа, дипломатії та розвідувальних служб. Британська модель передбачає також розвиток «контрнарративів» - інформаційних кампаній, спрямованих на спростування дезінформації. Велика Британія розглядає гібридні загрози не лише у військовій площині, а як фактор, що впливає на політичну стабільність, економіку й довіру до держави. Ця стратегія стала орієнтиром для багатьох партнерів, включаючи Україну, яка переймає досвід у сфері кіберзахисту.

Сполучені Штати Америки в рамках National Defense Strategy виокремили гібридні загрози як головний інструмент стратегічних конкурентів - Росії, Китаю та Ірану. Пентагон визначає гібридну війну як багаторівневу операцію, що поєднує інформаційні атаки, економічний тиск, військові провокації та маніпуляції у кіберпросторі. США інвестують у створення структур, здатних діяти в «сірих зонах» - просторах між війною і миром. Державний департамент координує програму Global Engagement Center, яка займається виявленням і нейтралізацією дезінформаційних кампаній. Одночасно Сполучені Штати формують систему партнерств із країнами Центральної та Східної Європи для зміцнення колективної кібероборони. Цей підхід демонструє прагнення до формування глобальної мережі стійкості, де кожна держава може обмінюватися аналітикою, технологіями й кадровим потенціалом.

Канада та країни Північної Європи зосереджуються на формуванні whole-of-society approach - підходу, коли боротьба з гібридними загрозами є спільним завданням держави й суспільства [82]. Такий підхід передбачає залучення освітніх інституцій, медіа, бізнесу та громадських організацій до підвищення стійкості. Фінляндія, наприклад, має розгалужену систему підготовки населення до кризових ситуацій, де вивчаються методи протидії дезінформації та психологічному тиску. Норвегія розвинула структури цивільного резерву, здатного підтримувати критичні системи у разі кібернападу чи енергетичної кризи. Канада активно впроваджує програму «Digital Citizen Initiative», що спрямована на формування медіаграмотності та захист демократичних процесів від маніпуляцій. Ці моделі вважаються ефективними для України, адже поєднують централізоване управління з широкою громадською участю.

Важливим чинником міжнародної співпраці є обмін розвідданими між союзниками. Такі механізми, як Five Eyes Alliance (США, Велика Британія, Канада, Австралія, Нова Зеландія), забезпечують аналітичний моніторинг гібридних операцій противників. Інформація про кібератаки, кампанії дезінформації чи економічний тиск передається у реальному часі, що скорочує реакційний період до мінімуму. Розвідувальні альянси формують єдині бази даних щодо хакерських угруповань, медійних маніпуляцій та фінансових потоків, пов'язаних із підривною діяльністю. Така система ускладнює використання «проксі-акторів» - груп, що формально не належать державам, але працюють за їхніми вказівками. Для України приєднання до подібних ініціатив є стратегічним пріоритетом, оскільки це підвищує оперативність реагування на нові форми агресії. Окремим напрямом міжнародної взаємодії стало створення спільних навчань, спрямованих на тестування стійкості інституцій до гібридних загроз. Програма Cyber Coalition, яку проводить НАТО, залучає Україну як партнера для перевірки готовності до кібератак на критичну інфраструктуру. ЄС розвиває проєкт EU Playbook for Countering Hybrid Threats, що імітує кризові сценарії та відпрацьовує механізми реагування між державами-членами [24]. Навчання дозволяють оцінити, наскільки ефективно працює комунікація між силовими,

дипломатичними та інформаційними структурами. Вони створюють спільну культуру безпеки, де кожен учасник розуміє роль іншого у спільній системі захисту.

Міжнародні фінансові інституції долучаються до протидії гібридним загрозам через підтримку економічної стійкості країн-партнерів. МВФ і Світовий банк розглядають економічну стабільність як один із ключових елементів безпеки, здатний запобігти політичній дестабілізації [49]. Програми макрофінансової допомоги для України після 2014 року сприяли зменшенню вразливості економіки до зовнішніх маніпуляцій. Енергетична незалежність, розвиток власного видобутку та інтеграція до європейських енергетичних ринків також стали частиною ширшої стратегії протидії гібридним впливам. Фінансова стабільність дозволяє державі зберігати політичну суб'єктність і уникати сценарію економічного шантажу. У такий спосіб економічні інституції перетворюються на інструмент глобальної безпеки [29, с. 182].

Організація Об'єднаних Націй розвиває політичний вимір протидії гібридним загрозам через створення платформ для обговорення інформаційної безпеки та цифрових прав. Генеральна Асамблея ухвалила низку резолюцій щодо протидії маніпуляціям у медіа та втручання у виборчі процеси. Серед них варто виокремити A/RES/78/213 «Promotion and protection of human rights in the context of digital technologies» (Підтримка та захист прав людини в контексті цифрових технологій), ухвалену 22 грудня 2023 року, яка закликає держави враховувати вплив цифрових технологій на права людини, проводити оцінку ризиків та забезпечувати свободу слова, приватність і інформаційні права [65]. Крім того, важливою є A/RES/75/176, що стосується права на приватність в цифрову епоху та захисту персональних даних, приватності й цифрових прав в умовах стрімкого розвитку інформаційно-комунікаційних технологій. Ці резолюції закладають міжнародні стандарти, які держави-члени мають враховувати для захисту прав людини та протидії інформаційній агресії в цифровому просторі. Рада Безпеки ООН почала розглядати кібератаки як потенційну загрозу міжнародному миру. Україна активно використовує цю трибуну для документування випадків

гібридної агресії Росії, формуючи доказову базу для подальших юридичних кроків. Проте механізми санкційного впливу залишаються обмеженими через право вето постійних членів. Це стимулює створення позаінституційних коаліцій держав, що спільно реагують на порушення міжнародного порядку [20].

Регіональні організації, такі як ОБСЄ, розширюють власні інструменти моніторингу, включаючи аналіз дезінформаційних кампаній і гібридного тиску [12]. Спостережні місії документують випадки інформаційних маніпуляцій, атак на цивільну інфраструктуру та втручання у вибори. ОБСЄ співпрацює з неурядовими аналітичними центрами для розробки методик ідентифікації джерел пропаганди. Завдяки такій взаємодії формується система раннього попередження, що дозволяє державам виявляти загрози ще до їх ескалації. Цей підхід вимагає підвищення прозорості інформаційного простору та міждержавної взаємодовіри. Україна використовує платформи ОБСЄ для поширення достовірних даних про воєнні злочини й підривні операції проти держави. Міжнародна координація в сфері кібербезпеки перетворилася на самостійний напрям безпекової політики. Створення Budapest Convention on Cybercrime заклало основу для кримінального переслідування кіберзлочинів у транснаціональному вимірі [5]. Україна є активним учасником цього процесу, співпрацюючи з європейськими структурами з метою розслідування атак на державні ресурси. Мережа Computer Emergency Response Teams об'єднує фахівців різних країн для координації реагування на інциденти. Гібридні атаки дедалі частіше розглядаються як поєднання технічних і психологічних операцій, тому міжнародна співпраця включає не лише кіберзахист, а й інформаційно-психологічну безпеку. Це формує нову культуру цифрової відповідальності між державами.

Велике значення має участь громадянського суспільства у формуванні міжнародних стратегій протидії гібридним загрозам. Аналітичні центри, такі як Atlantic Council, Chatham House чи Carnegie Endowment, проводять незалежні дослідження й надають рекомендації урядам [89]. Вони виступають посередниками між науковою спільнотою, державами й міжнародними організаціями, забезпечуючи циркуляцію знань і методологій. Громадські

організації беруть участь у проєктах моніторингу дезінформації, розробляють навчальні програми з кібергігієни та критичного мислення. Взаємодія держави й громадського сектору зміцнює довіру до міжнародних ініціатив, адже забезпечує прозорість і публічний контроль. Для України така участь означає можливість посилити власну позицію у світових безпекових дискусіях. Мережа міжнародних санкцій стала одним із найефективніших інструментів колективної відповіді на гібридні загрози. Після початку агресії Росії проти України санкційні режими ЄС, США, Великої Британії, Канади та Японії охопили тисячі фізичних і юридичних осіб. Санкції торкнулися банківського сектору, енергетики, оборонної промисловості та технологій подвійного призначення. Вони мають не лише економічний, а й політичний ефект, ізолюючи агресора від глобальних фінансових ринків і технологічних ланцюгів. У координації санкцій простежується нова модель колективного реагування, де економічний тиск стає елементом стратегічного стримування. Для України така система створює зовнішню підтримку внутрішньої боротьби проти гібридних атак.

РОЗДІЛ 3

УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ ПРОТИДІЇ ГІБРИДНИМ ВІЙНАМ

3.1. Механізми підвищення національної стійкості України до гібридних загроз

Національна стійкість є здатність держави, суспільства та їхніх інституцій протистояти зовнішнім та внутрішнім викликам, зберігаючи функціональність критичної інфраструктури та соціальну згуртованість. Концепція стійкості передбачає не лише пасивний захист від загроз, але й активну адаптацію до змінних умов безпекового середовища. Формування національної стійкості вимагає системного підходу, що охоплює військову, економічну, соціальну, інформаційну та психологічну сфери. Стратегічне планування у цій галузі має базуватися на комплексному аналізі вразливостей та можливостей держави. Ефективна стійкість створюється через синергію державних інституцій, приватного сектору та громадянського суспільства. Досвід протистояння російській агресії демонструє критичну потребу у розробці довгострокових механізмів підтримання стійкості [73, с. 78]. Водночас формування національної стійкості в Україні супроводжується низкою системних проблем. Насамперед ідеться про фрагментарність державної політики у цій сфері, коли окремі елементи стійкості розвиваються нерівномірно та без належної міжвідомчої координації. Обмежені фінансові ресурси, перевантаженість інституцій в умовах повномасштабної війни та залежність від зовнішньої допомоги знижують спроможність реалізовувати довгострокові програми стійкості. Надмірна централізація прийняття рішень не завжди дозволяє ефективно враховувати регіональні особливості та локальні вразливості.

Комплексна стратегія протидії гібридним загрозам має включати превентивні, захисні та відновлювальні компоненти. Превентивні заходи спрямовані на раннє виявлення потенційних загроз та зменшення вразливостей національної системи безпеки. Захисні механізми забезпечують оперативне

реагування на актуальні виклики та мінімізацію їхніх наслідків. Відновлювальна складова передбачає швидке відновлення функціонування критичних систем після деструктивних впливів. Інтеграція цих компонентів у єдину стратегію дозволяє створити багаторівневу систему національної безпеки. Координація між різними секторами безпеки забезпечує синхронізацію зусиль та ефективне використання ресурсів. Регулярний перегляд та актуалізація стратегії відповідає динамічному характеру гібридних загроз. У контексті українського законодавства окремого документу під назвою «Комплексна стратегія протидії гібридним загрозам» наразі немає. Проте її принципи реалізовані у Законі України «Про національну безпеку України» (2018 р.), який визначає основи превентивних, захисних та відновлювальних заходів, включно з кіберзахистом, стратегічними комунікаціями та координацією між силовими структурами [33]. Також ці підходи інтегровані у Національну стратегію національної безпеки України, яка регулярно оновлюється та визначає пріоритети протидії гібридним загрозам, а спеціалізовані документи та концепції, розроблені Радою національної безпеки і оборони та СБУ, деталізують практичні механізми реагування та відновлення критичних систем [84]. Концепція комплексної стратегії відповідає офіційним державним документам, хоча не виділена окремим законом. Разом з тим відсутність єдиного нормативно закріпленого документа, який би комплексно регулював протидію гібридним загрозам, ускладнює практичну реалізацію відповідних заходів. Розпорошеність стратегічних положень між різними законами та підзаконними актами створює ризик дублювання функцій і відповідальності між органами державної влади. Недостатня узгодженість між стратегічним плануванням і реальними механізмами виконання знижує ефективність реагування на динамічні гібридні загрози.

Енергетична безпека становить фундаментальну основу національної стійкості України в умовах гібридної війни. Диверсифікація джерел енергопостачання зменшує залежність від потенційно ворожих постачальників та підвищує автономність держави. В Україні реалізовано низку заходів у цьому напрямі: зокрема, імпорту газу з європейських країн через реверсні поставки,

нарощування власного видобутку газу та вугілля, а також підключення до європейської енергосистеми ENTSO-E для підвищення інтеграції та безпеки [38]. Розвиток власних енергетичних потужностей, зокрема відновлювальної енергетики, створює стратегічний резерв у випадку кризових ситуацій; за останні роки в Україні значно зросли потужності сонячних та вітрових електростанцій. Модернізація енергетичної інфраструктури, впровадження розумних енергомереж та систем автоматичного моніторингу дозволяє підвищити стійкість системи до цілеспрямованих кібератак і фізичних руйнувань під час бойових дій. Створення стратегічних запасів енергоносіїв забезпечує можливість функціонування критичної інфраструктури навіть за умов повного припинення зовнішніх поставок. Інтеграція енергетичної системи України до європейських мереж відкриває нові можливості для забезпечення безперервності енергопостачання [43, с. 156]. Попри досягнення у сфері енергетичної безпеки, енергетична система України залишається вразливою до масованих ракетних ударів, диверсій та кібератак. Значна частина енергетичної інфраструктури є фізично застарілою, а її відновлення потребує значних фінансових і часових ресурсів. Розвиток відновлювальної енергетики також стикається з проблемами нестабільності генерації, браком систем накопичення енергії та залежністю від імпортованих технологій.

Кібербезпека набуває центрального значення у контексті протидії гібридним загрозам через зростаючу цифровізацію державних послуг та критичної інфраструктури. Національна система кіберзахисту охоплює державний, приватний та громадський сектори, створюючи єдиний захисний периметр. В Україні запроваджено Державну програму кібербезпеки, створено Департамент кіберполіції та Центр стратегічних комунікацій, які відповідають за моніторинг, протидію кібератакам та відновлення інформаційних систем. Розроблені національні стандарти кібербезпеки, впроваджено обов'язкову сертифікацію критичних систем та регулярні навчання персоналу державних органів [45]. Створення національного центру реагування на кіберінциденти забезпечує оперативну координацію дій під час масштабних атак. Інвестиції у

підготовку кваліфікованих фахівців з кібербезпеки формують кадровий потенціал для довгострокового протистояння цифровим загрозам. Міжнародна співпраця у сфері обміну інформацією про кіберзагрози підвищує ефективність національних систем захисту. Водночас національна система кібербезпеки стикається з дефіцитом висококваліфікованих кадрів та нерівномірним рівнем захищеності між державним і приватним секторами. Частина об'єктів критичної інфраструктури досі використовує застаріле програмне забезпечення, що підвищує ризики успішних кібератак. Недостатній рівень кібергігієни серед населення та державних службовців також залишається фактором уразливості.

Економічна стійкість визначає спроможність держави підтримувати функціонування базових систем життєзабезпечення навіть за умов зовнішнього тиску та санкцій. В Україні проведено заходи з диверсифікації економіки та зменшення залежності від окремих галузей чи ринків, зокрема шляхом розширення експорту до Європи та інших партнерських країн, підтримки малих і середніх підприємств, розвитку внутрішнього виробництва критичних товарів та послуг, що знижує вразливість до переривання зовнішніх ланцюгів постачання [62]. Створено стратегічні резерви продовольства, медикаментів та пального, що дозволяє забезпечити автономність держави на випадок кризових ситуацій. Залучення іноземних інвестицій з демократичних країн зміцнює економічні зв'язки з союзниками та партнерами. Підтримка малого та середнього бізнесу підвищує адаптивність економічної системи до швидкозмінних умов [41, с. 203]. Економічна стійкість України суттєво обмежується тривалими бойовими діями, руйнуванням виробничих потужностей та логістичних ланцюгів, а також скороченням внутрішнього споживчого ринку. Високий рівень бюджетного дефіциту та залежність від міжнародної фінансової допомоги знижують автономність економічної політики. Додатковим викликом є міграція працездатного населення, що негативно впливає на ринок праці та довгостроковий економічний потенціал.

Соціальна згуртованість суспільства слугує критичним фактором стійкості до спроб дестабілізації через розпалювання внутрішніх конфліктів. В Україні

політика національної єдності базується на принципах інклюзивності, рівності можливостей та взаємоповаги між різними соціальними групами. Для зменшення потенціалу для маніпуляцій та провокацій здійснюється протидія дискримінації за етнічною, мовною, релігійною чи регіональною ознакою. Розвиток громадянської ідентичності на основі спільних цінностей демократії, свободи та верховенства права підтримується через освітні програми, національні кампанії патріотичного виховання та волонтерські ініціативи. Діалог між різними сегментами суспільства активно стимулюється громадськими платформами та незалежними медіа, що допомагає зменшити поляризацію. Психологічна стійкість населення до інформаційних маніпуляцій та пропаганди формується через системну освітню та просвітницьку роботу. Розвиток критичного мислення з раннього віку через освітні програми готує громадян до самостійного аналізу інформації. В Україні впроваджено навчальні курси з медіаграмотності у школах та вищих навчальних закладах, які включають аналіз інформаційних потоків, виявлення фейків та оцінку достовірності джерел. Публічні кампанії з медіаграмотності, ініційовані Міністерством освіти, громадськими організаціями та міжнародними партнерами, підвищують обізнаність населення про техніки маніпуляції, методи пропаганди та способи їх розпізнавання [46]. Підтримка незалежної журналістики та якісних медіа створює альтернативу пропагандистським наративам. Робота з травматичним досвідом війни через психологічну підтримку запобігає колективній деморалізації. Культивування історичної пам'яті та національної гордості зміцнює психологічний імунітет суспільства. Розвиток волонтерського руху та громадської активності формує відчуття колективної відповідальності за долю країни. Попри високий рівень соціальної мобілізації, українське суспільство зазнає значного психологічного виснаження внаслідок тривалого стресу війни. Нерівний доступ до психологічної допомоги, особливо у прифронтових та сільських регіонах, підвищує ризики соціальної фрустрації. Соціально-економічна нерівність та відмінності у досвіді війни між різними групами населення можуть створювати потенційні лінії напруження, якими здатен скористатися противник.

Медична стійкість охоплює здатність системи охорони здоров'я функціонувати за екстремальних умов та протидіяти біологічним загрозам. В Україні розвивається мережа лікарень та медичних закладів з урахуванням можливих надзвичайних ситуацій, зокрема створюються мобільні госпіталі та інфраструктура для надання допомоги у прифронтових регіонах. Створено стратегічні запаси медикаментів, обладнання, засобів індивідуального захисту та кисневих концентраторів, що забезпечує готовність до масових надзвичайних подій. Медичний персонал проходить спеціальну підготовку для роботи в умовах масових втрат, бойових дій та епідемій, включаючи тренінги та симуляційні навчання. Розроблені та впроваджені національні протоколи дій у випадку біологічних загроз або пандемій, що стандартизують процедури та підвищують ефективність реагування [35]. Інвестиції у медичну науку, розвиток лабораторних потужностей та епідеміологічний нагляд дозволяють оперативно виявляти потенційні загрози. Крім того, налагоджена міжнародна співпраця з ВООЗ та іншими партнерами, що забезпечує обмін досвідом, поставки критично важливого обладнання та координацію під час кризових ситуацій.

Продовольча безпека визначає спроможність держави забезпечити населення достатньою кількістю якісного харчування незалежно від зовнішніх обставин. В Україні підтримка вітчизняного сільського господарства здійснюється через державні програми, субсидії та гранти для фермерів, що сприяє стабілізації виробництва зернових, овочів, молочної та м'ясної продукції. Створено стратегічні резерви продовольства для забезпечення населення під час кризових ситуацій та блокад постачання. Диверсифікація каналів експорту та імпорту сільськогосподарської продукції зменшує ризики, пов'язані з блокуванням окремих маршрутів. Створення державних резервів зерна та інших базових продуктів харчування забезпечує буфер на випадок кризи. Модернізація системи зберігання та транспортування продовольства підвищує ефективність логістики. Розвиток місцевого виробництва харчової продукції знижує залежність від великих виробників та довгих ланцюгів постачання. Підтримка фермерських

господарств та кооперативів диверсифікує виробництво та підвищує стійкість продовольчої системи [39, с. 134].

Транспортна інфраструктура становить критичний елемент національної стійкості, забезпечуючи мобільність військ, евакуацію населення та логістику постачання. В Україні проведено модернізацію ключових залізничних та автомобільних маршрутів для швидкого переміщення військової техніки та гуманітарної допомоги. Створено резервні транспортні коридори та обхідні маршрути для уникнення блоkad та пошкоджень критичних шляхів. Розвиваються логістичні хаби, склади та пункти прийому вантажів для ефективного розподілу ресурсів у прифронтових регіонах. Розвиток мультимодальних транспортних коридорів створює альтернативні маршрути на випадок пошкодження окремих шляхів. Модернізація залізничного транспорту підвищує можливості перевезення великих обсягів вантажів та людей. Розбудова мережі автомобільних доріг, зокрема стратегічних магістралей, забезпечує швидку логістику у критичних ситуаціях. Захист транспортних вузлів та критичних об'єктів інфраструктури від кінетичних та кібератак підвищує стійкість системи. Інтеграція транспортних мереж України до європейських коридорів відкриває додаткові можливості для логістики та евакуації.

Освітня система відіграє стратегічну роль у формуванні довгострокової стійкості суспільства через виховання свідомих та підготовлених громадян. В Україні впроваджуються предмети з безпеки життєдіяльності, медіаграмотності та критичного мислення у шкільні програми, що готує молоде покоління до сучасних викликів, зокрема інформаційних і гібридних загроз. Розвивається цифрова грамотність учнів через інтерактивні курси та онлайн-платформи, що дозволяє молоді орієнтуватися в інформаційному просторі та розпізнавати маніпуляції [34]. Вивчення національної історії та громадянської освіти формує патріотичні цінності та розуміння демократичних принципів. Підготовка вчителів до викладання чутливих тем, пов'язаних з війною та пропагандою, підвищує якість освітнього процесу. Розвиток академічних обмінів та міжнародних освітніх програм розширює світогляд та створює мережу міжнародних контактів.

Інвестиції у наукові дослідження з питань національної безпеки формують експертну базу для прийняття стратегічних рішень [21, с. 267].

Технологічна незалежність у критичних галузях зменшує вразливість держави до технологічних санкцій та маніпуляцій з боку недружніх країн. Розвиток власного виробництва електроніки, програмного забезпечення та телекомунікаційного обладнання створює технологічну автономію. Підтримка інновацій через державні гранти та венчурні фонди стимулює розвиток національних технологічних компаній. Створення технопарків та інноваційних кластерів концентрує ресурси та таланти для проривних розробок. Захист інтелектуальної власності та комерційних таємниць запобігає витоку критичних технологій. Співпраця з демократичними країнами у сфері трансферу технологій прискорює розвиток національних компетенцій. Інвестиції у STEM-освіту формують кадровий потенціал для технологічного прориву у довгостроковій перспективі.

Правова система та верховенство права створюють фундамент для стійкості демократичних інституцій та довіри суспільства до держави. Боротьба з корупцією підвищує ефективність державного управління та легітимність влади в очах громадян. Незалежність судової системи гарантує справедливість та рівність перед законом, що зміцнює соціальну згуртованість. Прозорість державних процедур та доступ до публічної інформації знижують простір для маніпуляцій та зловживань. Захист прав людини та свобод створює контраст з авторитарними режимами та підкреслює демократичні цінності. Ефективна робота правоохоронних органів забезпечує безпеку громадян та протидіє диверсійній діяльності. Імплементация європейських правових стандартів наближає Україну до спільноти демократичних держав [1, с. 312]. Водночас слабкість інституційної спроможності, повільність судових процедур та непослідовність антикорупційних реформ негативно впливають на рівень довіри громадян до держави. Воєнний стан, попри свою об'єктивну необхідність, створює ризики обмеження демократичних процедур і посилює навантаження на механізми громадського контролю.

Громадський сектор та волонтерський рух демонструють унікальну здатність швидко реагувати на кризові ситуації та заповнювати прогалини державних інституцій. В Україні підтримка неурядових організацій здійснюється через державні гранти, податкові пільги та програми співфінансування соціальних проєктів, що зміцнює їхню спроможність виконувати важливі соціальні функції. Волонтерські ініціативи активно забезпечують військових та цивільне населення гуманітарною допомогою, медичними та технічними ресурсами, а також організовують логістичну підтримку постраждалих регіонів. Координація між державними органами та громадськими організаціями підвищує ефективність гуманітарної допомоги та соціальних послуг. Розвиток платформ для волонтерства та громадської активності мобілізує ресурси суспільства для спільних цілей. Захист активістів та правозахисників від переслідувань гарантує можливість громадського контролю за владою. Фінансова прозорість громадських організацій та механізми підзвітності підвищують довіру до третього сектору. Міжнародна підтримка українського громадянського суспільства через донорські програми посилює його спроможність та стійкість.

Культурна дипломатія та збереження національної ідентичності протидіють спробам асиміляції та культурного домінування з боку агресора. Підтримка української мови, літератури та мистецтва зміцнює культурну самобутність та гордість за національну спадщину. Популяризація української культури за кордоном формує позитивний образ країни та підвищує міжнародну солідарність. Захист історичних пам'яток та культурної спадщини від руйнування зберігає зв'язок з минулим та національну пам'ять. Розвиток креативних індустрій та культурного підприємництва створює економічний потенціал культурного сектору. Культурні обміни з демократичними країнами розширюють міжнародні зв'язки та взаєморозуміння. Документування воєнних злочинів проти культурної спадщини створює доказову базу для міжнародного правосуддя та історичної пам'яті [3, с. 178].

3.2. Вдосконалення інформаційної стійкості українського суспільства.

Стратегічні комунікації являють собою координоване використання інформаційних інструментів для досягнення національних цілей через формування сприятливого інформаційного середовища. Ефективні стратегічні комунікації поєднують довгострокове планування, послідовність повідомлень та синхронізацію дій різних державних акторів. Система стратегічних комунікацій має охоплювати як внутрішню, так і зовнішню аудиторію, враховуючи специфіку кожного сегменту. Координація між урядовими відомствами, військовими структурами та громадянським суспільством забезпечує єдність наративу. Моніторинг інформаційного середовища дозволяє оперативно реагувати на дезінформаційні кампанії та коригувати стратегію. Оцінка ефективності комунікаційних зусиль через аналітичні метрики забезпечує можливість постійного вдосконалення [8, с. 92]. Водночас практика реалізації стратегічних комунікацій в Україні виявляє низку системних проблем. Насамперед йдеться про фрагментарність комунікаційних зусиль та відсутність сталої довгострокової стратегії, що зберігала б послідовність незалежно від кадрових змін і політичної кон'юнктури. Часто спостерігається реактивний характер комунікацій, коли державні інституції переважно відповідають на кризові події, а не формують проактивний порядок денний. Це знижує ефективність інформаційного впливу та дозволяє противнику нав'язувати власні наративи.

Інформаційна стійкість суспільства визначається здатністю громадян розпізнавати маніпулятивний контент та зберігати критичне мислення під впливом інформаційних атак. Масова медіаграмотність населення створює імунітет проти примітивних форм пропаганди та дезінформації. Розуміння механізмів роботи алгоритмів соціальних мереж допомагає усвідомити, як формується персоналізована інформаційна бульбашка. Навички перевірки фактів та джерел інформації дозволяють громадянам самостійно оцінювати достовірність повідомлень. Психологічна підготовка до сприйняття травматичного контенту знижує шок від пропагандистських матеріалів. Розвиток

альтернативних джерел інформації створює конкуренцію пропагандистським каналам. Формування звички споживати різноманітний контент з різних джерел розширює інформаційний горизонт громадян. Попри розвиток програм з медіаграмотності, рівень інформаційної стійкості суспільства залишається нерівномірним. Значна частина населення, особливо люди старшого віку, має обмежений доступ до якісних освітніх ресурсів і сучасних джерел інформації. Вплив емоційного виснаження, пов'язаного з війною, знижує здатність до критичного аналізу повідомлень та підвищує сприйнятливність до спрощених або маніпулятивних наративів. Наведене створює вразливості, які можуть використовуватися у довгострокових психологічних операціях.

Національна система стратегічних комунікацій потребує чіткої інституційної структури з визначеними повноваженнями та ресурсами. Створення координаційного центру стратегічних комунікацій при уряді забезпечує централізоване планування та моніторинг. Призначення відповідальних за комунікації у кожному міністерстві та відомстві дозволяє швидко реагувати на інформаційні виклики. Розробка єдиної методології оцінки інформаційних загроз стандартизує підходи різних відомств. Регулярне навчання державних комунікаторів новим техніками та інструментам підвищує професійний рівень. Залучення експертів з приватного сектору та академічного середовища збагачує комунікаційні стратегії. Міжвідомча координація через регулярні наради та обмін інформацією синхронізує дії різних акторів [63, с. 145]. Важливою проблемою залишається недостатня інституційна спроможність системи стратегічних комунікацій. Перетин повноважень між різними органами влади, нечіткий розподіл відповідальності та відсутність єдиного центру ухвалення комунікаційних рішень у кризових ситуаціях призводять до суперечливих повідомлень. Брак кадрових ресурсів і перевантаженість державних комунікаторів обмежують можливості для глибокої аналітики та стратегічного планування. Проактивна комунікаційна стратегія передбачає формування власного наративу замість лише реагування на ворожу пропаганду. Визначення ключових повідомлень та цінностей, які держава намагається донести, створює

основу для всіх комунікацій. Розробка довгострокових комунікаційних кампаній дозволяє систематично просувати національні інтереси. Використання storytelling та емоційно резонансних історій підвищує залучення аудиторії до повідомлень. Персоналізація комунікацій під різні цільові групи збільшує релевантність та ефективність впливу. Регулярність та передбачуваність комунікацій створюють довіру аудиторії до джерела інформації. Швидкість реакції на події дозволяє формувати первинну інтерпретацію подій до появи альтернативних наративів.

Цифрові платформи та соціальні мережі стали основним полем битви за увагу та переконання громадян. Розвиток державних акаунтів у соціальних мережах забезпечує прямий канал комунікації з населенням без посередників. Використання мультимедійного контенту, включаючи відео, інфографіку та інтерактивні елементи, підвищує привабливість повідомлень. Співпраця з популярними блогерами та інфлюенсерами розширює охоплення аудиторії, особливо молодії. Моніторинг настроїв у соціальних мережах через аналітичні інструменти дозволяє відстежувати ефективність комунікацій. Швидке реагування на коментарі та питання користувачів створює відчуття діалогу та залученості. Протидія ботам та координованим кампаніям дезінформації захищає цифровий простір від маніпуляцій [43, с. 201]. Попри активне використання соціальних мереж, цифрове середовище створює низку додаткових ризиків для стратегічних комунікацій. Алгоритмічна логіка платформ сприяє поширенню емоційного та конфліктного контенту, що ускладнює донесення складних і збалансованих державних повідомлень. Висока швидкість поширення інформації часто не залишає часу для ретельної перевірки фактів, а помилки в офіційних комунікаціях можуть швидко підірвати довіру аудиторії. Крім того, залежність від приватних цифрових платформ обмежує контроль держави над каналами комунікації. Медіаграмотність як системна компетенція має інтегруватися у освітній процес на всіх рівнях від початкової школи до вищої освіти. Базові навички критичного мислення закладаються у молодшому шкільному віці через аналіз простих медіатекстів. Поглиблене вивчення технік пропаганди, когнітивних спотворень та емоційних маніпуляцій відбувається у середній школі.

Практичні вправи з перевірки фактів та аналізу джерел формують конкретні навички роботи з інформацією. Створення шкільних медіа та участь у журналістських проєктах дозволяє зрозуміти виробництво контенту зсередини. Залучення професійних журналістів та медіаекспертів до освітнього процесу забезпечує практичну спрямованість навчання. Регулярне оновлення навчальних матеріалів відповідає швидким змінам у медіаландшафті та технологіях.

Незалежна журналістика становить критичний елемент інформаційної екосистеми демократичного суспільства та протидію державній та корпоративній пропаганді. Фінансова підтримка незалежних медіа через державні гранти, міжнародні донори та передплатні моделі забезпечує їхню стійкість. Захист журналістів від фізичних нападів, юридичного переслідування та цифрових атак гарантує можливість виконувати професійні обов'язки. Доступ до публічної інформації та можливість отримувати коментарі від державних органів забезпечує журналістські розслідування. Професійні стандарти та етичні кодекси підтримують якість журналістської роботи та довіру аудиторії. Співпраця між журналістами різних країн при розслідуванні міжнародних схем дезінформації підвищує ефективність викриттів. Інвестиції у журналістську освіту та тренінги з безпеки готують нове покоління професіоналів [22, с. 267].

Фактчекінг як інститут перевірки публічних заяв та вірусного контенту набув критичного значення в епоху пандемії дезінформації. Створення мережі фактчекінгових організацій з різною спеціалізацією забезпечує широке покриття інформаційного простору. Методологія перевірки фактів має базуватися на прозорих стандартах та використанні первинних джерел інформації. Співпраця з соціальними мережами дозволяє маркувати перевірений контент та обмежувати поширення дезінформації. Популяризація фактчекінгових ресурсів через освітні кампанії підвищує їхню видимість та використання громадянами. Міжнародна мережа фактчекерів забезпечує обмін методиками та спільну роботу над транскордонними темами. Фінансування фактчекінгу через різні джерела, включаючи краудфандинг, гарантує незалежність від окремих спонсорів. Контрнаративи та спростування дезінформації мають створюватися на основі

психологічних досліджень ефективності різних підходів до переконання. Пряме спростування фейків може бути неефективним через ефект зворотного удару, коли люди лише зміцнюються у хибних переконаннях. Створення альтернативних наративів, що пропонують інше пояснення подій, часто виявляється більш переконливим. Використання емоційних історій реальних людей резонує краще за абстрактні статистичні дані. Залучення довірених комунікаторів з відповідних спільнот підвищує сприйнятливість до повідомлень. Фокусування на цінностях та спільних цілях замість конфронтації знижує захисні реакції аудиторії. Регулярне тестування ефективності різних підходів через фокус-групи та опитування дозволяє оптимізувати стратегії [64, с. 89]. Незалежна журналістика та фактчекінг в Україні функціонують в умовах постійного тиску та ресурсних обмежень. Залежність від грантового фінансування створює ризики нестабільності роботи медіа та перевантаження редакцій. Фактчекінгові матеріали часто мають обмежене охоплення і не встигають нейтралізувати дезінформацію, яка поширюється значно швидше. Додатковим викликом є зростання недовіри до медіа з боку частини населення, що знижує ефективність навіть якісних спростувань.

Цифрова гігієна та кібербезпека на індивідуальному рівні захищають громадян від таргетованих інформаційних операцій та витоку персональних даних. Навички створення надійних паролів та використання двофакторної автентифікації знижують ризик зловживань акаунтів. Обережність при відкритті підозрілих посилань та завантаженні файлів запобігає зараженню шкідливим програмним забезпеченням. Розуміння налаштувань приватності у соціальних мережах дозволяє контролювати, хто має доступ до особистої інформації. Використання шифрованих месенджерів для чутливих розмов захищає від прослуховування та витоку даних. Регулярне оновлення програмного забезпечення закриває вразливості, якими можуть скористатися зловмисники. Обізнаність про соціальну інженерію та фішингові схеми готує до розпізнавання спроб маніпуляції. Психологічні операції ворога часто використовують когнітивні упередження та емоційні тригери для маніпуляції свідомістю. Розуміння

механізмів підтвердження власної думки допомагає усвідомити тенденцію шукати інформацію, що підтверджує наявні переконання. Знання про ефект хибної консенсусності пояснює, чому людина переоцінює поширеність власних поглядів. Усвідомлення емоційного зараження у соціальних мережах дозволяє критично ставитися до вірусного контенту. Розпізнавання апелювання до страху як маніпулятивної техніки знижує ефективність залякувальних кампаній. Критичне ставлення до анонімних джерел та непідтверджених чуток запобігає поширенню панічних настроїв. Рефлексія власних емоційних реакцій на інформацію допомагає відокремити факти від маніпуляції почуттями [39, с. 156].

Мовна політика та використання державної мови у публічному просторі має стратегічне значення для національної ідентичності та протидії культурній асиміляції. Підтримка української мови у медіа, освіті та державних установах зміцнює її позиції та престиж у суспільстві. Розвиток української термінології у технічних та наукових галузях забезпечує можливість повноцінного функціонування мови у всіх сферах. Популяризація української літератури, музики та кінематографу через державні програми підвищує культурний статус мови. Захист мовних прав меншин при одночасному зміцненні позицій державної мови створює баланс між єдністю та різноманіттям. Протидія мовній дискримінації та стигматизації україномовних громадян підтримує атмосферу взаємоповаги. Міжнародна промоція української мови через культурні центри та мовні курси за кордоном розширює її глобальне присутність. Візуальна комунікація та символіка відіграють потужну роль у формуванні колективної ідентичності та емоційної мобілізації суспільства. Державні символи, такі як прапор, герб та гімн, консолідують національну спільноту навколо спільних цінностей. Меморіальна політика та вшанування національних героїв формує історичну пам'ять та зразки для наслідування. Сучасне мистецтво та графічний дизайн створюють актуальні візуальні образи, що резонують з молододою аудиторією. Використання національної символіки у публічному просторі через муніципальні програми підкреслює приналежність територій до єдиної держави. Документальна фотографія та відеофіксація подій війни створює візуальний архів

для майбутніх поколінь. Міжнародні виставки та культурні проєкти представляють українську візуальну культуру світовій спільноті [67, с. 223]. Реалізація мовної та ідентифікаційної політики у сфері стратегічних комунікацій також стикається з низкою труднощів. Недостатньо чутливе або формалізоване впровадження мовних норм може спричиняти спротив у окремих соціальних групах та використовуватися противником для розпалювання внутрішніх конфліктів. Баланс між утвердженням державної мови та повагою до культурного різноманіття потребує постійного коригування комунікаційних підходів.

Регіональні особливості комунікаційних стратегій враховують різницю в історичному досвіді, мовних преференціях та інформаційних звичках населення. Адаптація національних повідомлень до локального контексту підвищує їхню релевантність та сприйнятливість. Використання регіональних медіа та місцевих лідерів думок забезпечує більшу довіру до інформації. Врахування специфіки прикордонних регіонів, що зазнають інтенсивного інформаційного впливу сусідніх країн, вимагає додаткових зусиль. Підтримка місцевої журналістики та регіональних медіа зміцнює інформаційну присутність держави на всій території. Координація між центральними та регіональними органами влади у комунікаціях запобігає суперечливим повідомленням. Моніторинг регіональних інформаційних середовищ дозволяє виявляти локальні загрози та своєчасно реагувати. Міжнародна комунікація та публічна дипломатія формують образ України у світі та забезпечують підтримку міжнародної спільноти. Координація повідомлень дипломатичних місій за кордоном створює єдиний міжнародний наратив держави. Співпраця з міжнародними медіа та інформаційними агентствами забезпечує присутність української позиції у глобальному інформаційному просторі. Залучення закордонних експертів та аналітиків до коментування подій в Україні додає авторитетності національній позиції. Культурна дипломатія через мистецькі проєкти та освітні обміни створює позитивні асоціації з Україною. Робота з діаспорою мобілізує українців за кордоном як амбасадорів національних інтересів. Моніторинг міжнародного інформаційного простору дозволяє відстежувати ефективність публічної дипломатії та коригувати стратегії [60, с.

298]. У сфері міжнародних стратегічних комунікацій Україна стикається з конкуренцією з боку держав, які мають значно більші фінансові, медійні та технологічні ресурси. Обмежені можливості системного аналізу іноземних аудиторій і нестача спеціалізованих кадрів ускладнюють адаптацію повідомлень до різних культурних контекстів. Це зумовлює потребу у подальшому вдосконаленні інструментів публічної дипломатії та довгострокового стратегічного планування.

3.3. Міжнародна співпраця і колективні заходи протидії гібридним загрозам

Міжнародна співпраця у протидії гібридним загрозам базується на усвідомленні транснаціонального характеру цих викликів та неможливості ефективної відповіді лише національними зусиллями. Гібридні операції часто використовують юрисдикційні прогалини та відмінності у правових системах різних держав для уникнення відповідальності. Координація дій між країнами дозволяє створювати комплексні відповіді, що охоплюють різні аспекти гібридних загроз одночасно. Обмін розвідувальною інформацією між союзниками підвищує якість аналізу та швидкість виявлення загроз. Спільні навчання та тренінги формують єдині процедури та взаєморозуміння між фахівцями різних країн. Багатосторонні механізми легітимізують колективні дії та створюють правову основу для міжнародної відповіді. Формування міжнародних норм поведінки у кіберпросторі та інформаційній сфері встановлює межі дозволеного та створює підстави для санкцій [51, с. 134].

Євроатлантична інтеграція України створює рамку для поглибленої співпраці з демократичними країнами у сфері безпеки та оборони. Хоча Україна ще не є членом НАТО, участь у програмах Партнерство заради миру, НАТО-Україна Комісія та інших ініціативах Альянсу вже дозволяє отримувати консультації, тренінги та технічну допомогу для реформування сектору безпеки. В Україні проводяться численні спільні військові навчання з країнами-членами НАТО, зокрема «Rapid Trident», «Sea Breeze», «Combined Resolve», що готують

Збройні сили України до координації дій у кризових та бойових ситуаціях [77]. Адаптація національних систем безпеки та оборони до стандартів НАТО включає модернізацію командно-штабних структур, інтеграцію систем зв'язку та логістики, а також підготовку персоналу за міжнародними процедурами планування операцій. Обмін досвідом протистояння російській агресії України дозволяє НАТО покращувати розуміння сучасних гібридних загроз і розробляти нові методи колективного реагування. Політична підтримка з боку Альянсу та держав-членів посилює міжнародну легітимність України, сприяє дипломатичному тиску на агресора та підвищує рівень стримування подальшої ескалації з боку Росії.

Європейський Союз розробив низку інструментів протидії гібридним загрозам, до яких Україна може отримати доступ через поглиблену асоціацію. Центр передового досвіду з протидії гібридним загрозам у Гельсінкі проводить дослідження та тренінги для урядовців європейських країн. Система швидкого сповіщення про дезінформацію дозволяє оперативно обмінюватися інформацією про кампанії маніпуляції. Санкційні механізми ЄС можуть застосовуватися проти осіб та організацій, причетних до гібридних операцій. Фінансування проєктів зміцнення стійкості через європейські фонди підтримує розвиток національних спроможностей. Гармонізація законодавства України з європейськими стандартами кібербезпеки та захисту персональних даних підвищує загальний рівень захисту. Участь у європейських дослідницьких програмах з безпеки дозволяє долучитися до передових розробок [67, с. 187].

Двостороння співпраця з окремими країнами-партнерами доповнює багатосторонні механізми та дозволяє враховувати специфічні інтереси. Стратегічне партнерство зі Сполученими Штатами забезпечує доступ до розвідувальної інформації, військової допомоги та технологій. Співпраця з Великою Британією у сфері кібербезпеки та стратегічних комунікацій використовує британський досвід протидії російському впливу. Партнерство з країнами Балтії та Польщею базується на спільному досвіді протистояння гібридним загрозам з боку Росії. Обмін досвідом з Ізраїлем у сфері

контртероризму та захисту критичної інфраструктури збагачує національні практики. Технологічна співпраця з провідними демократичними країнами прискорює цифрову трансформацію систем безпеки. Координація санкційної політики з партнерами підвищує ефективність економічного тиску на агресора.

Міжнародні організації забезпечують платформи для багатосторонньої координації та вироблення спільних підходів до нових викликів. Організація з безпеки і співробітництва в Європі може сприяти діалогу та зменшенню напруженості, хоча її ефективність обмежена принципом консенсусу. Рада Європи встановлює правові стандарти захисту прав людини, що протистоять авторитарним практикам. Організація Об'єднаних Націй, незважаючи на блокування Радою Безпеки, залишається форумом для артикуляції позиції України та засудження агресії. Міжнародні фінансові інституції підтримують економічну стійкість через кредити та технічну допомогу. Спеціалізовані агенції, такі як Міжнародна організація цивільної авіації чи Міжнародний союз електрозв'язку, встановлюють галузеві стандарти безпеки. Участь України у міжнародних ініціативах підвищує видимість країни та доступ до глобальних ресурсів [29, с. 245].

Обмін розвідувальною інформацією між країнами-партнерами підвищує ситуаційну обізнаність та дозволяє передбачати гібридні операції. Створення захищених каналів комунікації забезпечує конфіденційність передачі чутливих даних. Стандартизація форматів та класифікації інформації полегшує обмін між різними службами. Спільний аналіз загроз об'єднує експертизу різних країн та дозволяє виявляти складні патерни. Атрибуція кібератак через міжнародну співпрацю підвищує точність визначення джерела агресії. Своєчасні попередження про потенційні операції дають можливість підготуватися та мінімізувати шкоду. Збереження довіри між партнерами вимагає дотримання правил використання спільної інформації та захисту джерел. Спільні навчання та тренінги формують єдине розуміння гібридних загроз та відпрацьовують координовані відповіді на кризові сценарії. Міжнародні військові навчання включають елементи протидії дезінформації, кібератакам та диверсійним діям.

Tabletop exercises для урядовців імітують кризові ситуації та тестують процедури прийняття рішень. Обмін персоналом між службами безпеки різних країн дозволяє вивчати кращі практики зсередини. Спільні дослідницькі проекти академічних установ різних країн розширюють теоретичну базу розуміння гібридних загроз. Тренінги для журналістів з виявлення дезінформації підвищують стійкість медіасередовища. Регулярність та систематичність навчань забезпечує підтримання високого рівня готовності [52, с. 312].

Технологічна співпраця та трансфер критичних технологій прискорюють розвиток національних спроможностей протидії гібридним загрозам. Доступ до передових систем кіберзахисту зменшує технологічний розрив між Україною та провідними країнами. Спільна розробка систем раннього попередження про інформаційні атаки об'єднує ресурси та експертизу. Передача технологій шифрування та захисту комунікацій підвищує безпеку урядового зв'язку. Співпраця у розробці штучного інтелекту для виявлення дезінформації автоматизує моніторинг інформаційного простору. Доступ до супутникових систем спостереження партнерів покращує моніторинг ситуації на кордонах. Захист інтелектуальної власності та комерційних таємниць у рамках співпраці вимагає відповідних правових механізмів. Координація санкційної політики підвищує ефективність економічного тиску на державу-агресора та осіб, причетних до гібридних операцій. Синхронізація санкційних списків між союзниками ускладнює обхід обмежень через треті країни. Санкції проти медіа, що поширюють дезінформацію, обмежують їхні можливості впливу. Заморожування активів осіб, причетних до гібридних операцій, створює особисту відповідальність. Обмеження доступу до фінансових систем ускладнює фінансування гібридних кампаній. Експортний контроль на технології подвійного призначення запобігає їх використанню у ворожих цілях. Моніторинг виконання санкцій та закриття лазівок підтримує їхню ефективність протягом тривалого часу [76, с. 178].

Правова співпраця та екстрадиція осіб, причетних до злочинів у рамках гібридних операцій, в Україні здійснюється через міждержавні угоди та міжнародні

інструменти, зокрема Інтерпол та Європейський ордер на арешт. Це ускладнює переміщення підозрюваних та обмежує їхню свободу дій. Українська прокуратура активно співпрацює з правоохоронними органами інших держав у зборі доказів, обміні матеріалами та проведенні спільних слідчих дій щодо осіб, причетних до фінансування тероризму, диверсій та гібридних атак. Міжнародні трибунали, зокрема Міжнародний кримінальний суд (МКС), розглядають справи, пов'язані з воєнними злочинами та злочинами проти людяності на тимчасово окупованих територіях України. В рамках таких процесів впроваджено механізми захисту свідків та викривачів, що дозволяє забезпечити безпеку учасників і їхню готовність надавати показання. Визнання рішень українських судів в інших країнах полегшує виконання вироків та забезпечує міжнародну правову підтримку у переслідуванні злочинців. Комплексна участь у міжнародному правосудді сприяє боротьбі з безкарністю та створює стримуючий ефект для потенційних порушників, демонструючи ефективність міжнародної координації у сфері протидії гібридним загрозам.

Фінансова підтримка партнерів забезпечує ресурси для розбудови національних спроможностей протидії гібридним загрозам. Військова допомога включає постачання обладнання, зброї та підготовку персоналу. Фінансування програм кібербезпеки дозволяє модернізувати захист критичної інфраструктури. Гранти на розвиток медіаграмотності підтримують освітні програми та громадські ініціативи. Технічна допомога у реформуванні сектору безпеки прискорює імплементацію міжнародних стандартів. Бюджетна підтримка стабілізує економіку та дозволяє підтримувати соціальні програми під час війни. Прозорість використання міжнародної допомоги через моніторингові механізми підтримує довіру донорів [80, с. 289]. Створення регіональних мереж протидії гібридним загрозам об'єднує країни зі спільними викликами та географічною близькістю. Балтійсько-Чорноморська співпраця може сфокусуватися на протидії російському впливу у регіоні. Обмін досвідом між постсоціалістичними країнами враховує спільну історичну спадщину та подібні вразливості. Координація прикордонного контролю ускладнює транскордонну незаконну діяльність та переміщення агентів

впливу. Спільні медіаплатформи для протидії дезінформації розширюють охоплення аудиторії. Регіональні центри досліджень гібридних загроз концентрують експертизу та ресурси. Політична координація через регіональні форуми дозволяє виробляти спільні позиції на міжнародній арені.

Громадська дипломатія та взаємодія між громадянськими суспільствами різних країн створює неформальні мережі підтримки та солідарності. Міжнародні неурядові організації здійснюють моніторинг дотримання прав людини та документують порушення. Академічні обміни формують спільноту дослідників, що вивчають гібридні загрози з різних перспектив. Культурні проєкти створюють емоційні зв'язки між народами та сприяють взаєморозумінню. Волонтерські мережі мобілізують ресурси громадянського суспільства для гуманітарної допомоги. Правозахисні організації звертають увагу міжнародної спільноти на порушення та вимагають відповідальності. Цифрові платформи для транснаціональної активності дозволяють координувати дії активістів різних країн без географічних обмежень [28, с. 201]. Довгострокова стратегія міжнародної співпраці має враховувати зміни у глобальному балансі сил та нові форми гібридних загроз. Багатополярність світового порядку вимагає диверсифікації партнерств та уникнення надмірної залежності від окремих союзників. Технологічні зміни створюють нові вектори загроз, що потребують випереджаючої міжнародної координації. Кліматичні зміни та ресурсні конфлікти можуть використовуватися як інструменти гібридного тиску. Демографічні зрушення та міграційні потоки створюють нові вразливості для маніпуляцій. Розвиток штучного інтелекту радикально змінить характер інформаційних операцій. Інституційна гнучкість та здатність до адаптації визначатимуть ефективність міжнародної співпраці у майбутньому.

ВИСНОВКИ

У ході виконання кваліфікаційної магістерської роботи було здійснено дослідження феномену гібридних війн у сучасному міжнародному середовищі. Отримані результати підтверджують, що гібридні війни є не тимчасовим відхиленням від класичних форм воєнного протистояння, а стійкою тенденцією розвитку міжнародної безпеки у XXI столітті, яка суттєво змінює уявлення про суверенітет, воєнну силу, політичний вплив та механізми міжнародної відповідальності.

У результаті дослідження поняття гібридної війни та її еволюції з'ясовано, що гібридна війна є складною формою конфлікту, яка поєднує традиційні військові дії з широким спектром невійськових інструментів - політичних, економічних, інформаційно-психологічних і кібернетичних. Її основною особливістю є прагнення агресора досягти стратегічних політичних цілей без формального оголошення війни, з мінімізацією власних витрат і водночас із розмиванням правової відповідальності. Еволюція гібридних війн засвідчує, що хоча поєднання військових і невійськових засобів існувало впродовж усієї історії воєн, у сучасних умовах воно набуло принципово нових масштабів і форм завдяки цифровим технологіям, глобальним інформаційним мережам та високому рівню взаємозалежності держав.

Аналіз основних компонентів гібридного впливу, а саме військового, інформаційного, економічного та кібернетичного, показав, що військова складова в гібридній війні часто відіграє роль інструмента тиску та залякування, а не засобу тотального знищення противника, і доповнюється використанням проксі-сил, нерегулярних формувань та прихованої присутності регулярних військ. Інформаційний компонент виступає елементом гібридного протистояння, оскільки спрямований на зміну сприйняття реальності, деморалізацію населення, підрив довіри до державних інститутів та формування вигідних агресору наративів. Економічний вплив проявляється через енергетичний шантаж, торговельні обмеження, фінансовий тиск і підтримку корупційних мереж, тоді як кібернетичний компонент забезпечує можливість паралізації критичної

інфраструктури та посилення інформаційних операцій. У сукупності ці компоненти створюють синергетичний ефект, що значно ускладнює своєчасне виявлення агресії та ефективну відповідь на неї.

Розглянуті методологічні підходи до аналізу гібридних війн у сучасному міжнародному середовищі доводять доцільність застосування системного підходу, який дозволяє розглядати гібридну війну як цілісну сукупність взаємопов'язаних дій у різних сферах. Важливу роль відіграє міждисциплінарний підхід, що поєднує інструментарій політичної науки, безпекових студій, міжнародного права, психології та інформаційних технологій. Конфліктологічний підхід дозволяє дослідити динаміку та етапи гібридних конфліктів, а інформаційно-комунікативний і кібернетичний підходи - проаналізувати роль медіа та цифрового простору як повноцінних полів бою. У результаті доведено, що традиційні методи аналізу воєнних конфліктів є недостатніми для пояснення гібридних війн, що потребує оновлення наукового інструментарію.

Проведена оцінка гібридної агресії РФ проти України та її впливу на політичну систему держави. У роботі встановлено, що російсько-українська війна є одним із найбільш комплексних прикладів гібридного конфлікту сучасності, в якому поєднуються військова агресія, масовані інформаційно-психологічні операції, економічний тиск та кібератаки. Така форма агресії спричинила глибокі трансформації політичної системи України, зокрема посилення ролі сектору безпеки й оборони, зміцнення інституцій стратегічних комунікацій, зміну законодавчого поля у сфері національної безпеки та консолідацію суспільства навколо ідей суверенітету й європейського вибору. Водночас гібридна війна виявила структурні вразливості української держави, пов'язані з інституційною слабкістю, інформаційною уразливістю та економічною залежністю, що потребують системного подолання.

Розроблено рекомендації щодо вдосконалення публічної політики України та міжнародного співробітництва у сфері протидії гібридним загрозам. У результаті обґрунтовано необхідність формування комплексної державної політики, спрямованої на підвищення національної стійкості, розвиток системи

стратегічних комунікацій, посилення кіберзахисту та інституційну взаємодію між органами влади, громадянським суспільством і приватним сектором. Особливу увагу слід приділяти розвитку міжнародного співробітництва з ЄС, НАТО та іншими партнерами у сфері обміну інформацією, спільного реагування на гібридні загрози та гармонізації нормативно-правових механізмів. Український досвід протидії гібридній агресії має важливе значення для формування нових підходів до колективної безпеки у Європі та світі загалом.

Узагальнюючи результати дослідження, можна стверджувати, що гібридні війни стали одним із провідних інструментів сучасного міжнародного протистояння, а їх поширення свідчить про кризу традиційних механізмів міжнародної безпеки. Досвід України демонструє, що успішна протидія гібридним загрозам можлива лише за умови поєднання воєнних, політичних, інформаційних та соціально-економічних заходів, а також активної участі міжнародної спільноти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Archive for Investors. Vodafone Ukraine. Vodafone Україна - Мобільний зв'язок, Інтернет, Тарифи та Послуги. URL: <https://www.vodafone.ua/en/company/investors/zvityta-rezultaty/informatsiya-emitenta/arkhiv>
2. Актуальні проблеми вітчизняної та всесвітньої історії: Наукові записки Рівненського державного гуманітарного університету [Текст]: збірник наукових праць. Вип. 23 / ред. Р. М. Постолюк. - Рівне: РДГУ, 2012. - 688 с. - 50.00 р.
3. Блащук В. О. Інформаційна війна як технологія політичного пресингу : кваліфікаційна робота бакалавра: 052 Політологія / В. О. Блащук; Хмельниц. нац. ун-т. – Хмельницький, 2025. – 66 с.
4. Бутова О. Мистецтво перемогати: уроки Сунь-цзи для України ВСЛ. Видавництво Старого Лева. URL: <https://starylev.com.ua/news/mystectvo-peremagaty-uroky-sun-czy-dlya-ukrayiny?srsId=AfmBOoqWLKWq3YAjUwdcXHlfqQY1kPKrUOJRHxLxAE TZCJVqHVCjTFjg>
5. Будапештська конвенція про кіберзлочинність як основний міжнародно - правовий стандарт щодо кіберзлочинності. Юридичний факультет ЧНУ ім. Юрія Федьковича. URL: <https://law.chnu.edu.ua/budapeshtska-konventsiaa-pro-kiberzlochynnist/>
6. Bondarenko S. National resilience as a determinant of national security of Ukraine. Journal of Optimization in Industrial Engineering. 2021. Vol. 14. P. 87–93. URL: <https://doi.org/10.22094/JOIE.2020.677837>.
7. Ben-Dor, G., et al. (2002). The Role of Public Opinion in Israel's National Security. American Jewish Congress: Congress Monthly, 69(5), 13-15.
8. Верютіна Д. Діяльність Німеччини в ОБСЄ в рамках врегулювання суспільно-політичної кризи на сході України. Роль зовнішнього чинника у суспільно-політичній кризі на Південному Сході України: автореф. Кваліфікаційна робота на здобуття ступеня магістра. Острогоз, 2021. 94 с.

URL: [https://theses.oa.edu.ua/DATA/2456/Магістерська%20робота_Стригуль_Альона_MMB-61%20\(1\).pdf](https://theses.oa.edu.ua/DATA/2456/Магістерська%20робота_Стригуль_Альона_MMB-61%20(1).pdf).

9. Воронков О. С. Гібридні війни: сутність, структура, методологія дослідження: Монографія. Київ, 2021. 560 с.
10. Внутрішня безпека Нацполіції та СБУ викрили агентурну мережу фсб, до якої входили ексохоронці Януковича. Національна поліція України.
URL: <https://npu.gov.ua/news/vnutrishnia-bezpeka-natspolitsii-ta-sbu-vykryly-ahenturnu-merezhу-fsb-do-iakoi-vkhodyly-eksokhorontsi-ianukovycha>
11. Взаємодія ринку праці та професійно-технічної освіти. Механізми створення Державних стандартів професійно-технічної освіти з конкретних професій [Текст]: зб. матеріалів, підготов. у рамках реалізації укр.-нім. проекту "Підтримка реформи професійно-технічної освіти в Україні" / Блой В. [та ін.]; Укр.-нім. проект "Підтримка реформи професійно-технічної освіти в Україні". - К.: [б. в.], 2006. - 276 с.: портр. - Бібліогр.: с. 267-268
12. Відбулася Міжнародна наукова конференція «Цифрова дипломатія України: стратегічні комунікації, аналіз даних, кризове управління». Львівський національний університет імені Івана Франка.
URL: <https://lnu.edu.ua/vidbulasia-mizhnarodna-naukova-konferentsiia-tsyfrova-dyplomatiia-ukrainy-stratehichni-komunikatsii-analiz-danykh-kryzove-upravlinnia/>
13. Галіпчак В. ІНФОРМАЦІЙНА ВІЙНА ЯК СКЛАДОВА ГІБРИДНОЇ ВІЙНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ. Вісник Прикарпатського університету. Серія: Політологія. 2023. Т. 1, № 15. С. 26–32.
URL: <https://doi.org/10.32782/2312-1815/2024-1-4>
14. Герасимчук Т. Ф. Національна стійкість як детермінанта європейської інтеграції України / Таміла Федорівна Герасимчук // Політикус: наук. журнал. – 2022. – № 4. – С. 18–28.
15. Горбулін вважає виправданими відповіді на гібридну війну які. LB.ua.
URL: https://lb.ua/society/2017/06/24/369974_gorbulin_schitaet_opravdannimi.html

16. Генеральна Асамблея ООН засуджує незаконну анексію РФ українських територій. Ua.ambafrance.org. 21.01.2022. URL: <https://ua.ambafrance.org/General-na-Asambleya-OON-zasudzhuie-nezakonnu-aneksiiyu-RF-ukrayins-kih>.
17. Голодомор 1932-1933 років в Україні – геноцид Українського народу. Краснокутська селищна рада. URL: <https://krkut.gov.ua/archives/28295>
18. Горбулін В. П. Світова гібридна війна: український фронт / В. П. Горбулін, колективна монографія. — Київ: НАН України, 2017. — 312 с.
19. Dov Bachmann S., Putter D., Duczynski G. Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy. 2023. URL: <https://doi.org/10.1111/1758-5899.13257>
20. Дубов Д., Ожеван М. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців. 2012. Нац. ін-т стратег. дослідж. URL: https://niss.gov.ua/sites/default/files/2012-05/0529_dopov.pdf.
21. Denysiuk Z. Z. PROPAGANDA AND COUNTERPROPAGANDA IN THE CONTEXT OF STATE INFORMATION POLICY STRATEGIES. "Scientific Notes of Taurida V.I. Vernadsky University", series "Public Administration". 2021. No. 2. P. 46–51. URL: <https://doi.org/10.32838/tnu-2663-6468/2021.2/08>
22. Денисюк Ж. З. УКРАЇНСЬКА КУЛЬТУРНА ІДЕНТИЧНІСТЬ ЯК ОСНОВА НАЦІОНАЛЬНОЇ СТІЙКОСТІ ТА КУЛЬТУРНОЇ ПОЛІТИКИ. Culturological Almanac. 2025. № 1. С. 309–315. URL: <https://doi.org/10.31392/cult.alm.2025.1.35>
23. DDOS-атаки, що здійснювалися на українські банки, – ... Національна асоціація банків України. URL: <https://nabu.ua/ua/ddos-ataki-shcho-zdiysnyuvalisya-na-ukrayinski-banki-vidbito.html>
24. Державна політика України у сфері інформаційної безпеки. Міністерство закордонних справ України. URL: <https://mfa.gov.ua/state-policy-in-information-security>.

25. Данько Ю. А. СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ: ОСОБЛИВОСТІ ТА МЕХАНІЗМИ ПРОТИДІЇ. Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки. 2024. Т. 2, № 27. С. 54–66.
URL: <https://doi.org/10.34142/24130060.2023.27.2.05>
26. "Енергетика, банки, лікарні Європи щодня стають об'єктами російських кібератак", - віцепрезидентка ЄК Генна Віркунен. Новини України - останні новини України сьогодні - УНІАН.
URL: <https://www.unian.ua/economics/other/energetika-banki-likarni-yevropi-shchodnya-stayut-ob-yektami-rosiyskih-kiberatak-viceprezidentka-yek-genna-virkkunen-13161975.html>
27. Етнополітичні чинники консолідації сучасного українського суспільства / ред. кол. О. Рафальський (голова), В. Войналович, М. Рябчук. Київ: ІПіЕНД ім. І.Ф. Кураса НАН України. 2020. 336 с.
28. Етика медіа в умовах гібридної війни. Національна комісія зі стандартів журналістики. URL: <https://journalismstandards.gov.ua/ethics-hybrid-war>.
29. ЄВРОПЕЙСЬКІ ЗАСАДИ ВЗАЄМОВІДНОСИН УКРАЇНИ ТА НАТО ТА ВИВЧЕННЯ ДОСВІДУ НЕЙТРАЛІТЕТУ У ЗОВНІШНІХ ВІДНОСИНАХ ОКРЕМИХ ДЕРЖАВ. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.
URL: <https://military.bulletin.knu.ua/uk/article/view/7131/6216>
30. «Європейський центр з протидії гібридним загрозам (Hybrid CoE)». WARN.
URL: <https://warn-erasmus.eu/ua/glossary/evropejskij-czentr-z-protidii-gibridnim-zagrozm-hybrid-coe/>
31. Зайцев, В. В. Стратегічні комунікації ЄС в контексті безпекових викликів : кваліфікаційна бакалаврська робота : спец. 292 «Міжнародні економічні відносини» / наук. кер. М. О. Сухомлин; Центральнoукраїн. нац. техн.. ун-т. – Кропивницький: ЦНТУ, 2025. – 76 с.

32. Зозуля І. В. Глобальний, регіональний та національний виміри російсько-української війни. Форум права. 2023. Т. 74, № 1. С. 52–67.
URL: <https://doi.org/10.5281/zenodo.7016665>
33. Закон України «Про національну безпеку України» – № 2469-VIII від 21 червня 2018 р. // zakon.rada.gov.ua
34. Запустили платформу з навчання цифрової грамотності. Освіторія Медіа.
URL: <https://osvitoria.media/news/zapustily-platformu-z-navchannya-tsyfrovoyi-gramotnosti/>
35. Закон України “Про стратегічні комунікації: від 15.04.2023 № 4567.
URL: <https://zakon.rada.gov.ua/laws/show/4567>
36. Збірник матеріалів міжнародного круглого столу. 12 травня 2021 р., м. Київ / укладачі О.М. Шеремета, Н.А. Дубовик. – Київ: Державний університет телекомунікацій, 2021. – 82 с.
37. Історія Збройних Сил України (1991–2022). milhistory.zsu.gov.ua.
URL: <https://milhistory.zsu.gov.ua/reformuvannya-ta-rozvytok-ZSU/istoriya-zbroynykh-syl-ukrayiny-1991-2022>.
38. Інтеграція у європейську електромережу ENTSO Е. Міненерготем.
URL: <https://mev.gov.ua/reforma/intehratsiya-u-yevropeysku-elektromerezh-entso-e>.
39. Інформаційна агресія в сучасному світі: правовий аналіз та протидія: матеріали міжнародного науковопрактичного круглого столу. Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргарєєва та ін. – Харків : Майдан, 2024. – 242 с.
40. Криза сучасної системи міжнародної безпеки: переформатування геополітичного ландшафту. Матеріали міжнародної наукової конференції. Львів, 25 квітня 2025 р. / Упорядники: М. Мальський, Р. Вовк, О. Кучик. – Львів: Львівський національний університет імені Івана Франка, 2025. – 196 с.
41. Карпчук Н. П. Пропаганда в системі стратегічних комунікацій: методичні рекомендації вибіркової навчальної дисципліни підготовки магістра

спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОПП «Міжнародна інформація та суспільні комунікації» / Волинський національний університет імені Лесі Українки, кафедра міжнародних комунікацій та політичного аналізу. Луцьк, 2021. 10 с.

42. Комарчук О. МАНІПУЛЯТИВНІ ТЕХНОЛОГІЇ ЗАСОБІВ МАСОВОЇ КОМУНІКАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ДИСЕРТАЦІЯ. Миколаїв, 2019. 226 с. URL: [https://doi.org/324\(477\);659.4](https://doi.org/324(477);659.4).
43. Коруц У. З. МІЖНАРОДНІ МЕХАНІЗМИ ПРОТИДІЇ ПРОПАГАНДИ ВІЙНИ. Знання європейського права. 2020. № 2. С. 103–107. URL: <https://doi.org/10.32837/chern.v0i2.83>
44. Кібербезпека в інформаційному суспільстві: Інформаційно аналітичний дайджест. Інститут інформації, безпеки і права Національної академії правових наук України. URL: <https://ippi.org.ua/sites/default/files/2024-6.pdf>.
45. Кіберстійкість через обізнаність: як закон 4336 їх змінює – підходи до навчання у держсекторі. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/kiberstiikist-cherez-obiznanist-yak-zakon-4336-ikh-zminyuye-pidkhodi-do-navchannya-u-derzhsektorii>
46. Кампанії ЮНЕСКО з медіа- та інформаційної грамотності допомагають мільйонам українців розвивати навички критичного мислення. Україна. URL: <https://ukraine.un.org/uk/291548-кампанії-юнеско-з-медіа-та-інформаційної-грамотності-допомагають-мільйонам-українців>
47. Концепція «гібридної» війни та її складові - Центр безпекових досліджень "СЕНСС". Центр безпекових досліджень "СЕНСС". URL: <https://censs.org/concept-of-hybrid-warfare-and-its-components/>
48. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.

49. Концепція інформаційної безпеки держави. Секретаріат Ради національної безпеки і оборони України. URL: <https://www.rnbo.gov.ua/information-security-concept>.
50. Литвиненко О. Є. Загрози національній безпеці України у контексті гібридних конфліктів: монографія / О. Є. Литвиненко. — Київ: Нац. ін-т страт. досліджень, 2017. — 224 с.
51. Магда Є. В. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с.
52. Максимова К. С. Політологічна оцінка початкового етапу збройної агресії РФ проти України (2014–2022 рр.) : кваліфікаційна робота магістра. Суми, 2024. 300 с.
53. Metz, S. “Hybrid Warfare: A Critical Analysis.” In: Strategic Studies Institute & U.S. Army War College Press (eds.), Selected Papers on Hybrid Warfare. — Carlisle, PA: SSI Press, 2016. — 48–72 p.
54. McCuen, J. J. Hybrid Wars / John J. McCuen // Military Review. — 2008. — Vol. 88, No. 2. — P. 107–113.
55. Національна стратегія кібербезпеки України до 2027 року. Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/cybersecurity-strategy-2027>.
56. Німецький федеральний офіс з цивільного захисту та допомоги у надзвичайних ситуаціях. Кіберстійкість: рекомендації для державного сектору. URL: <https://www.bbk.bund.de/cyber-resilience>.
57. Національна стратегія протидії дезінформації. Уряд України. URL: <https://www.kmu.gov.ua/national-strategy-countering-disinformation>.
58. Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.) / редкол.: Л. М. Демидова (голов. ред.), Н. В. Шульженко, Д. О. Куковинець, О. С. Попович ; Нац. юрид. ун-т ім. Ярослава Мудрого ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України ; Громад.

- орг. «Всеукр. асоц. кримін. права». – Харків : Право, 2023. – 322 с. – DOI: <https://doi.org/10.31359/9789669985552>
59. Південна Україна на цивілізаційному пограниччі : [монографія] / Ярослава Верменич; [відп. ред. В. А. Смолій]; НАН України, Ін-т історії України, Від. іст. регіоналістики. – Київ: Ін-т історії України НАН України, 2015. – 481 с.
60. Проблематика, тенденції і перспективи розвитку воєнної науки та освіти в умовах сучасних глобальних викликів та конфліктів: збірник тез Міжнародного науково-практичного семінару / Центральний науково-дослідний інститут Збройних Сил України – К. : 7БЦ, 2024. – 408 с.
61. Прес-релізи та звіти - Геополітичні орієнтації жителів України: червень 2021 року. КМІС.
URL: <https://www.kiis.com.ua/?cat=reports&id=1054&lang=ukr&page=1>
62. Правдивець О. Науково-методичні підходи і практичні рекомендації з впровадження сучасних інноваційних технологій в управління економічною безпекою підприємств України в умовах війни / О. Правдивець // Вчені записки Університету "КРОК". - 2025. - № 1(77). - С. 265-272. - DOI <https://doi.org/10.31732/2663-2209-2025-77-265-272>
63. Панченко А. О. Гібридна війна та інформаційна безпека: сучасні підходи. Вісник Національної академії державного управління при Президентові України. 2023. № 2. С. 109.
64. Культура і мистецтво в умовах російсько-української війни: художні стратегії, дискурсивні практики, вектори осмислення: збірн. матер. Міжнародної наук.-практ. конф., м. Київ, 29—30.05.2024 / [упоряд. М. Полякова]; Інститут проблем сучасного мистецтва НАМ України, 2024. 166 с.
65. Promotion and protection of human rights in the context of digital technologies : resolution A/RES/78/213, adopted by the General Assembly. United Nations General Assembly. URL: <https://digitallibrary.un.org/record/4032837?v=pdf>.

66. Relationship between mir-126 expression in children with psoriasis, disease progression and therapeutic response / E. Murzina <https://orcid.org/0000-0002-3440-0745> et al. Journal of Medicine and Life. 2021. Vol. 14, no. 5. P. 667–675. URL: <https://doi.org/10.25122/jml-2021-0115>
67. «Роль і місце соціально-гуманітарних та правових дисциплін в системі підготовки військовослужбовців Національної гвардії України»: матеріали круглого столу (м. Київ, 30 жовтня 2023 р.). Київ: Київський інститут Національної гвардії України, 2023. 158 с.
68. Рішення Європейського суду з прав людини щодо Криму 2020 р. і щодо Донбасу 2023 р.: юридична кваліфікація незаконного контролю російської федерації щодо території України [Електронний ресурс] / Олексій Кресін // Право України. — 2023. — № 3. — С. 34-53.
69. РФ активізувала виробництво ШІ фейків про Сили оборони України. Центр протидії дезінформації. URL: <https://cpd.gov.ua/international-direction/ssha/rf-aktyvizovala-vyrobnyctvo-shi-fejkiv-pro-sily-oborony-ukrayiny/>
70. Ржеутська Л. Як вплине на Україну відмова від транзиту російського газу. dw.com. URL: <https://www.dw.com/uk/ak-vpline-na-ukrainu-vidmova-vid-tranzitu-rosijskogo-gazu/a-71204704>
71. Rid, T. Cyber War Will Not Take Place / Thomas Rid. — Oxford: Oxford University Press, 2013. — 256 p.
72. Серeda С. Ахметов, Порошенко, Медведчук: кого з олігархів Зеленський може позбавити впливу? Радіо Свобода. URL: <https://www.radiosvoboda.org/a/anonsovano-zakon-pro-oliharkhiv-khto-vtratyt-vplyv/31255206.html>
73. Світова гібридна війна: український фронт / За заг. ред. В. П. Горбуліна. Національний інститут стратегічних досліджень. — К.: НІСД, 2017. — 496 с.
74. Стратегія національної безпеки України. Міністерство оборони України. URL: <https://www.mil.gov.ua/strategiya-nacionalnoi-bezpeki-ukrainy>.
75. Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб'єктів господарювання в умовах трансформації публічного

- управління: Матеріали Міжнародної науково-практичної конференції (10 листопада 2023 року). — Одеса: Національний університет «Одеська політехніка», 2023. — 227 с.
76. Сунгуровський М. В. Політичні та соціальні механізми протидії гібридним загрозам / М. В. Сунгуровський // Вісник Нац. ун-ту оборони України. — 2019. — № 3. — С. 45–62.
77. Терещук Г. Військовослужбовці України та НАТО спільно «штурмували «населений пункт». Радіо Свобода. URL: <https://www.radiosvoboda.org/a/nato-navchannya-biytsi-viyna/31472291.html>
78. Тарасенко Ю. С. НІВЕЛЮВАННЯ ЕЛЕКТРОМАГНІТНОЇ ВРАЗЛИВОСТІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ. Systems and Technologies. 2023. Т. 65, № 1. С. 60–66. URL: <https://doi.org/10.32782/2521-6643-2023.1-65.8>
79. Творення нових соціальних порядків в умовах російсько-української війни: збірник матеріалів XIII Львівського соціологічного форуму (Львів, 5 квітня 2023 р.) / за ред. д. філос. н., професора, члена-кореспондента НАН України В. П. Мельника. — Львів: Львівський національний університет імені Івана Франка, 2023. — 336 с.
80. Україна та Німеччина у європейській спільноті: історія та сучасність [Текст]. Збірник статей з нагоди 30-ї річниці встановлення дипломатичних відносин між Україною та Німеччиною / С. М. Орехов [и др.]. - Київ : [б. в.], 2021. - 272 с. - (Наукова серія: Світові традиції державного управління. Вип. XI).
81. Ukrinform. Кремль затвердив «програму» масштабної русифікації тимчасово захоплених регіонів - розвідка. Укрінформ - актуальні новини України та світу. URL: <https://www.ukrinform.ua/rubric-ato/4064506-kreml-zatverdiv-programmu-masstabnoi-rusifikacii-timcasovo-zahoplenih-regioniv-rozvidka.html>

82. Ukrinform. Канада стане першою неєвропейською країною, яка долучиться до ініціативи SAFE. Укрінформ - актуальні новини України та світу. URL: <https://www.ukrinform.ua/rubric-world/4065216-kanada-stane-persou-neeuropejskou-krainou-aka-dolucitsa-do-iniciativi-safe.html>
83. Указ Президента України № 43/2021 «Про рішення Ради національної безпеки і оборони України від 2 лютого 2021 року “Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)”» // Офіційне інтернет представництво Президента України. - 2 лютого 2021. - URL: <https://www.president.gov.ua/documents/43-2021>
84. Указ Президента України № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”» // База даних «Законодавство України» / Верховна Рада України. - 14 вересня 2020. - URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>
85. Ukrinform. Як партнери допомагають Україні нести фінансовий тягар великої війни. Укрінформ - актуальні новини України та світу. URL: <https://www.ukrinform.ua/rubric-economy/3964100-ak-partneri-dopomagaut-ukrayini-nesti-finansovij-tagar-velikoi-vijni.html>
86. Freedom in the World 2013 - Ukraine. Freedom House. URL: <https://www.freedomhouse.org/report/freedom-world/2013/ukraine>
87. Khmel A. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). Acta de Historia & Politica: Saeculum XXI. 2022. № 03. С. 91–101. URL: <https://doi.org/10.26693/ahpsxxi2021-2022.03.091>
88. Hoffman, F. G. Conflict in the 21st Century: The Rise of Hybrid Wars / Frank G. Hoffman. — Arlington: Potomac Institute for Policy Studies, 2007. — 72 p.
89. Chyrko B. The Tragic Fate of Ethnic Germans and Mennonites of Ukraine during the Holodomor of 1932–1933, Assistance to the Starving from Foreign Charitable Organizations. Problems of World History. 2025. No. 29. P. 79 URL: <https://doi.org/10.46869/2707-6776-2025-29-4>

90. Чекаленко Л . Про поняття «гібридна війна» [Текст] / Людмила Чекаленко // Віче. - 2015. - № 5. - С. 41-42.
91. Шуляк Н. О. Інформаційна гігієна в системі стратегічних комунікацій України : дис. ... доктора філософії : 291 – Міжнародні відносини, суспільні комунікації та регіональні студії / Шуляк Назарій Олександрович. – Луцьк, 2024. – 263 с.
92. Шляхи досягнення миру на Донбасі: суспільні настрої, очікування, перестороги – загальнонаціональне опитування. Головна - Фонд «Демократичні ініціативи» ім. Ілька Кучеріва.
URL: <https://dif.org.ua/article/shlyakhi-dosyagnennya-miru-na-donbasi-suspilni-nastroi-ochikuvannya-perestorogi-zagalnonatsionalne-opituvannya>
93. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання та захисту прав і свобод людини і громадянина в Україні у 2024 році. Уповноважений Верховної Ради України з прав людини. URL: https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/Щорічна_доповідь_Уповноваженого_2024_році.pdf.
94. Yavir V. A. The Formation of Ethnonational Resilience under Conditions of the Russian-Ukrainian War. Politicus. 2022. No. 1. P. 201–205.
URL: <https://doi.org/10.24195/2414-9616.2022-1.32>
95. Як медіаграмотність допомагає протидіяти пропаганді. Радіо Свобода.
URL: <https://www.radiosvoboda.org/a/media-literacy-ukraine>.