

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ**

Кафедра політології та публічного управління

На правах рукопису

ЛУЦЬОК ОЛЕНА ОЛЕКСАНДРІВНА

ГІБРИДНІ ВІЙНИ ЯК ІНСТРУМЕНТ МІЖНАРОДНОЇ ПОЛІТИКИ

Спеціальність: 052 «Політологія»

Освітньо-професійна програма: «Політологія та державне управління»

Робота на здобуття освітнього ступеня
«Бакалавр»

Науковий керівник:
Пахолок Василь Миколайович,
кандидат політичних наук, доцент

РЕКОМЕНДОВАНО ДО ЗАХИСТУ

Протокол №

засідання кафедри політології та
публічного управління

від 2025 р.

Завідувач кафедри

проф. Бусленко В. В.

ЛУЦЬК–2025

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН	
1.1. Поняття та еволюція гібридних війн.....	6
1.2. Стан наукової розробки проблеми	12
РОЗДІЛ 2. ІНСТРУМЕНТИ ТА МЕХАНІЗМИ ГІБРИДНИХ ВІЙН	
2.1. Військові та парамілітарні засоби	15
2.2. Інформаційні операції та кібернапади	17
2.3. Економічні та торгівельні засоби боротьби	20
РОЗДІЛ 3. ЧИННИК ГІБРИДНИХ ВІЙН У СУЧАСНІЙ ГЕОПОЛІТИЦІ	
3.1. Безпекова політика міжнародних організацій (НАТО, ЄС) стосовно гібридних війн	23
3.2. Світові політичні зрушення як наслідки гібридних конфліктів.....	27
3.3. Зусилля світового співтовариства у протидії гібридним загрозам.....	31
ВИСНОВКИ	35
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	39

ВСТУП

Актуальність теми. У ХХІ столітті традиційні збройні зіткнення все частіше поступаються місцем гібридним загрозам, що включають дезінформацію, кібератаки, економічний тиск, диверсійні операції та використання проксі-акторів. Такі війни ускладнюють визначення агресора, а також унеможлиблюють ефективну реакцію з боку міжнародних організацій та держав.

Особливої значущості тема набуває у світлі російсько-української війни, яка демонструє широкий спектр гібридних загроз: від інформаційних маніпуляцій до створення реальних загроз всередині країни. Дослідження цього явища дозволяє зрозуміти механізми його функціонування, оцінити вплив на міжнародну безпеку та розробити ефективні стратегії протидії. У сучасному світі гібридні війни стають невід'ємною частиною зовнішньополітичної стратегії різних держав, що робить їх вивчення надзвичайно важливим для формування національної безпеки та міжнародної стабільності.

Наукова новизна. У роботі здійснюється спроба систематизувати підходи до визначення гібридної війни, розкрити її структурні елементи та механізми впливу на міжнародні відносини. Аналіз сучасних стратегій протидії та виявлення їх ефективності дозволяє запропонувати рекомендації щодо вдосконалення національної та міжнародної політики безпеки. Здійснено спробу поглибити розуміння трансформації сучасних конфліктів і розширити наукову основу для подальших політологічних досліджень інструментів гібридної війни.

Мета роботи – політологічний аналіз гібридних війн як інструменту міжнародної політики, зокрема їхніх характеристик та методів впливу на глобальну безпеку.

Для досягнення мети поставлено такі **завдання**:

- уточнити теоретичні підходи до визначення поняття «гібридна війна» та її відмінності від традиційних конфліктів;
- визначити основні складові гібридної війни;

- окреслити динаміку застосування гібридних методів тиску у міжнародній політиці;
- оцінити механізми регулювання гібридних війн у міжнародному праві;
- з'ясувати стратегії протидії гібридним загрозам на національному та міжнародному рівнях;
- розробити рекомендації щодо зміцнення інформаційної, кібернетичної та військової безпеки держави в умовах гібридних загроз.

Об'єктом дослідження є феномен гібридних війн у сучасних політичних відносинах.

Предметом дослідження є гібридні війни як інструмент міжнародної політики.

Джерельною базою дослідження є наукові праці, аналітичні звіти, документи міжнародних організацій, законодавчі акти, а також публікації експертів у сфері міжнародної безпеки та військової стратегії. Особливу увагу приділено дослідженню офіційних доповідей НАТО, ЄС, ООН щодо гібридних загроз. Додатково враховуються статті з авторитетних видань, що розкривають сучасні підходи до протидії гібридним війнам та оцінюють їхній вплив на міжнародну політику.

Практичне значення одержаних результатів. Практичне значення одержаних результатів дослідження полягає у потенційній можливості їх застосування для розробки стратегій протидії гібридним загрозам. Висновки та рекомендації можуть бути корисними для органів державної влади, військових структур, аналітичних центрів та експертів у сфері безпеки при формуванні політики інформаційного захисту, кібербезпеки та оборони.

Результати роботи також можуть бути використані в освітньому процесі під час викладання політологічних дисциплін пов'язаних з предметом дослідження. Дослідження сприяє кращому розумінню сучасних методів ведення гібридної війни та допомагає виробити ефективні механізми реагування на них.

Апробація результатів дослідження. Окремі положення дослідження було апробовано на практичних заняттях та семінарських обговореннях проблем дотичних до предмету бакалаврської роботи.

Структура бакалаврської роботи складається зі вступу, трьох розділів, структурованих на вісім підрозділів, висновків та списку використаних джерел.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН

1.1. Поняття та еволюція гібридних війн

Специфіка військових протистоянь, а також роль і значення військової сили в політиці закономірно залежать від рівня розвитку суспільства та наявних технологій. Ускладнення озброєнь та методів ведення бойових дій відбувається хвилеподібно й тісно пов'язане з еволюцією суспільних структур, змін у свідомості. В інформаційну епоху формуються нові типи протистоянь, які можуть не мати ані збройного, ані відкритого характеру. Питання аналізу розвитку форм і методів ведення збройної боротьби у сучасних і майбутніх конфліктах активно висвітлюється у наукових дослідженнях як в Україні, так і за кордоном. Це пов'язано як із динамічними змінами, які фахівці розглядають як появу воєн нового покоління, так і з необхідністю формування ефективної стратегії оборони держави [12, с. 2].

У сучасному розумінні, гібридна війна – це прагнення однієї держави нав'язати іншій (іншим) свою політичну волю шляхом комплексу заходів політичного, економічного, інформаційного характеру і без оголошення війни відповідно до норм міжнародного права [11, с. 4].

Прояви гібридних методів ведення війни можна знайти в різних періодах світової історії, хоча сам термін «гібридна війна» є відносно новим. Ще в античні часи держави використовували не лише військову силу, а й політичні інтриги, економічні блокади, пропаганду та диверсії для досягнення своїх цілей. Наприклад, під час Пелопоннеської війни (431–404 рр. до н.е.) між Афінами і Спартою окрім відкритих бойових дій застосовувались економічні санкції, інформаційні маніпуляції та залучення союзників до підривної діяльності.

У середньовіччі одним із проявів гібридної війни стали релігійні війни, під час яких поряд із воєнними кампаніями активно використовувалися

пропаганда, економічний тиск та дипломатичні інтриги. Наприклад, під час Реконквісти в Іспанії католицькі монархи не лише вели збройну боротьбу проти мусульман, але й використовували релігійний фанатизм як засіб мобілізації населення, водночас здійснюючи економічний тиск на мусульманські громади.

Термін «гібридна війна» вперше застосовано генералом Джеймсом Н. Меттісом у вересні 2005 року під час оборонної конференції, організованої Інститутом ВМС США та Асоціацією Корпусу морської піхоти. Згодом матеріали цієї конференції були опубліковані спільно з Ф. Гоффманом у листопаді 2005 року в статті під назвою «Майбутня війна: зліт гібридних воєн» [23, с. 173].

Гібридна війна суттєво відрізняється від традиційних та асиметричних конфліктів за методами ведення, цілями та засобами досягнення результату. Традиційна війна передбачає відкриті збройні зіткнення регулярних армій із чітким поділом на фронт і тил, а також офіційно оголошене військове протистояння між державами. У таких конфліктах військові дії є основним інструментом досягнення політичних чи територіальних цілей, а перемога залежить від переваги у силі, ресурсах і тактиці.

Асиметричні конфлікти, своєю чергою, характеризуються боротьбою між нерівними за силою сторонами, де слабша сторона використовує партизанську тактику, диверсії, тероризм та інформаційну війну для компенсації військової переваги супротивника. Війни в Іраку, Афганістані, а також війна в Україні демонструють явище, коли навіть високорозвинені країни, оснащені сучасною та потужною зброєю, можуть виявитися вразливими. У таких конфліктах військової могутності недостатньо для гарантування належного рівня безпеки та ефективної нейтралізації противника [14, с. 41].

Гібридна війна поєднує елементи традиційного та асиметричного протистояння, використовуючи широкий спектр методів, що охоплюють не лише військові дії, але й політичні, економічні, інформаційні та кібернетичні атаки. Головною відмінністю є її комплексний і прихований характер, коли агресор уникає прямого військового вторгнення, натомість застосовуючи

дестабілізаційні методи, які ускладнюють ідентифікацію та відповідь на агресію. Прикладом є російсько-українська війна, де поряд із військовими діями Росія активно використовує пропаганду, диверсії, економічний тиск і кібератаки для досягнення своїх цілей.

Основними характеристиками гібридної війни є розмиття меж між війною та миром, активне використання інформаційних технологій для дезінформації та маніпуляції суспільною свідомістю, залучення нерегулярних збройних формувань, підбивна діяльність усередині держави-жертви, а також економічний тиск і кібернетичні атаки. Такий підхід ускладнює ідентифікацію агресора, що робить ефективну міжнародну відповідь проблематичною.

Гібридні війни стали особливо актуальними в XXI столітті, коли технологічний розвиток та глобалізація створили нові можливості для ведення конфліктів.

Термін «гібридна війна» не є суто військовим поняттям. У військовій теорії традиційно використовують низку специфічних критеріїв для типології воєнних конфліктів, що дозволяють врахувати всі їхні основні аспекти. Серед таких критеріїв – масштаб охоплення, сфера дії, типи сторін-учасників, їхній соціально-політичний устрій, характер відносин між сторонами, ступінь організованості та рівень ескалації.

Залежно від форм прояву, визначених способами застосування військової сили, конфлікти поділяють на приховані (латентні) та відкриті. Різноманіття форм воєнних конфліктів часто виникає завдяки комбінації трьох моделей: формальної, неформальної та війни сірої зони.

- Формальна війна – це зіткнення збройних сил двох держав, яке супроводжується офіційним оголошенням війни.
- Неформальна війна передбачає участь принаймні однієї недержавної сторони.
- Сіра зона виникла після завершення Холодної війни й характеризується поєднанням збройного протистояння та організованої злочинності (як приклад – конфлікт у Республіці Ічкерія).

Формальні війни бувають традиційними та нетрадиційними. У традиційних війнах регулярні збройні сили однієї держави протистоять регулярним або нерегулярним (партизанським) силам іншої з використанням звичайних засобів боротьби. Такі війни передбачають безпосередній контакт сторін. Розвиток технологій і нових засобів ведення бою привів до появи сучасних форм – мережевих і мережоцентричних воєн [5, с. 18–22].

Гібридна війна включає набір взаємопов'язаних компонентів, які забезпечують одночасний багатовекторний вплив на противника. Основними складовими цього явища є інформаційний, ідеологічний, психологічний, економічний, політичний, дипломатичний, військовий, технологічний, ресурсний та енергетичний аспекти. Одним із ключових елементів гібридних воєн є економічний чинник, який набув особливої ваги після переходу від національних господарств до глобальної економічної системи з міжнародним поділом праці та розширенням світової торгівлі. Історія демонструє широкий спектр методів економічного протистояння, які застосовувалися в рамках гібридних конфліктів. Для України особливо значущим є енергетичний вимір гібридної війни. Використання енергоресурсів як інструменту політичного тиску безпосередньо впливає на міжнародний баланс сил. Зі зростанням технологічних можливостей і посиленням економічних взаємозв'язків з'являються нові форми ресурсного протиборства, зокрема транспортні, енергетичні та водні блокади, які можуть спричиняти екологічні катастрофи та навіть екоцид цілих регіонів. Ще однією важливою сферою гібридних операцій є культура. Культурно-цивілізаційні цінності та соціальна чутливість населення стають об'єктами маніпуляцій, де форма подачі інформації має пріоритет над її змістом. Це дозволяє агресору нав'язувати спотворене світосприйняття, використовуючи змінювані образи та перекручення фактів для досягнення своїх стратегічних цілей [8].

Сучасні «гібридні війни» вже не обмежуються традиційним тривимірним простором (суходіл, море, повітря), а виходять у четвертий вимір – свідомість і психіку воюючих сторін. Ба більше, такі війни зазвичай починаються раптово,

що значно ускладнює підготовку до них. Військовим дедалі важче адаптуватися до нових загроз, адже класичні моделі ведення війни стають менш ефективними, а час грає на користь агресора. Хоча фундаментальні знання традиційних воєн залишаються важливими, сьогодні вони вже не є достатніми для ефективної протидії. Успішна боротьба вимагає комплексної інформаційної стратегії, яка має впроваджуватися на різних рівнях [9, с.53].

У XXI столітті гібридні війни набули нових форм та інтенсивності, що зумовлено розвитком технологій, цифровізації та глобалізації. На відміну від традиційних війн минулого, сучасні гібридні конфлікти ведуться не лише на полі бою, а й у кіберпросторі, інформаційному середовищі та економічній сфері. Вони часто залишаються прихованими, що ускладнює ідентифікацію агресора та вироблення ефективної відповіді.

Одним із ключових аспектів сучасних гібридних війн є масове використання дезінформації, маніпуляцій у соціальних мережах та кібератак, що дозволяють впливати на політичні процеси та суспільну свідомість. Технології штучного інтелекту, алгоритми персоналізованого контенту та соціальні платформи створили безпрецедентні можливості для поширення фейкових новин і пропаганди, що руйнують довіру до урядів та демократичних інститутів.

Важливу роль відіграє й економічний тиск: санкції, маніпуляції з енергоресурсами, блокади та фінансові махінації стали частиною гібридних стратегій. Кібератаки на критичну інфраструктуру, банківські системи та державні установи можуть паралізувати цілу країну без жодного пострілу.

Російська агресія проти України є яскравим прикладом сучасної гібридної війни, яка поєднує класичні військові дії з інформаційною війною, диверсіями, кібератаками та економічним шантажем. Війна на Донбасі та повномасштабне вторгнення 2022 року демонструють, як агресор використовує всі доступні інструменти – від пропаганди та фейкових наративів до руйнування критичної інфраструктури та енергетичних систем.

Сучасний етап розвитку гібридних війн також включає активне використання проксі-акторів, тобто нерегулярних військових формувань, найманців і терористичних груп, що діють в інтересах великих держав без офіційного оголошення війни. Це дозволяє агресору уникати прямої відповідальності та маніпулювати міжнародним правом.

З огляду на ці тенденції, XXI століття стало епохою невидимих воєн, де боротьба точиться не лише на полі бою, а й у медіа, економіці, кіберпросторі та свідомості людей. Успішна протидія таким загрозам вимагає нових підходів до безпеки, інтеграції технологій у військову стратегію та посилення інформаційної стійкості суспільства.

Український інформаційний сектор має низку слабких місць у боротьбі з інформаційною агресією, що ускладнює ефективну протидію російським впливовим операціям. Для оцінки дієвості механізмів, які Україна використовує в інформаційному просторі, необхідно детально проаналізувати ці проблеми. На думку українського дослідника І. Лубковича, основні недоліки можна поділити на кілька категорій. По-перше, це неефективність реагування як на конкретні випадки дезінформації, так і на подання власної об'єктивної інформації щодо подій та явищ. По-друге, проблема сили та обізнаності: сила визначає наявність засобів ведення інформаційної війни, тоді як обізнаність – рівень ефективного їх застосування. По-третє, існує недостатність якісного інформаційного забезпечення з боку державних органів, що створює прогалини в інформаційній політиці. Окремим викликом є фінансовий аспект. Значна частина українських медіа, зважаючи на економічні труднощі, не відмовляється від трансляції російських телесеріалів, фільмів і телепередач, оскільки це приносить прибуток. Небажання втрачати фінансові надходження створює додаткові ризики в інформаційному просторі, сприяючи подальшому поширенню російських наративів [10, с. 182–187].

Гібридні методи активно застосовуються і на Близькому Сході. Наприклад, війна в Сирії включала не лише традиційні бойові дії, а й інформаційні кампанії, пропаганду, підтримку терористичних угруповань

різними державами, а також використання приватних військових компаній. Росія, Іран, США та Туреччина активно впливали на перебіг конфлікту через проксі-угруповання, що ускладнило ситуацію та зробило війну багатовимірною.

У Латинській Америці гібридні війни проявляються через економічний тиск, підтримку антиурядових рухів та інформаційні операції. Наприклад, у Венесуелі політична боротьба між владою та опозицією супроводжується зовнішнім втручанням, санкціями, енергетичними обмеженнями та інформаційними маніпуляціями, які впливають на суспільну думку як у країні, так і за її межами.

Гібридні конфлікти в Азії також мають свої особливості. Китай використовує інформаційні та економічні важелі для впливу на Тайвань, Південно-Східну Азію та Західні країни. Наприклад, кібератаки на іноземні урядові установи, економічний шантаж, розширення впливу через проєкт «Один пояс – один шлях», який теж є частиною стратегії Китаю зміцнення своєї геополітичної позиції.

Отже, дослідження самого поняття та еволюції форм гібридних війн показало, що цей феномен є невід'ємною частиною сучасних міжнародних політичних конфліктів, де мають місце поєднання традиційних військових дії з інформаційними, економічними, кібератаками та іншими асиметричними методами впливу. На відміну від класичних війн, гібридні війни спрямовані не лише на фізичне знищення противника, а й на підірив його політичної стабільності, економічної спроможності та суспільної єдності.

1.2. Стан наукової розробки проблеми

Західна наукова література активно досліджує проблему гібридних воєн, розглядаючи їх як ключовий виклик сучасній міжнародній безпеці. Концепція гібридної війни стала предметом глибокого аналізу після подій 2014 року, коли Росія застосувала комплексний набір гібридних методів у своїй агресії проти України. Втім, окремі елементи цього явища досліджувалися ще раніше в

контексті асиметричних конфліктів, інформаційних операцій та нетрадиційних воєнних стратегій.

Американський військовий аналітик і політолог Френк Хофман (Frank Hoffman) вперше запропонував поняття «гібридна війна». На його думку, це концепція, яка стосується військової стратегії. Його роботи стали основою для подальшого аналізу в НАТО та оборонних структурах західних держав[28].

Західні вчені, такі як Марк Галеотті, активно вивчають стратегію Кремля, що поєднує інформаційну війну, економічний тиск, військову агресію та політичні маніпуляції [26].

Також важливим напрямом досліджень є роль НАТО у протидії гібридним загрозам. У працях аналітиків Альянсу підкреслюється необхідність адаптації традиційних оборонних стратегій до нових викликів, зокрема через зміцнення інформаційної безпеки, розвиток кіберзахисту та посилення розвідки.

Одним із перших поняття «гібридна війна» у наукових дослідженнях почав використовувати американський вчений М. Маклюен, аналізуючи роль інформації у сучасному світі. Над вивченням цього феномену працювали такі науковці, як М. Айшервуд, Є. Магда [11. 12], В. Власюк, І. Тодоров, Г. Динис та І. Рущенко. Іноземні дослідники, зокрема Д. Ласіка, М. Маклюен і Ф. Хофман, акцентували увагу на відмінностях гібридних воєн від класичних, досліджуючи стратегії й тактичні підходи до їх ведення. М. Сенченко, О. Їжак та Г. Яворська[25] розглядали гібридну війну як комплексне явище, а А. Котенко зосередився на її організаційній структурі. С. Полумієнко провів детальний аналіз стратегій цього виду насильства та їх взаємозв'язків. У роботі Джеймса Візера «Осмищення гібридної війни» наголошується на залежності аналізу поняття від контексту його застосування. О.А. Сищук детально дослідив інформаційно-психологічний аспект гібридної війни [22, с. 6].

Одним із фундаментальних досліджень є монографія «Світова гібридна війна: український фронт» Володимира Міська, видана Національним інститутом стратегічних досліджень у 2017 році. У цій праці гібридна війна

розглядається як новітній вид глобального протистояння, що поєднує військові, політичні, економічні, соціальні, гуманітарні та інформаційні виміри. Монографія аналізує причини та передумови російської агресії проти України, її стратегічні цілі, а також особливості ведення гібридної війни у різних вимірах [31].

Також варто відзначити статтю М. М. Тараненка «Гібридна війна в Україні: історія та сучасність», де автор аналізує основні методи і форми гібридної війни в Криму і на Сході України, а також порівнює ці події з гібридними війнами в інших країнах, таких як Хорватія, Боснія і Герцеговина [32].

У статті «Гібридна війна: сутність, складові та ключові поняття» автори аналізують гібридну війну як сукупність заздалегідь підготовлених і оперативно реалізованих дій військового, дипломатичного, економічного та інформаційного характеру, спрямованих на досягнення стратегічних цілей. Вони також визначають основні ознаки, компоненти та особливості гібридної війни, включаючи використання різноманітних комбінацій військових і невійськових засобів тиску на країну-жертву [23].

Загалом, українські науковці активно досліджують гібридну війну, розглядаючи її як складне та багатовимірне явище, що вимагає міждисциплінарного підходу та глибокого аналізу для розробки ефективних стратегій протидії.

Отже, наукові підходи до вивчення гібридних війн перебувають у стані постійного розвитку, що відображає їхню актуальність та складність у сучасному міжнародному середовищі. Подальші дослідження вимагають міждисциплінарного підходу, який враховуватиме не лише військовий аспект, а й політичні, економічні та інформаційні виміри цього явища.

РОЗДІЛ 2

ІНСТРУМЕНТИ ТА МЕХАНІЗМИ ГІБРИДНИХ ВІЙН

2.1. Військові та парамілітарні засоби

Використання регулярних збройних сил у гібридних війнах під прикриттям «невизнаних» операцій є однією з ключових тактик сучасних конфліктів. Держави-агресори застосовують цей метод для досягнення військових і політичних цілей, уникаючи при цьому офіційного визнання участі у війні. Це дозволяє їм діяти у «сірій зоні» міжнародного права, заперечувати свою причетність і маніпулювати громадською думкою.

Основним підходом до такої тактики є введення військових підрозділів без розпізнавальних знаків, що дозволяє державі приховувати офіційну участь у бойових діях. Ці сили можуть діяти під виглядом «місцевого ополчення», «повстанських рухів» або «громадських активістів», створюючи ілюзію внутрішнього конфлікту в країні-мішені. Прикладом такого підходу стала анексія Криму у 2014 році, коли російські військові підрозділи діяли без офіційної символіки, а їхню присутність заперечувала російська влада.

Сучасні війни експерти розглядають як окремий прояв ширшого поняття – «збройний конфлікт» (armed conflict), який обов'язково включає два ключові елементи: існування організованих озброєних формувань і ведення бойових дій певного рівня інтенсивності. З цього визначення випливає, що війна насамперед є фізичним та матеріальним явищем, що охоплює використання зброї – танків, літаків, ракет, військових кораблів – та її застосування для завдання ударів, проведення оборонних операцій і знищення стратегічних об'єктів. Людські втрати, загибель як військових, так і цивільного населення в ході бойових дій, також належать до цього виміру. Втрата людського життя є незворотною, і саме у фізичному аспекті війна завдає найбільш фатальних наслідків [25, с. 42].

Ще одним способом застосування регулярних військ у «невизнаних» операціях є використання їх у складі приватних військових компаній (ПВК). Держава фінансує та контролює такі структури, але юридично не несе

відповідальності за їхні дії. Це дозволяє здійснювати військові операції за межами власної території без прямої конфронтації з міжнародним співтовариством.

Важливу роль у таких операціях відіграють спеціальні сили та розвідувальні підрозділи, які проводять диверсійні акції, інформаційні атаки та операції з дестабілізації ситуації в цільовій державі. Такі дії можуть включати підготовку місцевих бойових груп, організацію провокацій та контроль над інформаційним простором.

Застосування цієї тактики суттєво ускладнює реагування міжнародної спільноти, оскільки офіційне визнання збройної агресії потребує наявності чітких доказів.

Маніпуляція миротворчими силами та використання приватних військових компаній (ПВК) є поширеними інструментами у сучасних гібридних конфліктах, що дозволяють державам досягати стратегічних цілей без відкритого воєнного втручання. Використання миротворчих місій у політичних або військових інтересах може спотворювати їхню початкову мету – забезпечення стабільності та захист цивільного населення. Деякі країни використовують міжнародні миротворчі механізми для затягування конфліктів, легітимізації окупаційних дій або контролю над стратегічно важливими територіями.

Приватні військові компанії (ПВК) та охоронні фірми є комерційними підприємствами, що надають спеціалізовані консультаційні та інші послуги, пов'язані з діяльністю в умовах збройних конфліктів або воєнних операцій. Більшість компаній, що зосереджені на забезпеченні безпеки персоналу та уникають безпосередньої участі в бойових діях, позиціонують себе як приватні охоронні структури [20, с. 231].

Найманці, які діють у складі ПВК, часто виконують бойові завдання, розвідку, охороняють стратегічні об'єкти або навчають місцеві збройні формування. Завдяки юридичним «сірим зонам» такі компанії можуть

здійснювати військові дії, уникаючи міжнародних санкцій та дипломатичних ускладнень.

Крім того, використання ПВК дозволяє зменшити політичні ризики, адже втрати серед їхніх бійців не враховуються у державній статистиці загиблих військових, що мінімізує суспільне невдоволення війною. Приватні військові компанії часто діють у зонах конфліктів, де офіційні армії не можуть або не хочуть бути присутніми, виконуючи завдання держав чи корпоративних інтересів.

Отже, маніпуляція миротворчими силами та активне залучення ПВК є потужними інструментами сучасної військової стратегії, що дозволяють контролювати ситуацію в регіонах конфліктів, впливати на їхній розвиток і уникати юридичної та політичної відповідальності за проведення збройних операцій. З огляду на постійні зміни у світі та трансформацію характеру воєн, у сучасних війнах четвертого покоління приватизація військових функцій стає неминучою. Гібридні війни та збройні конфлікти сприятимуть зростанню попиту на військові послуги, що зумовить активний розвиток приватних військових компаній та інших недержавних військових структур [20, с. 231].

2.2. Інформаційні операції та кібернапади

Кіберзагрози та електронна війна також стали невід'ємною частиною сучасної військової стратегії, оскільки цифрові технології відіграють критично важливу роль у функціонуванні державних структур, економіки, оборони та інформаційного простору.

До основних типів кіберзагроз належать кіберзлочинність, кібертероризм, кібершпигунство та кібервійна. Важливим завданням є розробка інформаційного кодексу, що об'єднає всі норми інформаційного права в єдину правову систему. Ефективна протидія кіберзагрозам можлива лише за умови спільних зусиль державних органів, громадянського суспільства та міжнародних партнерів. Необхідно закріпити поняття кібервійни в міжнародному праві, а також визначити кібершпигунство як злочин на

глобальному рівні. Це дозволить уніфікувати чинні правові норми та забезпечити їхню ефективну імплементацію в міжнародній практиці. Україна потребує подальшого зміцнення системи кібербезпеки, оскільки кіберзлочинці часто випереджають існуючі механізми захисту, які використовуються державними органами. Забезпечення високого рівня кібербезпеки є ключовою умовою стабільного функціонування цифрових мереж та інформаційних систем. Кібервійна головним чином спрямована на підлив роботи комп'ютерних систем і доступу до Інтернету, що використовуються державними установами, фінансовими та бізнес-центрами. Вона має на меті створення хаосу та дестабілізацію суспільного життя в країнах, де цифрові технології є невід'ємною частиною повсякденного функціонування. За допомогою кібератак можливо спрямовувати, змінювати або блокувати потік інформації, впливаючи на суспільну думку, рішення державних посадовців і дії військових структур. Наразі Міністерство оборони України працює над офіційним визначенням поняття «кібервійна» у правовому полі [13, с. 602].

На думку дослідників, кібертероризм сьогодні становить серйозну загрозу для всієї міжнародної спільноти. Це небезпечне явище поєднує в собі два ключові аспекти — кіберзлочинність і тероризм, що робить проблему інформаційних загроз у кіберпросторі наднаціональною. Визнанням цього факту стала декларація, ухвалена на саміті НАТО в Уельсі у 2014 році (п.п. 72-73), де зазначалося, що кібератаки можуть досягати рівня загрози євроатлантичній безпеці, стабільності та добробуту. Водночас рішення щодо застосування статті 5 у відповідь на кібератаки ухвалюватиметься Північноатлантичною радою у кожному конкретному випадку окремо [30].

Електронна війна охоплює радіоелектронну боротьбу, що передбачає глушіння сигналів супутникового зв'язку, перехоплення військових комунікацій і вплив на системи навігації. Використання технологій радіоелектронної боротьби дозволяє не лише ускладнювати управління військами противника, а й дезорієнтувати його сили на полі бою, що дає значну тактичну перевагу.

Застосування кіберзасобів у військових стратегіях має ще одну важливу мету – інформаційні операції. Через хакерські атаки можна поширювати дезінформацію, маніпулювати громадською думкою та впливати на виборчі процеси, що фактично робить кіберпростір новим театром військових дій.

Кібернапади є ще одним ефективним інструментом гібридної війни, який дозволяє завдати шкоди без фізичного вторгнення. Вони можуть бути спрямовані на державні установи, критичну інфраструктуру, фінансову систему та військові об'єкти. Використовуючи методи хакерських атак, такі як злам баз даних, розповсюдження шкідливого програмного забезпечення або DDoS-атаки, противник може паралізувати роботу ключових систем держави, спричинити економічні збитки та посилити паніку серед населення.

Комбінація інформаційних операцій і кібернападів дає змогу агресору досягати значних стратегічних переваг, не вдаючись до традиційних воєнних дій. Такі атаки важко швидко ідентифікувати та нейтралізувати, що робить їх особливо небезпечними. У відповідь держави змушені розвивати системи кіберзахисту, посилювати контроль за інформаційним простором та зміцнювати стійкість суспільства до маніпуляцій і деструктивного впливу.

Вторгнення Російської Федерації в Україну у 2022 році не стало початком кібератак з її боку, але значно посилило їхню інтенсивність та масштаби, перетворившись на каталізатор для розгортання нової хвилі кіберзлочинів. Щоденно здійснюються атаки різного рівня складності, спрямовані на дестабілізацію ситуації та завдання шкоди критично важливій інфраструктурі. Один із ключових напрямів такої діяльності – підтримка ведення бойових дій через цілеспрямовані кібератаки на державні та регіональні об'єкти, зокрема банки, енергетичні компанії, засоби масової інформації та сервери великих корпорацій. Злам і виведення з ладу цих систем може спричинити масштабні перебої в роботі життєво важливих секторів економіки та зв'язку. Крім того, кібератаки є невід'ємною складовою гібридної війни, що дозволяє Росії впливати на цільові країни без розгортання відкритого збройного конфлікту із Заходом, Європейським Союзом чи НАТО. У поєднанні з інформаційними

кампаніями та політичним тиском вони створюють умови для маніпуляції суспільною думкою, послаблення урядів та розколу в демократичних державах. Важливо зазначити, що кібервійна не обмежується лише періодами активних бойових дій – вона ведеться постійно, навіть у мирний час, що робить її одним із головних інструментів сучасної війни [18].

Тому, важливо зауважити, що кіберзагрози та електронна війна відіграють ключову роль у сучасних конфліктах, доповнюючи традиційні військові методи й забезпечуючи агресору можливість впливати на противника без відкритого воєнного втручання. Держави, які не мають належного рівня кібербезпеки та електронного захисту, стають особливо вразливими до атак, що може мати катастрофічні наслідки для їхньої обороноздатності та національної безпеки.

2.3. Економічні та торговельні засоби боротьби

Економічні та торговельні важелі відіграють ключову роль у сучасних воєнних конфліктах, доповнюючи традиційні військові методи та створюючи потужний інструмент тиску на противника. В умовах гібридної війни, коли збройні дії часто супроводжуються непрямими формами боротьби, економічні санкції, фінансові обмеження та торговельні бар'єри стають ефективними засобами ослаблення держави-агресора. Застосування економічних інструментів створює вагомі стимули для деескалації конфлікту та його попередження. У деяких випадках економічні санкції стають чи не єдиним доступним механізмом реагування як з боку міжнародної спільноти, так і окремих держав на акти агресії, особливо коли вони набувають гібридного характеру [1, с. 3].

Санкційна політика дозволяє впливати на країну-опонента, обмежуючи її доступ до світових фінансових ринків, технологій та критично важливих ресурсів. Це може значно ускладнити функціонування її економіки, знизити здатність фінансувати військові кампанії та викликати внутрішнє незадоволення населення. Наприклад, після початку війни в Україні у 2022 році

західні країни застосували масштабні санкції проти Росії, що обмежило її торгівлю, фінансові операції та технологічний розвиток.

У межах гібридної війни активно застосовувалися як тарифні, так і нетарифні методи регулювання торговельних відносин з обох сторін. Збільшення зовнішньоторговельного сальдо між Україною та Росією у 2017 році засвідчило труднощі, з якими зіткнулися окремі українські галузі під час переорієнтації своєї продукції на ринки Європи, Азії та Африки. Попри введення торговельних бар'єрів і підвищення митних ставок, економічні зв'язки між країнами зберігали певну сталість. Водночас боротьба України з торговельним тиском з боку РФ не повинна обмежуватися лише застосуванням дзеркальних санкцій. У ситуації зменшення прибутковості та зростаючої непередбачуваності російського ринку необхідно поступово позбуватися економічної залежності від нього, використовуючи весь спектр доступних інструментів макроекономічної та зовнішньоторговельної політики, економічної дипломатії та міжнародного торговельного права [19, с. 73].

Торговельні обмеження також використовуються як інструмент стратегічного впливу. Блокування експорту чи імпорту певних товарів може створити дефіцит на ринку, підірвати виробничі процеси та посилити економічну нестабільність. Особливо значущими є енергетичні санкції, адже контроль над поставками нафти, газу та інших ресурсів може стати критичним важелем у геополітичній боротьбі. Російське використання енергоресурсів як засобу впливу на Європу та, у відповідь, спроби ЄС диверсифікувати постачання енергоносіїв є яскравим прикладом цієї тактики.

Крім санкцій та торговельних обмежень, важливу роль відіграють маніпуляції фінансовими ринками та інвестиціями. Обмеження доступу країни-агресора до міжнародних кредитів та фінансових операцій може уповільнити її економічне зростання та зменшити можливості фінансування військових програм. Також використовуються механізми замороження активів політичних еліт та стратегічних компаній, що посилює економічний тиск і створює додаткові важелі впливу.

Таким чином, економічні та торговельні важелі стають невід’ємною частиною сучасних воєнних конфліктів, дозволяючи досягати стратегічних цілей без прямого збройного зіткнення. Їхнє застосування може суттєво послабити противника, вплинути на політичні рішення та змінити динаміку війни, що робить їх важливим елементом сучасної безпекової політики.

РОЗДІЛ 3

ЧИННИК ГІБРИДНИХ ВІЙН У СУЧАСНІЙ ГЕОПОЛІТИЦІ

3.1. Безпекова політика міжнародних організацій (НАТО, ЄС) стосовно гібридних війн

Гібридні війни суттєво змінюють сучасну систему міжнародної безпеки, розмиваючи межі між миром і війною, державними та недержавними акторами, військовими та невійськовими засобами впливу. На відміну від традиційних збройних конфліктів, гібридні загрози включають кібератаки, інформаційні маніпуляції, економічний тиск, саботаж і використання нерегулярних збройних формувань, що ускладнює їх ідентифікацію та стримування.

Одним із головних наслідків поширення гібридних війн є підриг колективної безпеки, оскільки вони спрямовані не лише на військове протистояння, а й на дестабілізацію суспільств, ослаблення державних інституцій та розкол міжнародних союзів. Це створює серйозні виклики для міжнародних організацій, таких як НАТО та ЄС, які змушені адаптувати свої підходи до безпеки та розробляти нові стратегії протидії прихованим загрозам.

Епоха, коли кризи та конфлікти мали чітко визначених учасників, залишилася в минулому. Натомість сучасні гібридні загрози, що поєднують військові та цивільні інструменти, створюють значну невизначеність, ускладнюючи контроль над ситуацією. Дослідники, аналізуючи виклики та перспективи для НАТО, звертають увагу на те, що гібридний характер сучасних загроз робить процес ухвалення рішень в Альянсі більш складним, а інколи й суттєво його сповільнює. З огляду на це, боротьба з гібридними загрозами стала пріоритетним завданням для НАТО, і починаючи з 2015 року, держави-члени систематично розширювали інструменти для реагування на такі виклики. Важливим кроком у цьому напрямку стало створення в 2017 році Об'єднаного управління розвідки та безпеки, у межах якого діє спеціальний відділ з моніторингу та аналізу гібридних загроз. Це сприяє покращенню здатності НАТО формувати цілісне розуміння ситуації, що є критично важливим у

сучасних умовах безпеки. Враховуючи зростаючу роль інформації, розвідувальні дані стають не менш цінним ресурсом, ніж військова техніка, включаючи танки, безпілотники та ракетні системи [4, с. 30].

НАТО вибудовує багаторівневу систему співпраці у сфері протидії гібридним загрозам, поєднуючи військову, кібернетичну та інформаційну безпеку. Такий підхід дозволяє зміцнювати стійкість як країн-членів, так і партнерів, а також забезпечувати ефективну відповідь на сучасні виклики у сфері безпеки. Оскільки гібридні загрози поєднують військові, інформаційні, економічні та кібернетичні методи, координація зусиль і обмін розвідувальними даними стають важливими елементами безпекової політики.

У рамках співпраці між державами-членами НАТО проводяться регулярні навчання, зокрема серія тренувань «Locked Shields» та «Cyber Coalition», які моделюють сценарії гібридних атак, включаючи кібератаки на критичну інфраструктуру, кампанії з дезінформації та втручання у виборчі процеси. Країни-члени також тісно співпрацюють у межах Центру передового досвіду з кібероборони в Таллінні, де розробляються нові стратегії протидії кіберзагрозам [17].

Важливу роль відіграє взаємодія НАТО з Європейським Союзом, оскільки багато викликів у сфері гібридної війни впливають як на країни НАТО, так і на держави-члени ЄС. Спільні ініціативи включають посилення захисту критичної інфраструктури, боротьбу з дезінформацією та створення механізмів швидкого реагування на гібридні атаки.

Окрім країн-членів, НАТО активно співпрацює з партнерами, такими як Україна, Грузія та Швеція, які мають значний досвід у протидії гібридним загрозам. Для цього були створені програми, що передбачають посилення кібербезпеки, обмін розвідувальною інформацією та консультації щодо реформ сектору безпеки. Наприклад, Україна є одним із ключових партнерів НАТО у сфері кіберзахисту, отримуючи технічну та експертну підтримку для зміцнення національних оборонних спроможностей.

Співпраця в межах Альянсу також включає посилення стратегічних комунікацій, що допомагає країнам-членам та партнерам ефективно реагувати на інформаційні атаки та пропаганду. Важливим кроком у цьому напрямі стало створення Центру передового досвіду з питань стратегічних комунікацій у Латвії, який займається виявленням дезінформаційних кампаній та розробкою методів їхнього нейтралізації.

Спільна політика безпеки та оборони Європейського Союзу відіграє ключову роль у забезпеченні стабільності та реагуванні на сучасні виклики. Гібридні загрози стали одним із пріоритетних напрямів цієї політики, оскільки вони поєднують військові, інформаційні, кібернетичні та економічні методи впливу, які ускладнюють традиційні механізми оборони та кризового реагування.

Звернемо увагу на документ «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» (2016 р.), який був представлений у Спільному повідомленні Європейського парламенту та Ради. У ньому зазначається, що Європейська Рада у червні 2015 року підкреслила важливість мобілізації інструментів ЄС для протидії гібридним загрозам, наголосивши на необхідності збереження гнучкості в їхньому визначенні, з огляду на їхню динамічну та еволюційну природу. Концепція боротьби з гібридними загрозами передбачає поєднання примусових та підривних дій, а також використання як традиційних, так і нетрадиційних методів, серед яких дипломатичні, військові, економічні та технологічні інструменти. Ці заходи можуть застосовуватися державними чи недержавними суб'єктами у скоординований спосіб для досягнення стратегічних цілей без офіційного оголошення війни [27].

Варто зазначити, що протидія гібридним загрозам передусім є сферою відповідальності та компетенції держав-членів. На відміну від ЄС чи інших міжнародних організацій, національні уряди мають у своєму розпорядженні необхідні інструменти, зокрема розвідувальні та контррозвідувальні служби (як цивільні, так і військові), правоохоронні органи, механізми комунікації з населенням і засоби реагування на кіберінциденти. Водночас, хоча національна

безпека є пріоритетом кожної окремої держави, гібридні загрози нерідко виходять за межі національних кордонів. У таких випадках Європейський Союз відіграє ключову роль у зміцненні стійкості своїх членів, надаючи необхідну підтримку у ситуаціях, коли заходи, вжиті на національному рівні, виявляються недостатньо ефективними [29].

Європейський Союз активно розширює свої можливості у цій сфері, інтегруючи заходи з кібербезпеки, стратегічних комунікацій та розвідки у загальну систему колективної безпеки, щоб ефективно реагувати на сучасні виклики та забезпечувати стійкість своїх держав-членів.

НАТО та Європейський Союз розглядають гібридні загрози як один із головних викликів сучасній системі безпеки, проте їхні підходи до протидії таким загрозам суттєво відрізняються. Якщо НАТО зосереджується переважно на військовому та стратегічному аспекті, включаючи кібероборону та протидію інформаційним атакам, то ЄС робить акцент на нормативно-правовому регулюванні, економічних інструментах і зміцненні стійкості держав-членів.

Альянс розглядає гібридні війни як частину загальної системи колективної оборони. Після саміту в Уельсі у 2014 році НАТО офіційно визнало гібридні загрози ключовою проблемою і поступово адаптувало свою стратегію для ефективнішого реагування. Організація створила спеціалізовані підрозділи для аналізу кіберзагроз, посилила механізми стратегічних комунікацій і розширила співпрацю з національними розвідками країн-членів. Одним із важливих рішень стало включення кібератак у перелік загроз, які можуть активувати статтю 5 Вашингтонського договору про колективну оборону.

Європейський Союз, своєю чергою, розглядає гібридні загрози через призму економічної, кібернетичної та інформаційної безпеки. У 2016 році було ухвалено Спільну рамкову стратегію з протидії гібридним загрозам, яка спрямована на зміцнення кібербезпеки, захист критичної інфраструктури та координацію між країнами-членами в боротьбі з дезінформацією. ЄС також активно використовує санкційну політику як один із ключових інструментів

стримування, накладаючи економічні обмеження на держави та суб'єкти, що займаються гібридною агресією.

Попри різні підходи, НАТО та ЄС тісно співпрацюють у цій сфері. У 2016 році вони підписали угоду про посилене партнерство в боротьбі з гібридними загрозами, що передбачає обмін розвідувальними даними, спільні навчання та координацію стратегічних комунікацій. Одним із важливих кроків стало створення Європейського центру передового досвіду з протидії гібридним загрозам у Гельсінкі, який об'єднує експертів з обох організацій.

3.2. Світові політичні зрушення як наслідки гібридних конфліктів

Серед головних факторів, що спричиняють сучасні воєнно-політичні конфлікти, вітчизняний дослідник О. Батрименко виокремлює контроль над світовими ресурсами та територіями, розпад поліетнічних держав і соціальних структур, що веде до зростання соціально-політичної напруженості, а також втрата народами національної ідентичності, яка загострює етнонаціональні та релігійні суперечності. Крім того, конфлікти можуть виникати внаслідок боротьби за домінування певних духовних і культурних цінностей, що проявляється у прагненні окремих політичних сил змінити суспільно-політичний устрій або правлячу еліту. Світова практика свідчить, що ці чинники зазвичай поєднуються, формуючи комплексні передумови для виникнення конфліктів [3, с.95].

Один із ключових наслідків гібридних конфліктів – розмивання меж між війною і миром, що створює нестабільність у міжнародній системі. Традиційні механізми безпеки, зокрема механізми колективної оборони НАТО або миротворчі місії ООН, стикаються з труднощами у реагуванні, оскільки гібридні загрози часто діють без офіційного оголошення війни, через проксі-сили, дезінформацію або економічний тиск. Це призводить до необхідності перегляду підходів до стримування та реагування на нові виклики.

Зміни у геополітичному балансі проявляються в посиленні конфронтації між ключовими глобальними гравцями. Використання гібридних методів

ведення війни дозволяє державам здійснювати прихований вплив на внутрішню політику інших країн, втручатися у виборчі процеси, підривати довіру до демократичних інституцій. Це сприяє загостренню протистояння між Заходом та авторитарними державами, такими як Росія та Китай, що веде до нових політичних і економічних санкцій, торговельних війн та військової ескалації у стратегічних регіонах.

Одночасно гібридні конфлікти призводять до зміцнення військових альянсів і перегляду оборонних стратегій. Наприклад, агресивна політика Росії щодо України та використання гібридних загроз стимулювали розширення НАТО, зокрема вступ Фінляндії та Швеції до Альянсу. Європейський Союз також активізував свою безпекову політику, зміцнюючи кіберзахист, стратегічні комунікації та механізми колективного реагування на інформаційні атаки.

Гібридні конфлікти суттєво трансформували діяльність міжнародних організацій, змусивши їх адаптувати свої стратегії безпеки та управління кризами. Оскільки такі конфлікти поєднують військові, інформаційні, економічні та кібернетичні методи, традиційні механізми реагування, розроблені для класичних війн і дипломатичних протистоянь, виявилися недостатньо ефективними.

ООН, будучи традиційно зосередженою на дипломатичних механізмах врегулювання конфліктів, опинилася в складному становищі. Гібридні війни часто ведуться через проксі-групи, недержавних акторів або економічні санкції, що ускладнює визначення відповідальних сторін і застосування міжнародного права. Це обмежує можливості Ради Безпеки ООН у прийнятті ефективних рішень, особливо коли серед постійних членів є країни, які самі використовують гібридні методи у своїй зовнішній політиці. Через специфічні особливості гібридних воєн і тероризму миротворчі операції ООН стикаються з низкою серйозних викликів. Гібридні конфлікти розмивають межі між комбатантами та цивільним населенням, що значно ускладнює ідентифікацію загроз для миротворчих сил. Додаткову складність створює участь

недержавних акторів, зокрема терористичних угруповань, що робить оперативне середовище ще більш непередбачуваним. У таких умовах навіть цивільна інфраструктура може бути перетворена на об'єкт атаки або використана для проведення бойових операцій, що підвищує ризики для місцевого населення та ускладнює виконання миротворчих місій [24, с. 354]. Проте ООН активно працює над оновленням своїх механізмів кібербезпеки та миротворчих операцій, зокрема через посилення контролю за інформаційними війнами та боротьбу з фейковими новинами в міжнародному просторі.

Гібридні конфлікти сприяють поглибленню розколу в міжнародній політиці, загострюючи суперництво між державами та спричиняючи перегрупування сил на глобальній арені. Використання прихованих методів боротьби, таких як економічний тиск, кібератаки, інформаційні війни та підтримка проксі-груп, дозволяє країнам просувати власні інтереси, уникаючи відкритого збройного конфлікту. Це створює атмосферу постійної напруженості та недовіри між державами, що посилює глобальну нестабільність.

Світ дедалі більше ділиться на конкуруючі блоки, де авторитарні режими, такі як Росія та Китай, протистоять західним демократіям, представленим США, Європейським Союзом та їхніми союзниками. Гібридні методи використовуються для ослаблення демократичних інституцій, втручання у виборчі процеси та розколу суспільства через дезінформацію. Це призводить до посилення геополітичного суперництва, зростання гонки озброєнь та зміцнення військових альянсів, таких як НАТО та новостворені оборонні партнерства на кшталт AUKUS.

Одним із найяскравіших проявів поляризації стала економічна та технологічна війна між США та Китаєм. Контроль за критично важливими ресурсами, такими як напівпровідники, рідкоземельні метали та штучний інтелект, став інструментом стратегічного протистояння, що впливає на світові ринки та змушує країни обирати сторони у глобальному суперництві. Подібна ситуація спостерігається і в енергетичному секторі, де використання

енергоресурсів як геополітичного важеля впливає на стабільність міжнародних відносин [2].

Гібридні конфлікти суттєво впливають на внутрішню політику держав, оскільки спрямовані на підриг стабільності, послаблення урядів та маніпуляцію суспільною думкою. Використовуючи інструменти інформаційної війни, кібератак, економічного тиску та підтримки внутрішніх опозиційних рухів, зовнішні сили можуть змінювати політичний ландшафт держави без прямого збройного втручання.

Одним із ключових наслідків гібридних конфліктів є політична дестабілізація. Внутрішні протистояння загострюються через інформаційні кампанії, спрямовані на дискредитацію урядів, створення хаосу та недовіри до державних інституцій. Дезінформація, фейкові новини та маніпуляції у соціальних мережах використовуються для поляризації суспільства, формування протестних настроїв та підтримки певних політичних сил, що відповідають інтересам зовнішніх гравців.

Окремої уваги заслуговує той факт, що ініціаторами дестабілізації політичної системи можуть виступати не лише внутрішні чинники, а й зовнішні сили — суб'єкти міжнародних відносин, які переслідують власні інтереси. До них належать як окремі держави чи їхні коаліції, так і транснаціональні корпорації, юридичні та фізичні особи, які для досягнення своїх цілей створюють спеціальні організації, такі як фонди чи трасти. У глобалізованому світі будь-яка держава має як прихильників, так і опонентів, і далеко не завжди їхні наміри є конструктивними для подальшого розвитку політичної системи. Дестабілізаційні процеси можуть бути спрямовані на загострення суспільних проблем, нав'язування певних політичних рішень або зміну економічних і стратегічних пріоритетів держави. У такому випадку негативний вплив подібних процесів на суспільство є очевидним. В цьому контексті цікавою є думка одного з провідних світових економістів Е. Райнерта, який співпрацював із урядами 80 країн. Він зазначає, що політика вільного ринку перетворює Україну на аграрну державу, а вимоги МВФ мають деструктивний характер. За

його словами, дії МВФ щодо України нагадують сценарії, які призвели до економічних криз у країнах Латинської Америки у 1980-х роках [6].

Вибірчі процеси стають однією з головних цілей гібридних атак. Втручання у вибори через кібератаки, маніпуляцію інформацією та фінансування політичних партій сприяє підризу демократичних інституцій. Це особливо актуально для країн, що мають слабку систему політичного контролю над впливом іноземних сил. Такий підхід дозволяє зовнішнім акторам змінювати внутрішній політичний баланс, просуваючи лояльні до них уряди або створюючи кризу легітимності влади.

Гібридні конфлікти також впливають на державну безпекову політику, змушуючи уряди посилювати заходи контролю, запроваджувати закони щодо боротьби з дезінформацією, кіберзлочинністю та зовнішнім втручанням. У деяких випадках це призводить до посилення авторитарних тенденцій, коли під приводом боротьби з гібридними загрозами влада обмежує свободу слова, посилює контроль над ЗМІ та впроваджує жорсткі заходи проти опозиції.

Отже, гібридні конфлікти, поєднуючи військові, економічні, інформаційні та кібератаки, суттєво впливають на політичні процеси держав, що стають їх жертвами. Вони призводять до трансформації внутрішньої та зовнішньої політики, змінюючи пріоритети державного управління та міжнародних відносин.

3.3. Зусилля світового співтовариства у протидії гібридним загрозам

Світове співтовариство активно реагує на виклики, які створюють гібридні загрози, формуючи комплексні стратегії для їхнього подолання. Країни та міжнародні організації об'єднують зусилля, посилюючи співпрацю у сферах безпеки, кіберзахисту та інформаційної протидії. Особливо значну роль у цьому процесі відіграють такі об'єднання, як НАТО, Європейський Союз та ООН, які виробляють спільні політики та впроваджують програми для посилення стійкості своїх членів до гібридних атак.

НАТО відіграє ключову роль у протидії гібридним загрозам, зосереджуючи свої зусилля на кібербезпеці та колективній обороні. Одним із важливих кроків Альянсу стало створення Центру передового досвіду з кібероборони у Таллінні, Естонія. Цей центр є платформою для досліджень, навчання та обміну досвідом у сфері кіберзахисту, де фахівці з різних країн розробляють нові методи протидії кіберзагрозам і відпрацьовують сценарії реагування на атаки [15].

Крім того, НАТО регулярно проводить спільні військові та кібернавчання, наприклад, Cyber Coalition, які дозволяють відпрацьовувати навички колективного реагування на гібридні загрози. Ці навчання зміцнюють співпрацю між країнами-членами, підвищують рівень готовності кіберпідрозділів і забезпечують ефективну взаємодію в кризових ситуаціях. У навчаннях беруть участь приблизно 1000 фахівців із кібербезпеки, які представляють 26 країн-членів Альянсу, а також Фінляндію, Швецію, Грузію, Ірландію, Японію, Швейцарію, Європейський Союз та представників промислових і наукових кіл [16].

Важливою складовою діяльності Альянсу є розробка комплексної стратегії боротьби з гібридними загрозами, яка охоплює як військові, так і немілітаризовані аспекти конфліктів. У стратегії особливу увагу приділено кібербезпеці, протидії дезінформації та захисту критичної інфраструктури. Відтак, НАТО послідовно адаптує свої підходи до сучасних загроз, зміцнюючи обороноздатність не лише окремих держав, а й усього євроатлантичного простору.

Європейський Союз активно протидіє гібридним загрозам, приділяючи особливу увагу боротьбі з дезінформацією та зміцненню кібербезпеки. Одним із ключових інструментів ЄС у цій сфері стала ініціатива EUvsDisinfo, створена в межах діяльності East Strat Com Task Force. Її метою є виявлення та спростування фейкових новин, а також підвищення обізнаності громадськості про інформаційні маніпуляції. Платформа публікує аналітику та приклади

dezінформації, спрямованої проти європейських країн, допомагаючи медіа та громадянам краще розпізнавати неправдиві наративи [7].

Окрім боротьби з фейками, ЄС посилює заходи кібербезпеки, розвиваючи співпрацю між країнами-членами для захисту критичної інфраструктури та запобігання кібератакам. Важливим кроком стало створення Агентства Європейського Союзу з кібербезпеки (ENISA), яке координує діяльність у сфері цифрової безпеки та сприяє підвищенню стійкості державних і приватних систем до кіберзагроз. Таким чином, Європейський Союз комплексно протидіє гібридним викликам, поєднуючи інформаційну безпеку з технологічними рішеннями для захисту своїх громадян і спільних цінностей.

Організація з безпеки та співробітництва в Європі (ОБСЄ) відіграє важливу роль у протидії гібридним загрозам, зокрема через моніторинг інформаційного простору та посередництво у врегулюванні конфліктів. ОБСЄ активно відстежує прояви дезінформації та інформаційних атак, які можуть загрожувати стабільності та безпеці країн-учасниць. Особлива увага приділяється захисту свободи слова та підтримці незалежних медіа як ключового інструмента протидії пропаганді.

Водночас ОБСЄ виступає посередником у мирному врегулюванні конфліктів, спричинених гібридними загрозами. Організація організовує переговори між сторонами конфліктів, сприяє деескалації напруженості та моніторить виконання домовленостей. Наприклад, Спеціальна моніторингова місія ОБСЄ в Україні відігравала важливу роль у фіксуванні порушень режиму припинення вогню та висвітленні ситуації на сході країни [21].

Окремі країни світу активно розробляють власні стратегії для протидії гібридним загрозам, поєднуючи заходи у сферах кібербезпеки, інформаційної протидії, дипломатії та оборони.

Сполучені Штати Америки зосереджуються на комплексному підході до боротьби з гібридними загрозами. Уряд США ухвалив національну стратегію кібербезпеки, спрямовану на захист критичної інфраструктури та реагування на кібератаки. Особливу увагу приділено протидії дезінформації та пропаганді, яка

загрожує демократичним процесам. Крім того, США активно застосовують санкції проти країн, що використовують гібридні методи для дестабілізації міжнародної безпеки.

Великобританія зосереджує свої зусилля на зміцненні кіберзахисту та боротьбі з інформаційними загрозами. У країні створено Національний центр кібербезпеки (NCSC), який координує дії державних і приватних структур для протидії кібератакам. Велика увага приділяється інформаційній гігієні: уряд впроваджує освітні програми для населення та співпрацює з медіа для виявлення та спростування фейків.

Україна, маючи власний досвід протидії гібридній агресії, зосереджується на посиленні обороноздатності та інформаційної безпеки. Після початку війни та гібридних атак з боку Росії країна активно співпрацює з НАТО та ЄС, переймаючи досвід у сфері кібербезпеки та стратегічних комунікацій. В Україні запроваджено програми протидії дезінформації та створено Центр протидії інформаційним загрозам. Водночас держава посилює кіберзахист стратегічних об'єктів та енергетичної інфраструктури.

Отже, зусилля світового співтовариства у протидії гібридним загрозам є багатограними та взаємопов'язаними. Вони поєднують технологічні інновації, інформаційну безпеку, дипломатичний тиск і військове співробітництво, створюючи комплексний захист від новітніх викликів глобального світу.

ВИСНОВКИ

У процесі дослідження теоретико-методологічних основ гібридних війн, ми зробили такі висновки:

1. З'ясовано, що більшість сучасних теоретичних підходів до трактування поняття «гібридна війна» акцентують увагу на її багатовимірному характері. На відміну від традиційних військових конфліктів, які ґрунтуються переважно на відкритому збройному протистоянні регулярних армій, гібридна війна передбачає поєднання конвенційних і неконвенційних засобів впливу. Вона включає широкий спектр дій – від інформаційних атак, кібероперацій, економічного тиску до використання нерегулярних збройних формувань, провокацій та політичного шантажу. Встановлено, що ключовою відмінністю гібридної війни є її прихований, асиметричний і часто позаправовий характер, що ускладнює своєчасне виявлення агресора та формування адекватної відповіді з боку держави-жертви. Такий тип конфлікту розмиває межі між війною та миром, що потребує нових підходів до безпекової політики, міжнародного права та оборонного планування.

2. Визначено, що гібридна війна є комплексною формою ведення агресії, яка поєднує як традиційні, так і нетрадиційні методи впливу. Основними її складовими виступають: військова агресія із застосуванням регулярних або нерегулярних збройних формувань; інформаційно-психологічні операції, спрямовані на дезорієнтацію суспільства та послаблення національної єдності; кібератаки як засіб паралізування інфраструктури та порушення інформаційної безпеки; економічний тиск, включно з енергетичним шантажем, санкціями або блокадою; а також політична дестабілізація, яка реалізується через підтримку маріонеткових режимів або провокування внутрішнього конфлікту. Комплексне застосування цих елементів дозволяє агресору досягати стратегічних цілей без прямої та формальної оголошеної війни. Це суттєво ускладнює адекватну реакцію з боку міжнародної спільноти та правової системи.

3. Встановлено, що застосування гібридних методів тиску в міжнародній політиці демонструє сталу тенденцію до зростання, зокрема в умовах трансформації глобальної системи безпеки та послаблення ефективності традиційних механізмів дипломатичного впливу. Від початку XXI століття, а особливо після подій 2014 року в Україні, гібридні засоби – такі як кібератаки, дезінформація, економічне шантажування, політична дестабілізація, використання проксі-груп та невизнаних акторів – дедалі частіше застосовуються не лише окремими державами, але й транснаціональними структурами для досягнення своїх стратегічних цілей. Ці методи дозволяють агресору діяти без оголошення війни, розмиваючи межі між станом миру й конфлікту, що суттєво ускладнює як виявлення джерел впливу, так і реагування на них. Характерною рисою сучасної гібридної агресії є її постійна еволюція, адаптація до нових технологій, зокрема використання штучного інтелекту, big data та соціальних медіа як інструментів маніпуляції громадською думкою.

4. Доведено не повну міру готовності системи міжнародного права до викликів, які породжує нова форма конфліктів. Гібридна війна, як поєднання традиційних військових дій з інформаційними атаками, кіберагресією, економічним тиском і політичним впливом, виходить за межі класичних уявлень про війну та мир. На сьогоднішній день міжнародне гуманітарне право, а також норми, закріплені в Статуті ООН, Женевських конвенціях і численних резолюціях, лише частково охоплюють новітні форми гібридного впливу. Попри наявність окремих правових інструментів, зокрема санкційних механізмів, інституту відповідальності за агресію, а також засобів реагування на кібератаки й дезінформацію, міжнародне право часто не встигає за швидкістю та змінністю гібридних загроз. Основною проблемою залишається відсутність чіткого юридичного визначення поняття «гібридна війна» та комплексного підходу до її правового регулювання. Разом з тим, окремі міжнародні ініціативи, як-от Будапештська конвенція про кіберзлочинність, Стратегії НАТО щодо гібридної загрози, а також кейси розгляду агресії в

міжнародних судах, свідчать про поступову адаптацію міжнародного права до нових умов.

5. Виявлено, що ефективна протидія гібридним загрозам вимагає системного, багатовекторного підходу, який поєднує інструменти безпекової політики, кіберзахисту, інформаційної гігієни, дипломатії та правового реагування. На національному рівні ключову роль відіграє створення єдиної координаційної системи між силовими структурами, службами безпеки, медіа та громадянським суспільством. При цьому особливо важливо забезпечити інформаційну стійкість держави, розвиток національних стратегічних комунікацій та впровадження механізмів оперативного реагування на кібератаки, дезінформацію й інші нетрадиційні форми впливу. На міжнародному рівні протидія гібридним загрозам здійснюється завдяки співпраці в межах НАТО, ЄС, ООН та інших багатосторонніх інституцій, які формують спільні підходи до виявлення, стримування та нейтралізації гібридних викликів. Важливими аспектами цієї взаємодії є обмін розвідувальною інформацією, узгодження правових рамок та спільні навчання, що дозволяють підвищити колективну безпеку.

6. Визначено комплекс ймовірних заходів щодо посилення інформаційної, кібернетичної та військової безпеки України. Встановлено, що ефективна протидія гібридним впливам потребує не лише розбудови технологічної спроможності держави, але й системної взаємодії між державними інституціями, громадянським суспільством та міжнародними партнерами. Зокрема, в сфері інформаційної безпеки наголошено на необхідності посилення національного медіапростору, впровадження механізмів раннього виявлення фейкових кампаній, розвитку цифрової грамотності населення та підтримки незалежної журналістики. Водночас кібербезпека вимагає модернізації технічної інфраструктури критичних об'єктів, посилення державного контролю за кіберзагрозами, а також створення умов для тісної співпраці з приватним сектором у сфері цифрового захисту. У військовій площині особливий акцент зроблено на розвитку сил територіальної

оборони, адаптації стратегічних підходів до умов асиметричних конфліктів, інтеграції технологій штучного інтелекту, а також активному залученні досвіду країн НАТО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Базилюк Я. Б., Бурбела Т. М., Гавриленко Н. М., Давиденко С. В., Діденко Н. Г., Суходоля О. М., Шаров О. М., Юлдашев Р. Е. Економічні інструменти протидії гібридній агресії. Київ: НІСД, 2020. 69 с. URL: <https://niss.gov.ua/sites/default/files/2020-09/dopovid-economichni-instrumenty-protydii-gibrydniy-agresii-1.pdf> (дата звернення: 17.02.2025).
2. Баловсяк Н. Глобальне технологічне протистояння. Китай та США сперечаються за контроль над інноваціями. *Тиждень.ua*, 2023. URL: <https://tyzhden.ua/hlobalne-tekhnologichne-protystoiannia-kytaj-ta-ssha-sperechaiutsia-za-kontrol-nad-innovatsiiamy/> (дата звернення: 16.02.2025).
3. Березовська-Чміль О., Кобець Ю., Міщук М. Управління системою національної безпеки в умовах воєнно-політичного конфлікту. *Грані*. 2021. № 24(9). С. 70–76. URL: <https://grani.org.ua/index.php/journal/article/view/1697/1672> (дата звернення: 16.02.2025).
4. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці МАУП. Політичні науки та публічне управління*. 2024. № 2(74). С. 24–31. URL: <https://journals.maup.com.ua/index.php/political/article/view/4319/4632> (дата звернення: 17.02.2025).
5. Василенко О. В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому. *Наука і оборона*. 2009. Т. 4. С. 18–23.
6. Герман О., Мицишин Т. Гібридні війни: історичні і психологічні аспекти. *Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки*: збірник тез III Міжнародної наукової конференції, 20–21 квітня 2023 р. / упоряд. Криськов А. А., Габрусєва Н. В. Тернопіль: ФОП Паляниця В. А., 2023. С. 98–100. URL: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://elartu.tntu.edu.ua/bitstream>

- /lib/41097/2/MCTD_2023_Herman_O-Hybrid_wars_historical_and_98-100.pdf
(дата звернення: 10.02.2025).
7. Ерік Райнерт: МВФ сьогодні робить з Україною те саме, що відбувалося з Латинською Америкою у 1980-х роках. *ХВИЛЯ*. 2016. URL: <https://hvylya.net/> (дата звернення: 12.02.2025).
 8. Європейська служба зовнішніх справ. *Офіційний вебсайт Європейського Союзу*. URL: <https://eeas.europa.eu/> (дата звернення: 14.02.2025).
 9. Замулін І. Ю. «Гібридні війни» у світовому політичному процесі. URL: <chrome-extension://efaidnbmnnnibpcajpcgklclefindmkaj/https://philarchive.org/archive/TR ESJO> (дата звернення: 11.02.2025).
 10. Концепція «гібридної» війни та її складові. (2024) *Центр безпекових досліджень «СЕНСС»*. URL: <https://senss.org/> (дата звернення: 16.02.2025).
 11. Левантович О. Гібридні війни ХХІ століття: нові виклики для медіапростору. *Вісник Львівського університету. Серія: Журналістика*, 2019. Вип. 45. С. 52-59. URL: http://nbuv.gov.ua/UJRN/VLNU_Jur_2019_45_9 (дата звернення: 15.02.2025).
 12. Лещенко О. Гібридні війни: аспекти цивільного захисту. *Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки*: збірник тез І Міжнародної наукової конференції присвяченої 35 роковинам аварії на ЧАЕС, 22–23 квітня 2021 р. / упорядники: А. А. Криськов, В. В. Вишньовський та Н. В. Габрусєва. Тернопіль: ФОП Паляниця В. А., 2021. С. 113–115. URL: chrome-extension://efaidnbmnnnibpcajpcgklclefindmkaj/https://elartu.tntu.edu.ua/bitstream/lib/35099/2/MCTD_2021_Leshchenko_O-Hybrid_wars_aspects_113-115.pdf (дата звернення: 11.02.2025).
 13. Лубкович І. М. Місце українських медій в інформаційній війні 2013–2014 рр. *Наукові записки Інституту журналістики*. 2014. Т. 56. С. 182–187. URL: http://nbuv.gov.ua/UJRN/Nzizh_2014_56_37 (дата звернення: 15.02.2025).

14. Магда Є. М. Гібридна війна: сутність та структура феномену. *International relations, part «Political sciences»*. (4). 2014. URL: http://journals.iir.edu.ua/index.php/pol_n/article/view/2489 (дата звернення: 11.02.2025).
15. Магда Є. М. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с. URL: chrome-extension://efaidnbmnnnibpcajpcgicfindmkaj/https://balka-book.com/files/2017/06_10/12_24/u_files_store_6_68818.pdf (дата звернення: 11.02.2025).
16. Мазур Я. П. Основні кіберзагрози в умовах ведення інформаційної війни. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. Розділ VII. Адміністративне право і процес; фінансове право; інформаційне право. URL: <chrome-extension://efaidnbmnnnibpcajpcgicfindmkaj/https://app-journal.in.ua/wp-content/uploads/2024/12/100.pdf> (дата звернення: 05.02.2025).
17. Макаренко Н. Г. Асиметричні війни як вид сучасних збройних конфліктів: соціогуманітарний аспект. *XVIII міжнародна науково-практична конференція «Конфліктологічна експертиза: теорія та методика»*. Київ, 2019. С. 41–45. URL: <https://ekmair.ukma.edu.ua/handle/123456789/16005> (дата звернення: 11.02.2025).
18. Місько В. Світова гібридна війна: український фронт: монографія. Харків: Фоліо, 2017. 496 с.
19. НАТО відкриває новий Центр передового досвіду з питань кібернетичного захисту. *NATO*. 2008. URL: https://www.nato.int/cps/uk/natohq/news_7266.htm?selectedLocale=uk (дата звернення: 10.02.2025).
20. НАТО проводить в Естонії навчання з кібербезпеки – беруть участь 26 країн. *Укрінформ*. 2022. URL: <https://www.ukrinform.ua/rubric-technology/3624766-nato-provodit-v-estonii-navcanna-z-kiberbezpeki-berut-ucast-26-krain.html> (дата звернення: 16.02.2025).
21. Павлюк О. В Естонії почались найбільші кібернавчання НАТО, Україна вперше бере участь. *Європейська правда*. 2022. URL:

- <https://www.eurointegration.com.ua/news/2024/04/24/7184563/> (дата звернення: 16.02.2025).
22. Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2022. № 2(53).
 23. Пахолок В. М. Органи місцевого самоврядування як суб'єкт дипломатичного тиску в умовах російської агресії. *Актуальні проблеми міжнародних відносин і регіональних досліджень: матеріали II Міжнародної науково-практичної Інтернет-конференції* (м. Луцьк, 09 листопада 2022 р.) / укладачі: С. Кулик, А. Моренчук. Луцьк, Волинський національний університет імені Лесі Українки, 2022. С. 53–56. URL: <https://evnuir.vnu.edu.ua/handle/123456789/27078> (дата звернення: 16.02.2025).
 24. Пахолок В. М. Фактор України в глобальних політико-безпекових ризиках: за рубрикою журналу Time «Топ-10 глобальних ризиків». *Всеукраїнські політологічні читання імені професора Богдана Яроша: зб. наук. та навч.-метод. пр. / за заг. ред. В. І. Бортнікова, Я. Б. Яроша*. Луцьк: Вежа-Друк, 2024. Вип. 13. 188 с.
 25. Петришин Б. Кібербезпека в умовах гібридної війни. *ІА Рубрик*. 2022. URL: <https://rubryka.com/article/14-den-vijny/> (дата звернення: 10.02.2025).
 26. Рева Т. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2022. Вип. 40. С. 186–191. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://fps-visnyk.lnu.lviv.ua/archive/40_2022/24.pdf (дата звернення: 13.02.2025).
 27. Саркісян Л. Г., Самсонова Л. В. Гібридні загрози в торговельно-економічних відносинах. *Актуальні проблеми розвитку економіки регіону: науковий журнал*. 2020. Вип. 16. Т. 2. С. 62–76. URL: <http://hdl.handle.net/123456789/10155> (дата звернення: 08.02.2025).
 28. Семенюк Ю. В. Застосування приватних військових компаній для забезпечення національних інтересів і безпеки держави. *Вчені записки ТНУ*

- імені В. І. Вернадського. Серія: Державне управління. 2020. Т. 31 (70). № 2. С. 230–235. (дата звернення: 18.02.2025).
29. Спеціальна моніторингова місія ОБСЄ в Україні. OSCE. URL: <https://www.osce.org/uk/special-monitoring-mission-to-ukraine-closed> (дата звернення: 18.02.2025).
30. Тараненко М. М. Гібридна війна в Україні: історія та сучасність. *Вісник НТУУ «КПІ» Політологія. Соціологія. Право*. 2016. № 3/4 (31/32). URL: <https://visnyk-psp.kpi.ua/article/view/140532/137618> (дата звернення: 13.02.2025).
31. Тетерчук А. Інформаційно-психологічний вплив засобами візуальних комунікацій у гібридній війні. Національний університет «Острозька академія», 2022. 114 с.
32. Узденова Ю. М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. Т. 35 (74). № 4. С. 172–179. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pubadm.vernadskyjournals.in.ua/journals/2024/4_2024/28.pdf (дата звернення: 09.02.2025).
33. Чорняк Р. А. Гібридні війни як різновид інформаційних війн XXI ст. *Інформаційні технології і системи в документознавчій сфері*. 2024. С. 164–167. URL: <https://jitas.donnu.edu.ua/article/view/15971> (дата звернення: 11.02.2025).
34. Чернявський М. В. Виклики миротворчих операцій ООН в умовах гібридних війн і тероризму. *Розбудова держави і права: питання теорії та конституційної практики. Право і суспільство*. 2024. № 5. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.pravoisuspilstvo.org.ua/archive/2024/5_2024/53.pdf (дата звернення: 09.02.2025).
35. Шевчук Д. Б. «Гібридні» війни як інструмент реалізації національних інтересів в умовах глобальної нестабільності. Західноукраїнський національний університет навчально-науковий інститут міжнародних відносин ім. Б. Д. Гаврилишина. 2021. 74 с. URL: [chrome-](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.pravoisuspilstvo.org.ua/archive/2024/5_2024/53.pdf)

- extension://efaidnbmnnnibpcajpcglclefindmkaj/http://dspace.wunu.edu.ua/bitstream/316497/44358/1/%D0%A8%D0%B5%D0%B2%D1%87%D1%83%D0%BA%20%D0%94..pdf (дата звернення: 11.02.2025).
36. Шостаківська Н., Коваль А. Гібридні війни: історичні та психологічні аспекти. *Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки*: збірник тез IV Міжнародної наукової конференції, 18–19 квітня 2024 р. / упоряд. А. А. Криськов, М. Я. Блавіцький, Н. В. Габрусєва. Тернопіль: ФОП Паляниця В. А., 2024. С. 85–87.
37. Яворська Г. М. Гібридна війна як дискурсивний конструкт. *Стратегічні пріоритети. Серія: Політика*. 2016. № 4. С. 41–48. URL: <https://ippi.org.ua/sites/default/files/yavorskaya.pdf> (дата звернення: 09.02.2025).
38. Galeotti M. *Controlling Chaos: How Russia manages its political war in Europe*. 2017. URL: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/ (date of application: 05.02.2025).
39. Hagelstam A. Співпраця заради протидії гібридним загрозам. *NATOREVIEW*. 2018. URL: <https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsyazaradi-protid-gbridnim-zagrozm/index.html> (date of application: 05.02.2025).
40. Horbulin V. *The World Hybrid War. Ukrainian Forefront*. 2017. Kyiv. URL: https://niss.gov.ua/sites/default/files/2017-01/GW_engl_site.pdf (date of application: 15.02.2025).
41. Kalniete S., Pildegovičs T. Strengthening the EU's resilience to hybrid threat. *European View*, 20 (1). 2021. URL: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.martenscentre.eu/wp-content/uploads/2021/07/4.pdf> (date of application: 14.02.2025).
42. Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales on 05 Sep. 2014. NATO. URL: https://www.nato.int/cps/cn/natohq/official_texts_112964.htm (date of application: 13.02.2025).

АНОТАЦІЯ

Луцюк Олена Олександрівна. Гібридні війни як інструмент міжнародної політики.

Робота на здобуття освітнього ступеня «Бакалавр». Спеціальність: 052 «Політологія». Освітньо-професійна програма: «Політологія та державне управління». – Волинський національний університет імені Лесі Українки, Луцьк, 2025.

У Вступі обґрунтовано актуальність теми дослідження, сформульовано її мету і завдання, об'єкт і предмет дослідження, методологічну базу та наукову новизну отриманих результатів, джерельну основу дослідження, практичне значення одержаних результатів, окреслено структуру роботи.

Об'єктом дослідження є феномен гібридних війн у сучасних політичних відносинах.

Предмет дослідження – гібридні війни як інструмент міжнародної політики.

У Розділі 1 «Теоретико-методологічні основи дослідження гібридних війн» розкрито сутність поняття «гібридні війни», їх основні види та форми, а також проаналізовано стан наукової розробки предмету дослідження.

У Розділі 2 «Інструменти та механізми гібридних війн» визначено основні засоби ведення гібридних війн, особливу увагу приділено мілітарним та парамілітарним, проаналізовано потенціал інформаційних операцій та кібернападів у сучасних війнах, досліджено економічні та торговельні засоби боротьби.

Розділ 3 «Чинник гібридних війн у сучасній геополітиці» розкриває безпекову політику міжнародних організацій, світові політичні зрушення як наслідки гібридних конфліктів та зусилля світового співтовариства у протидії гібридним загрозам.

У Висновках підсумовано теоретичні засади дослідження, проаналізовано успішні світові практики запобігання гібридних загроз, узагальнено безпекові зусилля світового співтовариства стосовно запобігання та припинення гібридних війн. Визначено комплекс ймовірних заходів щодо посилення інформаційної, кібернетичної та військової безпеки України.

Ключові слова: гібридні війни, міжнародна політика, міжнародні конвенції, міжнародні організації, зарубіжний досвід, інформаційні операції, кібернапади.