

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кам'янець-Подільський національний університет імені Івана Огієнка

Історичний факультет

Кафедра політології та філософії

Кваліфікаційна робота

на здобуття ступеня вищої освіти «магістр»

з теми: «ГІБРИДНІ ВІЙНИ ЯК НОВИЙ ВИКЛИК ДЛЯ МІЖНАРОДНОЇ
БЕЗПЕКИ: УКРАЇНСЬКИЙ ДОСВІД»

Виконав: здобувач вищої освіти

спеціальності 052 Політологія

заочної форми здобуття вищої освіти

Бондар Юрій Георгійович

Керівник:

кандидат філософських наук

доцент

Сулятицька Тетяна Василівна

Рецензент: _____

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. СТАН ДЖЕРЕЛЬНОЇ БАЗИ ТА НАУКОВОЇ РОЗРОБКИ ПРОБЛЕМИ.....	9
РОЗДІЛ 2. Теоретико-методологічні засади дослідження гібридних війн	13
2.1. Поняття та сутність гібридної війни в сучасних міжнародних відносинах	13
2.2. Інструменти та технології гібридного впливу	18
РОЗДІЛ 3. ГІБРИДНА АГРЕСІЯ РОСІЇ ПРОТИ УКРАЇНИ ЯК ПРИКЛАД СУЧАСНОЇ ГІБРИДНОЇ ВІЙНИ	25
3.1. Передумови та етапи розгортання гібридної війни проти України (2014– 2024).....	25
3.2. Інформаційно-пропагандистські та психологічні операції рф.....	29
3.3. Кіберзагрози та економічний тиск як компоненти агресії.....	36
РОЗДІЛ 4. УКРАЇНСЬКИЙ ДОСВІД ПРОТИДІЇ ГІБРИДНІЙ АГРЕСІЇ ТА ПЕРСПЕКТИВИ ПОСИЛЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ	42
4.1. Модернізація сектору безпеки та оборони України	42
4.2. Стратегічні пріоритети України щодо зміцнення кібер та інформаційної безпеки	45
4.3. Міжнародні підходи до протидії гібридним загрозам та роль світової підтримки у протидії гібридній агресії	49
ВИСНОВКИ	58
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ	62
ДОДАТКИ	
.....	Error! Bookmark not defined.

ВСТУП

Актуальність дослідження «Гібридні війни як новий виклик для міжнародної безпеки: український досвід» є надзвичайно високою, оскільки з початку XXI століття міжнародна система безпеки зіткнулася з якісно новою формою агресії, яка принципово відрізняється від класичних військових конфліктів. Гібридні війни – це стратегія, що поєднує конвенційні військові дії, економічну, інформаційну та кібернетичну агресію, використовуючи при цьому як державні, так і недержавні актори. Цей підхід дозволяє агресору діяти нижче порогу оголошення війни, дезорієнтуючи міжнародну спільноту та ускладнюючи застосування колективної відповіді та механізмів міжнародного права.

Варто сказати, що Україна, починаючи з 2014 року, стала ключовим полігоном для гібридної агресії російської федерації, демонструючи світові всю руйнівну силу та багатовекторність цього виклику. Український досвід виявив критичні вразливості демократичних держав, особливо у сфері інформаційного простору, критичної інфраструктури та державного управління. Тому дослідження гібридних загроз через призму української практики є життєво необхідним для формування ефективних механізмів колективної безпеки, розробки стратегій національної стійкості, що включають концепцію Всеохоплюючої оборони та посилення медіаінформаційної грамотності населення.

Вважаємо, що ігнорування або неадекватне реагування на гібридні загрози створює критичні ризики для національної безпеки, що підтверджується тимчасовою окупацією українських територій. Тому вивчення досвіду країн-партнерів, насамперед країн НАТО та ЄС (зокрема, Польщі та Балтійських країн), які також зазнають гібридного тиску, є наріжним каменем для вироблення ефективних контрзаходів. Співпраця з міжнародними інституціями, такими як Hybrid CoE та EU INTSEN, а також використання економічних (санкційних) та правових (міжнародно-правових) механізмів стає невід’ємною частиною архітектури колективної безпеки.

Переконані, що актуальність теми дослідження посилюється потребою України у стратегічній інтеграції з європейськими та євроатлантичними структурами, що вимагає гармонізації національних безпекових механізмів з найкращими світовими практиками. Надважливим завданням є не лише військова відсіч, але й забезпечення ментальної стійкості суспільства через розвиток медіаінформаційної грамотності, яка є основним гуманітарним інструментом протидії пропаганді. Відтак, дослідження міжнародного досвіду, правових рамок та інституціональних механізмів, спрямованих на боротьбу з гібридною агресією, має фундаментальне теоретичне та прикладне значення для забезпечення життєздатності Української держави у довгостроковій перспективі.

Об'єктом дослідження є процеси виникнення, розвитку та протидії гібридним війнам як формі конфлікту, що змінює архітектуру міжнародної безпеки. **Предметом дослідження** є сукупність сутнісних характеристик, інструментів, українського досвіду протидії, а також міжнародних стратегій та механізмів реагування на гібридні війни.

Хронологічні межі дослідження охоплюють період з 2014 року до 2025 року. Нижній поріг (2014 р.) пов'язаний з початком гібридної агресії РФ проти України, що стало тригером для міжнародних безпекових змін. Верхній поріг (2025 р.) відображає поточний стан розвитку стратегій та експертних оцінок.

Територіальні межі дослідження охоплюють: росію винуватця конфлікту, Україну – як ключовий приклад жертви гібридного конфлікту та суб'єкт формування національної системи протидії. А також держави-члени НАТО та ЄС (з акцентом на країни Східного флангу) – як суб'єктів, що розробляють колективну відповідь та імплементують уроки українського досвіду.

Метою роботи є комплексний аналіз сутності та еволюції феномену гібридних війн як нового фундаментального виклику для міжнародної безпеки, а також систематизація та оцінка українського досвіду протидії цим загрозам для вироблення рекомендацій щодо посилення національної та колективної стійкості.

Завдання дослідження:

1. охарактеризувати джерельну базу дослідження та історіографію проблеми й з'ясувати ступінь їх дослідженості;
2. розкрити теоретичні основи та еволюцію концепції гібридної війни в контексті сучасної світової політики та воєнної стратегії;
3. визначити та класифікувати сутність, структуру та основні інструменти гібридної агресії російської федерації проти України (військові, інформаційно-психологічні, економічні, кібернетичні);
4. охарактеризувати українську систему протидії гібридним загрозам;
5. проаналізувати міжнародні стратегічні рамки (ЄС та НАТО), інституційну співпрацю та нормативно-правові й економічні інструменти, спрямовані на протидію гібридній агресії та виокремити ключові уроки для України;
6. сформулювати практичні рекомендації щодо підвищення національної стійкості та ефективності протидії гібридній агресії рф.

Методологічні засади дослідження «Гібридні війни як новий виклик для міжнародної безпеки (український досвід)» базується на комплексному, міждисциплінарному підході, що поєднує традиційні методи соціально-політичних наук, системний аналіз та спеціалізовані методи безпекових досліджень. Використання широкого спектру методів дозволило забезпечити всебічне вивчення багатовимірного феномену гібридної агресії, оцінити український досвід протидії та систематизувати міжнародні механізми реагування.

Загальнонаукові та філософські методи. На фундаментальному рівні ми застосовували філософські та загальнонаукові методи, які забезпечили структуру та логіку наукового пізнання. Зокрема, діалектичний метод використовувався для розгляду гібридної війни в динаміці її розвитку та протиріч, аналізуючи взаємодію між агресором (рф) та об'єктом агресії (Україною та міжнародною спільнотою) як постійний процес «дії-протидії» та «виклику-відповіді». Системний метод дозволив розглянути гібридну агресію не

як сукупність окремих інструментів (кібератаки, дезінформація, військові дії), а як цілісну систему скоординованих дій, спрямованих на досягнення стратегічної мети – підризу національної стійкості. Метод аналізу та синтезу використовувався для розкладання феномену гібридної війни на складові (економічна, інформаційна, військова, кібернетична) та вивчення їхніх функцій, а також дозволив інтегрувати отримані дані для формулювання цілісного уявлення про сутність гібридної загрози та шляхи її нейтралізації. Метод індукції та дедукції застосовувалася при узагальненні конкретних випадків гібридної агресії (наприклад, саботаж інфраструктури, дезінформаційні кампанії) для виведення загальних закономірностей та стратегій агресора. Дедукція використовувалася для перевірки теоретичних положень (наприклад, про ключову роль суспільної довіри) на конкретних прикладах українського та міжнародного досвіду.

Спеціальні методи соціально-політичних наук. Порівняльно-правовий метод застосовувався для зіставлення нормативно-правових актів України (Закон «Про основи національної безпеки», Воєнна доктрина) з міжнародними стратегіями (Joint Framework ЄС, політика НАТО) та національним законодавством країн-партнерів (наприклад, Латвії щодо заборони ЗМІ чи досвід СААТSA). Це дозволило виявити спільні підходи та прогалини в правовому регулюванні. Контент-аналіз та дискурс-аналіз: використовувалися для дослідження інформаційно-психологічного складника гібридної агресії. Історико-ретроспективний метод дозволив простежити еволюцію гібридних методів агресії з 2014 року до сьогодення, від «м'якої сили» та проксі-сил до повномасштабного застосування військових інструментів у поєднанні з невійськовими. Це забезпечило розуміння динаміки розвитку виклику. Прогностичний метод використовувався для формулювання обґрунтованих рекомендацій щодо подальшого посилення національної стійкості, базуючись на оцінці поточних тенденцій та можливих сценаріїв розвитку гібридних загроз.

До принципів наукового дослідження відносимо наступні: принцип об'єктивності, що передбачав неупереджений аналіз усіх джерел та фактів,

незалежно від ідеологічних чи політичних міркувань, забезпечуючи достовірність отриманих висновків; Принцип системності, який вимагав розгляду всіх елементів об'єкта дослідження (загроз, механізмів протидії) в їхньому взаємозв'язку та цілісності; Принцип історизму наполягав на вивченні гібридної війни як явища, що розвивається в часі, з урахуванням історичних передумов та еволюції; Принцип верифікованості (перевірюваності): спрямовував на використання достовірних джерел (нормативно-правові акти, офіційні звіти НАТО/ЄС, наукові публікації) та забезпечення можливості перевірки отриманих результатів.

Елементи наукової новизни дослідження:

1. уточнено сутність феномену гібридних війн як нового системного виклику, що вимагає перегляду принципів міжнародного права та колективної оборони;

2. обґрунтовано концепцію суспільної довіри як ключового чинника стійкості до гібридних загроз, інтегрованого з медіаінформаційною грамотністю (MIL) як елементом національної безпеки;

3. проаналізовано правозастосовну практику використання міжнародних актів та санкційного механізму для юридичної кваліфікації та протидії гібридній агресії;

4. систематизовано український досвід у контексті глобальних військових трансформацій;

5. розширено розуміння колективної безпеки у системі раннього виявлення загроз ЄС та НАТО.

Практичне значення дослідження полягає у тому, що його результати можуть бути використані для вдосконалення національних стратегій, зокрема Стратегії національної безпеки, з акцентом на невійськових компонентах протидії та підвищенні кіберстійкості. Також матеріали дослідження стануть інформаційною базою для поглиблення співпраці, надання військово-технічної допомоги та синхронізації санкційної політики. Вважаємо, що дослідження є цінним матеріалом для розробки навчальних курсів з міжнародної безпеки,

геополітики та стратегічних комунікацій.

Структура дослідження. Матеріал роботи викладено у проблемно-хронологічній формі. Дослідження складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і літератури (54 позиції), додатків (5). Загальний обсяг роботи становить 72 сторінки, основний зміст викладено на 61 сторінці.

ВИСНОВКИ

Встановлено, що дослідженні джерела включають низку важливих національних (закони, доктрини) та міжнародних (акти ЄС, НАТО, США) нормативно-правових документів, що дозволяє дослідити правові та політичні аспекти протидії гібридній агресії на різних рівнях. Історіографія представлена як фундаментальними монографічними працями, що осмислюють сутність гібридної війни, так і прикладними дослідженнями українських та європейських експертів щодо конкретних механізмів контрзаходів. Такий підхід забезпечує як теоретичну глибину (аналіз дискурсу гібридної війни), так і практичну значущість (оцінка ефективності військ, санкцій, МІЛ) отриманих результатів. Отже, обрана джерельна та історіографічна база повністю відповідає меті та завданням роботи і забезпечує необхідну верифікованість висновків.

Доведено, що сучасна гібридна війна є не просто сукупністю різних методів, а глибоко продуманим стратегічним інструментом, що виник як спосіб обійти неприйнятні ризики великомасштабних конвенційних конфліктів, особливо в умовах наявності зброї масового знищення. Її визначальною рисою є свідоме та навмисне розмивання юридичних і фактичних меж миру та війни (*blurring the lines*), що дозволяє агресору діяти нижче порогу прямої військової відповіді. Це досягається шляхом синхронізації військових (часто прихованих, як «зелені чоловічки») і невійськових засобів впливу, включаючи інформаційні, кібернетичні, економічні, політичні та енергетичні важелі.

Вважаємо, що успіху російського агресора на початкових етапах значною мірою сприяли системні прогалини в українському медіа-ландшафті до 2014 року: залежність від російського контенту, олігархічний контроль та інформаційна регіоналізація, що дозволило маніпулювати населенням Криму та Донбасу. Методологія агресора була гнучкою та всеосяжною, включаючи залякування, хибну логіку, маніпуляцію свідомістю через розважальні канали та використання меметичної зброї («кримнаш», «ватники») з сильним емоційним складником. Стратегічною метою ІПсО було руйнування національної

ідентичності та посилення внутрішнього розколу в Україні, зокрема через інспірування конфліктів навколо мовного та релігійного питань (використання УПЦ МП). На окупованих територіях ці операції набувають тотального характеру через блокування українського контенту, нав'язування російської освіти з «переписаною історією» та примусове громадянство. Кіберзагрози, були і в значній мірі є сьогодні, засобом кіберрозвідки (АРТ-атаки, такі як Petya-A та Black Energy), а також паралізації діяльності критичної інфраструктури (енергетичний сектор, ЦВК, держреєстри). Україна використовувалася росією як полігон для тестування новітніх шкідливих програм. Успіху цих атак сприяла технологічна залежність України (використання російського та неліцензійного ПЗ) та низький рівень кібергігієни до 2014 року. З початком повномасштабного вторгнення кібератаки стали інтенсивнішими, хоча покращення заходів кіберзахисту (діяльність CERT-UA) призвело до зниження кількості критичних інцидентів. Переконані, що економічний тиск також був важливим системним інструментом, спрямованим на консервацію енергетичної залежності (через ГТС, ядерне паливо, нафтопродукти) та контроль над ключовими економічними активами. Росія активно сприяла проникненню свого бізнесу та участі у приватизації українських підприємств, зокрема у військово-промисловому комплексі. Це створювало вразливість до дій рф з блокування імпорту та економічного шантажу. Тому гібридна агресія рф є комплексом синхронізованих ударів по військовому, інформаційному, кібернетичному та економічному вимірах, метою яких є знищення української державності.

Проаналізовано українську систему протидії гібридним загрозам, яка є комплексною, багаторівневою та динамічною, сформованою як пряма відповідь на агресію російської федерації з 2014 року. Ця модель успішно поєднує військові та невійськові засоби для захисту суверенітету та стійкості суспільства. Система ґрунтується на принципі міжвідомчої координації, де ключову роль у стратегічному плануванні та оцінці загроз виконує Рада національної безпеки і оборони (РНБО). Вона реалізує концепцію «всеохоплюючої оборони», що залучає до протидії не лише силові структури

(СБУ, ГУР, ЗСУ), а й цивільний сектор та органи місцевого самоврядування. Приділяється критична увага інформаційному простору через активну боротьбу з дезінформацією та ворожими ІПсО, а також існує потужний кіберзахисний компонент (ДССЗІ). Система є інтегрованою у міжнародний безпековий простір, що забезпечується тісною співпрацею з НАТО та ЄС для обміну даними та адаптації стандартів.

Доведено, що системний аналіз сутності гібридної агресії російської федерації підтвердив її комплексний, багатовекторний характер, спрямований на дестабілізацію України шляхом використання широкого арсеналу засобів, що діють нижче порогового рівня військового конфлікту, але мають руйнівні наслідки для національної безпеки. Було встановлено, що головною метою гібридної війни є не пряме військове завоювання як таке, а підірив національної стійкості через маніпулятивний вплив на суспільну свідомість, знищення критичної інфраструктури, дезорганізацію державного управління та ерозію довіри до інститутів влади, що унеможлиблює ефективне функціонування держави в кризових умовах. Дослідження класифікувало ключові інструменти агресора, виділивши інформаційно-психологічні операції, економічний шантаж та використання кіберпростору як основних полів для ведення нелінійних бойових дій. У відповідь на ці виклики, Україна успішно впровадила концепцію оборони, що передбачало залучення всіх секторів суспільства та держави до відсічі агресії. Це включало законодавче забезпечення та формування Військ територіальної оборони (ТрО), що забезпечило залучення до протидії невійськових компонентів, підвищивши стійкість у тилу та забезпечивши гнучкість реагування на приховані загрози. Ця модель продемонструвала свою ефективність у перші фази повномасштабного вторгнення. Критичне значення тут має розвиток медіаінформаційної грамотності (MIL) як ключового елемента ментальної стійкості. Було доведено, що MIL виступає універсальним інструментом протидії пропаганді та психологічним операціям, оскільки забезпечує індивіду навички критичного мислення та фактчекінгу, що є найсильнішим захистом від гуманітарної агресії.

З'ясовано, що на міжнародному рівні досвід України став каталізатором для розробки нових стратегічних рамок і механізмів колективної безпеки. Це виразилося в ухваленні Спільної рамкової структури ЄС у 2016 році та розширенні співпраці з НАТО у сфері кібербезпеки та стратегічних комунікацій, закріпленому у спільних деклараціях 2016 та 2018 років. Створення Hybrid CoE у Гельсінкі та Групи збору даних про гібридні загрози (HFC) в рамках EU INTSEN свідчить про глибоку інституціоналізацію міжнародної протидії та визнання багатовимірності гібридних загроз. Застосування економічних санкцій [CAATSA] та використання міжнародного права підтвердило важливість юридичних та економічних інструментів для стримування агресора, оскільки ці заходи легітимізують контрдії проти невійськових загроз. Зокрема, досвід Польщі та країн Балтії у формуванні власних Військ територіальної оборони та законодавчому обмеженні пропагандистських медіа є цінним уроком для подальшої розбудови української системи національної безпеки, зокрема у сфері енергетичної стійкості та захисту критичної інфраструктури. Ці країни також посилюють свою стійкість через від'єднання від російських енергосистем, демонструючи політичну рішучість. Водночас переконані, що довгострокова стійкість України може бути забезпечена лише шляхом інтегрованої відповіді, яка передбачає боротьбу з корупцією (останній скандал в оточенні президента Зеленського лише підтверджує реальність цієї загрози), постійну міжнародну військово-технічну підтримку, технологічну модернізацію оборонного комплексу та, що найголовніше, фундаментальне зміцнення суспільної довіри та єдності між усіма елементами держави та суспільством. Це єдиний спосіб ефективно нейтралізувати головну мету гібридної агресії – дезінтеграцію нації.

Визначено, що для підвищення національної стійкості та ефективності протидії гібридній агресії РФ необхідно зосередитися на кількох критичних напрямках. Слід негайно децентралізувати протидію дезінформації, створюючи регіональні хаби для оперативного спростування локалізованих ІІсО та посилення медіа-грамотності населення, акцентуючи на практичних навичках розпізнавання маніпуляцій. Одночасно держава має інвестувати у власне

українське контент-виробництво, яке формує позитивну національну ідентичність, замість постійної реакції на ворожі наративи. У сфері кібербезпеки критично важливим є регулярний аудит захисту об'єктів критичної інфраструктури та стимулювання розробок суверенних технологій для зменшення залежності від іноземного ПЗ. Економічна стійкість вимагає прискореної диверсифікації енергетичного сектору та підтримки бізнесу, який інвестує у резервне обладнання для швидкого відновлення роботи. Крім того, необхідно інституціоналізувати міжвідомчі оперативні команди (СБУ, РНБО, Мінцифри) для цілодобового реагування на інциденти, забезпечуючи миттєвий обмін інформацією. Слід також перетворити «Пункти Незламності» на постійні центри соціальної стійкості з можливістю надання психологічної допомоги та активізувати публічну дипломатію, щоб поширювати український досвід протидії гібридним загрозам на міжнародному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ:

1. H.R.3364 – Countering America’s Adversaries Through Sanctions Act. Library of Congress. URL: <https://www.congress.gov/bill/115th-congress/house-bill/3364/text> (дата звернення: 29.10.2025).
2. Joint communication to the European Parliament and the Council: Joint Framework on countering hybrid threats a European Union response. URL: <http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=text> (дата звернення: 29.10.2025).
3. Paris Declaration on Media and Information Literacy in the Digital Era (2014). *www.unesco.org*. Retrieved from URL: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/paris_mil_declaration.pdf [in English]. (дата звернення: 29.10.2025).
4. Воєнна доктрина України : Указ Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року “Про нову редакцію Воєнної доктрини України”» від 24.09.2015 № 555/2015. Офіційний вісник Президента України : офіц. вид. від 05.10.2015. № 22. С. 19, ст. 1291. URL: <https://zakon.rada.gov.ua/laws/show/648/2004#Text> (дата звернення: 29.10.2025).
5. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV (зі змінами та доповненнями). URL: <http://zakon2.rada.gov.ua/laws/show/964-15> (дата звернення: 31.10.2025).
6. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління*. 2024. Випуск 2(74). С. 24-31
7. Бусол О. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. №4. С. 4-15
8. Гищук Р., Жовтованюк Р., Носова Г. Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. URL: https://www.researchgate.net/publication/343300812_Gibridni_zagrozi_u_kiberprosto_ri_faktori_vplivu_na_prirodu_viniknenna/link/5f8013dba6fdccfd7b51e44c/download?

_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (дата звернення: 28.10.2025).

9. Гібридна війна під водою: загрози для Балтії й уроки для України. URL: <https://geostrategy.org.ua/media/komentari-ekspertiv/gibrydna-viyna-pid-vodoyu-zagrozy-dlya-baltiyi-y-uroky-dlya-ukrayiny> (дата звернення: 19.10.2025).

10. Гібридна війна Росії – виклик і загроза для Європи. Київ : Центр Разумкова, грудень 2016 р. С. 3-8

11. Гібридна війна, як явище. URL: http://resource.history.org.ua/cgi-bin/eiu/history.exe?Z21ID=&I21DBN=EIu&P21DBN=EIU&S21STN=1&S21REF=10&S21FMT=eiu_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=TRN=&S21COLORTERMS=0&S21STR=gibrydna_vijna (дата звернення: 19.10.2025).

12. Гібридна війна. URL: https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0 (дата звернення: 28.10.2025).

13. Гібридні загрози та комплексна безпека: навчальний посібник. Укл. Карпенко О., Осипова Є. Київ : ТОВ «ТРОПЕА», 2024. 76 с.

14. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Підготовлено за результатами досліджень в рамках проекту «Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз». За загальною редакцією В.Мартинюка (керівника проекту) Експертна група проекту: М.Гончар, А.Чубик, С.Жук, О.Чижова, Г.Максак, Ю.Тищенко, О.Зварич. Київ: 2018. 106 с.

15. Гібридні загрози: чи вистойть Україна? URL: https://yvu.com.ua/gibrydni-zagrozy-chy-vystoyit-ukrayina/#google_vignette (дата звернення: 28.10.2025).

16. Глосарій з гібридних загроз. / За ред. Гришко С.В. Харків : ХНУРЕ, 2021. URL: <https://warn-erasmus.eu/ua/glossary/> (дата звернення: 28.10.2025).

17. Дворянов В. Історичні передумови сучасного воєнного конфлікту. *Проблеми сучасних трансформацій. Серія право, публічне управління та адміністрування*. 2023. №9. С. 1-8
18. Дерев'янка С. Гібридна війна: інформаційно-безпековий вимір. *Вісник Прикарпатського університету. Серія: Політологія. Випуск 18*. 2024. С. 101-113
19. Загорулько А. Удосконалення державного управління правоохоронними органами як фактор підвищення їх ефективності в умовах гібридної війни. *Вісник національного університету цивільного захисту України. Серія «Державне управління» Збірник наукових праць*. Випуск 2 (9). С. 14-23
20. Зінченко М., Плугова О., Драглюк О. В. Інформаційна війна, засоби реалізації та протидії. *Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції*. Київ: НУОУ, 2017. С. 38-40
21. Зубченко С. Сучасний гуманітарний інструментарій протидії гібридній війні РФ проти України. *Стратегічні пріоритети*. 2017. № 4 (45). С. 207–214.
22. Ієрусалимов В. Гібридні гендерні загрози як елемент дестабілізації діяльності Верховної Ради України. *Інформаційна безпека людини, суспільства, держави*. 2019. № 2. С. 109-115
23. Концепція «гібридної» війни та її складові. URL: <https://censs.org/concept-of-hybrid-warfare-and-its-components/> (дата звернення: 19.10.2025).
24. Кравченко В. Теорія «гібридної війни»: український вимір. *Вісник Дніпропетровського університету*. 2015. № 2. С. 139-148
25. Кулініч А. Сучасні виклики міжнародним відносинам: проблема гібридної війни постмодерну». Дипломна робота. Харків : 2023. 76 с.
26. Литвиненко О. Тотальна війна по-путінські: «гібридна» війна РФ проти України. Київ : Центр Разумкова, грудень 2016 р. С. 45-49
27. Луцьок О. Гібридні війни як інструмент міжнародної політики. Бакалаврська робота. Луцьк : 2025. 45 с.
28. Маркітантов В., Рибщун О., Віннічук О.В. Російська гібридна війна: від доктрини до тактики : навчальний посібник. Вид. 2-ге, перероб. і доп.

Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 248 с.

29. Мартин ван Кревельд Онлайн книга «Трансформація війни». . URL: https://loveread.ec/read_book.php?id=44369&p=81 (дата звернення: 16.10.2025).

30. Огризко В. Мета російської агресії – знищення української державності. Київ : Центр Разумкова, грудень 2016 р. С. 19-20

31. Ониськів Ю. «Гібридна війна як форма новітнього конфлікту». Магістерська робота. Острог : 2023. 94 с.

32. Паралельні світи. URL: <https://day.kyiv.ua/article/media/paralelni-svity> (дата звернення: 19.10.2025).

33. Парахонський Б., Яворська Г. Дестабілізація Європи: гібридна війна рф. *Strategic panorama*. 2021. № 1–2. С. 5-29

34. Парахонський Б., Яворська Г. Онтологія війни і миру: безпека, стратегія, смисл : монографія . Київ : НІСД, 2019. 560 с.

35. Парубій А. Війна Росії проти України і світу. URL: <https://www.pravda.com.ua/articles/2014/08/06/7034046/> (дата звернення: 19.10.2025).

36. Плисюк Я. Гібридні війни як загроза міжнародній безпеці : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 291 Міжнародні відносини, суспільні комунікації та регіональні студії / наук. кер. Н. І. Романюк ; Волинський національний університет імені Лесі Українки. Луцьк, 2025. 60 с.

37. Погромський В. Національна безпека України в умовах гібридних загроз (2014-2024 рр.). Бакалаврська робота. Київ : 2025. 97 с.

38. Присяжнюк М. Інформаційна складова сучасних гібридних воєн. *Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції*. Київ: НУОУ, 2017. С. 68-71

39. Рева Т. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2022. Випуск 40. С. 186-191

40. Рижук О. Інформаційні та гібридні війни в глобальному інформаційному суспільстві. *Науковий журнал «ПОЛІТИКУС»*. 2017. № 5. С. 101–105.
41. Російська «гібридна» агресія в Україні та Європі: позиції і оцінки експертів. Київ : Центр Разумкова, грудень 2016 р. С. 29-36
42. Російсько-український конфлікт очима громадян (результати загальнонаціонального соціологічного дослідження). Київ : Центр Разумкова, грудень 2016 р. С. 36-45
43. Сахно Б. Інструменти ведення сучасної гібридної війни. Магістерська робота. Одеса: 2024. 101 с.
44. Світова гібридна війна: український фронт / За заг. ред. В. П. Горбуліна. Національний інститут стратегічних досліджень. Київ.: НІСД, 2017. 496 с.
45. Сидорук С. Гібридні загрози та європейська система безпеки. Бакалаврська робота. Вінниця : 2022. 60 с.
46. Смола Л. Інформаційно-психологічний складник «гібридної» війни. Київ : Центр Разумкова, грудень 2016 р. С. 53-57
47. Сучасні технології гібридної війни: практичний посібник / Ю. І. Когут; за ред. док-ра тех. наук, проф. А. С. Довгополого Київ : Консалтингова компанія «СІДКОН» ; ВД «Дакор», 2024. 368 с.
48. Уздєнова Ю. Гібридна війна: сутність, складові та ключові поняття. *Публічне управління у сфері державної безпеки та охорони громадського порядку*. 2024. Вип.35 (74). №4. С. 172-179
49. Фролов В., Саганюк Ф. Стратегія переходу в умовах гібридної війни до нового формату стратегічного керівництва сектором безпеки і оборони України. *Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського. Воєнна стратегія*. 2017. Київ. С.6-12
50. Чуб С. Міжнародні нормативно-правові засоби протидії гібридним загрозам в умовах агресії РФ проти України. *Право і державне управління*. 2022. №4. С. 257-263
51. Юрчак Ю. Науково-прагматичні аспекти гібридної війни Російської Федерації проти України. *Честь і закон*. № 3 (86)/2023. С. 80-89

52. Яворська Г. Гібридна війна як дискурсивний конструкт. *Стратегічні пріоритети*. 2016. 4(41). С. 41-48

53. Bilal, A. (30.11.2021). Hibrydna viina – novi zahrozy, skladnist i «dovira» yak antydot [Hybrid Warfare – New Threats, Complexity, and ‘Trust’ as the Antidote]. NATO Reviu – NATO review. www.nato.int Retrieved from. URL: www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html [in Ukrainian]. (дата звернення: 19.10.2025).

54. How Hybrid Warfare Could Change Asia. URL: <https://thediplomat.com/2016/06/how-hybrid-warfare-could-change-asia/> (дата звернення: 19.10.2025).