DOI 10.31558/2519-2949.2025.4.17
УДК 327.56:355.02(73)

ORCID ID: https://orcid.org/0000-0003-3586-9614
Вітман К. М., Національний університет «Одеська юридична академія»

ORCID ID: https://orcid.org/0009-0003-8252-6566
Капсамун О. Г., Національний університет «Одеська юридична академія»

ГІБРИДНА ВІЙНА В СТРАТЕГІЇ США: ПОРІВНЯЛЬНИЙ АНАЛІЗ АДМІНІСТРАЦІЙ ТРАМПА І БАЙДЕНА ТА ВИКЛИКИ XXI СТОЛІТТЯ

У статті досліджено еволюцію стратегій США щодо гібридної війни у XXI столітті та порівняно підходи адміністрацій Дональда Трампа (2017–2021 та з початку 2025–дотепер) і Джо Байдена (2021–2025). Проаналізовано ключові інструменти гібридних операцій, включно з кібернетичними атаками, інформаційними кампаніями, економічним та політичним тиском, санкціями, застосуванням нерегулярних сил та технологічно-асиметричних засобів, а також методами впливу на громадську думку. Показано, що перший термін Трампа орієнтувався на силове стримування, пріоритет національних інтересів та обмежену підтримку України, акцентуючи увагу на кібернетичній перевазі та випереджувальних заходах у «сірих зонах». Адміністрація Байдена застосовувала комплексний, коаліційний підхід із превентивним кібер- та інформаційним реагуванням, широкою підтримкою партнерів і інтеграцією багатодоменної стратегії, включно із захистом критичної інфраструктури та інформаційною стійкістю. Другий термін Трампа поєднує попередній прагматизм із новим акцентом на внутрішню безпеку, технологічну перевагу та превентивне стримування глобальних гібридних загроз, водночас обмежуючи коаліційну взаємодію. Проведено аналіз останніх досліджень та публікацій, що висвітлюють гібридну війну, інформаційні операції, кібербезпеку та роль союзників, і виділено невирішені проблеми, зокрема ефективність різних моделей,, інтеграцію технологічних інструментів і вплив новітніх технологій на гібридні конфлікти. Обґрунтовано, що американська стратегія гібридної війни XXI століття розвивається у напрямку комплексності, адаптивності та технологічної переваги, поєднуючи військові, економічні, інформаційні та дипломатичні інструменти. Це дозволяє США ефективно реагувати на «сіро-зонні» конфлікти, підтримувати стратегічну перевагу у глобальному масштабі та координувати дії з союзниками. Окремо висвітлено роль України у стратегіях протидії гібридним загрозам і особливості технологічного та інформаційного стримування Китаю та росії. Вказано перспективи подальших досліджень у сфері багатодоменної протидії, ролі коаліцій і союзників, а також впливу новітніх технологій, штучного інтелекту і соціальних мереж на розвиток і нейтралізацію гібридних загроз.

***Ключові слова**: гібридна війна, США, кібербезпека, інформаційні операції, стратегія національної безпеки, «сірозонні» конфлікти, коаліційна взаємодія, технологічне стримування, Україна, глобальна безпека.*

Постановка проблеми. Гібридна війна стала центральним елементом сучасної міжнародної безпеки. Для США вона набуває особливого значення в контексті глобальної конкуренції з росією, Китаєм та іншими суб'єктами міжнародних відносин. Наукова проблема полягає у недостатньому аналізі еволюції підходів американської адміністрації до гібридних загроз, зокрема в порівнянні стратегій Дональда Трампа та Джо Байдена, з урахуванням другого терміну Трампа. Практичне значення дослідження полягає у формуванні ефективних моделей реагування на гібридні загрози, що включають комплексну взаємодію із союзниками, інформаційне стримування, кіберзахист та економічні санкції, а також у підвищенні готовності держав до «сірозонних» конфліктів і цифрових загроз.

Метою статті є всебічний аналіз гібридного виміру національної безпеки США, порівняння

підходів адміністрацій Д. Трампа (першого та другого термінів) та Дж. Байдена, виявлення принципових відмінностей у стратегіях протидії гібридним загрозам, а також дослідження практичних кейсів, зокрема щодо України, кібербезпеки та взаємодії зі стратегічними союзниками.

Аналіз останніх досліджень і публікацій. У науковій літературі останніх років гібридна війна розглядається як складне мультидоманне явище. Так, М. Гері, Д. Солен, Л. Сперанца досліджують ключові вектори гібридних загроз для США (перш за все, з боку рф та Китаю). М. Вайсманн, М. Малік, М. Салім, А. Хаквані та інші розробляють концептуальні моделі гібридних загроз і їхнього нейтралізації у «сірих зонах» конфліктів. О. Брусиловська досліджує гібридну стратегію адміністрації Трампа у контексті реконфігурації світового устрою, висвітлюючи прагматичні та технологічні аспекти протидії глобальним загрозам. Аналіз кейсів України проводять М. Павлунько, О. Посмітюх, О. Салій, С. Тищук та інші, які оцінюють вплив комплексної американської підтримки на протидію російським гібридним атакам. У цих дослідженнях акцент зроблено на стратегічному плануванні, координації з союзниками, кібербезпеці та інформаційній протидії, що створює фундамент для порівняльного аналізу адміністрацій США.

Виділення невирішених раніше частин проблеми. Незважаючи на численні дослідження, залишаються відкритими питання щодо порівняльного ефекту різних адміністрацій США у протидії гібридним загрозам: наскільки ефективним є трансформаційний підхід Байдена у порівнянні з прагматично-транзакційним підходом Трампа, які механізми «whole-of-government» працюють у різних контекстах, як змінюється роль союзників і стратегічних партнерів, і який вплив ці стратегії мають на практичні кейси, такі як протидія рф в Україні та стримування Китаю в Азіатсько-Тихоокеанському регіоні. Також недостатньо проаналізовані аспекти гібридної стратегії другого терміну Трампа, особливо у сфері кіберзахисту, економічних інструментів та управління інформаційними операціями.

Виклад основного матеріалу. Гібридна війна на початку XXI століття стала одним з ключових викликів для Сполучених Штатів, що змусило Вашингтон докорінно переглянути військово-стратегічне мислення й оновити національну систему безпеки. Дослідники відзначають, що феномен гібридної війни більше не є периферійною проблемою, а визначає «тотальну конкуренцію» між великими державами, у якій інформаційні операції, кібердії, підрив критичної інфраструктури, економічний тиск і політичні диверсії стають важливішими, ніж класичні бойові дії [13; 24; 30; 31]. Стратегія США, починаючи з президентства Барака Обами і особливо після 2014 року, еволюціонувала від розуміння гібридних загроз до комплексного концепту протидії мультидоменним операціям росії, Китаю, Ірану та недержавних акторів.

У цьому контексті порівняння стратегічних підходів адміністрацій Дональда Трампа і Джо Байдена дозволяє пояснити, як США розгортають інструменти гібридної війни, якими загрозами оперують та які механізми обирають для стримування противників. Аналіз цих доктрин демонструє не лише різницю у риториці, а й відмінності у концептуальних моделях: від «примату національних інтересів» у Трампа до «коаліційної протидії» та інституційної стійкості у Байдена, а потім силового реалізму у Трампа за другого терміну його президентства.

Варто зазначити, що сучасні підходи до гібридної війни охоплюють широкий спектр інструментів: від інформаційних і психологічних операцій до кібернетичних атак та маніпуляції демократичними процесами [4; 5; 11]. Серед її ключових інструментів: кібероперації (проти критичної інфраструктури, систем зв'язку, інформаційних мереж); дезінформація, вплив на громадську думку, інформаційні кампанії; економічні санкції, торговельний та фінансовий тиск; політичний, дипломатичний вплив, маніпуляції через «треті сторони» тощо. Політичні актори застосовують комбінації вищенаведених інструментів залежно від мети, для дестабілізації, шантажу, зміни політики, підриву довіри до інститутів. Гібридність розуміється як комбінація регулярних і нерегулярних методів, що створюють стратегічну невизначеність та унеможливлюють однозначну ідентифікацію нападу [29; 32]. Це – «сіра зона», де домінують конкуренція, відмова від офіційної ескалації й системне тестування вразливостей супротивника [9; 31].

Гібридна війна для США часто означає не лише реагування на зовнішні загрози, а й посилення власної кібербезпеки, захист демократії, координацію з союзниками, створення нових форм оперативної відповіді. У національних стратегічних документах останнього десятиліття гібридні загрози розглядаються як ключовий інструмент ревізіоністських держав, що прагнуть підірвати світовий порядок, заснований на правилах. Кібероперації проти критичної інфраструктури, вплив на виборчі процеси, інформаційно-психологічні атаки, маніпуляції енергетичними ресурсами та

використання приватних військових компаній – усі ці методи стали невід'ємною частиною конфліктів нового покоління.

На даний час критичними для США залишаються три вектори гібридної загрози: російські інформаційні та військово-спеціальні операції (дезінформаційні кампанії, втручання у вибори, операції ГРУ та спецслужб рф) [2; 8]; китайські мультидоменні стратегії (промислова розвідка, кібероперації, вплив в інфосфері, «legal warfare» і «public opinion warfare» [25; 26]; іранські та північнокорейські кіберзагрози (атаки на інфраструктуру, криптофінансування операцій, хакерські групи APT) [10]. Усі вони лягли в основу офіційних документів США, включно з Національною стратегією безпеки 2025 року [19], прийнятою в листопаді цього року, яка фіксує гібридну війну як ключовий вимір глобальної конкуренції.

Гібридна війна у стратегії Сполучених Штатів за Дональда Трампа (при першому терміні його президенства) сформувалася як відповідь на усвідомлення того, що глобальне безпекове середовище остаточно втратило біполярну логіку. З приходом Трампа до влади у 2017 році у стратегічному мисленні США домінуючими стали категорії конкуренції великих держав та ревізіоністського тиску, який здійснюють противники у «сірій зоні». Національна стратегія безпеки США 2017 року [18], яку аналітики Німецького фонду Маршалла Сполучених Штатів (далі – GMF) називають найбільш «конкурентною» за риторикою з часів холодної війни, визначила росію та Китай «державами, що прагнуть переосмислити міжнародний порядок» шляхом використання кібернетичних, інформаційних, економічних, політичних і нерегулярних інструментів [28]. Порівняно з попередніми адміністраціями, документ не лише констатував факт гібридної діяльності противників, але й інтегрував цей феномен у саму структуру стратегічного планування. До основних положень Стратегії 2017 року щодо гібридних загроз можна віднести: вперше офіційне визначення росії та Китаю, як держав, що здійснюють довготривалу конкуренцію у «сірих зонах», застосовуючи методи, які не досягають порогу відкритої війни; опис рф як держави, що використовує дезінформацію, кібератаки, енергетичний шантаж та військових найманців для підриву демократичних інститутів; акцент уваги на зростанні «постійного простіру стратегічного суперництва», де комбінуються такі інструменти тиску, як кібероперації, економічні санкції, інформаційні кампанії [18].

Значна увага в документі приділяється кібербезпеці, а кіберпростір визначається як головний домен сучасного конфлікту, у якому держави змішують шпигунство, викрадення даних і саботаж. Вперше на рівні стратегічного документу проголошено завдання досягти домінування США в кіберпросторі. Для цього кіберкомандування США отримало розширений мандат на проведення наступальних операцій, що дозволило здійснювати превентивні дії. Розширення кібероперацій мало на меті не просто відбивати атаки, а створювати постійний тиск на російські, китайські та іранські мережеві структури, демонструючи здатність США проникати у системи супротивників та нейтралізовувати загрози до того, як вони матимуть шанси реалізуватися. Крім того, в документі окремо зазначено, що США мають підтримувати країни, які стикаються з російською агресією (включно з Україною) через зміцнення кіберзахисту, протидію інформаційним операціям і розвиток оборонних можливостей.

Другим важливим документом стала Стратегія національної оборони 2018 року [27], яка фактично оголосила кінець ери боротьби з тероризмом як головним пріоритетом, змістивши акцент на конкуренцію з росією та Китаєм, які застосовують гібридні інструменти. Стратегія описує тривале змагання, де США повинні діяти не реактивно, а проактивно: відбивати, стримувати та карати гібридні атаки супротивника. В документі підкреслено, що майбутні конфлікти розгортатимуться у мультидоменному просторі, де кібер- та інформаційні впливи будуть вирішальними, тому США визнають необхідність протидії цілеспрямованим кібератакам на військову інфраструктуру.

У 2018 році також було прийнято Огляд ядерної політики, який також містить положення щодо гібридних загроз. В документі вперше визнається, що ядерний стримувальний потенціал США має враховувати можливість гібридних сценаріїв ескалації, а росія звинувачується у стратегії, яка може включати конвенційні гібридні атаки з подальшою загрозою ядерного застосування. У документі зазначено, що рф комбінує звичайні сили, кібератаки та інформаційні операції, формуючи «непрямі та приховані інструменти» впливу на сусідів (перш за все на Україну) [22].

Ще один документ – Національна кіберстратегія США 2018 року [16], яка визначає завдання діяти превентивно, а не лише реагувати на загрози. Крім того, вона відзначає, що кібер- та інформаційні атаки повністю інтегровані у стратегії росії та Китаю щодо підриву політичної стабільності союзників США. В Стратегії зазначено, що кібероперації здатні зупинити військові системи, зламати критичну

інфраструктуру, впливати на громадську думку через інформаційні маніпуляції.

У 2019 році прийняті Стратегічні рамки Міністерства національної безпеки США (DHS) щодо боротьби з тероризмом та цілеспрямованим насильством [6], де мова йде про внутрішні гібридні загрози. В офіційній стратегії вперше зазначено, що США стикаються з такими загрозами, вони поєднують радикалізацію, онлайн-маніпуляції і зовнішнього втручання у суспільні процеси. Окремий розділ документу присвячений дезінформації та опису іноземних операцій впливу у США, зокрема російські кампанії, що експлуатують соціальні розколи.

Отже, значної уваги на першому терміні президентства Трампа було приділено інформаційним операціям. Адміністрація виокремила їх як основний інструмент російської та китайської стратегії, звертаючи увагу на комплексність цих операцій: від маніпуляцій у соціальних мережах до використання медіаплатформ, «фабрик думок» і локальних політичних акторів для впливу на політичний процес. У звітах аналітичних центрів (Центру стратегічних та міжнародних досліджень (далі – CSIS) [10] і GMF [28] наголошувалося, що Трампівська стратегія поставила перед США завдання не лише «реагувати на дезінформацію», але й системно змінювати архітектуру інформаційної безпеки, зміцнюючи взаємодію держави з приватним сектором, який володіє основними цифровими платформами. Саме за президенства Трампа розпочалася формалізація нового режиму співпраці між урядом і соціальними мережами у виявленні іноземних операцій впливу, що стало основою для того, як США реагували на гібридні втручання під час виборів 2020 та 2024 років.

Адміністрація Трампа (2017-2021 рр.) також системно акцентувала увагу на зростанні ролі економічних інструментів у гібридній війні. Санкції проти росії (хоча й менш масштабні, ніж у період Байдена) були посилені щодо ключових підприємств оборонного комплексу, експорту технологій та фінансового сектору. У дослідженнях аналітичних центрів зазначається, що саме за Трампа відбулася переорієнтація санкцій: замість широких секторальних обмежень адміністрація почала використовувати точкові технологічні санкції, які обмежували доступ рф до високотехнологічних компонентів подвійного призначення. Ці санкції були пов’язані з розумінням того, що майбутня війна є гібридною по суті та значною мірою залежатиме від можливостей країни виробляти системи управління, сенсори, електроніку та безпілотні технології. Підхід Трампа до України у 2017–2020 роках був двояким і часто інтерпретується дослідниками як прояв прагматичного реалізму. З одного боку, адміністрація підтримувала санкційний тиск проти рф та дозволила постачання летальної зброї оборонного типу (зокрема ПТРК Javelin). З іншого боку, Трамп не вважав Україну ключовим пріоритетом і розглядав конфлікт навколо неї як периферійний для національних інтересів США. Деякі американські дослідники трактують це як прагнення уникати надмірного залучення у конфлікти, які не мають прямого впливу на американську безпеку, але потребують значних ресурсів [1; 2]. Разом із тим саме у цей період США почали системно аналізувати російські гібридні операції в Україні як модель можливих дій проти західних держав, що заклало основу для подальшої уваги Вашингтона до гібридних загроз.

Президентство Джо Байдена ознаменувалося радикально іншим підходом до гібридних загроз порівняно з Трампом. У стратегії адміністрації Байдена ключовими стали концепти «союзництва та колективної безпеки», «глобальної демократії» та «стійкої економіки», що безпосередньо впливало на підходи до гібридної війни. На відміну від прагматичного, транзакційного стилю Трампа, адміністрація Байдена орієнтувалася на багаторівневу координацію з союзниками НАТО, ЄС, партнерами у Азії та Африці [7]. Це означало, що гібридні загрози, зокрема російська дезінформація чи кібератаки, розглядались не лише як виклики національної безпеки США, а як загроза глобальній архітектурі безпеки, яку необхідно нейтралізувати колективно. Водночас адміністрація активно розвивала концепт «whole-of-government», що передбачав залучення цивільного, військового, розвідувального та економічного блоків для протидії гібридним операціям.

Американські стратегічні документи часів адміністрації Байдена приділяють особливу увагу гібридним, кібернетичним та «сірозонним» загрозам, підкреслюючи їхню системність і зростаючу складність. У Стратегії національної безпеки США 2022 року наголошується, що Сполучені Штати зіштовхуються з постійними та еволюціонуючими гібридними загрозами, які поєднують кібератаки, інформаційні операції та економічний тиск з метою підриву демократичних інститутів і суспільної стійкості держав-партнерів [20]. Такий підхід демонструє усвідомлення Вашингтоном того, що сучасні конфлікти розгортаються переважно поза межами традиційного військового протистояння.

Україна стала ключовим кейсом для відпрацювання цієї моделі. На відміну від Трампа, Байден не обмежувався постачанням летальної зброї: у 2021–2025 роках США інвестували значні ресурси у

модернізацію систем ППО, кіберзахисту, розвідки та фінансових механізмів протидії рф. Поставки HIMARS, удосконалені розвідувальні можливості та навчальні програми для українських військових дозволили не лише відбивати атаки, а й проводити комплексні превентивні операції. Особливо важливою була координація інформаційної політики: американські структури разом з союзниками формували єдині інформаційні повідомлення, контратакуючи російські кампанії дезінформації, включно з фейками про нібито «американську експансію» чи «зовнішнє втручання в конфлікт на Донбасі». Ці заходи визнані дослідниками прикладом «глобальної моделі гібридного стримування», де США застосовують одночасно політичні, економічні, кібернетичні та інформаційні інструменти, не залучаючи безпосередньо регулярні сили у конфлікт [2; 3].

Іншим ключовим компонентом стала кіберстратегія. У Стратегії національної безпеки США 2022 підкреслюється, що кіберпростір став одним з ключових доменів сучасної конкуренції. Захист критичної інфраструктури визначається як пріоритет, оскільки супротивники використовують кібервплив для формування політичних результатів, дестабілізації економічних систем та підриву суспільної довіри [20]. Одночасно акцентується увага на інформаційній безпеці: «ворожі інформаційні операції намагаються експлуатувати соціальні розколи шляхом кампаній дезінформації та маніпуляцій онлайн, ставлячи під загрозу цілісність відкритих суспільств» [20]. У контексті України ці положення знайшли своє відображення у програмній підтримці протидії російським інформаційним впливам та забезпеченні стійкості до дезінформації.

Адміністрація Байдена ввела новий стандарт реагування на кіберзагрози, розглядаючи їх як елемент гібридної війни рівноцінно військовим операціям. Після масованих атак на американські держструктури та приватні корпораці та активних спроб втрутитися у вибори 2020 року, США офіційно сформулювали політику превентивних кіберударів у відповідь на гібридну агресію, що поєднує технологічну оборону, превентивне проникнення у системи противника та координацію з приватним сектором. Особливо акцент зроблено на захист критичної інфраструктури та енергетичних систем, включно з транспортом та телекомунікаційними мережами [14; 15; 23].

У Стратегії національної безпеки США 2022 чітко сформульованою є доктрина коаліційності, відповідно до якої посилення колективної стійкості разом з НАТО, ЄС та іншими партнерами підсилює здатність стримувати та відповідати на гібридну агресію в Європі, Індо-Тихоокеанському регіоні та за їх межами [20]. Це закладає основу для трансформації підходів США до системної взаємодії з Україною, зокрема у сферах кіберзахисту, обміну розвідданими та підтримки критичної інфраструктури. У Стратегії національної оборони 2022 року гібридний вимір безпеки розкрито ще ширше. Документ визначає, що національна оборона має адаптуватися до середовища багатодоменної конкуренції, де супротивники діють «нижче порогу збройного конфлікту» («below the threshold of military conflict») в так званій «сірій зоні», оперуючи одночасно у кібер-, інформаційному, космічному та традиційних доменах [17]. Міністерство оборони США підкреслює необхідність інтеграції різних типів спроможностей, зокрема кібернетичних, космічних, інформаційних та звичайних засобів для протидії спробам супротивників експлуатувати вразливості у політичних, економічних та соціальних системах союзників [17]. Кібероборона розглядається як складова активного превентивного стримування. Це повністю корелює з тими інструментами, які Пентагон і Агентство з кібербезпеки та інфраструктурної безпеки (CISA) застосовують у співпраці з Україною після 2022 року, зокрема щодо захисту енергетичних систем, урядових мереж та військової комунікації. Документ також підкреслює важливість союзницької взаємодії та визначає, що пріоритетом є формування сумісних оборонних спроможностей для протидії сіро-зонним загрозам, адже згуртованість партнерів підсилює стримування та стійкість [17]. У контексті України цей підхід втілюється також через підтримку НАТО у формуванні стійкості критичної інфраструктури, спільні навчальні програми та розширення співпраці у сфері кіберобміну.

Глобальна конкуренція з Китаєм стала ще одним полем гібридної війни. Байденська адміністрація поєднувала економічні санкції, технологічні обмеження, дипломатичний тиск та інформаційні кампанії для протидії впливу Пекіна. Важливим елементом була координація дій з союзниками у сфері безпеки Тайваню, що включала не лише військові гарантії, а й превентивне блокування спроб Китаю впливати на міжнародні медіа та соціальні платформи. Такі операції характеризуються як «сірозонні», бо Китай уникає прямої агресії, використовуючи гібридні інструменти: економічний тиск, кібероперації, інформаційні кампанії та дипломатичні маніпуляції.

У сфері внутрішньої безпеки США Байден акцентував на комплексній протидії дезінформації та кібератакам, що потенційно можуть впливати на демократію. Під час виборів 2022 та 2024 років було

розгорнуто інтегровану систему моніторингу цифрових загроз, що включала співпрацю ФБР, DHS, приватних ІТ-компаній і громадських організацій. Ця система дозволила не лише виявляти координаційні кампанії зовнішніх акторів, а й формувати протидію у режимі реального часу, блокуючи спроби впливу на політичний процес через соціальні мережі, фейкові акаунти та маніпулятивний контент. Особливе значення адміністрація надавала міжнародним коаліціям. У рамках НАТО та співпраці з ЄС США активно впроваджували стандарти протидії гібридним загрозам: обмін розвідданими, спільні навчання, розвиток кіберстійкості, узгодження інформаційних кампаній. Наприклад, у 2023 році НАТО ініціювала навчання у Балтійському регіоні, імітуючи атаки на критичну інфраструктуру та кібероперації, що відображає практичне застосування концепції «сірозонних конфліктів» [13]. Водночас США розширювали участь союзників у глобальному стримуванні росії, використовуючи Україну як полігон для тестування та демонстрації гібридних стратегій. Економічні інструменти Байден теж інтегрував у гібридну стратегію, застосовуючи санкції не лише проти держав-агресорів, а й проти окремих компаній та технологічних ланцюгів. Це дозволяє одночасно нейтралізувати загрозу і посилити партнерство зі стратегічними союзниками, адже санкційна політика узгоджується з європейськими та азійськими партнерами. Окремо відзначається роль фінансових та енергетичних обмежень як засобів непрямого впливу, що змушують держави-агресори коригувати поведінку без відкритого військового протистояння.

Таким чином, стратегічні документи адміністрації Байдена формують цілісне розуміння гібридної війни як поліструктурного явища, у якому інформаційні, кібернетичні та економічні впливи є ключовими засобами держав-конкурентів. Їх інтеграція в загальнонаціональну систему безпеки, пріоритет коаліційної взаємодії та акцент на стійкості критичної інфраструктури визначають сучасну траєкторію американської політики протидії гібридним загрозам.

Починаючи з січня 2025 року, адміністрація Дональда Трампа (другого терміну) суттєво переосмислила гібридну стратегію США, опублікувавши оновлену Національну стратегію безпеки 2025 року [19], яка поєднує принципи «America First» з новим усвідомленням глобальних гібридних загроз. Гібридний вимір американської стратегії змінився відповідно до його ширшої зовнішньополітичної лінії, яка передбачала скорочення міжнародних зобов'язань, переформатування участі США в альянсах і посилення внутрішнього пріоритету безпеки. У цій логіці гібридна війна розглядається не як глобальна відповідальність США, а як інструмент захисту національних інтересів з мінімізацією зовнішніх витрат. Аналітики CSIS відзначають, що у 2025 році адміністрація робить ставку на «асиметричні відповіді» у кіберсфері, спрямовані проти Китаю та Ірану, тоді як європейський напрям, включно з Україною, отримує менш пріоритетну, більш транзакційну увагу [10]. Водночас кіберкомандування США отримує розширений мандат на операції «в глибокому полі», що дозволяє здійснювати точкові атаки на інфраструктури противників без оголошення цих операцій публічно. Адміністрація прагне обмежити участь США у глобальних військових місіях, переорієнтовуючи ресурси з Європи на Тихоокеанський регіон, що відображає стратегічний перегляд пріоритетів у контексті зростаючого тиску Китаю та потенційних мультидоменних конфліктів. Цей підхід узгоджується з висновками С. Аббаса [4], М. Вайсманна, Н. Нільссона та Б. Палмерца [21] про необхідність асиметричних та технологічно орієнтованих відповідей на гібридні загрози.

Гібридний вимір стосується і НАТО: адміністрація Трампа продовжує лінію тиску на союзників щодо збільшення оборонних витрат, при цьому більше покладаючись на індивідуальні домовленості з ключовими державами, ніж на внутрішні механізми Альянсу. Це створює новий контекст для гібридної політики США, оскільки зменшення уваги до колективних структур підвищує роль двосторонніх операцій у сфері кіберзахисту, боротьби з дезінформацією та контрвпливових заходів. У кіберсфері Трамп концентрується на превентивних та випереджувальних заходах: активне проникнення у мережі потенційних противників, блокування кібератак і посилення координації з приватним сектором для захисту критичних систем. Інформаційна складова гібридної стратегії передбачає моніторинг соціальних мереж, боротьбу з дезінформацією та управління наративами, що дозволяє запобігати впливу зовнішніх акторів на внутрішній політичний процес і суспільну думку. Особлива увага приділяється кіберстійкості та оперативному обміну розвідувальною інформацією із союзниками, що створює умови для своєчасного реагування на загрози в «сірих зонах».

Щодо Китаю, Трамп обирає жорстку лінію, застосовуючи інструменти економічної та технологічної гібридної боротьби: введення обмежень на критичні технології, контроль інвестицій і блокування китайських цифрових платформ. Ці заходи відповідають оцінкам експертів [25] про підготовку Китаю до мультидоменних гібридних конфліктів і свідчать про прагнення США зупинити

стратегічну експансію Пекіна без відкритого військового протистояння. Російський напрям за другого терміну президентства Трампа отримує більш транзакційний характер: США залишаються готовими підтримувати кіберстійкість України, забезпечувати санкційний тиск на рф і взаємодіяти з союзниками у рамках НАТО, але обсяги військової допомоги періодично переглядаються, що створює стратегічну невизначеність і змушує партнерів адаптувати власну політику. Такий підхід демонструє прагматизм адміністрації, яка намагається балансувати між стримуванням рф та обмеженням зовнішніх ресурсних витрат [1]. Особливої ваги набуває цифровий вимір гібридного протистояння. Після подій виборів 2024 року США активізують операції з виявлення китайських і російських цифрових мереж, які намагаються впливати на внутрішній американський дискурс. Масштабні кампанії з використанням deepfake-технологій, які вплинули на інформаційне середовище виборів, стають підставою для глибшого реформування інформаційної політики, включно з регулюванням платформ штучного інтелекту. Трампівська адміністрація при цьому робить акцент на партнерстві з ІТ-корпораціями, очікуючи від них більшої відповідальності у сфері безпеки.

Різниця ж між підходами двох президентів США полягає у пріоритетах, інструментах та стратегічній логіці: Трамп будує модель силового стримування та національної самозахищеності, з обмеженим зовнішнім залученням, тоді як Байден формував широкомасштабну коаліційну систему гібридної оборони, орієнтовану на запобігання, стійкість і багатодоменно інтегровані дії. У результаті американська стратегія протидії гібридним загрозам у період Трампа має більш реактивний і силовий характер, тоді як у період Байдена більш системний, комплексний і координаційний.

Висновки і перспективи подальших розвідок. Стратегія США щодо гібридної війни у XXI столітті еволюціонувала від фрагментарного підходу до комплексної системної доктрини, що інтегрує військові, кібернетичні, економічні та інформаційні інструменти у національну безпеку. Перший термін Трампа (2017–2021) орієнтувався на силове стримування, пріоритет національних інтересів і обмежену допомогу Україні через технології та санкції. Адміністрація Байдена (2021–2025) змінила логіку: протидія гібридним загрозам відбувалась через глобальні коаліції, комплексну підтримку України, кіберзахист та інформаційне стримування, застосовуючи «whole-of-government» підхід. Другий термін Трампа (з 2025) поєднує попередній прагматизм із системним усвідомленням гібридних загроз, фокусуючись на внутрішній безпеці, кіберзахисті, технологічній перевазі та випереджувальному стримуванні, хоча коаліційна взаємодія обмежена. Новий підхід Трампа підвищує здатність протистояти «сіро-зонним» загрозам. Посилення контролю критичної інфраструктури відповідає сучасним викликам, хоча обмежена інтеграція з союзниками знижує ефективність глобального стримування. Швидкість рішень і автономність дій роблять цей підхід ефективним у «сірих зонах» за мінімальної координації з партнерами. Подальші дослідження мають зосередитися на інтеграції багатодоменної протидії, ролі союзників і коаліцій, а також впливі новітніх технологій, штучного інтелекту та соціальних мереж на розвиток і нейтралізацію гібридних загроз.

Бібліографічний список:

1. Брусиловська О. І. Гібридна стратегія адміністрації Д. Трампа у контексті реконфігурації світового устрою. *Міжнародні та політичні дослідження*. 2019. № 32. С. 13-26. https://doi.org/10.18524/2304-1439.2019.32.173834

2. Павлунько М., Посмітюх О., Тищук С., Салій О., Смольков О. *«Гібридна війна» – сучасна стратегія Російської Федерації в збройній агресії проти пострадянських держав та України. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* 2022. № 3(76). С. 18-23. https://doi.org/10.33099/2304-2745/2022-3-76/18-23

3. Тригуб О. П., Місяць М. Феномен гібридної війни в українській та зарубіжній політології. *Наукові праці. Політологія*. 2019. Випуск 312. Том 324. С. 66-70. https://politics.chdu.edu.ua/article/view/200683

4. Abbas S. R. The Emergence of Hybrid Warfare and the Future of Global Security: a comparative study of Russian and NATO's hybrid infrastructure in Ukraine. *Journal of politics and development*. 2025. Vol. 15(2). P. 198-211. *PhilArchive*. https://philarchive.org/archive/ABBTEO-13

5. Caliskan M. Hybrid Warfare through the Lens of Strategic Theory. *Defense and Security Analysis*. 2019. № 35(1). P. 40-58. https://doi.org/10.1080/14751798.2019.1565364

6. DHS Strategic Framework for Countering Terrorism and Targeted Violence. 2019. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

7. Genini D. Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*. 2025. №33(18). https://doi.org/10.1177/2336825X251322719

8. Geri M. Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future 'energy-resources-climate' security nexus. *Journal of Strategic Security*. 2024. Vol. 17, No. 3. P. 15-34.

https://www.jstor.org/stable/48793907

9. Gregg H. S. Hybrid Threats and Strategic Competition. *The Quarterly Journal Connections*. 2024. № 2. P. 159-171. https://doi.org/10.11610/Connections.23.2.01

10. Harding E. The National Security Strategy: The Good, the Not So Great, and the Alarm Bells. December 5, 2025. *Center for Strategic and International Studies*. https://www.csis.org/analysis/national-security-strategy-good-not-so-great-and-alarm-bells

11. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. *Potomac Institute for Policy Studies*, 2007. www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

12. Hybrid Warfare Reference Curriculum. Volume I / Edited by Z. Jobbágy, E. Zsigmond. Budapest, 2024. 202 p. https://csnsc.uk/wp-content/uploads/2024/06/2022_Hybrid_warfare_reference_curriculum_volume_I.pdf

13. Khakwani A., Saleem M. Malik M. M. Hybrid Warfare, Grey Zone Conflicts, and the Battle of Narratives: Discourse as a Strategic Weapon. *Social Prism*. 2025. № 2(2). P. 1-14. https://doi.org/10.69671/socialprism.2.2.2025.37

14. Li T., Pan Yu., Zhu Q. Decision-Dominant Strategic Defense Against Lateral Movement for 5G Zero-Trust Multi-Domain Networks (October, 2, 2023). *arXiv.org e-Print archive.* https://doi.org/10.48550/arXiv.2310.01675

15. Minici M., Luceri L., Cinus F., Ferrara E. Uncovering Coordinated Cross-Platform Information Operations Threatening the Integrity of the 2024 U.S. Presidential Election Online Discussion (September 20, 2024). *arXiv.org e-Print archive*. https://doi.org/10.48550/arXiv.2409.15402

16. National Cyber Strategy of the United States of America. September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

17. National Defense Strategy. 2022. 80 p. *U.S. Department of War*. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf

18. National Security Strategy of the United States of America. December 2017. 68 p. *The White House* https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

19. National Security Strategy of the United States of America. November 2025**.** *The White House*. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

20. National Security Strategy of the United States of America. October 2022. *The White House*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

21. Nilsson N., Weissmann M., Palmertz B. P. Hybrid Threats and the Intelligence Community: Priming for a Volatile Age. *International Journal of Intelligence and CounterIntelligence*. 2025. № 39. P. 109-131. https://doi.org/10.1080/08850607.2024.2435265

22. Nuclear Posture Review. FEBRUARY 2018. *U.S. Department of War*. https://media.defense.gov/2018/Feb/02/2001872877/-1/-1/1/2018-Nuclear-Posture-Review-Report.pdf

23. Orleans-Bosomtwe P.K. Critical Infrastructure Security: Penetration Testing and Exploit Development Perspectives (July, 24, 2024). *arXiv.org e-Print archive.* https://doi.org/10.48550/arXiv.2407.17256

24. Person R., Kulalic I., Mayle J. Back to the future: the persistent problems of hybrid war. *International Affairs.* 2024. Vol. 100, Issue 4. P. 1749–1761. https://doi.org/10.1093/ia/iiae131

25. Solen D. *Fight Fire with Fire: The PLA Studies Hybrid Warfare.* China Aerospace Studies Institute. 2022. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2022-03-23%20Fight%20Fire%20with%20Fire.pdf

26. Speranza L. A Strategic Concept for Countering Russian and Chinese Hybrid Threats. Atlantic Council, Scowcroft Center for Strategy and Security, 2020. 28 p. https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Strategic-Concept-for-Countering-Russian-and-Chinese-Hybrid-Threats-Web.pdf

27. Summary of the National Defense Strategy. Sharpening the American Military's Competitive Edge. 2018. *U.S. Department of War*. https://media.defense.gov/2020/May/18/2002302061/-1/-1/1/2018-NATIONAL-DEFENSE-STRATEGY-SUMMARY.PDF

28. The Trump Administration's National Security Strategy / A. de Hoop Scheffer, D. Kliman, B.S. Glaser etc. 2025. *German Marshall Fund of the United States*. https://www.gmfus.org/news/trump-administrations-national-security-strategy

29. Värk R. Legal Complexities in the Service of Hybrid Warfare. *Kyiv-Mohyla Law & Politics Journal.* 2020. № 6. P. 27-43. https://doi.org/10.18523/kmlpj220732.2020-6.27-43

30. Weissmann M. Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. *Hybrid Warfare / M. Weissmann, N. Nilsson, B. Palmertz and P. Thunholm.* Tauris, 2021. P. 61-82. https://doi.org/10.5040/9781788317795.0011

31. Weissmann M. Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*. 2019. № 5(1). P. 17-26. *Center for Security Studies*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC_2_23829230%20-%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20and%20hybrid%20threats%20today%20and%2

0tomorrow_%20towards%20an%20analytical%20framework.pdf

32. Załęski K. *Hybrid warfare as a strategic tool for shaping policy of the Russian Federation.* Humanities and Social Sciences. 2020. Vol. XXV, 27 (1/2020). P. 109-122. https://czasopisma.prz.edu.pl/hss/article/view/42/27

Referenses:

1. Brusy`lovs`ka, O. I. (2019). Gibry`dna strategiya administraciyi D. Trampa u konteksti rekonfiguraciyi svitovogo ustroyu. *Mizhnarodni ta polity`chni doslidzhennya*, 32, 13-26. https://doi.org/10.18524/2304-1439.2019.32.173834

2. Pavlun`ko, M., Posmityux, O., Ty`shhuk, S., Salij, O., Smol`kov, O. (2022). «Gibry`dna vijna» – suchasna strategiya Rosijs`koyi Federaciyi v zbrojnij agresiyi proty` postradyans`ky`x derzhav ta Ukrayiny`. *Zbirny`k naukovy`x pracz` Centru voyenno-strategichny`x doslidzhen` Nacional`nogo universy`tetu oborony` Ukrayiny` imeni Ivana Chernyaxovs`kogo*, 3(76), 18-23. https://doi.org/10.33099/2304-2745/2022-3-76/18-23

3. Try`gub, O. P., Misyacz`, M. (2019). Fenomen gibry`dnoyi vijny` v ukrayins`kij ta zarubizhnij politologiyi. *Naukovi praci. Politologiya*, Vy`pusk 312, Tom 324, 66-70. https://politics.chdu.edu.ua/article/view/200683

4. Abbas, S. R. (2025). The Emergence of Hybrid Warfare and the Future of Global Security: a comparative study of Russian and NATO's hybrid infrastructure in Ukraine. *Journal of politics and development*, 15(2), 198-211. *PhilArchive*. https://philarchive.org/archive/ABBTEO-13

5. Caliskan, M. (2019). Hybrid Warfare through the Lens of Strategic Theory. *Defense and Security Analysis*, 35(1), 40-58. https://doi.org/10.1080/14751798.2019.1565364

6. DHS Strategic Framework for Countering Terrorism and Targeted Violence (2019). https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

7. Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives,* 33(18). https://doi.org/10.1177/2336825X251322719

8. Geri, M.(2024). Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future 'energy-resources-climate' security nexus. *Journal of Strategic Security*, Vol. 17, No. 3, 15-34. https://www.jstor.org/stable/48793907

9. Gregg, H. S. (2024). Hybrid Threats and Strategic Competition. *The Quarterly Journal Connections,* 2, 159-171. https://doi.org/10.11610/Connections.23.2.01

10. Harding, E. (2025). The National Security Strategy: The Good, the Not So Great, and the Alarm Bells. December 5. *Center for Strategic and International Studies*. https://www.csis.org/analysis/national-security-strategy-good-not-so-great-and-alarm-bells

11. Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. *Potomac Institute for Policy Studies.* www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

12. Hybrid Warfare Reference Curriculum. Volume I / Edited by Z. Jobbágy, E. Zsigmond (2024). Budapest. 202 p. https://csnsc.uk/wp-content/uploads/2024/06/2022_Hybrid_warfare_reference_curriculum_volume_I.pdf

13. Khakwani, A., Saleem, M., Malik, M. M. (2025). Hybrid Warfare, Grey Zone Conflicts, and the Battle of Narratives: Discourse as a Strategic Weapon. *Social Prism,* 2(2), 1-14. https://doi.org/10.69671/socialprism.2.2.2025.37

14. Li, T., Pan, Yu., Zhu, Q. (2023). Decision-Dominant Strategic Defense Against Lateral Movement for 5G Zero-Trust Multi-Domain Networks (October, 2). *arXiv.org e-Print archive.* https://doi.org/10.48550/arXiv.2310.01675

15. Minici, M., Luceri, L., Cinus, F., Ferrara, E. (2024). Uncovering Coordinated Cross-Platform Information Operations Threatening the Integrity of the 2024 U.S. Presidential Election Online Discussion (September 20). *arXiv.org e-Print archive*. https://doi.org/10.48550/arXiv.2409.15402

16. National Cyber Strategy of the United States of America. September (2018). https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

17. National Defense Strategy (2022). 80 p. *U.S. Department of War*. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf

18. National Security Strategy of the United States of America (2027). 68 p. *The White House* https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

19. National Security Strategy of the United States of America (2025)**.** *The White House*. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

20. National Security Strategy of the United States of America (2022). *The White House*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

21. Nilsson, N., Weissmann, M., Palmertz, B. P. (2025). Hybrid Threats and the Intelligence Community: Priming for a Volatile Age. *International Journal of Intelligence and CounterIntelligence,* 39, 109-131. https://doi.org/10.1080/08850607.2024.2435265

22. Nuclear Posture Review (2018). *U.S. Department of War*.

https://media.defense.gov/2018/Feb/02/2001872877/-1/-1/1/2018-Nuclear-Posture-Review-Report.pdf

23. Orleans-Bosomtwe, P.K. (2024). Critical Infrastructure Security: Penetration Testing and Exploit Development Perspectives (July, 24). *arXiv.org e-Print archive.* https://doi.org/10.48550/arXiv.2407.17256

24. Person, R., Kulalic, I., Mayle, J. (2024). Back to the future: the persistent problems of hybrid war. *International Affairs,* Vol. 100, Issue 4, 1749–1761. https://doi.org/10.1093/ia/iiae131

25. Solen, D. (2022). *Fight Fire with Fire: The PLA Studies Hybrid Warfare.* China Aerospace Studies Institute. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2022-03-23%20Fight%20Fire%20with%20Fire.pdf

26. Speranza, L. A (2020). Strategic Concept for Countering Russian and Chinese Hybrid Threats. Atlantic Council, Scowcroft Center for Strategy and Security. 28 p. https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Strategic-Concept-for-Countering-Russian-and-Chinese-Hybrid-Threats-Web.pdf

27. Summary of the National Defense Strategy. Sharpening the American Military's Competitive Edge (2018). *U.S. Department of War*. https://media.defense.gov/2020/May/18/2002302061/-1/-1/1/2018-NATIONAL-DEFENSE-STRATEGY-SUMMARY.PDF

28. The Trump Administration's National Security Strategy / A. de Hoop Scheffer, D. Kliman, B.S. Glaser etc. (2025). *German Marshall Fund of the United States*. https://www.gmfus.org/news/trump-administrations-national-security-strategy

29. Värk, R. (2020). Legal Complexities in the Service of Hybrid Warfare. *Kyiv-Mohyla Law & Politics Journal,* 6, 27-43. https://doi.org/10.18523/kmlpj220732.2020-6.27-43

30. Weissmann, M. (2021). Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. *Hybrid Warfare / M. Weissmann, N. Nilsson, B. Palmertz and P. Thunholm.* Tauris, 61-82. https://doi.org/10.5040/9781788317795.0011

31. Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security,* 5(1), 17-26. *Center for Security Studies*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC_2_23829230%20-%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20and%20hybrid%20threats%20today%20and%20tomorrow_%20towards%20an%20analytical%20framework.pdf

32. Załęski, K. (2020). *Hybrid warfare as a strategic tool for shaping policy of the Russian Federation. Humanities and Social Sciences*, Vol. XXV, 27 (1/2020), 109-122. https://czasopisma.prz.edu.pl/hss/article/view/42/27

Vitman K., Kapsamun O. Hybrid warfare in US strategy: A Comparative Analysis of the Trump and Biden Administrations and the Challenges of the 21st Century

This article examines the evolution of the U.S. hybrid warfare strategy and provides a comparative analysis of the approaches of the Donald Trump administrations (first and second terms) and the Joe Biden administration in the context of 21st-century security challenges. It is established that hybrid warfare, combining military, informational, cyber, and economic instruments of influence, has become a central element of both U.S. national and global security. The study analyzes how the Trump administration during its first term employed a pragmatic and transactional approach to "gray-zone" conflicts, emphasizing sanctions, targeted technological restrictions, and limited support for allies, particularly Ukraine. The second term of Trump is characterized by increased attention to domestic security, cyber defense, informational deterrence, and preemptive asymmetric measures against major rival states. In contrast, the Biden administration is shown to implement a comprehensive coalition-based model, focused on close coordination with NATO and the EU, the integration of cyber and informational tools, the support of critical infrastructure, and personnel preparedness, ensuring preventive counteraction to hybrid threats, including Russian attacks against Ukraine. The article considers practical cases of U.S. engagement with Ukraine, as well as strategies for deterring China and responding to cyber threats in the global context. It analyzes recent studies and publications addressing hybrid warfare, informational operations, cyber security, and the role of allies, highlighting unresolved issues such as the effectiveness of different "whole-of-government" models, the integration of technological instruments, and the impact of emerging technologies on hybrid conflicts. The findings substantiate that the U.S. hybrid warfare strategy in the 21st century is evolving toward complexity, adaptability, and technological superiority, combining military, economic, informational, and diplomatic instruments. This enables the United States to respond effectively to gray-zone conflicts, maintain strategic advantage on a global scale, and coordinate actions with allied partners.

***Keywords**: hybrid warfare, United States, Trump and Biden administrations, gray-zone conflicts, cyber security, informational operations, strategic deterrence, Ukraine, global security.*