https://doi.org/10.26565/1992-2337-2025-2-18
УДК 355.02:327.7(477)

Дворянов Віктор Петрович,
аспірант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: victordvorianov1977@gmail.com https://orcid.org/0000-0002-6705-6549

АНАЛІЗ СТАНУ ДЕРЖАВНИХ МЕХАНІЗМІВ В УКРАЇНІ З ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Анотація. Стаття присвячена комплексному аналізу державних механізмів які відповідають за протидію гібридним загрозам. Розглянуто еволюцію концепту «гібридна війна» та «гібридні загрози» від військової доктрини до міждисциплінарного феномену. Досліджено моделі протидії гібридним загрозам у країнах НАТО та Європейського Союзу, а також підходи постадянських держав. Особливу увагу приділено механізмам з протидії інформаційно-психологічним операціям противника, а також які відповідають за кібероборону держави. Відзначена необхідність змін вітчизняного законодавства у частині доповнення повноважень Національної ради України з питань телебачення і радіомовлення стосовно соціальних мереж. А також враховуючи багатоаспектність гібридних загроз та велику кількість задіяних для протидії різних державних установ та організацій запропоновано визначити окремого віцепрем'єр-міністра України, який здійснював би загальну координацію. Фахівцями рекомендується також створення Національного центру протидії гібридним загрозам як єдиного координаційного органу з розширеними оперативними повноваженнями. Дослідження може бути використане для удосконалення систем національної безпеки та підвищення стійкості держави до війн нового типу. На підставі аналізу сформульовано стратегічні рекомендації щодо підвищення обороноздатності України через поглиблення європейської та євроатлантичної інтеграції, технологічну модернізацію та підвищення ефективності міжвідомчої координації.

Ключові слова: гібридні загрози, гібридна війна, державна служба, державні механізми, кібербезпека, публічне управління, стійкість.

Постановка проблеми. Сучасний етап розвитку міжнародних відносин характеризується глибокими трансформаційними процесами, пов'язаними з інтенсифікацією глобалізації.

Як цитувати: Дворянов В. П. Аналіз стану державних механізмів в Україні з протидії гібридним загрозам. *Державне будівництво*. 2025. № 2 (38). С. 286–313. https://doi.org/10.26565/1992-2337-2025-2-18

In cites: Dvorianov, V.P. (2025). Analysis of the state of state mechanisms in Ukraine to counter hybrid threats. *State Formation, no. 2 (38), 286–313.* https://doi.org/10.26565/1992-2337-2025-2-18 [in Ukrainian].

Ці процеси суттєво впливають на систему національної безпеки держав, створюючи як нові можливості для міжнародної співпраці, так і безпрецедентні виклики для суверенітету та територіальної цілісності. Для України питання адаптації системи національної безпеки та оборони до умов глобалізації набуло особливої актуальності в контексті російської збройної агресії, яка розпочалася у 2014 році та переросла у повномасштабне вторгнення у лютому 2022 року.

Актуальність дослідження зумовлена кількома ключовими факторами. По-перше, російська агресія проти України продемонструвала кризу глобальної системи безпеки та неспроможність існуючих міжнародних інституцій ефективно запобігати порушенням міжнародного права [51]. По-друге, характер сучасних воєнних конфліктів змінюється під впливом глобалізації, набуваючи гібридних форм, що поєднують традиційні військові дії з кібератаками, інформаційними операціями та економічним тиском [46]. По-третє, євроатлантична інтеграція України вимагає трансформації оборонного сектору відповідно до стандартів НАТО та адаптації до нових форм колективної безпеки [49]. По-четверте, технологічна глобалізація створює як нові вразливості критичної інфраструктури, так і можливості для модернізації Збройних Сил [42].

Огляд останніх наукових публікацій. Аналіз наукової літератури свідчить про значний інтерес дослідників до проблематики взаємозв'язку глобалізації та національної безпеки. Теоретичні основи вивчення впливу глобалізації на міжнародну безпеку закладені у роботах Збігнева Бжезінського [40], Семюела Хантінгтона [47], Джозефа Ная [50], Баррі Бузана [41]. Українські дослідники, зокрема С. Авраменко, Н. Варенья, І. Рижов [33], В. Горбулін [5], О. Дзьобан [23], Ю. Когут [15], І. Кукін [16] та Ю. Лісовська [19], зробили вагомий внесок у розуміння специфіки безпекових викликів для України. Сучасні дослідження фокусуються на гібридних загрозах, кібербезпеці, інформаційних війнах та трансформації характеру збройних конфліктів у глобалізованому світі [44; 46; 51].

Водночас існує потреба у комплексному дослідженні, яке б системно проаналізувало державні механізми які відповідають за протидію гібридним загрозам.

Мета статті: Мета дослідження полягає у проведенні аналізу стану державних механізмів з протидії гібридним загрозам.

Завдання дослідження:

1. Проаналізувати еволюцію концепту «гібридна війна» та «гібридні загрози» від військової доктрини до міждисциплінарного феномену.
2. Дослідити моделі протидії гібридним загрозам у країнах НАТО та Європейського Союзу, а також підходи пострадянських держав.
3. Оцінити стан державних механізмів в контексті глобалізаційних викликів для безпеки та оборони України, включаючи воєнно-політичні, економічні, інформаційно-кібернетичні та транснаціональні загрози.
4. Розробити стратегічні рекомендації щодо підвищення обороноздатності України в контексті глобалізаційних процесів.

Застосована методологія: Дослідження вимагає комплексного методологічного підходу, що поєднує різні методи та інструменти аналізу. Зокрема, системний аналіз системний підхід дозволяє розглядати національну безпеку як складну систему взаємопов'язаних елементів, включаючи політичний, військовий, економічний, інформаційний, екологічний та інші компоненти.

Компаративний метод використовується для порівняння досвіду різних країн у адаптації своїх систем національної безпеки до викликів глобалізації. Особливу увагу приділено досвіду країн Центральної та Східної Європи, які пройшли шлях трансформації від пострадянських держав до членів НАТО та ЄС. Аналіз успішних практик дозволяє сформулювати рекомендації для України.

Структурно-функціональний аналіз фокусується на дослідженні структури системи національної безпеки та оборони України, функцій різних інституцій та механізмів їхньої взаємодії. Цей метод дозволяє виявити недоліки в організації сектору безпеки та запропонувати шляхи його реформування.

Статистичний аналіз використовується для обробки кількісних даних щодо оборонних витрат, військового потенціалу, економічних показників, що дозволяє виявити тенденції та закономірності.

Виклад основного матеріалу. Результати воєн змінюють історію, і тому війна залишається важливим фактором формування та функціонування механізмів державного управління. В. Сухонос та В. Сухонос відзначають, що у механізмі забезпечення національної безпеки вирішальну роль відіграють держава та її інститути. При цьому інституціонально в цьому механізмі задіяні не лише державні органи, установи та підприємства, а й державні збройні формування, зокрема і збройні сили [32, с. 4]. Під механізмом держави фахівці запропонували розуміти цілісну систему державних організацій чи технологій, що практично здійснюють державну владу, завдання і функції держави [32, с. 98]. Зокрема, О. Пушкар у монографії «Розвиток державної інформаційної політики України: практичні механізми, теоретичні та методологічні підходи» зазначає, що «Ключовими складовими механізму формування та реалізації інформаційної політики є нормативно-правове забезпечення, яке визначає правові засади інформаційної діяльності; організаційне забезпечення, що включає діяльність державних і громадських інституцій у сфері інформаційної політики; та інформаційно-технічне забезпечення, яке створює необхідні цифрові та технологічні умови для реалізації інформаційних процесів» [29, с. 280].

Відповідно до Закону України «Про національну безпеку України» сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки. Функції та повноваження складових сектору безпеки і оборони визначаються законодавством України. Керівництво у сферах національної безпеки і оборони відповідно до Конституції України здійснює Президент України. Координацію у сферах національної безпеки і оборони здійснює Рада націона-

льної безпеки і оборони України відповідно до статті 107 Конституції України та Закону України «Про Раду національної безпеки і оборони України» [30]. Демократичний цивільний контроль над силовим сектором є фундаментальним принципом демократії, який гарантує, що збройні сили служать суспільству, а не є інструментом політичних амбіцій або державних переворотів. Необхідно відмітити створення інституту військового омбудсмена, який працює при президентові України, зокрема, приймає скарги військовослужбовців, здійснює перевірки у військових частинах та взаємодіє з іншими органами влади. Щоправда, Л. Голопатюк і Р. Тимошенко до повномасштабного вторгнення Росії в Україну 24 лютого 2022 р. стверджували, що «Воєнна сила не є вирішальною у сучасному воєнному конфлікті, мета досягається в першу чергу оптимальним поєднанням економічної, інформаційної і воєнної складових» [4, с. 26]. Однак подібна думка є сумнівною у зв'язку з незрозумілістю меж зазначеного поєднання через їх випадковий характер. Американський економіст, лауреат Нобелівської премії 2005 року Томас Шеллінг у своїй праці «Стратегія конфлікту» вказує, що «Остаточне рішення або критична дія, з яких починається необоротний процес, – це не те, що очікуєш, що буде зроблено навмисно. «Випадковість» допомагає вирішити, чи відбудеться чи ні розв'язування тотальної війни, причому ймовірність цього є предметом суджень, заснованих на природні обмеженої війни та контексті, в якому вона ведеться [38, с. 181]. Сучасні воєнні конфлікти справді включають не лише військову складову, але воєнна небезпека сьогодні найактуальніша як для України, так і для багатьох країн світу та міжнародних організацій. За оцінками Світового банку, Європейської комісії, ООН та українського уряду потреба у відновленні критичної інфраструктури, житла та важливих соціальних та транспортних об'єктів України на початок 2025 р. становила 524 млрд доларів США.

Понятійний апарат сучасних загроз, що отримав назву у фахівців «гібридних», загалом сформовано наприкінці XX – на початку XXI століття. І неодмінними властивостями цих загроз є: їх неоголошеність і прихованість, економічний тиск, експлуатація течій сепаратистського характеру та екстремістських угруповань, пріоритетна роль спецслужб, масштабне застосування методів інформаційно-психологічного протиборства тощо. Те саме стосувалося і гібридної війни. Хоча це є також і основними ознаками традиційного міжнародного збройного конфлікта. Зокрема, незаконна війна Росії проти України з 2014 р. розгорнута на новій технологічній основі за всіма можливими напрямами. Однак фахівці визнають, що концепція гібридних загроз є проблематичною. Сучасній науці бракує спільного визначення і термінологія залишається спірною. Загалом, термін гібридні загрози є лише одним із безлічі різних, що використовуються для опису подібних явищ, це: «антогоністичні загрози», «гібридна тактика», «гібридні методи», «асиметрична війна», «безконтактна війна», «сірі війни», «гібридна війна», «війна наступного покоління», «неоднозначна війна», «нерегулярна війна», «нелінійна війна», «необмежена війна», «операції повного спектру», «нетрадиційна війна» та інші [45, с. 4]. Однак вважається за

правильне відзначити, що заходи щодо протидії гібридним загрозам обов'язково повинні ураховувати досвід світових та холодної воєн, коли пропагандистські й економічні війни виявилися вирішальним фактором для результату протистояння тільки після врівноваження сил супротивників у результаті тривалої збройної боротьби.

«Тваринний або рослинний організм, виведений за допомогою схрещування (гібридизації). Поміс; неприродне поєднання чого-небудь», – сучасний тлумачний словник української мови так розкриває значення слова «гібрид» [39, с. 130]. Український дослідник М. Паламарчук звертає увагу на те, що: «Коли порівнюєш поступову зміну класів кораблів з еволюцією біологічних груп, виникає відчуття подібності цих процесів…Приміром, у ході еволюції певної біологічної групи в багатьох випадках поступово зростають розміри її представників, які «захоплюють» нові екологічні ніші. У кораблів так само. Тоннаж американських авіаносців зі зміною поколінь збільшився майже у вісім разів» [27, с. 9]. Таким чином, зв'язок поняття «гібрид» та військової сфери виглядає обґрунтовано.

Зважаючи на незворотність європейського та євроатлантичного курсу України, особливо важливими для дослідження є бачення концепції гібридних загроз у Європейському Союзі (ЄС) та Організації Північноатлантичного договору (НАТО). Зокрема, у спільному повідомленні Європейського парламенту і Ради «Спільна структура протидії гібридним загрозам Європейського Союзу», гібридні загрози концептуально визначено як «поєднання примусової та підривної діяльності, традиційних і нетрадиційних методів (тобто дипломатичних, військових, економічних, технологічних), які можуть бути скоординовано використані державними чи недержавними суб'єктами для досягнення конкретних цілей, залишаючись на рівні нижче порогу формально оголошеної війни». «Гібридна загроза» також розглядається як «явище, яке виникає внаслідок конвергенції та взаємозв'язку різних елементів, які разом утворюють більш складну та багатовимірну загрозу», а її крайнє вираження, «гібридну війну», визначають як «ситуацію, у якій країна вдається до відкритого використання збройних сил проти іншої країни на додаток до комбінації інших засобів (тобто економічних, політичних та дипломатичних)» [3, с. 18]. Проте за такого одностороннього тлумачення гібридної війни може виявитися, що збройна агресія з боку держави або коаліції (союзу) держав не є вирішальним фактором. Хоча негативні наслідки складного протистояння за участю різних країн світу, ООН та НАТО, можуть настати саме після здійснення погрози, тобто застосування військової сили. Зазначене вище бачення сучасної війни було актуальним у 90-х рр. XX століття, коли ще пам'ятали період «розрядки» у міжнародній політиці, закінчилася холодна війна, розпад СРСР і у світі настала епоха американської гегемонії. Однак, з огляду на те, що ЄС і Китай відіграють все більш помітну роль на міжнародній арені, США зосередили увагу на Індо-Тихоокеанському регіоні, Росія намагається утвердитися як глобальна держава завдяки своїм доходам від нафти і газу, а Україна перетворюється на потужну військову силу, ситуація на

геополітичній арені стала менш передбачуваною. Тому поняття гібридної війни потребує уточнення або навіть перегляду.

У ЄС доволі чітко ідентифікували гібридні загрози для протидії створенню Росією осередків напруження й нестабільності. У ЄС класифікують сфери протидії таким загрозам, як інформаційна сфера, енергетика, транспорт та інфраструктура, космос, військова сфера, охорона здоров'я і продовольча безпека, кіберпростір, фінансова сфера, промисловість, громадський або суспільний вимір [3, с. 17–20]. Однак як уже зазначалося вище, нинішня концепція гібридної війни суперечить існуючій ситуації безпеки у світі. Сукупність наявних і потенційно можливих явищ та факторів, що створюють небезпеку правильно називати загрозами, а не війною. Не заперечуючи впливу світових економічних чинників, заходи протидії гібридним загрозам та війні у країнах Заходу очевидно вже зараз формуються під впливом російсько-української війни або Війни за Незалежність України. Зокрема, у НАТО вважають, що з початку повномасштабної війни Росії проти України загальне число загиблих і поранених перевищило один мільйон людей [31]. Введені масштабні економічні та індивідуальні санкції країн Заходу через військову агресію Росії проти України не змусили Кремль припинити бойові дії. Їхній ефект, очевидно, ще досліджуватиметься після війни, проте імперіалістичні наміри нинішнього російського керівництва через бажання досягти цілей так званої «СВО», незважаючи на втрати, лише підживилися бажанням отримати компенсацію за втрачені кошти та майно. Тобто лише агресивна торговельна політика та збільшення оборонних витрат не є війною.

Л. Веселова зазначає, що гібридні загрози не лише різноманітні, вони спеціально пристосовані до ураження слабких місць конкретних цілей. Це означає, що кожна країна повинна мати своє власне розуміння типу гібридних загроз, які можуть бути застосовані проти неї. Це досягається ретельним вивченням власних слабких місць, а не за рахунок універсальної дефініції неуніверсальної концепції [1, с. 376–377]. Зокрема, Ю. Кучеренко, А. Носик та О. Дзьобань сучасною війною називають мережеву війну і визначають її як соціально-політичну, соціально-економічну та культурну інновацію на основі інформаційно-комунікативних технологій, що застосовується інститутами управління, певними групами для досягнення цілей управління й контролю. Мережеві агресивні дії в умовах мережевих війн провокують людину на прийняття ризикованих дій, що в свою чергу створює більш нестабільну соціокультурну ситуацію, що, в результаті, сприяє досягненню цілей мережевих війн [17, с. 53].

Не можна не погодитися із професором О. Карпенко, що розвиток стійкості до гібридних загроз вимагає виходу за межі стійкості в окремих сферах, розбудовуючи її системно, враховуючи залежності та взаємозалежності між різними частинами суспільства – «Модель комплексної екосистеми стійкості («The comprehensive resilience ecosystem (CORE) model»), яка має полегшити процес прийняття обґрунтованих управлінських рішень на різних рівнях управління. Модель комплексної екосистеми стійкості – це системне представлення

демократичного суспільства в цілому. Вона показує, як гібридні загрози крок за кроком кидають виклик демократичним системам, створюючи різні види стресу. Це також дозволяє відстежувати залежності та можливі каскадні ефекти. Це важливо для виявлення гібридних загроз. Передбачення відіграє вирішальну роль у цьому процесі [13, с. 181–182].

Відповіддю ЄС на численні виклики, які зумовлені впливом гібридних загроз, є також більш рання розробка «Концептуальної моделі гібридних загроз» («Hybrid Threats conceptual model»), яка є результатом спільних зусиль Об'єднаного дослідницького центру Європейської комісії (JRC) та Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE). У «Концептуальній моделі гібридних загроз» виділено чотири основні стовпи, шо необхідно вивчити, щоб мати можливість повністю зрозуміти ландшафт гібридних загроз: ворожі актори (та їхні стратегічні цілі); інструменти, які використовує ворожій актор; цільові домени (сфери); фази (включаючи види діяльності, що спостерігаються в кожній фазі). Зокрема, гібридна війна передбачає синхронізоване використання багатьох інструментів впливу, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів [13, с. 179–181]. Проте британський професор воєнних досліджень Л. Фрідман слушно зазначає, що часто такі дії йдуть у власний спосіб, і вони можуть не бути добре скоординованими [37, с. 477]. Л. Фрідман звертає увагу, що розмови про гібридну війну наштовхували на думку, що докорінно відмінні на перший погляд дії були належно інтегровані для досягнення певного ступеня синергії. Але це часто було не так під час протистояння Росії з Україною. Існували обмеження щодо того, чим можна було керувати та координувати із центру. Не було єдиної вертикалі командування, а їх існувало кілька, і деякі були міцнішими за інші. За мотузки в Росії тягнули ділові та політичні спільники Путіна, а також ФСБ і ГРУ. З іншого кінця мотузок були лідер озброєних формувань в Україні. Вони ухвалювали власні рішення щодо того, як боротися з відданими українському уряду військами [37, с. 477]. Саме відсутність чітких військових цілей у 2014 р., а також переоцінений психологічний фактор у 2022 р. не дозволили досягти стратегічного перелому, а саме повернути всю Україну назад у сферу впливу Російської Федерації. Доцільно зазначити, що повномасштабний напад Росії на Україну характеризується постійним порушенням норм міжнародного права, що відрізняє його від конвенційної війни.

Одним з механізмів протидії гібридним загрозам у ЄС є створений ще у вересні 2005 р. координуючий орган – Європейське агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency – ENISA), що розміщений на території Греції. Агентство діє через загальноєвропейську та національні команди з реагування на комп'ютерні надзвичайні події (Computer Emergency Response Teams). З червня 2019 р. Європейське агентство з мережевої та інформаційної безпеки має назву Агентство ЄС з кібербезпеки (EU Cybersecurity Agency). Однак це Агентство взяло ту саму абревіатуру – ENISA. ENISA є наглядовим органом ЄС у сфері кібербезпеки для підтримки

держав-членів ЄС у подоланні та протидії кіберзагрозам та кібератакам. Агентство ENISA має проводити щорічні європейські навчання з кібербезпеки та обмін розвідувальною інформацією щодо кіберзагроз шляхом створення Центрів обміну інформацією та аналізу (Information Sharing and Analyses Centres) [14, с. 266]. ENISA підвищує надійність продуктів, послуг і процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС і допомагає Європі підготуватися до кібервикликів завтрашнього дня [43]. Зокрема, Директива ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (Директива NIS) закладає єдині правила та вимоги у сфері кібербезпеки для всіх країн ЄС, але залишає за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви в національне законодавство. Директива вимагала від країн-членів упровадження цих правил ще до 9 травня 2018 р. [1, с. 382]. Про увагу до протидії кібервійні в Європейському Союзі свідчить нова Стратегія ЄС з кібербезпеки (2020).

Серед організаційних заходів посилення суб'єктного складу забезпечення кібербезпеки варто виділити діяльність з вересня 2017 р. згадуваного вище Європейського центру протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats). Рішення про створення фінського Центру було прийнято в квітні 2017 р. представниками країн НАТО та ЄС. Серед засновників 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Велика Британія, Іспанія, Польща, Естонія, Латвія і Литва. Метою Центру є протидія «новим загрозам, спрямованим на дестабілізацію ситуації в європейських країнах». Діяльність Центру спрямовано на: проведення досліджень, аналіз гібридних загроз та методів боротьби з ними; організацію спільного навчання для країн-учасниць; проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО, залучення до діалогу урядових та неурядових експертів [1, с. 371–372]. Зокрема, концепція комплексної безпеки або фінська модель готовності передбачає, що влада, бізнес, неурядові організації та громадяни несуть спільну відповідальність за захист життєдіяльності суспільства. Мета полягає в тому, щоб під час кризи все фінське суспільство могло швидко мобілізувати ресурси, де це необхідно, швидко відновитися і адаптувати свої функції на основі отриманих уроків. Коріння концепції – в доктрині «Тотальної оборони» після Другої світової війни, коли все суспільство мобілізувалося як частина військових оборонних зусиль [2, с. 58]. Проте концепція національної безпеки еволюціонувала під впливом глобалізації від традиційного розуміння, зосередженого на захисті території від зовнішньої військової агресії, до більш широкого підходу, що включає економічну, енергетичну, екологічну, інформаційну, кібернетичну та інші виміри безпеки. Копенгагенська школа безпекових студій запропонувала концепцію секторального підходу, виділяючи військовий, політичний, економічний, соціальний та екологічний сектори безпеки. Зокрема, базуючись на дослідженнях Hoffman (2007) та сучасному досвіді європейських країн (European Centre of Excellence for Countering Hybrid Threats, 2019), фахів-

цями рекомендується створення Національного центру протидії гібридним загрозам як єдиного координаційного органу з розширеними оперативними повноваженнями. Цей центр має забезпечувати прямі канали зв'язку з усіма ключовими відомствами, можливості швидкого прийняття рішень в кризових ситуаціях (CISA, 2024) та ефективну інтеграцію розвідувальних та аналітичних функцій. Матрична система управління дозволить формувати гнучкі міжвідомчі робочі групи для вирішення конкретних завдань без порушення існуючої організаційної структури. Таким чином, буде забезпечена управлінські стійкість як здатність держави забезпечувати безпеку через сильні державні інституції.

Л. Веселова звертає увагу на те, що у НАТО та ЄС є чітке розуміння того, що гібридним загрозам потрібно запобігати як «пасивними» елементами (посилення стійкості до потрясінь чи несподіванок), так і більш активними, включно з потужними заходами з підготовки й захисту функцій і структур, які найбільш вірогідно стануть мішенями гібридних атак. У цьому контексті неможливо перебільшити важливість активних дій з посилення цивільної готовності, вільної преси, освіченості населення й дієвої правової структури [1, с. 376]. Європейський Союз бачить підвищення обізнаності громадськості та боротьбу з пропагандою як центральне завдання в інформаційному секторі [12, с. 56–57]. У вересні 2015 р. розпочала роботу оперативна робоча група зі стратегічних комунікацій Європейського Союзу – East StratCom Task Force. Серед іншого, діяльність групи спрямована на надання інформаційної підтримки делегаціям ЄС в Азербайджані, Вірменії, Білорусі, Грузії, Молдові, Україні. Одним з прикладів діяльності комісії є спростування міфів щодо нацизму в Україні [1, с. 369–370]. Крім того, у листопаді 2025 р. Колегія Європейської комісії затвердила проєкт «Європейський щит демократії», метою якого є боротися з гібридними загрозами та дезінформацією з боку РФ. Ініціатива покликана захистити інформаційний простір, зміцнити демократичні інституції та підвищити стійкість суспільства. Для зміцнення демократичних інституцій передбачено підтримку вільних виборів та незалежних медіа, включно з фінансуванням до 9 млрд євро (за матеріалами медіа). Такий досвід необхідно застосувати в Україні з огляду на складний через бойові дії матеріально-технічний та фінансовий стан вітчизняних медіа.

Багатогранність гібридних загроз також виявилася в енергетичній сфері. Загрози енергетичній безпеці країн світу, насамперед країн Європи, йдуть від сучасної структури світового ринку енергетики. Уже не перше десятиліття актуальним напрямом енергетичної політики ЄС є необхідність забезпечення енергетичної безпеки, яка є проблемною галуззю у зв'язку з високою залежністю ЄС від імпорту енергоресурсів, переважно з Російської Федерації. Тому питання диверсифікації постачання постачальників та маршрутів постачання енергоресурсів стало невід'ємною частиною зовнішньої енергетичної політики ЄС після масштабної агресії Росії проти України [14, с. 42–45]. Проте розвиток фізичної інфраструктури не тягне за собою автоматичне підвищення енергетичної безпеки, на думку фахівців, вирішальне значення має забезпечення належного дотримання загального законодавства на рівні ЄС у газовому та в електроенерге-

тичному секторі. О. Карпенко серед дієвих механізмів протидії гібридним загрозам в країнах ЄС стосовно забезпечення енергетичної безпеки називає зменшення залежності від російських енергоресурсів через диверсифікацію постачальників. Наприклад, Польща й Литва створили LNG-термінали, що дозволило їм знизити залежність від російського газу. Також створення Енергетичного союзу ЄС, який забезпечує інтеграцію енергетичних систем країн-членів [13, с. 178]. Для України багатогранність гібридних загроз також виявилася в енергетичній сфері. Щоправда, окупація Запорізької АЕС означає не лише втрати нашої країни в електроенергії. Три відомі атаки безпілотників на тренувальний центр ЗАЕС та інші воєнні ризики можуть поставити під сумнів загалом відродження ядерної енергетики у світі. І входження України до складу Ради керівників Міжнародного агентства з ядерної енергії (МАГАТЕ) на 2023–2025 роки ситуацію не змінило. А це, у свою чергу, може зруйнувати як плани майже 30 країн світу, які внесли ядерну енергію в плани до 2030 р., представлені згідно з Паризькою угодою 2015 р., так і більш довгострокові стратегії досягнення нульового рівня викидів. Отже, у підсумку, буде надзвичайно складно забезпечити екологічну стійкість. Також корупційні скандали в енергетичній сфері, що періодично виникають, можуть значно уповільнити темпи реалізації важливих для національної безпеки України проєктів.

Але сучасна війна передбачає боротьбу не тільки у кіберпросторі або на енергетичних ринках. І позитивних результатів у сфері безпеки та оборони досягли не лише країни Заходу. Найбільш важливим новаторством Польщі вважається посилення уваги до розвитку структур спеціального призначення. Чисельність спеціальних військ, які діють у рамках польської доктрини «Спеціальні операції DD/3.5», сягає 2,5 тисячі військових, що становить 2,1% чисельності всіх ЗС РП. Бійці спецназу використовують тактику й техніки, що істотно відрізняються від прийнятих в інших видах ЗС Польщі. Для спецназу є законодавчий акт (Dz.U.2016.904), що дозволяє йому протистояти регулярним загрозам (наприклад, спецпідрозділам агресора, найманцям та ін.). І парамілітарним структурам (незаконні збройні формування, терористичні групи та ін.), якщо дії останніх з використанням зброї або вчинені ними дестабілізаційні заходи проти держави визнаються терористичними [5, с. 143–144]. З іншого боку, позитивні результати є також і при вирішенні питань цивільного забезпечення суспільної і приватної життєдіяльності людей. Цікавим для України може бути досвід Польщі і у галузі державно-приватного партнерства (ДПП), оскільки відповідні механізме співпраці як гармонізовані з директивами Європейського Союзу, зокрема Директивою 2014/23/EU, так і допомогли реалізувати станом на 2025 рік понад 200 проєктів з розвитку інфраструктури країни. Польська модель характеризується наявністю єдиного координаційного органу – Міністерства фондів та регіональної політики (Ministerstwa Inwestycji i Rozwoju), функціонуванням національного Порталу ДПП, широкими повноваженнями органів місцевого самоврядування та активним залученням приватного сектору до реалізації інфраструктурних проєктів. К. Д’яченко зазначає, що відсутність єдиного упов-

новаженого органу, складність процедур, низький рівень проєктної спроможності місцевих громад та брак стандартної документації сьогодні є ключовими бар'єрами до розвитку українського інституту ДПП [9].

Як зазначалося, незаконна війна Росії проти України з 2014 р. розгорнута на новій технологічній основі за всіма можливими напрямами. Характерними ознаками першого повномасштабного міжнародного збройного конфлікту у XXI столітті у світі є використання високотехнологічної зброї, прийняття інноваційних рішень, економічні санкції, використання проксі-сил, безжальне ставлення до цивільного населення, агресивну пропаганду з метою підірвати довіру до будь-яких джерел інформації та заперечення ведення самої війни. В. Горбулін стверджує, що робота створеного у 2014 р. і скасованого у 2019 р. Міністерства інформаційної політики продемонструвала нездатність такої організації стати ефективним органом, тому своєчасним і логічним видається створення таких профільних підрозділів у структурах розвідки, СБУ, Міноборони, Держслужби спеціального зв'язку та захисту інформації України. Разом вони мають становити сили/війська інформаційної протидії й кібероборони [5, с. 110–111].

І. Кукін навпаки зазначає, що саме на Міністерство культури та інформаційної політики України мають покладатися завдання щодо розроблення документів стратегічного планування у сфері забезпечення інформаційної безпеки, інформаційної безпеки особистості та координації діяльності у цій сфері інших суб'єктів [16, с. 328–329].

Кабінет Міністрів України (далі – КМУ) ухвалив постанову від 29 жовтня 2025 р. № 1396, якою перейменував Міністерство культури та стратегічних комунікацій України (нова назва Міністерства культури та інформаційної політики України – авт.) на Міністерство культури України. Згідно з новою структурою, сфера стратегічних комунікацій буде виокремлена з міністерства: Держкомтелерадіо, «Укрінформ», іномовлення, Центр стратегічних комунікацій та інформаційної безпеки підпорядковуватимуться безпосередньо КМУ. Водночас формування інформаційної політики, безпека журналістів та євроінтеграційний напрям залишаються у компетенції Міністерства культури України. Також необхідно відзначити, що Міністерству культури також підпорядковуються Державне агентство України з питань мистецтв та мистецької освіти, а також Державне агентство України з питань кіно. Серед відомих українському глядачеві фільмів частково профінансованих державою: «Снайпер. Білий Ворон» (2022 р.) та «Довбуш» (2023 р.). В структурі КМУ функціонує і Віце-прем'єр-міністр з гуманітарної політики України – Міністр культури України.

У роз'яснювальній діяльності важливо уникнути звинувачень у проголошенні ультранаціоналістичних слоганів. Тому рекомендується, щоб наступники Міністерства культури та стратегічних комунікацій України, а також Міністерство освіти і науки України, Міністерство молоді та спорту України, Державний комітет телебачення і радіомовлення України, Національна рада України з питань телебачення і радіомовлення, Український інститут національної пам'яті при виконанні своїх завдань не тільки активно взаємодіяли між собою. Це сто-

сується і Державної служби України з етнополітики та свободи совісті, Уповноваженого із захисту державної мови та інших органів державної влади залучених до формування стратегічного наративу держави, але і підтримували постійний фаховий зв'язок з Інститутом історії України Національної академії наук України. Для демократичного державного механізму варто уникати «полювання на відьом», важливо зважати на історичний контекст та дотримуватися усіх передбачених Конституцією України, Законом України «Про основні засади державної політики у сфері утвердження української національної та громадянської ідентичності» та іншими нормативно-правовими актами процедур, інакше можливе «державне» свавілля призведе до безладу та допоможе державі-агресору досягнути своїх цілей. При трансформації цих відомств важливо звернути особливу увагу на необхідність дотримання принципу деполітизації державної служби. Досягнути соціальної стійкості буде неможливо якщо відсутнє розвинуте громадянське суспільство та демократія.

Важливість ратифікації 21 серпня 2024 р. Верховною Радою України Римського статуту Міжнародного кримінального суду 1998 р. обумовлена тим, що головним міжнародно-правовим інструментом на шляху до притягнення до відповідальності російських воєнних злочинців є саме Міжнародний кримінальний суд (МКС). 25 червня 2025 р. Президент України підписав Угоду з Радою Європи про створення Спеціального трибуналу щодо злочину агресії проти України, а 15 липня 2025 р. у День Державності Верховна Рада України її ратифікувала. Відтак подібні міжнародні механізми забезпечать легітимність претензій України до РФ. Рішення міжнародних судів мають стати основою нової гуманітарної політики країни. У контексті присудження народу України премії Європейського парламенту імені Андрія Сахарова «За свободу думки» та відзначення Нобелівською премією миру 2022 р. української організації Центр громадянських свобод, нова гуманітарна політика України не має будуватися на мотиві помсти за розв'язаний геноцид [35]. Тобто не нагадувати гібридну тоталітарну ідеологію «рашизм».

Очевидно, що діяльність департаментів інформаційної діяльності та комунікацій з громадськістю у структурі обласних військових адміністрацій відрізняється від діяльності у структурі цивільних обласних адміністрацій. Наприклад, це інформаційна допомога для ВПО, учасникам бойових дій або інтерактивні мапи пунктів незламності та укриттів. Проте визначити яке місце посідають у єдиній системі державних органів в Україні ці структури можна лише після завершення процесу децентралізації, а не після завершення війни. Говорити про завершення реформи без прийняття нового закону про місцеві державні адміністрації чи префектури, що враховує нові політичні, економічні та культурні реалії, без відповідної правозастосовчої практики щодо адміністративного нагляду очевидно передчасно. У 2020 р. у Верховній Раді України був зареєстрований та прийнятий у першому читанні законопроєкт № 4298 «Про внесення змін до ЗУ «Про місцеві державні адміністрації» та деяких інших законодавчих актів України щодо реформування територіальної організації виконавчої влади в

Україні». Проте повномасштабне вторгнення Росії в Україну відтермінувало розгляд законопроєкту [20]. Інший законопроєкт № 13124, зареєстрований 20 березня 2025 р. у Верховній Раді України, також передбачає переформатування місцевих державних адміністрацій в органи префектурного типу. Метою є створення ефективної системи забезпечення законності в діяльності органів місцевого самоврядування, а також координацію територіальних органів центральної влади на місцях. Очевидно, лише після завершення бойових дій та під час активного відновлення країни можлива реалізація зазначених реформ у повному обсязі. Тому першочерговими для публічного управління мають бути зусилля для досягнення тривалого і справедливого миру.

Необхідно уважно поставитися і до думки доктора Андерса Ослунда та колишнього прем'єр-міністра Литви Андрюса Кубілюса які стверджують, що наразі головною проблемою українського державного управління загалом є функціонування центральних органів державної влади. Міністрам надають занадто короткий термін перебування на посаді (у багатьох випадках – лише пів року), а виконуючі обов'язків міністрів з обмеженими повноваженнями часто продовжують працювати в уряді. Справді, у 2016 р. в Україні набув чинності новий закон про державну службу. Він заклав підґрунтя для сучасної професійної державної служби, що базуються на заслугах, але його дотримуються не завжди. Персонал часто змінюється на основі особистої лояльності до начальства, а не завдяки професійним заслугам [24, с. 110–111].

Кабінет Міністрів України не повинен перетворитися на «Уряд, який не може впоратися зі своїм платіжним балансом, не здатен зібрати податки чи не може домогтися політичної єдності заради власного захисту, може зрадіти допомозі, яку відкинув би, маючи контроль над власними ресурсами» [38, с. 27]. Щоб комунікація між урядом і громадянами відбувалася на належному рівні, важливо також, щоб плани залучити 800 млрд доларів на післявоєнне відновлення України були підкріплені реальними заходами і мали фінансову основу у вигляді акціонерного капіталу, грантів, боргових зобов'язань і внесків приватного сектора. Міністерство економіки не є «міністерством війни», проте від рішень і дій його керівників та фахівців часто залежатиме не тільки загальна стабільність держави, а й успіхи на фронтах гібридних загроз та війни. Звичайно, найкращою гарантією безпеки України є її інтеграція в європейські та євроатлантичні структури, проте це займе певний час і цей процес буде пов'язаний із зовнішнім тиском та внутрішніми суперечностями. Це не додає впевненості в позитивному результаті. Можливо саме політика розвитку українських виробників «Зроблено в Україні» забезпечить відчутний результат для економіки. За даними уряду, у 2025 р. 72 тисячі українських підприємств скористалися державною підтримкою. 10 тисяч українців стали підприємцями, отримавши мікрогранти «Власна Справа». За 11 місяців 2025 р. переробна промисловість забезпечила 17,9% податкових надходжень зведеного бюджету – найбільше серед усіх секторів. І демонструє найвищі темпи зростання в абсолютних числах: +69,2 млрд грн до минулого року. Комунікація важлива, оскільки навіть найкраща стратегія

не працює, якщо про неї знає лише топменеджмент. Працівники на всіх рівнях мають розуміти, як їхня щоденна діяльність вписується в стратегічну картину. Це формує відчуття залученості, відповідальності та якість командної взаємодії. Коли кожен співробітник бачить свій внесок у загальний успіх – бізнес працює як цілісний, узгоджений механізм [7]. Зокрема, Морозова М. Е. визначає стратегічне планування як процес постановки стратегічних цілей і розробки багатоваріантного стратегічного плану їх досягнення на основі обраної стратегії [22]. Таким чином, буде забезпечена економічна стійкість через ефективне державне регулювання та залучення приватного сектора. Війна показала, що саме громадські організації (ГО) часто діють найоперативніше, сягаючи віддалених громад та найбільш вразливих верств населення, де державні механізми менш гнучкі. Вони активно сприяють економічному відродженню, створюючи робочі місця, підтримуючи соціальне підприємництво та мобілізуючи місцеві ресурси, зменшуючи залежність від зовнішньої допомоги. У всіх на слуху та благодійні фонди та організації, як «Повернись живим», Фонд Притули та «Таблеточки». Зважаючи на рішення США щодо скорочення фінансування низки програм в Україні, виникає ризик втрати кваліфікованих команд, які роками розбудовували свій досвід та експертизу. Крім диверсифікації джерел фінансування завдяки європейським грантовим програмам як-от Erasmus+, Horizon Europe та інші, необхідне також законодавче сприяння соціальному підприємництву та запровадження прозорих і справедливих механізмів державних закупівель соціальних послуг у ГО [18].

Однак саме дезінформація та неправдива інформація вперше очолили список найбільших короткострокових глобальних ризиків у світі. Про це говорилося в опублікованій 10 січня 2024 р. Доповіді про глобальні ризики, підготовленій Всесвітнім економічним форумом (World Economic Forum). У 2025 р. найбільшим ризиком, який загрожує світовій стабільності, було названо державні збройні конфлікти (World Economic Forum). І. Феськов зазначає, що недостатня увага до питань парирування інформаційних загроз може завдати значної шкоди політичній системі будь-якої держави аж до руйнування самої держави [36, с. 74]. Тому ЄС і США ввели санкції проти таких російських каналів, як Sputnik, Russia Today, Rossiya24, TV center International, RTR Planeta, «Перший канал», «Росія-1», «Рен-ТВ», «НТВ-Світ» та інших. Вказані інформаційні ресурси відключили від кабельної, супутникової та інтернет-трансляції. Крім того, в рамках 16-го пакету економічних та індивідуальних обмежуваних заходів проти Росії ухвалених Радою ЄС у лютому 2025 р. призупинено дію ліцензій ЄС на мовлення восьми російських ЗМІ, це: EADaily/Eurasia Daily, Fondsk, Lenta, NewsFront, RuBaltic, SouthFront, Strategic Culture Foundation, Красная звезда/ТВ Звєзда. Ці засоби масової інформації відіграли важливу роль у просуванні та підтримці агресивної війни Росії проти України, а також у дестабілізації сусідніх країн, а також ЄС та його держав-членів (сайт Арміяinform). Але М. Давидюк наголошує, що головним ресурсом пропаганди Кремля часів Путіна є телебачення. Інтернет і соціальні мережі так і не змогли стати конкурентами телеба-

ченню в Росії. Проте й не заперечує важливість соціальних мереж у внутрішній політиці Кремля та інформаційних, військових кампаніях зовні [6, с. 114].

Національна рада України з питань телебачення і радіомовлення – незалежний постійно діючий колегіальний державний орган, що діє на підставі Конституції України, Закону «Про медіа» та інших законів України і здійснює державне регулювання, нагляд та контроль у сфері медіа. Національна рада складається з восьми осіб. З них чотири члени Національної ради призначаються Верховною Радою України і чотири члени Національної ради призначаються президентом України. Для забезпечення виконання повноважень Національної ради в Автономній Республіці Крим, областях, містах Києві та Севастополі призначаються представники Національної ради. Наразі в Україні не існує державного органу, який відповідає за платформи YouTube, Instagram чи TikTok. А Національна рада, яку багато хто помилково зараховує до таких, не має повноважень регулювати цю сферу, вона передусім медійний регулятор [10]. Вітчизняне законодавство потребує змін у частині доповнення повноважень, наприклад, Національної ради України з питань телебачення і радіомовлення стосовно зазначених платформ. Слід визнати обґрунтованою думку фахівців, що на відміну від збройних конфліктів минулого під час російсько-української війни наративи формували не традиційні ЗМІ, війна розгорталась на цифрових платформах. Соціальні мережі перетворилися на поле бою. Ситуація ускладнюється, що той же Telegram утримується іноземним суб'єктом за межами України. Очевидно, корисним може бути досвід США стосовно соціальної мережі TikTok, де навіть Верховний суд підримав закон, який вимагає від TikTok усунути стурбованість тим, що платформа може становити загрозу національній безпеці (за матеріалами медіа).

С. Авраменко, Н. Варенья, І. Рижов стверджують, що в Україні поняття «інформаційна безпека» набуває «вузького» змісту [33, с. 208]. Кібербезпека концептуалізується не тільки як сам собою захист інформації, а як цілісний і повноцінний захист усієї системи в інформаційному полі (поле комп'ютерних технологій) загалом. Вони роблять висновок про те, що у цьому ж ракурсі й розвивається система публічного управління щодо інформаційної безпеки [33, с. 233]. Однак Л. Веселова вважає, доречним відокремлення кібербезпеки від інформаційної, не дивлячись на цілком логічне узагальнення. Використання кіберпростору у якості полігону гібридної агресії є мало дослідженим, тому що є більш характерним для сучасної стратегії воєнної агресії. В 2012 р. НАТО визнало кіберпростір новим театром воєнних дій. Гібридна війна значно посилює вплив кіберзагроз на українське суспільство та на фоні глобальних тенденцій загрози у кіберпросторі актуалізує небезпеку від цілеспрямованих кібератак як інструменту агресії проти нашої держави [1, с. 16, 25, 33]. Зважаючи на необхідність забезпечення кіберстійкості та технологічної стійкості, розглянемо суб'єктів забезпечення кібербезпеки.

До суб'єктів забезпечення кібербезпеки в Україні належить держава, що здійснює свої функції через відповідні органи: Президент України; Верховна

Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; СБУ, МВС, Міністерство оборони України, Збройні Сили України, а також інші правоохоронні органи та військові формування, утворені відповідно до Законів України [19, с. 20–21].

Діяльність суб'єктів кібербезпеки передбачена Конституцією України, Законами України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про електронні комунікації», «Про Національний банк України», «Про національну безпеку України», «Про Національну поліцію», «Про оборону України» та «Про основні засади забезпечення кібербезпеки України» та «Про Службу безпеки України». Крім того, Доктриною Військ зв'язку та кібербезпеки ЗСУ, Стратегією воєнної безпеки України, Стратегією забезпечення державної безпеки, Стратегією інформаційної безпеки, Стратегією кібербезпеки України, Стратегією національної безпеки України та іншими нормативно-правовими актами.

Про реформування системи публічного управління свідчить адаптація структури державного апарату до діяльності в умовах цифровізації. Зокрема, у 2019 році було створено Міністерство цифрової трансформації України (далі – Мінцифри). Відповідно до Положення, Мінцифри забезпечує формування та реалізацію державної політики у сфері цифровізації, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства [28].

Безпосередня діяльність щодо забезпечення кіберзахисту покладена на спеціальний орган, який функціонує у складі Державної служби спеціального зв'язку та захисту інформації України – Державний центр кіберзахисту Держспецзв'язку. Серед основних завдань: у взаємодії з іншими суб'єктами забезпечення кібербезпеки, розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм та методик проведення кібернавчань [25].

У складі Державної служби спеціального зв'язку та захисту інформації України функціонує Урядова команда реагування на комп'ютерні надзвичайні події України – CERT-UA. Завдання: накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам та інше [11]. Зокрема, від початку 2022 р. Національною командою реагування на кіберінци-

денти, кібератаки та кіберзагрози CERT-UA задокументовано понад 100 кіберінцидентів, пов'язаних з російськими хакерськими угрупуваннями UAC-0056, понад 110 – з UAC-0001 та понад 170 кіберінцидентів – з UAC-0002. Останнє угрупування відповідальне за найбільш резонансні атаки на АТ «Укрзалізниця», державні реєстри України і ПрАТ «Київстар». Про це йдеться в заяві МЗС України від 19 липня 2025 р. щодо запровадження кіберсанкцій проти Російської Федерації.

Фахівці відзначають, що несподіване використання зброї в електромагнітному полі може спричинити й цілий спектр психічних явищ – від розгубленості до паніки. Наприклад, за інформацією Державної служби спеціального зв'язку та захисту інформації України 21 липня 2022 р. було здійснено кібератаку на сервери та мережі радіостанцій TAVR Media. В управлінні радіогрупи знаходяться дев'ять провідних радіостанцій. Для протидії таким загрозам, Міністерство закордонних справ України і відомства ще 10 країн наприкінці 2023 р. створили Талліннський механізм з кібербезпеки. До об'єднання долучилися Велика Британія, Данія, Естонія, Канада, Нідерланди, Німеччина, Польща, США, Франція та Швеція. Талліннський механізм очевидно допоможе зміцнити кібербезпеку та цивільний вітчизняний кіберпотенціал.

Кібернетичним атакам також протидіють Національний координаційний центр кібербезпеки який є робочим органом Ради національної безпеки і оборони України, Національний банк України, Департамент Кіберполіції Національної поліції України, Ситуаційний центр забезпечення кібербезпеки (СБУ) та Війська зв'язку та кібербезпеки.

Основними завданнями при веденні сучасних війн, в тому числі і у війні РФ проти України фахівці вважають: виведення з ладу систем управління військами і бойовими засобами ЗС, систем збору та аналізу інформацій за супротивника, комп'ютерних та телекомунікаційних мереж, різних систем зв'язку, а також здійснення психологічного впливу в ході проведення операцій (інформаційного, психологічного характеру і певних дій) на війська противника, політичне (військове) керівництво країни, суспільство та особистість [23, с. 563]. Ю. Кучеренко та А. Носик звертають увагу на те, що сучасний солдат повинен мати здатність витримувати великі як фізичні, так і психологічні (стресові) навантаження. Тому, слід приділити морально-психологічному стану особового складу військ які діють в умовах постійного ведення супротивником великої кількості інформаційних (психологічних) операцій в інформаційній сфері та на полі бою особливу увагу [23, с. 553].

Відомо, що у сучасному воєнному конфлікті неможливо перемогти без спеціального захищеного зв'язку гарантованої стійкості. Війська зв'язку та кібербезпеки Збройних Сил України (ЗСУ) – спеціальні війська, призначені для планування та забезпечення розгортання, згортання, функціонування системи зв'язку та інформаційних систем, систем бойового управління та оповіщення, їх нарощування в мирний час, особливий період, в умовах надзвичайного та воєнного стану з метою вирішення завдань забезпечення управління військами

(силами) Збройних Сил України, а також здійснення заходів функціонування національної системи кібербезпеки та відбиття воєнної агресії у кіберпросторі (кібероборони) [26]. В Доктрині Військ зв'язку та кібербезпеки ЗСУ зазначається, що «Сучасні виклики, які зумовлені переходом провідних країн світу до концепції ведення мережецентричних війн, перенесенням театру воєнних дій у площину кіберпростору, все більше і більше вимагають від особового складу Військ зв'язку та кібербезпеки ЗС України опанування та впровадження новітніх засобів зв'язку та технологій, надання сервісів зв'язку для забезпечення функціонування єдиного інформаційного середовища ЗС України та досягнення оперативної й технічної взаємосумісності з іншими складовими сил оборони та державами-членами НАТО» [8, с. 4]. Нині Міністерство оборони України активно працює над можливістю вивести поняття «кібервійна» у правове поле. Передбачається у системі Міністерства оборони України формування кібервійськ або Кіберсил та набуття ними відповідних спроможностей. Забезпечення їх належними фінансовими, кадровими та технічними ресурсами для надання відсічі агресору актуальне та потребує термінового вирішення. Частини та підрозділи Військ зв'язку та кібербезпеки входять до складу усіх видів та окремих родів військ (сил) Збройних Сил України.

Загалом ЗСУ у питанні цифрової трансформації досягнули певних позитивних результатів. В ЗСУ розгорнуті інформаційно-комунікаційні системи та інформаційні мережі: інформаційно-довідкова система АСУ «Дніпро», ІСД-Інтернет, СЕДО, ЗСУ 001, ЗСУ 002, «Персонал» «Оберіг» та інші. Їх метою є зменшення кількості помилок внаслідок людського фактору і заощадити ресурси держави та людини завдяки цифровізації (Урядовий портал). Крім того, DOT-Chain – це інноваційна ІТ-система від Державного оператора тилу для управління тиловими потребами ЗСУ. Зокрема, вже переведено в цифру паперові документи для оптимізації роботи військових. Замість 30 тис. паперів щотижня, які мали опрацьовувати військові, тепер потрібно зробити лише кілька кліків у системі. Це суттєво зменшує обсяг роботи начпродів. За перші дев'ять місяців роботи мобільного застосунку «Армія+» (з серпня 2024 р. – авт.) 180000 військовослужбовців подали щонайменше один електронний рапорт. Загалом понад 1500 військових частин почали роботу з рапортами в застосунку. Крім того, у мобільному додатку «Резерв+» за наявності правових підстав можна оформити відстрочку від мобілізації. Нині на всіх рівнях Сил оборони України впроваджена бойова система DELTA. DELTA – це бойова цифрова екосистема, яка створює технологічну перевагу українського війська: дозволяє бачити поле бою в реальному часі, планувати операції та обмінюватись інформацією в межах підрозділу, бригади, угруповання, а за потреби – і з союзниками. DELTA успішно пройшла перевірку інформаційної безпеки та реальне випробування боєм: під час оборони Києва у 2022, під час знищення Чорноморського флоту, звільнення острова Зміїний і деокупації Херсона. Також Міністерство оборони України розгортає цифрову систему обліку та управління військовослужбовцями «Імпульс». Ця система оптимізує роботу служб персоналу та забезпечує швид-

кий доступ до даних про особовий склад. Крім того, у ЗСУ введено в експлуатацію інформаційну систему «Бюджет», яка дозволяє значно точніше керувати фінансуванням. Розпочато тестування системи «Майно» для автоматизованого обліку всього військового майна, що робить облік, переміщення та розподіл майна значно швидшим, прозорим та безпечнішим (сайт Міністерства оборони України).

Кібернетичною війною фахівці називають комплекс технічних та організаційно-технологічних заходів у межах стратегії гібридної війни, що спрямований на здобуття переваги в інформаційних мережах та кіберпросторі або виведення їх з ладу для підриву дієздатності держави-супротивника [15, с. 250]. Втім, як зазначає Ю. Когут, попри активне використання міжнародною спільнотою терміну «кібервійна», у світі досі не існує загальноприйнятного та вичерпного єдиного визначення цього поняття. Країни-члени ЄС в офіційних документах віддають перевагу нейтральним виразам – «кібератаки» або «кіберзахист» [15, с. 206]. Із законодавством України та сама ситуація. Зокрема, концепція гібридних загроз також є проблематичною. Сучасній науці бракує спільного визначення і термінологія залишається спірною. Через зростання потужності штучного інтелекту та покращення інструментів, що забезпечують взаємодію зі ШІ неможливо погодитись із відсутністю терміну «кібервійна» у Законі України «Про основні засади забезпечення кібербезпеки України». Люди все більше стають залежними від комп'ютерних чи інформаційних технологій (ІТ), що може вплинути на їхню поведінку. Повноваження державних установ також повинні бути чітко визначені. Нагадаємо, що у 2023 році Україна підписала декларацію Блетчлі з безпеки штучного інтелекту. Але нагадаємо також, що ядерна війна породила серед іншого й інтернет. Пол Берен, працюючи на RAND Corporation над питанням забезпечення військового зв'язку під час ядерної війни, розвинув ідею комутації пакетів [34, с. 65]. Через ситуацію розмитості формулювань у російських сценаріях застосування ядерної зброї існує пряма загроза застосування військами РФ тактичної ядерної зброї. Тому українським політикам та державним службовцям необхідно згадати човникові операції стратегічної авіації США під кодовою назвою «Френтік» (англ. Operation Frantic – «Несамовитий») під час Другої світової війни та ініціювати появу чогось схожого на Програму спільного використання ядерної зброї в НАТО (Nuclear Sharing). Запекла суперечка 28 лютого 2025 р. у Білому домі Зеленського з Трампом та Венсом не повинна впливати на відносини між двома народами. Необхідно також поглибити заходи спрямовані на забезпечення безпеки країни від зброї масового знищення, насамперед ядерної, в рамках вже існуючих угод з Великою Британією та Францією. Зокрема, у Польщі неодноразово висловлювали бажання приєднатися до програми ядерного обміну Nuclear Sharing серед країн НАТО. Також Естонія готова приймати на своїй території винищувачі союзників, які можуть нести тактичну ядерну зброю. Нині проблему «безпекового дисбалансу» у Східній Європі здатна вирішити лише ядерна зброя.

На основі проведеного аналізу стану державних механізмів з протидії гібридним загрозам можна сформулювати наступні стратегічні рекомендації:

В основі успішного протистояння, повинно бути виховання фізично і психологічно здорових, розумних патріотів країни через використання ідеологічної парадигми існування незалежної Української держави. Нова гуманітарна політика України не має будуватися на мотиві помсти за розв'язаний геноцид. Тобто не нагадувати гібридну тоталітарну ідеологію «рашизм». Інакше, враховуючи існуючи історичні, політичні, етнічні, мовні, економічні та соціальні суперечності в Україні може початися громадянська війна.

Сектор безпеки і оборони України здатен стати надійною опорою, що гарантує суспільству і кожному громадянину захист від загроз. Однак непідготовлені та невмотивовані військовослужбовці не можуть бути ефективною силою на полі бою навіть з водневою бомбою. Тому, видається правильним підвищення вимог до здоров'я військовослужбовців, тому що у віці 45+ складно витримувати марші у десятки кілометрів з великим навантаженням. Складно позбутися і «втоми війни» через вікові фізичні та психологічні проблеми. Достатньо звернути увагу на те, скільки чорного гумору породила нинішня система проходження військово-лікарських комісій (ВЛК) військовослужбовцями ЗСУ. Більше того, має бути загалом змінено «біологічний» підхід на професійний при комплектації військ. Якщо у осяжній перспективі зазначені питання не вирішити, то зважаючи на проблеми самовільного залишення частин військовослужбовцями та алкоголізму, будь-які морально-психологічні заходи не матимуть сенсу.

Поширення ударних БпЛА, переносних зенітно-ракетних комплексів, мінометів, великокаліберних кулеметів, засобів радіоелектронної боротьби (РЕБ) та систематичне порушення норм міжнародного гуманітарного права призводить до тяжких втрат при евакуації військовослужбовців ЗСУ з поля бою. Або взагалі робить подібну евакуацію неможливою. До сфери військової медицини має бути особлива увага в державі, оскільки тільки так можна гарантувати допомогу у разі отримання травми (поранення, контузії, каліцтва), забезпечити реабілітацію всім військовослужбовцям.

Через вартість озброїти та оснастити всім необхідним можливо лише відносно невелику професійну армію. Те саме і з виплатами військовослужбовцям гідного грошового забезпечення та забезпеченням житлом. Добровольчі формування Сил ТрО вже сьогодні є підготовленим та вмотивованим резервом для професійної армії. Таким чином, запровадження повністю професійної армії має стати стратегічною метою публічного управління. Оскільки, при веденні сучасних бойових дій перемога над противником буде досягатись через перевагу в отриманні достовірної і різнотипної інформації, мобільності, бистроті реакції, в точному вогневому і інформаційному впливі військ (сил), що відбувається в реальному масштабі часі по багатьом об'єктам його економіки, військовим об'єктам і при мінімально можливому ризику для своїх сил і засобів [17, с. 106]. Все це можливо лише при наявності професійно підготовленого та технічно забезпеченого персоналу.

Досвід російсько-української війни показав пріоритетність засобів далекого ураження, бойових літаків, комплексів ППО/ПРО та ракет класу «земля – повітря» з поліпшеними характеристиками, високотехнологічних автономних систем озброєння та сучасної бронетехніки. Зокрема, завдання далекобійних високоточних ударів розмиває межі між стратегічним, оперативним і тактичним рівнем війни. Це не лише нові технології, додаткові робочі місця, збільшення виробництва, а й захист десятків мільйонів людей. Війна за Незалежність України переконливо продемонстрували, що за допомогою нестандартних рішень, високоточної, масової та відносно дешевої зброї разом із застосуванням традиційних систем можна ефективно протистояти великим за чисельністю силам супротивника.

Після завершення війни рекомендується як дослідити громадську думку, так і переглянути конституційну заборону на розташування на території України іноземних військових баз. Необхідно поглибити заходи спрямовані на забезпечення безпеки країни від зброї масового знищення, насамперед ядерної, в рамках вже існуючої угоди між Україною та Францією. Враховуючи двосторонні безпекові домовленості передбачені в Угоді про сторічне партнерство між Україною та Сполученим Королівством Великої Британії і Північної Ірландії, питання ядерної безпеки доцільно базуючись на реалістичному підході також розглянути і з Великою Британією. Це може стати основою для дієвих міжнародно-правових гарантій безпеки від європейських сил. При цьому без'ядерний статус країни не зміниться і Україна не порушить жодних своїх міжнародних зобов'язань.

Висновки з даного дослідження і перспективи подальших досліджень. Проведене дослідження щодо вдосконалення державних механізмів протидії гібридним загрозам в умовах глобалізації дозволяє сформулювати наступні ключові висновки:

1) Концепт «гібридна війна» та «гібридні загрози» еволюціонував від військової доктрини до міждисциплінарного феномену. Поширення неправдивої або маніпулятивної інформації залишається провідним ризиком у коротко- та середньостроковій перспективах. Нинішня концепція гібридної війни потребує переосмислення, оскільки суперечить існуючій ситуації безпеки у світі. Однак сучасна війна є війною на основі інформаційно-комунікативних технологій.

2) В ЄС розвиток стійкості до гібридних загроз вимагає виходу за межі стійкості в окремих сферах, розбудовуючи її системно, враховуючи залежності та взаємозалежності між різними частинами суспільства. Досвід протидії гібридним загрозам та війні у країнах НАТО передбачає комплекс заходів як організаційного та нормативно-правового характеру, так і суто військового.

3) Україна загалом побудувала ефективну систему боротьби з дезінформацією, здатну сформувати стратегічний наратив держави. Однак при доборі персоналу необхідно дотримуватися принципу деполітизації державної служби. Крім того, саме інформаційний напрямок, а не контроль незалежних медіа має

бути головним у діяльності державних відомств. Необхідно уважно ставитись до будь-яких обмежень діяльності медіа. Щоправда, вітчизняне законодавство потребує змін у частині доповнення повноважень, наприклад, Національної ради України з питань телебачення і радіомовлення стосовно соціальних мереж. Враховуючи багатоаспектність гібридних загроз та велику кількість задіяних для протидії різних державних установ та організацій, вважається за доцільне визначити окремого віцепрем'єр-міністра України, який здійснював би загальну координацію. Необхідно врахувати і необхідність поліпшення матеріально-технічного забезпечення та фінансового стану редакцій медіа.

4) Необхідно розглянути можливість прийняття закону про гібридні загрози та гібридну війну, який має визначити правові основи протидії, повноваження органів влади та процедури координації дій, механізми швидкого реагування та принципи екстериторіальної юрисдикції. Крім того, необхідно також визначитися з терміном «кібервійна» та внести відповідні зміни до чинного законодавства. Фахівцями рекомендується створення Національного центру протидії гібридним загрозам як єдиного координаційного органу з розширеними оперативними повноваженнями. Інтеграція України в ЄС і НАТО є ключовою гарантією безпеки.

Подальші наукові дослідження мають бути спрямовані на природу та сутність гібридної війни, як війни нового типу. А також, на забезпечення ядерної безпеки в умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Веселова Л. Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади : монографія. Одеса : ВД «Гельветика», 2020. 488 с.

2. Гібридні загрози та комплексна безпека : навч. посіб. Укл. Карпенко О. О., Осипова Є. Л. Київ : ТОВ «ТРОПЕА», 2024. 76 с. https://doi.org/10.32703/978-617-8268-30-5

3. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ. Київ : Центр глобалістики «Стратегія XXI», 2018. 17-20 с. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf

4. Голопатюк Л., Тимошенко Р. Визначення та аналіз особливостей складових сучасних воєнних конфліктів. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2017. № 1. URL: http://znp-cvsd.nuou.org.ua/article/view/125468

5. Горбулін В. Як перемогти Росію у війні майбутнього. Київ : Брайт Букс, 2021. 243 с.

6. Давидюк М. Як працює путінська пропаганда. Київ : Смолоскип, 2016. 200 с.

7. Дія. 21.04.2025. URL: https://business.diia.gov.ua/history-of-success/yak-stratehichne-planuvannia-dopomahaie-biznesu-pratsiuvaty-systemno

8. Доктрина військ зв'язку та кібербезпеки Збройних Сил України. Київ : «ЦУЛ», 2024. 48 с.

9. Д'яченко К. С. Порівняльний аналіз правового регулювання державно-приватного партнерства в республіці Польща та в Україні. *Молодіжний соціологічний форум НТУ «ХПІ»: матеріали міжнар. наук.-практ. конф. студентів і аспірантів, присвяченої 140-річчю Національного технічного університету «Харківський політехнічний інститут», 16 травня 2025 р., м. Харків.* 2025. С. 118-121. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/5077aba5-6780-49e7-b310-39fad933529c/content

10. Історія і статус. *Сайт Національної ради України з питань телебачення і радіомовлення*. URL: https://webportal.nrada.gov.ua/pro-natsionalnu-radu/#misia

11. CERT-UA. *Державні сайти України*. URL: https://cert.gov.ua/about-us

12. Карамишев Д., Соболь Р., Мирна Н., Євдокимов В. Вплив гібридних загроз на сучасну національну безпеку України. *Державне будівництво*. 2023. № 2(34). 54–66. https://doi.org/10.26565/1992-2337-2023-2-05

13. Карпенко О. Європейський досвід протидії гібридним загрозам для економічного відродження України. URL: https://iepjournal.com/journals/41/2024_41_12_Karpenko.pdf

14. Когут Ю. І. Гібридна війна нового типу як загроза національній безпеці держав. Київ : Консалтингова компанія «СІДКОН»; ВД «ДАКОР», 2023. 348 с.

15. Когут Ю. І. Сучасні технології гібридної війни : практ. посіб. Київ : Консалтингова компанія «СІДКОН»; ВД «Дакор», 2024. 368 с.

16. Кукін І. В. Державне управління інформаційною безпекою особистості : монографія. Київ : ВД «Дакор», 2023. 416 с.

17. Кучеренко Ю. Ф., Носик А. М., Дзьобань О. П. Війни XXI століття: концептуальні аспекти створення мережецентричних систем управління військового призначення : монографія. Ін-т інформації, безпеки і права Нац. акад. прав. наук України. Харків : Право, 2025. 252 с.

18. Левчук Н. Як український NGO-сектор рятує економіку і сам себе. Сайт «Економічна правда». 11 липня 2025 р. URL: https://epravda.com.ua/finances/yak-ukrajinskiy-ngo-sektor-ryatuye-ekonomiku-i-sam-sebe-809076/

19. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : ВД «Кондор», 2019. 272с. URL: http://pdf.lib.vntu.edu.ua/books/2021/Lisovska_2019_272.pdf

20. Лукеря Т. Запровадження місцевих адміністрацій префектурного типу: що це і навіщо Україні? *Портал «Децентралізація»*. 2023, 22 лютого. URL: https://decentralization.ua/news/16147

21. Міністерство культури України. Сайт Міністерства культури України. URL: https://mcsc.gov.ua/pro-ministerstvo/

22. Морозова М. Е. Стратегічне планування. Поняття і етапи стратегічного планування. URL: https://lib.iitta.gov.ua/id/eprint/718325/1/%D0%9C%D0%BE%D1%80%D0%BE%D0%B7%D0%BE%D0%B2%D0%B0_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F_.pdf

23. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О.П. Дзьобаня ; Ін-т інформації, безпеки і права Нац. акад. прав. наук України ; Нац. юрид. ун-т ім. Ярослава Мудрого. 2-ге вид., перероб. й допов. Харків : Право, 2025. 856 с.

24. Ослунд Андерс, Кубілюс Андрюс. Відбудова, реформування та вступ України до ЄС. Львів : Вид-во Старого Лева, 2024. 144 с.

25. Основні завдання Державного центру кіберзахисту Держспецзв'язку. Сайт Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk

26. Островський С. Правовий статус військ зв'язку та кібербезпеки в системі Збройних Сил України. *Київський часопис права*. 2022. № 3. https://doi.org/10.32782/klj/2022.3.13

27. Паламарчук М. Бойові кораблі: еволюція лінкорів та авіаносців. Київ : Віхола, 2024. 352 с. (Серія «Життя»)

28. Положення про Міністерство цифрової трансформації України. *Урядовий портал.* URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919

29. Пушкар О. А. Розвиток державної інформаційної політики України: практичні механізми, теоретичні та методологічні підходи : монографія. Київ : Юрінком Інтер, 2025. 460 с.

30. Про національну безпеку України : Закон України від 21 черв. 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

31. Сааков В. НАТО: Число жертв війни в Україні досягло мільйона. *Медіакомпанія Deutsche Welle (DW).* 2024, 12 груд. URL: https://www.dw.com/uk/nato-cislo-zertv-vijni-v-ukraini-dosaglo-miljona/a-71040820

32. Сухонос В., Сухонос В. Державний механізм забезпечення національної безпеки: інституціонально-правова та технологічна парадигми : монографія. Суми : ПФ «Видавництво «Університетська книга», 2023. 288 с.

33. Сучасні виклики міжнародному порядку: передумови появи та механізми протидії інформаційним і терористичним загрозам : монографія / авт. кол. [С. І. Авраменко, Н. М. Варенья, І. М. Рижов та ін.]; за ред. Н. М. Варенья; УАМП. Київ : Фенікс. Одеса, 2022. 302 с. (Серія монографій: Сучасні виклики міжнародному порядку).

34. Нік Даєр-Візефорд, Матвієнко С. Кібервійна і революція. Інститут Критики; Український науковий Інститут Гарвардського університету. Київ : Критика, 2021. 328 с.

35. Про Заяву Верховної Ради України «Про вчинення Російською Федерацією геноциду в Україні : Постанова Верховної Ради України від 14 квітня 2022 року № 2188-IX. URL: https://zakon.rada.gov.ua/laws/show/2188-IX#Text

36. Феськов І. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики*. 2016. Вип. 58. С. 66–76. URL: http://surl.li/gmhmn

37. Фрідман Л. Командування. Політики військових операцій від Кореї до України. Харків : Книжковий Клуб «Клуб Сімейного Дозвілля», 2025. 672 с.

38. Шеллінг Томас. Стратегія конфлікту. Київ : «ЦЕРЕМ», 2025. 328 с.

39. Яковлева А. М., Кошечкіна Т. М. Сучасний тлумачний словник української мови. Харків : Навчальна література, 2020. 672 с. (Словники від А до Я).

40. Brzezinski Z. The Grand Chessboard: American Primacy and Its Geostrategic Imperatives. New York : Basic Books, 1997. 240 p.

41. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. Boulder : Lynne Rienner Publishers, 1998. 239 p.

42. Castells M. The Rise of the Network Society. 2nd ed. Oxford : Wiley-Blackwell, 2010. 608 p.

43. ENISA. An official website of the European Union. URL: https://www.enisa.europa.eu/about-enisa/regulatory-framework

44. Galeotti M. The Weaponization of Everything: A Field Guide to the New Way of War. New Haven : Yale University Press, 2022. 224 p.

45. CounterIntelligence. Published online: 27 Jan 2025. URL: https://www.researchgate.net/publication/388425995_Hybrid_Threats_and_the_Intelligence_Community_Priming_for_a_Volatile_Age

46. Hoffman F. G. Hybrid Warfare and Challenges. Washington, DC : National Defense University, 2009. 24 p.

47. Huntington S. P. The Clash of Civilizations and the Remaking of World Order. New York : Simon & Schuster, 1996. 368 p.

48. NATO. Strategic Concept 2022. Brussels, 2022. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

49. NATO. The NATO Comprehensive Approach to Security. Brussels, 2022. URL: https://www.nato.int/cps/en/natohq/topics_52877.htm

50. Nye J. S. Soft Power: The Means to Success in World Politics. New York : PublicAffairs, 2004. 208 p.

51. Rid T. Cyber War Will Not Take Place. London : Hurst & Co., 2013. 256 p. https://doi.org/10.1080/01402390.2011.608939

52. United Nations. Charter of the United Nations. 1945. URL: https://www.un.org/en/about-us/un-charter

Стаття надійшла до редакції 13.08.2025 р.
Стаття рекомендована до друку 15.09.2025 р.
Опубліковано 30.12.2025 р.

Dvorianov V. P.,
post-graduate student of the Department of Public Policy
of the Educational and Scientific Institute «Institute of Public Administration»
of V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine.
e-mail: victordvorianov1977@gmail.com https://orcid.org/0000-0002-6705-6549

ANALYSIS OF THE STATE OF STATE MECHANISMS IN UKRAINE TO COUNTER HYBRID THREATS

Annotation. The article is devoted to a comprehensive analysis of state mechanisms responsible for countering hybrid threats. The evolution of the concept of «hybrid war» and «hybrid threats» from military doctrine to an interdisciplinary phenomenon is considered. Models of countering hybrid threats in NATO and the European Union countries, as well as the approaches of post-Soviet states, are studied. Particular attention is paid to mechanisms for countering information and psychological operations of the enemy, as well as those responsible for the cyber defense of the вчаапмиииииии2,

The need for changes in domestic legislation in terms of supplementing the powers of the National Council of Ukraine on Television and Radio Broadcasting with respect to social networks is noted. Also, taking into account the multifaceted nature of hybrid threats and the large number of various state institutions and organizations involved in countering them, it is proposed to identify a separate Deputy Prime Minister of Ukraine who would carry out general coordination. Experts also recommend the creation of the National Center for Countering Hybrid Threats as a single coordination body with expanded operational powers. The study can be used to improve national security systems and increase the state's resilience to new types of wars. Based on the analysis, strategic recommendations have been formulated to increase Ukraine's defense capabilities through deepening European and Euro-Atlantic integration, technological modernization, and increasing the effectiveness of interagency coordination.

Keywords: hybrid threats, hybrid warfare, civil service, state mechanisms, cybersecurity, public administration, resilience.

REFERENCES

1. Veselova, L.Yu. (2020). Cybersecurity in the context of hybrid warfare: administrative and legal principles: monograph. Odesa: Helvetica Publishing Hous. 488 p. [in Ukrainian].

2. Hybrid Threats and Integrated Security: A Study Guide. incl. Karpenko O.O., Osypova E.L. (2024). Kyiv: "TROPEA" LLC. https://doi.org/10.32703/978-617-8268-30-5 [in Ukrainian].

3. Hybrid threats to Ukraine and public security. The experience of the EU and the Eastern Partnership. (2018). *Analytical document*. Kyiv: Center for Global Studies “Strategy XXI”. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf [in Ukrainian].

4. Holopatyuk, L., Tymoshenko, R. (2017). Definition and analysis of the features of the components of modern military conflicts. *Collection of scientific works of the Center for Military and Strategic Studies of the Ivan Chernyakhovsky National Defense University of Ukraine, no. 1.* URL: http://znp-cvsd.nuou.org.ua/article/view/125468 [in Ukrainian].

5. Gorbulin, V. (2021). How to defeat Russia in the war of the future. Kyiv: Bright Books, 243 p. [in Ukrainian].

6. Davydyuk, M. (2016). How Putin's propaganda works. Kyiv: Smoloskyp. 200 p. [in Ukrainian].

7. Action. 04/21/2025. (2025). URL: https://business.diia.gov.ua/history-of-success/yak-stratehichne-planuvannia-dopomahaie-biznesu-pratsiuvaty-systemno [in Ukrainian].

8. Doctrine of the Signal Troops and Cybersecurity of the Armed Forces of Ukraine. (2024). Kyiv: "TsUL". 48 p. [in Ukrainian].

9. Dyachenko, K.S. (2025). Comparative analysis of legal regulation of public-private partnership in the Republic of Poland and in Ukraine. *Youth sociological forum of NTU "KhPI": materials of the international scientific-practical conference of students and postgraduates dedicated to the 140th anniversary of the National Technical University "Kharkiv Polytechnic Institute", May 16, 2025, 118-121.* URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/5077aba5-6780-49e7-b310-39fad933529c/content [in Ukrainian].

10. History and status. Website of the National Council of Ukraine for Television and Radio Broadcasting. URL: https://webportal.nrada.gov.ua/pro-natsionalnu-radu/#misia [in Ukrainian].

11. CERT-UA. State websites of Ukraine. URL: https://cert.gov.ua/about-us

12. Karamyshev, D., Sobol, R., Myrna, N., Yevdokimov, V. (2023). The impact of hybrid threats on the modern national security of Ukraine. *State Formation, no. 2 (34), 54–66*. URL: https://doi.org/10.26565/1992-2337-2023-2-05 [in Ukrainian].

13. Karpenko, O. (2024). European experience in countering hybrid threats for the economic revival of Ukraine. URL: https://iepjournal.com/journals/41/2024_41_12_Karpenko.pdf [in Ukrainian].

14. Kohut, Y.I. (2023). Hybrid war of a new type as a threat to the national security of states. Kyiv: Consulting company "SIDCON"; VD "DAKOR". 348 p.

15. Kohut, Yu.I. (2024). Modern technologies of hybrid warfare: a practical manual. Kyiv: Consulting Company "SIDKON"; VD "Dakor". 368 p. [in Ukrainian].

16. Kukin, I.V. (2023). State management of information security of the individual: monograph. Kyiv: VD "Dakor". 416 p. [in Ukrainian].

17. Kucherenko, Yu.F., Nosyk, A.M., Dzyoban, O.P. (2025). Wars of the 21st century: conceptual aspects of creating network-centric military control systems: monograph. Inst. of Information, Security and Law of the National Academy of Law of Ukraine. Kharkiv: Pravo, 2025. 252 p. [in Ukrainian].

18. Levchuk, N. (2025). How the Ukrainian NGO sector saves the economy and itself. / Website "Economic Pravda". July 11, 2025. URL: https://epravda.com.ua/finances/yak-ukrajinskiy-ngo-sektor-ryatuye-ekonomiku-i-sam-sebe-809076/ [in Ukrainian].

19. Lisovska, Yu.P. (2019). Cybersecurity: risks and measures: a training manual. Kyiv: Publishing house "Kondor", 2019. 272 p. URL: http://pdf.lib.vntu.edu.ua/books/2021/Lisovska_2019_272.pdf [in Ukrainian].

20. Lukerya, T. (2023). Introduction of local prefectural-type administrations: what is it and why does Ukraine need it? Portal "Decentralization". 2023, February 22. URL: https://decentralization.ua/news/16147 [in Ukrainian].

21. Ministry of Culture of Ukraine. Website of the Ministry of Culture of Ukraine. URL: https://mcsc.gov.ua/pro-ministerstvo/ [in Ukrainian].

22. Morozova, M.E. Strategic planning. Concept and stages of strategic planning. URL: https://lib.iitta.gov.ua/id/eprint/718325/1/%D0%9C%D0%BE%D1%80%D0%BE%D0%B7%D0%BE%D0%B2%D0%B0_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F_.pdf [in Ukrainian].

23. National Security: Worldview and Theoretical and Methodological Principles: Monograph (2025). General Editor O.P. Dzyobanya; Institute of Information, Security and Law of the National Academy of Law of Ukraine; Yaroslav the Wise National Law University. 2nd ed., revised and supplemented. Kh: Pravo. 856 p. [in Ukrainian].

24. Aslund Anders, Kubilius Andrius. (2024). Reconstruction, Reform and Ukraine's Accession to the EU.: Anders Åslund, Andrius Kubilius; translated from English. Andriya Kovalchuk. Lviv: Stary Lev Publishing House. 144 p. [in Ukrainian].

25. Main tasks of the State Cyber Defense Center of the State Special Communications and Information Protection Service of Ukraine / Website of the State Cyber Defense Center of the State Special Communications and Information Protection Service of Ukraine. URL: https://scpc.gov.ua/uk [in Ukrainian].

26. Ostrovsky, S. (2022).Legal status of signal troops and cybersecurity in the system of the Armed Forces of Ukraine. *Kyiv Law Journal, no. 3*. https://doi.org/10.32782/klj/2022.3.13 [in Ukrainian].

27. Palamarchuk, M. (2024). Battleships: the evolution of battleships and aircraft carriers / Maksym Palamarchuk. Kyiv: Vikhola. 352 p. (Series “Life”) [in Ukrainian].

28. Regulations on the Ministry of Digital Transformation of Ukraine / Government Portal. URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919 [in Ukrainian].

29. Pushkar, O.A. (2025). Development of the State Information Policy of Ukraine: Practical Mechanisms, Theoretical and Methodological Approaches: Monograph. Kyiv: Yurinkom Inter. 460 p.

30. On National Security of Ukraine. (2018). Law of Ukraine of June 21, 2018 No. 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

31. Saakov, V. (2018). NATO: The number of victims of the war in Ukraine has reached a million. Deutsche Welle (DW) media company. 2024, December 12. URL: https://www.dw.com/uk/nato-cislo-zertv-vijni-v-ukraini-dosaglo-miljona/a-71040820 [in Ukrainian].

32. Sukhonos, V., Sukhonos, V. (2023). The state mechanism for ensuring national security: institutional, legal and technological paradigms: monograph. Sumy: PF "University Book Publishing House". 288 p. [in Ukrainian].

33. Modern challenges to the international order: prerequisites for the emergence and mechanisms for countering information and terrorist threats: monograph (2022). S.I. Avramenko, N.M. Varenya, I.M. Ryzhov and others [Eds.]; edited by N. M. Varenya; UAMP. Kyiv: Phoenix. Odesa, 2022. 302 p. [in Ukrainian].

34. Nick Dyer-Wiseford, Matvienko S. (2021). Cyberwar and revolution. *Institute of Criticism; Ukrainian Research Institute of Harvard University*. Kyiv: Kritika. 328 p. [in Ukrainian].

35. Resolution of the Verkhovna Rada of Ukraine “On the Statement of the Verkhovna Rada of Ukraine “On the Commission of Genocide in Ukraine by the Russian Federation” dated April 14, 2022 No. 2188-IX. (2018). URL: https://zakon.rada.gov.ua/laws/show/2188-IX#Text [in Ukrainian].

36. Feskov, I. (2016). Basic methods of conducting hybrid warfare in the modern information society. *Current Policy Issues, is. 58, 66–76.* URL: http://surl.li/gmhmn [in Ukrainian].

37. Fridman, L. (2025). Command. Policies of military operations from Korea to Ukraine / Lawrence Fridman; trans. from English. T. Mykytyuk. Kharkiv: Book Club “Family Leisure Club”. 672 p. [in Ukrainian].

38. Schelling, T. (2025). Conflict Strategy / Thomas Schelling. Kyiv: “CERTAINTY”. 328 p. [in Ukrainian].

39. Yakovleva, A.M., Koshechkina T.M. (2020).Modern Explanatory Dictionary of the Ukrainian Language. Kharkiv: Educational Literature. 672 p. (Dictionaries from A to Z). [in Ukrainian].

40. Brzezinski, Z. (1997). The Grand Chessboard: American Primacy and Its Geostrategic Imperatives. New York: Basic Books. 240 p.

41. Buzan, B., Wæver, O., de Wilde, J. (1998). Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers. 239 p.

42. Castells, M. (2010). The Rise of the Network Society. 2nd ed. Oxford: Wiley-Blackwell. 608 p.
43. ENISA. An official website of the European Union. URL: https://www.enisa.europa.eu/about-enisa/regulatory-framework (дата звернення: 22.12.2023).
44. Galeotti, M. (2022). The Weaponization of Everything: A Field Guide to the New Way of War. New Haven: Yale University Press. 224 p.
45. CounterIntelligence. Published online: 27 Jan 2025. (2025). URL: https://www.researchgate.net/publication/388425995_Hybrid_Threats_and_the_Intelligence_Community_Priming_for_a_Volatile_Age (дата звернення: 03.07.2025).
46. Hoffman, F.G. (2009). Hybrid Warfare and Challenges. Washington, DC: National Defense University. 24 p.
47. Huntington, S.P. (1996). The Clash of Civilizations and the Remaking of World Order. New York: Simon & Schuster. 368 p.
48. NATO. (2022). Strategic Concept 2022. Brussels. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept
49. NATO. (2022). The NATO Comprehensive Approach to Security. Brussels. URL: https://www.nato.int/cps/en/natohq/topics_52877.htm
50. Nye, J.S. (2004). Soft Power: The Means to Success in World Politics. New York: PublicAffairs. 208 p.
51. Rid, T. (2013). Cyber War Will Not Take Place. London: Hurst & Co. 256 p. https://doi.org/10.1080/01402390.2011.608939
52. United Nations. (1945). Charter of the United Nations. URL: https://www.un.org/en/about-us/un-charter

The article was received by the editors 13.08.2025.
The article is recommended for printing 15.09.2025.
Published 30.12.2025.