УДК 355.1
DOI https://doi.org/10.51547/ppp.dp.ua/2024.6.14

Яровой Тихон Сергійович,
доктор наук з державного управління, доцент,
завідувач кафедри національної безпеки, менеджменту та публічного адміністрування
Чернігівського інституту інформації, бізнесу і права
ЗВО «Міжнародний Науково-технічний університет імені академіка Юрія Бугая»
ORCID ID: 0000-0002-7266-3829

Снісар Богдан Юрійович,
аспірант кафедри національної безпеки, публічного управління та адміністрування
Державного університету «Житомирська політехніка»
ORCID ID: 0009-0007-0091-0943

ФОРМУВАННЯ ВОЄННОЇ БЕЗПЕКИ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ: ВИКЛИКИ І ПЕРСПЕКТИВИ СЬОГОДЕННЯ

FORMATION OF MILITARY SECURITY IN THE SYSTEM OF PUBLIC ADMINISTRATION: CHALLENGES AND PROSPECTS FOR TODAY

Стаття присвячена дослідженню формування воєнної безпеки в системі державного управління з акцентом на сучасні виклики та перспективи забезпечення обороноздатності держави в умовах мінливого геополітичного та технологічного ландшафту. У дослідженні проаналізовано теоретичні засади воєнної безпеки, розглянуто традиційні та сучасні підходи до оборонних стратегій держави. Приділено увагу зростаючій ролі кібернетичних війн, гібридних конфліктів та інформаційних операцій у формуванні сучасної політики безпеки. Обґрунтовано необхідність інтеграції міжвідомчої координації, стратегічного планування та технологічних інновацій в управління воєнною безпекою для посилення національної системи оборони. Дослідження підкреслило критичну роль державних інституцій у синхронізації військових, дипломатичних, економічних і технологічних ресурсів для ефективного реагування на нові загрози. Аналіз засвідчив, що адаптація оборонних стратегій до заходів кібербезпеки, застосування штучного інтелекту і сучасних систем спостереження, значно підвищує стійкість структур національної безпеки. Визначено основні ризики, пов'язані з сучасними загрозами безпеці, включаючи кібершпигунство, асиметричну тактику ведення війни та геополітичну нестабільність, які потребують адаптивних політичних рішень та проактивних механізмів управління. Дослідження окреслило потенційні вразливості систем національної безпеки, що виникають через бюрократичну неефективність, брак міжвідомчої співпраці та затримку у прийнятті рішень у кризових ситуаціях. Виявлено перспективи подальших досліджень щодо розробки стратегічних політик безпеки, які включають новітні оборонні технології, стійкість до кібернетичних війн та процеси прийняття рішень на основі розвідданих. Дослідження запропонувало рекомендації щодо підвищення ефективності управління воєнною безпекою, шляхом постійної інституційної модернізації, міжнародної співпраці та високоадаптивних законодавчих реформ.

Ключові слова: *воєнна безпека, державне управління, національна оборона, кібербезпека, гібридна війна, штучний інтелект, стратегічне планування, загрози безпеці, прогнозування загроз безпеці, перспективи розвитку системи безпеки, оборонна політика, геополітична нестабільність.*

The article is devoted to the study of the formation of military security within the system of public administration, emphasizing contemporary challenges and prospects for ensuring national defense capabilities in an evolving geopolitical and technological landscape. The research analyzed the theoretical foundations of military security, considering traditional and modern approaches to state defense strategies. Attention was paid to the increasing role of cyber warfare, hybrid conflicts, and information operations in shaping contemporary security policies.

Substantiated was the necessity of integrating interagency coordination, strategic planning, and technological innovation into military security management to enhance national defense systems. The study highlighted the critical role of government institutions in synchronizing military, diplomatic, economic, and technological resources to respond effectively to emerging threats. The analysis demonstrated that the adaptation of defense strategies to include cybersecurity measures, artificial intelligence applications, and advanced surveillance systems significantly increases the resilience of national security structures.

Determined were the primary risks associated with modern security threats, including cyber espionage, asymmetric warfare tactics, and geopolitical instability, which necessitate adaptive policy responses and proactive governance mechanisms. The study outlined the potential vulnerabilities of national security systems stemming from bureaucratic inefficiencies, lack of interagency cooperation, and delayed decision-making in crisis situations.

Investigated were the prospects for further research on the development of strategic security policies that incorporate emerging defense technologies, cyber warfare resilience, and intelligence-driven decision-making processes. The study proposed recommendations for improving the effectiveness of military security governance through continuous institutional modernization, international collaboration, and adaptive legislative reforms.

Key words: *military security, public administration, national defence, cybersecurity, hybrid warfare, artificial intelligence, strategic planning, security threats, forecasting security threats, prospects for the development of the security system, defence policy, geopolitical instability.*

Обґрунтування актуальності теми дослідження. Формування воєнної безпеки в системі державного управління набуває першочергового значення в сучасному геополітичному та технологічному ландшафті, що стрімко змінюється. Сучасні держави стикаються з безпрецедентним спектром безпекових викликів – традиційні військові загрози зберігаються паралельно зі зростанням кібератак, гібридних війн та інформаційної зброї. У цьому контексті надійна воєнна безпека не може бути досягнута виключно за допомогою традиційних оборонних заходів; вона вимагає добре скоординованого підходу, який об'єднує військові, дипломатичні, технологічні та економічні ресурси. Державне управління стає стрижнем для гармонізації цих різноманітних елементів, забезпечуючи правові, фінансові та організаційні рамки, необхідні для розробки, впровадження та підтримки комплексної політики безпеки.Актуальність даного дослідження підкреслюється все більш взаємопов'язаним глобальним середовищем, де проблеми національної безпеки переходять у міжнародну сферу, і навпаки. Оскільки альянси, міжнародні договори та механізми забезпечення безпеки стають дедалі складнішими, здатність системи державного управління ефективно управляти цими взаємодіями стає одночасно стратегічним активом і мірилом загальної стійкості держави. Тому, вивчення формування воєнної безпеки в контексті державного управління є не лише академічно актуальним, але й необхідним для прийняття політичних рішень, спрямованих на збереження національної стабільності, захист громадян і підтримку міжнародного миру і безпеки.

Аналіз останніх досліджень і публікацій. Вивчення проблем та перспектив воєнної безпеки в системі державного управління привертає значну увагу науковців, особливо – в контексті еволюції геополітичної напруженості, технологічного прогресу та адміністративних реформ. Дослідники вивчають історичну еволюцію та теоретичні засади воєнної безпеки, підкреслюючи вплив глобальних змін у розстановці сил, стратегічної конкуренції та зростаючої ролі гібридних загроз на формування національної оборонної політики (Бондаренко В. Д., Buzan B., Frederickson H. G., Smith K. B., Larimer C., Licari M. J., Hoffman F. G., Писаренко Т. В., Кваша Т., Гаврис Т., Попов В. М., Богатов О. І., Кріслата О., Резнікова О. О., Поліщук А. С., Шишкін І., Воронова О., Дацьо Т.). Наукові дослідження підкреслюють необхідність комплексного підходу, який поєднує традиційні військові стратегії з сучасними імперативами безпеки, включаючи кібербезпеку, застосування штучного інтелекту та заходи космічної безпеки. Проте, аналіз загроз і перспектив подальшого розвитку публічного управління воєнною безпекою, зберігає свою актуальність і надалі.

Метою дослідження є аналіз специфіки формування сучасної воєнної безпеки в системі державного управління, визначення ключових викликів та перспектив її ефективної реалізації в сучасному геополітичному та технологічному ландшафті.

Основний зміст дослідження. Традиційні концепції військової безпеки зосереджувалися на захисті територіальної цілісності і підтримці збройних сил, здатних стримувати або відбивати загрози, що, зокрема, було сформульовано Клаузевіцем, коли він описав війну як продовження політичної взаємодії, сформованої стратегічними і тактичними міркуваннями [1]. Згодом Бузан запропонував розширений погляд на безпеку, який охоплює не лише територіальні чи військові виміри, але й економічні, екологічні та соціальні чинники, тим самим визнаючи багатогранність загроз, з якими стикаються сучасні держави [2]. У сучасну епоху, яка характеризується високо взаємопов'язаними глобальними ланцюгами постачання, складними цифровими мережами і безперервними технологічними інноваціями, сфера військової безпеки ще більше розширилася, включивши в себе ряд нових проблем, таких як кібербезпека, космічна безпека і енергетична безпека.

Державне управління забезпечує основні структури, процеси і правові рамки, за допомогою яких формулюється і впроваджується оборонна політика і військові операції – важлива функція, на якій наголошують Фредеріксон, Сміт і Ларімер, підкреслюючи, що добре функціонуючі адміністративні інститути є необхідними для забезпечення ефективного управління в сфері оборони [3]. Адміністративні органи відповідають не

лише за розподіл ресурсів, стратегічне планування і оцінку програм, але й за інтеграцію різних державних структур, в тому числі – міністерств оборони, розвідувальних служб, законодавчих комітетів і судових органів, – в єдину структуру, здатну реагувати на загрози, які часто виходять за межі компетенції будь-якого окремого відомства. Дж. Розенау наголошує, що управління як на національному, так і на міжнародному рівнях значною мірою формує середовище безпеки, ілюструючи, як узгодженість політики, правові інструменти і механізми підзвітності можуть узгодити дії міністерств оборони, міністерств закордонних справ і неурядових суб'єктів таким чином, щоб підвищити стійкість.

Нещодавні дослідження в галузі безпеки привернули увагу до комплексних загроз, які діють у різних сферах, причому гібридна війна стає критично важливою проблемою, яка поєднує звичайні військові дії, нерегулярну тактику і цілеспрямовані кібератаки. Хоффман підкреслює, що ці гібридні загрози часто використовують інституційні слабкості на різних рівнях управління, що зумовлює необхідність синхронізованих відповідей, які об'єднують військову готовність, обмін розвідданими і дипломатичну взаємодію в єдиний, уніфікований підхід [4]. Інформаційна війна, що ведеться за допомогою дезінформаційних кампаній і маніпуляцій у соціальних мережах, може дестабілізувати політичні інститути і підірвати довіру до органів державної влади, що вимагає додаткових адміністративних компетенцій у сфері кібербезпеки, стратегічних комунікацій і правового нагляду. Інший феномен пов'язаний з поширенням суб’єктів, що діють за межами традиційних державних кордонів, включаючи терористичні організації та транснаціональні злочинні мережі, чия здатність підривати національну оборону зросла в умовах глобального мережевого середовища. Досягнення в галузі штучного інтелекту, автономних систем озброєнь і можливостей ведення кібервійни, вимагають переоцінки структури і управління військовою безпекою. Дедалі ширше використання алгоритмів машинного навчання для вдосконалення розвідувальних операцій, аналізу стратегічних ризиків і автоматизації оборонних систем підкреслює зростаючу роль технологій у забезпеченні військової готовності. Однак, залежність від цифрових систем створює додаткові вразливості, в тому числі ризик кібер-саботажу, радіоелектронної боротьби і використання штучного інтелекту для наступальних операцій [5]. Відтак, перед урядами стоїть завдання не лише регулювати ці технології, але й забезпечувати етичний нагляд, міжнародне співробітництво та комплексні захисні механізми для зменшення ризиків для безпеки, пов'язаних з новими технологіями.

Прискорена інтеграція штучного інтелекту і кібервійни в сучасні військові стратегії, створює як безпрецедентні можливості, так і значні виклики безпеці, оскільки державні і недержавні суб'єкти все частіше використовують вразливості в мережах критичної інфраструктури (у тому числі в електромережах, фінансових установах і системах зв'язку), що призводить до потенційних збоїв, які не лише загрожують національній безпеці, але й підривають довіру громадськості до урядових інститутів. Військове застосування ШІ, починаючи від автономної зброї і закінчуючи складними аналітичними системами, що використовуються в розвідувальних операціях, вимагає створення всеосяжної правової бази, механізмів етичного нагляду та адаптивних політичних заходів для забезпечення відповідальної розробки, розгортання і регулювання, тим самим зменшуючи ризики, пов'язані з алгоритмічними упередженнями, збоями в роботі систем і ненавмисною ескалацією конфліктних сценаріїв.

Зважаючи на зростаючу складність загроз воєнній безпеці, органи державного управління повинні постійно адаптувати правові рамки, моделі управління і механізми міжвідомчої співпраці до нових викликів, що виникають. Взаємопов'язаний характер сучасного стратегічного ландшафту свідчить про те, що односторонні заходи можуть виявитися недостатніми, що посилює необхідність спільних механізмів управління, які виходять за межі національних кордонів. Стратегічні партнерства, регіональні оборонні союзи та багатосторонні безпекові ініціативи відіграють ключову роль у зміцненні колективної безпеки, вимагаючи від держав проактивної дипломатії та зусиль з правової гармонізації.

Розширення мілітаризації космічного простору, коли технологічно розвинені країни посилюють свої можливості з розгортання протисупутникової зброї, підвищує складність сучасної військової безпеки, вводячи нові виміри геополітичного суперництва, які виходять за рамки наземних конфліктів, що вимагає скоординованих заходів міжнародної політики, які збалансовують технологічний прогрес з правовими і дипломатичними імперативами, спрямованими на запобігання широкомасштабним конфронтаціям у космосі [6]. Зростаюча залежність від супутникових систем зв'язку, спостереження і навігації підкреслює нагальність розробки нормативно-правової бази,

яка б вирішувала питання управління космосом, контролю над озброєннями і стратегічної стабільності, що змушує тих, хто формує оборонну політику, інтегрувати космічну безпеку в ширші стратегії військового і державного управління. Зростаюче поширення гібридної війни, що характеризується одночасним розгортанням звичайних збройних сил, іррегулярної тактики ведення бойових дій, економічного примусу, кібероперацій і дезінформаційних кампаній, вимагає фундаментальної переоцінки традиційної оборонної політики з огляду на те, що противники використовують асиметричні переваги, інтегруючи кінетичні і некінетичні стратегії для дестабілізації державних структур, не вступаючи в повномасштабну військову конфронтацію [7]. Складність цих еволюціонуючих загроз безпеці вимагає від органів державного управління багатовимірного підходу, що сприяє міжвідомчій співпраці між оборонним, розвідувальним та правоохоронним секторами, а також включає в себе передові аналітичні можливості для виявлення, протидії та нейтралізації гібридних загроз на різних рівнях управління. Відродження стратегічного суперництва між великими світовими державами, що виражається в ескалації нарощування військових сил, економічних санкціях і дипломатичних перегрупуваннях, відродило традиційні дилеми безпеки, які змушують держави переоцінювати свою національну оборонну політику, інвестувати в модернізацію військового потенціалу і зміцнювати альянси, щоб протистояти потенційним загрозам, пов'язаним з геополітичними маневрами супротивників. Необхідність для інститутів державного управління формулювати довгострокові стратегічні рамки безпеки, що включають військову готовність, розвідувальні можливості та економічну стійкість, стає все більш очевидною в умовах, коли нові регіональні альянси і зміна динаміки сили впливають на траєкторію розвитку глобальної архітектури безпеки. Однією з найбільш фундаментальних стратегій зміцнення воєнної безпеки в рамках державного управління є запровадження комплексного та інтегрованого підходу до управління, за якого міністерства, відповідальні за оборону, внутрішні справи, зовнішню політику та управління фінансами, разом з розвідувальними службами, беруть участь у безперешкодному співробітництві з метою забезпечення цілісної та ефективної стратегії безпеки. Інституціоналізація рад національної безпеки, міжвідомчих координаційних органів і спеціалізованих робочих груп, що займаються оцінкою загроз і управлінням реагуванням на них, значно посилює спроможність підтримувати єдиний політичний курс, створюючи середовище, в якому обмін розвідданими, швидке прийняття рішень і синхронізовані оперативні зусилля зменшують вразливість як до традиційних, так і до новітніх загроз [8]. Здатність інституціоналізувати механізми обміну даними в режимі реального часу, покращити взаємодію між суб'єктами безпеки та інтегрувати технологічні інновації в стратегічні операції забезпечує узгодження цілей національної безпеки з сучасними оборонними вимогами, мінімізуючи неефективність, яка може виникнути через бюрократичну фрагментацію.Пріоритетність досліджень, розробок і технологічних інновацій у секторі безпеки є важливим компонентом сучасних стратегій воєнної безпеки, що вимагає цільових інвестицій у системи кібербезпеки, аналітику на основі штучного інтелекту, автономні оборонні платформи і зашифровані системи зв'язку, які підвищують оперативну стійкість. Співпраця між державними установами і приватними технологічними компаніями дає можливість прискорити інновації, використовуючи досвід у таких нових галузях, як квантові обчислення, супутникове спостереження і прогнозна оцінка загроз на основі машинного навчання, забезпечуючи при цьому, щоб органи державного управління здійснювали регуляторний нагляд за дотриманням імперативів національної безпеки і стандартів захисту даних [9]. Розробка законодавчої бази, яка регулює ці технологічні досягнення, разом з надійними механізмами нагляду, що забезпечують баланс між міркуваннями безпеки і громадянськими свободами, гарантує, що розвиток військових технологій слугуватиме цілям національної оборони, водночас зменшуючи ризики, пов'язані з несанкціонованим доступом, експлуатацією або етичними дилемами, що оточують автономне прийняття військових рішень.З огляду на зростаючу складність транснаціональних загроз безпеці – від кібершпигунства до асиметричної війни і геополітичної нестабільності – здатність держав зміцнювати міжнародні і регіональні альянси стає важливим фактором забезпечення стійкості національної оборони і військової готовності. Розширення співпраці через угоди про обмін розвідданими, багатонаціональні спільні операції та регіональні оборонні структури дозволяє державам отримувати вигоду від колективного досвіду, спільних ресурсів та скоординованих стратегічних відповідей на еволюціонуючі загрози [10]. Гармонізація політики безпеки, розробка уніфікованих оперативних доктрин і укладання юридично зобов'язуючих

угод, які сприяють оперативній сумісності між оборонними установами країн Альянсу, не лише посилюють потенціал стримування, але й забезпечують узгодженість заходів з національної безпеки з більш широкими зусиллями з підтримки регіональної стабільності. Впровадження механізмів реагування на транскордонні кризи, дипломатичні ініціативи з врегулювання конфліктів і спільні військові навчання ще більше посилюють здатність органів державного управління орієнтуватися в складних сучасних викликах безпеці в глобально взаємо-пов'язаному оборонному ландшафті.Забезпечення ефективного управління воєнною безпекою потребує висококваліфікованих і добре підготовлених державних службовців, здатних управляти складними політичними, адміністративними і стратегічними аспектами, пов'язаними з національною обороною. Розробка структурованих навчальних програм, які наголошують на стратегічному передбаченні, плануванні реагування на кризові ситуації, управлінні програмами і методології оцінки розвідданих, посилює інституційну спроможність вирішувати багатогранні безпекові виклики. Ініціативи з розвитку лідерства, які заохочують етичне врядування, міжвідомчу співпрацю та адаптивне прийняття рішень в органах безпеки, сприяють створенню професійного середовища, в якому реалізація політики узгоджується з пріоритетами національної оборони, що змінюються. Інтеграція передових освітніх програм, цільових стратегій розвитку персоналу та інституційних механізмів обміну знаннями зміцнює фундамент людського капіталу, необхідний для довгострокової стійкості структур управління воєнною безпекою.

Висновки та перспективи подальших досліджень. Розвиток воєнної безпеки в рамках державного управління залишається критично важливим компонентом національних оборонних стратегій, що вимагає багатовимірного підходу, який інтегрує міжвідомчу координацію, технологічний прогрес, міжнародне співробітництво, розбудову потенціалу та адаптивні політичні рамки. Зростаюча складність сучасних викликів безпеці вимагає переходу до цілісних моделей управління, які підвищують швидкість реагування, стійкість і стратегічне передбачення у протидії як традиційним, так і новим загрозам. Необхідність міжвідомчої координації підкреслює важливість безперешкодної співпраці між міністерствами оборони, розвідувальними службами, зовнішньополітичними відомствами і фінансовими установами, що забезпечує узгодження стратегічних цілей з імперативами національної безпеки. Інтеграція обміну розвідданими в режимі реального часу, синхронізованих оперативних механізмів і міжсекторальної гармонізації політики значно зменшує вразливість, посилюючи стабільність системи воєнної безпеки перед обличчям нових геополітичних загроз.Майбутні дослідження мають бути зосереджені на впливі новітніх технологій на управління військовою безпекою, еволюції стратегій гібридної війни та ролі штучного інтелекту в розвідувальних операціях. Крім того, оцінка довгострокових наслідків загроз кібербезпеці, ефективності регіональних оборонних угод і стійкості систем державного управління в умовах кризових сценаріїв надасть цінну інформацію для політиків. Постійно вдосконалюючи моделі управління і адаптуючи стратегічні підходи, державне управління може відігравати вирішальну роль у формуванні ефективної політики воєнної безпеки, що забезпечує національну і міжнародну стабільність в умовах дедалі більшої невизначеності глобального ландшафту.

REFERENCES:

1. Bondarenko V. D. (2021) Kontseptsiia vzaiemopoviazanosti «viiny» ta «polityky» Karla fon Klauzevitsa u konteksti vedennia voiennykh dii u KhKhI stolitti na prykladi rosiisko-ukrainskoho voienno-asymetrychnoho konfliktu [«Carl von Clausewitz's concept of the interrelationship of «war» and «politics» in the context of conducting military operations in the 21st century on the example of the Russian-Ukrainian military-asymmetric conflict»]. *Molodyj vchenyj*. vol. 5(1). pp. 85-88. Available at http://nbuv.gov.ua/UJRN/molv_2021_5(1)_19.

2. Buzan B. (1993), Societal Security, State Security, and Internationalisation, in Waever et al, Identity, Migration and the New Security Agenda in Europe, London, Pinter, P. 41–58.

3. Frederickson, H. G., Smith, K.B., Larimer, C., & Licari, M. J. (2016). The Public Administration Theory Primer (3rd ed.). Routledge. Available at https://doi.org/10.4324/9780429494369

4. HoffmanF.G.(2009).Hybridvs.compoundwar.ArmedForcesJournal,Oct.Availableathttp://armedforcesjournal.com/hybrid-vs-compound-war/ .

5. Pysarenko T. V., Kvasha T., Havrys T. (2021), *Analiz svitovykh tekhnolohichnykh trendiv u vijs'kovij sferi*: [Analysis of world technological trends in the military sphere], za zah. redaktsiieiu T. V. Pysarenko. UkrINTEI, Kiev, Ukraine Available at https://mon.gov.ua/static-objects/mon/sites/1/innovatsii-transfer-tehnologiy/2021/09/30/Analiz.svit.tekhn.trend.viysk.sferi-2021.30.09.pdf

6. Popov V. M., Bohatov O. I. (2020). Mizhnarodne kosmichne pravo i militaryzatsiia kosmosu [International Space Law and the Militarization of Space]. *Mizhnarodne pravo*. vol. 3. pp. 231-239. Available at https://doi.org/10.32842/2078-3736/2020.3.35 .

7. Krislata O. (2018). Krislata O. Hibrydna viina ta yii informatsiina skladova [Hybrid War and Its Information Component]. *Zbirnyk prats' Naukovo-doslidnoho instytutu presoznavstva*. Vyp. 8. pp. 190-199. Available at http://nbuv.gov.ua/UJRN/ZPNDZP_2018_8_14 .

8. Reznikova O. O. (2021), *Orhanizatsiia systemy zabezpechennia natsional'noi stijkosti na rehional'nomu i mistsevomu rivniakh*. [Organization of the System for Ensuring National Stability at the Regional and Local Levels.Kyiv]. NISD, Kyiv. Ukraine. Available at https://niss.gov.ua/sites/default/files/2021-09/analytrep_08_2021.pdf

9. Polischuk A. S. (2023), Innovatsii yak stratehichnyi imperatyv peremohy u rosiisko-ukrainskii viini: vyklyky i mozhlyvosti dlia oboronno-promyslovoho kompleksu Ukrainy [Innovation as a strategic imperative for victory in the Russian-Ukrainian war: challenges and opportunities for the defense-industrial complex of Ukraine]. *Transformatsijna ekonomika*. vol. 5 (05). pp. 103-108. Available at https://transformations.in.ua/index.php/journal/article/view/72

10. Shyshkin I., Voronova O. and Dats'o T. (2023). Mizhnarodni vidnosyny Ukraina – NATO: suchasnyi stan i shliakhy rozvytku [International relations Ukraine – NATO: current state and ways of development]. *Journal of Innovations and Sustainability*, vol.7(3), Available at https://doi.org/10.51599/is.2023.07.03.02.