Вісник Львівського університету. Серія філос.-політолог. студії. 2025. Випуск 62, с. 345–351
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 62, p. 345–351

УДК 351.321
DOI https://doi.org/10.30970/PPS.2025.62.41

ДЕМОКРАТИЧНА ЕКОСИСТЕМА НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ПОЛІТИЧНІ ЧИННИКИ ФОРМУВАННЯ

Вячеслав Сергеєв
Державний університет «Житомирська політехніка»,
кафедра політології та державного управління
вул. Чуднівська, 103, 10005, м. Житомир, Україна

У статті проаналізовано демократизацію ухвалення рішень та практик аналізу ситуації в безпековому секторі, що є основою більш оперативного та якісного відпрацювання безпекових завдань на широкій міждисциплінарній основі для сучасної України, яка перебуває в стані війни. Дослідження розкриває класичні доробки та новітні досягнення доречно звернутися до питання формування гнучких структур політичної безпеки на міжнародному й національному рівнях. Особлива увага приділяється інституціоналізації демократичної безпекової мережа, яка повинна ґрунтуватися на спільних демократичних цінностях, повазі до суверенітету та прагматичному підході до співпраці, який адаптується до геополітичної колаборації ціннісно споріднених держав. У цьому контексті розкрито спроможність інтегрувати наявні двосторонні та багатосторонні домовленості про безпеку, зменшуючи спірні позиції та сприяючи взаємодії між державами-членами. Виокремлено ключові характеристики безпекової мережі, якими є створення безпечної, сумісної комунікаційної інфраструктури, що забезпечує обмін інформацією в режимі реального часу.

Досліджено та проаналізовано інституалізацію мережної безпекової інфраструктури, яка сприятиме швидкому поширенню інформації про загрози, пов'язані з тероризмом, кібератаками, гібридною війною та іншими викликами безпеці. Зокрема, оцінено перспективи впровадження алгоритмів та протоколів антикризового менеджменту, яке передбачає задіяння механізмів ситуаційної співпраці, оперативних нарад і конкретних рішень в умовах викликів ризиків та загроз. Обґрунтовано важливість практик горизонтальної безпекової співпраці керівництва правоохоронних та безпекових структур в Україні.

Ключові слова: демократичне врядування, політична безпека, національна безпека, політичні загрози, політичні інститути, громадянське суспільство, політичні експерти.

Постановка проблеми. У сучасних країнах НАТО та ЄС відбуваються процеси інституційної модернізації визначення ризиків, загроз і небезпек, пов'язаних з політичним урядуванням, захистом прав людини та стійкості нормативно-правового середовища. Нормативно-правові засади, закладені всередині другої половини XX століття, не повною мірою відповідають реаліям цифрової політики. Штучний бюрократичний розподіл предметів відання, а також відповідальності й джерел ресурсного забезпечення політичного врядування на сучасному етапі дещо гальмує ухвалення рішень та оперативні дії в безпековому секторі. Тому країни Північноатлантичного альянсу, а також Японії, Південної Кореї, Австралії тощо, реалізують програми міжінституційного та міжсекторного твінінгу, які дають змогу фахівцям та експертам з різних сфер формувати кооперативні простори для виконання спільних завдань.

Сучасне ІТ збагачує процес ухвалення рішень у демократичних інституціях на основі більш чіткої ситуативної обізнаності акторів ухвалення рішень. Також забезпечується можливість моделювання та стимулювання типових управлінських ситуацій. Для

сучасної України, яка перебуває в стані війни, демократизація ухвалення рішень і практик аналізу ситуації в безпековому секторі є основою більш оперативного та якісного відпрацювання безпекових завдань на широкій міждисциплінарній основі. Також в умовах повоєнного відновлення буде актуальною швидка інтеграція українських політико-урядувальних структур до європейського середовища політико-безпекового управління.

Аналіз публікацій. Дослідження І. Тейлора щодо безпеки як політичної концепції пропонує розглядати безпеку не просто як захист, а як складний політичний конструкт [11]. Наковці І. Лоудер та Н. Вокер розглянули цивілізаційний вимір безпеки, балансування безпеки з правами людини та гідністю [6]. Класична праця Дж. С. Мілля розглядає завдання системи безпеки в контексті захисту особистої автономії в межах заходів соціальної безпеки [7]. Не менш знаний ліберальний мислитель Р. Нозік підкреслює важливість добровільних структур безпеки над примусовими [8]. Відповідно до теорії свободи та управління П. Петтіта, є інтегрований погляд на безпеку, який поважає демократичну участь та права окремих осіб, сприяючи почуттю колективної відповідальності без шкоди для особистої свободи [9]. С. Ф'єдер наполягає на стійкості в глобалізованих контекстах, яка відображається в адаптивні стратегії безпеки, що підтримують демократичні цінності у взаємопов'язаному світі [3]. Попри класичні доробки та новітні досягнення, доречно звернутися до питання формування гнучких структур політичної безпеки на міжнародному й національному рівнях.

Мета статті – виявити інституційні засади демократичної системи міжнаціональної безпеки. Завдання – розкрити чинники формування інноваційних структур політичного управління безпековими викликами.

Основний зміст статті. Створення демократичної мережі аналізу й прогнозування стану безпеки між державами-членами ЄС та НАТО надає можливість зміцнити колективну безпеку, сприяти взаємній довірі та скоординовано реагувати на нові загрози. Така інституційна мережа повинна ґрунтуватися на спільних демократичних цінностях, повазі до суверенітету та прагматичному підході до співпраці у сфері безпеки, який адаптується до геополітичної колаборації ціннісно споріднених держав. Про це свідчить текст «Спільної заяви Японії, США та Південної Кореї», які наголосили на важливості зміцнення енергетичної безпеки, що базується на американському зрідженому природному газі та інших джерелах енергії і технологіях. Суб'єкти співпраці заради подальшої диверсифікації ланцюгів постачання критично важливих мінералів та інших життєво важливих ресурсів зобов'язалися посилити тристоронній діалог щодо критично важливих мінералів та співпрацювати в різних регіонах, як-от Південно-Східна Азія та Африка на південь від Сахари, шляхом подальшого сприяння активній співпраці в межах тристоронньої Системи раннього попередження. Крім того, вони погодилися продовжувати діалог з питань економічної безпеки. Для задоволення дедалі більших енергетичних потреб відповідно до найвищих стандартів ядерної безпеки, захисту та нерозповсюдження Державний секретар США та Міністри закордонних справ Японії і Південної Кореї зобов'язалися прискорити спільні зусилля щодо розробки та розгортання передових цивільних ядерних реакторів [4].

Фундамент гнучкої інформаційно-аналітичної мережі демократичної безпеки має розпочатися з формалізації комплексної системи, яка заохочує регулярне спілкування, обмін розвідувальними даними, спільне навчання та скоординоване стратегічне планування. Ця система функціонуватиме як парасолька, під якою можна буде інтегрувати двосторонні та багатосторонні домовленості про безпеку, зменшуючи спірні позиції та сприяючи взаємодії між державами-членами. Згідно з тристоронньою «Спільною заявою», держави-партнери привітали розвиток відчутної співпраці в розробці та захисті критично

важливих та нових технологій, включно зі тристоронніми семінарами з квантової промислової безпеки у вересні та другою тристоронньою програмою навчання лідерів технологій у червні. Вони також висловили свою підтримку дослідницькій співпраці між національними лабораторіями трьох країн [4].

Основний принцип інституалізації новітніх систем політичної безпеки полягає у створенні гнучкого, але при цьому структурованого середовища, де держави-члени можуть швидко реагувати на кризи. Ключовим компонентом цієї мережі є створення безпечної, сумісної комунікаційної інфраструктури, яка забезпечує обмін інформацією в режимі реального часу. Це може передбачати модернізацію каналів зв'язку та розробку стандартизованих протоколів, сумісних між агентствами безпеки НАТО та ЄС. Також доречно звернути увагу на формування лідерського потенціалу. Згідно з текстом «Спільної заяви», повноважні представники Японії, Південної Кореї та США привітали програму «Молоді тристоронні лідери» як внесок у зміцнення міжособистісних зв'язків та посилення тристоронньої співпраці. Рішуче виступаючи проти економічного примусу та неринкової політики та практики, включно з обмеженням експорту, які можуть призвести до значних перебоїв у ланцюжку поставок, вони підтвердили свою відданість вільному та справедливому світовому економічному порядку. Вони також висловили свою підтримку успішному проведенню АТЕС 2025 року в Республіці Корея та досягнення змістовних результатів на Тижні економічних лідерів АТЕС пізніше цієї осені [4].

Інституалізація мережної безпекової інфраструктури сприятиме швидкому поширенню інформації про загрози, пов'язані з тероризмом, кібератаками, гібридною війною та іншими новими викликами безпеці. Крім того, спільна база цих індикаторів загроз та передового досвіду може слугувати орієнтиром для всіх учасників, що дає змогу вживати превентивних заходів та координувати реагування. Мережа демократичної безпеки також повинна акцентувати на спільних навчальних акціях та ініціативах з нарощування потенціалу. На основі досвіду кризового управління в сучасних США доцільно масштабувати практики взаємодії та кооперації, згідно з якими в основу спільних протоколів дій буде покладено Національну систему управління інцидентами (NIMS), яка забезпечує стандартизовану основу для управління інцидентами на всіх урядових рівнях. Ця система гарантує, що федеральні, державні та місцеві установи можуть ефективно працювати разом, використовуючи спільну мову та набір процедур. Завдяки NIMS установи можуть інтегрувати свої ресурси та зусилля, мінімізуючи надмірність і максимізуючи ефективність [1].

Регулярне моделювання кризових сценаріїв дає змогу виявити прогалини в міжінституційній взаємодії, покращити координацію та зміцнити довіру між силами країн-учасників. Спільні протоколи можуть охоплювати низку загроз – від звичайних воєнних конфліктів до кібервійни та гібридних операцій. Це особливо актуально контексті досвіду сучасної України.

У цьому контексті також слід зазначити, що комунікація в кризових ситуаціях є ще одним важливим компонентом федеральних протоколів надзвичайних ситуацій. Система командування інцидентами (ICS) є ключовим інструментом, який використовується для управління комунікацією під час кризи. Вона встановлює чіткий ланцюг командування та розмежовує ролі й обов'язки, забезпечуючи безперебійний потік інформації між усіма залученими сторонами. Ця система має вирішальне значення для підтримки ситуаційної обізнаності та забезпечення швидкого ухвалення рішень [1].

Крім того, між демократичними державами в найближчому майбутньому можуть бути укладені угоди про інформаційно-комунікаційну взаємодопомогу, за якими держави-члени зобов'язуються підтримувати одна одну під час кризи через розгортання вій-

ськових ресурсів, розвідувальної підтримки чи гуманітарної допомоги. Кібербезпека є критичним виміром сучасної політичної безпеки, і демократична мережа безпеки повинна надавати пріоритет спільним ініціативам кіберзахисту. Успіх спільних антикризових безпекових протоколів значно залежить від використання технологій. Передові системи зв'язку, як-от супутникові пристрої та безпечне інтернет-з'єднання, використовують для підтримки ліній зв'язку навіть у найскладніших умовах. Як свідчить досвід України, ці технології дають змогу обмінюватися інформацією в режимі реального часу, що важливо для координації зусиль та ефективного розподілу ресурсів [1].

Уніфікація політико-безпекових підходів демократичних країн передбачає створення спеціальної платформи для обміну розвідувальною інформацією про кіберзагрози, координацію протоколів реагування на інциденти та проведення спільних навчань з кіберзахисту. Ураховуючи транснаціональний характер кіберзагроз, співпраця в цій сфері може значно зменшити вразливості та підвищити стійкість у всій мережі.

Ще один важливий аспект інституалізації міжнаціональної безпекової колаборації передбачає розробку спільних стратегічних доктрин та оперативних рекомендацій, які поважають суверенітет кожного члена, одночасно сприяючи єдиному підходу до викликів безпеці. Ці доктрини повинні бути адаптованими до різних сценаріїв загроз та здатними до інтеграції з чинною політикою НАТО та ЄС.

Створення спільних структур командування та управління для конкретних місій або інформаційного реагування на кризи може ще більше підвищити оперативну ефективність і зменшити час на бюрократичні узгодження. Безпекова моніторингова та аналітична мережа також повинна сприяти залученню країн-партнерів і регіональних організацій для сприяння ширшій стабільності. Хоча основна відповідальність залишається на членах ЄС та НАТО, залучення сусідніх держав та організацій, як-от ОБСЄ, може розширити охоплення та вплив колективних зусиль безпеки. Проте, згідно з досвідом США, доречно докласти зусиль для адаптації нової мережі до мінливих умов. Федеральні агентства, яким доручено управління кризами, стикаються з кількома суттєвими викликами. Зокрема, спостерігаються швидкі темпи розвитку загроз. Характер насильницьких подій постійно змінюється, з'являються нові загрози, які вимагають оновлених стратегій та технологій. Крім того, ефективне управління кризами вимагає безперебійної координації між кількома агентствами, якій можуть перешкоджати бюрократичні перешкоди та прогалини в комунікації [1].

Для забезпечення сталості та розвитку мережі безпеки доречно створити наглядову мережу, що налічує представників інституцій ЄС, НАТО та дружніх країн. Наявні доктринальні положення НАТО публічно наголошують на забезпеченні наявності потрібних ресурсів у потрібний час і в потрібному місці. Це є постійною проблемою, особливо в разі масштабних інцидентів. При цьому йдеться про надання своєчасної та точної інформації громадськості під час кризи, що є критично важливим, але водночас складним завданням, особливо з огляду на швидке поширення дезінформації [1].

Об'єднана політико-безпекова мережа контролюватиме впровадження, оцінюватиме ефективність та адаптуватиме стратегії залежно від появи нових загроз. Регулярні огляди та оновлення даних забезпечать чутливість мережі до технологічних досягнень, геополітичних зрушень і розвитку інноваційних парадигм безпеки. Фінансування та розподіл ресурсів – це практичні міркування, які вимагають прозорих і справедливих домовленостей представників сталих демократій. Запобігання кризам та їх урегулювання є одним із трьох основних завдань НАТО, для чого вона використовує відповідне поєднання політичних та військових інструментів для врегулювання криз у дедалі складнішому середовищі безпеки [2].

Держави-члени повинні робити внески відповідно до своїх можливостей, об'єднуючи ресурси, спрямовані на спільні проєкти, розвиток інфраструктури та дослідницькі ініціативи. Зовнішнє фінансування з бюджету ЄС або програм інвестицій у безпеку НАТО може доповнювати внески, особливо для масштабної технологічної модернізації та досліджень. Глобальна безпекова мережа демократичних країн тісно пов'язана з двома іншими основними завданнями НАТО: стримуванням й обороною, завдяки яким союзники захищають один одного, підтримуючи потужні оборонні можливості та сили; і спільною безпекою, завдяки якій НАТО сприяє глобальній стабільності, взаємодіючи з партнерами (країнами, що не є членами, та іншими міжнародними організаціями) для вирішення спільних викликів [2].

Нормативно-правові рамки, покладені в основу перспективної інформаційно-аналітичної мережі безпеки, мають забезпечувати дотримання демократичних принципів, прав людини та міжнародного права. Угоди, що регулюють обмін інформацією та спільні операції, повинні містити гарантії захисту громадянських свобод і запобігання неправомірному використанню розвідувальних даних або військових ресурсів. Механізми прозорості й підзвітності важливі для підтримки суспільної довіри та легітимності. Сучасне НАТО є однією з небагатьох міжнародних організацій, які мають досвід, а також інструменти для проведення операцій із запобігання та врегулювання криз [2].

Слід брати до уваги, що створення демократичної мережі інформування й аналізу щодо питань безпеки між країнами ЄС та НАТО передбачає створення структурованої, але адаптивної системи, яка посилює співпрацю в різних сферах політичної безпеки. Це вимагає вкладання інвестицій у комунікаційну інфраструктуру, спільне навчання, кібербезпеку. НАТО забезпечує систему, у межах якої члени можуть працювати та навчатися разом, щоб планувати та проводити багатонаціональні операції з урегулювання криз, часто в стислі терміни [2].

Створення демократичної інформаційно-аналітичної та моніторингової мережі безпеки між державами-членами ЄС та НАТО, а також азійськими союзниками дає змогу зміцнити глобальну колективну безпеку, сприяти взаємній довірі та скоординовано реагувати на нові загрози. Така мережа повинна ґрунтуватися на спільних демократичних цінностях, повазі до суверенітету та прагматичному підході до співпраці у сфері комплексної аналітики безпеки, який адаптується до змін у сучасній глобальній політиці.

Ключовим компонентом перспективної аналітико-прогностичної мережі є створення безпечної, сумісної комунікаційної інфраструктури, яка буде забезпечувати обмін інформацією в режимі реального часу. Це може містити модернізацію каналів зв'язку та розробку стандартизованих протоколів, сумісних між агентствами безпеки НАТО та ЄС, Південної Кореї, Японії, Австралії тощо. Така інфраструктура сприятиме швидкому поширенню розвідувальних даних та їх аналітичних оцінок про загрози, пов'язані з тероризмом, кібератаками, гібридною війною та іншими новими викликами безпеці. Крім того, спільна база цих індикаторів загроз і передового досвіду може слугувати орієнтиром для всіх членів, даючи змогу вживати превентивних та скоординованих заходів реагування.

Висновки. Так, спільні декларації та регулятивні документи ЄС і НАТО та країн-партнерів відкривають широку можливість для взаємодії інститутів політичного врядування й захисту національної безпеки. Наявність алгоритмів та протоколів антикризового менеджменту передбачає задіяння механізмів ситуаційної співпраці, оперативних нарад і конкретних рішень в умовах викликів ризиків та загроз. Відомчі інформаційно-аналітичні центри мають можливості обміну інформацією, успішними кейсами й практиками підвищення ситуаційної обізнаності.

Практики сучасного демократичного врядування в країнах ЄС та НАТО передбачають прозорість безпекової політики в контексті діяльності парламентів і громадянського суспільства. Процедури парламентських служб та слухань є дієвим механізмом не лише контролю, а й адекватності розуміння безпековим інститутами політичного порядку денного. Це формує дієвий механізм «звіряння годинників» між безпековим сектором і представницькими ланками. Для сучасної України надзвичайно важливими є практики горизонтальної співпраці керівництва правоохоронних і безпекових структур з місцевими громадами та регіональними представницькими асамблеями. Означена співпраця є основою для сталих практик підтримки належного рівня політичної безпеки в мінливих умовах. Подальший розвиток теми, порушений у статті, здійснюватиметься в межах уточнення інституційних компетенцій політичного врядування та сектору демократичної національної безпеки.

Список використаної літератури

1. Crisis Management for Violent Events: Understanding Federal Protocols. URL: https://federal-criminal.com/violent-crimes/crisis-management-for-violent-events-us-federal-emergency-protocols/
2. Crisis management NATO. URL:https://www.nato.int/cps/en/natohq/topics_49192.htm
3. Fjäder C. The nation-state, national security and resilience in the age of globalisation. *Resilience.* 2014. № 2(2). P. 114–129. https://doi.org/10.1080/21693293.2014.914771
4. Joint Statement from the Trilateral Meeting of the United States of America, Japan, and the Republic of Korea in New York City. URL: https://www.state.gov/releases/office-of-the-spokesperson/2025/09/joint-statement-from-the-trilateral-meeting-of-the-united-states-of-america-japan-and-the-republic-of-korea-in-new-york-city/
5. Lenard P. T. How Should Democracies Fight Terrorism? Cambridge: Polity Press, 2020. 132 p.
6. Loader I. and N. Walker. Civilizing Security. Cambridge: Cambridge University Press, 2007. 244 p.
7. Mill J. S. On Liberty. In On Liberty and Other Essays, edited by J. Grey, 5–130. Oxford: Oxford University Press, 1991. 346 p.
8. Nozick R. Coercion. In Philosophy, Science, and Method: Essays in Honor of Ernest Nagel, edited by S. Morgenbesser, P. Suppes, and M. White, 440–472. New York: St. Martin's Press, 1969. 256 p.
9. Pettit P. On the People's Terms: A Theory of Freedom and Government. Cambridge: Cambridge University Press, 2012. 154 p.
10. Ramsay P. The Insecurity State: Vulnerable Autonomy and the Right to Security in the Criminal Law. Oxford: Oxford University Press, 2012. 246 p.
11. Taylor I. Security as a political concept. Inquiry, 2024. P. 1–27.

DEMOCRATIC ECOSYSTEM OF NATIONAL SECURITY: POLITICAL FACTORS OF FORMATION

Viacheslav Sergeev
State University "Zhytomyr Polytechnic",
Department of Political Science and Public Administration
Chudnivska Str., 103, 10005, Zhytomyr, Ukraine

The article analyzes the democratization of decision-making and practices of situation analysis in the security sector is the basis for more efficient and high-quality implementation of security tasks on a broad interdisciplinary basis For modern Ukraine, which is in a state of war. The study reveals classical achievements and new achievements, it is appropriate to address the issue of forming flexible structures of political security at the international and national levels. Particular attention is paid to the institutionalization of a democratic security network, which should be based on shared democratic values, respect for sovereignty, and a pragmatic approach to cooperation that adapts to geopolitical collaboration between value-related states. In this context, the ability to integrate existing bilateral and multilateral security arrangements is revealed, reducing contentious positions and facilitating interaction between member states. The key characteristics of a security network are highlighted, which are the creation of a secure, interoperable communication infrastructure that ensures real-time information exchange. The institutionalization of a network security infrastructure that will facilitate the rapid dissemination of information about threats related to terrorism, cyberattacks, hybrid warfare, and other security challenges is investigated and analyzed. In particular, the prospects for the implementation of algorithms and protocols of anti-crisis management, which involves the use of situational cooperation mechanisms, operational meetings and specific solutions in the face of challenges of risks and threats, are assessed. The importance of horizontal security cooperation practices of the leadership of law enforcement and security structures with local communities and regional representative assemblies of Ukraine is substantiated.

Key words: democratic governance, political security, national security, political threats, political institutions, civil society, political experts.

Дата першого надходження рукопису до видання: 22.09.2025
Дата прийнятого до друку рукопису після рецензування: 23.10.2025
Дата публікації: 23.12.2025