https://doi.org/10.26565/1684-8489-2025-2-14
УДК 351:355.02(477)

Пупяліс Єгор Вікторович,
аспірант кафедри права, національної безпеки та європейської інтеграції
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна

e-mail: pravo.nb.ei@karazin.ua *https://orcid.org/0009-0006-8972-1091*

КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНСТИТУЦІАЛІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Анотація. Представлено концептуальну модель інституціалізації публічного управління національною безпекою, адаптовану до специфічних викликів гібридної війни. Обґрунтовано необхідність фундаментального переосмислення традиційних підходів до організації безпекових інституцій через неефективність секторальної спеціалізації та жорсткого розмежування компетенцій у протидії комплексним багатовимірним загрозам. Розроблено багаторівневу модель, що інтегрує стратегічний, оперативний та регіональний рівні управління через систему базових принципів, архітектурних елементів та механізмів адаптації. Запропоновано тринадцять базових принципів побудови інтегрованої системи управління, включаючи системну цілісність, адаптивну архітектуру, мережецентричність, інформаційну інтеграцію, проактивність, розподілену стійкість, інклюзивність, континуальність, технологічну інноваційність, стратегічну комунікацію, правову легітимність, безперервне навчання та економічну ефективність. Детально розкрито архітектуру системи на трьох рівнях з інноваційним принципом функціональних кластерів на оперативному рівні та створенням Національного центру стійкості як міжвідомчої координаційної структури. Обґрунтовано механізми адаптації системи до еволюції гібридних загроз через раннє виявлення слабких сигналів, сценарне прогнозування, організаційну та технологічну гнучкість, когнітивну адаптивність. Доведено, що запропонована модель забезпечує синергетичний ефект через інтеграцію різнорідних компонентів при збереженні їх функціональної спеціалізації та операційної автономії, що є критичним для ефективної протидії мультидоменним загрозам сучасної гібридної агресії.

Ключові слова: інституціалізація, публічне управління, національна безпека, гібридна війна, інтегрована система управління, адаптивна архітектура, міжвідомча координація, стратегічне планування.

Постановка проблеми. Сучасна гібридна війна, яку Україна веде проти російської агресії з 2014 року, продемонструвала критичні вразливості традиційних моделей організації системи національної безпеки. Природа гібридних загроз, що одночасно охоплюють військову, політичну, економічну, інформаційну, кібернетичну та соціальну сфери, вимагає якісно нових підходів до інституціалізації публічного управління безпековим сектором. Досвід десятиліття протистояння довів неспроможність фрагментованих систем

Як цитувати: Пупяліс Є. В. Концептуальна модель інституціалізації публічного управління національною безпекою в умовах гібридної війни. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 285–302. https://doi.org/10.26565/1684-8489-2025-2-14

In cites: Pupialis, Y.V. (2025). Conceptualization and mechanisms of digital citizen engagement in local development: from electronic participation to contractual-participatory relations. *Pressing Problems of Public Administration, 2 (67), 285–302.* https://doi.org/10.26565/1684-8489-2025-2-14 [in Ukrainian].

з жорстким розмежуванням відомчих компетенцій ефективно протидіяти комплексним загрозам, які експлуатують міжвідомчі розриви та організаційні розломи. Противник систематично використовує одночасні скоординовані дії в різних доменах для досягнення синергетичного ефекту, натомість традиційна секторальна організація безпекових структур унеможливлює адекватну інтегровану відповідь на такі багатовимірні виклики [23].

Проблема посилюється тим, що гібридна агресія характеризується не лише багатовекторністю, а й принциповою непередбачуваністю форм та методів, постійною еволюцією тактик, швидкою адаптацією до контрзаходів. Статичні організаційні структури з фіксованими процедурами виявляються структурно нездатними до швидкого реагування на нові типи загроз, що постійно виникають.

Відсутність ефективних механізмів горизонтальної координації між відомствами призводить до дублювання зусиль, марнування обмежених ресурсів, втрати критичного часу на узгодження дій. Інформаційна роз'єднаність, коли кожне відомство володіє фрагментом загальної картини ситуації без можливості її інтеграції, унеможливлює формування цілісного розуміння характеру загроз та вироблення адекватної стратегії протидії.

Водночас міжнародний досвід країн, що стикалися з гібридними загрозами, демонструє можливість створення ефективніших моделей організації безпекового управління через глибоку інституційну інтеграцію при збереженні функціональної спеціалізації. Естонія після масованих кібератак 2007 року радикально трансформувала свою систему кібербезпеки, створивши інтегровану модель взаємодії державних, приватних та міжнародних акторів. Фінляндія розробила концепцію всеохопної безпеки, що об'єднує зусилля всіх секторів суспільства в єдину систему протидії гібридним загрозам. Литва після подій 2014 року запровадила нову архітектуру національної безпеки з посиленими механізмами міжвідомчої координації та створенням спеціалізованих структур протидії гібридній агресії [9]. Проте механічне копіювання зарубіжних моделей без адаптації до специфічного українського контексту є неприйнятним, оскільки кожна країна має унікальну комбінацію історичних, культурних, інституційних та ресурсних особливостей.

Отже, постає нагальна потреба у розробці концептуальної моделі інституціалізації публічного управління національною безпекою, яка би органічно поєднувала кращі міжнародні практики з українською специфікою, забезпечувала ефективну інтеграцію різнорідних компонентів безпекової системи при збереженні необхідної функціональної автономії, створювала механізми швидкої адаптації до еволюції загроз. Така модель має базуватися на чітких концептуальних принципах, передбачати конкретні архітектурні рішення для всіх рівнів управління, включати дієві механізми координації та адаптації.

Огляд літератури. Проблематика інституціалізації публічного управління національною безпекою в умовах гібридних загроз активно досліджується українськими та зарубіжними науковцями, проте більшість праць зосереджена на окремих аспектах без створення цілісної концептуальної моделі. Фундаментальні засади теорії гібридної війни закладені в роботах Ф. Гофмана, який визначив гібридні загрози як конвергенцію різних способів ведення війни [23], та Дж.Маккуена, що розробив типологію гібридних конфліктів [26]. Українські дослідники зробили вагомий внесок у розуміння специфіки гібридної агресії проти України. Г. Ситник розробив концептуальні засади

забезпечення національної безпеки в умовах гібридної війни, обґрунтувавши необхідність системної трансформації безпекового сектору [11]. О. Власюк аналізував національну безпеку України в контексті гібридних загроз, акцентуючи увагу на необхідності інституційних змін [2]. Є. Магда досліджував специфіку гібридної війни проти України, акцентуючи увагу на необхідності формування суспільної стійкості [7].

Зарубіжні дослідники також приділяють значну увагу адаптивності систем національної безпеки до нових викликів. Б. Джексон та Д. Фрелінгер розробили концепцію адаптивного управління в контексті безпеки, обґрунтовуючи необхідність організаційної гнучкості [24]. П. Сенге запропонував теорію навчальних організацій, яка знайшла застосування в безпековому секторі [28]. Питання технологічної трансформації систем національної безпеки розглядалися в працях М. Лібіцкі, який аналізував роль кібернетичного простору в гібридних конфліктах [25]. Р. Кларк та Р. Кнейк вивчали кібервійни та їх імплікації для національної безпеки [18].

Проте, незважаючи на значний доробок, в існуючих дослідженнях бракує комплексних концептуальних моделей, які би системно інтегрували всі аспекти інституціалізації публічного управління національною безпекою в умовах гібридної війни. Більшість праць зосереджена або на теоретичному осмисленні гібридних загроз, або на окремих інституційних механізмах без створення цілісної архітектури системи. Недостатньо розробленими залишаються питання практичної реалізації принципів інтеграції на різних рівнях управління, конкретні механізми координації різнорідних компонентів системи, інструменти адаптації до постійної еволюції загроз.

Мета статті полягає в розробці та обґрунтуванні концептуальної моделі інституціалізації публічного управління національною безпекою, адаптованої до специфічних викликів гібридної війни, що інтегрує базові принципи, багаторівневу архітектуру та механізми адаптації в цілісну систему управління.

Методологія дослідження. Дослідження ґрунтується на комплексному застосуванні загальнонаукових та спеціальних методів наукового пізнання. Системний підхід використано для визначення інституціоналізації як цілісного процесу формування механізмів публічного управління національною безпекою в умовах гібридної війни. Структурно-функціональний аналіз застосовано для виявлення взаємозв'язків між елементами системи публічного управління національною безпекою та визначення їх ролі в протидії гібридним загрозам. Компаративний метод використано для порівняння вітчизняного та зарубіжного досвіду інституціоналізації систем національної безпеки в умовах гібридних конфліктів. Методи синтезу та узагальнення дозволили сформулювати концептуальні засади інституціоналізації публічного управління національною безпекою України. Інституціональний аналіз застосовано для дослідження процесів формування, функціонування та трансформації інститутів публічного управління у сфері національної безпеки. Метод експертного оцінювання використано для визначення пріоритетних напрямів удосконалення системи публічного управління національною безпекою в умовах гібридної війни. Методологічною основою дослідження є теорія інституціоналізації, концепції гібридної війни, теорія публічного управління та системний підхід до дослідження національної безпеки.

Основні результати дослідження. Фундаментом запропонованої концептуальної моделі є розуміння того, що протидія гібридним загрозам

вимагає не просто координації існуючих структур, а глибокої інституційної інтеграції на основі чітко визначених принципів організації. Системна цілісність постає наріжним каменем моделі, оскільки ефективність інтегрованої системи визначається не арифметичною сумою потенціалів окремих відомств, а якістю зв'язків між ними, швидкістю обміну критичною інформацією, синхронізацією дій у часі та просторі.

Емерджентні властивості, що виникають із взаємодії елементів системи, створюють додаткову цінність, яку неможливо досягти через просте додавання зусиль окремих структур [1]. Практична реалізація цього принципу вимагає створення інституційних механізмів справді глибокої інтеграції на основі єдиного стратегічного бачення, а не поверхневої координації паралельних дій різних відомств.

Адаптивна архітектура як базовий принцип відображає необхідність поєднання структурної стабільності з операційною гнучкістю, що є критично важливим в умовах динамічного характеру гібридних загроз. Система має бути достатньо стійкою для забезпечення передбачуваності функціонування, але водночас здатною до швидкої реконфігурації відповідно до змін характеру викликів. Модульна побудова системи дозволяє базовим функціональним модулям об'єднуватися в різні конфігурації залежно від конкретних завдань без руйнування організаційної цілісності. Створення постійного інституційного ядра, доповненого гнучкими тимчасовими структурами, забезпечує оптимальний баланс між стабільністю та адаптивністю.

Мережецентричність передбачає перехід від традиційної ієрархічної піраміди до розподіленої мережі взаємопов'язаних вузлів, що відповідає децентралізованому характеру сучасних гібридних загроз. Ієрархічні структури виявляються занадто повільними через необхідність проходження інформації через численні бюрократичні інстанції, що неприйнятно в умовах швидкоплинних кризових ситуацій. Мережева організація забезпечує прямі зв'язки між елементами системи без непотрібних посередників, водночас зберігаючи вертикальні зв'язки для стратегічного управління та доповнюючи їх горизонтальними для оперативної координації. Така гібридна топологія поєднує переваги централізованого керівництва з гнучкістю децентралізованого виконання [15].

Інформаційна інтеграція є критичним принципом в умовах інформаційної насиченості гібридної війни, де своєчасний доступ до достовірної інформації визначає ефективність рішень. Традиційна модель закритих відомчих інформаційних систем створює небезпечні інформаційні силоси, унеможливлюючи формування цілісної картини безпекової ситуації. Створення єдиного інформаційного простору з диференційованим рольовим доступом дозволяє всім учасникам системи оперативно отримувати необхідну інформацію в реальному часі. Реалізація цього принципу вимагає не лише технічної сумісності систем різних відомств, а й подолання глибоко вкоріненої культури відомчої монополії на інформацію через організаційні та психологічні зміни [29].

Проактивність як принцип управління означає перехід від реактивного реагування на вже реалізовані загрози до їх завчасного виявлення та превенції. В умовах гібридної війни противник часто діє приховано, використовуючи тривалі підготовчі фази для створення сприятливих умов, тому реактивна модель неминуче призводить до постійного відставання від подій. Розвиток потужних прогностичних спроможностей, систем раннього попередження, механізмів виявлення слабких сигналів про зароджувані загрози стає кри-

тично важливим для ефективного управління. Це також вимагає готовності приймати рішення на основі неповної інформації та ймовірнісних оцінок, для чого необхідна висока толерантність керівництва до фундаментальної невизначеності.

Розподілена стійкість передбачає, що здатність системи витримувати удари та швидко відновлюватися не концентрується в одному центральному вузлі, а розподіляється по всій системі через множину автономних елементів. Така архітектура набуває особливого значення в умовах гібридних атак, спрямованих на критичні централізовані вузли для паралічу всієї системи.

Свідоме дублювання критичних функцій у різних елементах, створення резервних каналів управління, розвиток значних автономних спроможностей регіональних компонентів забезпечують здатність системи ефективно функціонувати навіть за тимчасової втрати зв'язку з центром. Кожен елемент має власний запас міцності, альтернативні канали функціонування, внутрішні механізми самовідновлення після ушкоджень.

Інклюзивність як принцип передбачає залучення до системи управління національною безпекою широкого кола акторів за межами традиційних силових структур, включаючи інші державні органи, приватний сектор, організації громадянського суспільства. Оскільки гібридні загрози атакують все суспільство одночасно в різних сферах від економіки до культури, відповідь також має бути загальносуспільною з мобілізацією всіх доступних ресурсів. Створення ефективних механізмів партнерства дозволяє використовувати унікальні ресурси та компетенції недержавних акторів при збереженні державного контролю над критичними функціями. Особливо важливим є залучення технологічного сектору з його інноваційним потенціалом, медіа як каналів стратегічних комунікацій, освітніх інституцій для формування суспільної стійкості.

Континуальність управління відображає розуміння того, що в умовах тривалої гібридної війни не існує чіткої межі між станом миру та війни, між нормальним та кризовим станом функціонування держави. Система має ефективно функціонувати в усьому спектрі станів від відносного спокою до гострої кризи без необхідності фундаментальної перебудови при кожному переході. Створення масштабованих механізмів управління, що можуть плавно нарощувати інтенсивність діяльності та обсяг залучених ресурсів без структурної трансформації, забезпечує необхідну гнучкість. Наявність резервних елементів системи, які можуть бути швидко активовані за потреби, дозволяє підтримувати постійну готовність без надмірного виснаження обмежених ресурсів у спокійні періоди [8].

Технологічна інноваційність визнає критичну роль передових технологій у забезпеченні конкурентних переваг над противником у довгостроковій перспективі. Штучний інтелект для аналізу величезних масивів даних, аналітика великих даних для виявлення прихованих патернів, квантові технології для захищених комунікацій, блокчейн для забезпечення цілісності критичної інформації створюють принципово нові можливості для інтеграції управління та ефективної координації розподілених дій. При цьому технології розглядаються не як самоціль, а як практичні інструменти реалізації інших фундаментальних принципів системи. Створення механізмів швидкого впровадження перевірених інновацій, безпечного експериментування з новими підходами, масштабування успішних пілотних рішень стає критичним фактором довгострокової ефективності в технологічній гонці з противником.

Стратегічна комунікація перетворюється з допоміжної функції на інтегральну частину процесу управління національною безпекою в умовах гібридної війни, де боротьба за уми населення є не менш важливою за військові дії. Цілеспрямоване формування сприятливого інформаційного середовища, переконливих наративів, широкої суспільної підтримки безпекової політики вимагає тісної синхронізації публічних меседжів різних відомств для уникнення суперечностей. Проактивне формування інформаційного порядку денного замість пасивного реагування, максимально швидке спростування ворожої дезінформації до її масового поширення стають критично важливими елементами ефективного управління [12].

Правова легітимність як принцип підкреслює, що навіть в екстремальних умовах екзистенційних загроз система управління національною безпекою має неухильно діяти в межах правового поля та конституційних норм. Це створює складний баланс між операційною ефективністю, яка часом вимагає швидких нестандартних рішень, та безумовною законністю всіх дій. Розробка спеціальних правових механізмів, адекватних специфіці гібридних загроз, включаючи гнучкі режими підвищеної готовності з розширеними повноваженнями, спрощені процедури прийняття рішень для кризових ситуацій, механізми постфактум легалізації екстрених рішень через парламентський контроль, дозволяє зберегти фундаментальний правовий характер демократичної держави без критичної втрати оперативної ефективності [13].

Безперервне навчання визнає об'єктивний факт, що в динамічному середовищі гібридної війни з постійною еволюцією тактик та технологій жодна система не може бути ідеально досконалою назавжди. Механізми систематичного вивчення практичних уроків з реальних операцій, глибокого аналізу помилок та невдач, активного поширення виявлених кращих практик між підрозділами, планомірної адаптації застарілих процедур на основі накопиченого досвіду мають бути органічно вбудовані в структуру системи. Це включає проведення регулярних оглядів ефективності всієї системи, організацію незалежних зовнішніх аудитів для об'єктивної оцінки, створення механізмів зворотного зв'язку від операційного до стратегічного рівня.

Формування організаційної культури, яка заохочує експериментування з новими підходами та конструктивно визнає помилки як джерело навчання замість їх приховування, стає критичною передумовою довгострокової ефективності через здатність системи до самовдосконалення [20].

Економічна ефективність визнає обмеженість доступних державних ресурсів навіть в умовах війни та необхідність їх максимально оптимального використання. Глибока інтеграція управління дозволяє уникнути марнотратного дублювання функцій у різних відомствах, досягти економії масштабу через консолідацію закупівель та сервісів, оптимізувати використання дефіцитних специфічних ресурсів через їх спільне використання. Механізми спільного стратегічного планування потреб, консолідованих централізованих закупівель для всього сектору безпеки, створення спільних сервісів для забезпечуючих функцій можуть радикально підвищити ефективність безпекових видатків бюджету. При цьому критично важливо розуміти, що економія державних коштів ніколи не повинна досягатися за рахунок деградації критичних оперативних спроможностей системи.

Архітектура запропонованої моделі будується на трьох рівнях управління, кожен з яких має специфічні функції та механізми координації (табл. 1).

Таблиця 1. Архітектура багаторівневої моделі інституціалізації публічного управління національною безпекою України

Table 1. Architecture of a multi-level model of institutionalization of public management of national security of Ukraine

Рівень управління Level of governance	**Структурні компоненти Structural components**	**Ключові функції Key functions**	**Механізми координації Coordination mechanisms**	**Специфіка для України 2025 Specific features for Ukraine 2025**
Стратегічний	– РНБО з розширеними повноваженнями – комітет з планування та координації – аналітичний центр при РНБО	– Стратегічне планування та прийняття рішень – консолідація розвідувальної інформації – формування єдиної картини загроз – координація безпекової політики	– Постійно діючі засідання комітету – централізована аналітика з усіх джерел – безпосереднє керівництво кластерами	–Перехід від консультативної до виконавчої ролі РНБО – врахування досвіду гібридної війни 2014-2025 – інтеграція з євроатлантичними структурами
Оперативний	Функціональні кластери: – військовий (МОУ) – внутрішньої безпеки (МВС) – розвідувальний – кібер-безпековий Спеціалізована структура: національний центр стійкості	Кластерні функції: Координація спорідніх відомств Операційне планування Усунення дублювання Функції НЦС: – захист критичної інфраструктури – цивільний захист – кризове управління	– Єдине оперативне командування в кластерах – міжкластерна взаємодія – координація держави-приватного сектору через НЦС	– Врахування бойового досвіду ЗСУ – адаптація до російських гібридних тактик – захист енергетичної інфраструктури – протидія кібератакам на критичні системи
Регіональний	– мережа регіональних центрів безпеки та стійкості – постійні представники безпекових відомств – зв'язок з обласними адміністраціями	Територіальна координація: – моніторинг регіональних загроз – управління територіальною обороною – взаємодія з місцевою владою	– Подвійне підпорядкування (вертикальне/ горизонтальне) – регіональні ситуаційні центри – координація з громадськістю	– Особлива роль прикордонних областей – врахування регіональної специфіки – координація з ТрО та волонтерами – протидія диверсійним групам

**Джерело: розробка автора.*

**Source: author's own work.*

Стратегічний рівень формується навколо Ради національної безпеки і оборони України як центрального координаційного органу з реальними важелями впливу замість нинішньої консультативно-дорадчої інстанції. Створення постійно діючого Стратегічного комітету з планування та координації безпекової політики забезпечує необхідну безперервність стратегічного управління між періодичними засіданнями повного складу Ради. До складу комітету входять керівники всіх ключових безпекових відомств, що дозволяє

оперативно координувати стратегічні рішення без зайвих бюрократичних процедур. Паралельно Інтегрований аналітичний центр при РНБО системно консолідує розвідувальну, аналітичну та прогностичну інформацію з усіх джерел незалежно від відомчої приналежності для формування єдиної картини безпекового середовища, необхідної для обґрунтованого прийняття стратегічних рішень вищим політичним керівництвом держави.

Оперативний рівень архітектури будується на інноваційному принципі функціональних кластерів, кожен з яких організаційно об'єднує відомства зі спорідненими функціями під єдиним оперативним керівництвом для максимальної координації та синергії. Військовий кластер під керівництвом Міністерства оборони інтегрує Збройні Сили України, Національну гвардію, Державну прикордонну службу в частині їх бойового застосування проти зовнішнього противника. Така інтеграція забезпечує єдність командування в операційній зоні, уникнення конфлікту повноважень, оптимальне використання бойових спроможностей різних формувань. Кластер внутрішньої безпеки під координацією Міністерства внутрішніх справ об'єднує правоохоронні функції різних структур, забезпечення громадського порядку, організацію цивільного захисту населення. Розвідувальний кластер системно об'єднує всі спеціалізовані розвідувальні служби держави під стратегічною координацією для уникнення дублювання зусиль та оптимального використання обмежених розвідувальних ресурсів. Кібербезпековий кластер консолідує розпорошені зусилля Держспецзв'язку, кіберпідрозділів різних силових відомств під єдиним оперативним командуванням, що є критично важливим в умовах інтенсивних кібератак [6].

При цьому інноваційним елементом архітектури є створення Національного центру стійкості як міжвідомчої координаційної структури, безпосередньо відповідальної за забезпечення безперебійного функціонування критичної інфраструктури держави, координацію заходів цивільного захисту населення, управління кризовими ситуаціями невоєнного характеру від природних катастроф до техногенних аварій. Центр організаційно інтегрує координовані зусилля профільних міністерств з вузькою спеціалізацією, регіональних державних адміністрацій з їх знанням місцевої специфіки, приватних операторів критичної інфраструктури з їх технічною експертизою. Його ключовим завданням є стратегічна координація зусиль різних акторів, систематичний моніторинг критичних вразливостей системи, розробка детальних планів забезпечення безперервності функціонування, проведення практичних навчань та реалістичних симуляцій кризових сценаріїв. Така структура заповнює існуючу прогалину в українській системі національної безпеки, де відповідальність за критичну інфраструктуру розпорошена між численними відомствами без належної координації.

Регіональний рівень архітектури передбачає створення мережі Регіональних центрів безпеки та стійкості як інтегрованих міжвідомчих структур на обласному рівні, що об'єднують постійних представників усіх ключових безпекових відомств для координації на місцях. Ці центри функціонують як регіональні координаційні хаби всієї системи, практично забезпечуючи оперативну координацію дій різних структур на місцях, систематичний моніторинг специфічних регіональних загроз, управління територіальною обороною області, ефективну взаємодію з обласною владою та місцевою громадськістю. Важливою особливістю їх організації є подвійне підпорядкування: вертикальне центральним органам влади для забезпечення

єдності політики та горизонтальне обласним адміністраціям для врахування регіональної специфіки. Така структура дозволяє оптимально балансувати між необхідним централізованим стратегічним управлінням та доцільною регіональною автономією в оперативних питаннях, що є критично важливим для країни з значними регіональними відмінностями.

Мережевий компонент архітектури представлений розгалуженою системою горизонтальних зв'язків між різними елементами системи на різних рівнях ієрархії та у різних функціональних кластерах для подолання відомчої роз'єднаності. Створення Єдиної захищеної телекомунікаційної мережі сектору безпеки і оборони з сучасним шифруванням забезпечує надійну технічну основу для безперешкодного обміну критичною інформацією між усіма учасниками.

Паралельно численні міжвідомчі робочі групи з конкретних актуальних питань, таких як протидія дезінформації, захист критичної інфраструктури, координована протидія гібридним загрозам, формують гнучкі механізми оперативної координації без зайвої бюрократії. Система постійних взаємних представників між ключовими безпековими структурами забезпечує швидку неформальну координацію повсякденних питань без бюрократичних затримок на офіційні запити, створюючи міжособистісні зв'язки між фахівцями різних відомств.

Інформаційна підсистема архітектури базується на концепції єдиного інформаційного простору всього безпекового сектору з диференційованим рольовим доступом залежно від функціональних потреб. Національна платформа безпекових даних технологічно інтегрує розпорошені інформаційні системи всіх безпекових відомств через уніфіковані інтерфейси, практично забезпечуючи технічну можливість комплексного міжвідомчого аналізу даних з різних джерел. Така інтеграція дозволяє виявляти приховані зв'язки між подіями в різних сферах, які неможливо побачити при фрагментованому аналізі відомчих даних. Система розподілених ситуаційних центрів, надійно пов'язаних в єдину координовану мережу, забезпечує якісну візуалізацію актуальної оперативної обстановки на всіх рівнях управління від національного до регіонального. Широке використання технологій штучного інтелекту для автоматизованої обробки величезних масивів даних, своєчасного виявлення статистичних аномалій, імовірнісного прогнозування можливого розвитку ситуації суттєво підвищує якість інформаційно-аналітичного забезпечення процесу прийняття управлінських рішень на всіх рівнях.

Механізм прийняття рішень в новій архітектурі базується на комбінованому принципі розподіленого консенсусу для стратегічних питань довгострокового характеру та делегованої автономії для поточних оперативних питань. Стратегічні рішення з довгостроковими наслідками обов'язково приймаються колегіально в рамках засідань РНБО або спеціалізованих профільних комітетів з попереднім ретельним аналізом можливих альтернатив та комплексною оцінкою пов'язаних ризиків.

Така процедура забезпечує широке врахування різних відомчих перспектив, мінімізує ризик односторонніх помилкових рішень, створює широку підтримку прийнятих рішень серед усіх відомств для їх успішної імплементації. Натомість поточні оперативні рішення тактичного характеру свідомо делегуються на найнижчий компетентний рівень управління з наступним обов'язковим інформуванням вищих інстанцій для контролю. Така делегація забезпечує швидкість реагування на динамічні ситуації без втрати часу на узгодження, використання специфічних знань місцевого

рівня, розвиток управлінських компетенцій на нижчих рівнях. При цьому чітка система червоних ліній однозначно визначає критерії, за яких рішення обов'язково потребують попереднього узгодження на вищому рівні, а які можуть прийматися автономно нижчими рівнями в межах їх компетенції.

Ресурсне забезпечення в рамках нової архітектури передбачає стратегічний перехід від традиційного відомчого принципу виділення коштів до програмно-цільового фінансування за пріоритетами. Консолідований бюджет всього сектору безпеки і оборони має розподілятися не за формальною відомчою належністю структур-отримувачів, а за цільовими міжвідомчими програмами розвитку конкретних спроможностей незалежно від того, які відомства їх реалізують. Така модель фінансування забезпечує концентрацію обмежених ресурсів на критичних пріоритетах, уникнення розпорошення коштів між численними дрібними проектами, можливість об'єктивної оцінки ефективності використання ресурсів через вимірювання досягнення конкретних цілей програм.

Створення спеціалізованої Агенції оборонних закупівель як єдиного професійного закупівельного центру для всього сектору дозволяє досягти суттєвої економії масштабу через консолідацію попиту, надійно уникнути дублювання аналогічних закупівель різними відомствами, забезпечити вищі стандарти прозорості та підзвітності використання коштів. Механізм гнучкого оперативного перерозподілу бюджетних ресурсів між програмами залежно від зміни стратегічних пріоритетів та актуальних загроз значно підвищує адаптивність всієї системи до непередбачуваних змін.

Кадрова підсистема архітектури передбачає створення єдиного кадрового резерву всього сектору безпеки і оборони з практичною можливістю як горизонтальної мобільності персоналу між різними відомствами на одному рівні, так і вертикальної мобільності між рівнями управління. Така мобільність руйнує відомчі бар'єри, створює цілісне безпекове співтовариство з єдиною професійною ідентичністю, забезпечує кращу взаємну обізнаність про специфіку роботи різних структур. Уніфікація базової загальної підготовки для співробітників всіх безпекових структур незалежно від відомчої приналежності з подальшою обов'язковою вузькою спеціалізацією за профілем діяльності цілеспрямовано створює єдину професійну корпоративну культуру безпекового співтовариства. Така підготовка включає спільні курси з теорії національної безпеки, основ гібридної війни, принципів міжвідомчої координації, стратегічних комунікацій, що формує спільну понятійну базу для ефективної взаємодії. Система обов'язкової періодичної ротації керівних кадрів між різними відомствами розвиває цінне міжвідомче розуміння специфіки роботи партнерів та формує неформальні міжособистісні зв'язки між керівниками, які згодом значно полегшують координацію на практичному рівні. Створення міжвідомчого навчального центру вищого рівня забезпечує систематичну підготовку нової генерації безпекових менеджерів з необхідним системним стратегічним мисленням замість вузького відомчого підходу.

Механізми контролю та підзвітності органічно вбудовані в архітектуру на всіх рівнях для запобігання зловживанням та забезпечення ефективності. Парламентський демократичний контроль здійснюється через спеціалізований профільний комітет Верховної Ради з істотно розширеними порівняно з нинішніми повноваженнями доступу до секретної інформації для обізнаного контролю. Така модель запозичує кращі практики демократичних країн, де парламентський контроль за спецслужбами є дієвим інструментом

балансу повноважень без шкоди для оперативної ефективності. Громадський контроль з боку активного суспільства практично реалізується через створену Громадську раду при РНБО на національному рівні та мережу регіональних громадських рад безпеки в областях. Залучення авторитетних незалежних експертів, представників громадських організацій, журналістів до діяльності цих рад забезпечує суспільний нагляд за діяльністю безпекових структур в межах, сумісних з вимогами секретності. Система внутрішнього професійного аудиту з централізованою Службою інспекції всього сектору безпеки систематично забезпечує дотримання встановлених процедур та ефективність використання виділених ресурсів. Механізм періодичної незалежної зовнішньої оцінки ефективності системи із обов'язковим залученням авторитетних міжнародних експертів з багатим досвідом об'єктивно забезпечує неупередженість оцінок та можливість порівняння з міжнародними стандартами.

Технологічна платформа архітектури базується на прогресивних принципах хмарних розподілених обчислень, що дозволяють гнучке масштабування потужностей та надійне географічне резервування критичних даних для забезпечення їх безпеки навіть у разі фізичного знищення окремих центрів обробки даних.

Використання інноваційних блокчейн-технологій для зберігання найбільш критичних даних гарантує їх повну незмінність та прозору відстежуваність всіх операцій, що є критично важливим для запобігання внутрішнім маніпуляціям з даними та забезпечення довіри між різними відомствами.

Системи штучного інтелекту різного призначення органічно інтегровані на всіх рівнях управління для ефективної підтримки прийняття обґрунтованих рішень через аналіз величезних масивів даних, виявлення прихованих патернів, прогнозування розвитку ситуацій.

Квантово-захищені канали зв'язку з теоретично недосяжним рівнем безпеки гарантують абсолютну конфіденційність найбільш чутливих стратегічних комунікацій навіть від противника з необмеженими обчислювальними ресурсами.

Цифрові двійники всіх об'єктів критичної інфраструктури дозволяють безпечно моделювати наслідки різноманітних атак та систематично відпрацьовувати ефективні контрзаходи без ризику для реальних об'єктів.

Динамічна природа гібридних загроз, їх постійна еволюція та здатність до швидкої трансформації вимагають від системи національної безпеки не просто ефективних механізмів протидії існуючим викликам, а розвинених адаптаційних механізмів, що забезпечують випереджувальне пристосування до майбутніх, ще не проявлених форм агресії. Створення таких механізмів передбачає фундаментальний перехід від реактивної до проактивної парадигми безпекового управління, де система не лише реагує на зміни, а активно формує умови, що ускладнюють реалізацію гібридних стратегій противника.

Концептуальною основою адаптаційних механізмів є розуміння коеволюційної динаміки між системою національної безпеки та гібридними загрозами, де кожна дія захисту породжує контрдію нападу, кожне вдосконалення оборонних механізмів стимулює пошук нових вразливостей. Ця діалектика вимагає від системи не просто високої швидкості реакції, а здатності до антиципації, тобто передбачення напрямків еволюції загроз та завчасної підготовки контрзаходів [17].

Система раннього виявлення слабких сигналів про еволюцію загроз базується на концепції периферійного зору організації, коли увага приділяється не лише центральним добре відомим загрозам, а й маргінальним сигналам на периферії уваги. Традиційні системи моніторингу фокусуються на відомих типах загроз та встановлених індикаторах, натомість адаптивна система шукає аномалії, незвичайні патерни, слабкі сигнали, що можуть вказувати на формування нових типів загроз. Використання методів аналітики великих даних дозволяє обробляти величезні масиви неструктурованої інформації з відкритих джерел, таких як соціальні мережі, форуми, наукові публікації, для виявлення ранніх ознак нових гібридних тактик. Моніторинг дискусій у технологічних спільнотах може виявити потенційні нові вектори кібератак, аналіз трендів у соціальних мережах може вказати на підготовку інформаційних кампаній, відстеження наукових публікацій може попередити про технологічні прориви з безпековими імплікаціями.

Механізм сценарного прогнозування еволюції загроз поєднує експертні методи з комп'ютерним моделюванням для розробки альтернативних сценаріїв розвитку безпекового середовища. Регулярні стратегічні форсайт-сесії залучають не лише безпекових експертів, а й футурологів, технологів, соціологів для вироблення альтернативних сценаріїв розвитку гібридних загроз на горизонті від трьох до п'яти років.

Такий міждисциплінарний підхід дозволяє подолати відомчі та професійні шори, побачити загрози під різними кутами зору, врахувати несподівані фактори впливу. Комп'ютерне моделювання дозволяє симулювати поведінку противника в різних умовах та тестувати його можливі адаптації до наших контрзаходів, виявляючи потенційні вразливості нашої системи до їх реальної експлуатації. Створення каталогу сценаріїв від найбільш ймовірних до граничних, але можливих, дозволяє системі мати готові шаблони реагування на широкий спектр ситуацій.

Організаційна гнучкість як ключовий адаптаційний механізм реалізується через модульну архітектуру безпекових структур, коли замість жорстких організаційних форм створюються адаптивні модулі, що можуть швидко переконфігуруватися для протидії новим типам загроз. Механізм швидкого прототипування організаційних рішень дозволяє тестувати нові структури та процеси в обмеженому масштабі перед повномасштабним впровадженням, мінімізуючи ризики помилкових реформ. Створення експериментальних підрозділів, які працюють за новими принципами паралельно з основними структурами, дозволяє порівняти ефективність різних підходів в реальних умовах. Інноваційні лабораторії в рамках безпекових структур мають мандат на експериментування з новими підходами без обмежень традиційних бюрократичних процедур, що критично важливо для подолання інституційної інерції великих організацій [31].

Технологічна адаптивність забезпечується через створення технологічного радару як системи постійного моніторингу нових технологій, що можуть бути використані як для створення нових загроз, так і для протидії їм. Відстеження технологічних трендів у галузях штучного інтелекту, квантових обчислень, біотехнологій, нанотехнологій, автономних систем дозволяє завчасно оцінити їх потенційне безпекове значення. Механізм швидкого впровадження дозволяє тестувати та інтегрувати нові технології в операційну діяльність за тижні, а не роки, що є критичним в умовах швидкого технологічного прогресу. Створення власних дослідницьких центрів з фокусом

на технології подвійного призначення забезпечує технологічну автономію та можливість розробки унікальних рішень, недоступних противнику через комерційні канали. Партнерство з провідними технологічними компаніями та дослідницькими університетами дозволяє використовувати їх інноваційний потенціал для безпекових потреб.

Когнітивна адаптивність системи реалізується через механізми подолання ментальних моделей та когнітивних упереджень, що заважають розпізнавати нові типи загроз. Програми когнітивної різноманітності забезпечують залучення людей з різним бекграундом, досвідом, способом мислення до аналізу загроз, що дозволяє уникнути групового мислення та побачити ситуацію з різних перспектив. Ігри з альтернативними реальностями тренують здатність мислити поза усталеними рамками та уявляти неочікувані сценарії, розвиваючи креативність аналітиків. Техніки структурованої аналітичної дискусії, такі як метод адвоката диявола або аналіз конкуруючих гіпотез, допомагають критично оцінювати домінуючі припущення та виявляти альтернативні пояснення подій. Створення посади головного скептика в аналітичних підрозділах, чиєю роботою є систематичне оскарження консенсусних висновків, інституціоналізує критичне мислення.

Механізм навчання та еволюції системи перетворює кожен інцидент та кризу на джерело вдосконалення через створення адаптивних циклів навчання. Систематичний аналіз після дій включає не лише розбір того, що сталося, а й екстраполяцію уроків на майбутні сценарії через питання що якби. Бази даних уроків, систематизовані за типами інцидентів та контекстами, дозволяють швидко знаходити релевантний досвід для нових ситуацій. Механізми швидкого поширення виявлених кращих практик між підрозділами через внутрішні конференції, бюлетені, тренінги забезпечують масштабування успішних підходів. Створення посад менеджерів знань в кожному відомстві професіоналізує процес організаційного навчання, перетворюючи його з випадкового на систематичний процес.

Метаадаптивність, тобто здатність адаптувати самі механізми адаптації, забезпечує стійкість системи в довгостроковій перспективі через регулярний перегляд адаптаційних механізмів на предмет їх ефективності. Моніторинг швидкості та якості адаптацій дозволяє виявити проблеми в адаптаційних процесах до того, як вони призведуть до критичних збоїв.

Бенчмаркінг з іншими адаптивними системами, не обов'язково безпековими, такими як біологічні екосистеми, еволюційні алгоритми, адаптивні бізнес-організації, може надати несподівані інсайти для вдосконалення власних механізмів. Експерименти з новими формами адаптивності в контрольованих умовах дозволяють безпечно тестувати радикальні підходи. Таким чином, система може не лише адаптуватися до загроз, а й постійно вдосконалювати свою здатність до адаптації, створюючи позитивну спіраль еволюції.

Еволюційність архітектури свідомо закладена через спеціальні механізми регулярного критичного перегляду та планомірної адаптації до змін. Щорічні всебічні стратегічні огляди системно оцінюють адекватність існуючої архітектури новим викликам та загрозам, виявляючи структурні вразливості та функціональні прогалини до того, як вони будуть експлуатовані противником. Обмежені пілотні проекти дозволяють безпечно тестувати перспективні інноваційні організаційні рішення перед ризикованим повномасштабним впровадженням на всю систему, мінімізуючи ризики масштабних помилок.

Механізм сплячих елементів дозволяє швидко активувати додаткові резервні компоненти системи в гострих кризових ситуаціях без попередньої тривалої підготовки, забезпечуючи раптове нарощування спроможностей. Модульність всієї архітектури технічно забезпечує практичну можливість органічного додавання принципово нових елементів у майбутньому без руйнування та перебудови вже існуючої працюючої структури, що критично важливо для еволюційного розвитку без революційних потрясінь.

У цілому, запропонована концептуальна модель представляє собою інтегровану систему, де всі елементи взаємопов'язані та взаємозалежні, створюючи синергетичний ефект, що перевищує просту суму окремих компонентів. Базові принципи визначають філософію побудови системи, архітектурні рішення втілюють ці принципи в конкретні організаційні форми, механізми адаптації забезпечують динамічну відповідність системи еволюційній природі загроз. Модель є достатньо конкретною для практичної імплементації, але водночас достатньо гнучкою для адаптації до специфічних національних умов та еволюції безпекового середовища. Вона враховує як міжнародні кращі практики, так і унікальний український контекст, поєднуючи універсальні принципи ефективного управління з особливостями гібридної війни на сході Європи.

Висновки з даного дослідження і перспективи подальших досліджень. На основі проведених вище досліджень можна зробити такі узагальнені висновки.

1) Обґрунтована модель інституціалізації публічного управління національною безпекою в умовах гібридної війни представляє собою цілісну систему принципів, архітектурних рішень та механізмів адаптації, що забезпечують ефективну протидію комплексним багатовимірним загрозам через глибоку інтеграцію безпекових структур при збереженні їх функціональної спеціалізації. Тринадцять базових принципів моделі, від системної цілісності до економічної ефективності, формують концептуальну основу для подолання вразливостей традиційних секторальних підходів та створення справді інтегрованої системи управління. Ці принципи не є абстрактними теоретичними конструктами, а представляють собою практичні настанови для організації безпекових інституцій, кожен з яких відповідає на конкретні виклики гібридної війни та забезпечує певний аспект ефективності системи. Багаторівнева архітектура з інноваційним принципом функціональних кластерів на оперативному рівні, створенням Національного центру стійкості та мережі Регіональних центрів безпеки забезпечує організаційну основу для ефективної координації різнорідних компонентів системи на всіх рівнях від стратегічного до регіонального. Особливістю цієї архітектури є те, що вона не руйнує існуючі інституції, а створює над ними координаційні механізми, які забезпечують синергію без втрати спеціалізованої експертизи окремих відомств. При цьому запропонована модель враховує як кращі міжнародні практики країн, що успішно протидіяли гібридним загрозам, так і специфічний український контекст з його історичними, культурними та інституційними особливостями.

2) Практична реалізація моделі вимагає не лише структурних реформ, а й глибоких змін в організаційній культурі безпекових структур, подолання відомчого егоїзму, розвитку міжвідомчої довіри та співпраці. Відомчий егоїзм, коли структури розглядають інформацію, ресурси, повноваження як

відомчу власність, а не як інструменти для досягнення загальнонаціональних цілей, є однією з найсерйозніших перешкод для інтеграції. Подолання цієї ментальності вимагає не лише структурних змін, а й трансформації систем мотивації, кар'єрних траєкторій, професійної освіти.

3) Тому подальші дослідження мають зосередитися на розробці детальних механізмів імплементації запропонованої моделі в специфічних умовах України, включаючи правове забезпечення, ресурсні вимоги, поетапний план трансформації існуючих структур. Правове забезпечення вимагає розробки нового базового законодавства про національну безпеку, яке закріпить принципи інтеграції, повноваження координаційних структур, механізми міжвідомчої взаємодії. Ресурсні вимоги мають бути ретельно оцінені для забезпечення реалістичності плану трансформації.

4) Окремої уваги потребує розробка системи показників оцінювання ефективності інтегрованої системи управління національною безпекою, що дозволить об'єктивно вимірювати прогрес реформ та вносити корективи на основі емпіричних даних. Показники мають охоплювати різні аспекти ефективності системи від швидкості реагування на інциденти до якості стратегічного прогнозування. Система показників має бути збалансованою, включаючи як кількісні, так і якісні метрики, як короткострокові, так і довгострокові індикатори, як внутрішні процесні, так і зовнішні результативні показники.

5) Важливим є також дослідження міжнародного виміру інтеграції національних систем безпеки в контексті євроатлантичних структур та розвитку спільних спроможностей з партнерами для протидії транснаціональним гібридним загрозам. Гібридні загрози за своєю природою часто є транснаціональними, експлуатуючи вразливості глобалізованого світу, тому ефективна протидія їм вимагає міжнародної координації та співпраці. Інтеграція української системи національної безпеки з євроатлантичними структурами безпеки передбачає гармонізацію процедур, стандартів, термінології для забезпечення сумісності. Участь у програмах обміну інформацією з партнерами дозволяє отримувати ранні попередження про транснаціональні загрози. Спільні навчання та операції з союзниками розвивають практичні навички координації в реальних умовах.

6) Розвиток спільних спроможностей з партнерами може включати створення регіональних центрів протидії специфічним типам гібридних загроз, спільні дослідницькі проекти з розробки нових технологій безпеки, програми обміну персоналом для поширення кращих практик. Особливо перспективним є співробітництво у сфері кібербезпеки, де транснаціональний характер загроз робить міжнародну координацію критично важливою. Участь у міжнародних механізмах швидкого реагування на кіберінциденти, обмін індикаторами компрометації, спільні операції з атрибуції атак підвищують ефективність національних зусиль через міжнародну синергію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамов В. І., Ситник Г. П., Смолянюк В. Ф. Глобальна та національна безпека : підручник / За заг. ред. Г.П. Ситника. Київ : НАДУ, 2016. 784 с.
2. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: вибрані наукові праці. Київ : НІСД, 2016. 528 с.
3. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.
4. Горбулін В. П., Власюк О. С., Лібанова Е. М., Ляшенко О. М. Донбас і Крим: ціна повернення : монографія. Київ : НІСД, 2015. 474 с.

5. Гордієнко С. Г., Доронін І. М. Державна безпека України в сучасних умовах: проблеми компетенції державних органів. *Інформація і право*. 2021. № 2(37). С. 81–92. https://doi.org/10.37750/2616-6798.2021.2(37).238340

6. Ліпкан В. А. Національна безпека України : монографія. Київ : Кондор, 2009. 552 с.

7. Магда Є. В. Гібридна війна: вижити і перемогти. Харків : Віват, 2015. 304 с.

8. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 456 с.

9. Резнікова О. О., Цюкало В. Ю., Паливода В. О., Дрьомов С. В., Сьомін С. В. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналітична доповідь. Київ : НІСД, 2015. 58 с.

10. Світова гібридна війна: український фронт. *Вісник Національної академії наук України*. 2017. № 2. С. 3–8. https://nasplib.isofts.kiev.ua/handle/123456789/114454

11. Ситник Г. П. Національна безпека України: теорія і практика : навч. посіб. Київ : Кондор, 2007. 616 с.

12. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України : підручник / за ред. Г.П. Ситника. Київ : МАУП, 2021. 372 с.

13. Турченко О. Г., Груценко Ю. І. Національна безпека і державна безпека: поліваріантність визначення та співвідношення. *Правничий часопис Донецького національного університету імені Василя Стуса*. 2023. № 2. С. 66–74. https://doi.org/10.31558/2786-5835.2023.2.8

14. Alberts D. S., Hayes R. E. Understanding Command and Control. Washington : CCRP Publication Series, 2006. 284 p.

15. Arquilla J., Ronfeldt D. Swarming and the Future of Conflict. Santa Monica : RAND Corporation, 2000. 112 p.

16. Carlucci P., Mumford A. Hybrid Warfare: The Continuation of Ambiguity by Other Means. *European Journal of International Security*. 2023. Vol. 8. Is. 2. P. 192–206. https://doi.org/10.1017/eis.2022.19

17. Christensen C.M. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Boston : Harvard Business Review Press, 2016. 252 p.

18. Clarke R.A., Knake R.K. Cyber War: The Next Threat to National Security and What to Do About It. New York : Ecco, 2010. 290 p.

19. Dannreuther R. International Security: The Contemporary Agenda. Cambridge : Polity Press, 2007. 256 p.

20. Dziundziuk V. Stopping Cyberterror. *Per Concordiam. Journal of European Security and Defense Issues*. 2011. Vol. 2. Issue 2. P. 17–21.

21. Dziundziuk V. A War of Words. *Per Concordiam. Journal of European Security and Defense Issues*. 2015. Vol. 6. Issue 1. P. 50–55.

22. Garvin D. A., Edmondson A. C., Gino F. Is Yours a Learning Organization? *Harvard Business Review*. 2008. Vol. 86. No. 3. P. 109–116.

23. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007. 72 p.

24. Jackson B. A., Frelinger D. R. Understanding Why Terrorist Operations Succeed or Fail. Santa Monica : RAND Corporation, 2009. 68 p.

25. Libicki M. C. Cyberdeterrence and Cyberwar. Santa Monica : RAND Corporation, 2009. 240 p.

26. McCuen J. J. Hybrid Wars. *Military Review*. 2008. Vol. 88. No. 2. P. 107–113.

27. Nye J. S. The Future of Power. New York : PublicAffairs, 2011. 320 p.

28. Senge P. M. The Fifth Discipline: The Art and Practice of the Learning Organization. New York : Doubleday, 2006. 445 p.

29. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York : Oxford University Press, 2014. 320 p.

30. Weissmann M., Nilsson N., Palmertz B., Thunholm P. Hybrid Warfare: Security and Asymmetric Conflict in International Relations. London : I.B. Tauris, 2021. 288 p.

31. Wither J. K. Hybrid Warfare Revisited. A Battle of 'Buzzwords'. *Connections: The Quarterly Journal*. 2023. Vol. 22. No. 1. P. 7–27. https://doi.org/10.11610/Connections.22.1.02

Стаття надійшла до редакції 12.10.2025 р.
Стаття рекомендована до друку 15.11.2025 р.
Опубліковано 30.12.2025 р.

Pupialis Yegor Viktorovich,
Doctor of Law, Professor,
PhD student of the Department of Law, National Security and European Integration,
Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine

e-mail: pravo.nb.ei@karazin.ua *https://orcid.org/0009-0006-8972-1091*

CONCEPTUAL MODEL OF INSTITUTIONALIZATION OF PUBLIC ADMINISTRATION OF NATIONAL SECURITY IN HYBRID WAR CONDITIONS

Abstract. This article presents a comprehensive conceptual model for institutionalizing public administration of national security specifically adapted to address the multifaceted challenges of hybrid warfare. The research substantiates the critical necessity for fundamental transformation of traditional security institution approaches, demonstrating how sectoral specialization and rigid competency demarcation prove structurally inadequate when confronting complex multidimensional threats that systematically exploit inter-agency gaps and organizational fractures.

The study develops an innovative multilevel integration model that synthesizes strategic, operational, and regional management levels through a systematic framework of foundational principles, architectural elements, and adaptive mechanisms. Thirteen core principles are proposed for constructing an integrated management system: systemic integrity, adaptive architecture, network-centricity, information integration, proactivity, distributed resilience, inclusiveness, continuity, technological innovation, strategic communication, legal legitimacy, continuous learning, and economic efficiency. These principles address specific vulnerabilities of fragmented security systems while ensuring operational effectiveness in dynamic threat environments.

The architectural framework operates across three distinct levels, featuring an innovative functional cluster approach at the operational level that organizes related agencies under unified command structures. Key innovations include establishment of a National Resilience Center as an inter-agency coordination structure responsible for critical infrastructure protection and crisis management, alongside a network of Regional Security and Resilience Centers providing territorial coordination capabilities. This architecture maintains functional specialization while achieving deep institutional integration through horizontal networking mechanisms and shared information platforms.

Critical adaptation mechanisms enable system evolution in response to hybrid threat dynamics through early weak signal detection systems, scenario-based forecasting methodologies, organizational flexibility protocols, and cognitive adaptability frameworks. The model incorporates advanced technological platforms including artificial intelligence analytics, quantum-secured communications, blockchain data integrity systems, and digital twin infrastructure modeling capabilities.

The research demonstrates that this integrated approach generates synergistic effects exceeding the arithmetic sum of individual agency capabilities, while preserving essential functional autonomy and operational specialization. The model addresses the fundamental challenge of coordinating heterogeneous security components against multi-domain threats characteristic of contemporary hybrid aggression. Implementation requires not merely structural reforms but transformational changes in organizational culture, inter-agency trust development, and professional education approaches. The framework provides concrete architectural solutions for all management levels while maintaining sufficient flexibility for adaptation to evolving security environments and national contexts.

Keywords: institutionalization, public administration, national security, hybrid warfare, integrated management system, adaptive architecture, inter-agency coordination, strategic planning.

REFERENCES

1. Abramov, V.I., Sytnyk, H.P., & Smolianiuk, V.F. (2016). Global and National Security. Kyiv: NADU [in Ukrainian].
2. Vlasiuk, O.S. (2016). National Security of Ukraine: Evolution of Domestic Policy Problems. Kyiv: NISD [in Ukrainian].
3. Horbulin, V.P. (2017). World Hybrid War: Ukrainian Front. Kyiv: NISD, 496 p. [in Ukrainian].
4. Horbulin, V.P., Vlasiuk, O.S., Libanova, E.M., & Liashenko, O.M. (2015). Donbas and Crimea: The Price of Return. Kyiv: NISD [in Ukrainian].

5. Hordiienko, S.H., & Doronin, I.M. (2021). State Security of Ukraine in Modern Conditions: Problems of Competence of State Bodies. *Informatsiia i pravo, 2(37), 81–92.* https://doi.org/10.37750/2616-6798.2021.2(37).238340 [in Ukrainian].

6. Lipkan, V.A. (2009). National Security of Ukraine. Kyiv: Kondor [in Ukrainian].

7. Mahda, Ye.V. (2015). Hybrid War: Survive and Win. Kharkiv: Vivat [in Ukrainian].

8. Reznikova, O.O. (2022). National Resilience in a Changing Security Environment. Kyiv: NISD [in Ukrainian].

9. Reznikova, O.O., Tsiukalo, V.Yu., Palyvoda, V.O., Dromov, S.V., & Somin, S.V. (2015). Conceptual Foundations for the Development of Ukraine's National Security System. Kyiv: NISD [in Ukrainian].

10. World Hybrid War: Ukrainian Front. (2017). *Visnyk Natsionalnoi akademii nauk Ukrainy, 2, 3–8.* https://nasplib.isofts.kiev.ua/handle/123456789/114454 [in Ukrainian].

11. Sytnyk, H.P. (2007). National Security of Ukraine: Theory and Practice. Kyiv: Kondor [in Ukrainian].

12. Sytnyk, H.P., & Orel, M.H. (2021). National Security in the Context of Ukraine's European Integration. Kyiv: MAUP [in Ukrainian].

13. Turchenko, O.H., & Hrutsenko, Yu.I. (2023). National Security and State Security: Polyvariance of Definition and Correlation. *Pravnychyi chasopys Donetskoho natsionalnoho universytetu imeni Vasylia Stusa, 2, 66–74.* https://doi.org/10.31558/2786-5835.2023.2.8 [in Ukrainian].

14. Alberts, D.S., & Hayes, R.E. (2006). Understanding Command and Control. Washington: CCRP Publication Series, 284 p.

15. Arquilla, J., & Ronfeldt, D. (2000). Swarming and the Future of Conflict. Santa Monica: RAND Corporation, 112 p.

16. Carlucci, P., & Mumford, A. (2023). Hybrid Warfare: The Continuation of Ambiguity by Other Means. *European Journal of International Security, 8(2), 192–206.* https://doi.org/10.1017/eis.2022.19

17. Christensen, C.M. (2016). The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Boston: Harvard Business Review Press, 252 p.

18. Clarke, R.A., & Knake, R.K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco, 290 p.

19. Dannreuther, R. (2007). International Security: The Contemporary Agenda. Cambridge: Polity Press, 256 p.

20. Dziundziuk, V. (2011). Stopping Cyberterror. Per Concordiam. *Journal of European Security and Defense Issues, Vol. 2, Issue 2, 17–21.*

21. Dziundziuk V. (2015). A War of Words. Per Concordiam. *Journal of European Security and Defense Issues, Vol. 6, Issue 1, 50–55.*

22. Garvin, D.A., Edmondson, A.C., & Gino, F. (2008). Is Yours a Learning Organization? *Harvard Business Review, 86(3), 109–116*.

23. Hoffman, F.G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 72 p.

24. Jackson, B.A., & Frelinger, D.R. (2009). Understanding Why Terrorist Operations Succeed or Fail. Santa Monica: RAND Corporation, 68 p.

25. Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica: RAND Corporation, 240 p.

26. McCuen, J.J. (2008). Hybrid Wars. *Military Review, 88(2), 107–113.*

27. Nye, J.S. (2011). The Future of Power. New York: PublicAffairs, 320 p.

28. Senge, P.M. (2006). The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Doubleday, 445 p.

29. Singer, P.W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 320 p.

30. Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (2021). Hybrid Warfare: Security and Asymmetric Conflict in International Relations. London: I.B. Tauris, 288 p.

31. Wither, J.K. (2023). Hybrid Warfare Revisite. *A Battle of 'Buzzwords'. Connections: The Quarterly Journal, 22(1), 7–27.* https://doi.org/10.11610/Connections.22.1.02

The article was received by the editors 12.10.2025.
The article is recommended for printing 15.11.2025. Published 30.12.2025.