DOI 10.52363/2414-5866-2025-2-2
УДК 316.334.3 ; 316.334.4

Неводчікова І.М., *аспірант, НУЦЗУ, м. Черкаси,*
ORCID: 0009-0008-5998-8822

Nevodchokova I., *postgraduate student of National University of Civil Defence of Ukraine, Cherkasy*

ПЕРСПЕКТИВИ МОДЕЛЮВАННЯ ТА СТРАТЕГУВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ ГІБРИДНИМИ РИЗИКАМИ В СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ ПІД ЧАС РОЗВИТКУ КРИЗОВИХ СИТУАЦІЙ

PROSPECTS FOR MODELING AND STRATEGIZING PUBLIC MANAGEMENT OF HYBRID RISKS IN THE SECURITY AND DEFENSE SECTOR OF UKRAINE DURING THE DEVELOPMENT OF CRISIS SITUATIONS

Визнано необхідність доопрацювання чинної правової бази у сфері сектору й оборони України з позиції здійснення оцінювання стану його функціонування. У цьому контексті наполягається на забезпеченні розвитку такого інструментарію, як моделювання та стратегування. Виявлено перспективи розвитку інституційних (організаційних, інформаційно-аналітичних та ін.) механізмів управління у сфері управління гібридними ризиками в секторі безпеки і оборони.

Ключові слова*: публічне управління, система публічного управління, національна безпека, сектор безпеки й оборони, кризові ситуації, стратегування, моделювання, оцінювання.*

The need to finalize the current legal framework in the field of the security and defense sector of Ukraine from the perspective of assessing the state of its functioning is recognized. In this context, it is insisted on ensuring the development of such tools as modeling and strategizing. Prospects for the development of institutional (organizational, information and analytical, etc.) management mechanisms in the field of hybrid risk management in the security and defense sector are identified.

Key words: *public administration, public administration system, national security, security and defense sector, crisis situations, strategizing, modeling, evaluation.*

Постановка актуальності. Сучасний етап розвитку державного управління в Україні характеризується необхідністю адаптації до багатовимірних і непередбачуваних викликів, що постають перед сектором безпеки й оборони. В умовах триваючої збройної агресії російської

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

федерації, масштабних кібератак, інформаційних впливів, енергетичних криз і технологічних дестабілізацій формується новий тип ризиків – гібридні, які поєднують військові, інформаційні, політичні, економічні та соціальні загрози. Ці ризики підривають сталість державних інституцій, ускладнюють процес ухвалення управлінських рішень і потребують запровадження нових підходів до моделювання та стратегування у сфері публічного управління. Відтак, актуальність дослідження обумовлюється потребою розроблення національної системи стратегічного моделювання гібридних ризиків, інтегрованої в державну політику безпеки, оборони, інформаційної та кіберстійкості. Йдеться про створення адаптивної управлінської архітектури, яка поєднає аналітичні, прогнозні й комунікаційні інструменти, здатні забезпечити стійкість суспільства та ефективне реагування на кризові події.

Аналіз останніх досліджень і публікацій. Особливості формування механізмів управління в умовах криз досліджували В. Бакуменко, С. Бєлай, О. Бондаренко, А. Васильєв, І. Волков, В. Горбулін, Ю. Гладун, Ю. Древаль, Є. Живіло, О. Кравчук, О. Крюков, О. Ляшевська, Н. Нижник, В. Новіков, В. Олуйко, О. Пархоменко-Куцевіл, С. Порока, О. Труш, Т. Яровой та ін. [1; 2; 3]. Їхні роботи становлять важливу теоретико-методологічну базу для осмислення й аналізу механізмів держави у сфері гарантування безпеки крізь призму розвитку кризових ситуацій.

Постановка завдання. Мета статті полягає у визначенні перспектив моделювання та стратегування публічного управління гібридними ризиками в секторі безпеки і оборони України під час розвитку кризових ситуацій.

Виклад основного матеріалу дослідження. Поняття «гібридні ризики» у контексті публічного управління охоплює комплекс взаємопов'язаних загроз, які діють у різних площинах – політичній, інформаційній, економічній, воєнній, соціальній та технологічній. Вони поєднують асиметричні дії противника, маніпулятивні комунікації, кібероперації, дезінформаційні кампанії, використання енергетичних та економічних важелів впливу. Методологічно їхнє вивчення потребує синтезу стратегічного аналізу, системного підходу, ситуаційного моделювання та теорії складних адаптивних систем.

У публічному управлінні моделювання таких ризиків спирається на концепції resilience (стійкості), anticipatory governance (передбачувального управління) та network governance (мережевого врядування) (рис. 1). Вони передбачають розроблення інтегрованих моделей прогнозування, аналізу сценаріїв і побудову системних механізмів взаємодії між органами державної влади, силовими структурами, громадянським суспільством та приватним сектором. Одним із важливих методологічних підходів є мультиагентне моделювання (multi-agent modeling), що дає змогу оцінити поведінку різних акторів у кризових ситуаціях. У системі публічного

управління цей підхід дозволяє прогнозувати розвиток гібридних криз – від інформаційних атак до масових панічних реакцій – і вибудовувати адаптивні управлінські сценарії реагування.

Після 2014 року Україна зробила суттєвий поступ у створенні інституційної основи протидії гібридним загрозам. Було ухвалено Стратегію національної безпеки України (2020 р.), Стратегію кібербезпеки України (2021 р.), Доктрину інформаційної безпеки (2017 р.), а також Закон України «Про національний спротив» (2021 р.), які визначили стратегічні напрями державної політики у сфері гібридної безпеки.

Рис. 1. Концепції моделювання публічного управління гібридними ризиками в секторі безпеки і оборони України

Джерело: авторська розробка

Практика засвідчує, що система публічного управління у сфері безпеки залишається фрагментованою: існує дублювання функцій між силовими структурами, недостатня координація між міністерствами та обмежені можливості аналітичного прогнозування ризиків. Суттєвим недоліком є реактивний характер управлінських рішень, коли дії вживаються після виникнення кризи, а не на етапі її формування.

На цьому тлі позитивним прикладом можна вважати діяльність Національного координаційного центру кібербезпеки при РНБО України, який впроваджує системи моніторингу кіберзагроз і аналізу вразливостей критичної інфраструктури. У сфері інформаційної безпеки ефективним стало створення Центру стратегічних комунікацій та інформаційної безпеки, що координує інформаційні кампанії протидії ворожій пропаганді. Також спостерігається тенденція до інституціоналізації аналітичних структур у складі міністерств і регіональних адміністрацій, які займаються оцінкою ризиків і плануванням дій у кризових ситуаціях.

Гібридний характер сучасних конфліктів змінює саму логіку стратегічного планування в секторі безпеки. Якщо традиційна оборонна стратегія спиралася на військову силу та мобілізаційний потенціал, то нині ключовим ресурсом стає інформація, аналітика і швидкість управлінської реакції. Гібридні ризики мають нестандартну структуру впливу: вони здатні одночасно діяти на політичному, медійному, економічному й соціальному рівнях, утворюючи каскадні ефекти. Для України це означає необхідність створення єдиної аналітичної платформи оцінки гібридних ризиків, що охоплюватиме дані з сектору оборони, розвідки, енергетики, фінансової системи, кіберпростору та соціальних медіа.

Одним із ключових напрямів стратегування має стати інституціоналізація системи ситуаційного прогнозування (early warning system), яка забезпечить завчасне виявлення ознак гібридного впливу – дезінформаційних кампаній, кібератак, енергетичних диверсій тощо. Такі системи вже функціонують у країнах НАТО та ЄС (зокрема в Польщі, Естонії, Швеції), де моделі ситуаційного прогнозування інтегровані у процес прийняття державних рішень.

Щодо моделювання кризових ситуацій у секторі безпеки, то він передбачає використання цифрових симуляцій, алгоритмів машинного навчання, систем аналізу великих даних (Big Data) та аналітичних панелей для підтримки рішень. Застосування таких технологій дозволяє створювати динамічні моделі розвитку гібридних криз, визначати критичні точки управління та прогнозувати ефекти взаємодії різних секторів.

Перспективним є впровадження інтегрованих ситуаційних центрів, які об’єднують інформаційні потоки з різних державних і відомчих джерел. У цих центрах використовуються системи data fusion для узагальнення даних про події, що дозволяє оперативно реагувати на гібридні загрози. Особливої актуальності такі центри набувають у період воєнного стану, коли необхідно швидко ухвалювати рішення щодо евакуації, енергопостачання, протидії кібератакам і забезпечення громадського порядку.

Нормативно-правова база публічного управління у сфері протидії гібридним загрозам поступово розвивається, проте залишається недостатньо інтегрованою. Потребують оновлення положення Кодексу цивільного захисту України, Закону України «Про національну безпеку» (2018 р.) та суміжних актів, аби врахувати специфіку інформаційно-кібернетичних ризиків і соціальних впливів.

Необхідним кроком є розроблення Державної концепції управління гібридними ризиками, що визначатиме основні напрями стратегічного планування, аналітичного моніторингу, цифрової безпеки та взаємодії державних і недержавних акторів. У правовому полі це сприятиме закріпленню відповідальності за інформаційні диверсії, кібершантаж, деструктивні

психологічні операції, що нині часто залишаються поза межами правового реагування.

Висновки. Моделювання та стратегування публічного управління гібридними ризиками стає центральним напрямом реформування сектору безпеки й оборони України. Ефективність майбутньої системи державного управління визначатиметься здатністю синтезувати аналітику, технології, прогнозування та міжвідомчу координацію. На нашу думку, перспективними напрямами розвитку публічного управління гібридними ризиками є такі: 1) створення єдиної міжвідомчої системи аналітичного прогнозування гібридних ризиків; 2) впровадження цифрових моделей управління кризами на базі штучного інтелекту; 3) розвиток стратегічної культури аналітичного управління в органах державної влади; 4) формування національної школи сценарного планування у сфері безпеки; 5) інституційне зміцнення партнерства між державою, науковою спільнотою та ІТ-сектором. Таким чином, перехід від реактивного до прогностично-стратегічного управління гібридними ризиками є не лише вимогою часу, але й основою формування нової парадигми безпекового врядування, здатної забезпечити довгострокову стійкість України в умовах глобальної нестабільності.

Список використаних джерел:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. Харків: НУЦЗУ, 2024. 244 с.

2. Живило Є.О. Формування та запровадження ситуаційного управління сектором безпеки та оборони держави – основа ефективної системи державного управління. Публічне управління XXI століття: погляд у майбутнє : збірник тез XXI Міжнародного наукового конгресу. Харків : Вид-во ХарРІ НАДУ “Магістр”, 2021. DOI: https://doi.org/10.34213/mnkongr.2021.

3. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // *Public administration and state security aspects.* 2023. Vol. 2. P. 43–51.

References:

1. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the state sector: monograph. Kharkiv: NUCZU, 2024. 244 p.

2. Zhivylo E.O. Formation and implementation of situational management of the security and defense sector of the state - the basis of an effective system of public administration. Public administration of the 21st century: a look into the future: collection of abstracts of the 21st International Scientific Congress. Kharkiv: Publishing house of KharRI NAPU “Master”, 2021. DOI: https://doi.org/10.34213/mnkongr.2021.

3. Novikov V.O. Information and hybrid wars in the current environment: public-administrative aspect // Public administration and state security aspects. 2023. Vol. 2. P. 43–51.

дата надходження статті: 20.10.2025
дата прийняття статті: 24.11.2025
дата публікації: 27.12.2025