МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

ISSN 3083-6557 print

НАУКОВІ ПРАЦІ МАУП

Проблеми модернізації України

Випуск 1 (48), 2025

Київ
2025

УДК 330-339; 321.7; 159.9
М58

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 4 від 28.05.2025)

Редакційна колегія:
С. В. Храпатий (голова), д-р фіз.-мат. наук, проф.
І. А. Семенець-Орлова, д-р наук з держ. упр., проф.
Я. М. Раєвська, д-р психол. наук, проф.
С. О. Лисенко, д-р юрид. наук, проф.
А. І. Федосов, д-р мед. наук, проф.
М. І. Зубрицький, д-р. юрид. наук
О. М. Гордієнко, канд. техн. наук
В. І. Меджебель (*Чуєнко*), канд. юрид. наук
Л. М. Крива, канд. істор. наук
І. М. Капеліста (виконавчий редактор), канд. наук з держ. упр.
Є. Я. Черняк

Матеріали подано в авторській редакції.
Відповідальність за зміст та орфографію матеріалів несуть автори.

Міжрегіональна Академія управління персоналом.
М58 Наукові праці МАУП. Проблеми модернізації України / редкол.: С. В. Храпатий (голова) [та ін.]. Вип. 1 (48). Київ: Міжрегіональна Академія управління персоналом, 2025. 686 с. Бібліогр. в кінці ст.

У збірнику висвітлено матеріали X Міжнародної науково-практичної конференції "Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності" (Київ, Міжрегіональна Академія управління персоналом, 20–22 травня 2025 р.).

Наведено тези доповідей учасників науково-практичної конференції МАУП з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

Видається з 2001 року.
Періодичність: 1 раз на квартал.
Засновник: *ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом".*
УДК 330-339; 321.7; 159.9

© Міжрегіональна Академія управління персоналом (МАУП), 2025

А. П. Гринчук
Проведення оцінювання діяльності громадських організацій та установ, як окремий вид оціночної діяльності *506*

Ю. Е. Пашко
Охорона земель в містах а також інших населених пунктах *508*

Д. В. Святецький
Банкрутство фермерських господарств у новій реальності: виклики економіки та менеджменту *510*

Р. О. Поливач
Економічні санкції як відповідь міжнародного співтовариства на ядерну програму Ірану *513*

Я. В. Кушнір
Оренда території Гуантанамо як виклик принципу територіальної цілісності держав у міжнародному публічному праві *515*

А. А. Тернавська
Деякі аспекти криміналізації суспільно небезпечних діянь у сфері радіоекологічної безпеки *518*

СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

С. О. Лисенко
Формування державної політики у сфері інформаційної безпеки: пріоритети та інституційне забезпечення *521*

І. В. Сервецький
Моральна риторика, як ширма під час війни: між словом і смертю *523*

С. Г. Голубицький
Фінансові ризики в умовах сучасної геополітичної ситуації, як загроза економічній безпеці *525*

А. І. Тараненко
Забезпечення інформаційної безпеки фінансових установ в системі державного управління: сучасна методологія *528*

О. І. Ткаченко
Ідентифікація джерел інформації щодо викликів і загроз безпеці, крізь призму публічного управління *530*

О. В. Поляков
Перспективи розвитку нотаріату в умовах цифровізації: правовий аспект *532*

О. І. Полотнянко
Технічні інформаційні загрози виборчому процесу: правовий аспект *535*

Д. В. Шейбут
Сучасні міграційні процеси в ЄС: безпековий вимір *537*

С. О. ЛИСЕНКО
д-р юрид. наук, проф., ПрАТ "ВНЗ "МАУП"
директор Інституту безпеки, м. Київ, Україна
sl-bezpeka@iapm.edu.ua
ORCID ID: https://orcid.org/0000-0002-7050-5536

ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРІОРИТЕТИ ТА ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ

Становлення державної політики у сфері інформаційної безпеки в сучасних умовах є визначальним чинником стійкості державного управління, національної безпеки та забезпечення суверенітету в інформаційному просторі. В умовах гібридної агресії, масових дезінформаційних кампаній, кібератак, маніпулятивного втручання в суспільну свідомість та цифрової трансформації державного управління, питання ефективного формування та реалізації державної політики інформаційної безпеки набуває першочергового значення. Особливо це актуалізується для держави, яка перебуває у стані збройного конфлікту, оскільки інформаційна безпека постає не лише як складова національної безпеки, а й як інструмент стратегічного опору агресії.

Сучасна державна політика у сфері інформаційної безпеки повинна бути багаторівневою, інтегрованою та здатною до адаптації у відповідь на швидкі зміни інформаційного середовища. Її формування передбачає визначення стратегічних пріоритетів, зокрема: захисту критичної інформаційної інфраструктури; протидії кіберзагрозам; забезпечення інформаційного суверенітету; формування культури безпеки в інформаційному суспільстві; протидії дезінформації та маніпуляціям у цифровому просторі; розвитку кіберосвіти та цифрової грамотності населення; гармонізації національного законодавства з міжнародними нормами та стандартами, зокрема директивою NIS2 [1], стратегією ЄС з кібербезпеки, рекомендаціями НАТО та Ради Європи щодо електронного врядування та інформаційної демократії.

Одним із ключових викликів є слабка міжінституційна координація в системі державного управління інформаційною безпекою. В Україні існує низка органів, дотичних до регулювання цієї сфери: Рада національної безпеки і оборони, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Міністерство оборони, Міністерство цифрової трансформації, Національний координаційний центр кібербезпеки, Національний банк України (в частині кіберзахисту фінансового сектору) та інші [2]. Водночас відсутність чітко визначених сфер від-

повідальності, інституційна фрагментованість, дублювання повноважень, нерівномірність цифрової спроможності органів влади, відсутність єдиних стандартів та оперативного обміну інформацією між секторами істотно знижують ефективність реагування на загрози.

Для усунення зазначених диспропорцій необхідним є створення єдиної системи стратегічного планування у сфері інформаційної безпеки, що базується на принципах сценарного прогнозування, ризик-орієнтованого підходу, використання Threat Intelligence та принципів Zero Trust для державних систем. Ключовим інструментом має стати міжвідомчий ситуаційний центр на базі НКЦК при РНБО з розширеними функціями аналітичної підтримки прийняття рішень, координації галузевих SOC-центрів (fin-SOC, gov-SOC, edu-SOC), інтеграції кіберіндикаторів, автоматизованого виявлення інцидентів за STIX/TAXII та обміну даними з партнерами через єдину платформу MISP (Malware Information Sharing Platform). Пріоритетним напрямом розвитку має стати удосконалення законодавчої бази. Діючі нормативні акти — Закон України "Про основні засади забезпечення кібербезпеки", Закон "Про захист інформації в інформаційно-телекомунікаційних системах", окремі положення Закону "Про національну безпеку" — містять загальні принципи, проте не визначають алгоритмів реалізації політики, індикаторів ефективності, вимог до звітності та відповідальності [3]. Доцільним є ухвалення нового Кодексу інформаційної безпеки, який би уніфікував положення щодо захисту критичної інфраструктури, кіберінцидентів, аудиту, сертифікації безпеки цифрових систем, державного контролю та стандартів стійкості. Важливим також є нормативне закріплення індикаторів інформаційної безпеки (Key Cyber Indicators) із обов'язковою щорічною публікацією звітів органами державної влади, що дозволить сформувати публічну довіру до прозорості державного управління у сфері безпеки.

Інституційна модель державного управління інформаційною безпекою повинна ґрунтуватися на принципах централізованого стратегічного контролю та децентралізованого оперативного реагування. Такий підхід передбачає делегування певних повноважень галузевим суб'єктам — міністерствам, органам місцевої влади, державним підприємствам — за умови забезпечення прозорості, наявності внутрішніх політик ІБ, обов'язкових аудитів та сертифікацій. Зокрема, медичні установи, оператори мобільного зв'язку, енергетичні компанії, банки мають розробляти внутрішні стратегії інформаційної безпеки, погоджені з національними вимогами, проходити щорічний аудит на відповідність та звітувати про вжиті заходи в рамках державного моніторингу. Особливого значення набуває кадрове та експертне забезпечення реалізації інформаційної політики. Станом на сьогодні в Україні існує дефіцит висококваліфікованих фахівців у сфері кібербезпеки, аудиту, цифрової правової експертизи, інформаційної аналітики. Вирішення цього виклику потребує створення системи підготовки та підвищення кваліфікації кадрів для державного сектору за спеціалізованими навчальними програмами на базі університетів, наукових центрів, а також через спільні програми з міжнародними організаціями та структурами НАТО [4]. Доцільним є створення національного реєстру сертифікованих фахівців з інформаційної безпеки та введення обов'язкової сертифікації службовців, які працюють із критичними інформаційними системами.

Державна політика інформаційної безпеки має бути частиною ширшої стратегії цифрової трансформації держави, що передбачає побудову довіри до державних інститутів, забезпечення прозорості, надання якісних цифрових послуг громадянам та бізнесу в безпечному середовищі. Важливою є також інтеграція України в європейську систему кібербезпеки, зокрема шляхом участі у спільних проектах з ENISA

(Агентство ЄС з кібербезпеки), імплементації стандартів ETSI, спільного реагування на інциденти в рамках CSIRT-мереж, обміну best practices, участі в пілотних проєктах EU Cyber Resilience Act.

Джерела

1. *Шаповал Р. В.* Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. *Наше право*. 2014. № 6. С. 5–9. URL: http://nbuv.gov.ua/UJRN/Nashp_2014_6_3.
2. *Федорченко О. С.* Удосконалення координації діяльності суб'єктів забезпечення національної системи кібербезпеки. *Нове українське право*. 2024. Вип. 5. С. 71–77. URL: https://doi.org/10.51989/NUL.2024.5.10.
3. *Тарасюк А. В.* Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: юридичні науки. 2020. Т. 31 (70). Ч. 2. № 2. С. 119–124. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf
4. *Шемчук В. В.* Інформаційна безпека держави та інформаційна війна. Україна під час російсько-української війни 2014–2023 рр.: ґенеза національної стійкості крізь призму наукових досліджень : монографія / за заг. ред. Б. Попкова, С. Пєткова. Київ: Ліра-К, 2023. 272 с. С. 140–161. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/6494

І. В. СЕРВЕЦЬКИЙ

д-р юрид. наук, доц., професор кафедри кримінального права та процесу Київського університету права, м. Київ, Україна
siv2055@gmail.com
ORCID (https://orcid.org/0000-0002-5713-8911)

МОРАЛЬНА РИТОРИКА ЯК ШИРМА ПІД ЧАС ВІЙНИ: МІЖ СЛОВОМ І СМЕРТЮ

У тезах досліджено феномен використання філософсько-релігійної риторики під час війни, зокрема в українському контексті. Ми намагаємось довестиводить, що моральні гасла, які часто лунають з вуст українських посадовців, можуть виконувати не лише об'єднавчу функцію, але й функцію прикриття реального болю, втрат, героїзму та відповідальності кожного громадянина під час війни. Риторика добра і жертовності іноді стає ширмою для відсторонення від реального спротиву агресору РФ, а також інструментом легітимації політичної безвідповідальності.

З кожним днем війни Україна втрачає тисячі життів, десятки тисяч громадян пропали безвісті. А в цей же час у політичному та медійному просторі все частіше лунають висловлювання про "боротьбу добра зі злом", "світло переможе темряву", "святість жертви". Такі гасла без сумніву мають мобілізаційний і єднальний мотив, з одного боку. Проте, з іншого, виникає загроза: коли моральна риторика стає ширмою, що затуляє реальність — горе, біль, смерть і спротив мільонів українців, які виконують функцію захтсту вітчизни. Тези спрямовані на викриття цього явища як форми прихованого політичного лицемірства.

З одного боку мральна риторика як інструмент легітимації влади, під час війни моральна така мова слугує обґрунтуванням правоти, створенням морального під-