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

DOI: 10.52363/2414-5866-2026-1-9
УДК: 35.746

Клочко А.М., *д.ю.н., проф., ХНУВС, м. Харків*
ORCID: 0000-0002-6898-964X

Борисова Л.В., *к.ю.н., доц., НУЦЗУ, м. Харків*
ORCID: 0000-0001-6554-1949

Трефілова Л.М., *д.фіз.-мат.н, проф., НУЦЗУ, м. Харків*
ORCID: 0000-0001-8939-6491

Klochko A., *Doctor in Law Sciences, Professor, Vice-Rector, Kharkiv National University of Internal Affairs, Kharkiv*

Borysova L., *Ph.D in Law Sciences, Associate Professor, National University of Civil Protection of Ukraine, Kharkiv*

Trefilova L.M., *Doctor of Physical and Mathematical Sciences, Professor, National University of Civil Protection of Ukraine, Kharkiv*

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ, ІНСТИТУЦІЙНИЙ МЕХАНІЗМ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

THEORETICAL AND LEGAL FOUNDATIONS, INSTITUTIONAL FRAMEWORK AND PROSPECTS FOR THE DEVELOPMENT OF UKRAINE'S STATE POLICY IN THE FIELD OF INFORMATION SECURITY

Стаття присвячена комплексному аналізу державної та публічної політики України у сфері інформаційної безпеки в умовах сучасних загроз, зокрема збройного конфлікту та інформаційної війни. Методологічну основу дослідження становлять нормативно-правовий і порівняльний підходи. Розглянуто еволюцію поняття інформаційної безпеки через державоцентричний, правозахисний та інженерно-технічний підходи,

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

обґрунтовано необхідність їх інтеграції у двокомпонентну модель, що поєднує технічний і стратегічний виміри. Проаналізовано інституційну структуру, нормативно-правову базу та механізми формування політики, з урахуванням ролі держави та міжнародних партнерів. Визначено сильні сторони (розбудова інституцій, розвиток кіберзахисту) та ключові проблеми (фрагментація підходів, непрозорість, кадровий дефіцит). Окрему увагу приділено європейським та євроатлантичним орієнтирам розвитку, зокрема вимогам NIS 2, GDPR і підходам НАТО, що пов'язано з оновленням стратегічного циклу, юридичною гармонізацією з європейськими стандартами, впровадженням публічних показників ефективності, окреслити сильні та слабкі сторони чинної моделі в контексті європейських і євроатлантичних орієнтирів. Зроблено висновок про необхідність поєднання технічної безпеки з протидією когнітивним загрозам та забезпечення балансу між безпекою і правами людини як основи стійкості демократичної держави.

Ключові слова: державна політика, інформаційна безпека, кібербезпека, національна безпека, інформаційна політика, стандартизація, європейські та євроатлантичні орієнтири.

This article is devoted to a comprehensive analysis of Ukraine's state and public policies in the field of information security in the context of contemporary threats, particularly armed conflict and information warfare. The methodological framework of the study is based on regulatory-legal and comparative approaches. The evolution of the concept of information security is examined through state-centric, human rights-based, and engineering-technical approaches, and the necessity of integrating them into a two-component model combining technical and strategic dimensions is substantiated. The institutional structure, regulatory framework, and policy-making mechanisms are analyzed, taking into account the role of the state and international partners. Strengths (institutional development, cyber defense development) and key challenges (fragmented approaches, lack of transparency, personnel shortages) are identified. Particular attention is paid to

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

European and Euro-Atlantic development benchmarks, specifically the requirements of NIS 2, GDPR, and NATO approaches, which are linked to updating the strategic cycle, legal harmonization with European standards, and the introduction of public performance indicators, to identify the strengths and weaknesses of the current model in the context of European and Euro-Atlantic benchmarks. The conclusion was reached that it is necessary to combine technical security with countering cognitive threats and ensuring a balance between security and human rights as the foundation of a democratic state's resilience.

Keywords: public policy, information security, cybersecurity, national security, information policy, standardisation, European and Euro-Atlantic benchmarks.

Постановка проблеми. Що ми маємо на увазі, коли говоримо «інформаційна безпека» в контексті державної політики? Відповідь на це запитання може здаватися очевидною, але насправді вона далеко не однозначна. Для інженера це передусім захист серверів, баз даних і каналів зв'язку. Для правника – гарантії доступу до інформації та захист персональних даних. Для політика – це стійкість держави до зовнішнього інформаційного тиску. Кожна з цих відповідей правильна, але жодна не є повною.

Україна, мабуть, як жодна інша європейська держава, відчула на собі, що всі ці виміри існують не окремо, а в одному полі. Атака вірусу NotPetya у червні 2017 року одночасно паралізувала інформаційні системи десятків державних і приватних організацій та підірвала суспільну довіру до цифрової інфраструктури. Масована атака на «Київстар» у грудні 2023 року залишила без зв'язку мільйони абонентів і показала вразливість критичної інфраструктури навіть великого приватного оператора. В обох випадках технічний збій миттєво перетворювався на суспільно-політичну проблему. І навпаки, кампанії дезінформації, формально далекі від «технічної» кібербезпеки, мали цілком практичні наслідки для обороноздатності та соціальної згуртованості.

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

У політичній науці існують два усталені підходи до розуміння національної безпеки, і обидва релевантні для цієї теми. Реалістичний, пов'язаний передусім з ідеями Г. Моргентау (Morgenthau, 1949) [1], зосереджений на захищеності території та державних інститутів. Альтернативний підхід Human Security [2] значно ширший: він охоплює економічні, соціальні, гуманітарні, екологічні та інформаційні аспекти (UNDP, 1994). Саме другий підхід дозволяє побачити інформаційну безпеку як багатовимірне явище, а не як вузьку технічну дисципліну.

Стаття 17 Конституції України відносить забезпечення інформаційної безпеки до найважливіших функцій держави. Це формулювання стало юридичним фундаментом для розвитку цілої системи стратегій, законів, підзаконних актів і координаційних механізмів. Водночас, і це слід визнати, сам конституційний припис є доволі загальним, і його змістовне наповнення відбувалося вже на рівні поточного законодавства, часом непослідовно і з помітними лакунами.

Актуальність дослідження пояснюється не лише безпековою ситуацією. Не менш важливе те, що українська модель інформаційної безпеки зараз перебуває в стані одночасної внутрішньої перебудови і зовнішньої адаптації до підходів ЄС та НАТО. Ці два процеси не завжди рухаються синхронно, і саме напруга між ними становить дослідницький інтерес.

Мета статті – проаналізувати державну політику України у сфері інформаційної безпеки: її теоретичні засади, нормативно-правове регулювання, інституційне забезпечення та перспективи розвитку в умовах євроінтеграції й цифрових трансформацій. Для цього потрібно вирішити кілька завдань: простежити, як змінювалося саме поняття «інформаційна безпека» у науковому й правовому дискурсі; визначити, яким чином співвідносяться державна та публічна політика у цій сфері; описати нормативну й інституційну архітектуру України; і, нарешті, окреслити сильні та слабкі сторони чинної моделі в контексті європейських і євроатлантичних орієнтирів.

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

Аналіз наукових джерел. Дослідженню та аналізу питання державної політики України у сфері інформаційної безпеки присвячено велику кількість наукових праць. Вивченням державної політики в галузі інформаційної безпеки займаються такі науковці, як С. Байрак, Г. Почепцов, А. Рось, В. Клочко, А. Черниченко, Нашинець-Наумова, В. Брижко, В. Гавловський, Р. Калюжний, А. Марущак, В. Цимбалюк, Л. Харченко, В. Ліпкан та ін.

Виклад основного матеріалу. Поняття «інформаційна безпека» і чому одного визначення недостатньо. Поняття інформаційної безпеки не з'явилося в межах однієї дисципліни. Воно склалося на перетині щонайменше трьох інтелектуальних традицій, і кожна з них залишила у ньому свій відбиток.

Державоцентрична традиція трактує інформаційну безпеку як складову захисту суверенітету, конституційного ладу та інформаційного суверенітету. Ліпкан (2009) [3], наприклад, послідовно розглядає її через призму національних інтересів і загроз державності. Правозахисний підхід зміщує акцент на права людини: доступ до інформації, свободу вираження поглядів, приватність, захист персональних даних. Тут інформаційна безпека – це не стільки про державу, скільки про людину в інформаційному середовищі. Третій інженерно-технічний підхід найпрактичніший: інформація трактується як ресурс, а безпека як комплекс заходів для його захисту.

На міжнародному рівні найбільш усталеним лишається визначення через класичну тріаду CIA: конфіденційність (confidentiality), цілісність (integrity), доступність (availability). Міжнародний стандарт ISO/IEC 27000:2018 доповнює цей перелік автентичністю, підзвітністю, незаперечністю та надійністю. У вузькому сенсі інформаційна безпека – це організаційно-технічна дисципліна, пов'язана з управлінням ризиками для інформаційних активів. Таке розуміння має свою сферу застосування, і відмовлятися від нього було б помилкою.

Але для аналізу державної політики його замало. Особливо коли мова йде про країну, яка перебуває в стані збройного конфлікту й

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

водночас є об’єктом масштабних інформаційних операцій. Тут безпека інформації нерозривно пов’язана зі стійкістю суспільства до дезінформації, пропаганди, маніпуляцій та когнітивних операцій. Як зазначає Г. Почепцов (2015) [4], інформаційна війна працює не стільки через зламування систем, скільки через зламування довіри.

Тому в цій статті використовується двокомпонентна рамка: організаційно-технічний вимір (захист систем, даних, інфраструктури) та державно-стратегічний вимір (захист суверенітету, суспільної свідомості, інформаційного середовища). Це розмежування не абсолютне і на практиці обидва виміри постійно перетинаються. Але воно дозволяє зрозуміти логіку чинної політики і, головне, побачити, де ця логіка дає збої.

В українському законодавстві інформаційна безпека визначається через стан захищеності інтересів людини, суспільства і держави та через здатність протидіяти як технічним загрозам, так і негативним інформаційним впливам. Це визначення, по суті, вже містить обидва виміри, хоча на практиці їхня інтеграція досі лишається скоріше завданням, ніж здобутком.

Державна і публічна політика у сфері інформаційної безпеки: хто приймає рішення і хто впливає на них. Державна і публічна політика близькі, але не тотожні поняття. Перше стосується діяльності органів влади у вироблені рішень, застосуванні владних механізмів, регулюванні суспільних відносин. Друге ширше: воно включає й бізнес, і громадянське суспільство, і міжнародних партнерів, і експертні спільноти. Як влучно сформулював,Томас Р. Дай (Dye, 2017) [5] публічна політика – це все, що уряд вирішує робити або не робити, але з доповненням, що на це рішення впливає набагато ширше коло учасників, ніж сам уряд. У сфері інформаційної безпеки публічний характер політики проступає особливо чітко. І ось чому.

По-перше, тут неможливо обійтися без балансу між безпекою та свободою слова. Рішення РНБО щодо санкцій проти телеканалів «112 Україна», NewsOne і ZIK у лютому 2021 року стало, мабуть, найяскравішою ілюстрацією цієї дилеми: для одних це був необхідний крок протидії

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

ворожій пропаганді, для інших – небезпечний прецедент обмеження медіасвободи [6]. Обидві позиції мали свої підстави, і саме наявність такої суперечності робить цю сферу по-справжньому публічною.

По-друге, жодна держава не здатна забезпечити інформаційну безпеку самостійно, без приватного сектору та міжнародних партнерів. Коли CERT-UA реагує на кіберінцидент, що зачіпає приватну телекомунікаційну компанію, – це вже не суто державна справа. Коли Meta чи Google видаляють координовані мережі акаунтів, що поширюють дезінформацію про Україну, – це теж елемент інформаційної безпеки, хоча й поза юрисдикцією української держави.

По-третє, суспільний контроль за рішеннями влади у цій сфері – не розкіш, а необхідність. Інакше «інформаційна безпека» легко перетворюється на зручне обґрунтування для обмеження публічного дискурсу.

Теоретично ці процеси можна описати через кілька класичних моделей аналізу політики. Раціональна модель [7, С.37-41] передбачає, що держава виявляє проблему, аналізує альтернативи й обирає оптимальне рішення. Ця логіка простежується, скажімо, у формуванні Стратегії кібербезпеки України (2021) або в створенні Центру протидії дезінформації. Інкременталістський підхід [7, С.41-44] краще пояснює поступовий, іноді надто повільний характер реформ: зміни до законодавства про захист персональних даних, еволюція вимог до кіберзахисту, поступова адаптація цифрових сервісів. Тут прогрес є, але він відбувається не ривками, а дрібними кроками. Чи завжди це недолік? У настільки чутливій сфері не обов'язково.

Особливо цікавою є теорія множинних потоків Кінгдона (Kingdon, 1984) [8, С.165-208]. Вона акцентує роль кризових подій, які відкривають «вікно можливостей» для політичних рішень. Після атаки NotPetya у 2017 році Україна суттєво прискорила розробку нормативної бази з кібербезпеки. Після повномасштабного вторгнення у 2022 році ще раз переглянула підходи до захисту критичної інфраструктури. Механізм той

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

самий: криза створює суспільний запит, а політична воля й інституційна готовність дозволяють цей запит реалізувати.

Мережева модель, мабуть, найточніше описує реальну конфігурацію цієї сфери. Інформаційна безпека давно формується не зусиллями однієї лише держави, а через складну взаємодію міжнародних організацій, приватного сектору, технологічних корпорацій і громадянських ініціатив. Разом із тим інституціональний підхід нагадує, що без формалізованих компетенцій і правових процедур жодна мережа не працюватиме стабільно. Українська політика фактично поєднує елементи всіх цих моделей іноді органічно, іноді з помітними суперечностями.

Нормативно-правова база та інституційна архітектура. Нормативний каркас державної політики у сфері інформаційної безпеки має кілька рівнів, і це не просто формальна класифікація, адже від рівня залежить юридична сила та практична застосовність норми.

Конституційний рівень уже згадувався: стаття 17 закріплює інформаційну безпеку як одну з найважливіших функцій держави. Стратегічний рівень представлений документами, що визначають загальні напрями політики такі як Стратегія національної безпеки (2020), Стратегія інформаційної безпеки (2021), Стратегія кібербезпеки України. Третій рівень – спеціальне законодавство: Закон України «Про основні засади забезпечення кібербезпеки України» (2017), закони про захист інформації, про електронні комунікації, підзаконні акти щодо критичної інфраструктури, інцидентного реагування тощо.

Авторами цієї статті не вдалося знайти систематизованого публічного огляду всієї нормативної бази у цій сфері, що, власне, саме по собі є симптомом. Документів багато, вони розпорошені між різними органами та періодами прийняття, і їхня внутрішня узгодженість не завжди очевидна навіть для фахівця.

Сучасна модель спирається на два взаємодоповнювальні контури. Перший – інформаційна безпека у широкому сенсі: стратегічні комунікації, протидія дезінформації, захист права на інформацію, безпека медіапростору. Другий – кібербезпека: захист систем і ресурсів у

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

кіберпросторі, реагування на інциденти, безпека державних реєстрів, телекомунікаційних мереж, об'єктів критичної інфраструктури. Формально межа між ними є. На практиці вона розмита, і це створює як проблеми координації, так і можливості для гнучкого реагування. Інституційна архітектура доволі розгалужена. Координаційну роль відіграє Рада національної безпеки і оборони України (РНБО), при якій діє Національний координаційний центр кібербезпеки. Окремим суб'єктом є Центр протидії дезінформації при РНБО. Ключові оперативні функції виконують Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку) і CERT-UA як національна команда реагування на кіберінциденти. До системи також залучені центральні органи виконавчої влади та органи місцевого самоврядування.

Тут варто зупинитися на одному практичному спостереженні. Коли в публічному дискурсі обговорюють інформаційну безпеку, її зазвичай зводять до одного з двох полюсів: або це «цензура», або це «захист серверів». Але реальні збої виникають саме на стику. Досвід реагування на атаку проти «Київстар» у грудні 2023 року показав, що технічне відновлення, хоч і тривале, зрештою відбулося, але публічна комунікація – хто, що й коли повідомляє суспільству виявилася значно менш відпрацьовано. Навіть локальний інцидент у системі документообігу районної адміністрації здатен перерости в кризу довіри, якщо немає зрозумілого алгоритму комунікації після нього. Саме в цьому місці, як видається, українська система ще формується: технічне реагування вже значно випередило комунікаційне.

Останні тенденції свідчать про рух до логіки безперервного захисту, або «життєвого циклу безпеки». Захист системи більше не розглядається як одноразова сертифікація. Натомість впроваджується безперервний процес авторизації, оцінювання відповідності, моніторингу, реагування. Ідея не нова і запозичена з міжнародної практики (зокрема з підходів NIST), але її адаптація до українських умов є окремою складною задачею, яка потребує і кадрів, і фінансування, і, що не менш важливо, зміни управлінської культури.

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

Сильні сторони, проблеми та прогалини. Було б несправедливо не відзначити того, що вже зроблено. За останні десять років Україна фактично з нуля побудувала інституційну архітектуру інформаційної та кібербезпеки. Існує більш-менш узгоджений стратегічний каркас, що пов’язує національну, інформаційну та кібербезпеку. Працюють координаційні механізми хоч і не ідеально, але вони є і функціонують. Система реагування на кіберінциденти, зокрема CERT-UA, здобула міжнародне визнання, особливо після 2022 року, коли обсяг атак зріс у рази (Microsoft Digital Defense Report, 2022) [9]. Поступово впроваджується ризик-орієнтований підхід, який наближає українську модель до стандартів ЄС.

Але говорити лише про здобутки було б не зовсім чесно. Найбільш помітна проблема – фрагментація між двома контурами. Кібербезпековий вимір виглядає більш формалізованим: є технічні стандарти, процедури, чіткі компетенції. А от гуманітарно-інформаційний компонент – стратегічні комунікації, медіаграмотність, протидія дезінформації, розвиток критичного мислення значно складніше піддається стандартизації. Як виміряти «стійкість суспільства до дезінформації»? На це питання поки що немає задовільної відповіді ані в Україні, ані, відверто кажучи, десь у світі.

Другою проблемою є непрозорість. Автору не вдалося знайти відкритих систематизованих даних про бюджетне забезпечення політики інформаційної безпеки, про показники її ефективності, про результати моніторингу імплементації стратегій. Наявність нормативного акта і його реальне виконання, як відомо, дві різні речі. Без публічних індикаторів зовнішня оцінка ефективності лишається, по суті, здогадкою.

Третє – кадри та інституційна пам’ять. Питання підготовки фахівців із кібербезпеки та інформаційної безпеки в Україні поки що вирішується фрагментарно. Ротація кадрів у державних органах призводить до втрати накопиченого досвіду. Культура кібергігієни навіть серед державних службовців лишається скоріше декларацією, ніж повсякденною практикою. Сказати, що це другорядні питання, не можна,адже саме вони нерідко визначають, чи спрацює система в момент реальної кризи.

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

Окремо слід згадати сферу захисту персональних даних. Тут Україна помітно відстає від європейського рівня деталізації. Процедури інцидентної звітності, критерії суттєвості інцидентів, строки повідомлення – все це потребує подальшого розвитку, особливо в контексті очікуваної адаптації до вимог GDPR та Директиви NIS 2.

Загальний висновок цього розділу, мабуть, такий: архітектура вже є, і вона непогана. Але її надійність потрібно постійно доводити на практиці, а саме з цим поки що складно.

Європейські та євроатлантичні орієнтири. Подальший розвиток української моделі логічно розглядати у контексті двох зовнішніх систем координат: ЄС і НАТО. Це вже не тільки зовнішньополітичний орієнтир, це практичний напрям внутрішньої реформи, зафіксований у тому числі в Угоді про асоціацію та у заявці на членство в ЄС.

Європейська модель відзначається високим рівнем правової формалізації. Директива NIS 2 (Directive 2022/2555) встановлює обов'язкові вимоги до управління ризиками, інцидентної звітності та корпоративної відповідальності для суб'єктів критичної інфраструктури. Регламент DORA (Digital Operational Resilience Act) додатково регулює цифрову стійкість фінансового сектору. GDPR, хоча формально стосується захисту даних, а не кібербезпеки, створює правову рамку, що безпосередньо впливає на безпекові практики. Підхід ЄС можна назвати структурованим і прагматичним: він чітко визначає, хто за що відповідає і що відбувається, коли ці вимоги не виконуються.

НАТО пропонує іншу, ширшу доктринальну рамку. Технічне ядро «information assurance» тут поєднується з протидією інформаційним і когнітивним загрозам. Безпека розуміється не лише як захист систем, а як захист інформаційного середовища загалом, включно з суспільною свідомістю та довірою до інституцій. Стратегічна концепція НАТО 2022 року вперше явно включила протидію дезінформації та інформаційним операціям до переліку ключових завдань Альянсу [10]. Цей підхід ширший, але й складніший для правової операціоналізації.

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

Українська модель рухається між обома орієнтирами. Вона вже містить елементи технічної стандартизації (ближче до логіки ЄС) і водночас приділяє значну увагу протидії дезінформації та інформаційним операціям (ближче до логіки НАТО). Подальша гармонізація, очевидно, має відбуватися одночасно у двох напрямах: поглиблення правової деталізації та стандартів стійкості, з одного боку, та посилення інституційної спроможності у сфері стратегічних комунікацій і реагування на когнітивні загрози з іншого. Не або-або, а обидва разом.

Втім, тут є одна практична складність, яку не варто замовчувати. Адаптація до вимог ЄС потребує значних фінансових, кадрових, організаційних ресурсів. В умовах воєнного часу ці ресурси обмежені, а пріоритети конкурують. Як забезпечити одночасну імплементацію NIS 2, GDPR і розбудову спроможностей стратегічних комунікацій є питанням, на яке наразі немає готової відповіді.

Висновки. Інформаційна безпека у сучасних умовах як категорія давно переросла суто технічне розуміння. Вона включає і захист систем та даних, і захист суверенітету, суспільної свідомості, інформаційного середовища. Спроба звести її до одного з цих вимірів неминуче збіднює картину.

Українська державна політика у цій сфері пройшла значний шлях. За десять років створено інституційну архітектуру, ухвалено стратегічні документи, розбудовано систему реагування на інциденти. Модель спирається на два контури – інформаційну безпеку та кібербезпеку, які мають діяти узгоджено. На практиці ця узгодженість поки що залишається скоріше амбіцією, ніж стабільним результатом.

Серед сильних сторін є наявність стратегічного каркасу, координаційних механізмів, ризик-орієнтованого підходу та визнаної на міжнародному рівні системи реагування. Серед слабких – фрагментація між технічним і гуманітарним контурами, непрозорість даних про ефективність, кадровий дефіцит і нерівномірність практичного впровадження норм. Іншими словами є механізми, але їх якість роботи неоднакова.

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

Нормативні рамки ЄС (насамперед NIS 2 та GDPR) і доктринальні підходи НАТО задають зовнішні орієнтири розвитку. Європейський підхід пропонує модель правової формалізації стійкості та відповідальності. Євроатлантичний показує необхідність інтеграції технічного захисту з протидією когнітивним загрозам. Для України актуальне поєднання обох, хоча ресурсні обмеження воєнного часу ускладнюють цей процес. Перспективи пов'язані з оновленням стратегічного циклу, юридичною гармонізацією з європейськими стандартами, впровадженням публічних показників ефективності, зміцненням кадрового потенціалу та збереженням балансу між безпекою і правами людини. Якщо це вдасться, інформаційна безпека може стати не лише сферою реагування на загрози, а однією з основ демократичного розвитку та державної стійкості України.

Список використаних джерел:

1. Morgenthau H. J. Politics Among Nations: The Struggle for Power and Peace. 2nd ed. New York : Alfred A. Knopf, 1955.
2. Nobel J. W. Morgenthau's Struggle with Power: The Theory of Power Politics and the Cold War. Review of International Studies. 1995. Vol. 21, № 1. P. 61–86.
3. The Human Security Framework and National Human Development Reports: Thematic Guidance Note. UNDP, 2006. URL: https://hdr.undp.org/content/human-security-framework-and-national-human-development-reports
4. Ліпкан В. А. Теорія національної безпеки : підручник. Київ : КНТ, 2009. 631 с.
5. Почепцов Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2015. 496 с.
6. Dye T. R. Understanding Public Policy. 15th ed. Florida State University.
7. Нацрада з телерадіомовлення повідомить провайдерам про необхідність дотримуватися рішення РНБО про санкції проти «112 Україна», ZIK і NewsOne. URL: https://webportal.nrada.gov.ua/natsrada-z-teleradiomovlennya-povidomyt-provajderam-pro-neobhidnist-

dotrymuvatysya-rishennya-rnbo-pro-sanktsiyi-proty-112-ukrayina-zik-i-newsone/

8. Дай Т. Р. Основи державної політики / пер. з англ. Г. Є. Краснокутського ; наук. ред. З. В. Балабаєва. Одеса : АО БАХВА, 2005. 468 с.

9. Kingdon J. W. Agendas, Alternatives, and Public Policies. Boston : Little, Brown and Company, 1984.

10. Kingdon J. W. Agendas, Alternatives, and Public Policies. 2nd ed. Boston : Little, Brown, 1995. P. 165–208.

11. Звіт про цифровий захист Microsoft 2022. URL: https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022

12. Стратегічна концепція НАТО 2022 року, ухвалена главами держав і урядів на Мадридському саміті НАТО 29 червня 2022 року. URL: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept-ukr.pdf

References:

1. Morgenthau, H. J. (1955). *Politics among nations: The struggle for power and peace* (2nd ed.). Alfred A. Knopf.

2. Nobel, J. W. (1995). Morgenthau's struggle with power: The theory of power politics and the Cold War. *Review of International Studies, 21*(1), 61–86.

3. United Nations Development Programme. (2006). *The human security framework and national human development reports: Thematic guidance note*. https://hdr.undp.org/content/human-security-framework-and-national-human-development-reports

4. Ліпкан, В. А. (2009). *Теорія національної безпеки*. КНТ.

5. Почепцов, Г. (2015). *Сучасні інформаційні війни*. Києво-Могилянська академія.

6. Dye, T. R. (n.d.). *Understanding public policy* (15th ed.). Florida State University.

7. Національна рада України з питань телебачення і радіомовлення. (n.d.). Нацрада з телерадіомовлення повідомить провайдерам про необхідність дотримуватися рішення РНБО про санкції

проти «112 Україна», ZIK і NewsOne. https://webportal.nrada.gov.ua/natsrada-z-teleradiomovlennya-povidomyt-provajderam-pro-neobhidnist-dotrymuvatysya-rishennya-rnbo-pro-sanktsiyi-proty-112-ukrayina-zik-i-newsone/

8. Дай, Т. Р. (2005). *Основи державної політики* (Г. Є. Краснокутський, пер.; З. В. Балабаєва, наук. ред.). АО БАХВА.

9. Kingdon, J. W. (1984). *Agendas, alternatives, and public policies*. Little, Brown and Company.

10. Kingdon, J. W. (1995). *Agendas, alternatives, and public policies* (2nd ed.). Little, Brown.

11. Microsoft. (2022). *Microsoft digital defense report 2022*. https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022

12. North Atlantic Treaty Organization. (2022). *NATO 2022 strategic concept*. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept-ukr.pdf

Фінансування. Дослідження виконано без залучення зовнішнього фінансування

Використання штучного інтелекту. Під час підготовки статті авторами використовувалися інструменти штучного інтелекту для технічного редагування списку використаних джерел і References. Усі результати дослідження, висновки та інтерпретації отримані авторами самостійно. Автори несуть повну відповідальність за зміст статті.

Подяки. Подяки відсутні.

Отримано: 24.03.2026
Прийнято: 26.05.2026
Опубліковано: 22.06.2026