УДК 354:004:001.126
Олександр Дубовський,
ад'юнкт штатний науково-організаційного відділення,
Військовий інститут Київського національного університету
імені Тараса Шевченка,
ag_dubovskiy@ukr.net
ORCID ID: 0009-0001-5587-7980
DOI 10.29038/2524-2679-2024-01-16-27

УПРАВЛІННЯ СВІТОВИМ ІНФОРМАЦІЙНИМ ПРОСТОРОМ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ

У статті обґрунтовано необхідність управління світовим інформаційним простором, здійснено огляд актуального правового забезпечення, визначено можливості та обмеження управління світовим інформаційним простором. Розкрито амбівалентність глобалізації інформаційного простору та відповідно до особливостей визначено властивості й принципи глобального управління. Розглянуто правове забезпечення регулювання світового інформаційного простору на рівні міжнародних, регіональних і національних правових актів. Представлено чинних суб'єктів потенційного управління світовим інформаційним простором. Проаналізовано виклики та проблеми регулювання світового інформаційного простору на міжнародному рівні. Визначено перспективні напрями подолання наявних обмежень і розв'язання проблемних аспектів. Можливості управління світовим інформаційним простором ґрунтуються на наявних правових нормах та стандартах, їх пластичності в межах загальних положень міжнародного права й національного законодавства, на ініціативах громадських організацій, експертних об'єднань, які швидше можуть реагувати на актуальні виклики; на використанні інформаційних технологій як внутрішнього механізму регулювання інформаційного простору; на впровадженні мережевого підходу з ієрархічною структурою множини управлінських груп, котрі взаємодіють на основі великої кількості взаємозв'язків, що відповідають логіці й темпам глобалізації. Обмеження управління світовим інформаційним простором стосуються неадаптованого до сучасних динамічних умов та неуніфікованого нормативно-правового забезпечення, відсутності прозорості й неупередженості в міжнародних

політичних відносинах через асиметричність у розподілі ресурсів і глибоку інтегрованість інформаційного простору в різні сфери суспільного буття; іррадіації наслідків управлінських заходів у регулюванні світового інформаційного простору на функціонування інших сфер суспільного буття та швидкості розвитку світової інформаційної інфраструктури.
Ключові слова: світовий інформаційний простір, інформаційна безпека, інтеграція, інформатизація суспільства.

Oleksandr Dubovskyi,
Military Institute of Taras Shevchenko National University of Kyiv,
ORCID ID: 0009-0001-5587-7980

GOVERNANCE OF GLOBAL INFORMATION SPACE: OPPORTUNITIES AND LIMITATIONS

The article substantiates the necessity of managing the global information space, reviews current legal provisions, identifies opportunities and limitations of managing the global information space. The ambivalence of the globalization of the information space is revealed, and the properties and principles of global management are determined in accordance with its features. The legal support for the regulation of the global information space at the level of international, regional and national legal acts is considered. The current actors of potential global information space management are presented. The challenges and problems of regulating the global information space at the international level are analyzed. Prospective directions for overcoming existing limitations and solving problematic aspects are determined. The possibilities of managing the global information space are based on: existing legal norms and standards, their flexibility within the general provisions of international law and national legislation, on the initiatives of public organizations, expert associations, which can quickly respond to current challenges; on the use of information technologies as an internal mechanism for regulating the information space; on the implemented network approach with a hierarchical structure of multiple management groups that interact on the basis of a large number of relationships, which corresponds to the logic and pace of globalization. Limitations of the global information space management include: non-adapted to modern dynamic conditions and non-unified regulatory and legal support; the lack of transparency and impartiality in international political relations due to the asymmetry in the distribution of resources and the deep integration of the information space into various spheres of social life; irradiation of the consequences of management measures in the regulation of the world information

space on the functioning of other spheres of social life and the speed of development of the world information infrastructure.
Key words: global information space, information security, integration, informatization of society.

1. ВСТУП

Постановка проблеми. Глобалізація різних сфер суспільного буття супроводжується розширенням інформаційних мереж, інтенсифікацією інформаційних потоків, збільшенням значення та вартості інформації. Розвиток інформаційних технологій об'єктивує інформаційний простір як кіберпростір, паралельну реальність, суб'єктивне відображення дійсності, екзопсихіку. Стабільність і захищеність економічної, політичної, соціальної, духовно-культурної та військово-оборонної сфер залежить від урегульованості та захищеності інформаційного простору, який є джерелом дестабілізувальних і конфліктогенних впливів в умовах невизначеності зон відповідальності, правового забезпечення, механізмів управління та його суб'єктності.

Аналіз останніх досліджень і публікацій. Із цієї проблематики можна відзначити дослідження правових аспектів захисту глобального інформаційного простору в умовах збройних конфліктів Х. Ламана, детермінант інформаційних загроз у глобальному інформаційному просторі О. Кузьменко, шляхів забезпечення захисту інформаційного простору держави С. Глобенка, інформаційного простору в контексті міжнародної безпеки К. Бугайчука, глобального інформаційного простору як інфраструктурного середовища інформаційної безпеки держави Я. Чмиря, штучного інтелекту як інструмента державного управління інформаційною безпекою В. Бондаря, критеріїв достатності інформаційної безпеки О. Бортнікової, інформаційних загроз і стратегій протидії В. Євдокімова.

Мета дослідження – визначити актуальні можливості та обмеження управління світовим інформаційним простором у глобальному й фрагментарному аспектах.

Для реалізації мети передбачено низку **завдань:** обґрунтувати необхідність управління світовим інформаційним простором, окреслити актуальне правове забезпечення, представити проблемні аспекти та можливості його реалізації.

Методика дослідження. Методологія дослідження ґрунтується на використанні феноменологічного підходу й загальнонаукових методів,

а саме гіпотетико-дедуктивного методу, аналізу, синтезу, порівняння та узагальнення.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Глобалізація створила плідні умови для проростання інформаційних потоків у різні сфери суспільного буття, надаючи інформації нової економічної та політичної ваги. Інформаційні відносини актуалізували четвертий вимір суспільного розвитку, підтверджуючи його рівність із загальновідомими, такими як дипломатичний, економічний та військовий рівні [1]. Глобалізація інформаційного простору породила також окремий вимір злочинності – кіберзлочинність: хакерські атаки, фішинг, зломи даних, поширення шкідливого програмного забезпечення, збір, зберігання та використання персональних даних без згоди користувачів. Її масштабність може сягати кібертероризму з атаками на критичну інфраструктуру держави й нового типу війни, яка в порівнянні з реальними військовими операціями є менш ризикованою та ресурсовитратною. Інформаційний простір може застосовуватися для поширення дезінформації та пропаганди з метою впливу на суспільну думку, політичні процеси, економічні рішення й суспільну стабільність [2]. Неоднаковий доступ до інформаційних технологій та інтернету створює цифровий розрив між різними соціальними групами й країнами, породжує культурну гомогенізацію через домінування певних культурних продуктів і медіа, сприяє монополізації ринку інформаційних ресурсів великими транснаціональними корпораціями. Соціальні мережі відкривають нову реальність соціального життя, звичні правила та закони якого тут не працюють [3]. Псевдоособистості, вплив на контент, великий ступінь довіри, лідери думок, генерування контенту штучним інтелектом, нейронні мережі та комерційні інтереси, викривлення сприймання формують нові виклики для розробки й упровадження правового регулювання та зон відповідальності.

Зважаючи на різноплановість і різномасштабність загроз, світовий інформаційний простір потребує управління та правового регулювання. Управління передбачає процес забезпечення глобальними акторами нівелювання негативних і посилення позитивних для людської спільноти ефектів глобалізації через використання засобів та механізмів, які діють на різних рівнях – локальному, національному, регіональному й глобальному [4, с. 71]. Такий системний підхід передбачає врахування особливостей світового інформаційного простору, що зумовлені загальними

глобалізаційними процесами та суспільною природою механізмів його саморегуляції. Особливостями світового інформаційного простору є всеохопний та сегментарний характер, системоутворюючий вплив на різні сфери суспільного буття й змістова відповідність сфері функціонування інформаційної інфраструктури, багатосуб'єктність та багатооб'єктність, висока проникність, відсутність геополітичної відповідності, високий ступінь довіри, залежність від темпів інформаційно-технологічного розвитку й доступності технологій, складність правового регулювання через високу динамічність, гнучкість і геополітичну, культурну суперечність правових норм.

Ураховуючи визначені особливості світового інформаційного простору, управління ним овинно володіти такими властивостями, як:

1) поліцентричність, що передбачає відсутність верховної інстанції й систему розподілених суверенітетів із колективними пошуками рішень і взаєморозумінням урядів країн високого рейтингу глобалізації;

2) плюралістичність, що відповідає багатосуб'єктності, котра передбачає залучення різних учасників – урядів, міжнародних і неурядових організацій, підприємницьких структур;

3) специфічність предмета й методів, що зумовлена перетином національних інтересів і владних відносин;

4) багаторівневість, яка передбачає регулювання на локальному, національному, регіональному та глобальному рівнях;

5) інституційна інноваційність, що зумовлена динамічністю й пластичністю світового інформаційного простору та потребує трансформацій звичних інституцій і структур [4, с. 76–77].

Принципами реалізації управління світовим інформаційним простором можуть бути:

1) принцип законності, що передбачає використання механізмів та технології управління на основі чинного законодавства й нормативно-правової бази, що регулює як суспільні інформаційні відносини, так і міжнародні відносини у сфері інформаційного співробітництва;

2) принцип примату норм міжнародного права над національним законодавством, що полягає в прямому застосуванні загальновизнаних принципів і норм міжнародного права, міжнародних договорів на території конкретної країни залежно від специфіки інформаційного ресурсу, який поширюється без кордонів;

3) принцип права власності на інформацію;

4) принцип економічної доцільності систем захисту інформації, зважаючи на величину економічної шкоди й тяжкість негативних наслідків у контексті національних та глобальних інтересів;

5) принцип неупередженості оцінки реальних і потенційних загроз інформації та її обігу, стану правової й організаційної бази;

6) принцип безперервності, що передбачає постійне застосування загальних і специфічних заходів та методів регуляції, моніторингу, контролю в межах системного підходу до управління світовим інформаційним простором [1].

Правове забезпечення регулювання світового інформаційного простору включає в себе комплекс міжнародних, регіональних та національних правових актів, що визначають правила й стандарти для застосування різних аспектів інформаційних технологій та використання кіберпростору.

Серед міжнародних правових актів можна виділити Конвенцію про кіберзлочинність (Будапештська конвенція, 2001); основний міжнародний договір, який визначає стандарти для боротьби з кіберзлочинністю та сприяє міжнародному співробітництву в цій сфері; Міжнародний пакт про громадянські і політичні права (1966), у якому ст. 19 гарантує право на свободу вираження поглядів, уключаючи право на доступ до інформації через будь-які засоби масової інформації; Конвенція ООН про права дитини (1989), що забезпечує права дітей, доступ до відповідної інформації та захист від шкідливого контенту; Резолюції Генеральної Асамблеї ООН щодо інформаційної безпеки.

До регіональних правових актів можна віднести Регламент Європейського Союзу про захист персональних даних (2018), що регламентує захист персональних даних громадян ЄС і встановлює вимоги до обробки даних; Європейську конвенцію про права людини (2010), у якій ст. 10 гарантує право на свободу вираження, що включає свободу отримувати та передавати інформацію без утручання державних органів незалежно від кордонів; Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (1981), що встановлює стандарти для захисту персональних даних у країнах-учасницях.

До національних правових актів належать Закони про захист даних, що регулюють обробку персональних даних на національному рівні; Закони про кібербезпеку, котрі регулюють питання кібербезпеки, уключаючи заходи щодо захисту критичної інфраструктури та протидії кіберзлочинності. Наприклад, Закони України «Про інформацію», «Про національну безпеку України», «Про Національну програму інформатизації», Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 р. № 685/202, та Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021 [5].

Правове забезпечення регулювання світового інформаційного простору вимагає комплексного підходу, що включає міжнародні договори, національні закони, а також активну участь міжнародних організацій і співпрацю між країнами.

До чинних суб'єктів потенційного управління світовим інформаційним простором можна віднести Internet Corporation for Assigned Names and Numbers (ICANN), що відповідає за координацію системи доменних імен та IP-адрес, забезпечуючи стабільність і безпеку функціонування глобальної мережі; internet Engineering Task Force (IETF), що розробляє стандарти технічного функціонування інтернету; World Wide Web Consortium (W3C), що розробляє вебстандарти для забезпечення взаємодії й доступності вебтехнологій; ООН, яка займається питаннями глобальної політики та прав людини в інформаційному просторі; ЮНЕСКО, що працює над розвитком етичних стандартів для інформаційних і комунікаційних технологій, наприклад у межах заходів щорічної з 2019 р. ініціативи Міжнародного дня загального доступу до інформації; Раду Європи, яка просуває стандарти прав людини, демократії й верховенства права в кіберпросторі через різні ініціативи та конвенції; International Telecommunication Union (ITU), що займається питаннями інформаційних і комунікаційних технологій, уключаючи стандартизацію та регулювання; національні уряди, що розробляють і впроваджують національні стратегії та законодавство щодо інформаційної безпеки, наприклад Центр глобальної взаємодії Державного департаменту США; транснаціональні компанії, наприклад Google, Facebook, Amazon, Microsoft, мають значний вплив на інформаційний простір і розробляють власні політики з управління даними й конфіденційності; громадські організації та спільноти, наприклад East Stratcom Task Force, Global Coalition for Digital Safety, Digital Trust & Safety Partnership [6].

Регулювання світового інформаційного простору на міжнародному рівні стикається з низкою складних викликів і проблем, основні з яких уключають:

1. Юрисдикційні розбіжності. Країни мають різні закони та норми, що регулюють використання інформації й кіберпростір. Це створює складнощі в ситуаціях, коли потрібно визначити, які закони застосовувати в конкретних випадках, особливо коли дані перетинають межі держав [7]. Кожна держава має свої власні правила та стандарти, що ускладнює створення єдиного міжнародного правового поля. Так, у питаннях захисту персональних даних стандарти ЄС суворіші за стандарти інших країн.

2. Безпека даних і конфіденційність. Забезпечення безпеки даних та приватності в умовах, коли інформація легко переміщується через

кордони, є величезною проблемою, зумовленою різними законами про захист даних. Необхідним є визначення правил і стандартів для збору, зберігання та обробки великих обсягів даних. Міжнародні організації й держави повинні знаходити баланс між захистом особистих даних і вимогами національної безпеки.

3. Кіберзлочинність. Міжнародне регулювання кіберзлочинності є складним через швидкі зміни в технологіях та методах злочинів [8]. Наявні закони часто застарівають швидше, ніж устигають адаптуватися до нових викликів. Складність міжнародного співробітництва в розслідуванні та переслідуванні кіберзлочинців.

4. Культурні й політичні розбіжності. Різні культурні погляди на цензуру, свободу слова та приватність можуть впливати на міжнародні угоди щодо регулювання інформаційного простору. Прийнятність в одній культурі не гарантує того самого в іншій.

5. Розвиток технологій. Швидкий розвиток штучного інтелекту та машинне навчання створюють нові виклики для регулювання, уключаючи етичні питання й потенційні зловживання. Необхідність установлення єдиних технічних стандартів для забезпечення взаємодії між різними системами та платформами.

6. Міжнародне співробітництво. Посилення міжнародного співробітництва необхідне для ефективного регулювання інформаційного простору, але політичні та економічні інтереси часто ускладнюють процес узгодження й упровадження загальноприйнятих норм і стандартів.

7. Баланс між свободою слова та цензурою. Проблеми визначення й видалення незаконного контенту, такого як мова ненависті, екстремістські матеріали, фейкові новини. Питання відповідальності соціальних мереж й інших платформ за контент, який розміщують їхні користувачі.

8. Монополізація. Домінування великих технологічних компаній, які контролюють значну частину ринку інформаційних послуг, вимагає розробки антимонопольного регулювання міжнародного рівня.

9. Штучний інтелект. Забезпечення етичного використання штучного інтелекту, уключаючи питання прозорості, справедливості й відповідальності, як-от розробка та впровадження Китайською Народною Республікою системи розумних міст.

10. Наявність обхідних шляхів регулювання. Інформаційне поле окремої країни не бігається з державними кордонами, на які поширюється дія нормативно-правових актів, що знижує ефективність їх регулятивної спроможності. Наприклад, 16 грудня 2022 р. Комісія з надзвичайних ситуацій Республіки Молдова призупинила дію ліцензій на мовлення шести

проросійських телеканалів, проте вони все ще активні через вебплатформи й соціальні мережі.

11. Асиметричність регулятивного впливу. Держави, що мають більшу технологічну перевагу, можуть використовувати додаткові можливості для активного впливу на світовий інформаційний простір. Наприклад, Китайська Народна Республіка активно намагається впливати на світовий інформаційний простір через трансформацію контенту місцевих медіа без маркування, що джерелом є іноземний уряд, через фільтрацію доступу до новинних каналів за допомогою контролю постачання послуг кабельного телебачення в країнах Африки, через убудовані функції цензурування повідомлень у телефонах, вироблених китайською корпорацією «Хіаomi».

Наявність розробленої системи забезпечення національної та міжнародної інформаційної безпеки є основою інформаційного суверенітету держав, забезпечення її гнучкості повинно ґрунтуватися на структурній відповідності мережевій природі простору її функціонування.

Управління світовим інформаційним простором є динамічною й суперечливою сферою, перспективними напрямами подолання наявних обмежень і розв'язання проблемних аспектів можуть бути:

1. Глобальна співпраця та багатосторонні механізми. Розробка нових міжнародних угод для врегулювання кібербезпеки, захисту персональних даних і прав людини в цифровому просторі. Створення форумів та платформ для міжнародного діалогу щодо питань глобального управлінням інтернетом, залучення держав, приватного сектору й громадянського суспільства. Реалізація мережевого підходу до управління світовим інформаційним простором. Мережа є гнучкою структурою, на відміну від сформованої системи інститутів [4, с. 74].

2. Гармонізація законодавства. Узгодження законодавства різних країн для ефективного регулювання світового інформаційного простору, наприклад установлення єдиних стандартів захисту персональних даних для всіх країн.

3. Посилення кібербезпеки. Розробка та впровадження уніфікованих міжнародних стандартів кібербезпеки для захисту критичної інфраструктури й особистих даних. Створення спільних центрів реагування на кіберзагрози, які об'єднують ресурси й інформацію різних країн для оперативного реагування на глобальні кіберзагрози. Використання AI та великих даних для аналізу кіберзагроз, виявлення аномалій і покращення кібербезпеки.

4. Регулювання контенту. Розробка етичних стандартів для платформ соціальних мереж та інших онлайн-сервісів із метою забезпечення

свободи слова й запобігання поширенню дезінформації. Використання технологій штучного інтелекту та алгоритмів для автоматичної модерації контенту, поєднаних із людським контролем для забезпечення точності й справедливості [9].

5. Цифрова інклюзія. Запуск міжнародних програм із підвищення цифрової грамотності, особливо в країнах, що розвиваються, та серед вразливих груп населення. Інвестиції в розбудову інтернет-інфраструктури в регіонах з обмеженим доступом до інтернету для забезпечення однакових можливостей доступу до інформації.

6. Етичні рамки та відповідальність. Розробка й упровадження етичних кодексів для ІТ-компаній, що регулюють відповідальність за використання даних і розробку технологій. Залучення громадських організацій та спільнот до контролю за діяльністю великих технологічних компаній для забезпечення прозорості й відповідальності.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Світовий порядок демонструє разом з інформатизацією суспільства зростання значимості інформації як визначального ресурсу економічного розвитку, політичного впливу та культурної експансії. Механізми стабілізації/дестабілізації суспільства все більше визначаються діяльністю інформаційних структур і технологічним рівнем розвитку країни. Інформаційний простір стає повноцінним виміром дипломатичних, економічних, військових, культурних відносин. Глобалізація цього виміру розширює можливості розвитку всіх сфер суспільного буття та викриває нові загрози й виклики через відсутність адаптованої до особливостей світового інформаційного простору системи регулювання. Управління світовим інформаційним простором зменшує рівень невизначеності та посилює міжнародну й національну інформаційну безпеку. Можливості управління ґрунтуються на наявних правових нормах і стандартах, їх пластичності в межах загальних положень міжнародного права та національного законодавства, на ініціативах громадських організацій, експертних об’єднань, які швидше можуть реагувати на актуальні виклики; на використанні інформаційних технологій як внутрішнього механізму регулювання інформаційного простору; на впровадженні мережевого підходу з ієрархічною структурою множини управлінських груп, які взаємодіють на основі великої кількості взаємозв’язків, що відповідає логіці та темпам глобалізації. Обмеження управління світовим інформаційним простором стосуються неадаптованого до сучасних динамічних умов і неуніфікованого нормативно-правового забезпечення; відсутності

прозорості та неупередженості в міжнародних політичних відносинах через асиметричність у розподілі ресурсів і глибоку інтегрованість інформаційного простору в різні сфери суспільного буття; іррадіації наслідків управлінських заходів у регулюванні світового інформаційного простору на функціонування інших сфер суспільного буття та швидкості розвитку світової інформаційної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bortnikova, O., Kashperska, D., Leonov, O., Rubel, K., & Chumak, O. (2024). Information security of the state: motives, necessity, and sufficiency criteria. *Lex Humana,* 16, 1. URL: https://seer.ucp.br/seer/index.php/LexHumana/ article/view/2837/3686

2. Chmyr, Y., Nekryach, A., Kochybei, L., Dakal, A., & Strelbytska, L. (2023). Postindustrial Society and Global Informational Space as Infrastructure Medium and Factor for Actualization of the State Informational Security. National Security Drivers of Ukraine, 61–73. DOI:10.1007/978-3-031-33724-6_4

3. Buhaichuk, K., Warawa, W., Batrachenko, T., Cherniavska, B., & Kondel, V. (2023). Cybercrimes in the global security system in modern conditions. *Lex Humana,* 15, 2, 26–44. URL: https://seer.ucp.br/seer/index.php/ LexHumana/article/view/2474

4. Юськів, Б. (2009) Глобалізація і трудова міграція в Європі. О. М. Зень.

5. Hlobenko, S. (2023). Information space of the state and problems of ensuring its protection in Ukraine. *Scientific Herald: Public Administration,* 1 (13), 195–210. https://doi.org/10.33269/2618-0065-2023-1(13)-195-210

6. Bondar, V. (2023). Artificial intelligence as a tool of public administration in ensuring informational and psychological security. USA experience. *Journal of Scientific Perspectives,* 12 (42), 81–87. DOI:10.52058/2708-7530-2023-12(42)-80-87

7. Lahmann, H. (2020). Protecting the global information space in times of armed conflict. *International Review of the Red Cross,* 102, 915, 1227–1248. DOI:10.1017/S1816383121000400

8. Ievdokymov, V., Frikel, A., Polishchuk, V., Savchuk, S., & Klimova, I. (2024). Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. *Economic Affairs, suppl. Special Issue,* 69, 61–69. DOI:10.46852/0424-2513.1.2024.8

9. Kuzmenko, O., Cyburt, A.,Yarovenko, H., Yesh, V., & Humenna, Y. (2021). Modeling of «information bubbles » in the global information space. *Journal of International Studies,* 14, 4. https://doi.org/10.14254/2071-8330.2021/14-4/18

REFERENCES

1. Bortnikova, O., Kashperska, D., Leonov, O., Rubel, K., & Chumak, O. (2024). Information security of the state: motives, necessity, and sufficiency criteria. *Lex Humana,* 16, 1. URL: https://seer.ucp.br/seer/index.php/LexHumana/ article/view/2837/3686

2. Chmyr, Y., Nekryach, A., Kochybei, L., Dakal, A., & Strelbytska, L. (2023). Postindustrial Society and Global Informational Space as Infrastructure Medium and Factor for Actualization of the State Informational Security. *National Security Drivers of Ukraine,* 61–73. DOI:10.1007/978-3-031-33724-6_4

3. Buhaichuk, K., Warawa, W., Batrachenko, T., Cherniavska, B., & Kondel, V. (2023). Cybercrimes in the global security system in modern conditions. *Lex Humana,* 15, 2, 26–44. URL: https://seer.ucp.br/seer/index.php/ LexHumana/article/view/2474

4. Yuskiv, B. (2009) Globalization and labor migration in Europe. O. M. Zen. (in Ukrainian).

5. Hlobenko, S. (2023). Information space of the state and problems of ensuring its protection in Ukraine. *Scientific Herald: Public Administration,* 1 (13), 195–210. https://doi.org/10.33269/2618-0065-2023-1(13)-195-210.

6. Bondar, V. (2023). Artificial intelligence as a tool of public administration in ensuring informational and psychological security. USA experience. *Journal of Scientific Perspectives,*12 (42), 81–87. DOI:10.52058/2708-7530-2023-12(42)-80-87.

7. Lahmann, H. (2020). Protecting the global information space in times of armed conflict. *International Review of the Red Cross,* 102, 915,1227–1248. DOI:10.1017/S1816383121000400.

8. Ievdokymov, V., Frikel, A., Polishchuk, V., Savchuk, S., & Klimova, I. (2024). Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. *Economic Affairs, suppl. Special Issue,* 69, 61–69. DOI:10.46852/0424-2513.1.2024.8.

9. Kuzmenko, O., Cyburt, A.,Yarovenko, H., Yesh, V., & Humenna, Y. (2021). Modeling of «information bubbles» in the global information space. *Journal of International Studies,* 14, 4. https://doi.org/10.14254/2071-8330.2021/14-4/18.

Матеріал надійшов до редакції 11.03.2024 р.

УДК 327.51[(1-622)НАТО:(470+571)]

Микола Стецюк,
аспірант кафедри міжнародних відносин та суспільних комунікацій, Чернівецький національний університет імені Юрія Федьковича,
ORCID ID: 0000-0003-0704-6530,
DOI 10.29038/2524-2679-2024-01-27-38

РОЗШИРЕННЯ НАТО НА СХІД ЯК ЧИННИК ПОГІРШЕННЯ ВІДНОСИН МІЖ ЗАХОДОМ ТА РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ

2019 р. можна вважати символічним для Організації Північноатлантичного договору. З одного боку, цей довговічний військово-політичний блок