

ШТУЧНИЙ ІНТЕЛЕКТ: ІНТЕГРАЛЬНИЙ ПОГЛЯД НА НОВУ ЦИФРОВУ РЕАЛЬНІСТЬ

МОНОГРАФІЯ

Гене́за та філосо́фія ШІ:
від алгоритмічних витоків
до концепції «цифрового розуму»
та етики суб'єктності

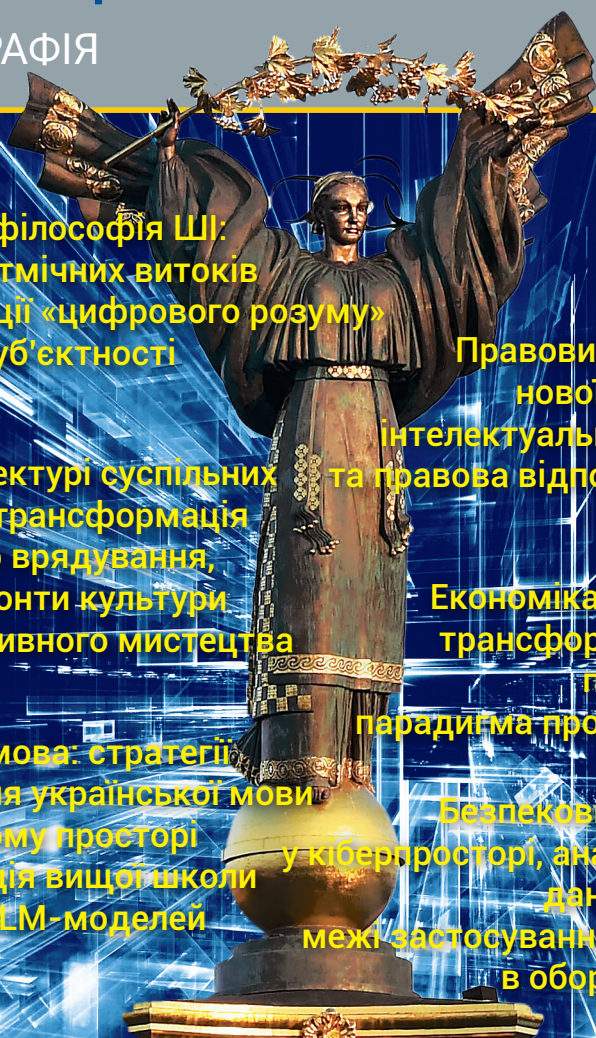
ШІ в архітектурі суспільних
відносин: трансформація
публічного врядування,
нові горизонти культури
та генеративного мистецтва

Освіта та мова: стратегії
збереження української мови
в цифровому просторі
та адаптація вищої школи
до епохи LLM-моделей

Правовий ландшафт
нової реальності:
інтелектуальна власність
та правова відповідальність
алгоритмів

Економіка алгоритмів:
трансформація ринку
праці та нова
парадигма продуктивності

Безпековий вимір: ШІ
у кіберпросторі, аналіз великих
даних та етичні
межі застосування технологій
в оборонній сфері



АНАЛІТИЧНИЙ ЦЕНТР СУЧАСНОЇ ГУМАНІТАРИСТИКИ

**ШТУЧНИЙ ІНТЕЛЕКТ:
ІНТЕГРАЛЬНИЙ ПОГЛЯД
НА НОВУ ЦИФРОВУ
РЕАЛЬНІСТЬ**

Монографія

Харків
«Право»
2026

Авторський колектив:

Л. М. Алексеєнко, доктор економічних наук, професор; С. С. Бескаравайний, кандидат філософських наук, доцент; О. В. Квасниця, кандидат економічних наук, доцент; З. О. Коваль, кандидат економічних наук, доцент; Л. Ю. Ковтунова, кандидат юридичних наук; О. В. Козут; М. А. Козловець, доктор філософських наук, професор; О. М. Кривонос, кандидат педагогічних наук, доцент; О. О. Рябуха; Г. Л. Рябцев, доктор наук з державного управління, професор; М. В. Сінельнікова, кандидат філософських наук, доцент; М. П. Требін, доктор філософських наук, професор; О. І. Тулай, доктор економічних наук, професор; Л. С. Шевченко, доктор економічних наук, професор

Рецензенти:

В. С. Бліхар – доктор філософських наук, професор (Львівський державний університет внутрішніх справ);

О. О. Дмитрик – доктор юридичних наук, професор (Національний юридичний університет імені Ярослава Мудрого);

В. Ф. Смолянюк – доктор політичних наук, професор, заслужений працівник освіти України (Військова академія імені Євгенія Березняка)

*Рекомендовано до видання вченою радою
ГО «Аналітичний центр сучасної гуманітаристики»
(протокол № 6 від 22 вересня 2026 р.)*

Штучний інтелект: інтегральний погляд на нову цифрову реальність
Ш94 : монографія / [Л. М. Алексеєнко, С. С. Бескаравайний, О. В. Квасниця та ін.] ; Аналіт. центр сучас. гуманітаристики. – Харків : Право, 2026. – 294 с. – DOI: <https://doi.org/10.31359/9786178852412>.

ISBN 978-617-8852-41-2

Колективну монографію присвячено комплексному міждисциплінарному дослідженню феномену штучного інтелекту (ШІ) як фундаментального чинника розвитку сучасної цивілізації. Проаналізовано філософські та генетичні витоки «цифрового розуму», досліджено трансформацію суспільних відносин, публічного врядування та культури під впливом генеративних технологій. Особливу увагу приділено адаптації вищої освіти до епохи LLM-моделей, а також правовому регулюванню інтелектуальної власності та відповідальності алгоритмів. Окреслено економічні наслідки впровадження ШІ на ринку праці та висвітлено безпековий вимір використання технологій у кіберпросторі та оборонній сфері.

УДК 004+14+16+32+33+34+35+37

© Алексеєнко Л. М., Бескаравайний С. С.,
Квасниця О. В. та ін., 2026

© ГО «Аналітичний центр сучасної
гуманітаристики», 2026

© ТОВ «Видавничий дім «Право», 2026

ISBN 978-617-8852-41-2

Зміст

Розділ 1

Концептуальні виміри та суспільні трансформації ІІІ: від філософських витоків до нових реалій врядування й культури

1.1. Чотири базові проблеми осмислення загального штучного інтелекту (<i>Бескаравайний С. С.</i>).....	5
Список використаних джерел.....	29
1.2. Штучний інтелект і трансформація цифрового врядування: від електронних послуг до інтелектуальної держави (<i>Рябуха О. О., Рябцев Г. Л.</i>).....	31
Список використаних джерел.....	59
1.3. Чи впорається культура з викликами сучасної технологічної епохи? (<i>Сінельнікова М. В.</i>).....	61
Список використаних джерел.....	72

Розділ 2

Штучний інтелект у просторі освіти і права: трансформація пізнання та регулювання цифрових активів

2.1. Генеративний штучний інтелект і трансформація суб'єкта пізнання в цифровій освіті (<i>Козловець М. А., Кривонос О. М.</i>).....	76
Список використаних джерел.....	100
2.2. Цифрова трансформація авторського права: соціально-філософські виміри доступності інформації (<i>Когут О. В.</i>).....	107
Список використаних джерел.....	133
2.3. Синтетичні зображення спортсменів: охороноздатність та ризики порушення прав інтелектуальної власності за законодавством України (<i>Ковтунова Л. Ю.</i>).....	138
Список використаних джерел.....	154

Розділ 3

Економіка алгоритмів: трансформація ринку праці та нова парадигма продуктивності

3.1. Економіка штучного інтелекту: бізнес і конкуренція (<i>Шевченко Л. С.</i>).....	156
Список використаних джерел.....	178
3.2. Алгоритмізація економіки як детермінанта трансформації адаптивних стратегій розвитку підприємств (<i>Коваль З. О.</i>).....	182
Список використаних джерел.....	195

3.3. Управління персональними фінансами територіально-господарських систем: поведінкові детермінанти та інформаційно-комунікаційне забезпечення євроінтеграційної згуртованості (Квасниця О. В.).....	197
Список використаних джерел.	210

Розділ 4

Безпековий вимір: ІІІ в кіберпросторі, аналіз великих даних та етичні межі застосування технологій в оборонній сфері

4.1. Міжнародна інтеграція та національні параметри безпекового простору: від бізнес-комунікацій до багаторівневого трансферу оборонних технологій в умовах нової цифрової реальності (Тулай О. І., Алексєєнко Л. М.).	216
Список використаних джерел.	231
4.2. Онтологічна трансформація дипломатії в алгоритмічному середовищі: від «розумної сили» до дипломатії даних (Требін М. П.).	238
Список використаних джерел.	261
4.3. Трансформаційні вектори розвитку інституту кібердипломатії в умовах експансії технологій штучного інтелекту (Требін М. П.).	264
Список використаних джерел.	287
Авторський колектив	292

31. Riordan S. Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. *USC Center on Public Diplomacy*. May 12, 2016. URL: <https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction>.
32. Riordan S. *Cyberdiplomacy: Managing Security and Governance Online*. Cambridge: Polity Press, 2019. ix, 134 p.
33. Seib P. *Real-time diplomacy: politics and power in the social media era*. New York: Palgrave Macmillan, 2012. 199 p.
34. Virilio P. *Speed and politics* / translated by Mark Polizzotti. Los Angeles, CA: Semiotext(e), 2006. 174 p.
35. Westcott N. *Digital Diplomacy: The Impact of the Internet on International Relations*. *Oxford Internet Institute. Research Report 16*. July 2008. 20 p. URL: <https://www.oii.ox.ac.uk/wp-content/uploads/old-docs/RR16.pdf>.

4.3. Трансформаційні вектори розвитку інституту кібердипломатії в умовах експансії технологій штучного інтелекту

Требін Михайло Петрович

доктор філософських наук, професор

професор кафедри міжнародних відносин і політичної філософії

Харківський національний економічний університет імені Семена Кузнеця

Дипломатія як фундаментальний інститут міжнародної політики та ключовий механізм урегулювання міждержавних відносин традиційно відзначається високою адаптивністю, а її еволюція є безпосереднім відображенням технологічного розвитку людської цивілізації. Кожна глобальна технологічна революція – від винайдення телеграфу та радіо до розбудови інтернету – не лише змінювала швидкість та канали комунікації між суверенами, а й вимагала докорінного переосмислення сутності дипломатичної практики. Протягом останніх десятиліть стрімка дифузія та експансія інформаційно-комунікаційних технологій (ІКТ) в усі сфери суспільно-політичного життя створили безпрецедентні виклики перед зовнішньополітичними відомствами

країн світу¹. Це змусило міністерства закордонних справ та міжнародні організації кардинально переглянути свої класичні підходи до ведення переговорів, збору інформації та реалізації національних інтересів, що зумовило появу та концептуалізацію таких новітніх феноменів, як технологічна, інноваційна та цифрова дипломатія².

Проте справжнім тектонічним зсувом для сучасного світового порядку, архітектури глобальної безпеки та безпосередньо інституту

¹ Див.: Верховцева І. Г., Шестаков В. І., Гребенюк В. М., Гайдук О. В. Новітня термінологія у дипломатичних практиках як маркер кібервпливів: цифрова дипломатія, кібердипломатія. *Публічне адміністрування та національна безпека*. 2025. № 5. С. 15–22; Кібердипломатія: матеріали Міжнародної науково-практичної конференції (м. Київ, 15–16 травня 2024 року), Науково-практичного круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року) / за заг. ред. чл.-кор. НАН України, доктора техн. наук, професора О. Г. Корченка; упорядники: І. Г. Верховцева, О. В. Гайдук. Київ: Дипломатична академія імені Геннадія Удовенка; Державний університет інформаційно-комунікаційних технологій, 2025. 132 с.; Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. *Україна дипломатична*. 2023. Вип. 24. С. 696–708; Поляков О. М. Кібердипломатія як важливий напрямок міжнародно-правового співробітництва в умовах режиму воєнного стану. *Нове українське право*. 2024. Вип. 6. С. 70–76; Цифрова дипломатія України: стратегічні комунікації, аналіз даних, кризове управління: матеріали міжнародної наукової конференції. Львів, 14 листопада 2025 р. / Упорядники: М. Мальський, Р. Вовк, О. Кучик. Львів: Львівський національний університет імені Івана Франка, 2025. 120 с.

² Див.: Банчук-Петросова О., Сулим Б. Цифрова дипломатія: вплив штучного інтелекту та великих даних на трансформацію дипломатичної практики. *Empirio*. 2026. Т. 3, № 1. С. 49–58; Кононенко В. П., Комарова Т. Г. Цифрова дипломатія як засіб стратегічної комунікації держави. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Питання політології*. 2024. Вип. 45. С. 15–20; Кузь О. М., Требін М. П. Дипломатія цифрової епохи. *Україна в часи випробувань: соціальні, культурні та політичні трансформації*: матеріали Всеукр. наук.-практ. конф. (ХЛІ Харків. політол. читання), м. Харків, 30 січ. 2026 р.) / [редкол.: Куц Г. М. (голова), Панфілов О. Ю., Погрібна В. Л. та ін.]; Аналіт. центр сучас. гуманітаристики; Харків. асоц. політологів. Харків: Право, 2026. С. 25–32; Піпченко Н. О., Макаренко С. А., Рижков М. М. Цифрова дипломатія: підруч. для студентів закл. вищ. освіти, які навчаються за спец. «Міжнародні відносини, суспільні комунікації та регіональні студії» / Київ. нац. ун-т ім. Тараса Шевченка. Київ: ВАДЕКС, 2019. 317 с.; Озернюк Г. Цифрова дипломатія та дипломатія даних: історичні передумови й концептуальні відмінності. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2025. № 2. С. 121–135; Яковюк І. В., Цвельні М. П. Цифрова дипломатія: впровадження електронних візових послуг в Україні. *Право та інновації*. 2022. № 3. С. 69–76.

дипломатії став стрімкий розвиток і комерціалізація технологій штучного інтелекту (ІІІ) та великих мовних моделей (LLM). Поява генеративного ІІІ ознаменувала перехід від кількісних змін у сфері обробки даних до якісних трансформацій у сфері стратегічної комунікації, прийняття рішень та формування смислового простору. За таких умов традиційні дипломатичні інструменти виявилися недостатньо ефективними, що актуалізує потребу в глибокій теоретичній рефлексії та практичному переформатуванні кібердипломатії як відносно нового, але вже критично важливого напрямку зовнішньополітичної діяльності¹.

Попри ранню появу терміна «кібердипломатія», у науковому обігу протягом майже двох десятиліть панувала еклектика. Поняття «цифрова дипломатія» (digital diplomacy)², «кібердипломатія» (cyber diplomacy)³, «мережева дипломатія» (network diplomacy)⁴ та «електро-

¹ Див.: Attatfa A., Renaud K., De Paoli S. Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*. 2020. Vol. 176. P. 60–69; Kuz O., Nepchatov D. Cyber Diplomacy as an Instrument of Cognitive Warfare in Cyberspace. *Actual Problems of International Relations*. 2026. Vol. 1, No. 167. P. 53–60. DOI: <https://doi.org/10.17721/apmv.2026.167.1.53–60>; Riordan S. Cyberdiplomacy: Managing Security and Governance Online. Cambridge: Polity Press, 2019. ix, 134 p.

² Див.: Степанов В. Ю., Бричук К. Г. Цифрова дипломатія як інструмент масової комунікації в публічному управлінні. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління*. 2020. № 3. С. 5–10; Чепелюк Ю. В. Цифрова дипломатія в контексті сучасних інформаційних комунікацій. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2021. Т. 4, № 2. С. 250–258; Lewis D. Digital diplomacy. *Gateway House*. December 19, 2014. URL: <http://www.gatewayhouse.in/digital-diplomacy-2>; Westcott N. Digital Diplomacy: The Impact of the Internet on International Relations. *Oxford Internet Institute. Research Report 16*. July 2008. 20 p. URL: <https://www.oii.ox.ac.uk/wp-content/uploads/old-docs/RR16.pdf>.

³ Див.: Barrinha A. Cyber-diplomacy: The Emergence of a Transient Field. *The Hague Journal of Diplomacy*. 2024. Vol. 19, Issue 3. P. 439–466. DOI: <https://doi.org/10.1163/1871191x-bja10183>; Kļaviņš D. Cyber Diplomacy. Latvia's Voice in the World. *Cybersecurity in Latvia: forging resilience amidst emerging threats* / edited by Mihails Potapovs and Kate E. Kanasta. London: Routledge, 2025. P. 150–174. URL: <https://www.taylorfrancis.com/reader/download/230471d2-6454-4606-abd5-9a376ac2f159/chapter/pdf?context=ubx>.

⁴ Див.: Metzl J. F. Network Diplomacy. *Georgetown Journal of International Affairs*. 2001. Vol. 2, No. 1. P. 77–87; Poda T. A. The development of “network diplomacy” as a new form of international interaction. *Вісник НАУ. Серія: Філософія. Культурологія*. 2020. № 1 (31). С. 84–88.

нна дипломатія» (e-diplomacy)¹ часто використовувалися як абсолютні синоніми. Свідченням цього є наукові праці початку XXI століття. Зокрема, відома колективна монографія «Кібердипломатія: управління зовнішньою політикою у XXI столітті»², яка вийшла 2002 року за редакцією Евана Поттера, попри свою назву, присвячена переважно процесам цифровізації дипломатичної служби. Автори дослідження зосереджували увагу на використанні МЗС перших вебсайтів, електронної пошти та інформаційних баз даних для оптимізації консульської діяльності та публічної промоції держави за кордоном. Тобто змістовне наповнення цієї наукової праці стосувалося того, що сьогодні класифікують як цифрову дипломатію, тоді як специфіка кіберпростору як нового середовища міжнародного суперництва та нормативного регулювання залишалася поза увагою.

Критично важливий крок для подолання цієї термінологічної конвергенції та виокремлення кібердипломатії в самостійну субдисципліну зробив відомий британський дипломат і теоретик міжнародних відносин Шон Ріордан. 2016 року в аналітичній статті «Кібердипломатія проти цифрової дипломатії: термінологічне розмежування»³ він вперше чітко артикулював сутність методологічної помилки, яка виникає через взаємозамінне вживання цих дефініцій. Ріордан наголосив, що змішування інструменту та предмета регулювання призводить до серйозних непорозумінь як у теоретичних дослідженнях, так і під час практичного формування зовнішньополітичних стратегій країн.

З метою делімітації цих понять Ріордан запропонував елегантну та логічну матрицю розмежування, яку він згодом, 2019 року, закріпив і детально розгорнув у фундаментальній монографії «Кібердиплома-

¹ Див.: Hanson F. Baked in and wired: eDiplomacy@State. *Foreign Policy at Brookings*. URL: <https://www.brookings.edu/wp-content/uploads/2016/06/baked-in-hansonf-5.pdf>; Hanson F. *Revolution @State: The spread of ediplomacy*. Sydney: Lowy Institute for International Policy, 2012. 34 p. URL: https://www.brookings.edu/wp-content/uploads/2016/06/03_ediplomacy_hanson.pdf.

² Див.: *Cyber-diplomacy: managing foreign policy in the twenty-first century* / edited by Evan H. Potter. Montreal: McGill-Queen's University Press, 2002. xii, 208 p.

³ Див.: Riordan S. *Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction*. *USC Center on Public Diplomacy*. May 12, 2016. URL: <https://usepublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction>.

тія: управління безпекою та врядуванням в онлайн-просторі». Дослідник сформулював класичну максиму: «Цифрова дипломатія – це застосування цифрових інструментів у дипломатії, тоді як кібердипломатія – це застосування дипломатичних методів до кіберпростору»¹. За такою логікою, цифрова дипломатія є інструментальною: вона досліджує, як соціальні мережі, алгоритми оптимізації контенту чи мобільні застосунки допомагають дипломату виконувати його традиційні функції (наприклад, інформування громадськості, проведення публічних роз'яснювальних кампаній або надання консульських послуг).

Натомість кібердипломатія має сутнісний, предметний характер. Вона визначається як стратегічна зовнішньополітична діяльність, спрямована на регулювання відносин між державами безпосередньо в цифровому середовищі, унормування відповідальної поведінки акторів, формування архітектури глобальної кібербезпеки та врегулювання міждержавних конфліктів, що виникають у мережі. Предметом кібердипломатії є не спосіб надсилання дипломатичних депеш, а глобальне управління інтернетом, захист критичної інфраструктури від транскордонних атак, нерозповсюдження кіберзброї та вироблення міжнародно-правових режимів контролю за віртуальним простором.

Розвиток генеративного штучного інтелекту та великих мовних моделей вносить радикальні корективи в цю класичну дихотомію, трансформуючи не лише безпосередній предмет міжнародного регулювання, а й саму внутрішню архітектуру та логіку функціонування дипломатичних інституцій. В епоху, коли алгоритми здатні самостійно генерувати смисли, тексти та стратегічні сценарії, традиційна модель міністерства закордонних справ як класичного «брамника» (gatekeeper) остаточно відходить у минуле. Протягом століть МЗС мало монополію на представництво держави на міжнародній арені, повністю контролюючи та фільтруючи інформаційні потоки, спрямовані зсередини країни назовні та у зворотному напрямку. Бюрократична ієрархія, закриті канали зв'язку та сувора протокольність забезпечували державі можливість бути єдиним та монолітним голосом у світовій політиці.

¹ Riordan S. Cyberdiplomacy: Managing Security and Governance Online. P. 5.

Сьогодні, під тиском глобальних технологічних гігантів (BigTech) та внаслідок дифузії технологій ІІІ, модель «брамника» виявляється нежиттєздатною та стрімко поступається місцем новітній моделі «поєднувача» або «медіатора меж» (boundary spanner). У цих нових реаліях дипломатичні відомства перетворюються на гнучкі, мережеві координаційні центри, що функціонують на динамічному стику внутрішньої та зовнішньої політики. Головною функцією МЗС стає не ізоляція внутрішнього простору, а спроможність ефективно об'єднувати навколо себе різномірних акторів для захисту національних інтересів в алгоритмічному середовищі.

Кібердипломатія в епоху ІІІ вимагає постійної синергії та побудови стійких міжвідомчих та транснаціональних коаліцій. Дипломати змушені інтегрувати у свою діяльність експертизу військових відомств (для розуміння сутності кібероперацій), розвідувальних структур (для верифікації джерел алгоритмічних загроз), академічної спільноти (для відстеження трендів розвитку ІІІ), громадянського суспільства (для захисту прав людини в цифрову епоху) та, що найважливіше, приватних технологічних корпорацій. Оскільки саме корпорації Microsoft, Google, OpenAI, Meta та інші мають обчислювальні потужності, коди та дата-центри, вони стають повноцінними суб'єктами міжнародних відносин. Кібердипломат нового покоління має виступати медіатором, який перекладає технічну мову алгоритмів на мову міжнародних договорів, поєднуючи державний суверенітет із корпоративними технологічними можливостями для протидії новітнім гібридним загрозам.

Становлення та первинне інституційне оформлення класичної кібердипломатії відбувалося під безпосереднім впливом масштабних і резонансних кібератак початку ХХІ століття, які наочно продемонстрували вразливість суверенних держав перед транскордонними цифровими загрозами. Хрестоматійним прикладом, що змусив світову спільноту та зовнішні відомства переглянути національні воєнні та дипломатичні доктрини, стали скоординовані та масовані удари по цифровій інфраструктурі Естонії у 2007 році¹. Ці атаки, які забло-

¹ Див.: Attatfa A., Renaud K., De Paoli S. Cyber Diplomacy: A Systematic Literature Review. P. 60.

кували роботу урядових вебсайтів, банківських установ, засобів масової інформації та систем зв'язку, чітко маркували появу нового виміру міждержавного протистояння. Проте на тому етапі розвитку технологій загрози мали виражений технічний і деструктивний характер. Основними інструментами зловмисних акторів були різноманітні модифікації шкідливого програмного забезпечення (malware), віруси-вимагачі (ransomware) та розподілені атаки на відмову в обслуговуванні (DDoS-атаки), спрямовані на виведення з ладу фізичних серверів, комунікаційних вузлів та баз даних.

Захист об'єктів критичної інформаційної інфраструктури (КІІ), розробка протоколів швидкого реагування на технічні інциденти та створення систем резервного копіювання даних залишаються фундаментальними завданнями національної безпеки й сьогодні. Проте стрімка експансія та комерціалізація технологій штучного інтелекту кардинально й безповоротно трансформували саму онтологічну природу цих загроз. Сучасна кібердипломатія змушена долати межі традиційного захисту фізичного чи мережевого периметра та переходити в якісно нову площину – управління когнітивною безпекою суспільства та регулювання алгоритмічного простору. Якщо в попередні десятиліття держави змагалися переважно за контроль над матеріальними компонентами мережі – серверами, трансокеанськими магістральними кабелями та реєстрами доменних імен, – то сьогодні головним полем геополітичної битви стає смисловий простір¹. У ньому ключовою зброєю стають не просто шкідливі коди, що руйнують залізо, а генеративний ШІ, високореалістичні дипфейки та повністю автоматизовані дезінформаційні системи, здатні деформувати суспільне сприйняття реальності.

Глибокий аналіз цієї трансформації подано в офіційних документах Агентства Європейського Союзу з кібербезпеки (ENISA). Згідно з останніми аналітичними звітами відомства, зокрема фундаментальними оглядами ENISA Threat Landscape 2025² та ENISA Threat

¹ Див.: Інформаційна війна та її вплив на суспільство: монографія / [Л. М. Алексєнко, О. М. Іванченко, У. В. Ільницька та ін.]; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2026. С. 86.

² Див.: ENISA threat landscape 2025. *European Union Agency for Cybersecurity (ENISA)*. October 2025. 86 p. DOI: 10.2824/1946374.

Landscape 2026¹, інтеграція генеративного ШІ в арсенал ворожих акторів дозволила автоматизувати та масштабувати шкідливу діяльність до промислових, конвеєрних обсягів. Узагальнюючи емпіричні дані, ENISA окремо наголошує на важливому методологічному аспекті: головна небезпека сучасного ШІ полягає не стільки у створенні принципово нових, небачених раніше типів кібератак, скільки в колосальному посиленні, модернізації та оптимізації вже наявних кримінальних і маніпулятивних технік за рахунок швидкості, гнучкості та масштабів їх розгортання. Для опису цього феномену європейське агентство використовує концептуальний термін «посилення спроможностей» (uplift), зазначаючи, що ШІ радикально знижує поріг входження (barriers to entry) для недержавних зловмисників і хакерських угруповань, які не мають глибоких технічних знань, але тепер отримують можливість автоматизувати конструювання складного шкідливого коду та генерацію бездоганного з лінгвістичного погляду фішингу².

Особливу увагу в контексті викликів для кібердипломатії привертають розділи звітів ENISA, присвячені інформаційним маніпуляціям та іноземній інтерференції (Information Manipulation and Interference). Експерти агентства б'ють на сполох через небезпеку активного використання великих мовних моделей (LLM) спеціалізованими зловмисними групами, які в кодифікації ENISA отримали назву IMS (Information Manipulation Sets). Ці організовані групи спроможні використовувати кастомізовані алгоритми для миттєвої генерації мільйонів унікальних, неповторюваних пропагандистських і дезінформаційних текстів. Більше того, ці тексти динамічно адаптуються під специфічний психологічний і соціокультурний профіль конкретних цільових аудиторій, що вкрай ускладнює роботу традиційних систем кіберзахисту та виявлення так званих «фабрик контенту» чи бот-мереж.

¹ Див.: ENISA threat landscape 2026. *European Union Agency for Cybersecurity (ENISA)*. September 2026. 101 p. DOI: 10.2824/0806036.

² Див.: ENISA's 2026 report identifies ransomware, vulnerability exploitation and AI-enabled attacks as leading EU cyber threats. *Civil Society Alliances for Digital Empowerment (CADE)*. September 23, 2026. URL: <https://cadeproject.org/updates/enisas-2026-report-identifies-ransomware-vulnerability-exploitation-and-ai-enabled-attacks-as-leading-eu-cyber-threats/>.

Агентство детально описує механіку того, як генеративний ІІІ дозволяє створювати так звані кампанії за індивідуальними лекалами, дефінуючи їх як таргетований персоналізований фішинг та високо-точну дезінформацію. За оцінками ENISA, інтеграція ІІІ в процеси соціальної інженерії (social engineering) набула такого масового характеру, що ІІІ-супроводжувані кампанії на сьогодні складають понад 80% від усієї світової активності цього типу¹. Це свідчить про те, що кіберзагрози остаточно перетворилися із суто технічних інцидентів на когнітивні операції, де об'єктом атаки є свідомість громадян, їхня довіра до державних інститутів та електоральні процеси в демократичних країнах.

Ситуація додатково загострюється через появу та вихід на тіньовий ринок спеціалізованих, зловмисних автономних систем ІІІ. Зокрема, у найновіших аналітичних оглядах ENISA офіційно попереджає про комерціалізацію та активне використання ворожими суб'єктами таких систем, як Xanthorox AI, що були цілеспрямовано створені суто для автоматизації розробки кіберзброї, генерації поліморфних вірусів та проведення масштабних скоординованих атак без участі людини². Подібні інструменти дозволяють зловмисникам здійснювати безперервний автоматизований пошук уразливостей у державних реєстрах та мережах МЗС. Водночас штучно згенеровані аудіо- та відеоматеріали (дипфейки) з лідерами держав, виконані на бездоганному технологічному рівні, стають здатними сфабрикувати масштабний дипломатичний скандал, обвалити фінансові ринки чи спровокувати паніку всередині країни за лічені хвилини. За таких умов ключовим завданням сучасної кібердипломатії стає не просто технічна протидія, а розробка та впровадження жорстких міжнародних механізмів швидкої верифікації контенту, взаємного сповіщення та юридично вивіреної атрибуції подібних складних атак.

Яскравим і водночас трагічним прикладом цієї глобальної трансформації є повномасштабна війна Росії проти України. Саме на тере-

¹ Див.: ENISA threat landscape 2025. Р. 6.

² Див.: ENISA releases 2025 Threat Landscape report on Europe's cybersecurity challenges. *CyberHubs*. October 15, 2025. URL: <https://cyberhubs.eu/enisa-releases-2025-threat-landscape-report-on-europes-cybersecurity-challenges/>.

нах України виник перший в історії прецедент тотальної гібридної війни, де складні кібероперації та інформаційно-психологічні атаки за допомогою генеративного ШІ стали невіддільною, глибоко інтегрованою частиною загальної воєнної стратегії держави-агресора¹. Російські гібридні загрози вже давно не обмежуються лінією фронту чи виключно українським цифровим простором – вони системно спрямовані на дестабілізацію всього європейського та трансатлантичного простору. Використовуючи ШІ для генерації дипфейків, створення фейкових новинних агенцій та автоматизованого поширення панічних наративів, агресор намагається спровокувати розкол у європейських суспільствах, підірвати солідарність союзників та дискредитувати концепцію допомоги Україні.

Досвід цієї війни наочно довів усій міжнародній спільноті, що кібербезпека в епоху ШІ більше не може розглядатися як суто технічна чи вузькоспеціалізована проблема ІТ-департаментів. Сьогодні це питання фундаментального виживання демократичних інститутів, збереження суверенітету та захисту конституційного ладу, яке вимагає жорсткої, скоординованої та проактивної дипломатичної відсічі на найвищому міжнародному рівні². Кібердипломатія, таким чином, еволюціонує від класичного інструменту «м'якої сили» (Soft Power) до критично важливого інструменту стратегічного стримування, протидії алгоритмічному тиску та захисту національного когнітивного суверенітету.

Експансія технологій штучного інтелекту не лише трансформувала ландшафт безпекових загроз, а й спричинила кардинальну реконфігурацію класичних інструментів геополітичного впливу, суттєво змінивши архітектуру «м'якої сили» (Soft Power) у міжнародних відносинах. Традиційно, у межах концепції, сформульованої американським політологом Джозефом Наєм, «м'яка сила» розглядалася як здатність держави отримувати бажані результати через привабливість

¹ Див.: Требін М. П. Феномен «гібридної» війни. *Гілея*. 2014. Вип. 87 (8). С. 366–371.

² Див.: Руднєва А. О., Мальована Ю. Г. Цифрова дипломатія у формуванні системи національної безпеки України в умовах війни з РФ. *Регіональні студії*. 2023. №34. С. 111–115.

власної культури, суспільно-політичних цінностей та легітимність зовнішньої політики, на противагу «жорсткій сили» (Hard Power) військового чи економічного примусу¹. Проте в епоху домінування великих мовних моделей та алгоритмічних систем управління інформацією престиж, авторитет і реальний вплив суверенного актора на світовій арені починають безпосередньо вимірюватися рівнем його технологічного лідерства, обчислювальними потужностями та спроможністю контролювати цифрову екосистему.

У сучасних реаліях штучний інтелект перетворився на ключовий чинник та інструмент реалізації оновленої «м'якої сили», де домінування забезпечується не стільки кінематографом чи гуманітарними програмами, скільки монополією на алгоритми генерації знань. Держави, які володіють передовими ШІ-моделями та суперкомп'ютерною інфраструктурою (насамперед Сполучені Штати Америки та Китайська Народна Республіка), отримують безпрецедентні важелі алгоритмічного впливу на глобальному рівні.

Критично важливим для розуміння сутності кібердипломатії є усвідомлення того, що великі мовні моделі (LLM) за своєю онтологічною природою не є й не можуть бути нейтральними чи об'єктивними посередниками. Будь-яка складна нейромережа створюється конкретними групами розробників і навчається на колосальних масивах текстових і візуальних даних, які неминуче відображають специфічні політичні погляди, культурні коди, ідеологічні установки та етичні норми країн їхнього походження. Як наслідок, ШІ-платформи стають ретрансляторами певних світоглядних парадигм.

За таких умов для міжнародної спільноти виникає реальний ризик «алгоритмічної колонізації», теоретиком якої є дослідник цифрового неокolonіалізму А. Бірхане². Держави, які не мають власних технологічних альтернатив, достатніх обчислювальних ресурсів чи національних аналогів LLM, змушені повністю імпортувати й інтегрувати іноземні ШІ-платформи в усі сфери свого функціонування. Штучні

¹ Див.: Nye J. S., Jr. Get Smart: Combining Hard and Soft Power. *Foreign Affairs*. 2009. Vol. 88, No. 4. P. 160–163. URL: <http://www.jstor.org/stable/20699631>.

² Див.: Birhane A. Algorithmic Colonization of Africa. *SCRIPTed*. 2020. Vol. 17, Issue 2. P. 389–409. DOI: 10.2966/scrip.170220.389.

інтелектуальні асистенти, пошукові системи нового покоління та автоматизовані освітні платформи, глибоко вкорінюючись у національні медіа, систему освіти, державне управління та бізнес інших країн, починають непомітно, але системно й пролонговано формувати світогляд і ціннісні орієнтири їхніх громадян. Цей процес відбувається через м'яку фільтрацію контенту, пріоритезацію певних інтерпретацій історичних подій чи політичних процесів відповідно до наративів, закладених розробниками базових моделей. Таким чином, алгоритмічна колонізація стає витонченою формою домінування, що руйнує когнітивний суверенітет держав без застосування класичних методів тиску¹.

Водночас цифрова епоха та експансія ШІ створюють унікальні вікна можливостей для переформатування традиційної ієрархії міжнародних відносин, де тривалий час домінував концепт фізичного масштабу держави. У сучасному кіберпросторі чітко проявляється феномен так званого нормативного підприємництва (погм entrepreneurship). Відома німецька дослідниця, політологиня та визнана європейська експертка у сферах кібербезпеки й протидії гібридним загрозам Мадлен Маятт у фундаментальній праці «Малі, розумні, потужні? Малі держави та конкуренція за перевагу в галузі кібертехнологій у цифрову епоху» слушно підкреслює: «Важливим елементом кіберсили є здатність впливати на норми та регулювання в кіберпросторі та формувати їх»².

У колі науковців М. Маятт здобула широке визнання саме завдяки детальному та глибокому дослідженню концепту кіберсили (cyber power) в контексті зовнішньої політики малих і середніх держав. Вона чи не першою детально й переконливо обґрунтувала, що невеликі країни не приречені бути беззахисними жертвами чи пасивними об'єктами маніпуляцій у цифрову епоху. За її концепцією, дефіцит фізичного масштабу, геополітичної ваги, території чи чисельності

¹ Див.: Bee D. Cognitive Sovereignty in Algorithmic Societies: A Methodological Framework for Reclaiming Human Agency. *Meaningfulness Media Group Technical Report No. 3*. 2026. 32 p. URL: <https://philarchive.org/archive/BEECSI>.

² Myatt M. Small, Smart, Powerful? Small States and the Competition for Cybertech Superiority in the Digital Age. *Competition in World Politics: Knowledge, Strategies and Institutions* / Daniela Russ, James Stafford (eds.). Bielefeld: Transcript, 2021. P. 252.

збройних сил може бути успішно компенсований за рахунок високої швидкості внутрішньої цифровізації, гнучкості державних інституцій та мобілізації інтелектуального капіталу.

Малі держави здатні успішно захищати свій суверенітет і навіть проєктувати вплив назовні через інструменти «нормативного підприємництва». Цей феномен полягає в активному, ініціативному просуванні та нав'язуванні міжнародній спільноті власних правил гри, концептуальних підходів, розробці інноваційних санкційних інструментів та стандартів безпеки штучного інтелекту. Яскравим практичним прикладом реалізації цієї стратегії є зовнішньополітична діяльність країн Балтії (Данії, Естонії, Латвії). Естонія, яка пережила згадані атаки 2007 року, трансформувала свій травматичний досвід у потужну міжнародну суб'єктність, ставши штаб-квартирою Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) та ключовим розробником Талліннського посібника з міжнародного права, що застосовується до кібероперацій (перше видання під керівництвом професора М. Шмітта надруковане 2013 року)¹. Еволюція цього документу від аналізу суто воєнних атак до масштабного розширення у версії *Tallinn Manual 2.0* (2017 р.)² і врешті – до редакції *Tallinn Manual 3.0* 2026 року, яка безпосередньо враховує виклики ІІІ-супроводжуваних операцій, наочно демонструє, як малі держави здатні формувати глобальний правовий порядок денний цифровізації.

Отже, сьогодні малі та середні технологічно розвинені держави наочно доводять, що в умовах експансії ІІІ брак традиційних геополітичних атрибутів компенсується перевагою в швидкості й адаптивності. Створюючи надзвичайно ефективні, стійкі внутрішні системи кіберзахисту та цифрового врядування і водночас проактивно

¹ Див.: Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence / general editor Michael N. Schmitt. Cambridge; New York: Cambridge University Press, 2013. xix, 282 p.

² Див.: Tallinn manual 2.0 on the international law applicable to cyber operations / prepared by the International Groups of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence; general editor Michael N. Schmitt; managing editor Liis Vihul. Cambridge; New York: Cambridge University Press, 2017. xli, 598 p.

виступаючи на міжнародних майданчиках, такі країни перетворюються на визнаних архітекторів глобальних стандартів кібербезпеки та етичного регулювання алгоритмічних систем. Кібердипломатія малих держав, яка спирається на нормативне підприємництво, стає дієвою протипагою як прямим гібридним загрозам з боку агресивних авторитарних режимів, так і ризикам алгоритмічної колонізації з боку глобальних технологічних монополій.

Російсько-українська війна, яка набула характеру першого у ХХІ столітті повномасштабного міждержавного конфлікту високої інтенсивності, стала водночас переломним моментом для розвитку сучасної кібердипломатії та переоцінки сутності національної безпеки в епоху алгоритмизації¹. На прикладі цього протистояння світова спільнота отримала безпрецедентний емпіричний досвід, який наочно продемонстрував, що кібератаки та когнітивні операції із залученням генеративного штучного інтелекту більше не є ізольованими чи допоміжними актами, а становлять інтегральну складову єдиної, скоординованої воєнної стратегії держави-агресора². Російська Федерація перетворила свій кібернетичний та інформаційний потенціал на цифрову зброю масового ураження, спрямовану на руйнування критичної інфраструктури України та системний підрив стійкості її західних союзників.

Російські гібридні загрози відзначаються комплексним, синергетичним характером, специфікою якого є повна нівеляція межі між віртуальним і фізичним просторами. Протягом війни ворожі актори продемонстрували здатність синхронізувати кінетичні удари (ракетні обстріли та атаки дронів) із масованими кібератаками на об'єкти енергетики, логістичні центри, державні реєстри та системи зв'язку України. Проте найбільш небезпечним вектором цієї гібридної експансії став вихід агресора у сферу когнітивної війни за допомогою

¹ Див.: Війна як модус соціального буття в міждисциплінарному науковому дискурсі: монографія / [Л. М. Алексеєнко, Ю. Г. Борейко, А. О. Бояр та ін.]; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2026. 338 с. DOI: <https://doi.org/10.31359/9786178759926>.

² Див.: Требин М. Российско-украинская война: динамика технического, организационного и человеческого измерений. *Историческая экспертиза*. 2025. №3 (44). С. 113–140.

ШІ-технологій¹. Використання великих мовних моделей дозволило ворожим інституціям дезінформації перейти до промислового виробництва персоналізованого контенту, адаптованого під політичні вразливості різних європейських країн. Завдяки автоматизованій генерації дипфейків, фальсифікації новинних ресурсів провідних світових медіа та використанню бот-мереж нового покоління, керованих ШІ, Росія здійснює перманентні спроби дестабілізувати внутрішньополітичну ситуацію в країнах ЄС та НАТО. Головною метою цих операцій є штучне поширення паніки, радикалізація суспільних настроїв, дискредитація демократичних інститутів та системний підрив солідарності трансатлантичних партнерів з Україною.

Досвід України у протистоянні цій агресії став фундаментальним уроком для глобальної архітектури безпеки, довівши, що цифрова стійкість є базовою умовою виживання сучасної суверенної держави. Українська кібердипломатія в цих екстремальних умовах змушена була діяти проактивно, формуючи нові прецеденти міжнародної взаємодії. Вона продемонструвала, що захист від алгоритмічного тиску вимагає негайної відмови від застарілих, неповоротких бюрократичних шаблонів класичної дипломатичної служби та переходу до динамічних моделей міжвідомчої та державно-приватної співпраці. Україна довела життєздатність концепту «медіатора меж» (boundary spanner) на практиці, сформувавши стратегічні альянси з провідними світовими технологічними корпораціями (зокрема Microsoft, Amazon, Google, Palantir)², які забезпечили збереження державних даних у своїх хмарних сховищах, організували кіберзахист національних мереж та надали інструменти аналітики даних на основі ШІ для моніторингу загроз.

Водночас досвід російсько-української війни спричинив глибоку трансформацію самого концепту технологічного суверенітету держа-

¹ Див.: Залкін С. В., Ревін О. В., Сідченко С. О., Хударковський К. І., Белімов В. В. Аналітичний огляд технологій підготовки і проведення операцій впливу Російською Федерацією. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2025. №4 (82). С. 106–115. DOI: <https://doi.org/10.30748/zhups.2024.82.14>.

² Див.: Ohle M. Palantir's Ukraine Expansion Highlights Growing Power of Private AI in Modern Warfare. *European capital insights*. February 05, 2026. URL: <https://europeancapitalinsights.substack.com/p/palantirs-ukraine-expansion-highlights>.

ви в міжнародному дискурсі. У попередні роки під цим поняттям розуміли переважно юридичну та технічну недоторканність цифрових кордонів, суверенний контроль над внутрішнім сегментом інтернету та захист національних серверів. Проте в умовах експансії штучного інтелекту, що вимагає колосальних обчислювальних ресурсів, наявності гігантських масивів даних та надсучасного апаратного забезпечення, концепція технологічного суверенітету зазнала радикальних змін¹. Сьогодні вона більше не обмежується віртуальними кордонами, а вимагає фізичної наявності власної розвиненої інфраструктури даних, розробки незалежних, суверенних національних моделей штучного інтелекту та, що найважливіше, диверсифікації й надійності глобальних ланцюжків постачання.

Як безпосередній наслідок цієї трансформації, класична дипломатична практика частково перетворилася на так звану «напівпровідникову дипломатію» (*semiconductor diplomacy*). Світова геополітика увійшла в епоху запеклого, безкомпромісного суперництва за доступ до критичних матеріальних елементів, без яких функціонування та розвиток ІІІ є фізично неможливими. Головним предметом дипломатичних переговорів, укладання стратегічних альянсів та запровадження санкційних режимів став контроль над географічними зонами видобутку й переробки рідкісноземельних металів, доступ до літографічного обладнання надвисокої точності та наявність потужностей з виробництва передових мікрочипів і суперкомп'ютерів². Держави, які потрапляють у повну технологічну залежність від іноземних монополій у сфері апаратного забезпечення ІІІ, ризикують втратити не лише свій цифровий, а й загальний державний суверенітет. Таким чином, кібердипломатія нового покоління реалізується на перетині геополітики, матеріального виробництва високих технологій та захисту когнітивного простору, де спроможність гарантувати технологічну незалежність стає головним мірилом суб'єктності держави на міжнародній арені.

¹ Див.: Cruzes S. AI Infrastructure Sovereignty. URL: <https://arxiv.org/pdf/2602.10900>.

² Див.: Miller C. Chip war: the fight for the world's most critical technology. New York: Simon & Schuster, 2022. xxvii, 431 p.

Аналіз сучасної архітектури кібердипломатії дозволяє констатувати формування багаторівневої та поліцентричної системи інституціоналізації цифрової безпеки. Цей контур охоплює як глобальні універсальні майданчики, так і гнучкі регіональні чи субрегіональні альянси. Кожен із досліджених форматів (ООН, ЄС, НАТО, NB8 та e-PINE) виконує специфічну функціональну роль, трансформуючи теоретичні норми відповідальної поведінки держав у практичні інструменти стримування та розбудови цифрової стійкості.

Сучасна кібердипломатія розгортається у складній багаторівневій системі міжнародних форматів.

Глобальний рівень (ООН). Діяльність Робочої групи відкритого складу (OEWG) та Групи урядових експертів (GGE) залишається головним легітимним треком для кодифікації міжнародного права в кіберпросторі. Головним історичним здобутком цього формату стало консенсусне визначення та кодифікація 11 добровільних норм відповідальної поведінки держав у кіберпросторі, які були вперше сформульовані у Звіті Групи урядових експертів (GGE) ООН 2015 року та згодом підтверджені Робочою групою відкритого складу (OEWG)¹. Цей нормативний компас, схвалений Резолюцією Генеральної Асамблеї ООН, де-факто заклав політико-правовий фундамент глобальної цифрової стабільності, структурувавши зобов'язання держав за кількома критичними векторами:

а) *захист критичної інфраструктури (KI)* (норми суворо забороняють державам здійснювати або свідомо підтримувати кіберактивність, яка завдає шкоди об'єктам KI інших країн, таким як енергетика, транспорт, фінансові системи, а також зобов'язують вживати заходів для захисту власних критичних секторів від транскордонних цифрових загрозливих чинників);

б) *безпека ланцюгів постачання та недоторканність ІКТ-продуктів* (актори міжнародних відносин мають утримуватися від навмисного внесення шкідливих функцій (бекдорів, вірусів) в ІКТ-

¹ Див.: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / [by the Secretary-General]. *United Nations General Assembly*. 2015. A/70/174. URL: <https://digitallibrary.un.org/record/799853? v=pdf>.

продукцію на етапі її розробки та постачання, що є ключовим елементом сучасного технологічного довіри);

в) *гуманітарний імунітет команд реагування* (норми встановлюють міжнародне табу на використання національних команд реагування на комп'ютерні надзвичайні події (CSIRTs / CERTs) як інструментів для проведення наступальних кібероперацій, гарантуючи їх нейтральний і виключно захисний статус);

г) *принцип належної обачності (Due Diligence) та міжнародна співпраця* (держави не повинні дозволяти використовувати свою суверенну територію та інфраструктуру для здійснення протиправних кібератак проти інших суб'єктів, водночас вони зобов'язані всебічно сприяти розслідуванню інцидентів, обмінюватися технічними даними та надавати допомогу країнам, які стали жертвами масштабної цифрової агресії).

Хоч ці 11 норм є добровільними й не мають юридично зобов'язальної сили (*soft law*), вони трансформувалися у загально-визнаний міжнародний стандарт та слугують головним референсом для атрибуції зловмисної кіберактивності на світовій арені: коли коаліція демократичних країн засуджує дії іноземних хакерських угруповань, то апелює саме до порушення цих засадничих норм ООН. Водночас на сучасному етапі ООН демонструє інституційну обмеженість у питаннях примусу до виконання цих норм, перетворюючись на арену жорсткого нормативного та світоглядного протистояння між демократичними та авторитарними блоками. Зокрема, у межах OEWG триває принципова дискусія щодо філософії регулювання цифрового простору: західні демократичні держави наполягають на суворому дотриманні та імплементації вже наявних норм міжнародного права, тоді як авторитарні режими (насамперед Росія та Китай) намагаються нав'язати створення нових, юридично зобов'язальних договорів. Під приводом «забезпечення кібербезпеки» такі ініціативи мають на меті легітимізувати тотальний внутрішній контроль над інформаційними потоками, суверенізацію національних сегментів інтернету та цензуру. Важливим інструментом інституційної стабілізації цього треку стало створення постійного Глобального механізму ООН із кібербезпеки, організаційна та перші предметні сесії якого успішно

стартували у березні та липні 2026 року. Цей крок дозволив міжнародній спільноті частково подолати кризу класичного мультилатералізму та перейти від багаторічних тимчасових *ad hoc* дискусій до постійної міждержавної взаємодії, спрямованої на впровадження норм відповідальної поведінки держав у цифровому середовищі¹.

Інтеграційний інституціоналізм (Європейський Союз та НАТО). ЄС змістив фокус кібердипломатії із суто декларативних заяв на практичний регуляторний, правовий та безпековий вимір та став одним із головних міжнародних майданчиків для формування спільних оборонних інструментів. Впровадження Директиви NIS2, Регламенту про кіберсолідарність (*Cyber Solidarity Act*) та розбудова Спільної кіберслужби (*Joint Cyber Unit*) демонструють послідовний перехід союзу до побудови єдиного захисного периметру. Дипломатичний інструментарій Брюсселя суттєво посилений механізмом «кібердипломатичної інструментальної скриньки» (*EU Cyber Diplomacy Toolbox*)². Цей найефективніший механізм колективної відсічі дозволяє країнам-членам не лише узгоджувати спільні політичні заяви чи здійснювати атрибуцію атак, а й застосовувати прямі обмежувальні заходи (зокрема, заморожування активів та заборону на в'їзд) проти третіх держав-агресорів та підконтрольних їм хакерських угруповань за зловмисну діяльність у мережі. Водночас ухвалення нових масштабних регуляторних актів – таких як Європейський акт про кіберстійкість (*Cyber Resilience Act*)³ та Європейський акт про ШІ (*EU AI Act*) – зумовлює жорсткі й безкомпромісні вимоги до безпеки цифрових продуктів, логістичних ланцюгів постачання та високотехноло-

¹ Див.: Rupp C. From launch to delivery, the UN's new cybersecurity mechanism faces old divides. *Binding Hook*. April 24, 2026. URL: <https://bindinghook.com/from-launch-to-delivery-the-uns-new-cybersecurity-mechanism-faces-old-divides/>.

² Див.: Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox"), 19 June 2017 (Document No. 10474/17). *Council of the European Union*. 4 p. URL: <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>; Revised implementing guidelines of the Cyber Diplomacy Toolbox (Document No. 10289/23). *Council of the European Union*. June 8, 2023. 26 p. URL: <https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf>.

³ Див.: Cyber Resilience Act. URL: <https://www.cyberresilienceact.eu/>.

гічних систем на внутрішньому ринку Європи, що де-факто масштабує правові стандарти ЄС на глобальний рівень.

Після історичного визнання кіберпростору окремим оперативним доменом на Варшавському саміті (2016) та оновлення Комплексної політики кібероборони на Брюссельському саміті (2021), НАТО послідовно інтегрує цифрову складову в загальну систему колективної оборони та стримування¹. Ключовим доктринальним зрушенням кібердипломатії Альянсу стало офіційне підтвердження того, що масштабні зловмисні кібератаки можуть досягати порогу збройного нападу і, як наслідок, стають підставою для застосування Статтю 5 Вашингтонського договору. Практичне забезпечення операційної сумісності, синергії та технологічної переваги союзників здійснюється через дворівневу інституційну архітектуру:

- оперативно-військовий складник – Центр операцій у кіберпросторі (СуОС) у Монсі (Бельгія), який забезпечує інтеграцію суверенних кіберспроможностей країн-членів у загальну структуру командування НАТО, здійснює цілодобовий моніторинг військових мереж та координацію тактичних дій у режимі реального часу;

- науково-дослідний та навчальний складник – Об'єднаний центр передового досвіду з кібероборони НАТО (CCDCOE) у Таллінні (Естонія), який має статус міжнародної військової організації і є головним аналітичним хабом євроатлантичного простору, забезпечуючи розробку методологічних стандартів (зокрема, фундаментального «Талліннського посібника з міжнародного права, що застосовується до кібероперацій»), проведення масштабних кібернавчань (Locked Shields) та стратегічну підготовку вищого дипломатичного корпусу).

Сучасний вектор кібердипломатії Альянсу спрямований на вирішення двох стратегічних завдань: колективну політичну атрибуцію транскордонних цифрових атак та формування концепції «стратегічної невизначеності». Навмисно не встановлюючи чіткого кількісного чи якісного порогу руйнувань, за якого автоматично застосовується військова сила у відповідь на цифрову агресію, НАТО залишає за собою право гнучкого реагування. Це дозволяє стримувати потенційних

¹ Див.: *Cyber Defence. North Atlantic Treaty Organization*. 2026. URL: <https://www.act.nato.int/activities/cyber/>.

супротивників (насамперед РФ та КНР) від проведення критичних операцій проти цивільної інфраструктури держав-членів, розмиваючи їхні розрахунки на безкарність гібридних дій.

Регіональні формати гнучкого реагування (NB8 та e-PINE). У сучасній архітектурі цифрової безпеки субрегіональні платформи – такі як формат Нордично-Балтійської вісімки (NB8) (Данія, Естонія, Фінляндія, Ісландія, Латвія, Литва, Норвегія, Швеція) та Партнерство розширеного співробітництва в Східній Європі (e-PINE) за безпосередньої участі США – представляють інноваційну та високоефективну модель «мережевої дипломатії». На відміну від великих міжнародних інституцій, обтяжених тривалими бюрократичними процедурами узгодження рішень, ці гнучкі майданчики функціонують на засадах горизонтальної координації та демонструють найвищу швидкість обміну операційними і розвідувальними даними. В умовах перманентної гібридної експансії з боку РФ, діяльність NB8 та e-PINE зазнала глибокої функціональної трансформації, сфокусувавшись на двох критичних треках.

По-перше, ідеться про захист критичної підводної та енергетичної інфраструктури, оскільки специфікою Балтійського регіону є наявність щільної мережі підводних кабелів зв'язку та газопроводів. Прикладами можуть бути, зокрема, кейси інцидентів з Balticconnector та лініями зв'язку в Балтійському морі. Субрегіональна дипломатія вищезазначених форматів забезпечила створення спільних систем моніторингу, де координація дій військово-морських сил, операторів зв'язку та кіберфахівців інтегрована в єдиний безпековий контур.

По-друге, слід зазначити протидію транскордонним гібридним загрозам. У межах e-PINE залучення технологічного та розвідувального потенціалу США дозволяє країнам Балто-Чорноморського регіону вибудовувати проактивні системи захисту від скоординованих кібератак на хмарну інфраструктуру та державні реєстри. Де-факто NB8 та e-PINE є «лабораторіями безпекових рішень» та передовими форпостами євроатлантичного простору. Вони тестують нові моделі колективної атрибуції кіберінцидентів та спільної протидії ШІ-

дезінформації, які згодом масштабуються до рівня рішень усього Альянсу НАТО та Європейського Союзу¹.

Практична апробація зазначених форматів радикально змінилася під впливом повномасштабної російсько-української війни. Український кейс переформатував глобальну та регіональну архітектуру кібербезпеки за двома ключовими напрямками: а) асиметричною стійкістю та приватно-публічним партнерством (Україна довела, що ефективна кібероборона сучасної держави неможлива без залучення глобальних технологічних гігантів, як-от Microsoft, Google, AWS, Cloudflare, а кібердипломатія змістила фокус із класичних міждержавних перемовин на взаємодію з недержавними акторами, що потребує нової правової рамки); б) «напівпровідниковою дипломатією» як базисом безпеки (досвід захисту критичної інфраструктури продемонстрував, що стійкість програмного забезпечення (софту) є вторинною щодо безпеки ланцюгів постачання апаратного забезпечення (хардверу), таким чином геополітика мікросхем, експортний контроль технологій подвійного призначення та санкційні обмеження щодо агресора стали невід’ємною частиною кібердипломатичних стратегій євроатлантичного простору).

Сучасна кібердипломатія еволюціонувала з допоміжного, суто технічного інструменту зовнішньої політики в самостійний, концептуально зрілий міждисциплінарний інститут глобальної системи міжнародних відносин. Вона визначається як комплексна політико-дипломатична діяльність держав та наддержавних об’єднань, спрямована на формування міжнародно-правових норм, управління транскордонними інцидентами, політичну атрибуцію кібератак та стратегічний захист національних інтересів у цифровому просторі через механізми двосторонньої й багатосторонньої взаємодії.

Проведене дослідження дозволяє констатувати, що архітектура цього інституту набула чітко вираженої трирівневої структури: глобальний рівень (нормативно-кодифікаційні процеси під егідою ООН); регіональний / інтеграційний рівень (регуляторно-санкційні механізми в межах ЄС та військово-політичне стримування в контурі НАТО);

¹ Див.: Kļaviņš D. Cyber Diplomacy. Latvia's Voice in the World.

субрегіональний рівень (оперативно-координаційна взаємодія в гнучких форматах типу NB8 або e-PINE). Ефективність зазначеної системи забезпечується не жорстким ієрархічним підпорядкуванням, а функціональним дублюванням, а також гнучким мережевим розподілом завдань між акторами. Водночас виявлено глибоку поляризацію на глобальному майданчику ООН, де формування універсального договору гальмується антагонізмом концепцій «відкритого, вільного та безпечного інтернету» (демократичний блок) та «цифрового суверенітету і державного контролю за контентом» (ревізійністські автократії). Це зумовлює об'єктивне перенесення реального центру безпекової координації на рівень регіональних і субрегіональних платформ.

У доктринальному вимірі класична атрибуція кібератак перетворилася з технічного завдання на суто дипломатичний акт політичної волі, а механізми колективної відповіді (зокрема EU Cyber Diplomacy Toolbox) демонструють високу ефективність лише за умови синхронного застосування економічних санкцій та інструментів технологічного стримування. Матеріальний базис кібердипломатії сучасної епохи виявився жорстко детермінованим географією виробництва та контролем за ланцюгами постачання мікроелектроніки. Це нерозривно пов'язує її з трендом «технонаціоналізму», де доступ до передових літографічних технологій та напівпровідників є головним чинником забезпечення суверенної кіберстійкості.

Повномасштабна війна проти РФ остаточно закріпила за Україною статус ключового суб'єкта формування практичного досвіду кібероборони. Для довгострокового забезпечення національних інтересів українська дипломатична служба має трансформуватися від пасивної моделі «реципієнта безпекової допомоги» до проактивної ролі «донора унікальних оперативних знань». Це передбачає ініціювання нових субрегіональних безпекових платформ та поглиблення інтеграції в передові євроатлантичні структури, такі як Спільна кіберслужба ЄС (Joint Cyber Unit) та Об'єднаний центр передового досвіду з кібероборони НАТО (CCDCOE).

Резюмуючи, підкреслимо, що епоха штучного інтелекту безпосередньо змінила ландшафт світової геополітики, перетворивши кі-

бердипломатію на ключове поле битви за національну безпеку та державний суверенітет. Сучасний алгоритмічний вплив здатний зруйнувати суспільний консенсус та дестабілізувати політичні системи без жодного пострілу чи класичного зламу фізичних серверів. У цих умовах стратегічну перевагу здобуває не той актор, який володіє більшою кількістю традиційних озброєнь, а той, чиї алгоритми здатні ефективніше захищати власний когнітивний простір та формувати глобальний порядок денний. Для демократичного світу єдиним шляхом протидії алгоритмічній тиранії є розбудова національної кіберстійкості, рішуча відмова від застарілих бюрократичних шаблонів та створення сильних міжнародних коаліцій, здатних дати жорстку, скоординовану й технологічно випереджальну відсіч будь-яким гібридним загрозам майбутнього.

==== Список використаних джерел

1. Банчук-Петросова О., Сулим Б. Цифрова дипломатія: вплив штучного інтелекту та великих даних на трансформацію дипломатичної практики. *Empirio*. 2026. Т. 3, № 1. С. 49–58.
2. Верховцева І. Г., Шестаков В. І., Гребенюк В. М., Гайдук О. В. Новітня термінологія у дипломатичних практиках як маркер кібервпливів: цифрова дипломатія, кібердипломатія. *Публічне адміністрування та національна безпека*. 2025. № 5. С. 15–22.
3. Війна як модус соціального буття в міждисциплінарному науковому дискурсі: монографія / [Л. М. Алексеєнко, Ю. Г. Борейко, А. О. Бояр та ін.] ; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2026. 338 с. DOI: <https://doi.org/10.31359/9786178759926>.
4. Залкін С. В., Ревін О. В., Сідченко С. О., Хударковський К. І., Белімов В. В. Аналітичний огляд технологій підготовки і проведення операцій впливу Російською Федерацією. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2025. № 4(82). С. 106–115. DOI: <https://doi.org/10.30748/zhups.2024.82.14>.
5. Інформаційна війна та її вплив на суспільство: монографія / [Л. М. Алексеєнко, О. М. Іванченко, У. В. Ільницька та ін.] ; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2026. 506 с.

6. Кібердипломатія: матеріали Міжнародної науково-практичної конференції (м. Київ, 15–16 травня 2024 року), Науково-практичного круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року) / за заг. ред. чл.-кор. НАН України, доктора техн. наук, професора О. Г. Корченка ; упорядники: І. Г. Верховцева, О. В. Гайдук. Київ: Дипломатична академія імені Геннадія Удовенка; Державний університет інформаційно-комунікаційних технологій, 2025. 132 с.
7. Кононенко В. П., Комарова Т. Г. Цифрова дипломатія як засіб стратегічної комунікації держави. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Питання політології*. 2024. Вип. 45. С. 15–20.
8. Кузь О. М., Требін М. П. Дипломатія цифрової епохи. *Україна в часи випробувань: соціальні, культурні та політичні трансформації*: матеріали Всеукр. наук.-практ. конф. (ХЛІ Харків. політол. читання), м. Харків, 30 січ. 2026 р.) / [редкол.: Куц Г. М. (голова), Панфілов О. Ю., Погрібна В. Л. та ін.] ; Аналіт. центр сучас. гуманітаристики; Харків. асоц. політологів. Харків: Право, 2026. С. 25–32.
9. Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. *Україна дипломатична*. 2023. Вип. 24. С. 696–708.
10. Озернюк Г. Цифрова дипломатія та дипломатія даних: історичні передумови й концептуальні відмінності. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2025. № 2. С. 121–135.
11. Піпченко Н. О., Макаренко Є. А., Рижков М. М. Цифрова дипломатія: підруч. для студентів закл. вищ. освіти, які навчаються за спец. «Міжнародні відносини, суспільні комунікації та регіональні студії» / Київ. нац. ун-т ім. Тараса Шевченка. Київ: ВАДЕКС, 2019. 317 с.
12. Поляков О. М. Кібердипломатія як важливий напрямок міжнародно-правового співробітництва в умовах режиму воєнного стану. *Нове українське право*. 2024. Вип. 6. С. 70–76.
13. Руднева А. О., Мальована Ю. Г. Цифрова дипломатія у формуванні системи національної безпеки України в умовах війни з РФ. *Регіональні студії*. 2023. № 34. С. 111–115.
14. Степанов В. Ю., Бричук К. Г. Цифрова дипломатія як інструмент масової комунікації в публічному управлінні. *Вісник Національної академії державного управління при Президентові України. Серія : Державне управління*. 2020. № 3. С. 5–10.

15. Требин М. Российско-украинская война: динамика технического, организационного и человеческого измерений. *Историческая экспертиза*. 2025. № 3(44). С. 113–140.
16. Требін М. Феномен «гібридної» війни. *Гілея*. 2014. Вип. 87 (8). С. 366–371.
17. Цифрова дипломатія України: стратегічні комунікації, аналіз даних, кризове управління: матеріали міжнародної наукової конференції. Львів, 14 листопада 2025 р. / Упорядники: М. Мальський, Р. Вовк, О. Кучик. Львів: Львівський національний університет імені Івана Франка, 2025. 120 с.
18. Чепелюк Ю. В. Цифрова дипломатія в контексті сучасних інформаційних комунікацій. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2021. Т. 4, № 2. С. 250–258.
19. Яковюк І. В., Цвелих М. П. Цифрова дипломатія: впровадження електронних візових послуг в Україні. *Право та інновації*. 2022. № 3. С. 69–76.
20. Attatfa A., Renaud K., De Paoli S. Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*. 2020. Vol. 176. P. 60–69.
21. Barrinha A. Cyber-diplomacy: The Emergence of a Transient Field. *The Hague Journal of Diplomacy*. 2024. Vol. 19, Issue 3. P. 439–466. DOI: <https://doi.org/10.1163/1871191x-bja10183>.
22. Bee D. Cognitive Sovereignty in Algorithmic Societies: A Methodological Framework for Reclaiming Human Agency. *Meaningfulness Media Group Technical Report No. 3*. 2026. 32 p. URL: <https://philarchive.org/archive/BEECSI>.
23. Birhane A. Algorithmic Colonization of Africa. *SCRIPTed*. 2020. Vol. 17, Issue 2. P. 389–409. DOI: 10.2966/scrip.170220.389.
24. Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities («Cyber Diplomacy Toolbox»), 19 June 2017 (Document No. 10474/17). *Council of the European Union*. 4 p. URL: <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>.
25. Cruzes S. AI Infrastructure Sovereignty. URL: <https://arxiv.org/pdf/2602.10900>.
26. Cyber Resilience Act. URL: <https://www.cyberresilienceact.eu/>.
27. Cyber Defence. *North Atlantic Treaty Organization*. 2026. URL: <https://www.act.nato.int/activities/cyber/>.
28. Cyber-diplomacy: managing foreign policy in the twenty-first century / edited by Evan H. Potter. Montreal: McGill-Queen's University Press, 2002. xii, 208 p.

29. ENISA releases 2025 Threat Landscape report on Europe's cybersecurity challenges. *CyberHubs*. October 15, 2025. URL: <https://cyberhubs.eu/enisa-releases-2025-threat-landscape-report-on-europes-cybersecurity-challenges/>.
30. ENISA threat landscape 2025. *European Union Agency for Cybersecurity (ENISA)*. October 2025. 86 p. DOI: 10.2824/1946374.
31. ENISA threat landscape 2026. *European Union Agency for Cybersecurity (ENISA)*. September 2026. 101 p. DOI: 10.2824/0806036.
32. ENISA's 2026 report identifies ransomware, vulnerability exploitation and AI-enabled attacks as leading EU cyber threats. *Civil Society Alliances for Digital Empowerment (CADE)*. September 23, 2026. URL: <https://cadeproject.org/updates/enisas-2026-report-identifies-ransomware-vulnerability-exploitation-and-ai-enabled-attacks-as-leading-eu-cyber-threats/>.
33. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / [by the Secretary-General]. *United Nations General Assembly*. 2015. A/70/174. URL: <https://digitallibrary.un.org/record/799853?v=pdf>.
34. Hanson F. Baked in and wired: eDiplomacy@State. *Foreign Policy at Brookings*. URL: <https://www.brookings.edu/wp-content/uploads/2016/06/baked-in-hansonf-5.pdf>.
35. Hanson F. Revolution @State: The spread of ediplomacy. Sydney: Lowy Institute for International Policy, 2012. 34 p. URL: https://www.brookings.edu/wp-content/uploads/2016/06/03_ediplomacy_hanson.pdf.
36. Kļaviņš D. Cyber Diplomacy. Latvia's Voice in the World. *Cybersecurity in Latvia: forging resilience amidst emerging threats* / edited by Mihails Potapovs and Kate E. Kanasta. London: Routledge, 2025. P. 150–174. URL: <https://www.taylorfrancis.com/reader/download/230471d2-6454-4606-abd5-9a376ac2f159/chapter/pdf?context=ubx>.
37. Kuz O., Nepochatov D. Cyber Diplomacy as an Instrument of Cognitive Warfare in Cyberspace. *Actual Problems of International Relations*. 2026. Vol. 1, No. 167. P. 53–60. DOI: <https://doi.org/10.17721/apmv.2026.167.1.53-60>.
38. Lewis D. Digital diplomacy. *Gateway House*. December 19, 2014. URL: <http://www.gatewayhouse.in/digital-diplomacy-2>.
39. Metzl J. F. Network Diplomacy. *Georgetown Journal of International Affairs*. 2001. Vol. 2, No. 1. P. 77–87.
40. Miller C. Chip war: the fight for the world's most critical technology. New York: Simon & Schuster, 2022. xxvii, 431 p.
41. Myatt M. Small, Smart, Powerful? Small States and the Competition for Cybertech Superiority in the Digital Age. *Competition in World Politics*:

- Knowledge, Strategies and Institutions* / Daniela Russ, James Stafford (eds.). Bielefeld: Transcript, 2021. P. 233–260.
42. Nye J. S., Jr. Get Smart: Combining Hard and Soft Power. *Foreign Affairs*. 2009. Vol. 88, No. 4. P. 160–163. URL: <http://www.jstor.org/stable/20699631>.
43. Ohle M. Palantir's Ukraine Expansion Highlights Growing Power of Private AI in Modern Warfare. *European capital insights*. February 05, 2026. URL: <https://europeancapitalinsights.substack.com/p/palantirs-ukraine-expansion-highlights>.
44. Poda T. A. The development of «network diplomacy» as a new form of international interaction. *Вісник НАУ. Серія: Філософія. Культурологія*. 2020. № 1 (31). С. 84–88.
45. Revised implementing guidelines of the Cyber Diplomacy Toolbox (Document No. 10289/23). *Council of the European Union*. June 8, 2023. 26 p. URL: <https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf>.
46. Riordan S. Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. *USC Center on Public Diplomacy*. May 12, 2016. URL: <https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction>.
47. Riordan S. *Cyberdiplomacy: Managing Security and Governance Online*. Cambridge: Polity Press, 2019. ix, 134 p.
48. Rupp C. From launch to delivery, the UN's new cybersecurity mechanism faces old divides. *Binding Hook*. April 24, 2026. URL: <https://bindinghook.com/from-launch-to-delivery-the-uns-new-cybersecurity-mechanism-faces-old-divides/>.
49. Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence / general editor Michael N. Schmitt. Cambridge; New York: Cambridge University Press, 2013. xix, 282 p.
50. Tallinn manual 2.0 on the international law applicable to cyber operations / prepared by the International Groups of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence ; general editor Michael N. Schmitt; managing editor Liis Vihul. Cambridge; New York: Cambridge University Press, 2017. xli, 598 p.
51. Westcott N. Digital Diplomacy: The Impact of the Internet on International Relations. *Oxford Internet Institute. Research Report 16*. July 2008. 20 p. URL: <https://www.oii.ox.ac.uk/wp-content/uploads/old-docs/RR16.pdf>.

Авторський колектив

Алексєнко Людмила Михайлівна, доктор економічних наук, професор, професор кафедри фундаментальних та спеціальних дисциплін, Нововолинський навчально-науковий інститут економіки та менеджменту Західноукраїнського національного університету (м. Нововолинськ).

Бескаравайний Станіслав Сергійович, кандидат філософських наук, доцент, в. о. завідувача кафедри філософії та українознавства навчально-наукового інституту «Український державний хіміко-технологічний університет», Український державний університет науки і технологій (м. Дніпро).

Квасниця Оксана Василівна, кандидат економічних наук, доцент, доцент кафедри фінансів ім. С. І. Юрія, Західноукраїнський національний університет (м. Тернопіль).

Коваль Зоряна Остапівна, кандидат економічних наук, доцент, доцент кафедри менеджменту персоналу і адміністрування, Національний університет «Львівська політехніка».

Ковтунова Лариса Юрївна, кандидат юридичних наук, викладач кафедри менеджменту та правового регулювання спортивної діяльності, Харківська державна академія фізичної культури.

Козут Олексій Вікторович, аспірант кафедри культурології та філософії культури, Національний університет «Одеська політехніка».

Козловець Микола Адамович, доктор філософських наук, професор, професор кафедри філософії та політології, заслужений діяч освіти України, Житомирський державний університет імені Івана Франка.

Кривонос Олександр Миколайович, кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук та інформаційних технологій, Житомирський державний університет імені Івана Франка.

Рябуха Ольга Олександрівна, аспірант Києво-Могилянської школи врядування імені Андрія Мелешевича, Національний університет «Києво-Могилянська академія».

Рябцев Геннадій Леонідович, доктор наук з державного управління, професор, професор Києво-Могилянської школи врядування імені Андрія Мелешевича, Національний університет «Києво-Могилянська академія».

Сінельнікова Марія Василівна, кандидат філософських наук, доцент, доцент кафедри філософії, Національний університет «Львівська політехніка».

Требін Михайло Петрович, доктор філософських наук, професор, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Тулай Оксана Іванівна, доктор економічних наук, професор, завідувач кафедри міжнародних відносин та дипломатії, Західноукраїнський національний університет (м. Тернопіль).

Шевченко Людмила Степанівна, доктор економічних наук, професор, заслужений професор Національного юридичного університету імені Ярослава Мудрого, Аналітичний центр сучасної гуманітаристики (м. Харків).

Наукове видання

Алексесенко Людмила Михайлівна,
Бескаравайний Станіслав Сергійович,
Квасниця Оксана Василівна та ін.

ШТУЧНИЙ ІНТЕЛЕКТ: ІНТЕГРАЛЬНИЙ ПОГЛЯД НА НОВУ ЦИФРОВУ РЕАЛЬНІСТЬ

Монографія

Редактор *Т. О. Чернишова*

Підписано до друку 28.09.2026. Формат 60×84/16.
Ум. друк. арк. 17. Обл.-вид. арк. 13. Тираж 100 пр. Зам. № 762

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20

Вебсайт: <https://pravo-izdat.com.ua>

E-mail для замовників послуг: verstka@pravo-izdat.com.ua

E-mail для покупців: sales@pravo-izdat.com.ua

Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт Плюс»,
вул. Весніна, 12, м. Харків, 61023, Україна
Тел. (097) 445-07-79

Вебсайт: <https://promart.in.ua>

Свідоцтво суб'єкта видавничої справи ДК № 8388 від 16.07.2025