УДК 327:004.056.5:351.746
DOI: 10.60022/2(3)-8S

Сумін Павло Павлович
здобувач третього (освітньо-наукового) рівня вищої освіти
факультет журналістики і міжнародних відносин
Київський Університет Культури, Україна
Sumin Pavlo
PhD Student
Faculty of Journalism and International Relations
Kyiv University of Culture, Ukraine
ORCID: 0009-0000-1029-4063

ГЛОБАЛЬНІ СТРАТЕГІЇ КІБЕРЗАХИСТУ: АНАЛІЗ МІЖНАРОДНИХ ІНІЦІАТИВ ТА ЇХ ВПЛИВ НА НАЦІОНАЛЬНІ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Статтю присвячено комплексному аналізу глобальних стратегій кіберзахисту в контексті міждержавної взаємодії, цифрового суверенітету та трансформації моделей безпеки в умовах цифрової взаємозалежності. Досліджено основні теоретичні парадигми управління кіберпростором – реалістичну, ліберальну, інституціоналістську та конструктивістську – через призму міжнародних ініціатив і політик. Особливу увагу приділено ролі ключових акторів (ООН, НАТО, ENISA, GFCE) та їх впливу на формування нормативної бази й механізмів координації. На основі компаративного аналізу стратегій ЄС, США, Китаю та України показано напруженість між прагненням до цифрового суверенітету та необхідністю глобального узгодження стандартів безпеки. Проаналізовано ключові виклики, що супроводжують впровадження міжнародних норм у сфері кібербезпеки. Акцентовано необхідність переходу до нової парадигми цифрової дипломатії, яка ґрунтується на принципах етики, відкритості, солідарності та колективної відповідальності. Проаналізовано концепцію цифрової солідарності як передумову забезпечення рівного доступу до безпечних технологій і роль цифрової етики у формуванні міжнародного регулювання поведінки в кіберпросторі. Запропоновано бачення глобальної інфраструктури кіберзахисту, що має поєднувати національні інтереси з універсальними цінностями цифрового суспільства. Перспективи подальших досліджень пов'язано з інституціоналізацією міжнародного кіберрегулювання на основі кращих світових практик.*

Ключові слова: *глобальний кіберзахист; цифровий суверенітет; кібербезпека; цифрова дипломатія, міжнародна координація;, інституціоналізація кіберрегулювання.*

GLOBAL CYBER SECURITY STRATEGIES: ANALYSIS OF INTERNATIONAL INITIATIVES AND THEIR IMPACT ON NATIONAL POLICIES IN THE FIELD OF INFORMATION SECURITY

Abstract. *The article is devoted to a comprehensive analysis of global cyber defense strategies in the context of interstate interaction, digital sovereignty, and the transformation of security models in conditions of digital interdependence. The main theoretical paradigms of cyberspace governance – realistic, liberal, institutionalist, and constructivist – are examined through the prism of international initiatives and policies. Particular attention is paid to the role of key actors (the UN, NATO, ENISA, GFCE) and their influence on the formation of the regulatory framework and coordination mechanisms.*

Based on a comparative analysis of the strategies of the EU, the US, China, and Ukraine, the tension between the desire for digital sovereignty and the need for global harmonization of security standards is demonstrated. The key challenges accompanying the implementation of international norms in the field of cybersecurity are analyzed, in particular the uneven participation of states in global initiatives and the limited effectiveness of sanction mechanisms. The need to transition to a new paradigm of digital diplomacy based on the principles of ethics, openness, solidarity, and collective responsibility is emphasized.

Special attention is paid to the issue of harmonizing national strategies with global regulatory

approaches. It is determined that the effective implementation of cyber defense policy requires not only technical modernization, but also a profound reassessment of the legal, ethical, and political mechanisms for responding to cyber threats. It is proposed to consider the concept of digital sovereignty not as an isolationist practice, but as a desire to independently determine policies within the framework of global interdependence.

The author also analyzes the concept of digital solidarity as a prerequisite for ensuring equal access to secure technologies and the role of digital ethics in shaping international regulation of behavior in cyberspace. Digital ethics emerges not only as a set of norms, but as a coherent system of value orientations capable of ensuring trust and stability in interactions between states, the private sector, and civil society.

The article proposes a vision of a global cyber defense infrastructure that combines national interests with the universal values of the digital society. Such an infrastructure involves the development of integrated data exchange platforms, strengthening the functions of multilateral institutions, and enhancing the role of digital education in shaping a culture of security. Prospects for further research are linked to the institutionalization of international cyber regulation based on best global practices, in particular through the formation of a global code of conduct in cyberspace and the development of models of digital sovereignty that do not contradict the principles of international cooperation.

***Keywords**: global cyber defense; digital sovereignty; cybersecurity; digital diplomacy; international coordination; institutionalization of cyber regulation.*

Постановка проблеми. У сучасному світі, що стрімко змінюється під впливом цифрових технологій, питання кібербезпеки набуває особливого значення. Інформаційні потоки щодня зростають, а технологічні новації впливають на всі аспекти життя від економіки до політики. На цьому тлі дедалі частіше виникають загрози: хакерські атаки на важливі об'єкти інфраструктури, витоки персональних і корпоративних даних, поширення неправдивої інформації через цифрові канали, шкідливе програмне забезпечення. Навіть найрозвиненіші держави не убезпечені від подібних викликів, що свідчить про вразливість сучасних цифрових систем. В рамках протидії таким загрозам, уряди різних країн активізують роботу над створенням і вдосконаленням національних стратегій у сфері кіберзахисту. Ці документи поєднують технологічні рішення з управлінськими підходами, формуючи комплексну відповідь на виклики кіберпростору. Водночас політика у сфері інформаційної безпеки дедалі частіше формується не лише всередині країни, а й під впливом міжнародного досвіду та практик. Світова спільнота прагне до тіснішої координації зусиль у сфері кіберзахисту. Європейське агентство з кібербезпеки (ENISA), ініціативи НАТО, напрацювання ООН і рекомендації Міжнародного союзу електрозв'язку (ITU) створюють підґрунтя для уніфікації правил та процедур у сфері цифрової безпеки. Такі платформи забезпечують обмін досвідом, сприяють швидкому реагуванню на інциденти та допомагають країнам зміцнювати власну кіберстійкість. У результаті формується більш узгоджена і передбачувана система захисту інформаційного простору на глобальному рівні.

Аналіз останніх досліджень і публікацій. В умовах зростаючої кількості цифрових загроз уряди держав дедалі частіше звертаються до розробки національних стратегій кібербезпеки, покликаних забезпечити скоординовану відповідь на сучасні виклики, що постають перед цифровою інфраструктурою. К. Тео, А. Махмуд [1] і Б. Блажич [2] вказують, що такі стратегії, як правило, охоплюють широке коло питань – від організації захисту критичних об'єктів до запобігання кіберзлочинності, розбудови професійного потенціалу, підвищення цифрової обізнаності громадян та налагодження міжнародної співпраці. На ефективність впровадження зазначених документів істотно впливає рівень конкретизації поставлених цілей і завдань, а також наявність механізмів моніторингу прогресу за допомогою об'єктивно вимірюваних індикаторів.

Підвищена увага до питань кіберзахисту значною мірою зумовлена низкою масштабних інцидентів, які виявили вразливість навіть найбільш технологічних цифрових систем. У цьому контексті ключову роль відіграють профільні інституції, зокрема Національний інститут стандартів і технологій США (NIST), які ініціюють напрацювання уніфікованих підходів до управління кіберризиками. С. Альмухаммаді, М. Альсалех [3] С. Ніфакос та ін. [4], вказують, що запропонована NIST рамкова структура стала важливим орієнтиром для побудови системи захисту критичної інфраструктури, враховуючи необхідність адаптації до нових технологічних загроз. О. Хасан та ін. [5] зауважують, що такі документи мають не лише нормативне, а й практичне значення, оскільки забезпечують міждисциплінарне розуміння кіберзагроз, охоплюючи як технічні, так і поведінкові компоненти.

Водночас міжнародне співробітництво у сфері кібербезпеки набуває дедалі більшої ваги.

Держави активно беруть участь у транснаціональних ініціативах, що дає змогу обмінюватися досвідом, технологіями реагування та аналітичними напрацюваннями. Л. Танцер та ін. [6] вказують на те, що особливо важливу роль у цьому процесі відіграють команди реагування на інциденти інформаційної безпеки (CSIRTs), які забезпечують швидку координацію між країнами у випадку кіберзагроз. Х. Чифчі, Е. Озкоч [7] зазначають, що розвиток політики кібербезпеки тісно переплітається з питаннями врядування: національні стратегії все частіше орієнтуються на міжнародні стандарти, прагнучи до їх інтеграції у спільне нормативно-правове поле.

С. Онищенко, А. Глушко, О. Маслій [8] акцентують увагу на концепті кіберстійкості як ключової складової національної безпеки України. Дослідники доводять, що ефективне функціонування держави в умовах гібридних загроз неможливе без цілісної системи реагування на кібератаки, яка ґрунтується на принципах міжвідомчої координації, адаптивності та проактивного моніторингу кіберзагроз.

У свою чергу, В. Бойко, М. Василенко, С. Кухаренко [9] досліджують еволюцію політики кібербезпеки в ЄС і держав-членів, окреслюючи ключові виклики, що постали перед регіоном у контексті транснаціональної цифрової загрози. Зокрема, автори акцентують на розбалансованості між рівнем готовності окремих країн до відбиття кіберзагроз і загальноєвропейськими стандартами захисту. Аналіз показав, що, попри наявність нормативної бази, ЄС досі стикається з труднощами у впровадженні єдиної системи кіберзахисту.

Аналіз правових механізмів ЄС у сфері кібербезпеки подає А. Грубінко [10]. Стаття підкреслює, що зростання кіберзагроз змусило ЄС формалізувати спільні стандарти кіберзахисту та розвинути такі інституційні інструменти, як ENISA (Агентство ЄС з кібербезпеки) та мережа CSIRT (команди реагування на інциденти комп'ютерної безпеки). Правове забезпечення стратегії кіберзахисту, на думку автора, є фундаментом для сталого функціонування цифрового простору ЄС.

В даному контексті О. Кузнєцов [11] звертається до практичних аспектів посилення кіберспроможностей в ЄС, акцентуючи увагу на модернізації цифрової інфраструктури, зокрема шляхом впровадження інноваційних технологій, а також на системі навчання фахівців. Автор доводить, що досвід ЄС у підготовці спеціалізованих кадрів, проведенні спільних навчань та формуванні публічно-приватного партнерства має важливе значення для держав, які прагнуть зміцнити власну кібербезпеку, зокрема Україну.

У сукупності, наведені джерела відображають мультидисциплінарний підхід до аналізу глобальних стратегій кіберзахисту: від правового регулювання і політичного планування до організаційних практик та технологічної модернізації. Дослідники в сукупності підкреслюють, що інтеграція міжнародного досвіду у національні стратегії кібербезпеки є не лише бажаною, але й необхідною умовою для забезпечення цифрового суверенітету в умовах зростаючих глобальних ризиків

Однак залишаються нерозв'язані питання та виклики. Зокрема, гостро відчувається нестача кваліфікованих фахівців, що ускладнює реалізацію навіть найбільш продуманих політик. Результати дослідження Х. Фам та ін. [12] вказують на необхідність посилення освітніх програм, орієнтованих на практичну підготовку кадрів у сфері кіберзахисту. За Ж. Одумесі та Б. Санусі [13] уряди, визнаючи цей виклик, активізують діяльність у напрямку розвитку цифрових компетентностей серед населення й фахівців, адже без належної людської підтримки будь-яка технічна стратегія залишатиметься декларативною.

Таким чином, майбутнє ефективної кібербезпеки значною мірою залежить від гармонійного поєднання зусиль національного рівня з активною участю у міжнародних ініціативах. В умовах, коли масштаби кіберзагроз постійно зростають, загострюється потреба в адаптивній політиці, яка враховує не лише технічні новації, а й людський фактор, міжгалузеву взаємодію та постійну координацію дій на глобальному рівні.

Метою статті є аналіз основних глобальних стратегій кіберзахисту, визначення їх ключових інструментів та оцінка впливу таких ініціатив на формування національних політик у сфері інформаційної безпеки. Особливу увагу приділено виявленню синергії між міжнародними рамками та локальними нормативними й інституційними рішеннями, а також визначенню бар'єрів на шляху до ефективної імплементації глобальних стандартів у внутрішню політику держав. Наукова новизна запропонованого дослідження полягає у комплексному підході до порівняльного аналізу стратегічних ініціатив у сфері кібербезпеки та виявленні їхньої ролі в трансформації архітектури національного кіберзахисту.

Виклад основного матеріалу. У процесі вивчення проблематики глобального кіберзахисту у фаховому середовищі поступово сформувалися різні підходи до аналізу управління кіберпростором на

міждержавномурівні.Середнайвідомішихконцепцій–реалістичний,ліберальний,інституціоналістський та конструктивістський підходи. Кожен із них висвітлює різні аспекти: від пріоритетної ролі держави як ключового гравця до важливості співпраці між країнами та недержавними структурами в умовах глобальної цифрової взаємозалежності.

У різних теоретичних підходах до кібербезпеки простежується розмаїття поглядів на роль держав і міжнародної взаємодії. Представники реалістичної школи сприймають кіберзахист як інструмент захисту національного суверенітету: кожна держава прагне самостійно зміцнювати свої кіберможливості, зосереджуючись на захисті критично важливої інфраструктури. Натомість ліберали наголошують на необхідності міжнародної співпраці, яка реалізується через створення спільних стандартів, механізмів узгодження політик і транснаціональних партнерств. Інституціоналісти, у свою чергу, підкреслюють провідну роль міжнародних організацій, таких як ООН, НАТО чи ENISA, які виступають координаторами у сфері глобального кіберрегулювання. Конструктивісти ж звертають увагу на те, як уявлення про кіберзагрози формуються під впливом ідей, домінуючих наративів і соціальних норм.

Попри відсутність уніфікованого правового визначення, глобальна стратегія кібербезпеки зазвичай тлумачиться як сукупність норм, інституцій, процедур і технічних рішень, які спрямовані на підтримання стабільності в цифровому середовищі поза межами національних юрисдикцій. У цьому контексті ключовими є документи й ініціативи таких структур, як ООН, ENISA та GFCE. Ці організації не лише орієнтовані на міждержавну взаємодію, а й активно залучають приватні компанії, наукову спільноту та громадські організації до формування системи кібердовіри й обміну інформацією.

Одним із найактуальніших понять, що набуває ваги в цій сфері, є цифровий суверенітет – тобто прагнення держав зберегти контроль над даними, інфраструктурою та технологіями в рамках власного правового поля. Проте така стратегія не завжди узгоджується з принципами відкритості та глобальної співпраці, що нерідко спричиняє фрагментацію міжнародної архітектури кібербезпеки. Відповідно, постає питання як знайти баланс між глобальною природою цифрового простору та прагненням держав зберегти автономію.

Мейнстримдослідженьвданійцаринізастосовуєміждисциплінарніаналітичнімоделі,якіпоєднують підходи з міжнародного права, інформаційних технологій, політичної географії та безпекознавства. Це дозволяє глибше осмислити як універсальні риси глобальних загроз, так і особливості їхнього національного регулювання. З-поміж міжнародних документів важливе місце посідає Будапештська конвенція 2001 р. (Convention on Cybercrime) [14] – перший системний міжнародний акт, присвячений боротьбі з кіберзлочинністю. Конвенція визначає як матеріальні, так і процесуальні правові рамки, а також встановлює механізми взаємодії між правоохоронними органами різних країн. Іншим вагомим інструментом є нормативна діяльність GFCE, що об'єднує представників держав, компаній, технічних експертів і дослідників задля обміну практиками та посилення глобального потенціалу. ООН активно долучається до розроблення правил поведінки держав у цифровому просторі. Зокрема, Група урядових експертів (GGE) та Відкрита робоча група (OEWG) націлені на формулювання рекомендацій щодо безпечного поводження держав у кіберпросторі. У межах ЄС функціонує цілісна інституційна система, заснована на Директиві NIS2 [15], Акті про кіберстійкість (Cyber Resilience Act) [16] і нормативній діяльності ENISA. Ця рамка встановлює єдині вимоги до кіберзахисту, стандарти сертифікації та правила реагування на інциденти. НАТО розглядає кіберпростір як п'ятий простір сучасної війни – поряд із сушею, морем, повітрям і космосом. Організація розробляє власні підходи до кібероборони та підтримує держави-члени в розвитку спроможностей до колективного реагування на загрози.

Попри спільні стратегічні цілі – запобігання інцидентам, розбудова механізмів стримування, підвищення обізнаності, міжнародна взаємодія – реальне впровадження цих підходів наштовхується на низку викликів. Ідеться про нерівномірну участь країн, труднощі з моніторингом виконання домовленостей та обмежену кількість санкцій за їх порушення. Навіть за наявності таких інструментів, як Глобальний індекс кібербезпеки ITU чи звіти про імплементацію NIS2, оцінка прогресу часто є неповною або умовною.

Загалом, система глобального кіберрегулювання ще перебуває на етапі становлення. Система вже демонструє ознаки інституційної зрілості в питаннях координації, проте потребує подальшого зміцнення прозорості, підзвітності та рівного доступу для всіх учасників. Результативність таких стратегій у майбутньому значною мірою залежатиме від здатності різних суб'єктів співпрацювати на основі взаємної довіри та спільних інтересів.

На практиці це вже помітно в державній політиці багатьох країн. У ЄС, наприклад, імплементація

Директиви NIS2 вимагає гармонізації національного законодавства з загальноєвропейськими вимогами. ENISA у цьому процесі відіграє ключову методологічну роль. У США визначальним документом стала Національна стратегія кібербезпеки 2023 р. [17], заснована на принципах NIST, які визнані на міжнародному рівні.

Китай, навпаки, поєднує риторику міжнародного партнерства з жорстким внутрішнім контролем. Китайське законодавство зобов'язує компанії зберігати дані в межах країни, сертифікувати обладнання та фільтрувати інформаційні потоки.

Україна в контексті євроатлантичної інтеграції поступово адаптує основні міжнародні стандарти: від Будапештської конвенції до принципів ISO та NIST. Створення CERT-UA, запуск системи обміну інформацією про кіберінциденти, оновлення національної стратегії – усе це свідчить про реальні кроки у напрямі міжнародної інтеграції.

Водночас питання зіставлення суверенних підходів із глобальними зобов'язаннями залишається актуальною. Авторитарні режими часто відмовляються від участі у глобальних ініціативах, мотивуючи це потребою зберегти контроль над цифровим середовищем. Проте й у демократичних країнах триває дискусія про межі передачі повноважень наднаціональним інституціям. З огляду на це, реалізація глобальних стратегій кібербезпеки не є прямолінійним процесом. Ця задача вимагає постійного пошуку компромісів, узгодження інтересів та гнучкого реагування на нові виклики, з якими стикається міжнародна спільнота в цифровому середовищі. Аналіз стратегій подано в табл. 1.

Таблиця 1

Стратегії кібербезпеки у контексті міжнародної координації та цифрового суверенітету

Країни	Інтеграція міжнародних стратегій	Ключові елементи впливу	Конфлікт із цифровим суверенітетом
Країни ЄС	Імплементація директиви NIS2, діяльність ENISA, гармонізація стандартів реагування та захисту критичної інфраструктури	Правове регулювання, інституційна архітектура, сертифікація, захист критичної інфраструктури	Низький; регуляції переважно гармонізовані в межах єдиного правового простору
США	Національна стратегія кібербезпеки 2023 р.; широке застосування NIST Cybersecurity Framework	Правове регулювання, стандарти реагування, публічно-приватне партнерство	Середній; обмеження щодо передачі даних у міжнародні юрисдикції
Китай	Селективне впровадження з акцентом на національний контроль; Закон КНР про кібербезпеку 2017 р.; локалізація даних	Захист інформаційного простору, централізований контроль, обмеження доступу	Високий; домінування концепції цифрового суверенітету над міжнародною координацією
Україна	Адаптація стандартів ЄС, НАТО; Стратегія кібербезпеки України 2021 р.; створення CERT-UA, розбудова роботи НКЦК	Інституційна архітектура, стандарти реагування, координація з міжнародними структурами	Середній; баланс між прагненням до інтеграції та збереженням незалежного контролю

Джерело: складено на основі [14–25]

У довгостроковій перспективі глобальний кіберзахист може стати не лише технологічним викликом, а й ключовим простором формування нової форми міжнародної взаємодії – *цифрової дипломатії*. Це поняття охоплює не лише політичний діалог між державами щодо поведінки в кіберпросторі, але й системний підхід до налагодження довіри в умовах постійної технологічної турбулентності. Така дипломатія повинна спиратися на спільні цінності, дотримання прав людини у цифровому середовищі, прозорість алгоритмів і рівний доступ до цифрових благ, а не лише на інтереси державного суверенітету та оборонної доктрини.

Сьогодні в міжнародному дискурсі переважає тенденція до посилення технократії та національного контролю над цифровою інфраструктурою. Це, з одного боку, очікувана реакція на зростання кіберзагроз, кібершпигунства та цифрової дезінформації. Проте такий підхід обмежує потенціал до спільного вирішення глобальних викликів, оскільки створює замкнені ізольовані екосистеми. У цьому контексті стає особливо актуальним перехід від концепції національного техноконтролю до нової парадигми – цифрової етики та кіберсолідарності; йдеться про спільне вироблення стандартів цифрової поведінки, які ґрунтуються не на конкуренції чи стримуванні, а на взаємному визнанні прав, обов'язків та відповідальності держав, бізнесу та громадянського суспільства.

Цифрова дипломатія в цьому розумінні передбачає, що держави відмовляються від односторонніх

кібероперацій на користь колективної безпеки, обміну інформацією про загрози, узгодження стратегій реагування та створення інклюзивних майданчиків для обговорення стандартів штучного інтелекту, обробки даних та Інтернет-інфраструктури. Інституції ООН, GGE, OEWG, а також платформи рівня IGF або GFCE можуть стати ґрунтом для розвитку таких механізмів співпраці, де кожен стейкхолдер – від уряду до технологічного стартапу – має право голосу і доступ до формування рішень.

Особливе значення має розвиток концепції *цифрової солідарності*, яка означає підтримку менш розвинених країн у створенні власних кіберспроможностей. Це не лише питання технічної допомоги, а й справедливого доступу до захищених технологій, знань, стандартів безпеки. В рамках даного підходу кібербезпека не повинна бути привілеєм, доступним лише країнам з високим рівнем цифрової зрілості. Натомість кібербезпека має розглядатися як глобальне суспільне благо, що вимагає спільного фінансування, навчання кадрів і відкритого обміну технологіями. Крім того, у цифрову дипломатію повинна бути інтегрована складова *цифрової етики* – як у питаннях штучного інтелекту, так і щодо поведінки держав у кіберпросторі. Це передбачає створення моральних меж для використання кібертехнологій у військових конфліктах, уникнення цілеспрямованого впливу на цивільне населення та заборону цифрових атак на критичну інфраструктуру мирного часу. В підсумку, лише за умови поєднання дипломатичного діалогу, етичних стандартів, відкритості технологій і солідарної участі всіх сторін – глобальна система кіберзахисту може перейти від фрагментарної та реактивної моделі до зрілої інфраструктури колективної цифрової безпеки.

Висновки. Дослідження глобальних стратегій кібербезпеки дає змогу не лише окреслити домінантні аналітичні парадигми, а й глибше зрозуміти, як формується сучасна міжнародна система управління цифровим простором. У центрі цієї дискусії – пошук балансу між національним суверенітетом, інституційною інтеграцією та транснаціональним співробітництвом, що постає як один із ключових викликів у XXI ст.. Проаналізовані підходи – реалістичний, ліберальний, інституціоналістський та конструктивістський – відображають різні акценти в розумінні природи кіберзагроз і варіантів реагування на них. Реалісти наголошують на необхідності самозахисту, інституціоналісти – на ролі міжнародних структур, а конструктивісти підкреслюють, що загрози не менш соціально сконструйовані, ніж технічно реальні.

Аналіз нормативно-інституційної бази засвідчив, що міжнародна архітектура кіберрегулювання хоч і демонструє ознаки функціональної зрілості (через документи рівня Будапештської конвенції, NIS2, Cyber Resilience Act, ініціативи ENISA), однак лишається фрагментованою та вразливою до політичної поляризації. Це особливо помітно у випадках, коли цифровий суверенітет держав починає суперечити принципам відкритості, транскордонного обміну інформацією та гармонізації правил. Китай у цьому контексті виступає прикладом моделі, що надає перевагу централізованому контролю, тоді як ЄС і США, попри відмінності у підходах, усе ж таки тяжіють до побудови спільного кіберпростору з узгодженими стандартами й механізмами. На прикладі України простежується поступове впровадження глобальних стандартів із одночасною спробою зберегти стратегічну автономію в умовах воєнних викликів. Інституціональні новації – такі як створення CERT-UA, запровадження обміну інформацією про інциденти – є кроками на шляху до реальної інтеграції в євроатлантичну систему кіберзахисту.

У перспективі глобальний кіберзахист як стратегічна сфера має потенціал стати зразком нової багатосторонньої дипломатії – цифрової дипломатії, де замість односторонніх силових рішень домінуватиме культура діалогу, компромісу й технологічної солідарності. Така трансформація неможлива без переосмислення пріоритетів: від домінування концепції національного техноконтролю – до системного впровадження принципів цифрової етики, кіберсолідарності та загального доступу до безпечних технологій. Подальші дослідження будуть направлені на питання інституціоналізації кіберрегулювання в рамках міжнародного досвіду.

Література

1. Teoh C., Mahmood A. Cybersecurity workforce development for digital economy. *The Educational Review USA*. 2018. №2(1). P. 136–146.

2. Blažič J. B. Cybersecurity skills in EU: new educational concept for closing the missing workforce gap. *IntechOpen*. 2021. 18 p. DOI: 10.5772/intechopen.97094

3. Almuhammadi S., Alsaleh M. Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology Conference Proceedings (CS & IT)*. 2017. P. 51–62.

4. Influence of human factors on cyber security within healthcare organisations: a systematic review / Nifakos S., Chandramouli K., Nikolaou C., Papachristou P., Koch S., Panaousis E., Koch S., Panaousis E.,

Bonacina S. *Sensors*. 2021. №21(15). P. 5119.

5. Enhancing cybersecurity through cloud computing solutions in the United States / Hassan O., Fatai F., Aderibigbe O., Akinde A., Onasanya T., Sanusi M., Odukoya O. *Intelligent Information Management*. 2024. №16(04). P. 176–193.

6. Tanczer L., Brass I., Carr M. CSIRTs and global cybersecurity: how technical experts support science diplomacy. *Global Policy*. 2018. №9(S3). P. 60–66.

7. Çifci H., Özkoç E. Analysis of national cybersecurity strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*. 2025. №7. P. 1–16.

8. Онищенко С., Глушко А., Маслій О. Кіберстійкість як основа національної безпеки України. *Innovations and prospects of world science: Proceedings of XI International Scientific and Practical Conference*, Vancouver, Canada, 22-24 June 2022. Vancouver: Perfect Publishing, 2022. С. 551–556.

9. Бойко В., Василенко М., Кухаренко С. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави*. 2019. №3(27). С. 57–69.

10. Грубінко А. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. *Актуальні проблеми правознавства*. 2021. №1(25). С. 5–10.

11. Кузнєцов О. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. *Інформація і право*. 2021. №1(36). С. 106–113.

12. Pham H., Brennan L., Parker L., Phan-Le N., Ulhaq I., Nkhoma M., Nguyen M. Enhancing cyber security behavior: an internal social marketing approach. *Information and Computer Security*. 2019. №28(2). P. 133-159.

13. Odumesi J., Sanusi B. Achieving sustainable development goals from a cybersecurity perspective. *Advances in Multidisciplinary & Scientific Research Journal Publication*. 2023. №2(1). P. 1–10.

14. Convention on Cybercrime. 2001. *Council of Europe* : website. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (last accessed: 03.06.2025).

15. NIS Directive 2. 2023. *European Union Agency for Cybersecurity (ENISA)* : website. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2 (last accessed: 03.06.2025).

16. EU Cyber Resilience Act. 2024. *European Commission – Digital Strategy* : website. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (last accessed: 03.06.2025).

17. The National Cybersecurity Strategy. 2023. *The White House* : website. URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ (last accessed: 03.06.2025).

18. ENISA attempts to move NIS2 forward with NIS360 findings. 2025. *Nexus Connect* : website. URL: https://nexusconnect.io/articles/enisa-attempts-to-move-nis2-forward-with-nis360-findings (last accessed: 03.06.2025).

19. ENISA releases Cyber Stress Testing handbook to boost critical infrastructure resilience under NIS2 Directive. 2025. *Industrial Cyber* : website. URL: https://industrialcyber.co/reports/enisa-releases-cyber-stress-testing-handbook-to-boost-critical-infrastructure-resilience-under-nis2-directive/ (last accessed: 03.06.2025).

20. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). *Stanford DigiChina Project* : website. URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (last accessed: 03.06.2025).

21. Chinese Cybersecurity Law and Regulations: what you need to know. 2024. *China Legal Experts* : website. URL: https://www.chinalegalexperts.com/news/chinese-cybersecurity-law-and-regulations (last accessed: 03.06.2025).

22. Digital Sovereignty and International Law: the case of China's cybersecurity measures. 2024. *Vision Factory* : website. URL: https://www.visionfactory.org/post/digital-sovereignty-and-international-law-the-case-of-china-s-cybersecurity-measures (last accessed: 03.06.2025).

23. Стратегія кібербезпеки України. 2021. *Законодавство України* : веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 03.06.2025).

24. Ukraine Cybersecurity Governance Assessment. 2020. *DCAF – Geneva Centre for Security Sector Governance* : website. URL: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf (last accessed: 03.06.2025).

25. National Cybersecurity Governance: Ukraine. 2024. *CCDCOE* : website. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf (last accessed: 03.06.2025).

References

1. Teoh, C., & Mahmood, A. (2018). Cybersecurity workforce development for digital economy. *The Educational Review USA*, 2(1), 136–146. [In English].

2. Blažič, J. B. (2021). Cybersecurity skills in EU: new educational concept for closing the missing workforce gap. *IntechOpen*, 18. DOI: https://doi.org/10.5772/intechopen.97094 [In English].

3. Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology Conference Proceedings (CS & IT)*, 51–62. [In English].

4. Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: a systematic review. *Sensors*, 21(15), 5119. [In English].

5. Hassan, O., Fatai, F., Aderibigbe, O., Akinde, A., Onasanya, T., Sanusi, M., & Odukoya, O. (2024). Enhancing cybersecurity through cloud computing solutions in the United States. *Intelligent Information Management*, 16(04), 176–193. [In English].

6. Tanczer, L., Brass, I., & Carr, M. (2018). CSIRTs and global cybersecurity: how technical experts support science diplomacy. *Global Policy*, 9(S3), 60–66. [In English].

7. Çifci, H., & Özkoç, E. (2025). Analysis of national cybersecurity strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*, 7, 1–16. [In English].

8. Onishchenko, S., Hlushko, A., & Masliy, O. (2022). Kiberstiikist′ yak osnova natsional′noi bezpeky Ukrainy [Cyber resilience as the basis of Ukraine's national security]. *Innovations and prospects of world science: Proceedings of XI International Scientific and Practical Conference, Vancouver, Canada, 22–24 June 2022*, 551–556. [In Ukrainian].

9. Boiko, V., Vasylenko, M., & Kukharenko, S. (2019). Kiberbezpeka v YeS ta krainakh-chlenakh: henezys ta problemy yii pidvyshchennia [Cybersecurity in the EU and member states: genesis and problems of its improvement]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy – Human, Society and State Information Security*, 3(27), 57–69. [In Ukrainian].

10. Hrubinko, A. (2021). Osoblyvosti formuvannia polityky kiberbezpeky Yevropeiskoho Soiuzu: pravovi aspekty [Peculiarities of EU cybersecurity policy formation: legal aspects]. *Aktualni problemy pravoznavstva – Current Issues of Jurisprudence*, 1(25), 5–10. [In Ukrainian].

11. Kuznietsov, O. (2021). Yevropeiskyi dosvid posylennia spromozhnostei u sferi zabezpechennia kiberbezpeky v suchasnykh umovakh [European experience in strengthening cybersecurity capabilities in modern conditions]. *Informatsiia i pravo – Information and Law*, 1(36), 106–113. [In Ukrainian].

12. Pham, H., Brennan, L., Parker, L., Phan-Le, N., Ulhaq, I., Nkhoma, M., & Nguyen, M. (2019). Enhancing cyber security behavior: an internal social marketing approach. *Information and Computer Security*, 28(2), 133–159. [In English].

13. Odumesi, J., & Sanusi, B. (2023). Achieving sustainable development goals from a cybersecurity perspective. *Advances in Multidisciplinary & Scientific Research Journal Publication*, 2(1), 1–10. [In English].

14. Council of Europe. (2001). *Convention on Cybercrime*. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 [In English].

15. European Union Agency for Cybersecurity (ENISA). (2023). *NIS Directive 2*. Available at: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2 [In English].

16. European Commission. (2024). *EU Cyber Resilience Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act [In English].

17. The White House. (2023). *The National Cybersecurity Strategy*. Available at: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ [In English].

18. Nexus Connect. (2025). *ENISA attempts to move NIS2 forward with NIS360 findings*. Available at: https://nexusconnect.io/articles/enisa-attempts-to-move-nis2-forward-with-nis360-findings [In English].

19. Industrial Cyber. (2025). *ENISA releases Cyber Stress Testing handbook to boost critical infrastructure resilience under NIS2 Directive*. Available at: https://industrialcyber.co/reports/enisa-releases-cyber-stress-testing-handbook-to-boost-critical-infrastructure-resilience-under-nis2-directive/ [In English].

20. Stanford DigiChina Project. (2017). *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*. Available at: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ [In English].

21. China Legal Experts. (2024). *Chinese Cybersecurity Law and Regulations: what you need to know*. Available at: https://www.chinalegalexperts.com/news/chinese-cybersecurity-law-and-regulations [In English].

22. Vision Factory. (2024). *Digital Sovereignty and International Law: the case of China's cybersecurity measures*. Available at: https://www.visionfactory.org/post/digital-sovereignty-and-international-law-the-case-of-china-s-cybersecurity-measures [In English].

23. Zakonodavstvo Ukrainy. (2021). *Stratehiia kiberbezpeky Ukrainy [Cybersecurity Strategy of Ukraine]*. Available at: https://zakon.rada.gov.ua/laws/show/447/2021#n12 [In Ukrainian].

24. DCAF – Geneva Centre for Security Sector Governance. (2020). *Ukraine Cybersecurity Governance Assessment*. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf [In English].

25. CCDCOE. (2024). *National Cybersecurity Governance: Ukraine*. Available at: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf [In English].