

УДК 004.056.5:351.862:502.131.1

DOI <https://doi.org/10.24144/2788-6018.2025.06.2.67>

КІБЕРБЕЗПЕКА ДЕРЖАВИ ЯК ІНСТРУМЕНТ СТАЛОГО РОЗВИТКУ ЦИФРОВОГО СЕРЕДОВИЩА

Оксінь В.Ю.,

*доктор юридичних наук, професор,
професор кафедри публічного управління,
адміністрування та права
Національного університету
«Полтавська політехніка імені Юрія Кондратюка»
ORCID 0000-0001-6080-7752
e-mail: feup.oksin@nuppu.edu.ua*

Левченко Д.С.,

*PhD в галузі право,
старший викладач кафедри менеджменту
та інноваційного розвитку
Вищого навчального закладу
«Університет економіки та права «КРОК»
ORCID 0000-0001-8343-2260
e-mail: levchenkod@krok.edu.ua*

Костенко І.В.,

*кандидат юридичних наук,
науковий співробітник Науково-дослідного інституту д
ержавного будівництва та місцевого самоврядування
Національної академії правових наук України
ORCID 0000-0002-8784-5422
e-mail: inessakostenko2014@gmail.com*

Оксінь В.Ю., Левченко Д.С., Костенко І.В. Кібербезпека держави як інструмент сталого розвитку цифрового середовища.

Вказується, стала цифровізація – це зростаюча тенденція, в якій цифрові технології використовуються для сприяння екологічній, соціальній та економічній стійкості. У статті запропоновано авторське визначення поняття «кібербезпека» як стану та процесу забезпечення захищеності життєво важливих інтересів особи, суспільства та держави у цифровому просторі, що досягається шляхом поєднання технічних, правових і поведінкових механізмів, які спрямовані на запобігання, виявлення та нейтралізацію загроз, пов'язаних із функціонуванням інформаційно-комунікаційних систем, обігом даних та цифровими взаємодіями людей. Розкрито, що кібербезпека охоплює обов'язкові державні заходи примусового характеру, заходи публічного адміністрування, та добровільні заходи дотримання громадянами та організаціями встановлених норм і правил у кіберпросторі, забезпечуючи цілісність, доступність і конфіденційність інформації, стабільність суспільних відносин та сталий розвиток цифрового середовища.

Встановлено, що забезпечення кібербезпеки стає невід'ємним елементом гарантування національної безпеки, сталого розвитку та суспільної стабільності. Зростання кількості та складності кіберзагроз підсилює вразливість цифрового середовища, у якому держава здійснює свої функції. Кібератаки здатні паралізувати роботу стратегічних галузей, спричиняти економічні збитки, унеможливлювати надання життєво необхідних послуг населенню та створювати реальні ризики для життя і здоров'я людей. У цьому контексті кібербезпека безпосередньо впливає на суверенітет, стійкість управлінських процесів та здатність держави виконувати свої конституційні обов'язки.

Розкрито зв'язок між кібербезпекою та сталим розвитком. Визначено, що у цифрову епоху кібербезпека стає одним із ключових чинників, що визначають можливість суспільства рухатися шляхом сталого розвитку.

Підкреслюється, що кібербезпека держави є умовою безпечного і сталого функціонування цифрового суспільства, що забезпечує здатність держави до розвитку, гарантує захист громадян у мережевому середовищі та формує цифрову інфраструктуру майбутнього.

Ключові слова: безпека, загрози, захист, інформаційні технології, кіберзахист, оборона, сталий розвиток, цифрове суспільство, штучний інтелект.

Oksin V.Y., Levchenko D.S., Kostenko I.V. State cybersecurity as a tool for sustainable development of the digital environment.

It is stated that sustainable digitalization is a growing trend in which digital technologies are used to promote environmental, social and economic sustainability. The article proposes the author's definition of the concept of "cybersecurity" as a state and a process of ensuring the protection of the vital interests of individuals, society, and the state in the digital space, achieved through a combination of technical, legal, and behavioral mechanisms aimed at preventing, detecting, and neutralizing threats related to the functioning of information and communication systems, data circulation, and digital interactions between people. It is revealed that cybersecurity encompasses mandatory state coercive measures, public administration measures, and voluntary compliance by citizens and organizations with established norms and rules in cyberspace, ensuring the integrity, availability, and confidentiality of information, the stability of social relations, and the sustainable development of the digital environment.

It is established that ensuring cybersecurity is becoming an integral element of guaranteeing national security, sustainable development, and societal stability. The growth in the number and complexity of cyber threats increases the vulnerability of the digital environment in which the state performs its functions. Cyberattacks can paralyze the operation of strategic sectors, cause economic losses, render the provision of essential services to the population impossible, and create real risks to human life and health.

The connection between cybersecurity and sustainable development is clarified. It is determined that in the digital age, cybersecurity becomes one of the key factors determining society's ability to move along the path of sustainable development.

It is emphasized that the cybersecurity of the state is a prerequisite for the safe and sustainable functioning of the digital society, which ensures the state's capacity for development, guarantees the protection of citizens in the networked environment, and shapes the digital infrastructure of the future.

Key words: security, threats, protection, information technology, cyber security, defense, sustainable development, digital society, artificial intelligence.

Актуальність теми. Стала цифровізація – це зростаюча тенденція, в якій цифрові технології використовуються для сприяння екологічній, соціальній та економічній стійкості. Кіберзагрози можуть підірвати зусилля щодо сталого розвитку, призводячи до економічних та соціальних потрясінь. Тому важливо розглядати кібербезпеку як невід'ємний компонент сталої цифровізації [1, с. 270].

Забезпечення кібербезпеки в контексті глобальних загроз, поряд зі спільними зусиллями міжнародної спільноти, диктує важливість моніторингу на національному рівні. Україна, як і всі країни світу, постійно зазнає загрози від кібератак та час від часу стикаються з викликами кібербезпеки. Основні загрози національній кібербезпеці цих країн слід розглядати в контексті російської інформаційної та кібераагресії, зокрема, кібератак на життєво важливу інфраструктуру [3, с. 12].

Відповідно, важливість кібербезпеки є очевидною, особливо для українців в умовах повномасштабного вторгнення, тому різні бачення кібербезпеки дозволяють більш якісно гарантувати стан інформаційної захищеності держави.

Огляд останніх досліджень. Основою дослідження стали праці зарубіжних вчених S. Goswami, S. Sarkar, K. Gupta, S. Mondal, A. Bolatito, A. Ige, E. Kupa, O. Ilori, F. Morales-Sáenz, J. Medina-Quintero, M. Reyna-Castillo, M. Bay, G. Adamson. Окрім того, важливою складовою роботи склали праці українських вчених – А. Єріної, І. Гончар, С. Заєць, І. Сопілко, А. Шолойко, О. Баранова, Г. Форос, В. Жогова.

При цьому, наукових досліджень щодо кібербезпеки держави як інструменту сталого розвитку цифрового середовища, нині, на жаль, замало, адже тематика є порівняно новою та інноваційною.

Мета статті полягає в тому, щоб проаналізувати кібербезпеку держави як інструмент сталого розвитку цифрового середовища.

Методологія дослідження. У статті використано діалектичний метод для виявлення взаємозв'язку, взаємозумовленості та розвитку кібербезпеки й сталого розвитку в умовах цифровізації. Системний метод став основою для розгляду кібербезпеки як елемента цілісної системи сталого розвитку, що впливає на економічну, соціальну, екологічну та інституційну сфери. Логіко-правовий метод використано для аналізу поняття «кібербезпека». Аналіз і синтез стали основою для виокремлення ключових елементів кібербезпеки та сталого розвитку та узагальнення їх у цілісну концептуальну модель.

Виклад основних положень. Перетин кібербезпеки та сталого розвитку являє собою новий рубіж, який має вирішальне значення для досягнення Цілей сталого розвитку (ЦСР) [2]. Для початку, слід визначитися – що розуміється під поняттям «кібербезпека»? Слово «кібербезпека» широко використовують як термін для позначення захисту від шкідливого програмного забезпечення та хакерських атак. Його часто застосовують у ситуативному значенні: під атакою можуть перебувати підключені пристрої окремої людини, корпорація може зазнати злому, або державна, життєво важлива інфраструктура може бути під загрозою. Але видається, що широта самого терміна може ускладнювати дослідження теоретичних аспектів кібербезпеки [8]. Кібербезпека забезпечується і підтримується державно-примусовими заходами. Крім того, в більшості нормативних актів правоохоронної сфери законодавець використовує досліджувану категорію саме в такому контексті [11, с. 128-134]. Інша група вчених в своїх працях розглядає кібербезпеку у широкому сенсі. Їхнє бачення полягає в тому, що кібербезпека – це сукупність вольових суспільних відносин, що складаються в процесі свідомого і добровільного дотримання громадянами встановлених в нормах права та в інших нормах неюридичного характеру правил поведінки в кіберпросторі, і тим самим забезпечуються злагоджене, стійке, спільне життя людей в умовах розвинутого суспільства [11, с. 128-134].

Якщо проаналізувати позиції українських вчених, то А. Баранов вважає, що кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [10, с. 61].

У цьому ж спектрі висловлювалися різні точки зору вчених-юристів про структуру і співвідношення «кібербезпеки» та «інформаційної безпеки». Так, на думку деяких вчених, в категорію «інформаційна безпека» входить і «кібербезпека». Бачення Г.В. Форос, В.С. Жогов полягає в тому, що поняття кібербезпеки у вузькому сенсі може бути використано практичними працівниками для аналізу сфери правоохоронної діяльності, спрямованої на захист конституційних прав і свобод громадян, а саме при встановленні об'єкта протиправного посягання, що має практичне значення в роботі правоохоронних органів. У теорії ж адміністративного права оптимальним буде звернення вчених до поняття кібербезпеки в широкому сенсі, так як розуміння даного інституту саме в широкому сенсі є необхідною умовою не тільки для більш поглибленого його вивчення, а й розвитку його розуміння в теорії права [11, с. 128-134].

З урахуванням вищевикладеного, можна запропоновувати авторське поняття, зокрема, кібербезпека – це стан та процес забезпечення захищеності життєво важливих інтересів особи, суспільства та держави у цифровому просторі, що досягається шляхом поєднання технічних, правових і поведінкових механізмів, які спрямовані на запобігання, виявлення та нейтралізацію загроз, пов'язаних із функціонуванням інформаційно-комунікаційних систем, обігом даних та цифровими взаємодіями людей. Кібербезпека охоплює обов'язкові державні заходи примусового характеру, заходи публічного адміністрування, та добровільні заходи дотримання громадянами та організаціями встановлених норм і правил у кіберпросторі, забезпечуючи цілісність, доступність і конфіденційність інформації, стабільність суспільних відносин та сталий розвиток цифрового середовища.

Люди у XXI столітті значну частину свого життя взаємодіють у комунікації, опосередкованій технологіями. Вона стала окремим виміром людського існування, а після пандемії COVID-19 дедалі частіше проявляється у роботі, навчанні та дозвіллі. Якщо спробувати знайти значення цього комунікаційного феномена, то сукупність таких технологій можна описати як кіберпростір. Кіберпростір – це поєднання мас-медіа та технологій у новій формі. З його власними практиками, моделями поведінки й маніфестами, функціональний кіберпростір можна розглядати як глобальну основу людського існування так само, як чисте повітря чи відсутність пандемії. Хоча кіберпростір стійкий до тотального контролю, він водночас є вразливим і потребує захисту, якщо людство хоче користуватися його перевагами. Кібербезпеку можна розглядати як захист безпосередніх, практичних і постійно задіяних технологічних елементів. Однак для того, щоб захистити будь-яку частину кіберпростору, необхідно захистити весь кіберпростір [9].

Потреба у кібербезпеці виникає через кілька чинників, зокрема: – зростаюча залежність від цифрових технологій: Із постійним збільшенням використання цифрових технологій у повсякденному житті кібербезпека набуває дедалі більшої важливості для захисту від кіберзагроз, що можуть підірвати цілісність, конфіденційність та доступність цифрових активів; – поширення кіберзагроз: кіберзагрози стають дедалі складнішими, частішими та масовішими, що ускладнює захист від них; – захист чутливих даних: захист чутливої інформації, такої як персональні та фінансові дані, є критично важливим для запобігання викраденню особистості, шахрайству та іншим формам кі-

берзлочинності; – безперервність бізнесу: кібербезпека відіграє ключову роль у підтриманні безперервності бізнес-процесів, запобіганні збоєм в роботі та захисті від фінансових і репутаційних втрат; – захист інтелектуальної власності: інтелектуальна власність, така як комерційні таємниці та патенти, є важливою для успіху багатьох компаній. засоби кібербезпеки допомагають захистити цю інтелектуальну власність від крадіжок і несанкціонованого використання; – кібербезпека під час віддаленої роботи: зростання кількості працівників, які працюють дистанційно, робить кібербезпеку ще більш актуальною. віддалені співробітники можуть отримувати доступ до конфіденційних даних компанії з особистих пристроїв і мереж; – захист критичної інфраструктури: атаки на критичну інфраструктуру можуть спричинити значні економічні та соціальні потрясіння, тому необхідні надійні заходи кібербезпеки для захисту від таких загроз; – захист приватності: кібербезпека є важливою для захисту приватності особи, особливо в епоху великих даних. кіберзагрози можуть скомпрометувати персональну інформацію, таку як онлайн-активність чи дані про місцеперебування, що призводить до порушення приватності. Потреба у кібербезпеці виникає через зростаючу залежність від цифрових технологій, поширення кіберзагроз, необхідність захисту чутливих даних, забезпечення безперервності бізнесу, національної безпеки, дотримання нормативних вимог, захисту інтелектуальної власності, забезпечення безпеки під час віддаленої роботи, захисту критичної інфраструктури та приватності [1, с. 270–285].

Перетворення кіберпростору на вимір суспільного життя, зумовлює необхідність комплексної кібербезпеки для держави. Більшість сучасних держав (в тому числі, Україна) функціонують в умовах всеосяжної цифрової взаємозалежності, коли критичні інфраструктурні об'єкти, органи публічної влади, фінансово-економічні системи та базові соціальні сервіси пов'язані через мережі та інформаційно-комунікаційні технології. Саме тому забезпечення кібербезпеки стає невід'ємним елементом гарантування національної безпеки, сталого розвитку та суспільної стабільності. Зростання кількості та складності кіберзагроз підсилює вразливість цифрового середовища, у якому держава здійснює свої функції. Кібератаки здатні паралізувати роботу стратегічних галузей, спричиняти економічні збитки, унеможлиблювати надання життєво необхідних послуг населенню та створювати реальні ризики для життя і здоров'я людей. У цьому контексті кібербезпека безпосередньо впливає на суверенітет, стійкість управлінських процесів та здатність держави виконувати свої конституційні обов'язки. Суттєвою причиною необхідності кібербезпеки є захист інформації, яка становить цінність для держави (персональні дані громадян, державні реєстри, відомості оборонного значення, фінансові й стратегічні ресурси тощо), уразливість яких прямо впливає на ефективність публічного управління.

Останньою складовою дослідження має бути зв'язок між кібербезпекою та сталим розвитком. У документі ООН «Перетворення нашого світу: порядок денний у сфері сталого розвитку до 2030 року» 17 Цілей Сталого Розвитку (ЦСР) охоплюють багато видів безпеки, а саме соціальну (до прикладу, ЦСР 1. Подолання бідності), продовольчу (до прикладу, ЦСР 2. Подолання голоду), екологічну (до прикладу, ЦСР 6. Чиста вода та належні санітарні умови), економічну (до прикладу, ЦСР 8. Гідна праця та економічне зростання), воєнну (до прикладу ЦСР 16. Мир, справедливість та сильні інститути) [4; 5; 6, с. 43–52]. Водночас, в умовах цифровізації економіки зростає кількість кіберзагроз і кібератак, що шкодять кібербезпеці як індивідів, так і суб'єктів господарювання та державі загалом. Тоді як у вищезгаданому документі ООН не виокремлено кібербезпеку як окрему ЦСР в силу відсутності гостроти проблеми на той момент часу (2015 р.), оскільки суттєвий стрибок у цифровізації відбувся саме в період пандемії (з 2020 р.) [6, с. 43–52].

Збільшення використання інформаційних технологій створює виклик, що виникає через ризики та загрози комп'ютерній безпеці в усіх сферах суспільства. У цьому сенсі кібербезпека постає як важливий стовп підтримки захисту інфраструктур, необхідних для сталого економічного та соціального розвитку країн [7]. Заходи кібербезпеки захищають критичну інфраструктуру, персональні дані та підтримують цілісність цифрових систем, що лежать в основі економічного зростання, соціальної інклюзивності та екологічної стійкості. Інновації у сфері кібербезпеки, зокрема застосування технології блокчейн, а також інтеграція штучного інтелекту та машинного навчання, відкривають трансформаційний потенціал для підвищення цифрової безпеки та підтримки зусиль зі сталого розвитку в різних секторах. Майбутній ландшафт на перетині кібербезпеки та сталого розвитку позначений як викликами, так і можливостями. Новітні технології створюють нові вразливості та кіберзагрози, які можуть підірвати зусилля зі сталого розвитку. Однак ці технології також пропонують безпрецедентні можливості для посилення цифрової безпеки, підвищення стійкості та стимулювання інновацій. Інтеграція кібербезпеки в систему сталого розвитку є необхідною умовою для створення безпечного, резильєнтного та сталого майбутнього. Завдяки подоланню викликів і використанню можливостей, які створюють нові технології, зацікавлені сторони можуть посилити заходи кібербезпеки для підтримки досягнення Цілей сталого розвитку [2].

У цифрову епоху кібербезпека стає одним із ключових чинників, що визначають можливість суспільства рухатися шляхом сталого розвитку. Саме тому кібербезпека перетворюється на механізм забезпечення безперервності та надійності систем, які формують основу сталого розвитку. Кібербезпека підтримує економічну стійкість, захищаючи критичну інфраструктуру та інтелектуальні ресурси, що забезпечують інноваційне зростання. У сфері екології кібербезпека забезпечує коректність цифрового моніторингу і безпеку технологій, що керують ресурсами та природоохоронними системами. Для державних інституцій надійна кібербезпека означає більш захищений внутрішній оборонний стан, стабільність управління, прозорість процесів та довіру громадян.

Таким чином, у цифрову епоху кіберпростір став базовою інфраструктурою суспільного розвитку, а тому захист його цілісності перетворюється на ключову функцію держави. Кібербезпека є стратегічним інструментом забезпечення стійкості економіки, ефективності публічного управління та довіри громадян до цифрових сервісів. Зростання кіберзагроз, уразливість критично важливих систем і залежність держави від інформаційних технологій створюють новий формат ризиків, здатних підірвати соціальну стабільність, доступність базових послуг, а подекуди й національну безпеку. Відповідно, кібербезпека стає структурним елементом сталого розвитку, що забезпечує безперервність електронних сервісів, охорону персональних та державних даних, стійкість інфраструктури та безпечну інтеграцію інновацій.

Сучасні технології (штучний інтелект, блокчейн, великі дані тощо) створюють одночасно нові можливості та вразливості, тому держава повинна формувати цифрове середовище, у якому розвиток інновацій поєднується з високим рівнем захисту. Отже, кібербезпека держави є умовою безпечного і сталого функціонування цифрового суспільства, що забезпечує здатність держави до розвитку, гарантує захист громадян у мережевому середовищі та формує цифрову інфраструктуру майбутнього.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Goswami, S.S., Sarkar, S., Gupta, K.K., & Mondal, S. (2023). The role of cyber security in advancing sustainable digitalization: Opportunities and challenges. *Journal of Decision Analytics and Intelligent Computing*, 3(1), 270–285. DOI: <https://doi.org/10.31181/jdaic10018122023g>.
2. Adebimpe Bolatito, Adebimpe Bolatito Ige, Eseoghene Kupa, Oluwatosin Ilori (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Advanced Research and Reviews*. DOI: <https://doi.org/10.30574/gscarr.2024.19.3.0236>.
3. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation*, 17(3), 3–13. DOI: <https://doi.org/10.15407/scine17.03.003>.
4. Сопілко І. М. (2021) Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник Повітряне і космічне право. НАУ*. № 2(59). С. 110–115. DOI: <https://doi.org/10.18372/2307-9061.59.15603>.
5. Перетворення нашого світу: Порядок денний у сфері сталого розвитку до 2030 року. *ПРООН в Україні*. 2024. URL: <https://www.undp.org/uk/ukraine/publications/peretvorennya-nashoho-svitu-poryadok-dennyy-u-sferi-staloho-rozvytku-do-2030-roku>.
6. Шолойко А. (2023) Кібербезпека як нова Ціль Сталого Розвитку. *Digital Economy*. Issue III (91). С. 43–52. DOI: <http://doi.org/10.34025/2310-8185-2023-3.91.03>.
7. Morales-Sáenz, F.I., Medina-Quintero, J.M., & Reyna-Castillo, M. (2024). Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. *Sustainability*, 16(14), 5884. DOI: <https://doi.org/10.3390/su1614588>.
8. Morten Bay (2018). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal For Media Research*. n° 6/2016. URL: https://frenchjournalformediaresearch.com/lodel-1.0/main/docannexe/file/988/morten_pdf.pdf.
9. Adamson, G. (2021). Cybersecurity as the protection of cyberspace. 2021 *IEEE International Symposium on Technology and Society (ISTAS)*, 1–8. DOI: <https://doi.org/10.1109/ISTAS52410.2021.96291>.
10. Баранов О.А. (2014) Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. № 2(42)/2014. С. 54–62. URL: <https://ippi.org.ua/sites/default/files/14boavpk.pdf>.
11. Форос Г. В., Жогов В. С. (2019) Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. № 33. С. 128–134. URL: http://nbuv.gov.ua/UJRN/Prav_2019_33_20.