УДК 342.951:004.056
DOI https://doi.org/10.32782/2524-0374/2024-7/154

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ ТА ЕВОЛЮЦІЇ ПОНЯТТЯ КІБЕРБЕЗПЕКИ

THEORETICAL AND LEGAL PRINCIPLES OF THE FORMATION AND EVOLUTION OF THE CONCEPT OF CYBERSECURITY

Колесник О.О., аспірант
Науково-дослідний інститут публічного права

Метою статті є теоретико-правовий аналіз процесу становлення та еволюції поняття «кібербезпека», узагальнення основних наукових підходів до його визначення, з'ясування змісту й структурних елементів цієї категорії, а також окреслення засад її сучасного розуміння у правовій науці. У статті представлено комплексне теоретико-правове дослідження процесу становлення та розвитку концепту «кібербезпека» у вітчизняній і зарубіжній правовій доктрині. Простежено закономірності переходу від концепції інформаційної безпеки, зорієнтованої переважно на захист даних, інформаційно-комунікаційних систем і технічних засобів, до ширшого правового розуміння кібербезпеки як стану захищеності життєво важливих інтересів особи, суспільства і держави у цифровому середовищі. Розкрито основні етапи становлення категоріального апарату кібербезпеки, визначено співвідношення понять «кібербезпека», «кіберзахист», «інформаційна безпека», «кіберстійкість». Показано, що еволюція цих понять відбувалася під впливом глобалізаційних, технологічних і політико-правових чинників, а також у процесі інституціоналізації міжнародно-правових стандартів і розбудови національних систем безпеки. Особливу увагу приділено аналізу трансформації кібербезпеки з техніко-правової категорії у комплексне міждисциплінарне явище, яке охоплює правові, управлінські та соціотехнічні компоненти. Обґрунтовано, що сучасне розуміння кібербезпеки має спиратися на системний підхід, у межах якого вона постає не лише як стан захищеності, а й як процес безперервного управління ризиками, забезпечення кіберстійкості та відновлення функціональності цифрових систем. Зроблено висновок, що кібербезпека є невід'ємною складовою сучасної архітектури національної та міжнародної безпеки, а її ефективне правове забезпечення вимагає гармонізації термінологічного апарату, уніфікації базових категорій і послідовного поєднання правових, організаційних та технологічних засад у єдину систему безпеки цифрового суспільства. Окреслено методологічні засади й практичну вагу висновків для держполітики та освітніх стандартів у сфері кібербезпеки.

Ключові слова: кібербезпека, інформаційна безпека, кіберзахист, національна безпека, правове регулювання, цифровий суверенітет.

The purpose of the article is a theoretical and legal analysis of the process of formation and evolution of the concept of «cybersecurity», a generalization of the main scientific approaches to its definition, clarification of the content and structural elements of this category, as well as an outline of the principles of its modern understanding in legal science. The article provides an extensive theoretical and legal analysis of the formation and evolution of the concept of cybersecurity within both Ukrainian and international legal doctrines. It traces the transformation of this category from the earlier and narrower concept of information security–primarily focused on the protection of data, communication systems, and technical infrastructures–toward a multidimensional legal and political phenomenon that includes the protection of the vital interests of the individual, society, and the state in the digital environment. The study identifies and characterises the main stages in the doctrinal development of cybersecurity, emphasising the gradual integration of legal, administrative, and technological perspectives. Particular attention is paid to the transition from the information-centric paradigm, which is primarily oriented toward the confidentiality and integrity of data, to a systemic vision of cybersecurity as an integral part of national and international security policy. The author highlights the conceptual shift from perceiving cybersecurity as a state of protection to understanding it as a dynamic process of risk management and resilience, which incorporates mechanisms of prevention, detection, response, and recovery. The article substantiates the coexistence of three interrelated theoretical perspectives: cybersecurity as (1) a legal state of protection ensuring the stability of digital systems and infrastructures; (2) a continuous process of managing cyber risks and guaranteeing the functionality of digital governance; and (3) a legal and social regime of coordinated interaction between state, private, and individual actors in cyberspace. This multidimensional approach demonstrates that cybersecurity has evolved into an interdisciplinary field that unites legal regulation, governance mechanisms, and technical safeguards. Drawing on the works of Ukrainian and foreign scholars the research outlines how the concept of cybersecurity has been shaped by global digitalisation, the increasing complexity of cyberspace as a domain of social interaction, and the institutionalisation of international norms of responsible behaviour in cyberspace. The author concludes that effective cybersecurity governance requires the harmonisation of its theoretical and terminological foundations. The establishment of a unified conceptual framework would enhance the coherence of legal regulation, strengthen inter-agency interoperability, and ensure the integration of academic research, education, and practical policy implementation within the national cybersecurity system.

Key words: cybersecurity, information security, cyber defence, national security, legal regulation, digital sovereignty, cyber resilience, cyber policy.

Актуальність теми. Стрімка цифровізація суспільства, економіки, державного управління та воєнної сфери зумовила появу нової реальності – кіберпростору, що став середовищем розвитку як позитивних соціальних процесів, так і нових ризиків. Кібербезпека у цьому контексті перетворилася на ключовий фактор національної та міжнародної стабільності. Проте саме поняття «кібербезпека» залишається багатозначним: у науковому, технічному, правовому й управлінському дискурсах воно наповнюється різним змістом. Відсутність узгодженого теоретико-правового підґрунтя призводить до термінологічних розбіжностей, ускладнює правотворчу діяльність, формування освітніх стандартів і ефективну практику забезпечення безпеки у кіберпросторі. У цьому полягає сучасна наукова й прикладна проблема, що потребує системного осмислення генези та змісту поняття «кібербезпека».

Питання теоретико-правового змісту поняття «кібербезпека» привертає значну увагу вітчизняних і зарубіжних дослідників. В Україні вагомий внесок у формування наукових засад кібербезпеки зробили О. А. Алексєєва [1], Л. А. Арсенович [2], С. Горліченко [5], які зосереджують увагу на термінологічних і освітніх аспектах підготовки фахівців у цій сфері. О. А. Баранов [3], В. С. Павленко [14], Г. А. Гончаренко [6], Д. Федченко [17] досліджують правову природу кібербезпеки як складової системи національної безпеки. Б. А. Кормич [8], В. А. Ліпкан та О. С. Ліпкан [10], Є. В. Кубанов [9], С. В. Мельник [12; 13], Л. Веселова [4] формують теоретико-правові підходи до категоріального апарату, принципів і структури системи кіберзахисту.

Серед зарубіжних учених особливе місце посідають дослідження L. Floridi [23], який розробив концепцію етики інформаційного простору; J. Kosseff [31], котрий визначає предмет і межі права кібербезпеки; A. Klimburg [29], L. Kello [27; 28], а також праця, присвячена національній безпеці в кіберпросторі [33], які розкривають еволюцію безпеки в кіберпросторі як нового виміру міжнародних відносин; а також V. Tzavara і S. Vassiliadis

[35], які обґрунтували концепцію кіберстійкості як сучасного етапу розвитку доктрини кібербезпеки. Важливий історико-аналітичний вимір досліджень представлено в роботі K. Tarhan [34], присвяченій закономірностям розвитку кібербезпеки як міждисциплінарного напряму безпекознавства.

Водночас, попри значний науковий доробок, низка ключових аспектів залишається неврегульованою. Насамперед це стосується відсутності цілісного теоретико-правового бачення сутності кібербезпеки, її співвідношення з суміжними категоріями – «інформаційна безпека», «кіберзахист», «кіберстійкість» – та визначення меж правового регулювання у цій сфері. У сучасній науці простежується методологічна неоднорідність у трактуванні кібербезпеки – як стану захищеності (станоцентричний підхід), діяльності з управління ризиками (процесуальний підхід) чи суспільно-правового режиму (режимний підхід), що потребує подальшої теоретичної інтеграції та вироблення узгодженої доктринальної моделі поняття.

Метою статті є теоретико-правовий аналіз процесу становлення та еволюції поняття *«кібербезпека»*, узагальнення основних наукових підходів до його визначення, з'ясування змісту й структурних елементів цієї категорії, а також окреслення засад її сучасного розуміння у правовій науці.

Виклад основного матеріалу. 1. Витоки поняття: від «інформаційної безпеки» до «кібербезпеки»

Сучасне поняття «кібербезпека» має глибоке історико-доктринальне коріння й виростає з попередньої правової та управлінської парадигми «інформаційної безпеки», що в українській правовій науці 1990–2000-х років була базовою категорією системи національної безпеки. У її межах безпека розумілася насамперед як нормативно впорядкований стан захищеності інформації, інформаційних ресурсів та інфраструктури, а основний зміст зводився до забезпечення конфіденційності, цілісності й доступності даних та їх правової охорони засобами адміністративного, кримінального й спеціального законодавства [8;10].

Концепт інформаційної безпеки в цей період набував системності. Його структура включала три взаємопов'язані компоненти: правову регламентацію режимів інформації, організаційно-управлінські механізми безпеки (розмежування доступу, повноваження суб'єктів), а також технічні інструменти захисту (криптографію, захист каналів зв'язку) [8;10]. Українська доктрина послідовно формувала понятійний апарат через категорії «інформаційна безпека держави», «інформаційна політика», «інформаційна сфера», акцентуючи провідну роль держави як координатора, гаранта й арбітра в питаннях забезпечення безпеки інформаційних процесів [8;10].

Поступово, з розширенням цифрових комунікацій та виходом інформаційної взаємодії за межі національних юрисдикцій, у науковому дискурсі з'являється усвідомлення зовнішньополітичного виміру інформаційної безпеки, її інтегрованості у глобальні мережеві процеси. Саме ця тенденція створила передумови для виникнення ширшого, багатовимірного поняття –«кібербезпеки» [11].

Показово, що ще до нормативного закріплення цього терміна у Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII він почав входити у науковий обіг. Так, Л. В. Скрипник ще у 2013 році слушно зазначала, що поняття «кібербезпека» дозволяє поєднати технічний, правовий і соціальний аспекти захисту інформаційних систем, відображаючи реальну природу нових загроз – не лише технологічних, а й політичних та суспільних [15]. У цьому контексті її праця засвідчила раннє переосмислення проблеми безпеки – від охорони інформаційних масивів до забезпечення стабільності функціонування інформаційного середовища як складової державного управління.

Поступово правова наука почала фіксувати межі так званого «інформаційного підходу». По-перше, орієнтація лише на режим доступу до даних не охоплювала питання безперервності функціонування систем і послуг. По-друге, розвиток електронного урядування та цифрових сервісів вимагав оцінки не лише законності оброблення інформації, а й стійкості процесів надання публічних послуг [14]. По-третє, виникла необхідність міжвідомчої координації суб'єктів безпеки, що виходило за межі традиційного розуміння «інформаційної безпеки» [17]. У сукупності ці чинники спричинили еволюцію термінології – від «захисту інформації» до більш комплексного поняття «кібербезпека», яке охоплює не лише правовий режим даних, а й цілісність функціонування соціотехнічних систем [14; 17].

Важливу роль у доктринальному оформленні цієї трансформації відіграла праця Г. А. Гончаренка [6], у якій автор переконливо доводить, що «кібербезпека» не є тотожною «інформаційній безпеці», а має власну предметну сферу – забезпечення стійкості та стабільності цифрового простору як компонента національної безпеки держави. Учений показав, що поява терміну «кібербезпека» не заперечує попередні дефініції, а інтегрує їх у вищий рівень системного осмислення – як форми узгодження правових, технічних і управлінських засобів у єдиній сфері національної політики безпеки.

Таким чином, у вітчизняній науці поступово утверджується трикутна модель розуміння кібербезпеки:

– як стану захищеності – результату реалізації норм, стандартів і заходів;

– як процесу управління ризиками – циклу запобігання, виявлення, реагування та відновлення;

– як суспільного режиму взаємодії суб'єктів у цифровому просторі, що визначає правила поведінки й відповідальність [3; 12; 17].

Паралельно у світовій науковій думці відбувається аналогічна зміна парадигми. У працях Л. Келло, А. Клімбурга та інших дослідників наголошується, що феномен «кіберреволюції» створив новий вимір глобальної безпеки, у якому порушення стабільності цифрових систем може мати наслідки, співмірні з традиційними воєнними або економічними кризами [27; 28; 29]. Відтак поняття «кібербезпека» починає асоціюватися не лише з охороною інформації, а й з підтриманням стійкості (resilience) систем, їх здатності до адаптації, збереження критичних функцій і відновлення після інцидентів [14; 17].

Українська наукова школа органічно інтегрувала ці підходи, розвиваючи ідею комплексної моделі безпеки, у якій поєднуються правові, організаційні та технологічні засоби забезпечення стабільності цифрових систем. Зокрема, дослідники наголошують на ролі системності, міжвідомчої координації та ризик-менеджменту як ключових принципів побудови національної системи кібербезпеки [3].

Змістовним каталізатором подальшої еволюції поняття стала поява категорії критичної інфраструктури (КІ) та її правове осмислення. Включення до кола об'єктів енергетики, транспорту, зв'язку, фінансових установ, охорони здоров'я та інших сфер життєзабезпечення суспільства призвело до усвідомлення, що предметом кібербезпеки є не лише дані, а передусім спроможність систем безперервно виконувати свої функції [1; 7]. Як слушно зазначається в працях О. Алексєєвої та М. Коваліва, для критичної інфраструктури ключовим стає не запобігання порушенню доступу, а підтримання оперативної здатності до відновлення й стабільного функціонування після інцидентів [1; 7].

Це, своєю чергою, зумовило уточнення об'єктів і меж кібербезпеки – від охорони інформації до захищеності процесів надання послуг, технологічного управління та комунікаційних систем. У сучасній українській право-

вій доктрині кібербезпека постає як багаторівнева категорія, що поєднує стан, процес і спроможність до відновлення, формуючи цілісну модель функціональної безпеки цифрового суспільства [3].

2. Еволюційні етапи розвитку поняття кібербезпеки в науці

Перші наукові спроби осмислення феноменів, які сьогодні об'єднуються поняттям кібербезпеки, сягають кінця XX – початку XXI ст., коли формується теоретична категорія cyberspace. У цей час наукова увага поступово зміщується від суто технічних аспектів функціонування комп'ютерних мереж до аналізу їхніх політико-правових наслідків. На тлі стрімкої експансії Інтернету й електронних комунікацій дослідники починають розглядати cyberspace як нову форму соціальної взаємодії, позбавлену чітких територіальних меж і традиційних юрисдикційних рамок.

Однією з перших фундаментальних праць цього етапу стала монографія Lucas Kello Cyber Legalism: Why It Fails and What to Do, побудована на матеріалах досліджень 2000-х років. Автор переконливо показав, що правові моделі, сформовані для фізичного простору, втрачають ефективність у віртуальному середовищі. Її теза про те, що «реалії кіберпростору» руйнують традиційні інститути територіальності, державного контролю та класичної юрисдикції, стала відправною точкою для становлення окремого напряму – cyber law, який згодом еволюціонував у галузь cybersecurity law [18].

Питання нової «доменності» та суб'єктності кіберпростору порушує L. Kello у статті The Meaning of the Cyber Revolution: Perils to Theory and Statecraft [27]. Учений доводить, що поява кіберпростору трансформувала уявлення про силу, загрозу і безпеку у міжнародних відносинах: межі між миром та конфліктом стали розмитими, а кібератаки – новою формою впливу, що не вписується у класичні правові категорії збройного нападу чи державного суверенітету. У цьому контексті кібербезпека постає не технічним, а політико-правовим феноменом, тісно пов'язаним із забезпеченням державності.

Розвиток доктрини міжнародного права в кіберпросторі відбувався передусім у межах американської правової школи. H. Koh у праці International Law in Cyberspace [30] наголошував, що міжнародне право не втрачає чинності у цифровому середовищі, проте потребує адаптації до нових акторів – корпорацій, приватних структур та навіть окремих осіб, здатних впливати на безпеку держав. Саме ці дискусії 2000–2010-х рр. сформували методологічне підґрунтя сучасного розуміння кібербезпеки як багаторівневого явища, що інтегрує технологічні, політичні та правові складові.

У 2010-х роках відбувається інституціоналізація терміна cybersecurity в офіційних міжнародних документах, національних стратегіях і академічних дослідженнях. Зміст поняття розширюється – від технічного захисту інформаційних систем до комплексної безпеки соціотехнічних мереж, у яких поєднуються технологічні, організаційні та людські фактори.

У цьому контексті особливого значення набуває концепція інформаційної етики L. Floridi, викладена у монографії The Ethics of Information [23]. Учений запропонував бачення інформаційного буття (infosphere) як морального простору, де кожен суб'єкт несе відповідальність за власні дії. Ця концепція заклала філософсько-етичний фундамент для формування правової доктрини кібербезпеки, орієнтованої не лише на технічний захист, а й на цінності довіри, справедливості та відповідальності .

Політичну та стратегічну рамку феномена поглиблює A. Klimburg у праці The Darkening Web: The War for Cyberspace [29]. Автор обґрунтовує, що боротьба за контроль над кіберпростором стала новою формою геополітичного протистояння, у якому перетинаються інтереси держав, бізнесу та громадянського суспільства. Він закликає до формування глобальної системи управління кібербезпекою, заснованої на принципах відкритості та спільної відповідальності.

Юридичну інституціоналізацію категорії розвиває J. Kosseff у статті Defining Cybersecurity Law [31] , де запропоновано трактування кібербезпеки як комплексного правового режиму, що інтегрує кримінальне, адміністративне, інформаційне та міжнародне право. Учений окреслює три взаємопов'язані виміри: запобігання загрозам, реагування на інциденти та відповідальність за шкоду, завдану у цифровому просторі. Саме в цей період кібербезпека набуває статусу самостійного предмета дослідження у правознавстві, політиці та етиці технологій.

У 2020-х роках дослідження кібербезпеки переходять до нової фази – акцент зміщується з «захищеності» на стійкість (resilience) соціотехнічних систем, тобто здатність не лише протидіяти загрозам, а й відновлювати функціонування після інцидентів. V. Tzavara та S. Vassiliadis у статті Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review простежують становлення цього поняття від стратегій НАТО та ЄС до сучасного розуміння як ключового елементу кібербезпеки [35]. Автори доводять, що стійкість системи ґрунтується на взаємозалежності технологічних, організаційних і людських чинників, а отже, кібербезпека має бути спрямована на адаптацію, навчання й відновлення.

Схожих висновків доходить K. Tarhan у статті Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies, де виокремлено три хвилі розвитку кібербезпеки: технічну (1990–2000-ті рр.), політико-правову (2010-ті) та соціальну (після 2020 р.), у межах якої головний акцент робиться на людському факторі, довірі, цифровому суверенітеті та спільному управлінні кіберпростором. На думку автора, сучасна кібербезпека – це міждисциплінарна сфера, що інтегрує елементи національної безпеки, права, етики, соціології та інженерії [34] .

Водночас у цей же період у центр академічних дискусій виходить феномен публічної атрибуції кіберінцидентів – тобто визначення суб'єкта, відповідального за конкретні кібератаки. Florian J Egloff у статті Public Attribution of Cyber Intrusions [20] наголошує, що публічне приписування дій стало інструментом стратегічної комунікації держав, проте створює ризики політичних маніпуляцій і помилкових звинувачень. M. Finnemore та D. Hollis у статті Beyond Naming and Shaming: Accusations and International Law in Cybersecurity підкреслюють, що такі публічні обвинувачення формують нові норми поведінки у міжнародному співтоваристві, навіть за відсутності чітких юридичних механізмів [22].

Таким чином, на початку 2020-х років поняття кібербезпеки досягає рівня теоретичної зрілості. Його зміст визначають ключові категорії resilience (стійкість), trust (довіра), accountability (відповідальність) та public attribution (публічна атрибуція), що засвідчують перехід від інженерно-технічної до соціально-правової парадигми. Кібербезпека перетворюється на цілісну систему, у якій технологічна надійність поєднується з етичною відповідальністю та правовою регламентованістю [20; 22].

3. Теоретико-правові підходи до сутності кібербезпеки

3.1. Кібербезпека як стан захищеності. У вихідній для вітчизняної доктрини інтерпретації кібербезпека постає як стан нормативно забезпеченої захищеності інформаційних систем, ресурсів та суб'єктів від зовнішніх і внутрішніх загроз. Саме таку, «станоцентричну», парадигму послідовно обґрунтовує О. Баранов, визначаючи кібербезпеку як стан захищеності життєво важливих інтересів особи, суспільства і держави у сфері використання інформаційних технологій; у його підході результат (досягнута стабільність функціонування) виступає центральним крите-

рієм правової оцінки [3]. Ця логіка знаходить підтримку і в роботі В. Павленка, який наголошує: кібербезпека має конститутивну природу правового стану – такого, що забезпечує недопущення несанкціонованих впливів на інформаційні ресурси та процеси й тим самим вписується у систему базових правових категорій «безпеки» поряд із громадською, національною та економічною [14]. Таке трактування дозволяє чітко окреслити нормативну мету й легітимні орієнтири публічної політики безпеки, однак водночас схильне до станоцентричності.

Справедлива у цьому контексті критика В. Стеця: зведення кібербезпеки лише до «стану» породжує ілюзію незмінності, тоді як кіберпростір є динамічним середовищем із постійно мінливим набором загроз і акторів [16]. Звідси висновок: «станоцентричне» тлумачення – важливе для фіксації правових гарантій та індикаторів належного стану, однак недостатнє як аналітична модель сучасних механізмів забезпечення безпеки.

3.2. Кібербезпека як процес і діяльність з управління ризиками. Еволюція доктрини закономірно веде до процесуального бачення кібербезпеки як безперервного управління ризиками за повним циклом: запобігання – виявлення – реагування – відновлення. Саме на це звертає увагу С. Горліченко: ефективна безпека вимагає не стільки «консервації» досягнутого стану, скільки формування компетентностей прогнозування загроз, оперативного інцидент-менеджменту та відновлення працездатності систем; відповідно, освітні стандарти мають віддзеркалювати логіку ризик-орієнтованого циклу [5].

У цьому ж ключі Є. Кубанов послідовно трактує кібербезпеку як інструмент публічного управління, що реалізується через організацію моніторингу, оцінювання загроз та ухвалення управлінських рішень; ефективність у такій моделі визначається не формальним масивом актів, а спроможністю інституцій діяти в режимі оперативного реагування [9]. С. Мельник, досліджуючи концептуально-категоріальний апарат професійної підготовки, підкреслює діяльнісний вимір: кібербезпека – це система знань, навичок і дій, спрямованих на забезпечення стабільного функціонування ІКТ, причому єдність теоретичного (нормативного) та практичного (процедурного) рівнів є умовою адекватного понятійного апарату [12; 13]. Л. Арсенович, узагальнюючи потреби органів державної влади, акцентує на єдиній методології підготовки кадрів як управлінського процесу, що інтегрує правові, організаційні та технічні аспекти [2].

Узагальнюючи, процесуальний підхід фіксує динамічну природу кібербезпеки: її зміст розкривається через процедури виявлення та зниження ризиків, підтримання безперервності, оперативне відновлення, а також постінцидентне навчання систем і організацій.

3.3. Кібербезпека як суспільно-правовий режим. Поглиблення міждисциплінарних досліджень висвітлює ще один – режимний – вимір: кібербезпека як суспільно-правовий режим узгодженої поведінки держави, бізнесу та громадян у цифровому середовищі. Л. Веселова, формулюючи «адміністративно-правову парадигму кібернетичної безпеки», пропонує бачити в ній наслідок упорядкування публічно-владних відносин, де термінологічний консенсус і міжсекторальна координація стають передумовами єдиного правового режиму кіберзахисту [4].

На міжнародному рівні режимний підхід набуває форми нормотворення поведінки (behavioural norm-setting). D. Broeders і F. Cristiano показують роль «м'якого права» і політик, що структурують очікування та практики держав і приватних суб'єктів без обов'язкової кодифікації [19]. M. Finnemore і D. Hollis демонструють, що міжнародні норми кіберповедінки конструюються в процесі взаємодії держав, корпорацій і експертних спільнот та функціонують як механізми узгодження очікувань у відсутність повної формалізації [21]. Водночас A. Grigsby слушно застерігає: дефіцит спільних правил у кіберпросторі підвищує ризики ескалації конфліктів і підриває довіру [24]. У межах цього ж напряму M. Raymond окреслює «режимний комплекс» децентралізованого врядування, де множинні актори виробляють робочі правила через практики координації та обміну інформацією [32].

У підсумку режимна перспектива фіксує те, що поза правовими нормами і технічними стандартами кібербезпека тримається на узгодженості практик і довірі між суб'єктами, а також на *ex ante* запобіжниках відповідальної поведінки.

3.4. Кібербезпека і кіберстійкість: від «абсолютної захищеності» до спроможності відновлення. На сучасному етапі ключовим є перехід від орієнтації на «абсолютну захищеність» до концепції кіберстійкості (cyber resilience) – здатності систем адаптуватися, підтримувати критичні функції та відновлюватися після інцидентів. У ґрунтовному історико-концептуальному огляді V. Tzavara та S. Vassiliadis показано, що resilience сформувалася як логічне продовження еволюції поняття кібербезпеки: у динамічному середовищі повної безпечності не існує, отже, критерієм стає життєздатність системи в умовах невизначеності [35]. K. Tarhan, синтезуючи розвиток галузі, фіксує зсув від парадигми «захисту від ризику» до управління стійкістю, де визначальними є взаємозалежність технологічних, організаційних і людських факторів та готовність до адаптації [34].

Це не заперечує «станового» та «процесуального» підходів, а інтегрує їх: стан (як нормативна мета) і процес (як інструмент досягнення) доповнюються характеристикою спроможності до відновлення – здатності вчитись на інцидентах, удосконалювати процедури та зменшувати кумулятивну вразливість систем. У правовому вимірі це означає зміщення акцентів від ексклюзивного запобігання до регуляторної підтримки безперервності (continuity), обов'язковості планів реагування й відновлення, стандартів інцидент-менеджменту та прозорих механізмів звітності [34; 35].

4. Термінологічні проблеми та шляхи їх подолання

У сучасній правовій науці та практиці публічного управління у сфері кібербезпеки спостерігається стійка термінологічна багатоманітність, яка часто набуває колізійного характеру. Вона проявляється щонайменше на трьох рівнях: міжгалузевому, міжмовному та інституційному.

По-перше, міжгалузеві колізії зумовлені різними методологічними оптиками права, інженерних наук і менеджменту. Юридична доктрина традиційно схильна фіксувати кібербезпеку як «стан захищеності» – нормативно визначений результат дотримання гарантій безпеки. Таке «станоцентричне» розуміння послідовно обґрунтовує О. Баранов, який акцентує на доцільності закріплення кібербезпеки як складника системи національної безпеки у формі стану забезпечення захищеності життєво важливих інтересів особи, суспільства і держави у сфері використання інформаційних технологій [3]. У такий спосіб формується стабільний правовий орієнтир, проте він схильний до статичності та не повною мірою враховує динаміку загроз.

Натомість у суміжних сферах – технічній, управлінській, освітній – центр ваги зміщується до процесуальної логіки: управління ризиками, готовність до інцидентів і відновлення спроможностей. С. Горліченко переконливо підкреслює, що сучасна кібербезпека має розумітися як безперервний процес функціонування і розвитку систем захисту; відповідно, оновлення термінологічного апарату та навчальних стандартів має відображати повний цикл «запобігання – виявлення – реагування – відновлення» [5]. У результаті «станоцентричне» і «процесуальне» тлумачення співіснують, породжуючи семантичну напругу між правом і практикою.

По-друге, міжмовні колізії зумовлені особливостями перекладу та відмінними семантичними традиціями. Зокрема, терміни *cybersecurity*, *information security*, *information assurance*, *resilience* далеко не завжди мають усталені відповідники й межі в українській мові. Л. Веселова справедливо ставить вимогу «термінологічного консенсусу» – уніфікованої системи понять, що інтегрує юридичні, управлінські та технічні компоненти державної політики у сфері кіберзахисту [4]. Без такого узгодження правозастосування неминуче стикається з тлумачними розривами, які підривають єдність адміністративно-правової парадигми.

По-третє, інституційні колізії випливають із фрагментарної регламентації на відомчому рівні. Є. Кубанов показує, що в системі публічного управління циркулюють різноспрямовані відомчі документи, де ключові дефініції подані неоднаково, залежно від функціональної ролі суб'єкта, що породжує інформаційні розриви між секторами та ускладнює міжвідомчу координацію [9]. Додатково освітній вимір проблеми артикулює С. Мельник: за відсутності цілісного концептуально-категоріального апарату підготовка фахівців втрачає єдину методологію, а засвоєння вузькотехнічних термінів відбувається без належного правового наповнення. Цей дисбаланс посилюється розсинхронізацією державних стандартів із сучасними категоріями міжнародних документів і технічних регламентів [12; 13].

Нарешті, системність проблеми підтверджує міждисциплінарний огляд S. Henrico та D. Putter: багатозначність компонента *cyber* є універсальним викликом –ним позначають і простір, і технологію, і стан, і діяльність, що неминуче множить тлумачення та ускладнює міждисциплінарну взаємодію [25].

Інтероперабельність термінів як практична вимога. У сфері міжнародного та безпекового співробітництва термінологічна точність має операційне, а не лише лінгвістичне значення. Дослідження R. Janczewski, G. Pilarski та M. Marczyk демонструє, що відсутність єдиного словника у НАТО істотно ускладнює інтероперабельність у кібероперація: різночитання понять *cyber defence*, *cyber incident*, *information assurance* веде до відмінних пріоритетів планування, різних порогів класифікації інцидентів і несумісних процедур реагування [26]. Звідси – очевидний нормативно-прикладний висновок: термінологічна інтероперабельність є передумовою ефективної взаємодії спільних структур і чинником довіри між партнерами; її досягнення потребує інституційного механізму постійної координації та періодичної ревізії глосаріїв, що синхронізує правову, технічну та політичну термінологію [26].

Висновки. Усвідомлення глибинного характеру термінологічних проблем у сфері кібербезпеки зумовлює необхідність їхнього комплексного теоретико-правового осмислення та вироблення єдиних засад понятійного апарату. Системність і послідовність у вживанні базових категорій становлять основу для формування зрілої правової доктрини, здатної забезпечити єдність державної політики, освітніх стандартів і наукового дискурсу [1; 3; 6; 8].

По-перше, ключовим завданням є уніфікація основних понять, що вже мають усталене використання в академічній і освітній літературі. Дослідники наголошують, що такі категорії, як *«кіберінцидент», «ризик», «стійкість», «вразливість», «критична послуга»*, повинні мати короткі, юридично узгоджені визначення, доповнені технічними та управлінськими відповідниками [2; 5; 12]. Це створить цілісну термінологічну основу, придатну для використання на всіх рівнях правового регулювання й практичного застосування.

По-друге, доцільним є формування міждисциплінарних таблиць відповідників термінів, що відображатимуть функціональний зміст понять у правовій, технічній і управлінській площинах. Такий підхід сприятиме усуненню відомчих розбіжностей та забезпечить комунікаційну єдність між секторами державного управління [9; 12; 13].

По-третє, формування термінологічної системи має спиратися на принципи однозначності, відтворюваності, технологічної нейтральності та ієрархічності. Зазначені засади узгоджуються з концепцією «термінологічного консенсусу», обґрунтованою у працях із адміністративно-правового забезпечення кібербезпеки [4; 16].

По-четверте, особливого значення набуває освітня інтеграція термінологічних стандартів. Єдиний глосарій має бути закріплений у державних стандартах підготовки фахівців органів публічної влади, у програмах закладів вищої освіти та системі підвищення кваліфікації [2; 5; 12]. Це забезпечить методологічну єдність і сприятиме формуванню висококваліфікованого кадрового потенціалу у сфері кібербезпеки.

По-п'яте, важливим напрямом подальшого розвитку є запровадження механізму постійної ревізії термінологічної бази з урахуванням міжнародного досвіду. Практика НАТО демонструє ефективність регулярного оновлення глосаріїв за участю представників науки, освіти, державних і приватних інституцій [26]. Такий підхід забезпечує актуальність термінів і їх відповідність технологічній динаміці.

Проведене дослідження підтверджує, що якість і внутрішня узгодженість термінологічної системи є визначальним чинником ефективності правового регулювання у сфері кібербезпеки [3; 6; 9]. Без гармонізації понять неможливо забезпечити єдність законодавства, координацію управлінських механізмів і результативну взаємодію суб'єктів на національному та міжнародному рівнях.

Термінологічна гармонізація має розглядатися не як технічна процедура, а як системоутворювальний елемент правового забезпечення кібербезпеки. Подолання семантичних розривів між правом, технікою та освітою стане запорукою узгодженості державної політики, ефективного управління ризиками та повноцінної інтеграції України у глобальний простір кібербезпеки.

ЛІТЕРАТУРА

1. Алексєєва О. А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури: понятійний апарат. *Інформація і право*. 2023. № 4. С. 168–176.

2. Арсенович Л. А. Понятійно-категоріальний апарат у сфері підготовки фахівців із кібербезпеки органів державної влади України. *Наукові перспективи*. 2022. № 2. С. 33–53.

3. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2(42). С. 54–62.

4. Веселова Л. Понятійно-термінологічний аппарат у системі адміністративно-правового забезпечення кібербезпеки. *Scientific Journal of Public and Private Law*. 2019. № 5(1). С. 138–143.

5. Горліченко С. Особливості сучасного понятійно-термінологічного апарату у сфері підготовки фахівців з кібербезпеки. *Кібербезпека: освіта, наука, техніка.* 2024. № 3(23). С. 171–181.

6. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «кібербезпека» в системі національної безпеки: теоретико-правовий аспект. *Journal of the Academy of Legal Sciences of Uzhhorod University*. 2024. № 5. С. 112–120.

7. Ковалів М., Скриньковський Р., Назар Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki.* 2021. № 3(3). С. 65–73.

8. Кормич Б. А. Правові та організаційні засади політики інформаційної безпеки України : дис. … д-ра юрид. наук : 12.00.07. Одеса : Нац. ун-т «Одеська юридична академія», 2004. 420 с.

9. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Аспекти публічного управління.* 2018. № 6(10). С. 37–46.

10. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. – 2-ге вид., доп. і перероб. Київ : Текст, 2008. 400 с.

11. Лук'янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки. *Гілея: науковий вісник*. 2013. № 72. С. 793–796.

12. Мельник С. В. Концептуально-категоріальний апарат у системі професійної підготовки майбутніх фахівців з інформаційної та кібербезпеки. *Інформаційні технології і засоби навчання*. 2016. Т. 55, № 5. С. 187–197.

13. Мельник С. В., Тихомиров О. О., Лєсков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Збірник наукових праць Київського національного університету імені Тараса Шевченка.* 2011. Вип. 30. С. 165–172.

14. Павленко В. С. Сутність кібербезпеки у теорії інформаційного права. *Право та державне управління*. 2021. № 2(47). С. 28–33.

15. Скрипник Л. В. Щодо кібербезпеки. *СТСЗИ*. 2013. Вип. 2(24). С. 126–130.

16. Стець В. Теоретико-правові проблеми визначення кібербезпеки. *Український журнал прикладних наук URAN*. 2019. Том 4 № 80. С. 24–28.

17. Федченко Д. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Юридичні Науки.* 2018. № 5(57). С. 653–658.

18. Lucas Kello, Cyber Legalism: Why It Fails and What to Do. – *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab014, URL: https://doi.org/10.1093/cybsec/tyab014

19. Broeders, Dennis and Cristiano, Fabio, Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road (April 2, 2020). Available at SSRN. URL: http://dx.doi.org/10.2139/ssrn.3819171

20. Florian J Egloff, Public attribution of cyber intrusions, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020. URL: https://doi.org/10.1093/cybsec/tyaa012

21. Finnemore M.; Hollis D. B. Constructing Norms for Global Cybersecurity. The American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425- 479 Published by: American Society of International Law Stable URL: http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425

22. Finnemore, Martha and Hollis, Duncan B., Beyond Naming and Shaming: Accusations and International Law in Cybersecurity (March 6, 2019). European Journal of International Law (forthcoming 2020), Temple University Legal Studies Research Paper No. 2019-14, Available at SSRN. http://dx.doi.org/10.2139/ssrn.3347958.

23. Floridi, Luciano, *The Ethics of Information* (Oxford, 2013; online edn, Oxford Academic, 23 Jan. 2014). URL: https://doi.org/10.1093/acprof:oso/9780199641321.001.0001

24. Grigsby A. The End of Cyber Norms. *Survival*. 2017. Vol. 59, No. 6. P. 109–122. URL: https://doi.org/10.1080/00396338.2017.1399730

25. Henrico, S., & Putter, D. (2025). Cyber What???-a Systematic Review. *Journal of Applied Security Research*, 2025. pp. 1–34. URL: https://doi.org/10.1080/19361610.2025.2544184

26. Janczewski R.; Pilarski G.; Marczyk M. Terminology as a barrier to NATO's interoperability in cyberspace operations. *Knowledge-Based Organization*. 2019. Vol. 25, No. 3. P. 31–35. URL: https://doi.org/10.2478/kbo-2019-0113.

27. Kello L. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*. 2013. Vol. 38, No. 2. P. 7–40. URL: https://doi.org/10.1162/ISEC_a_00138.

28. Kello L. The Virtual Weapon and International Order. New Haven : Yale University Press, 2017. 328 p.

29. Klimburg A. The Darkening Web: The War for Cyberspace. Updated ed. – New York : Penguin Books, 2021. 384 p.

30. Koh H. H. International Law in Cyberspace. *Harvard International Law Journal.* 2012. Vol. 54 (Online Symposium). P. 1–12.

31. Kosseff J. Defining Cybersecurity Law. *Iowa Law Review*. 2018. Vol. 103, No. 3. P. 985–1035.

32. Raymond M. Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot. *Strategic Studies Quarterly*. 2016. Vol. 10, No. 4. P. 123–149.

33. Patron, B. (2013). Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Http Dx https://doi.org/10108013523260 2013 776801.

34. Tarhan K. Historical development of cybersecurity studies: a literature review and its place in security studies. *Przegląd Strategiczny*. 2022. Issue 15. P. 327–345. URL: https://doi.org/10.14746/ps.2022.1.23

35. Tzavara, V., Vassiliadis, S. Tracing the evolution of cyber resilience: a historical and conceptual review. *Int. J. Inf. Secur.* 23, 2024. pp. 1695–1719. URL: https://doi.org/10.1007/s10207-023-00811-x