УДК 340.12.
DOI: https://doi.org/10.21564/2663-5704.66.337965

Трофименко Володимир Анатолійович, кандидат юридичних наук, доцент, доцент кафедри філософії, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: v.a.trofymenko@nlu.edu.ua
ORCID ID: 0000-0003-2240-3727

КІБЕРПРОСТІР: ДО ПРОБЛЕМИ ВРЕГУЛЮВАННЯ

Публікацію присвячено проблемі врегулювання кіберпростору. Ускладненість врегулювання на загальному рівні привела до того, що більше швидко іде регулювання окремих його сфер: економіки тощо. Також стверджується, що правові інститути, що існують, уже не є здатними створити ефективний механізм регуляції. У зв'язку з цим наукова спільнота пропонує створити особливі механізми регулювання, які базуються на правовій та технологічній основі кіберпростору.

Ключові слова: *кіберпростір, кібербезпека, громадянське суспільство, кіберфізичний простір, індустріальне громадянство, цифровізація.*

Постановка проблеми. Швидке та всеосяжне розростання кіберпростору приводить до того, що його ключові учасники – регулятори, зокрема держава, не встигають реагувати на нові виклики. Традиційні підходи до регулювання суспільних відносин та соціальних інститутів уже не спроможні врахувати новітні тенденції в мережі та технологічні особливості кіберпростору. На перший план виходять ті проблеми, що поза Інтернетом вважались вирішеними, наприклад анонімність, відсутність кордонів тощо.

Незважаючи на вже досить тривалий час існування кіберпростору також залишається відкритим питання поведінки ключових суб'єктів. Більше того, достеменно не визначений головний регулятор цієї сфери, хоча традиційно таким вважається держава, але близькі технологічні можливості вже можуть мати і приватні структури, а сама держава не має юрисдикції поза географічним кордоном. Окрема держава вже не спроможна врегулювати те нове, що виникає, а міжнародні інститути часто стикаються навіть із бойкотуванням процесу регулювання з боку деяких країн. Таким чином, регулювання кіберпростору вже виходить за межі державного правового кола та повинно стати синтезом міжнародного права, технологій та багатовимірності мережі.

Невирішеність фундаментальних питань регулювання кіберпростору, всеосяжне розширення інтернету екстраполюється на низку галузевих про-

блем окремих сфер кіберпростору. Такої точки зору дотримується й італійський дослідник Л. Мартіно. Кіберпростір, пише він, став ключовим елементом політичної, соціальної, фінансової та індивідуальної діяльності. Інформаційно-комунікаційні технології (ІКТ) покращили людську взаємодію та зробили внесок у «переосмислення» класичних концепцій, таких як політична участь, політичні дебати, прийняття рішень. Однак їхній всеохопний, всюдисущий характер та їхнє дедалі більше використання в політичних і військових цілях створює значні ризики для міжнародного миру, стабільності й безпеки. Низькі бар'єри для доступу до можливостей ІКТ, швидкість технологічного прогресу та складність середовища кіберпростору з огляду на традиційні юридичні визначення кордонів поставили перед державами (головними учасниками міжнародних відносин) нові виклики, такі як невід'ємна складність точного визначення причин кібератак. Саме ця складність і часте наполягання сторін приписувати кібератаки та інциденти «поза розумним сумнівом» дає можливість заперечувати відповідальність і зірвати спроби побудувати довіру та політичні стосунки в кіберпросторі. Дослідник вважає необхідним аналіз того, як кіберпростір впливає на міжнародну політику. Природа теми, на його думку, диктує використання якісного аналізу первинних і вторинних джерел, таких як офіційні звіти, декларації та політичні документи, а також академічний аналіз, щоб зрозуміти вплив і динаміку кібердомену на класичні концепції, такі як війна, мир і міжнародні відносини. Основна ідея вченого полягає в тому, що розвиток інформаційно-комунікаційних технологій (ІКТ) і пов'язана з цим еволюція воєнних дій спричинили відповідний вплив на динаміку сучасної міжнародної системи, підкреслюючи водночас як мілітаризація кіберсфери вплинула на міжнародну безпеку, мир і стабільність. Проте, констатує науковець, відсутність конкретних досліджень, пов'язаних із «впливом кіберпростору на міжнародну політику», підкреслює необхідність приділяти більше уваги цій темі, маючи на увазі, що більш широкий і тривалий аналіз динаміки кіберпростору може дати політикам можливість підвищити обізнаність щодо кіберзагроз, щоб керувати проблемами, які виникають у цифровій сфері [1].

Зважаючи на викладене, дослідження як загальних, так і галузевих питань кіберпростору залишається актуальним напрямком наукових розробок.

Аналіз останніх досліджень та публікацій. Однією з ключових проблем стосовно кіберпростору є проблема його врегулювання. Необхідність управління кіберпростором підкреслює американський вчений Грейман В. Одним із найбільших геополітичних викликів у XXI ст., вважає американський автор, буде боротьба за контроль над кіберпростором, п'ятою сферою кібервійни після землі, моря, повітря та космосу, а також головним економічним викли-

ком часу. З розвитком штучного інтелекту, інтернету речей, автономних транспортних засобів і безпілотних дронів ця проблема стає ще більшою. Дослідник за допомогою емпіричних доказів досліджує взаємодію між трьома силами, які формують кіберрозвідку та міжнародну безпеку: глобалізмом, регіоналізмом і націоналізмом. Останнім часом, на його думку, світова політика породила відчуття терміновості щодо нового світового порядку й того, що це означає для кібербезпеки та сфери кіберпростору. З огляду на нещодавні кібератаки, спрямовані на американську політичну систему, Міністерство закордонних справ Чеської Республіки, уряд Хорватії, а також атаки 2017 р. на кіберсистеми, якими керує український уряд, існує занепокоєння щодо стабільності глобального зв'язку та потенціалу зменшення глобальних кордонів. Автор стверджує, що занепокоєння щодо глобальної стабільності породжує питання про те, хто контролює кіберпростір і хто несе відповідальність, коли щось іде не так. Як висновок американський дослідник просуває концепцію кіберуправління для кращого контролю кібербезпеки урядами, міжурядовими організаціями та приватним сектором [2].

Нормативізація (правове регулювання) є основною темою наукових досліджень і британського науковця Н. Цагуріаса. У своїй статті він пише, що ситуація навколо врегулювання відносин у кіберпросторі демонструє: держави мають сумніви щодо застосовності до кіберпростору правил, що містяться в Талліннському посібнику[1]. Практика після Таллінна показує, що держави розглядають застосування міжнародного права до кібероперацій як необов'язкове; діють у паралельних правових і неправових напрямках поведінки; і беруть участь у поступовому застосуванні. Така ситуація запрошує до подальших досліджень наслідків поведінки держави в кіберпросторі для загальної теорії міжнародного права. Автор використовує цей останній пункт як трамплін для пояснення необхідності процесу нормативізації в кіберпросторі, тобто процесу підпорядкування кібероперацій і поведінки держав правовим стандартам. Для цього він скористався уявленням Оскара Шахтера про нормативний (правовий) порядок у вигляді триповерхової будівлі. Відповідно до цієї метафори, третій поверх займають суспільні цінності та загальні політичні прагнення; другий поверх займає право з його характерними нормативними моделями приписування, заборони й застосування; тоді як перший поверх займає соціальна реальність поведінки. Три поверхи не ізольовані, а з'єднані ескалаторами та сходами, які йдуть в обох напрямках [3]. Цій

[1] Талліннське керівництво, також відоме як «Талліннський посібник» або «Талліннський посібник з міжнародного права щодо кібервійн», – це незобов'язуюче академічне дослідження, що розглядає застосування міжнародного права до кіберконфліктів. URL: https://www.google.com/search?client=opera&q=талліннське+керівництво&sourceid=opera&ie=UTF-8&oe=UTF-8.

же проблемі врегулювання відносин у кіберпросторі на міжнародному рівні приділяє увагу китайський дослідник Дж. Ванг. Кіберпростір, пише він, відкритий і працює через кордони. Швидка інтеграція кіберпростору в життя людини вимагає регулювання його функціонування. Питання в тому, які правила можуть керувати кіберпростором. Автор стверджує, що звіти Експертної групи ООН з цієї проблематики чітко показують: серед міжнародної спільноти існує консенсус щодо того, що кіберпростір підпадає під дію міжнародного права, включаючи Статут ООН. У ньому також стверджується, що угоди, досягнуті державами на регіональному та двосторонньому рівнях, міжнародне звичаєве право та існуючі правила міжнародних організацій, таких як Світова організація торгівлі (СОТ), складають сукупність правил управління кіберпростором. Згідно з відповідними рішеннями Міжнародного суду (ICJ) і висновками Комісії міжнародного права (ILC) щодо ідентифікації звичаєвого міжнародного права, автор вважає, що звичайні норми, застосовні до кіберпростору, можуть бути створені через практику держав-користувачів як спеціальні норми звичаєвого міжнародного права, і що практика інтернет-компаній і організацій, незважаючи на їх необов'язковий характер для держав, може сприяти підтвердженню існування таких звичайних норм [4]. Стосовно міжнародного врегулювання відносин у кіберпросторі цікавою є думка ізраїльських вчених Н. Хассида та Е. Матанії. Вони розглядають теоретичні основи міжнародної безпеки та теорію режимів, які встановлюють суворі умови для створення міжнародних режимів, щоб пояснити природу кіберконфлікту та причини, які перешкоджають створенню глобального режиму кібербезпеки. У цій статті аналізуються занепокоєння та інтереси кібербезпеки провідних світових держав у кіберпросторі – Китаю, Європейського Союзу та Сполучених Штатів – на основі деяких ключових проблем кібербезпеки, які є предметом суперечки, серед іншого інформаційного суверенітету, мілітаризації кіберпростору та їхньої політики кібернорм. Вчені стверджують, що відсутність домінуючого гегемона в міжнародній системі та сприйняття кіберпростору не лише як сфери, що збільшує вразливість і загрози, але й як царини для отримання стратегічної переваги, не відповідає теоретичним передумовам для створення міжнародного режиму [5].

Сьогодні пропонуються і різні режими регулювання кіберпростору. На цю проблему звертає увагу японський дослідник П. Чачавалпонгпан. Свої пропозиції він розглядає на прикладі Таїланду. Він пише, що в розпал протестів 2020 р. уряд Таїланду запровадив жорстку онлайн-цензуру, щоб приборкати публічну критику монархії. При цьому уряд посилався на своє зобов'язання захищати «кібернетичний суверенітет» Таїланду. Автор стверджує, що ця концепція побудована як інструмент, який можна використову-

вати опортуністично для забезпечення безпеки режиму, яка значною мірою залежить від безпеки трону. Примітно, що державна конструкція кіберсуверенітету Таїланду, на думку вченого, побудована на основі територіального суверенітету: він має елементи територіальної нації, оскільки кіберпростір розглядається так, ніби він фізично існує. Однак така концептуалізація кіберсуверенітету є хибною, вважає дослідник: вона усуває значні відмінності між цими двома формами суверенітету, зокрема щодо суверенної влади та її меж. Незважаючи на всю помилковість, науковець вважає, що справа з Таїландом є частиною більш широкої поточної дискусії про кіберсуверенітет, згідно з якою одні країни просувають жорсткіший контроль за інтернетом, а інші підтримують більш ліберальний кіберрежим [6]. Однією з головних причин такого підходу є існування кіберпримусу. Цю проблему порушує американський вчений К. Ходгсон. За останнє десятиріччя кіберпростір, пише він, став темою популярних, політичних і наукових дискусій, від найвищих урядових кіл до кіноекрану. Держави борються з тим, як протистояти наростанню хвилі кіберзагроз для їхніх економік, особистої інформації їхніх громадян і все більше для політичної та соціальної єдності. Держави використовують кіберпотенціал як інструмент державного управління для досягнення політичних цілей. Вчений розглядає, як держави використовують кіберможливості, щоб примусити інших заради політичних цілей. Кіберпримус визначається ним як використання кіберможливостей, щоб змусити опонента виконати дію, яку він зазвичай не хотів би виконувати, і уникнути небажаного результату. Думка вченого спрямована на вирішення проблеми: як держава може використовувати кіберпотенціал, щоб змусити іншу державу (або недержавного актора) задовольнити свої амбіції; як може мати місце кіберпримус; а також способи, за допомогою яких Сполучені Штати та їхні партнери можуть розпізнавати, реагувати на спроби кіберпримусу та протистояти їм. Як приклад вчений розглядає використання кібероперацій Північною Кореєю та Росією в останні роки як частину їхніх більш широких стратегій впливу на своїх сусідів, показуючи, наскільки контекст, у якому відбуваються такі операції, є критично важливим [7].

Незважаючи на досить велику кількість наукових публікацій, проблема регулювання кіберпростору на міжнародному рівні залишається відкритою.

Формулювання мети. Метою роботи є показ того, що неврегульованість кіберпростору на загальному рівні не є перепоною для регулювання його окремих сфер.

Викладення основного матеріалу. Неврегульованість проблеми кіберпростору на міжнародному рівні не заважає державі втручатися в окремі його галузі. Прикладом може слугувати економіка.

На необхідність сприяння розвитку економіки в кіберпросторі звертає увагу американський вчений Дж. Вецнер. Він зазначає, що унікальний серед основних засобів комунікації інтернет приніс величезну суспільну користь, будучи спроєктованим, розробленим і розгорнутим переважно завдяки приватній ініціативі та неурядовому фінансуванню. У той же час, зазначає автор, ключові державно-політичні рішення були прийняті на ранньому етапі, які створили правові та нормативні основи, необхідні для процвітання економічних інновацій і свободи слова. Ці основи включають надійний захист свободи слова, обмеження відповідальності на інтернет-платформах, захист від надмірного державного стеження, відкриті технічні стандарти, захист конфіденційності особи та певну форму мережевого нейтралітету. Ці основи були закладені, коли інтернет був молодим. Але, стверджує вчений, оскільки діловий, соціальний і технічний вплив інтернету стає все більш очевидним у всьому світі, деякі з цих принципів потребують коригування, але всі залишатимуться важливими, якщо ми хочемо зберегти економічний потенціал інтернет-середовища в майбутньому [8].

Європеїзації цифрової економіки присвячено публікацію італійського дослідника А. Ренди. За останні три десятиріччя, відмічає він, кіберпростір поступово став двигуном нестійких результатів з економічної, соціальної та екологічної точок зору. Європейська комісія запустила кілька нових ініціатив, намагаючись відновити громадський контроль над кіберпростором, виправити розподільний дисбаланс, спричинений розвитком великомасштабних цифрових платформ, і сприяти цифровому суверенітету Європи. У документі стверджується, що ЄС зможе досягти бажаних цілей, лише впроваджуючи правила та цінності в «код» і зберігаючи відкритість до решти світу. На його думку, поточні ініціативи, такі як стратегія обробки даних, регулювання штучного інтелекту, закон про цифрові послуги та Європейська федерація хмарних технологій, здаються все ще надто рідкісними та нескоординованими, щоб справді реалізувати прагнення Європи стати лідером у світі щодо сталого використання технологій [9].

Однією з головних проблем кіберпростору залишається кібербезпека, зокрема і в економічній сфері. На це звертає увагу американський вчений М. Ходгінс, беручи за приклад США. Кібербезпека, пише він, є головним питанням політики США, і значна коаліція виступає за посилення державного втручання через передбачувані інформаційні проблеми. Більшість пропозицій, на його думку, не оцінюють, чи справді припис покращує передачу відповідних знань і належним чином спрямовує мотивацію на створення соціально оптимальної кібербезпеки. Насправді, вважає науковець, проблеми зі знаннями та стимулами, пов’язані з регуляторними режимами, можуть

поставити під загрозу здатність ринку до інновацій, що є критично важливим через динаміку кіберпростору. Неправильні політичні приписи, невизначеність режиму, процедурна жорсткість, збільшення бар'єрів для входу та спотворені стимули є одними з головних загроз для підприємництва на ринку кібербезпеки від державного втручання [10].

Покращенню результатів кібербезпеки може допомогти впровадження механізму соціального радару, вважає колектив китайський вчених Л. Фан, Ч. Зенг, Ю. Ванг та ін. На тлі безпеки кіберпростору, яка стає глобальною увагою, розвиток глобалізації інформації та розвідки, пишуть вони, вимагає поглибленого дослідження соціального радара. Це може допомогти краще розуміти та реагувати на складну суспільну динаміку більш розумно та чутливо. Соціальний радар, як здатність уважно спостерігати й інтерпретувати цю інформацію, на думку китайських вчених, допомагає краще розуміти суспільні тенденції, культурну еволюцію та міжособистісні взаємодії. Ця чутливість має вирішальне значення для своєчасного розуміння суспільних змін і прогнозування тенденцій. Вчені звертають увагу, що під час «арабської весни» 2010 р. соціальні медіа відіграли вирішальну роль у стимулюванні руху, що призвело до широкомасштабних жорстоких конфліктів, які мали значний вплив як на суспільство, так і на економіку. Ця подія знову представила соціальний радар як сервісну платформу, засновану на соціальних мережах. Він спрямований на використання модулів виявлення розширення ключових слів та інструментів аналізу настроїв, щоб узагальнити конкретні соціальні інформаційні панелі. Отримані результати допомагають владі планувати «стратегії контролю ризиків», видавати попередження підприємствам або урядам і відстежувати несподівані випадки. Дослідження соціального радара, вважають вчені, надають надійну підтримку, щоб краще адаптуватися до технологічних змін і керувати ними, дозволяючи чітко сприймати пульс суспільного розвитку та приймати мудріші рішення [11].

Підвищенню ефективності кібербезпеки допоможе впровадження поняття кіберфізичного простору. Таку думку висловлюють китайські вчені Х. Рьоджин, К. Лейлей та Х. Вечанг. Вони зазначають, що з розвитком технології взаємодії людини з комп'ютером концепція простору постійно розширюється. Оскільки технології продовжують упроваджуватися в повсякденне життя, межі між фізичним світом і кіберпростором стираються. Автори розглядають це складне середовище як кіберфізичний простір, який не тільки тісно пов'язаний із зовнішнім фізичним світом, але також має характеристики технології, віртуальності та незалежності. На їхню думку, на безпекову поведінку людини в кіберфізичному просторі впливатиме більше факторів у різних середовищах, оскільки вони відбуваються паралельно в двох просторах. Тому

в цій новій соціально-технічній системі потрібно переглянути, як керувати та допомагати людям у безпеці. У своїй статті дослідники зосереджуються на поведінці безпеки в кіберфізичному просторі та дослідницькому питанні про те, як надати допомогу для цього. З одного боку, розглядаються характеристики середовища, тобто кіберфізичний простір є продуктом технологічного розвитку. З іншого боку, на поведінку людини впливають її власні психологічні особливості та обмежена раціональність, тому характеристики суб'єкта поведінки також розглядаються. Починаючи з техніко-психологічної та техніко-економічної точки зору, науковці пропонують змінювати мотивацію, змінювати здібності, забезпечувати відповідні тригери або використовувати упередження людей щодо статусу-кво, упередження регресивного неприйняття, соціальний вплив для сприяння безпечній поведінці людини на основі технології переконання та теорії спонукання [12].

Ефективності кібербезпеки сприяє й ідентифікація суб'єктів кібератак. Цю проблему порушує американський вчений К. Ейсенхер. Автор пише, що наявність кібератак вимагає ідентифікації тих, хто відповідальний за погані дії, включно з державами, і точне приписування є вирішальним предикатом у таких різноманітних контекстах, як кримінальні звинувачення, суперечки щодо страхового покриття та кібервійни. Але складна технічна сторона приписування є лише попередником дуже суперечливих правових і політичних питань про те, коли і як звинувачувати уряди у відповідальності за кібератаки. Хоча політика може значною мірою визначати, чи будуть оприлюднені приписи, у своєму дослідженні вчений стверджує, що коли кібератаки публічно приписуються державам, такі приписи повинні регулюватися правовими стандартами.

Замість того, щоб блокувати розроблення стандартів доказів для приписування, як зараз роблять Сполучені Штати, Франція, Нідерланди та Великобританія, дослідник вимагає встановити вимогу міжнародного права про те, що публічні приписи повинні включати достатні докази для перехресної перевірки або підтвердження звинувачень. Цей функціонально визначений стандарт використовує як урядові, так і неурядові можливості атрибуції, щоб пролити світло на діяльність держав у кіберпросторі, а розуміння державної практики є необхідною передумовою для встановлення норм і звичаєвого міжнародного права для регулювання поведінки держави. Крім того, встановлення чіткого доказового стандарту для приписування кібератак потенційно може прояснити неврегульовані наразі загальні норми міжнародного права щодо доказів.

Компанії та аналітичні центри, продовжує науковець, нещодавно зробили кілька пропозицій щодо створення міжнародної організації, яка займатиметься приписуванням кібератак, спонсорованих державою. Незважаючи на те,

що ці пропозиції містять багато рекомендацій, дослідник згоден, що така організація повинна доповнювати, а не замінювати поточну децентралізовану систему атрибуції. Наявність безлічі авторів – як урядових, так і неурядових – збільшує ймовірність того, що публічні авторства слугуватимуть цілям, яких прагнуть досягти автори, а саме зміцнення захисту, стримування атак, покращення стабільності та уникнення конфліктів у кіберпросторі [13].

Варто відмітити, що не всі дослідники впевнені в можливостях міжнародного права регулювати кіберпростір. Такої позиції дотримується й американський вчений Н. Катагірі. У своїх дослідженнях він відповідає, чому міжнародне право та норми не змогли зберегти мир у кіберпросторі. Проблема виникає, на його думку, здебільшого через їхню неспроможність вирішити те, що недержавні актори, такі як окремі хакери та технологічні фірми, роблять у кіберпросторі. Міжнародне право, створене завдяки широкому внеску державних службовців десятиріччя тому, зосереджуючись на державах як головних суб'єктах міжнародної політики, не відповідає домінуванню недержавних акторів як фактичних операторів кіберпростору. Критична проблема міжнародного права та інституцій щодо відсутності «зубів» для покарання за недержавне насильство поширюється і на кіберпростір. У результаті недотримання міжнародного права, підкреслює науковець, стало практично можливим і навіть підштовхнуло приватний сектор, особливо великі технологічні фірми, утвердитися в правовій порожнечі, використовувати свої цифрові продукти для зміни норм і стати нормальними підприємцями в бізнесі цифрового захисту. Однак розмноження нормальних підприємців прискорилося неузгоджено, і те, як вони вибудували свої інтереси, не зовсім узгоджується з інтересами держави. Хоча деякі норми поведінки в кіберпросторі були прийняті, багато інших залишаються оскарженими. Тим часом, робить висновок вчений, дискурс норм на дипломатичних майданчиках, у тому числі під час багатосторонніх дебатів в Організації Об'єднаних Націй, став украй недемократичним, де домінує невелика суміш великих держав і активних середніх держав, які також є розділеними щодо того, які норми мають керувати державною та недержавною поведінкою [14]. Схожу позицію має інший американський дослідник – В. Грейман. Головоломка атрибуції, пише дослідник, уже давно є проблемою в кіберпросторі, де актори можуть таємно займатися своїми справами, не боячись помсти чи відплати. Виявлення осіб, відповідальних за кібератаки, є величезним викликом, хоча політика зазвичай визначає, чи будуть оприлюднені приписи. Коли і як звинувачувати уряди в кіберзлочинності, кібершпигунстві чи навіть акті кібервійни, це критичне питання для зменшення кіберконфліктів і заохочення кіберспівробітництва. Немає жодного міжнародного правового зобов'язання розкривати підстави, на яких ґрунту-

ється приписування, перш ніж вжити відповідних заходів. Держави також не зобов'язані надавати докази приписування, коли реагують на кібервторгнення іншої держави. Вчений визнає, що міжнародне звичаєве право не розробило набору розуміння чи визнаної державної практики щодо того, який рівень приписування є прийнятним або необхідним для встановлення відповідальності держави за дії в кіберпросторі [15]. Близька до попередніх позиція британського дослідника Л. Келло. Західні країни, на його думку, стикаються з кричущою проблемою покарання в кіберсфері. Неодноразово інші країни атакують їхні політичні та економічні інтереси. Західні лідери неодноразово попереджають про серйозність таких дій. І все ж неодноразово жертвам не вдавалося покарати, щоб стримати кривдників. Вчений розглядає цю ситуацію і намагається вирішити, чому та як вона виникла і що з нею робити. Західний підхід до запобігання кіберконфліктам, зазначає науковець, наголошує на центральній ролі існуючого міжнародного права та норм. Проте нормативно-правова база для цього не є адекватною, оскільки не дає достатніх підстав для достовірного реагування на дії, що не відповідають війні. Отже, західний підхід зазнав вражаючої невдачі. Він не в змозі зрозуміти головну істину про сучасні питання безпеки: значна частина сучасного міждержавного суперництва не відповідає ні руйнівним критеріям війни, ні прийнятним межам мирного суперництва. Швидше, це конфлікт або суперництво середнього спектра, яке завдає більшої шкоди, ніж традиційна діяльність у мирний час, але не є фізичним насильством, як війна. Країни, продовжує британський дослідник, використовують кіберпростір для досягнення деяких політичних і стратегічних цілей війни, не стріляючи з жодної зброї. Відсутність ефективної відповіді Заходу свідчить не про толерантність до агресії, а про неспроможність розробити стратегію відповіді, відповідну юридичній і доктринальній двозначності немиру. Існуюче право і норми є джерелом проблеми, а не її вирішенням. Автор пропонує своє бачення вирішення поставленої проблеми: проміжне рішення має бути знайдено в розробленні нової доктрини – у стратегії консеквенціалізму, яка впливає на матеріальні інтереси супротивників, щоб стримувати дії, які міжнародне право та стратегія безпеки зазвичай не визнають такими, що заслуговують на сильну відповідь [16].

Проблемі низького рівня кібербезпеки стосовно громадян приділяють свою увагу британські вчені Л. Колес-Кемп, Д. Ашенден та К. Охара. Уряд і постачальники технологій, зазначають вони, роблять припущення щодо владних відносин, які визначають використання засобів контролю технологічної безпеки та норм, за якими відбувається використання технологій. Автори представляють тематичне дослідження, проведене на північному сході Англії, у якому вивчалося, як спільнота може працювати разом, використовуючи

платформу обміну цифровою інформацією, щоб реагувати на тиск зміни політики соціального забезпечення. Вчені описують індуктивний розгляд цього дуже локального прикладу, перш ніж переглядати його в світлі ширшої теорії безпеки. Застосовуючи цей підхід, вони проблематизують тенденцію держави зосереджуватися на безпеці технологій за рахунок безпеки громадян. З огляду на розуміння конкретного випадку та подальшого огляду літератури науковці роблять висновок, що існують три основні недоліки, які не враховано в поточних проєктах архітектури кібербезпеки. Це відсутність: консенсусу щодо того, про чию безпеку йдеться, доказів еквівалентності між механізмами, які контролюють поведінку, та двосторонньої зрозумілості. Вчені стверджують, що, усунувши ці недоліки, можна побудувати основи довіри та співпраці, необхідні для ефективної кібербезпеки, а дизайн архітектури кібербезпеки та дизайн супутніх послуг має значний вплив на суспільний договір між громадянином і державою. Розгляд цієї нової перспективи проявляє нові напрямки для розуміння ефективності технологій кібербезпеки [17].

Впливу кіберпростору на громадянське суспільство в цілому присвячено роботу норвезьких вчених Дж. Кастіли та К. Пурсьонена. У статті досліджується вплив появи кіберпростору або цифровізації на громадянське суспільство та розробляється аналітична основа для цього. Автори розрізняють чотири типи громадянського суспільства: аполітичне, політичне, транснаціональне та негромадянське. Кожен тип громадянського суспільства розглядається окремо порівняно з розвитком кіберпростору, щоб зрозуміти, яке громадянське суспільство посилюється цими розробками і, навпаки, яке громадянське суспільство є обмеженим. Це розуміння, на думку авторів, допомагає зрозуміти, як кіберпростір змінив більш загальні відносини між суспільством і державою. Хоча можна визначити багато інструментальних змін і розвитку в практиках громадянського суспільства, у статті вченими робиться висновок, що поява кіберпростору не змінила глибоко суспільства з точки зору відносної влади одного типу громадянського суспільства над іншим. Таким чином, вважають вони, його трансформаційна сила досить обмежена в більш фундаментальному сенсі. Емпірична увага дослідження науковців зосереджена на норвезькому громадянському суспільстві, яке представляє західну розвинену демократичну державу, але стверджується, що хоча емпіричні результати можуть відрізнятися, аналітичну структуру, можливо, можна застосувати та адаптувати до будь-якого суспільства [18]. Ця проблема перебуває в центрі уваги італійського дослідника Ф. Томазелло. Зростання соціальної нерівності, вважає автор, викликає серйозне занепокоєння, пов'язане з цифровою революцією. Науковець розглядає це питання, досліджуючи, як можна переосмислити правила соціального забезпечення та по-

літику перерозподілу в епоху цифрового капіталізму. Він зосереджується на історії та тривалій кризі прав соціального громадянства у зв'язку з технологічними змінами, щоб провести порівняння між індустріальним та цифровим сценаріями. У першому розділі йдеться про зв'язок між промисловою революцією та зародженням соціальних прав. Він описує останню як легальну «машину», призначену для компенсації дисбалансу, спричиненого технологічним рухом індустріалізації. Другий і третій розділи вводять поняття «індустріального громадянства», щоб описати архітектуру соціальних прав у зрілих індустріальних суспільствах і стверджувати, що європейські системи соціального забезпечення все ще значною мірою моделюються за промисловим стандартом. У четвертій частині розглядається вплив цифрової революції на цю модель соціального громадянства. У ньому визначено дебати щодо базового доходу як основну траєкторію для переробки правил соціального забезпечення в постіндустріальну епоху, а цифрового користувача як важливого нового суб'єкта прав. У заключній частині досліджується, як цифрові користувачі можуть отримати соціальні права як постачальники даних. З цією метою вводиться ідея «цифрових соціальних прав», що є результатом включення принципів добробуту та перерозподілу в нові цифрові права. Таким чином, автор пропонує юридично-політичну основу для перерозподілу доходів, отриманих від даних, у формі «базового цифрового доходу» для громадян кіберпростору [19].

Роль громадянського суспільства на прикладі взаємин Європейського Союзу та Китаю є темою досліджень китайського вченого К. Налбантоглу. ЄС і Китай, зазначає автор, є глобальними державами, які можуть впливати та змінювати міжнародні відносини на політичному, економічному та суспільному рівнях. У той час як ЄС формує зовнішню політику в Європі, Китай відіграє вирішальну роль в азіатській політиці. В азіатсько-європейському міжрегіоналізмі та міжрегіональних відносинах відносини ЄС і Китаю мають важливе значення для консолідації глобальної та регіональної стабільності. У цьому контексті, продовжує науковець, управління даними стало геополітичною концепцією міжнародних відносин. Відмінності між підходами Китаю та ЄС до даних – доступу, обробки та збору – можуть призвести до геополітичних протистоянь. Дослідник стверджує, що обидва суб'єкти повинні залучати громадянське суспільство до процесу формування політики, щоб розглянути динаміку інформаційних технологій, співпрацювати для адаптації глобального підходу та уникати геополітичних протистоянь. Організації громадянського суспільства можуть допомогти учасникам зрозуміти основні ризики в кібербезпеці та сформувати неконфліктний підхід у структурах управління даними. Крім того, досліджуючи моделі управління даними

в ЄС і Китаї, вчений наголошує на важливості ролі організацій громадянського суспільства в подоланні потенційних ризиків і можливостей у кіберпросторі. Нарешті, вчений завершує свою роботу політичними рекомендаціями для Китаю та ЄС щодо співпраці в кіберпросторі із залученням організацій громадянського суспільства [20].

Висновки. Важливість та поширеність кіберпростору підтверджує потребу в його врегулюванні. Повільне його регулювання на міжнародному (міждержавному) рівні спонукає до більш швидкого регулювання окремих сфер мережі Інтернет. Це проявляє також відхід від класичної європейської ієрархізації правових норм у романо-германській правовій сім'ї, коли без загального регулювання не може бути галузевого, і показує можливість створення нової системи, яка може піти шляхом індукції. Також подібна система регуляції дозволяє впроваджувати нові принципи, наприклад принцип рівня технологічності, принцип доступності тощо.

Кібербезпека залишається однією з центральних проблем, для вирішення якої вчена спільнота пропонує залучити громадянське суспільство і як суб'єкта, і як механізму. При цьому часто наголошується на тому, що старі правові та звичаєві інститути вже не спроможні стати головними механізмами регуляції з причини неспроможності, застарілості та базування на традиційних принципах, які не враховують технологічний розвиток. Наукова спільнота пропонує створити нову правову галузь (як у міжнародному просторі, так і в окремих сферах кіберпростору) для ефективності регулювання інтернету. Вона має містити власний термінологічний апарат, особливі методи регулювання та нові підходи бачення кіберпростору.

У цілому варто відмітити, що проблематика врегулювання кіберпростору залишається відкритою науковою темою, яка оновлюється щоразу з розширенням інтернету.

ЛІТЕРАТУРА

1. Martino L. The Fifth Dimension of Conflictuality: The Rise of Cyberspace and Its Effects on International Politics. *Politica & societa*. 2018. № 7 (1). P. 61–75.
2. Greiman V. The Winds of Change in World Politics and the Impact on Cyber Stability. *International Journal of Cyber Warfare and Terrorism (IJCWT). 2019.* № 9 (4). P. 27–43.
3. Tsagourias N. The Slow Process of Normativizing Cyberspace. *AJIL Unbound*. 2019. № 113. P. 71–75. URL: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/61AA5CC087FC50963B2A15C86DBF49D1/S2398772319000096a.pdf/the-slow-process-of-normativizing-cyberspace.pdf (дата звернення: 15.052025).

4. Wang G. Are there international rules governing cyberspace? *Journal of international and comparative law*. 2021. № 8 (2). P. 357–383.
5. Hassid N., Matania E. A Global Regime for Cybersecurity and the Obstacles to Future Progress. *Global governance*. 2024. № 30 (1). P. 13–40.
6. Chachavalpongpun P. Nationhood in the Cloud: Cyber Sovereignty in Thailand. *Asian Studies Review.* 2022. № 47(2). P. 392–411.
7. Hodgson Q. Understanding and Countering Cyber Coercion. *10th International Conference on Cyber Conflict (CyCon) – Maximising Effects.* Proceeding's 10TH International conference on cyber conflict (CYCON X): Maximising effects. Tallinn, 2018. P. 73–88.
8. Weitzner Dj. Promoting Economic Prosperity in Cyberspace. *Ethics & international affairs.* 2018. № 32 (4). P. 425–439.
9. Renda A. Making the digital economy «fit for Europe". *European law journal*. 2020. № 26 (5/6). P. 345–354. URL: https://onlinelibrary.wiley.com/doi/10.1111/eulj.12388 (дата звернення: 20.05.2025).
10. Hodgins M. The perils of cybersecurity regulation. *Review of austrian economics*. 2024. URL: https://link.springer.com/article/10.1007/s11138-024-00660-4 (дата звернення: 20.05.2025).
11. Fan L., Zeng C., Wang Y., Ma J., Wang F. Social Radars: Finding Targets in Cyberspace for Cybersecurity. *IEEE-CAA journal of automatica sinica*. 2024. № 11 (2). P. 279–282.
12. Ruojin X., Leilei Q., Wenchang Sh. Human Security Behavior Assistance in the Cyber-Physical Space. *4th International Conference on Science of Cyber Security (SciSec).* Proceeding's 4th International Conference on Science of Cyber Security (SciSec). Matsue. 2022. P. 28–43.
13. Eichensehr K. The Law and Politics of Cyberattack Attribution. *Ucla law review*. 2020. № 67 (3). P. 520–598.
14. Katagiri N. Why international law and norms do little in preventing non-state cyber-attacks. Journal of Cybersecurity. 2021. Vol. 7, Issue 1. URL: https://academic.oup.com/cybersecurity/article/7/1/tyab009/6168044?login=false (дата звернення: 20.05.2025).
15. Greiman V. The Politics and Practice of Cyber Attribution: A Global Legal Perspective. *16th International Conference on Cyber Warfare and Security* (ICCWS). Proceeding's 16th international conference on cyber warfare and security (ICCWS 2021). Tennessee, 2021. P. 102–108.
16. Kello L. Cyber legalism: why it fails and what to do about it. Journal of Cybersecurity. 2021. Vol. 7 (1). URL: https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244?login=false (дата звернення: 25.05.2025).
17. Coles-Kemp L., Ashenden D., O'Hara K. Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen**.** *Politics and governance*. 2018. № 6 (2). P. 41–48. URL: https://www.cogitatiopress.com/politicsandgovernance/article/view/1333/804 (дата звернення: 20.05.2025).

18. Castilla J., Pursiainen C. Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not? *Journal of civil society*. 2019. №15 (4). P. 392–411. URL: https://munin.uit.no/bitstream/handle/10037/17950/article.pdf;jsessionid=C0650DEA3AAD0F4B72CBF61ED66F9807?sequence=2 (дата звернення: 20.05.2025).
19. Tomasello F. From industrial to digital citizenship: rethinking social rights in cybersp ace. *Theory and society*. 2023. №52 (3). P. 463–486. URL: https://link.springer.com/article/10.1007/s11186-022-09480-6#citeas (дата звернення: 22.05.2025).
20. Nalbantoglu C. EU – China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace. *Cuadernos europeos de deusto*. 2022. P. 51–73. URL: https://ced.revistas.deusto.es/article/view/2555/3068 (дата звернення: 25.05.2025).

REFERENCES

1. Martino, L. (2018). The Fifth Dimension of Conflictuality: The Rise of Cyberspace and Its Effects on International Politics. *Politica & societa*, *7(1), 61–75.*
2. Greiman, V. (2019). The Winds of Change in World Politics and the Impact on Cyber Stability. *International Journal of Cyber Warfare and Terrorism (IJCWT), 9(4), 27–43.*
3. Tsagourias, N. (2019). The Slow Process of Normativizing Cyberspace. *AJIL Unbound*, *113, 71–75.* URL: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/61AA5CC087FC50963B2A15C86DBF49D1/S2398772319000096a.pdf/the-slow-process-of-normativizing-cyberspace.pdf
4. Wang, G. (2021). Are there international rules governing cyberspace? *Journal of international and comparative law*, *8(2), 357–383.*
5. Hassid N., Matania, E. A. (2024). Global Regime for Cybersecurity and the Obstacles to Future Progress. *Global governance*, *30(1), 13–40.*
6. Chachavalpongpun, P. (2022). Nationhood in the Cloud: Cyber Sovereignty in Thailand. *Asian Studies Review, 47 (2), 392–411.*
7. Hodgson, Q. (2018). Understanding and Countering Cyber Coercion. *10th International Conference on Cyber Conflict (CyCon) – Maximising Effects:* proceeding's 10TH International conference on cyber conflict (CYCON X): Maximising effects. Tallinn, *73–88*.
8. Weitzner, Dj. (2018). Promoting Economic Prosperity in Cyberspace. *Ethics & international affairs, 32(4), 425–439*.
9. Renda, A. (2020). Making the digital economy «fit for Europe». *European law journal*, *26(5-6), 345–354.* URL: https://onlinelibrary.wiley.com/doi/10.1111/eulj.12388
10. Hodgins, M. (2024). The perils of cybersecurity regulation. *Review of austrian economics*. URL: https://link.springer.com/article/10.1007/s11138-024-00660-4
11. Fan, L., Zeng, C., Wang, Y., Ma, J., Wang, F. (2024). Social Radars: Finding Targets in Cyberspace for Cybersecurity. *IEEE-CAA journal of automatica sinica*, *11(2), 279–282.*

12. Ruojin, X., Leilei, Q., Wenchang, Sh. (2022). Human Security Behavior Assistance in the Cyber-Physical Space. *4th International Conference on Science of Cyber Security (SciSec)*: proceeding's 4th International Conference on Science of Cyber Security (SciSec). Matsue, *28–43.*
13. Eichensehr, K. (2020). The Law and Politics of Cyberattack Attribution. *Ucla law review*, *67(3), 520–598.*
14. Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber-attacks. Journal of Cybersecurity, *7(1).*
15. URL: https://academic.oup.com/cybersecurity/article/7/1/tyab009/6168044?login=false.
16. Greiman, V. (2021). The Politics and Practice of Cyber Attribution: A Global Legal Perspective. *16th International Conference on Cyber Warfare and Security* (ICCWS): proceeding's 16th international conference on cyber warfare and security (ICCWS 2021). Tennessee, *102–108.*
17. Kello, L. (2021). Cyber legalism: why it fails and what to do about it. Journal of Cybersecurity, 7(1).
18. URL: https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244?login=false
19. Coles-Kemp, L., Ashenden, D., O'Hara, K. (2018). Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and governance*, *6(2), 41–48*. URL: https://www.cogitatiopress.com/politicsandgovernance/article/view/1333/804
20. Castilla, J., Pursiainen, C. (2019). Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not? *Journal of civil society*, *15 (4), 392–411*. URL: https://munin.uit.no/bitstream/handle/10037/17950/article.pdf;jsessionid=C0650DEA3AAD0F4B72CBF61ED66F9807?sequence=2
21. Tomasello, F. (2023). From industrial to digital citizenship: rethinking social rights i n cyberspace. *Theory and society*, *52(3), 463–486.* URL: https://link.springer.com/article/10.1007/s11186-022-09480-6#citeas
22. Nalbantoglu, C. (2022). EU – China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace. *Cuadernos europeos de deusto*, *51–73*. URL: https://ced.revistas.deusto.es/article/view/2555/3068

Trofymenko Volodymyr Anatolevich, candidate of Legal Sciences, assistant professor, Department of Philosophy, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

CYBERSPACE: TOWARDS THE PROBLEM OF REGULATION

The publication is devoted to the problem of regulation of cyberspace. The complexity of regulation at the general level has led to the fact that the regulation of its individual spheres is more rapid: economy, etc. It is also argued that existing legal institutions are

no longer able to create an effective mechanism of regulation. In this regard, the scientific community proposes to create special mechanisms of regulation that are based on the legal and technological basis of cyberspace.

Keywords: *cyberspace, cybersecurity, civil society, cyberphysical space, industrial citizenship, digitalization.*