УДК 340.12.
DOI: https://doi.org/10.21564/2663-5704.59.289691

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

ДЕРЖАВА ЯК ОСОБЛИВИЙ СУБ'ЄКТ КІБЕРПРОСТОРУ

Публікацію присвячено статусу та місцю держави в кіберпросторі. Порушуються питання кіберсуверенітету та кібербезпеки держави. Окреслюються особливі можливості держави врегулюванні кіберпростору на законодавчому рівні. Окремо розглядається проблема зловживання держав можливостями кіберпростору з власними цілями та питання протистояння такій діяльності. Описується проблема кіберпростору на міжнародному рівні, а також проблеми міжнародного права в регулюванні цієї сфери.

Ключові слова: *кіберпростір, кібербезпека, кіберкордон, кіберзагроза, кібер-агресія, інформаційне суспільство.*

Постановка проблеми. Широкі можливості кіберпростору та способи його використання привели до того, що держава мусила звернути на нього свою увагу. При цьому виявилося, що можливості впливу держави на кіберпростір невеликі з причини його побудови та структури, що не дозволяє створити якісь кордони в ньому, гарантувати дієвість нормативно-правових актів, захист прав громадян тощо. Також з урахуванням швидкості розвитку нових технологій і застосування їх у мережі Інтернет зі сторони кіберпростору все більше зростає небезпека безпосередньо для державних інститутів. Тому наукова спільнота звертається до дослідження не тільки технічної, а й інших сторін кіберпростору.

Окремою групою, до якої звертаються науковці, є проблеми що визначають суб'єктний статус держави в кіберпросторі. До провідних із них можна віднести питання державного суверенітету в кіберпросторі, реалізації владних повноважень державою в кіберсфері. Нагальною є і проблема побудови та співвідношення міжнародного та національного законодавства стосовно кіберпростору. Усе частіше порушується проблема кібервійни та кібернетичної потужності держав. Окремо розглядається питання зловживання державою можливостями кіберпростору для реалізації власних цілей.

Дослідження окреслених проблем дозволить конкретизувати місце та статус держави в кіберпросторі та визначити її функціональні можливості.

Аналіз останніх досліджень і публікацій. Наукова спільнота не має єдиної думки стосовно контрольованості кіберпростору державою. Сформувалося два підходи. Перший проголошує, що держава може контролювати кіберпростір і в такий спосіб реалізовувати свої функції. Другий – що держава є обмеженою в цьому з причини невизначеності її суверенітету в цій сфері.

Дискусії стосовно природи самого кіберпростору та його контролю тривають уже доволі давно. На це звертає увагу англійський дослідник С. Мейнворінг [1]. Він намагається зрозуміти вплив цих дискусій на розуміння суверенітету держави. Понад двадцять років, пише вчений, люди були свідками інтригуючої дискусії про природу кіберпростору. І вчений ставить запитання: як це вплинуло на суверенітет держав? На його думку, було дві хвилі поглядів на цей феномен. Вчені початкової хвилі стверджували, що це різко зменшило централізований контроль із боку держав, чому сприяли глобалізація та свобода. Ці лібертаріанські вимоги були значними. Нещодавній новій хвилі публікацій стверджувалося, що держави почали відновлювати контроль у кіберпросторі, зосереджуючись або на роботі поліції авторитарних режимів, або на викриттях Едварда Сноудена. Але такі претензії, на думку науковця, були невідповідними. Він вважає, що часто неправильно розуміється суттєвість кіберпростору та його наслідки для контролю. Це не лише кидає виклик лібертаріанському наративу свободи, але й припускає, що анархічне уявлення інтернету як «Дикого Заходу» було навмисно пропаговане державами, щоб відвернути увагу від реальності. Інтернет, продовжує С. Мейнворінг, як і попередні форми електронного підключення, складається здебільшого з фізичної інфраструктури, розмішеної в певних географічних регіонах і юрисдикціях. Замість того, щоб обмежити суверенітет, він запропонував централізованій владі нові способи управління державою. Дослідник робить висновок: інтернет, високошвидкісні обчислення – усе це було результатом досліджень безпеки одного інформаційного гегемона, і тому воно завжди було під контролем.

Із тим, що кіберпростір (інтернет) можна контролювати, погоджується й австралійський вчений А. Штупару [2]. Внутрішня культура контролю за цією сферою, стверджує він, культивується серед значної кількості національних держав, хоча й проявляється різними способами. На національному рівні держава може зловживати кібервладою. Метою такого зловживання може бути безпека, ідеологія, політика та економіка, а засобами – навчання, блокування вебсторінок, відмова в доступі, атаки зловмисного програмного забезпечення, шпигунство, контроль інфраструктури, атаки на вебсайти еміграції / кібердисидентів, насильство щодо / затримання засобів масової інформації.

Отже, культура контролю, продовжує науковець, може мати різні наміри та коливальні рівні, але існує в багатьох країнах незалежно від державного устрою. Із цього дослідник робить свій висновок: справжня свобода інтернету – це утопія чи, можливо, історична ілюзія.

Не все так однозначно з місцем держави в кіберпросторі, на думку представників другого напрямку. Так, румунський вчений А. Тадор [3] зазначає, що стрімкий розвиток сучасних інформаційних технологій і комунікацій – неодмінної умови побудови інформаційного суспільства – справив великий вплив на суспільство, позначивши справжні мутації у філософії економічного, політичного та культурного життя, а також у повсякденному житті людей. По суті, продовжує вчений, нині легкий доступ до інформаційно-комунікаційних технологій (далі – ІКТ) є однією з передумов безперебійного функціонування сучасного суспільства. Кіберпростір, на його думку, характеризується відсутністю кордонів, динамізмом та анонімністю, породжуючи як однакові, засновані на знаннях можливості для розвитку інформаційного суспільства, так і ризики для його функціонування (на індивідуальному рівні, державному та навіть у транскордонному прояві. Чим більше суспільство комп'ютеризоване, тим більше вразливим воно стає, і забезпечення безпеки кіберпростору повинне бути основною турботою всіх залучених учасників, особливо на інституційному рівні, де основної уваги приділяється розробленню та реалізації відповідальної політики в цій галузі. Акцентуючи увагу на інституційному рівні, румунський дослідник вказує на особливий статус держави.

Схожої позиції дотримуються і південнокорейські вчені І. Чо та Дж. Чанг [4]. Як і традиційні простори безпеки в усьому світі, зазначають вони, глобальний кіберпростір є системою анархії без абсолютної влади чи інституційного статусу. У такій ситуації, спираючись на кіберсуверенітет і кібервладу, держава, на їхню думку, намагається створити інституцію, застосовану до внутрішнього та міжнародного кіберпростору, щоб зробити кіберсистему сприятливою для самої держави. Оскільки, на відміну від традиційної влади, кіберпотужність має як матеріальні, так і нематеріальні елементи, держава не може знати рівень кіберпотужності іншої держави. З цієї причини конфлікти між державами в кіберсфері посилюються. Найбільш активними державами, які змагаються за перевагу в кіберпросторі, є США та Китай. Вони ведуть до різних рівнів визнання та стратегій щодо кібердомену. Хоча конкуренція між Сполученими Штатами та Китаєм породжує конфлікт, вона також викликає тимчасову співпрацю між державами. Виходячи з цього, корейські науковці поєднують тему кіберсуверенітету з проблемою кібербезпеки та кіберзагроз. Окремо вони звертають увагу на можливу міжнародну співпрацю в цій сфері.

Аналізуючи наведені напрямки, варто відмітити, що представники другого з них, розглядаючи питання існування держави в кіберпросторі, виходять на більш широке коло проблем: кіберзагрози, кібервійни, міжнародна співпраця та формування норм міжнародного права стосовно кіберпростору, місце міжнародних організацій у регулюванні кіберпростору. Але головною залишається проблема кібербезпеки.

Формулювання мети. Метою публікації є з'ясувати місце та можливості держави в кіберпросторі, показати її особливості порівняно з іншими суб'єктами кіберпростору.

Виклад основного матеріалу. Проблематика кібербезпеки дуже часто перетинається з проблемою кіберсуверенітету держави. На це питання звертають увагу румунські вчені Д. Стефанеску та А. Папоі [5]. Глобалізація, зазначають вони, принесла залежність від електронних комунікацій, а також певні наслідки для держав світу, головним чином у сфері кібербезпеки. В останні роки після подій в Україні кіберзагроза стала певністю та ризиком. Науковці прогнозують, що кібератаки значно зростуть, і однією з їхніх форм є гібридна війна з її звичайними та нетрадиційними, військовими та невійськовими можливостями. Поява нового поля бою – кіберпростору – є реальністю, де військові дії проводяться за допомогою складних технологій. З цією метою, наполягають вони, державам необхідно посилити свої можливості кіберзахисту, щоб запобігати агресії з віртуального середовища на критичну інфраструктуру, системи зв'язку та що не менш важливо, на людей. А це веде до посилення кіберсуверенітету.

Своє бачення проблеми захисту кіберпростору з боку держави пропонують дослідники Мюнхенського університету М. Вейз та В. Янкаускас [6]. Функціонування сучасних суспільств, зазначають вони, все більше залежить від безпечного кіберпростору. Ураховуючи брак можливостей держав для захисту цього нового домену, уряди звертаються за підтримкою до різноманітних третіх сторін. Проте, пишуть вчені, вони стикаються з проблемою. Хоча встановлений контроль може обмежити компетенцію третіх сторін, відмова від ієрархічного контролю суперечить поширеному уявленню про національну безпеку. Тому дослідники ставлять запитання: яким чином держави орієнтуються між цими функціональними вимогами та вимогами національної безпеки, щоб розробити механізми управління? Автори знаходять одну переважну закономірність. Уряди делегують повноваження, але зберігають елементи ієрархічного контролю, коли вони відповідають на загрозливі атаки. Навпаки, уряди організовують посередників за допомогою м'яких спонукань для усунення ризиків і розсіювання вразливостей у кіберпросторі. Це сприяє як непрямій науці про управління, так і дебатам про кібербезпеку.

На критичну важливість кіберсуверенітету для реалізації заходів кібербезпеки звертає увагу грецький вчений А. Ліаропулос [7]. Кіберпростір, відзначає науковець, помилково характеризують як сферу, що виходить за межі фізичного простору, і, таким чином, вона є несприйнятливою до державного суверенітету та стійкою до міжнародного регулювання. Автор показує, що кіберпростір, як і інші чотири сфери (земля, море, повітря та космічний простір), незважаючи на свої унікальні характеристики, є лише відображенням поточної міжнародної системи. Питання державного суверенітету в кіберпросторі є критичним для будь-якої дискусії про майбутнє регулювання кіберпростору. Незважаючи на те, зазначає дослідник, що кіберпростір не має кордонів і характеризується анонімністю та повсюдністю, нещодавня державна практика надає достатньо доказів того, що кіберпростір або принаймні деякі його компоненти не захищені від суверенітету. Кіберпростір не є територіальним, але, на відміну від землі, моря, повітря та космічного простору, він не є частиною природи, він створений людиною, а отже, може бути не створеним і регульованим. Держави, звертає увагу автор, постійно підкреслюють своє право здійснювати контроль над кіберінфраструктурою, розташованою на їхній території, здійснювати свою юрисдикцію над кібердіяльністю на своїй території та захищати свою кіберінфраструктуру від будь-якого транскордонного втручання з боку інших держав або особи.

Зростання кількості та якості кіберзагроз показало необхідність появи та розвитку національних стратегій кібербезпеки, які є частиною законодавчої функції держави. На це звертає увагу румунський дослідник П. Патреску [8]. В останні роки, пише він, цифровий світ набув великого значення в застосуванні в багатьох сферах через переваги, а також через велику кількість користувачів як із державних, так і з приватних компаній. Концепція кібербезпеки, на думку автора, була породжена постійним розвитком ІКТ через збільшення кількості користувачів, кількості кіберзагроз і атак, а також через важливість цієї концепції як інструменту національної сили потужності. У всьому світі кіберпростір став полем, що поширювалося на дипломатичний, інформаційний, економічний та військовий рівні глобальної та національної політики. Кібербезпека мала висхідний курс, починаючи з технічної дисципліни, розвинувшись до тактичного рівня і, нарешті, досягнувши стратегічного рівня потужних країн. Розвиток кібербезпеки, зазначає румунський дослідник, став політикою країни та світовими директивами внаслідок збільшення кількості загроз та кібератак. Через це багато держав вжили багатьох контрзаходів для захисту національної кіберінфраструктури. Він відзначає, що цих контрзаходів було вжито під час атаки на кіберінфраструктуру або після неї. Таким чином, робить висновок вчений, після того як кібератаки стали загрозою для критичної кіберінфраструктури, країни по всьому світу почали враховувати,

що запобігання є основою кібербезпеки, і почали розробляти стратегії, а деякі з цих держав застосували закони кібербезпеки.

На проблему уніфікації національних стратегій кібербезпеки різних країн звертає увагу міжнародний колектив авторів – Д. Стілітіс, І. Ротомскіс, М. Лаурінетіс, С. Надвінічний та Н. Хорунжак [9]. Кібербезпека, зазначають автори, стала важливою проблемою як на рівні ЄС, так і на національному рівні. Зараз кібербезпека сприймається як частина національної безпеки. Якщо говорити про національні стратегії кібербезпеки, то позитивним є те, що більшість країн – членів ЄС уже схвалили такі стратегії. Проте, відмічають науковці, затверджені стратегії суттєво відрізняються за змістом та реалізацією. Вчені звертають увагу на відмінності в окремих національних стратегіях та аналізують аспекти їхньої уніфікації в очікуванні знайти оптимальний баланс між ступенем уніфікації та необхідністю зберегти відмінності, що виникають через внутрішні національні особливості.

На обов'язку держави із захисту прав людини в кіберпросторі акцентує увагу південноафриканський вчений А. Беркес [10]. Дослідник відмічає, що відсутність контролю територіальної держави над частиною своєї фізичної території тісно пов'язано з порушеннями прав людини в інтернеті, з одного боку, та обмеженим (але необов'язково відсутнім) контролем держави над кіберпростором – з іншого. Незважаючи на відсутність ефективного територіального контролю, автор стверджує, що територіальна держава продовжує мати право здійснювати свій суверенітет як над територією, так і над кіберпростором. Наслідком суверенітету в міжнародному праві прав людини є передбачувана юрисдикція територіальної держави над усією її національною територією. На думку автора, територіальна держава, не маючи ефективних засобів для повного контролю над своїм кіберпростором, як це відбувається на підконтрольних уряду територіях, має, проте, постійну юрисдикцію та, отже, зобов'язання захищати права людини в інтернеті від протиправних дій, що виникають, відбуваються або впливають на територію поза його ефективним контролем.

Однією з функцій держави з реалізації кіберсуверенітету та забезпечення кібербезпеки є міжнародна співпраця. Але варто відмітити, що міжнародна співпраця в цьому напрямку розвивається нешвидко і перший етап було завершено лише у 2021 р. Це відмічає турецький вчений Т. Ельдем [11]. Дослідник відмічає, що спочатку задуманий як простір вільного та відкритого спілкування між людьми, вільний від державного регулювання та втручання, кіберпростір за останнє десятиліття став основним предметом національної та глобальної політики. Імовірно фінансовані державою кібероперації проти Естонії в 2007 р., Грузії в 2008 р. та Ірану в 2010 р. відіграли важливу роль у перетворенні кібербезпеки на питання національної та міжнародної без-

пеки. Автор звертає увагу, що розвиток кібердипломатії та міжнародного права кібербезпеки залишився позаду мілітаризації кіберпростору, але, тим не менш, за останнє десятиліття було багато міжнародних ініціатив щодо прийняття міжнародних норм кібербезпеки. Перші переговори з цієї теми, продовжує науковець, проведені в рамках Першого комітету ООН із питань роззброєння та міжнародної безпеки, свідчать про перший етап формування міжнародних правил, пов'язаних із кіберпростором. Ці переговори було завершено в рамках Робочої групи відкритого складу ООН у 2021 р., і вони є критично важливими для переходу міжнародних норм кібербезпеки з першого на другий етап.

Зважаючи на важливість досягнень ООН, Україна перш за все цікавиться підходом до кібербезпеки з боку ЄС. Цьому питанню приділяє увагу румунський вчений Д. Онеску [12]. Європейський Союз, пише вчений, працює на кількох напрямках, щоб забезпечити кібербезпеку в Європі, від надання кращого інтернету для дітей до реалізації міжнародного співробітництва з кібербезпеки та кіберзлочинності. Оскільки суспільства, уряди та підприємства, зазначає автор, все більше покладаються на інтернет для нормального функціонування повсякденної діяльності та надання основних послуг, захист кіберпростору від зловмисних дій став критично важливою точкою дій для політиків у всьому світі. Постійний стрімкий розвиток ІКТ, глобалізація, різке збільшення обсягів даних і зростання кількості різноманітного обладнання, підключеного до мереж передачі даних, впливають на повсякденне життя, економіку та функціонування держави. З одного боку, такий рівень розвитку ІКТ сприятиме покращанню доступності та зручності використання послуг, підвищенню прозорості та участі громадян в управлінні та скороченню витрат державного та приватного секторів. З іншого боку, зростаюча важливість технологій супроводжується зростанням залежності держави від уже вкорінених електронних рішень і зміцнює очікування безперебійної роботи технологій. Тому, зазначає вчений, змістовна та ефективна співпраця між державним і приватним секторами в розвитку організації кібербезпеки, а також у запобіганні кіберінцидентам та вирішенні їх стає все більш неминучою. Національна оборона та внутрішня безпека залежать від інфраструктури та ресурсів приватного сектору, у той же час держава може допомагати постачальникам життєво важливих послуг та гарантам національної критичної інформаційної інфраструктури як координатор та балансир різних інтересів. Появу кібердипломатії в ЄС констатує міжнародний колектив учених – А. Каспер, А. Осала та А. Молнар [13]. За останні десятиліття, відмічають автори, кібербезпека стала наріжним каменем європейського цифрового розвитку. Поряд із розповсюдженням інформаційних і комунікаційних технологій і поглибленням (а також розширенням) Європейського Союзу, початкова вузька

та галузева політика безпеки даних розширилася до комплексної структури кібербезпеки, яка вирішує питання від стійкої інфраструктури та технологічного суверенітету до боротьби з кіберзлочинністю, до можливостей кіберзахисту та відповідальної поведінки держави в кіберпросторі. У цій складній мережі для регулювання наведених вище питань формується кібердипломатія. Дослідники вважають, що вона повинна враховувати транскордонні зв'язки кіберпростору та відображає зміни в міжнародних відносинах, де межі між зовнішньою та внутрішньою політикою, військовою та цивільною сферами розмито. Однак термін «кібердипломатія», зазначають вчені, мінливий, і не зовсім зрозуміло, які теми повинні бути під його «парасолькою», зокрема щодо кібербезпеки, де він, здається, найбільше пов'язаний.

Однак держави не тільки намагаються захистити свій кіберпростір, а й використовують його для реалізації власних потреб. На це звертає увагу японський вчений Дж. Осава [14]. Протягом останнього десятиліття, пише він, національні держави почали використовувати кібердомен як засіб для обслуговування своїх національних інтересів. Дослідивши тенденції кібератак за останнє десятиліття, дослідник доводить, що кібератаки часто відбуваються після інцидентів міжнародної суперечки чи конфлікту. Деякі національні держави брали участь у кібератаках з метою втручання у внутрішні справи сусідньої країни. Тому кібербезпека, на думку науковця, стала головним пріоритетом національної та міжнародної безпеки. Щоб зупинити потенційних державних супротивників, які здійснюють кібератаки проти національних інтересів, необхідно вжити рішучих заходів політики національної безпеки, таких як кіберстримування, колективна кібербезпека та обмін інформацією, щоб запобігти лихам серйозних кібератак. Більш глибоко проблему державного кібервтручання розглядає американський науковець Р. Крутоф [15]. Він зазначає, що держави не несуть відповідальності за переважну більшість своїх шкідливих кібероперацій, головним чином тому, що класифікації, створені у фізичному просторі, погано відповідають кібердомену. Більшість шкідливих та інвазивних кібероперацій, констатує автор, не є кіберзлочинами і не є кібервійною. А держави, які поширюють існуючі визначення протиправних дій, дозволяють контрзаходи на кібероперації (можливо, щоб уникнути створення прецеденту, що обмежує їхню власну діяльність). За відсутності відповідного ярлика, робить попередній висновок вчений, держави-жертви мають небагато ефективних і неекскалаційних варіантів реагування, а шкода, пов'язана з цими інцидентами, лежить там, де вона потрапляє.

Спираючись на принципи деліктного права та міжнародного права, Р. Крутоф, пропонує побудувати комплексну систему відповідальності держав у кіберпросторі, де вони несуть відповідальність за свої шкідливі та протиправні дії. Він визначає міжнародні кіберделікти – дії, які використовують,

заражають або підривають інтернет, комп'ютерну систему чи мережу і тим самим завдають значної транскордонної шкоди – на відміну від кіберзлочинності та кібервійни. Цей термін, на його думку, не тільки розрізняє певний вид шкідливих дій, але й підкреслює, як принцип відповідальності держави за транскордонну шкоду (який покладає на держави відповідальність за шкідливі наслідки їхньої як законної, так і незаконної діяльності) може корисно доповнити існуюче законодавство про відповідальність держави (що стосується лише протиправних державних актів). Встановлення відповідальності держави за міжнародні кіберпорушення, вважає дослідник, мінімізує ймовірність того, що держави-жертви вдадуться до ескалації, збільшує шанси на те, що постраждалі особи отримають компенсацію, і зберігає обмежену сіру зону для державних експериментів у кіберпросторі.

Проблемою правового розуміння державних кібератак та зловмисної кібератівності цікавиться і південноафриканський дослідник М. Уотні [16]. Багато країн, зазначає вчений, стали жертвами державних кібератак і зловмисних дій. На його думку, пов'язані з державою кібероперації створюють серйозні правові загрози та виклики для стабільності та безпеки кіберпростору. Дослідник пропонує визначити правове розуміння відмінностей і подібності між державними кіберопераціями, такими як кібератаки та зловмисна кібердіяльність. Поведінка, яка може розглядатися як зловмисна діяльність, зветься кібератаками. Однак, пише М. Уотні, кібератаки та зловмисна діяльність – це не одне й те саме, а наслідки та мотиви пов'язаної з державою транскордонної кібероперації можуть відрізнятися. Кібератаки, зазначає вчений, пов'язані з державою, визначаються як кібератаки, які, як обґрунтовано очікується, призведуть до травмування чи смерті людей або пошкодження чи знищення об'єктів (DDoS-атаки чи атаки програм-вимагачів). Пов'язана ж з державою зловмисна кібердіяльність складається з крадіжки інформації (шпигунства), дезінформації та фальшивих вебсайтів. Зловмисна діяльність не завдає фізичної шкоди людям або об'єктам. Однак шкода у випадку шпигунства може полягати у фінансових збитках та/або підриві довіри до здатності уряду захищати конфіденційну інформацію або сіянні політичних і соціальних розбратів, таких як втручання у вибори чи референдуми в іншій країні. Проведення чіткого розмежування є актуальним, коли йдеться про реакцію держави-жертви на кібероперацію іноземної держави в її кіберпросторі на національному, міжнародному та глобальному рівнях. Стабільності та безпеки в кіберпросторі, пише вчений, можна досягти за допомогою міжнародних норм, що регулюють поведінку держав, зокрема транскордонні кібероперації.

З наведеного вище можна побачити, що кіберагресії стають одним із найбільших викликів для суспільства. На це звертає увагу румунський вчений

А. Вевера [17]. З цієї причини, зазначає він, фундаментальною частиною національної безпеки будь-якої сучасної держави є забезпечення кібербезпеки. Оскільки кіберпростір держави набуває дедалі більшого значення для майже будь-якого аспекту сучасного суспільства, ризики та загрози національній безпеці продовжуватимуть зростати, оскільки державні та приватні установи продовжуватимуть розвиватися у формі мереж, громадяни будуть все більше покладатися на послуги інформаційного суспільства та використовувати кіберпростір у повсякденній діяльності тощо. Інформаційні та комунікаційні системи держави, а також дані, якими вони керують, мають тенденцію до побудови, оскільки технологічний прогрес стирає і навіть розчищає кордони між взаємодоповнювальними сферами, єдиним середовищем, «кіберпростором». Ця еволюція кіберпростору, зазначає науковець, викликає безпрецедентне явище, яке поширює ідеї, що впливають на величезні спільноти людей, визначає регіональні та континентальні події, змінює глобальні стратегії та малює нові кордони, держави чи зони впливу. Таким чином, на думку автора, національні держави та недержавні суб'єкти все більше цікавляться роллю, яку відіграє кіберпростір у формуванні та підтримці думок, що виходять за межі держави, у появі та поширенні ідеологій, що змінюють або ставлять під сумнів відносини громадянина з фундаментальними цінностями держави, такими як національна ідентичність, державна єдність, незалежність або суверенітет.

Для кращого забезпечення безпекових заходів у кіберпросторі пакістанські дослідники Н. Шакіл та Н. Хан [18] пропонують визначити кіберкордон держави. Безпека та безпека національних кордонів держави, пишуть вони, була першочерговою проблемою протягом десятиліть. Обов'язком уряду є захист і контроль доступу до кордону. Поява кіберзагроз викликала серйозне занепокоєння щодо безпеки в кіберпросторі та викликала тривогу в усьому світі через їхні серйозність та асиметричний характер. Прикордонні та кібернетичні загрози не є взаємовиключними та відокремленими від реального простору, тому держава, на думку вчених, повинна розробити політику та стратегії для вирішення проблем, якими кіберпростір впливає на національну безпеку. Розроблення та посилення кіберкордонів є першим кроком у захисті кіберпростору, який у більшості випадків є невидимим і нечітко визначеним. Дослідники прогнозують: кіберкордони, якщо вони чітко визначені та закріплені за допомогою політичних рамок, можуть допомогти захистити націю від майбутньої кіберзагрози та непередбачуваних подій.

Незважаючи на велику кількість публікацій із міжнародної співпраці стосовно кіберпростору та кібербезпеки, існує точка зору, що міжнародне право кібербезпеки перебуває у кризі. Таку позицію озвучує англійський науковець К. Макак [19]. Кілька показників, зазначає він, свідчать про те, що міжнарод-

не право кібербезпеки перебуває в розпалі кризи. По-перше, пропозиції міжнародно обов'язкових договорів провідних зацікавлених сторін були зустрінуті іншими державами з невеликим ентузіазмом і, як правило, розглядаються як такі, що мають обмежені шанси на успіх. По-друге, держави вкрай неохоче беруть на себе зобов'язання щодо конкретного тлумачення суперечливих правових питань. По-третє, замість того, щоб тлумачити або розвивати правила, представники держави шукають притулку в пустому терміні «норми». Вчений стверджує, що небажання держав брати участь у міжнародній правотворчості породило вакуум влади, що додає довіри твердженням про те, що міжнародне право не справляється з сучасними викликами, які породжує швидкий розвиток інформаційних і комунікаційних технологій. У відповідь низка недержавних нормотворчих ініціатив намагалися заповнити цей вакуум, наприклад пропозиція кібернорм Microsoft або проєкт Талліннського посібника. Таким чином, пише автор, ця нова сукупність необов'язкових норм дає державам критичну можливість повернути собі центральну законодавчу позицію, подібно до історичних прецедентів, включаючи розроблення правових режимів для Антарктиди та ядерної безпеки. Тому, на думку К. Макака, найближчим часом буде вирішено, чи призведе передбачувана криза міжнародного права до припинення міждержавного управління кіберпростором, чи до зміни правових підходів. Держави повинні взяти на себе центральну роль у цьому процесі, якщо вони хочуть гарантувати, що існуючий вакуум влади не буде використаний таким чином, що порушить їхню здатність досягати своїх стратегічних і політичних цілей.

Висновки. Як можна зрозуміти з вищенаведеного, держава є особливим суб'єктом кіберпростору, на відміну, наприклад, від людини-користувача. Особливий статус проявляється в деяких аспектах:

1. Маючи територіальний суверенітет, держава має можливість контролювати фізичні технічні засоби, які підтримують існування кіберпростору.

2. Держава може розробляти, приймати та контролювати дотримання правових норм, що стосуються кіберпростору і можуть поширюватись на все населення країни. Варто відмітити, що рівень контролю залежить від державного устрою та стану демократичності.

3. Держава є головним суб'єктом міжнародного права. На міжнародному рівні робиться спроба єдиного підходу до регулювання кіберпростору та проблеми кібербезпеки зокрема. Але варто зазначити, що не всі держави мають бажання міжнародного регулювання цього питання.

Наостанок необхідно зазначити, що питання статусу держави в кіберпросторі залишається відкритим. Особливості кіберпростору поки що не дають науковцям повністю розкрити цю проблему.

ЛІТЕРАТУРА

1. Mainwaring S. Always in control? Sovereign states in cyberspace. *European Journal of International Security.* 2020. № 5 (2). P. 215–232.
2. Stuparu A. National Cyber Power and the Inward Culture of Control. *13th International Conference on Cyber Warfare and Security (ICCWS – 2018).* Proceedings 13th International Conference on Cyber Warfare and Security (ICCWS – 2018). Washington, 2018. P. 474–481.
3. Tudor A. Threats to cyber security. *International Conference on Law between Modernization and Tradition – Implications for the Legal, Political, Administrative and Public Order Organization.* Proceedings International Conference on Law between Modernization and Tradition – Implications for the Legal, Political, Administrative and Public Order Organization. Bucharest, 2015. P. 659–664.
4. Cho Y., Chung J. Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity. *Pacific focus.* 2017. № 32 (2). P. 290–314.
5. Stefanescu D., Papoi A. New threats to the national security of states – cyber threat. *Scientific journal of silesian university of technology-series transport.* 2020. №107. P. 177–182. URL: https://sjsutst.polsl.pl/archives/2020/vol107/177_SJSUTST107_2020_Stefanescu_Papoi.pdf (дата звернення: 06.06.2023).
6. Weiss M., Jankauskas V. Securing cyberspace: How states design governance arrangements. *Governance-An international journal of policy administration and institutions.* 2019. Vol. 32 (2). P. 259–275.
7. Liaropoulos A. Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *8th International Conference on Information Warfare and Security (ICIW-2013).* Proceedings of the 8th international conference on information warfare and security (ICIW-2013). Denver, 2013. P.136–140.
8. Patrascu P. The Appearance and Development of National Cyber Security Strategies. *14th International Scientific Conference on eLearning and Software for Education – eLearning Challenges and New Horizons.* Proceedings 14th International Scientific Conference on eLearning and Software for Education – eLearning Challenges and New Horizons. Bucharest, 2018. P. 53–59.
9. Stilitis D., Rotomskis I., Laurinaitis M., Nadvynychnyy S., Khorunzhak N. National cyber security strategies: management, unification and assessment. *Independent journal of management & production*. 2020. Vol. 11 (9). P. 2341–2354.
10. Berkes A. Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control. *Israel law review.* 2019. Vol. 52 (2). P. 197–231. URL: https://bura.brunel.ac.uk/bitstream/2438/20725/2/FullText.pdf (дата звернення 12.06.2023).
11. Eldem T. International Cybersecurity Norms and Responsible Cyber Sovereignty. *Istanbul hukuk mecmuasi.* 2021. Vol. 79 (1). P. 347–378.
12. Onescu D. EU and cyber security. *12th International Scientific Conference on eLearning and Software for Education (eLSE).* Proceedings 12th International Scientific Conference on eLearning and Software for Education (eLSE). Bucharest, 2016. P. 436–441.

13. Kasper A., Osula A., Molnar A. EU cybersecurity and cyber diplomacy. *IDP-internet law and politics.* 2021. №34. P. 1–15. URL: https://raco.cat/index.php/IDP/article/view/n34-kasper/487930 (дата звернення: 13.06.2023).
14. Osawa J. The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-pacific review.* 2017. Vol. 24 (2). P. 113–131.
15. Crootof R. International cybertorts: expanding state accountability in cyberspace. *Cornell law review.* 2018. №103 (3). P. 565–644.
16. Watney M. A Legal Understanding of State-Linked Cyberattacks and Malicious Cyber Activities. *18th European Conference on Cyber Warfare and Security (ECCWS – 2019)*. Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS – 2019). Coimbra, 2019. P. 560–567.
17. Vevera A. From cyber threat to hostile action in cyberspace. *Romanian journal of information technology and automatic control-revista romana de informatica si automatica.* 2018. №28 (3). P. 17–30.
18. Shakeel N., Khan N. A framework to protect National Cyber Borders in peace and war. *16th Asia Joint Conference on Information Security (AsiaJCIS – 2021).* Proceedings 16TH Asia Joint Conference on Information Security (AsiaJCIS – 2021). Seoul, 2021. P. 17–22.
19. Macak K. Is the International Law of Cyber Security in Crisis? *8th International Conference on Cyber Conflict – Cyber Power (CyCon).* Proceedings 8th International Conference on Cyber Conflict – Cyber Power (CYCON U. S.). Tallinn, 2017. P. 127–139.

REFERENCES

1. Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security, 5*(2)*, 215–232.*
2. Stuparu, A. (2018). National Cyber Power and the Inward Culture of Control. *13th International Conference on Cyber Warfare and Security (ICCWS-2018):* proceedings 13th International Conference on Cyber Warfare and Security (ICCWS-2018). Washington, pp. 474–481.
3. Tudor, A. (2015). Threats to cyber security. *International Conference on Law between Modernization and Tradition – Implications for the Legal, Political, Administrative and Public Order Organization:* proceedings International Conference on Law between Modernization and Tradition – Implications for the Legal, Political, Administrative and Public Order Organization. Bucharest, pp. 659–664.
4. Cho, Y., Chung, J. (2017). Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity. *Pacific focus, 32*(2)*, 290–314.*
5. Stefanescu, D., Papoi, A. (2020). New threats to the national security of states – cyber threat. *Scientific journal of silesian university of technology-series transport, 107, 177–182.* URL: https://sjsutst.polsl.pl/archives/2020/vol107/177_SJSUTST107_2020_Stefanescu_Papoi.pdf

6. Weiss, M., Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. *Governance-An International journal of policy administration and institutions, 32*(2)*, 259–275.*
7. Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *8th International Conference on Information Warfare and Security (ICIW-2013):* proceedings of the 8th international conference on information warfare and security (ICIW-2013). Denver, pp. 136–140.
8. Patrascu, P. (2018). The Appearance and Development of National Cyber Security Strategies. *14th International Scientific Conference on eLearning and Software for Education – eLearning Challenges and New Horizons:* proceedings 14th International Scientific Conference on eLearning and Software for Education – eLearning Challenges and New Horizons. Bucharest, *53–59.*
9. Stilitis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., Khorunzhak, N. (2020). National cyber security strategies: management, unification and assessment. *Independent journal of management & production, 11*(9)*, 2341–2354.*
10. Berkes, A. (2019). Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control. *Israel law review, 52*(2)*, 197–231*. URL: https://bura.brunel.ac.uk/bitstream/2438/20725/2/FullText.pdf
11. Eldem, T. (2021). International Cybersecurity Norms and Responsible Cyber Sovereignty. *Istanbul hukuk mecmuasi, 79*(1)*, 347–378.*
12. Onescu, D. (2016). EU and cyber security *12th International Scientific Conference on eLearning and Software for Education (eLSE):* proceedings 12th International Scientific Conference on eLearning and Software for Education (eLSE). Bucharest, pp. 436–441.
13. Kasper, A., Osula, A., Molnar, A. (2021). EU cybersecurity and cyber diplomacy. *IDP-internet law and politics: 34, 1–15.* URL: https://raco.cat/index.php/IDP/article/view/n34-kasper/487930
14. Osawa, J. (2017). The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-pacific review, 24*(2)*, 113–131.*
15. Crootof, R. (2018). International cybertorts: expanding state accountability in cyberspace. *Cornell law review, 103*(3)*, 565–644.*
16. Watney, M. A (2019). Legal Understanding of State-Linked Cyberattacks and Malicious Cyber Activities. *18th European Conference on Cyber Warfare and Security (ECCWS-2019)*: proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS-2019). *Coimbra, 560–567.*
17. Vevera, A. (2018). From cyber threat to hostile action in cyberspace. *Romanian journal of information technology and automatic control-revista romana de informatica si automatica, 28*(3)*, 17–30.*
18. Shakeel, N., Khan, N. (2021). A framework to protect National Cyber Borders in peace and war. *16th Asia Joint Conference on Information Security (AsiaJCIS-2021):* proceedings 16TH Asia Joint Conference on Information Security (AsiaJCIS-2021). Seoul, *17–22.*

19. Macak, K. (2017). Is the International Law of Cyber Security in Crisis? *8th International Conference on Cyber Conflict – Cyber Power (CyCon):* proceedings 8th International Conference on Cyber Conflict – Cyber Power (CYCON U. S.). Tallinn, pp. 127–139.

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

THE STATE AS A SPECIAL SUBJECT OF CYBERSPACE

The publication is devoted to the status and place of the state in cyberspace. Issues of cyber sovereignty and cyber security of the state are being raised. The special capabilities of the state to regulate cyberspace at the legislative level are outlined. The problem of states abusing the opportunities of cyberspace for their own purposes and the issue of opposing such activities is considered separately. The problem of cyberspace at the international level is described, as well as the problems of international law in regulating this sphere.

Keywords: *cyber space, cyber security, cyber border, cyber threat, cyber aggression, information society.*