Ефективність державного управління
Efficiency of public administration
ISSN 2070-4011 (print)
ISSN 2786-6580 (online)
https://doi.org/10.36930/507813
Article received 17.05.2024
Article accepted 20.06.2024
УДК [351.746.1-047.64:351.865](477)
Correspondence author: V. O. Tkach, Tkach.Vsevolod@nltu.lviv.ua

В. О. Ткач
Національний лісотехнічний університет України, м. Львів, Україна

ГЛОБАЛЬНЕ УПРАВЛІННЯ У СФЕРІ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ СУЧАСНИХ ВИКЛИКІВ ТА ЗАГРОЗ УКРАЇНІ

Кібербезпеку розглянуто як основний фактор національної та міжнародної безпеки XXI століття. Аргументовано, що численні ініціативи у сфері правового забезпечення кібербезпеки охоплюють тільки невелику частину міжнародної правової системи, зокрема, щодо захисту критичної інфраструктури, захисту приватних даних у мережі, ведення війни із застосуванням кібертехнологій. Наголошено, що кібербезпека охоплює вже не тільки інформацію як об'єкт захисту, не тільки технічні засоби, які визначають можливості функціонування інформації, а, водночас, захист способів функціонування нової сутності – кіберпростору. Проаналізовано політико-правові документи, що визначають суть та спрямування національної політики кібербезпеки на прикладі окремих країн та визначено їх роль у міжнародно-правовому просторі. Особливу увагу приділено дослідженню агресивних стратегій Росії та Китаю у створенні критичних кіберзагроз. Розкрито особливі виклики, з якими стикається Україна під час активізації кібервійни з боку Російської Федерації як складника повномасштабного вторгнення. Аргументовано недоліки концептуального розуміння кібербезпеки в Україні, Європейському Союзі та США. Наголошено, що враховуючи те, що кібербезпека є глобальною проблемою, до неї потрібен глобальний підхід. Доведено необхідність міжнародного співробітництва, зокрема, на основі потрійної спіралі та механізмів кооперації. Конкурентне суперництво та закритість у цій сфері, орієнтація виключно на національно-державні інтереси приведуть до клаптевого характеру глобального управління кібербезпекою, що істотно знизить його потенціал.

Ключові слова: глобальне управління; кібербезпека; національна безпека; кіберзагрози; агресія; кіберпротистояння.

Вступ

Численні кіберінциденти, зафіксовані останніми роками, наочно показують, що кібербезпека стала частиною міжнародного порядку денного. Декілька міжнародних організацій висунули ініціативи в галузі управління кіберпростором, зокрема, Організація Об'єднаних Націй та Європейський Союз. ООН та ЄС прагнуть відігравати провідну роль у сфері політики щодо забезпечення стійкості перед кіберзагрозами. Проте ці ініціативи досі не забезпечили створення належних регулятивних норм.

Тим часом проблеми кібербезпеки ускладнені тим, що простір кібербезпеки став мішенню окремих злочинних груп, кіберзловмисників, одночасно здійснюються хакерські атаки на державні органи, міжнародні структури, йде кіберпротистояння між окремими державами в межах інформаційних воєн. Очевидною є нагальна потреба розширення міжнародного співробітництва та взаємодії кібердержав щодо забезпечення превентивних та невідкладних заходів у межах протидії кіберзлочинам. Потрібно вдосконалити систему управління із забезпечення кібербезпеки та активно застосувати нові технології у цій сфері.

Зараз цифровий ландшафт відображає геополітичну напруженість, а групи активістів адаптують свої стратегії відповідно до глобальних подій. Незважаючи на те, що пряма шкода від цих атак була відносно стриманою, їх постійність й еволюція характеру підкреслюють необхідність вжиття надійних заходів кібербезпеки.

Цей ландшафт кіберзагроз створює серйозний виклик для глобальної розвідки, інженерів та IT-спільноти. Однак для України загрози щораз більше загострюються через повномасштабну російську військову агресію. Водночас тісна співпраця Росії та Китаю потенційно може включати не тільки військову сферу, а й удосконалення засобів кібервійни. Подібно до того, як Росія зробила Україну "полігоном" для іранських ударних безпілотників, ці два агресивні авторитарні режими можуть "випробувати" в Україні свої останні спільні розробки засобів для ведення кібервійни.

Наразі Україна є однією з головних мішеней масштабних кібератак і, по суті, перебуває "на передовій" глобальної кібербезпеки. Навряд чи варто сумніватись, що це є "кібервиміром" триваючого вторгнення Росії в Україну, елементом гібридної війни, хоча визначити точні джерела цих атак доволі складно – адже потенційно їх можуть здійснювати кіберзлочинці у країнах, що симпатизують Росії та її агресії проти України.

Отже, існує нагальна потреба у виробленні ефективних способів оптимізації глобального управління у сфері кібербезпеки. Глобальні загрози кібербезпеці мають бути осмислені та систематизовані, а заходи з їх подолання в межах глобального управління мають бути

Інформація про авторів:
Ткач Всеволод Олегович, здобувач програми доктора філософії, кафедра публічного управління та адміністрування.
Email: Tkach.Vsevolod@nltu.lviv.ua; https://orcid.org/0009-0001-6582-0064

Цитування за ДСТУ: Ткач В. О. Глобальне управління у сфері кібербезпеки в контексті сучасних викликів та загроз Україні. *Ефективність державного управління* : зб. наук. пр. Вип. 1/2(78/79). Львів: НЛТУ України, 2024. С. 84–89.
Citation APA: Tkach V. O. (2024). Global management in the field of cyber security in the context of modern challenges and threats to Ukraine. *Efficiency of public administration, 1/2*(78/79), 84–89. https://doi.org/10.36930/507813

вжиті у співпраці держав. Отже, тема цього дослідження актуальна та своєчасна.

Методи та інформаційна база дослідження. Загальнонаукові методи набули застосування в межах статті в основному в теоретичному обґрунтуванні проблеми, під час розгляду питання розуміння феномену національної та глобальної кібербезпеки, механізму її забезпечення. Загальнонаукові методи представлені такими методами, як формалізація, аксіоматичний метод, гіпотетико-дедуктивний метод та ін., а також загальнологічними методами (аналіз, узагальнення, аналогія). У дослідженні використано метод описового якісного підходу, а інтерпретація результатів ґрунтується на позитивістській парадигмі наукового дослідження.

Предмет дослідження: вітчизняний та зарубіжний досвід забезпечення кібербезпеки; доктринальні підходи до проблем забезпечення кібербезпеки; правові категорії та поняття теорії кібербезпеки; теоретичні концепції та моделі механізму забезпечення національної безпеки загалом та кібербезпеки зокрема.

Аналіз останніх досліджень і публікацій. За останні три десятиліття кібербезпека стала невід'ємним компонентом міжнародних відносин. Незважаючи на політичну природу проблеми забезпечення кібербезпеки, у цій сфері досі не створено належних механізмів міжнародного регулювання. До переліку найбільш очевидних причин, що пояснюють подібну інертність, належать невизначеність масштабу, природи, сутності та понятійного апарату кібербезпеки [5, 8].

Термінологічна невизначеність має практичний вимір: визначення кібербезпеки в контексті залежить від того, що, від кого і в який спосіб намагаються захистити, а також від того, чи можлива атрибуція можливостей. Розпливчастість визначень означає, що не завжди можливо визначити, хто повинен брати відповідальність за забезпечення кібербезпеки, що напевно призведе (і призводить) до труднощів практичного та правового характеру.

Численні ініціативи у сфері забезпечення кібербезпеки охоплюють тільки невелику частину великої правової системи, наприклад, захист критичної інфраструктури (Директива ЄС з мережевої та інформаційної безпеки), захист приватних даних у мережі (Генеральний регламент ЄС про захист персональних даних), ведення війни із застосуванням кібертехнологій [10]. Отже, визначення концепції кібербезпеки найчастіше перебуває у залежності від конкретного правового середовища [7].

У тексті Закону про кібербезпеку Європейського Союзу використовують таке визначення: "Кібербезпека означає діяльність, необхідну для захисту мереж та інформації, користувачів інформаційних мереж та інших сторін, які можуть бути порушені кіберзагрозами" [4].

Законом України кібербезпека визначена як "захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі" [15].

Отже, європейське законодавство розглядає кібербезпеку як дію, а українське законодавство – як стан.

На відміну від Європейського Союзу, у США немає єдиного федерального закону, який регулює кібербезпеку та конфіденційність. Регулювання кібербезпеки у Сполучених Штатах розділено між федеральними законами та законами штатів. Кілька штатів мають власні закони про кібербезпеку та відповідні процедури повідомлення про порушення даних. Це створює значну проблему для організацій, які ведуть бізнес у всіх 50 штатах і в усьому світі [12]. Федеральна торгова комісія (FTC) відповідає за дотримання норм і законодавства з кібербезпеки на федеральному рівні. Крім того, Департамент внутрішньої безпеки (DHS) і Національний інститут стандартів і технологій (NIST) також відіграють роль у регулюванні кібербезпеки.

Виклад основного матеріалу дослідження з обґрунтуванням одержаних результатів

На погляд експерта міжнародної аудит-консалтингової корпорації Klynveld Peat Marwick Goerdeler (KPMG) Олексія Янковського [16], від початку повномасштабного вторгнення РФ, Україна стала ціллю чисельних кібератак. Ці атаки охопили як приватні організації та громадян, так і державні установи. Підприємства, що є частиною (елементом) критичної інфраструктури, також повинні перебувати у режимі підвищеної готовності, оскільки саме ці галузі у період війни часто вважають пріоритетними цілями. Це, зокрема, енергетичні, телекомунікаційні компанії, медіа та фінансові установи. Бізнес також має бути у готовності протидіяти цим викликам – компанії мають оцінити свою готовність до кіберінцидентів і, відповідно, також свою здатність швидко відновити діяльність.

Джошуа Стайн [11] вважає, що чіткої межі між "кібервійною" та "кіберзлочинністю" як такої не існує. Особливо, на його думку, це стосується ймовірних актів російської кіберагресії. Він справедливо стверджує, що кібератака на українського мобільного оператора "Київстар" (ймовірно здійснена російськими спецслужбами) є нагадуванням про потенційну небезпеку від кібероперацій для інфраструктури, приватних компаній і урядів у світовому масштабі.

Кібердіяльність у російському "варіанті" низка експертів розглядає як щось подібне до державно-приватного партнерства. Існує думка, що в цій діяльності задіяні як офіційні державні суб'єкти ("замовники" кібератак), так і неофіційні приватні хакерські мережі ("виконаці"), які майже напевно (хоча й неофіційно) санкціоновані, та перебувають під керуванням і захистом російської влади. Згідно з повідомленнями розвідок, найбільш задіяним до кібероперацій та небезпечним державним учасником російського кібертерроруу є так звана військова частина 74455 (частіше трапляється назва Sandworm). Цей підрозділ звинувачують, зокрема, в участі в кібератаках як мінімум з 2014 року. Ймовірно, недавня атака на телекомунікаційну інфраструктуру України була пов'язана саме з Sandworm, хоча конкретні стосунки важко встановити із 100-відсотковою впевненістю [11].

Однією з причин, яка визначає стурбованість США та інших союзників з НАТО щодо кібератак на Україну, та їх зацікавленості в "інвестуванні" у війну в Україні для забезпечення перемоги України, є те, що сьогоднішні кібератаки мають вплив на кібербезпеку, який відчувається далеко за межами України. Зокрема, Китай став головною хакерською загрозою у 2024 р. через нещодавню серію атак, спрямованих на критично важливу інфраструктуру США.

Агентство з кібербезпеки та безпеки інфраструктури США, Агентство національної безпеки та ФБР опублікували звіт, в якому детально описано, як група хакерів Volt Typhoon проникає у США. Подібно до згаданої вище Sandworm у Росії, Volt Typhoon є хакерською групою, пов'язаною з китайською урядовою компанією, чия єдина місія, здається, полягає в отриманні доступу до IT-мережі критичної інфраструктури США.

На відміну від російсько-українського конфлікту, де "зміщення фокусу в бік третіх сторін" зайняло місяці, у війні Ізраїль-Хамас кібергрупи швидко перейшли до нових цілей після заяв про солідарність з Ізраїлем. У таких країнах, як Сполучені Штати, Франція, Індія та Італія, існує помітне зростання кіберактивності проти них. Зокрема, атаки включали DDoS-атаки та пошкодження веб-сайтів з мінімальним впливом. Але вони були націлені на різні об'єкти, від національної інфраструктури до цифрових активів окремих політичних діячів, слугуючи перешкодою та сигналізуючи про присутність хактивістів у глобальному діалозі [14].

На сьогодні глобальна інформатизація активно "керує" існуванням і життєдіяльністю держав світової спільноти. Інформаційні технології застосовуються у процесі вирішення завдань забезпечення національної, воєнної, економічної безпеки та інших конкуруючих держав кіберпростору, який не є географічним у загальноприйнятому значенні цього слова, однак повною мірою є міжнародним.

У процесі, в якому відбувається формування кіберпростору глобального масштабу, існує *конвергенція комп'ютерних технологій військового та цивільного призначення*. Провідні держави інтенсивно розробляють нові засоби та методи активного впливу на інформаційну інфраструктуру потенційних противників. Держави створюють спеціалізовані кібернетичні центри та підрозділи з управління та командування, з покладеним на них основним завданням захисту державних і військових інформаційних інфраструктур, а також підготовки та проведення активних деструктивних дій у полі інформаційних систем супротивника.

Принципово новою сферою у протистоянні між гравцями на міжнародній арені стає протиборство у кіберпросторі. Різноманітні терміни та визначення з приставкою "кібер…" повсюдно використовують як у міжнародних дискусіях, так і у внутрішньодержавних документах, дедалі більшою мірою відображаються у стратегічних доктринах окремих держав та міжнародних організацій, зокрема й НАТО.

У своїх стратегічних документах Пентагон визнав кіберпростір новим полем можливих бойових дій, НАТО ототожнює кібератаки на країну-члена альянсу зі збройним нападом. Фахівці в галузі інформаційних технологій найрозвиненіших держав світу одностайно відзначають той факт, що "держава, яка контролює кіберпростір, контролюватиме війну та мир" [2]. Кібербезпека є стратегічною проблемою державної важливості, і стосується всіх верств суспільства. Державна політика кібербезпеки (National Cyber Security Strategy NCSS) функціонує у ролі засобу посилення безпеки та надійності інформаційних систем держави. Керуючись прикладом США, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія та багато інших держав ухвалили стратегії кібербезпеки.

Після російського вторгнення в Україну українські *організації* зазнали серйозних кібератак з боку російської держави та підтримуваних державою-агресором хакерських груп. До них належать зловмисне програмне забезпечення, яке стирає дані на жорстких дисках, фішинг, коли злочинці створюють спеціальні шкідливі електронні листи чи повідомлення, щоб обманом змусити "високоцінні цілі" поділитися своїми даними, а також витоки даних. Їхня спільна мета – дестабілізація країни. Так само підтримувані державою хакери атакували західних союзників України, щоб перешкодити підтримці українського опору та допомоги їх справі.

Оскільки війна триває, Росія стикається зі своїми власними труднощами, включаючи соціально-економічні санкції, запроваджені Заходом, і збільшення розриву в кваліфікації, оскільки її молоді люди переїжджають до інших країн, щоб уникнути можливого призову. Це спонукало суб'єктів загрози в країні застосувати нову тактику проти своїх опонентів, до яких належать багато західних урядів і компаній. Недавнє попередження Агентства з кібербезпеки та безпеки інфраструктури (CISA) стверджувало, що Росія зосереджена на покращенні своєї здатності націлюватися на інфраструктуру, включаючи підводні кабелі та промислові системи управління [9].

Поряд із загрозою з боку Росії, кібернапруженість між Китаєм і США також загострюється. Як відзначають експерти, кібертактика Китаю зміщується від шпигунства до націлювання на критичну інфраструктуру [3]. У Китаю є додаткові мотиви для здійснення кібератак, окрім спричинення збоїв. Оскільки гонка технологічних озброєнь вирує, країна використовує всі ресурси, щоб скоротити відставання від США та ЄС, особливо у сфері ШІ. Атаки на особисту ідентифікаційну інформацію організацій зі штучним інтелектом є високим ризиком, але від них важко захиститися: конкурувати з цілою національною державою, яка дає змогу суб'єктам загрози миттєво змінювати тактику, – це доволі важка справа.

Цікаво, що Китай є однією з країн, яка продовжує розвивати свою кіберпотужність. У 2004 р. китайський уряд мав бачення, описане генералом Сюй Сяоянем, колишнім головою Міністерства зв'язку Генерального штабу Китаю, про те, що Китаю потрібна технологія мережевої конфронтації для перехоплення, використання та знищення ворога для саботування функцій інформації системи через комп'ютерні мережі [1].

Опитування Інституту Пірсона/AP-NORC показало, що приблизно 7 із 10 американців вважають уряди Китаю та Росії великою загрозою кібербезпеці уряду США. Менше так говорять про неурядових акторів (рисунок).

Жодна країна не застрахована від можливості кібератаки, і будь-яка країна, галузь, бізнес чи організація можуть стати ціллю в будь-який момент. Отже, державний і приватний сектори повинні працювати разом, щоб ділитися останніми даними про атаки, одночасно переглядаючи свої стратегії кібербезпеки та зміцнюючи свою лінію захисту від наступної великої загрози.

Способи управління надають безпосередній вплив на структуру кіберпростору. Тут важливо враховувати управління технічною основою кіберпростору та суто фізичними зв'язками між окремими вузлами чи навіть областями кіберпростору. Але визначальну роль грає управління, здійснюване стосовно учасників кіберпростору – користувачів та їхніх груп. Під управлінням розуміють комплекс зусиль, що спрямований на підвищення кваліфікації учасників, стимулювання дій, сприятливих для розвитку кіберпростору і водночас приду-

шення чи пряма заборона зловмисних дій. Управління суб'єктами кіберпростору грає визначальну роль у виникненні, існуванні та підтримці основних властивостей цього утворення.

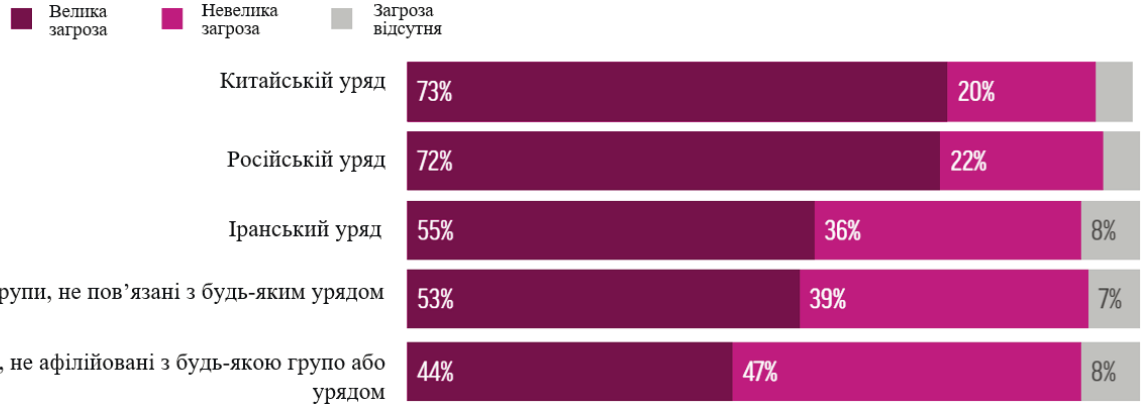

Рисунок. Результати, отримані Інститутом Пірсона на основі інтерв'ю "Наскільки великою є загроза для кібербезпеки уряду США?" [13]

Важливим завданням є правильно сформулювати поняття кібербезпеки, для точного визначення головних цілей роботи служб і засобів захисту кіберпростору від загроз, що виникають. Однак у концепціях учених та регуляторів, як українських, так і європейських, наводять формулювання, які не можуть задовольнити ці вимоги. Зокрема, в одному з проєктів концепції кібербезпеки дано таке визначення: "кібербезпека – сукупність умов, за яких усі складові кіберпростору захищені від максимально можливої кількості загроз та дій з небажаними наслідками" [6].

Зазначена постановка питання неявно закликає розробляти та виявляти дедалі нові загрози, створюючи нові засоби та інструменти захисту від них. Частка ресурсів, необхідних для забезпечення захисту, за такого підходу неухильно зростатиме, а стійке функціонування кіберпростору може навіть погіршуватися. Тому у визначенні кібербезпеки основний наголос і цільова установка мають бути зроблені на збереження сприятливого стану кіберпростору, а не на кількість загроз.

Кібербезпека не може бути спрямована на захист від максимальної кількості загроз, тим більше що їхня кількість стрімко зростає і вони постійно модифікуються. Потрібно забезпечити наявність середовища, максимально сприятливого для роботи користувачів та всіх систем у кіберпросторі.

Кібербезпека (так само, як і кіберпростір як такий) може бути описана за допомогою тріади складників її сутностей, що визначені на складових частинах кіберпростору: інформаційних ресурсах, комп'ютерній та мережевій архітектурах (інфраструктурі) та способах взаємодії користувачів. Кібербезпека охоплює вже не лише інформацію як об'єкт захисту, не лише технічні засоби, які визначають можливості функціонування інформації, а захист способів функціонування нової сутності – кіберпростору. Захищають діяльність людей, що здійснюється за допомогою інформації, яка розповсюджується за допомогою технічної інфраструктури ІКТ. У процесі забезпечення кібербезпеки важливо враховувати зазначені особливості кіберпростору та його найважливіший аспект – наявність взаємозв'язків між учасниками (користувачами), що призводить до виникнення ефекту синергії.

Необхідно докладно та ретельно дослідити основні властивості кіберпростору, динаміку його розвитку у різних масштабах часу від миттєвих до багаторічних, методи управління цією динамікою. Важливим є обґрунтування підходів до визначення специфічних показників кібербезпеки (окремо за показниками та в їх взаємозв'язку), розробити моделі їх оцінювання, виробити способи обґрунтування критеріїв. За відсутності системного аналізу та отримання оцінок застосування тих чи інших заходів неможливо побудувати ефективну систему кібербезпеки. Глобальне управління у сфері кібербезпеки має бути насамперед орієнтоване на таке системне бачення. Зокрема, доцільним є застосування механізмів потрійної спіралі (взаємодії між державою, бізнесом та академічною спільнотою). Завдяки підходу "потрійної спіралі" можна було б сприяти співпраці між підприємствами, урядовими установами та інститутами знань для підвищення цифрової стійкості глобального суспільства. Завдяки посиленій співпраці всі наявні навички та знання учасників потрійної спіралі використовуються оптимально, що призводить до кращих результатів.

Висновки та перспективи подальших досліджень

Видається доцільним до комплексу досліджень у галузі кібербезпеки включити такі напрямки:

1. Проєктування єдиної термінології стосовно кіберпростору та кібербезпеки, гармонізованої з наявною термінологією в галузі інформаційної безпеки.
2. Вироблення системи показників комплексного характеру, що охоплюють усі грані функціонування кіберпростору та його захисту від можливих загроз.
3. Розроблення моделей самого кіберпростору та основних факторів, що впливають на його функціонування. Безумовно, потрібна ретельно продумана модель загроз. Один із найважливіших напрямів передбачає створення математичних моделей, які дають змогу отримувати чисельні характеристики інформаційної безпеки (тобто, зокрема, ступеня загроз інформаційній безпеці, аналізу інформаційних ризиків, оцінювання ефективності заходів захисту).
4. Створення спеціальних методів забезпечення стійкості кіберпростору чи його сфер за впливом загроз. Тут можливим є:

- аналіз топологічної структури та вироблення рекомендацій щодо її зміни, способів та конкретних алгоритмів їх реалізації;
- нові методи криптографічного захисту, засновані не тільки на суто обчислювальних механізмах реалізації стійкості, а й на використанні переваг багатозв'язко-

вої архітектури зв'язків та великої кількості доброчесних користувачів;

- методи для забезпечення інформаційної безпеки, засновані на соціальних сервісах для протидії кібератакам із застосуванням спеціальних процедур аналізу поведінки груп.

5. Інтелектуальні методи кібербезпеки:

- методи для здійснення інтелектуальної ідентифікації користувачів;
- інтелектуальні методи запобігання вірусним та іншим атакам;
- інтелектуальні методи виявлення атак та проникнень;
- інструменти ситуаційного аналізу стану інформаційної безпеки;
- нові методи криптографічного захисту, що ґрунтуються на нейромережевих технологіях.

Кібербезпека є глобальною проблемою, і до неї потрібен глобальний підхід. Необхідне міжнародне співробітництво, зокрема на основі потрійної спіралі та механізмів кооперації (кооперація передбачає тактичні ходи, що поєднують співпрацю та протистояння: кооперацію та конкуренцію). Конкурентне суперництво та закритість у цій сфері, орієнтація виключно на національно-державні інтереси призведуть до клаптевого характеру глобального управління кібербезпекою, що істотно знизить його потенціал.

Кіберзагрози вже не можна вважати новими загрозами. Однак, ландшафт кіберзагроз змінюється швидко, і продовжить змінюватися швидко і в майбутньому. Віруси, хакери, зломи тощо все ще є частинами цього ландшафту, але основними проблемами безпеки зараз є кіберзброя та кібератаки, що походять від національних держав. Зловмисні гравці швидко вчаться один у одного, і їх інструменти швидко поширюються. Створення безпечнішого кіберпростору можливе тільки через співпрацю. Оскільки в кіберпросторі немає традиційних кордонів, союзники і партнери, і навіть суперники в технологічних гонках, несуть одні й ті самі відповідальності, і мають одні й ті самі можливості.

"Тінь" кібервійни назавжди змінює міжнародні відносини та глобальну політику. У цій новій реальності зобов'язання побудувати стійкий цифровий захист і плекати культуру співпраці в галузі кібербезпеки є не просто розумним вибором – це незамінна опора для збереження та процвітання цифрової долі кожної держави. Це заклик нашого часу, і держави повинні відповісти на нього з непохитною рішучістю та єдністю. Відповідно, існує нагальна потреба не тільки у поглибленні співпраці держав і бізнес-гравців у сфері створення гнучкого, масштабованого ландшафту кібербезпеки, здатного миттєво відповідати на нові виклики, що виникають, а й потреба у застосуванні міждисциплінарного підходу до дослідження питань глобального управління у сфері кібербезпеки, зокрема зі включенням геополітичної теорії до орбіти таких досліджень.

Список використаної літератури

1. Ardita, N., et al. (2023). Cyberwarfare between the United States and China 2014 -2022: in retrospect. *Jurnal Pertahanan Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity Nasionalism & Integrity, 9*(1), 17. URL: https://doi.org/10.33172/jp.v9i1.1869
2. Cavelty, M. (2014). Global cyber-security policy evolution. In: Cybersecurity in Switzerland, 9-25. URL: https://doi.org/10.1007/978-3-319-10620-5_2
3. Coman, V. (2022). The use of cyber attacks during traditional armed conflicts. specific and the commitment of state responsibility. *Journal of Law and Public Administration, 8*(15), 35-44.
4. European Union (EU). (2019). EU Non-Paper on Capacity Building to Advance Peace and Stability in Cyberspace, for the Work of the Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security", Submitted to the Second Substantive Session of the OEWG (10-14 February 2020). URL: https://unoda-web.s3.amazonaws.com/wp-content/up-loads/2019/09/eu-non-paper-submission-oewg-2019.pdf
5. Futter, A. (2018). Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies. *Journal of Cyber Policy, 3*(2), 201-216.
6. Holstein, W., & McLaughlin, M. (2023). *Battlefield Cyber: How China and Russia are Undermining Our Democracy and National Security*. Prometheus.
7. Kosseff, J. (2018). Defining Cybersecurity Law. *Iowa Law Review, 103*(3).
8. Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.
9. Saaida, M. (2023). The Use of Cyber Warfare and its Impact on International Security. *Science For All Publications, 1*(1), 1-5. URL: https://doi.org/10.5281/zenodo.10841886
10. Schmitt M., et al. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
11. Stein, J. (2024). Ukraine is on the front lines of global cyber security. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-is-on-the-front-lines-of-global-cyber-security/
12. Stoddart, K. (2022). Cyberwarfare: Threats to Critical Infrastructure. Palgrave Macmillan.
13. Suderman, A. (2021). Cyberattacks concerning to most in US: Pearson/AP-NORC poll. *AP News*. URL: https://apnews.com/article/joe-biden-technology-business-china-russia-c9a698542ed95bfa49f9cee0e96ef9a6
14. Whyte, C., & Mazanec, B. M. (2023). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Taylor & Francis.
15. Верховна Рада України (2017). Закон України "Про основні засади забезпечення кібербезпеки України" від 2017 р. Редакція від 04.04.2024, підстава – 3549-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
16. Янковський, О. (2022). Питання кібербезпеки в умовах воєнного часу. KPMG. URL: https://kpmg.com/ua/uk/blogs/home/posts/2022/4/pytannya-kiberbezpeky-v-umovakh-voyennoho-chasu.html

V. O. Tkach

Ukrainian National Forestry University, Lviv, Ukraine

GLOBAL MANAGEMENT IN THE FIELD OF CYBER SECURITY IN THE CONTEXT OF MODERN CHALLENGES AND THREATS TO UKRAINE

Introduction. Multiple cyber incidents recorded in recent years clearly show that cyber security has become part of the international agenda. However, existing initiatives have not yet ensured the creation of appropriate regulatory standards. It is necessary to improve the management system for ensuring cybersecurity and the active use of new technologies in this area.

Relevance of the study. States should work together to take steps to address global cybersecurity dangers through global governance, when they have been understood and categorized.

Methods. General scientific methods have mainly found application and are represented by such methods as formalization, axiomatic method, hypothetic-deductive method, etc., as well as general logical methods (analysis, generalization, analogy). The article is using a descriptive qualitative approach method and the findings are based on the positivist paradigm of scientific research.

Results. Cyberattacks might happen to any nation, sector, company, or organization at any time. No nation is safe from these threats. Therefore, in order to enhance their defenses against the next major threat and to reevaluate their cybersecurity policies, the public and commercial sectors must collaborate to exchange the most recent information obtained from assaults. It is important to correctly formulate the concept of cybersecurity so that the main goals of the services and means of protecting cyberspace from emerging threats are precisely defined. International cooperation is necessary, in particular, on the basis of triple helix and coopetition mechanisms. Competitive rivalry and closedness in this area, focusing exclusively on nation-state interests will lead to a patchwork nature of global cybersecurity management, which will significantly reduce its potential.

Keywords: cyber security; national security; cyber threats; aggression; cyber confrontation.