УДК 327
Сергій Федонюк,
кандидат географічних наук, доцент, доцент кафедри
міжнародних комунікацій та політичного аналізу,
Волинський національний університет імені Лесі Українки,
sergii.fedoniuk@vnu.edu.ua
ORCID ID: 0000-0003-2853-8905;

Ігор Карпук,
аспірант кафедри міжнародних комунікацій та політичного аналізу,
Волинський національний університет імені Лесі Українки
Karpuk.Igor@vnu.edu.ua
ORCID ID: 000-0003-4430-6004
DOI 10.29038/2524-2679-2022-03-111-136

КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АСПЕКТІ ІНТЕРЕСІВ ОСНОВНИХ МІЖНАРОДНИХ АКТОРІВ*

У цьому дослідженні розкрито суть політики щодо забезпечення інформаційної (кібер) безпеки, її витоків і цілей провідних міжнародних акторів із погляду міжнародного співробітництва. Проаналізовано підходи до аналізу міжнародного співробітництва у сфері інформаційної (кібер) безпеки, визначено предметну сферу дослідження з урахуванням основних наукових і нормативно-правових підходів, конкретизовано основні загрози в інформаційній сфері щодо інтересів суб'єктів міжнародних відносин і визначено пов'язані зі специфікою інформації та кіберпростору проблеми міжнародно-правового характеру. Розкрито підходи в реалізації політики й міжнародної діяльності основних міжнародних акторів у сфері інформаційної (кібер) безпеки – США, Росії, Китаю, Європейського Союзу. Установлено, що існує й надалі посилюється дихотомія головних концепцій інформаційної (кібер) безпеки, заснованих на глибинних відмінностях між демократичним й авторитарним підходами в цій сфері політики. В основу цих відмінностей покладено інтереси, критично важливі для кожної із систем. З одного боку, це інтереси демократичних систем, засновані на прозорості влади й необхідності збереження свободи інформації та вільної конкуренції.

*Підготовлено в межах проєкту «Стратегічні комунікації ЄС: протидія деструктивним впливам» програми ERASMUS+ напряму Модуль Жана Моне (№ 101047033 ERASMUS-JMO-2021-MODULE)

А з іншого – це інтереси авторитарних систем, сила яких ґрунтується на тотальному управлінні інформацією та її контролі. Також підґрунтя підходу авторитарних систем створює провідна участь держави в суспільному житті й економіці. На цих підходах ґрунтується внутрішня й зовнішня політика у сфері інформаційної (кібер) безпеки. Відповідно до своїх інтересів, головні міжнародні актори розробляють і просувають на міжнародних майданчиках відповідні концепції інформаційної (кібер) безпеки. Вони обґрунтовують позиції у сферах державного суверенітету, управління інтернетом, застосування міжнародного права в кіберсфері, доступності інформаційних технологій та ін.
Ключові слова: інформаційна безпека, політика, Захід, Схід.

Serhii Fedoniuk,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0003-2853-8905;

Ihor Karpuk,
Lesya Ukrainka Volyn National University,
ORCID ID: 000-0003-4430-6004

CONCEPTS OF INFORMATION SECURITY IN THE ASPECT OF THE INTERESTS OF MAIN INTERNATIONAL ACTORS

This study defines the matter of information (cyber) security policy, its origins, and the goals of leading international actors in terms of international cooperation. We analyzed existing approaches to the study of international cooperation in the field of information (cyber) security and determined the subject area of research while taking into account the main scientific and regulatory approaches. We defined the main threats in the information sphere in terms of the interests of international relations. Additionally, we analyzed issues of international law related to the specifics of information and cyberspace. The study researched the approach to the implementation of policy and international activities of major international actors in the field of information (cyber) security – the United States, Russia, China, the European Union.

We determined that the dichotomy of the main concepts of information (cyber) security, based on the profound differences between democratic and authoritarian approaches in this policy area, is still growing and strengthening. At the heart of these differences are interests that are critical to

each of the systems. On the one hand, these are the interests of democratic systems based on the transparency of government and the need to preserve freedom of information and free competition. On the other hand, these are the interests of authoritarian systems, the strength of which is based on the total management of information and its control. Also the basis of the approach of authoritarian systems is created by the dominant participation of the state in public life and economy. Domestic and foreign information (cyber) security policies are based on these approaches. In accordance with their interests, the main international actors develop and promote relevant concepts of information (cyber) security on international platforms. They substantiate positions in the areas of state sovereignty, Internet governance, application of international law in cyberspace, availability of information technology, etc.
Key words: information security, politics, West, East.

1. ВСТУП

Постановка проблеми. Проблема інформаційної безпеки загострюється з розширенням сфери застосування інформаційно-комунікаційних технологій та мережної взаємодії. Це впливає на міжнародні відносини й зовнішню політику країн світу. Відповідно, сьогодні наявні різні дослідницькі бачення й підходи, що відображають підходи основних міжнародних акторів у їхній внутрішній політиці й зовнішній стратегії стосовно розвитку сфери інформаційної безпеки. Протягом десятиліть триває конкуренція між цими акторами на рівні головних міжнародних майданчиків, а самі концепції підлягають впливу з боку змінної міжнародної обстановки, нових інформаційно-комунікаційних технологій і загалом суспільних відносин, що розвиваються й змінюються в умовах технологічного прогресу й інших чинників. Тому із погляду позиціонування в зовнішній політиці та стратегічного планування у сфері інформаційної (кібер) безпеки важливо розуміти підґрунтя зазначених явищ. Для цього потрібно проаналізувати підходи до дослідження міжнародного співробітництва у сфері інформаційної (кібер) безпеки; визначити предметну сферу дослідження з урахуванням основних наукових і нормативно-правових підходів; конкретизувати основні загрози в інформаційній сфері з погляду інтересів суб'єктів міжнародних відносин, визначити пов'язані зі специфікою інформації й кіберпростору проблеми міжнародно-правового характеру; дослідити підходи в реалізації політики й міжнародної діяльності основних

міжнародних акторів у сфері інформаційної (кібер) безпеки (США, Росії, Китаю, Європейського Союзу).

Аналіз останніх досліджень і публікацій. Відповідно до поставлених завдань ми розглянули різні публікації в аспекті виявлення принципових позицій і підходів щодо основних проблемних сфер інформаційної (кібер) безпеки. Зокрема, ураховано, що в академічному дискурсі більш поширений термін «кібербезпека» й у цьому контексті розглядаються злочинні та терористичні загрози, а також із такої позиції досліджують загрози військово-політичного характеру, переважно в аспекті інформаційно-технічного впливу (наприклад А. Венгер [1], Г. Джакомелло [2], М. Хансен і Г. Ніссенбаум [3], Е. Тік-Рінгас [4] та ін.). Натомість представники іншого погялду використовують термін «інформаційна безпека», ураховуючи чотири головні загрози національній і міжнародній безпеці в інформаційній сфері – загрозу злочинності, тероризму, військово-політичного впливу й загрозу порушення громадського порядку та стабільності через вплив на громадську думку в державі (М. Кучерявий [5], А. Смирнов [6], Д. Швець [7] й ін.). Це переважно російські автори.

Суттєво відрізняються думки науковців і на принципи управління інтернетом. Тут також виділяються саме представники російських дослідницьких кіл, які, вочевидь, стежать за державними підходами, характерними для росії, Китаю й деяких інших країн. Суть підходу полягає в «суверенізації» управління мережею. А представники держав Заходу відстоюють незалежність інтернету від державного контролю на користь моделі багатостороннього управління за участі всіх зацікавлених сторін (пор. статті А. Бикова [8], М. Якушева [9] й праці таких учених, як І. Курбалія [10], Т. Бальзак і М. Данн-Кавелті [11], Д. Маклін [12], Дж. Хоффман [13]).

Проблематика військово-політичних загроз в інформаційній сфері глибоко досліджена в низці праць, серед яких – найбільш відомі роботи М. Лібіцкі [14], Р. Моландера [15], А. Шафранскі [16] та ін. Тут потрібно відзначити, що для країн Заходу, як уже зазначалося, характерна суто утилітарна концепція використання кіберпростору у військово-політичному контексті. Натомість російські автори наполягають на концепції «інформаційних війн» у найширшому сенсі (Т. Анічкіна [17], І. Панарін [18], С. Туронок [19]).

Концептуальне сприйняття інформаційно-безпекового домену в контексті суб'єктної сфери світової політики досліджується як у загальнотеоретичному плані (Д. Бетц [20], Дж. Най [21],), так і в контексті взаємодії між провідними акторами в цій сфері, якими

визнаються США, росія й Китай (Р. Дайберт [22], Дж. Ліндсей [23]). У своєму дослідженні ми дотримуємося провідної в репрезентантів країн Заходу позиції, відповідно до якої до інформаційної сфери й забезпечення кібербезпеки застосовуються різні інструменти міжнародного співробітництва. Причому увага приділяється передусім кібербезпеці, проблематику розроблення нормативних основ якої на міжнародній арені висвітлювали такі науковці, як Д. Фаррелл [24], М. Фіннемор [25].

Проблематика інформаційної (кібер) безпеки з правового погляду представниками країн Заходу, зокрема членів НАТО, розкривається з позицій, висвітлених у виданні, відомому як «Талліннський посібник» [26], підготовленому в Центрі дослідження й моніторингу кіберзагроз НАТО. Але тут також поширені роботи авторів, котрі репрезентують два табори із суттєво відмінними поглядами на перспективи міжнародного права в цій сфері. Частина дослідників наполягає на необхідності адаптації права з урахуванням специфіки інформаційного простору, у той час як інші виступають за необхідність вироблення правил застосування вже наявних норм. До перших належать майже винятково російські автори (А. Коротков, О. Зінов'єва [27], О. Крутських [28], А. Федоров, О. Зінов'єва [29]), а іншу групу репрезентують представники країн Заходу, наприклад Л. Грінберг, С. Гудман, К. Су Ху [30] та ін.

Серед українських науковців немає одностайності в трактуванні розглянутих вище проблем в аспекті «західного» чи «східного» дискурсу, хоча до останнього часу переважали обґрунтування «сильної» позиції держави в питаннях інформаційної безпеки й «інформаційного суверенітету» (О. Солодка [31]), що характерно також для представників російських наукових шкіл, з охопленням сфери, ширшої, ніж та, що стосується кіберпростору в «західному» розумінні, наприклад питань «культурної експансії», розробки спеціального домену в міжнародному праві стосовно інформаційно-безпекових питань (В. Настюк і В. Бєлєвцева [32], О. Кісілевич-Чорнойван [33]), позитивного оцінювання відповідних російських ініціатив на рівні ООН у контексті «режиму міжнародної інформаційної безпеки» (О. Фролова [34; 35]). А. Костирев пояснює протиріччя в розглянутих концепціях інформаційної (кібер) безпеки прихильністю їхніх послідовників до ідеалістської або реалістської парадигм [36]. Сучасні публікації провідних науковців у цій сфері частіше розкривають реальний стан справ у балансуванні підходів основних акторів, країн і міжнародних організацій до політики інформаційної безпеки (М. Копійка [37], Ю. Романчук [38], Є. Макаренко, М. Рижков, М. Ожеван та ін. [39]).

Мета статті. Наше дослідження охоплює питання політики інформаційної безпеки на рівні основних міжнародних акторів щодо балансу між східною й західною концепціями інформаційної (кібер) безпеки з урахуванням основних тенденцій у цій сфері задля конкретизації й позиціювання їхніх підходів в аспекті міжнародної взаємодії.

Методика дослідження. Для досягнення мети дослідження використано описовий, аналітичний підходи базовані на аналізі джерел, що стосуються політики у сфері інформаційної (кібер) безпеки в аспекті основних світових концепцій. Із метою вивчення проблематики, що потребує дослідження стосовно розвитку міжнародних відносин, застосовано якісний підхід.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

По суті, існує два різних бачення інформаційної безпеки з погляду політики. Частина держав практикує норми, які включають сильний урядовий контроль над інформацією, тоді як інші сприймають таку позицію, як загрозу політичній стабільності.

Концепція країн Заходу

Концепція, що сформувалась у США, ґрунтується на розумінні інформаційної безпеки як безпеки даних і, відповідно, інформаційних систем, які з ними пов'язані. Регулювання сфери інформації стало пріоритетом американської державної політики раніше, ніж в інших країнах, оскільки США були епіцентром інформаційної революції вже в другій половині ХХ ст., і розвивалися відповідно до принципів функціонування демократичної соціально-економічної моделі. Головним завданням стало гарантування рівних можливостей виробництва й споживання інформації кожному індивіду.

Американське законодавство розглядає дані й інформацію в аспекті їх комерційного значення, володіння та розповсюдження якої уможливлює отримання вигоди або уникнення збитків. У федеральному Законі про свободу інформації (Freedom of Information Act, FOIA (1966) [40]) закріплено підзвітність влади народові, якому вона служить. Із погляду демократії поінформований електорат є критично важливим для її належного функціонування. Тому інформаційна безпека розкривається в аспекті кібербезпеки, тобто безпеки даних в інформаційних системах, і має на меті забезпечення їх функціонування задля належної діяльності виконавчої влади та її звітності перед народом.

Також держава повинна забезпечити охорону інформації як приватної власності, що належить особі. У США свобода волевиявлення й

свобода слова гарантовані першою поправкою до Конституції, а кодекс добросовісної інформаційної практики, що регулює збір, технічне обслуговування, використання й розповсюдження особистої інформації, що ведеться в системах записів федеральних органів, установлено з прийняттям у 1974 р. Закону про конфіденційність (The Privacy Act [41]). Держава не може безпосередньо вводити цензуру або фільтрувати зміст інформації, що теж становить основу свободи інформації й відповідної концепції інформаційної безпеки. Такий підхід відповідає характерному для США неприйняттю державного регулювання, а це забезпечує ефективні ринкові відносини. У цій моделі відносин між державою, громадянами та суб'єктами ринку, із погляду інформаційної безпеки, логічним виявляється забезпечення стійкого функціонування насамперед інфраструктури, а не самої інформації. Відтак у фокусі – саме процеси передавання, зберігання й обробки даних і відсутність принципового інтересу до проблеми впливу «шкідливого» контенту (небажаного інформаційного впливу) на діяльність держави, суспільства, особистості. Тому, наприклад, саме поняття «інформаційна безпека» розкривається Комітетом із систем національної безпеки США як захист інформації й інформаційних систем від несанкціонованого доступу, використання, розкриття, руйнування, зміни чи знищення задля забезпечення цілісності (захист від несанкціонованої модифікації чи знищення інформації), конфіденційності, а також доступності (забезпечення своєчасного та надійного доступу до інформації) [42]. У контексті інформаційної безпеки американська Асоціація аудиту й контролю інформаційних систем «забезпечує, що лише авторизовані користувачі (конфіденційність) мають доступ до точної й повної інформації (цілісність), коли це потрібно (наявність)» [43]). Загалом американський підхід утілено в низці національних документів стратегічного планування (Національна стратегія захисту кіберпростору (2003); Всеосяжна національна ініціатива з кібербезпеки (2008); Огляд політики в кіберпросторі (2009); Міжнародна стратегія для кіберпростору (2011); Національна кіберстратегія Сполучених Штатів Америки (2018)) й ініціативах США на рівні міжнародних організацій, насамперед ООН.

На подібних принципах засновано й політику Європейського Союзу у сфері інформаційної безпеки, що вперше сформульовано у 2001 р. в комюніке Європейської комісії «Мережева й інформаційна безпека: пропозиції для підходу європейської політики». У цьому документі визначено термін «мережева й інформаційна безпека» (Network and Information Security) як здатність мережі або інформаційної системи на заданому рівні надійності протистояти випадковим загрозам або умис-

ним шкідливим діям, які ставлять під загрозу доступність, достовірність, цілісність і конфіденційність збережених або переданих даних і пов'язаних із ними служб. Доступ до них здійснюється за допомогою таких мереж або систем. Також запропоновано принципи політики щодо забезпечення мережевої й інформаційної безпеки, загалом властиві західному підходу в цій сфері з урахуванням особливостей реалізації галузевих і секторальних політик ЄС [70]: забезпечення прикладного характеру правових норм на основі загального розуміння основних питань безпеки та спеціальних заходів щодо її забезпечення; 2) необхідність постійного вдосконалення правового регулювання з урахуванням технічного прогресу й породжуваних ним нових загроз; 3) потреба в доповненні ринкових механізмів політичними заходами (що відображає важливість проблеми інформаційної безпеки, котра розглядається на рівні комунітарної політики ЄС); 4) формування європейського внутрішнього ринку інформаційно-телекомунікаційних послуг.

Європейський Союз загалом підтримував ініціативи США у сфері кібербезпеки, реалізував власні проєкти щодо кібербезпеки й розвивав міжнародну співпрацю з партнерами переважно у формі «кібердипломатії», проте, починаючи з 2020 р., став проявляти значну активність у цій сфері, прийнявши відповідну стратегію й ініціювавши принципово новий формат взаємодії зацікавлених сторін на рівні ООН – ініціативу щодо реалізації Програми дій із відповідальної поведінки держав у кіберпросторі, позиції щодо якої таких сторін, як США, росія та Китай, ще не визначені.

Схоже бачення інформаційної безпеки і в японського уряду, який сформулював відповідні цілі в Стратегії кібербезпеки Японії у 2013 р. [45]. Це – забезпечення вільного й безпечного обміну інформацією; виведення проблеми кібербезпеки на більш високий рівень; оптимізація відповідних дій, спрямованих на розв'язання проблеми кібербезпеки; розробка плану дій і зміцнення співробітництва на основі принципів соціальної відповідальності. Як і в усіх випадках західного підходу у сфері інформаційної (кібер) безпеки уряд забезпечує надійність і стійкість кіберпростору, забезпечує захист від кібернападів, стимулює науково-дослідницьку діяльність для розвитку кіберпростору, на конкурентній основі залучає нові кадри для забезпечення кібербезпеки й забезпечує освіту громадян із питань кібербезпеки. При цьому держава не втручається в питання свободи інформації.

Кіберпростір

Із позиції країн Заходу переважно розглядається концепт кіберпростору – «Cyberspace», який визначається в рекомендації «Про розвиток і

використання багатомовності в загальному доступі до кіберпростору», прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 р., як «віртуальний світ цифрової й електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою» [46]. Наукове визначення інформаційного простору в західному трактуванні наближене до кіберпростору: «Тип інформаційної конструкції, у якій репрезентації інформаційних об'єктів розташовані в організованому просторі. У такому просторі розташування й напрямок мають значення, таким чином стають можливими створення карт і навігація» [110].

У дослідженні «Tallinn manual on the international law applicable to cyber operations» (2013) запропоновано визначення кіберпростору як середовища, сформованого з фізичних і нефізичних елементів, що характеризується використанням комп'ютерів та електромагнітного спектра для зберігання, зміни й обміну даними з використанням комп'ютерних мереж [26].

У типовому навчальному плані НАТО з кібербезпеки (2016 р.) [47] є модуль «Структура інформаційного простору: опорна мережа інтернету й мережева інфраструктура держав», що стосується винятково технічних аспектів інформаційного простору. Основну увагу при цьому приділено глобальній інфраструктурі, а також інформаційним системам, створеним у масштабі держав й окремих підприємств. А інформаційний простір уключає в себе архітектуру інтернету, комп'ютерні та мобільні мережі, де передусім розглядаються принципи загальної структури й конкретна топологія інтернету в окремих державах (тобто національна інфраструктура, що підтримує роботу мереж, провайдери телекомунікаційних послуг, а також схеми маршрутизації).

Концепції росії й Китаю

На відміну від розглянутого вище концептуального підходу, у країнах, для яких не характерно культивування цінностей розвинених демократичних суспільств, значну увагу приділяють питанню захисту держави, суспільства й особистості від негативного інформаційного контенту. Це, передусім, росія та Китай.

Одним із перших документів, у якому сформульовано таке бачення, стала Доктрина інформаційної безпеки російської федерації [48], затверджена у вересні 2000 р. У 2016 р. прийнято нову доктрину [49], що стала логічним продовженням першої – якщо в документі 2000 р. йдеться про зростання впливу інформаційних технологій на національні інтереси країни, то в новій версії вони вже визнаються невід'ємною частиною всіх сфер життя. Для російського підходу характерне формулювання загроз,

пов'язаних, передусім, не з функціонуванням інформаційних систем, а з обігом інформації й свободою інформації. Причому ці загрози трактуються переважно щодо національної безпеки. Так, у доктрині інформаційної безпеки від 2000 р. серед ключових проблем було «розкладання моральних цінностей молоді». Стосовно цього інформаційна безпека країни – це стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства й держави. У доктрині 2016 р. головними загрозами названо кібеерзлочинність і поширення інформаційних матеріалів з-за кордону, які «дестабілізують ситуацію в країні» (наприклад таких, що критикують російську федерацію, популяризують тенденції, котрі тиснуть на молодь). Такі «проблеми» подаються як загрозливі для суспільства й особи, а влада обґрунтовує своє втручання в перебіг інформаційних процесів необхідністю захисту національного інформаційного поля від іноземних впливів.

Підхід авторитарних держав не передбачає безумовного гарантування свободи слова й масової інформації, відкриваючи шлях до цензури та контролю інформаційної сфери. І російська доктрина 2000 р. це підтверджує, формулюючи одну з ключових проблем так: «недостатність нормативного правового регулювання відносин у галузі реалізації можливостей конституційних обмежень свободи масової інформації в інтересах захисту основ конституційного ладу, моральності, здоров'я, прав і законних інтересів громадян, забезпечення обороноздатності країни й безпеки держави суттєво ускладнює підтримання необхідного балансу інтересів особистості, суспільства й держави в інформаційній сфері». Це створює підстави для цензури, оскільки серед загроз інформаційній безпеці країни названо «девальвацію духовних цінностей, пропаганду зразків масової культури, заснованих на культі насильства, на духовних і моральних цінностях, що суперечать цінностям, прийнятим в російському суспільстві; зниження духовного, морального й творчого потенціалу населення росії» [48].

По суті, у російських доктринах декларується підґрунтя для державного контролю в інформаційній сфері, але під гаслами «інформаційного суверенітету», або «кіберсуверенітету». Концепцію «інформаційного суверенітету» в країнах, що тяжіють до авторитарного типу організації суспільства, розробляють і втілюють у практику від початку масового поширення інтернет-технологій. Так, у Китаї на державному рівні кібер-суверенітет формується, починаючи з початку 2000-х. Інформаційний суверенітет трактується російською владою як «нерозповсюдження»

іноземної інформації серед російських громадян та обмін «належною інформацією про росію з іноземними партнерами» [49], у той час як у західній концепції суверенітет в інформаційну епоху – це заохочення глобального обміну інформацією через безпечну технологічну інфраструктуру.

У квітні 2014 р. Максим Кавджарадзе, член ради федерації, верхньої палати російського парламенту, запропонував створити повністю недоступну з-за кордону національну внутрішню мережу росії. Тоді з'явилась і назва – «ЧебурашкаNet», на честь російського мультиплікаційного героя Чебурашки – персонажа з відомого анімаційного фільму [50]. А у 2019 р. прийнято зміни до федерального законодавства, які отримали неформальну назву «Закон про суверенний інтернет» [51]. Метою його є – автономних систем управління інтернетом і тим самим створення можливості відокремлення російського інтранету від глобальної мережі «Інтернет». Відповідно до цього закону, від національних постачальників інтернет-послуг вимагається використання лише тих точок обміну інтернетом, які затверджені державним регулятором телекомунікацій. Окрім того, оператори зв'язку зобов'язані встановити на точках обміну трафіком спеціальне обладнання для аналізу й фільтрування трафіка всередині країни й лініях транскордонного передавання даних. Також росія отримує змогу відключення національної мережі від глобальної системи доменних імен.

Закон викликав деяке протистояння громадськості, що розглядає цю ініціативу як нову форму цензури. На відміну від Китаю, громадяни якого увійшли в епоху інтернету майже в той самий час, коли уряд почав його регулювати, і звикли до такого способу життя, де інтернет є національною інтрамережею, громадяни росії завжди мали доступ до глобальної мережі й широкого спектра контенту й послуг із будь-якої країни. Окрім того, сьогодні, порівняно з періодом становлення масового інтернету, мережа вже міцно «вросла» в економіку, яка залежить від інтернету та безперебійного функціонування певних додатків і послуг. У наш час відключення від іноземних цифрових послуг має великий негативний вплив на національну економіку. Тому такий «цифровий суверенітет» може виявитися надто дорогим для росії, уряд якої, проте, переслідує таким чином насамперед політичні й геополітичні цілі.

Принципова позиція держав, котрі практикують такий «східний» підхід в інформаційній безпеці, полягає в безапеляційному «захисті» владою певного «інформаційного суверенітету», тобто ідеологічному й нормативному обґрунтуванні права влади на втручання в інформаційну

сферу та відкидання свободи інформації для громадян. Це відображено в усіх основних нормативних актах, що детермінують сферу інформаційної безпеки й визначають позицію держави в її міжнародній діяльності в цій сфері. У росії це, крім згаданих вище Доктрин інформаційної безпеки, також «Основи державної політики в галузі міжнародної інформаційної безпеки на період до 2020 р.» [52] та «Основи державної політики російської федерації в галузі міжнародної інформаційної безпеки» [53]. В останньому документі (від 2013 р.) закріплено такі тези, як «втручання у внутрішні справи суверенної держави з використанням ІКТ, порушення суспільної стабільності, розпалювання міжетнічної й міжнаціональної ворожнечі». На противагу державам Заходу, підходи, засновані на прозорості, не підтримуються російськими чиновниками через нібито загрозу національному суверенітету. Тому, наприклад, у 2012 р. росія заблокувала резолюцію про раннє попередження про кібератаки в ОБСЄ.

Як дієвий інструмент для досягнення своїх цілей росія використовує спеціально розроблену термінологію, послідовно просуваючи й закріплюючи її на міжнародних майданчиках. Наприклад, серед термінів і визначень, уміщених у текст російського проєкту «Конвенції про забезпечення міжнародної інформаційної безпеки» [54] можна знайти такий: «Загроза в інформаційному просторі (загроза інформаційній безпеці)» – чинники, що створюють небезпеку для особистості, суспільства, держави та їхніх інтересів в інформаційному просторі. І далі в переліку таких загроз – «протидія доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності у сфері інформатизації на шкоду іншим державам». Тобто, з позиції росії, технологічна перевага, отримана на основі вільної конкурентної боротьби на світовому ринку ІКТ, також становить загрозу інформаційній безпеці, якщо власник технології добровільно не надасть її в розпорядження тим, хто такою технологією не володіє. Очевидно, росія так намагається нівелювати своє все більш відчутне технологічне відставання у сфері ІТ. З іншого боку, російська ідея міжнародної інформаційної безпеки передбачає значну відповідальність уряду й контроль над інформаційними ресурсами, що не відповідає інтересам учасників ринку ІКТ. Тому росія, просуваючи ці ідеї на міжнародному рівні, стикається із сильним спротивом західних країн, які відстоюють свободу ринку, гарантії вільної конкуренції й недоторканості інформації з погляду приватної власності.

Документальну основу розглянутої вище концепції інформаційної безпеки в росії становлять доктрини (інформаційної безпеки рф від 2000

і 2016 рр., військова доктрина рф), документи військово-стратегічного планування («Концептуальні погляди на діяльність збройних сил російської федерації в інформаційному просторі» (2011 р.)), російські ініціативи й стратегічні документи у сфері міжнародного співробітництва (проєкт «Конвенції про забезпечення міжнародної інформаційної безпеки» (2011 р.), «Основи державної політики в галузі міжнародної інформаційної безпеки на період до 2020 року», «Основи державної політики рф у галузі міжнародної інформаційної безпеки» (2021 р.)), внутрішнє законодавство (про обробку персональних даних, про локалізацію даних на території рф (2014), зміни до федерального законодавства під неформальною назвою «Закон про суверенний інтернет» (2019 р.) та ін.).

Схожий підхід демонструє й китайська влада, визначивши в документі під назвою «Національна стратегія розвитку інформатизації на 2006–2020 рр.» інформаційну безпеку ключовим компонентом системи національної безпеки для забезпечення сталого, здорового застосування інформаційних технологій, а також для соціальної й культурної стабільності та ідеологічного розвитку [55].

Типово авторитарна концепція інформаційної безпеки означає винятковий пріоритет держави в питаннях інформаційної діяльності не лише на суверенній території, але й у певному інформаційному полі, яке держави вважають підконтрольним собі, оголошуючи над ним «інформаційний суверенітет». При цьому не береться до уваги глобальний характер мережі «Інтернет», яка і є технологічною основою цього інформаційного поля. Прикладом нормативного обмеження свободи інформації в інтернеті з мотивів її «захисту» є китайський закон про кібербезпеку, прийнятий у 2016 р. [56]. Відповідно до цього документа, який стосується збору, зберігання й використання персональних даних китайських громадян та інформації, що має стосунок до національної безпеки, такі відомості повинні зберігатись усередині країни. Також заборонено експорт економічних, технологічних, наукових даних, що «становлять загрозу національній безпеці чи громадським інтересам». У росії також із 2015 р. діє норма, що зобов'язує операторів обробляти й зберігати персональні дані росіян із використанням баз даних, розміщених на території країни. В основу законів, що охоплюють цивільну сферу безпеки кіберпростору в Китаї, покладено так звану «класифікацію багаторівневої системи захисту» (Multiple-level Protection Scheme, MLPS), відповідно до якої приймаються рішення про рівень допуску іноземних товарів у ту чи іншу сферу або систему. MLPS визначає п'ять рівнів інформаційної безпеки щодо потенційних

наслідків, від шкоди правам громадян й організацій і громадському порядку до загрози національній безпеці [57]. Покладаючись на MLPS та законодавство, влада вимагає доступу до протоколів шифрування й значної частини вихідного коду від компаній, що працюють у сфері фінансів, телекомунікацій, медицини, освіти й енергетики.

У часовому вимірі китайське законодавство у сфері інформаційної безпеки еволюціонувало від розроблених у 2000-х рр. Державної стратегії інформатизації (2006) і документа Держради КНР із просування інформатизації й розвитку чинної системи захисту інформаційної безпеки (2012) до законів КНР про боротьбу з тероризмом (2015), про кібербезпеку (2016), Міжнародної стратегії співробітництва в кіберпросторі, Положення про нагляд і перевірку безпеки в інтернеті (2018) і законів про захист особистої інформації (2021) і про безпеку даних (2021).

Однією з основних рис, що характеризують підхід китайської влади до мінімізації інформаційних загроз, є запобігання проникненню небажаної інформації всередину країни й обмеження витоку чутливої інформації за кордон, що реалізовано, зокрема, шляхом блокування соціальних мереж і пошукових систем. Адже щодо політичного керівництва Китаю суть інформаційної безпеки полягає в обмеженні поширення інформації, яку вона вважає небажаною [58].

Інформаційний простір

На відміну від властивої для країн Заходу концепції «кіберпостору» в російській офіційній практиці застосовується поняття «інформаційного простору», зручне з погляду обґрунтування «інформаційного суверенітету». Відповідно до запропонованого російською владою проєкту «Конвенції про забезпечення міжнародної інформаційної безпеки», поняття «інформаційний простір» подається як «сфера діяльності, пов'язана з формуванням, створенням, перетворенням, передачею, використанням, зберіганням інформації, що здійснює вплив, у тому числі на індивідуальну й суспільну свідомість, інформаційну інфраструктуру і власне інформацію» [54]. На відміну від більш поширеного в російськомовному науковому сегменті конструктивного розуміння «інформаційного простору» як сукупності інформаційних ресурсів, створених суб'єктами інформаційної сфери, засобів взаємодії таких суб'єктів, їх інформаційних систем і необхідної інформаційної інфраструктури (див., наприклад, у [59; 60]), тут це поняття відображає політичну думку російського керівництва про суть міжнародних відносин в інформаційній сфері як спосіб отримати певні вигоди для держави-актора.

Відмінності між західною та східною концепціями у сфері політики інформаційної безпеки проявляються на практиці в підходах до страте-

гії розвитку самого кіберпростору. У країнах Заходу базовий підхід до політики кібербезпеки в епоху інтернету – правило мережевого нейтралітету, що означає забезпечення рівного доступу та швидкості спілкування для кожного користувача, виключаючи таким чином будь-яку можливість маніпулювання вмістом. Принцип мережевого нейтралітету підтримується Федеральною комісією зв'язку США [61] на підставі Закону про комунікації (1934 р.), хоча й піддавався певним обмеженням у період президенства Д. Трампа. Також цей принцип присутній у більшості європейських стратегій кібербезпеки, а на рівні Європейського Союзу його закладено в стратегію Єдиного цифрового ринку ЄС (проголошено у 2015 р.). Основні рамки для забезпечення нейтралітету мережі на території всього Європейського Союзу, зокрема, установлено Регламентом ЄС 2015/2120 [62].

Країни, де домінує авторитарний підхід, не забезпечують невтручання в роботу мережі. Наприклад, у росії на початку 2018 р. кабінет міністрів запропонував формально відмовитися від принципу мережевого нейтралітету, який і так не підтримувався в країні [63]. Не застосовується принцип мережевої нейтральності й у Китаї, де уряд використовує інтернет-провайдерів для перевірки й регулювання вмісту, доступного для громадян країни. За допомогою так званого «великого брандмауера» блокуються як іноземні, так і китайські сайти, що надають інформацію, яку уряд не може ефективно змінити, наприклад IP-адреси соціальних мереж або інформаційні сайти [64].

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На рівні міжнародної стратегії провідних акторів щодо забезпечення інформаційної (кібер) безпеки сформовано два принципово відмінні підходи. Перший характерний для демократичних держав Заходу (США, їхні партнери по НАТО, країни ЄС, Японія). Послідовниками другого є росія, Китай і низка інших країн із відносно менш розвиненою демократією. Розподіл країн світу за підходами відображають, наприклад, результати голосування в ООН за проєкти резолюцій ГА ООН у 2018 р.: «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» (поданий росією) та «Заохочення відповідальної політики держав у кіберпросторі в контексті міжнародної безпеки» (США) й інших ініціатив зазначених держав у сфері інформаційної безпеки й протидії кіберзлочинності. Цікаво, що російський проєкт підтримали переважно держави, віднесені організацією Freedom House в її щорічних звітах [65],

відповідно до їх демократичного статусу до категорії «не-вільних». А «вільні» й «частково вільні» держави підтримали американську ініціативу. Зусилля й результати пошуку шляхів подолання суперечностей між прихильниками тих чи інших позицій у рамках обох підходів відображені у звітах Груп урядових експертів (ГУЕ) та Робочої групи відкритого складу (РГВС), скликаних згідно з цими резолюціями на рівні ООН.

Із погляду розглянутих підходів по-різному трактується поняття «інформаційна безпека». Держави, що забезпечують свободу інформації, орієнтуються майже лише на технічні питання безпеки кіберсерпростору (захист комп'ютерних мереж і ресурсів), що формулюється, як «кібербезпека», а не «інформаційна безпека». Із такого погляду інформація безпечна, доки безпечна технологічна інфраструктура, а відповідальність уряду полягає в тому, щоб кожен громадянин міг вільно користуватися безпечними технологіями. Натомість держави, котрі практикують авторитарні підходи, уключають у це поняття також політико-ідеологічні аспекти – протидію пропаганді й недопущення інформаційного впливу, а їхні уряди забезпечують безпеку не лише інфраструктури, але й самої інформації, декларуючи її невід'ємним складником національного суверенітету.

Відмінність між підходами проявляється в усіх аспектах інформаційної безпеки, таких як протидія злочинності, тероризму, загрозам військово-політичного характеру, застосування міжнародного права й міжнародне співробітництво у сфері безпеки кіберпростору. Наприклад російський підхід, порівняно зі сприйняттям кібертероризму в західних країнах, полягає в розгляді терористичних загроз у числі комплексних загроз особі, суспільству й державі (такого підходу притримується й китайська влада). Але на Заході кібертероризм трактують як загрозу інформаційним системам, що пов'язані передусім із критичною інфраструктурою.

Суттєво відрізняються підходи до розуміння інформаційних впливів із погляду військово-політичної стратегії. В авторитарних системах застосовується концепція «інформаційних війн», що означає інтегральний вплив усієї державної «машини» в комплексі із силовими структурами й підконтрольним медіасектором. Натомість західний підхід, характерний для США та країн НАТО, що відповідає реаліям суспільних комунікацій, де держава не втручається в медійну сферу, полягає в розділенні військових і цивільних інформаційних впливів у взаємозв'язку з реалізацією стратегічних інтересів уряду. Сьогодні це система «стратегічні комунікації» в складі компонентів – інформаційних операцій, інформаційно-психологічних операцій, публічної дипломатії, військової й цивільної комунікації.

Проблемою в аспекті міжнародного співробітництва є діаметрально різні підходи до розуміння ролі міжнародного права у сфері інформаційної (кібер) безпеки (безпеки кіберпростору). По-перше, право jus ad bellum (сфера Статуту ООН) розглядається росією та її однодумцями в позитивістському ключі, тобто вони наполягають на обмеженні застосування сили державами, а США й інші країни Заходу виступають за більш широкі можливості застосування сили. Це пов'язано переважно з відчутним відставанням перших в інформаційно-технологічному плані. По-друге, у сфері міжнародного гуманітарного права (jus in bello) росія, Китай, їхні союзники по ШОС і низка інших держав (які переважно не характеризуються високим рівнем демократії) виступають за формування в міжнародному праві окремого домену «інформаційної безпеки», створення спеціальних обов'язкових «правил поведінки» держав і просувають російську концепцію «міжнародної інформаційної безпеки» – правового режиму й формату співробітництва в цій сфері. Держави Заходу наполягають на застосовності до сфери кіберпростору чинних норм міжнародного права, спільного реагування на нові кіберзагрози й добровільних і необов'язових нормах поведінки держав у кіберпросторі. Натомість у випадку військових конфліктів, нападів в усіх передбачених нормами міжнародного гуманітарного права випадках цілком можуть застосовуватися чинні норми, що відображено в «Талліннському посібнику» (Tallinn Manual), розробленому в контексті діяльності НАТО.

Росія активно й послідовно просуває на рівні ООН і регіональних міжнародних організацій свою концепцію «міжнародної інформаційної безпеки», із кінця 1990-х рр. пропонуючи порядок денний, суть якого опрацьовується в контексті запропонованих нею проєктів резолюцій ГА ООН «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки», висуваючи на рівень ООН проєкти «правил поведінки» держав у кіберпросторі й конвенції про кіберзлочинність. В основу російських пропозицій покладено керівну роль держави в усіх аспектах і процесах інформатизації й телекомунікацій, у тому числі в управлінні інтернетом та «інформаційному суверенітеті». Головним треком розвитку співпраці на рівні ООН за ініціативами росії є Робоча група відкритого складу.

На двох останніх позиціях наполягає й Китай, загалом підтримуючи всі російські ініціативи. КНР також розширює сферу впливу щодо безпеки кіберпростору, розвиваючи співробітництво з державами, що становлять для нього стратегічний інтерес, і пропонуючи світові авторитарну модель управління інтернетом («Уженські ініціативи»).

Головним майданчиком для опрацювання спільних позицій Росії й Китаю в цьому аспекті є ШОС.

Сполучені Штати відстоюють свою концепцію ліберального підходу до розвитку кіберпростору та багатостороннього управління інтернетом, необов'язкових норм поведінки держав у кіберпросторі (проєкт резолюції ГА ООН «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки», 2018 р.). США наполягають на доцільності використання результатів, досягнутих у рамках Групи урядових експертів (2010, 2013 і 2015 рр.), запропонувавши однойменний трек у згаданій вище резолюції.

Також розглянуті концептуальні відмінності у сфері інформаційної безпеки проявляються і в підходах щодо кіберзлочинності. Тоді як США і ЄС активно пропагують розвиток міжнародної співпраці в протидії кіберзлочинності у форматі, визначеному «Будапештською конвенцією», росія наполягає на необхідності розробки спеціального формату співпраці в рамках промованого нею проєкту конвенції ООН, який би обмежував цю співпрацю й виводив кіберзлочинність зі сфери міжнародного контролю.

Розглянуті в статті суперечності покладено в основу проблеми пошуку єдиної основи для міжнародного співробітництва у сфері інформаційної безпеки. Росія й США активно просувають свої концепції в аспекті міжнародного права й управління інтернетом. Також протягом останніх років у цю дуалістичну систему противаг на рівні ООН уключився Європейський Союз. У таких умовах держави, що формують власну стратегію співпраці з міжнародними партнерами, повинні враховувати як основні, так і детальні особливості політики провідних світових акторів у царині кіберпростору й глобальної безпеки, що і є предметом наступних досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wenger, A. (2001) The Internet and the Changing Face of International Relations and Security. *Information and Security*, № 7, p. 5–11.

2. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. Ed by G. Giacomello. Bloomsbury Publishing USA, 2014.

3. Hansen, L., Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, №. 4, p. 1155–1175.

4. Tikk-Ringas, E. (2015). Evolution of the Cyber Domain: The Implications for National and Global Security. London. Routledge, for the International Institute for Strategic Studies, 212 p.

5. Кучерявый, М. М. (2013). Глобальное информационное общество и проблемы безопасности. *Власть. Общенациональный научно-политический журнал*, № 9 (сентябрь), с. 89–92.

6. Глобальная безопасность: инновационные методы анализа конфликтов/под ред. А. И. Смирнова. Москва: Общество «Знание» России, 2011, 272 с.

7. Швец, Д. Ю. (2005). Информационная безопасность Российской Федерации в современных международных отношениях: автореф. дис. … канд. социологических наук. Москва: МГИМО (У) МИД России.

8. Быков, И. А. (2008). Управление Интернетом как одна из проблем современных международных отношений. *Политэкс*, № 2. URL: https://cyberleninka.ru/article/n/upravlenie-internetom-kak-odna-iz-problem-sovremennyh-mezhdunarodnyh-otnosheniy (дата обращения: 18.11.2021).

9. Якушев, М. В. (1999). Информационное общество и правовое регулирование: новые проблемы теории и практики. *Информационное общество*, № 1. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e09339699c32568b1003ab653

10. Kurbalija, Jovan (2014). An Introduction to Internet Governance. *DiploFoundation*. 206 p.

11. Balzacq, T., Cavelty, M. D. (2016). A theory of actor-network for cyber-security, *European Journal of International Security*, № 2, p. 176–198.

12. Internet Governance: A Grand Collaboration. Ed. by D. MacLean. N.Y. *UN ICT Task Force Series*, 2005, 393 p.

13. Hofmann, J. (2005) Internet Governance: A Regulative Idea in Flux. Social Science Research Centre. Berlin. URL: http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf

14. Libicki, M. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation.

15. Molander, Roger C., Riddile, Andrew, Wilson, Peter A. (1996). Strategic Information Warfare. *A New Face of War. RAND*. *MR-661-OSD*. URL: https://www.rand.org/pubs/monograph_reports/MR661.html

16. Szafranski, R. (1995). A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*, №1.

17. Аничкина, Т. Б. (2007). О некоторых приемах информационной войны США. *США–Канада: экономика, политика, культура*, № 7, с. 123–127.

18. Панарин, И. (2006). Информационная война и геополитика. *Поколение*, 560 с.

19. Туронок, С. Г. (2003). Информационно-коммуникативная революция и новый спектр военно-политических конфликтов. *Политические исследования*, № 1, с. 24–38.

20. Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies*, № 5, p. 689–711.

21. Nye, J. (2011). The future of power. NY: Basic Books, 300 p.

22. Deibert, R. (2015) Trajectories for Future Cybersecurity Research. The Oxford Handbook of International Security/ed. by A. Gheciu and W. C. Wohlforth. Oxford: Oxford University Perss, p. 531–556.

23. Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, vol. 39, № 3, p. 7–47.

24. Farrell, H. (2015). Promoting Norms for Cyberspace. New York: Council on Foreign Relations.

25. Finnemore, M. (2011) Cultivating International Cyber Norms. America's Cyber Future: Security and Prosperity in the Information Age/ed. by K. Lord, T. Sharp. Washington, DC: Center for a New American Security, p. 89–101.

26. Tallinn Manual on the International Law Applicable to Cyber Warfare /ed. by M. Schmitt. New-York: Cambridge University Press, 2013, 282 p.

27. Коротков, А. В., Зиновьева, Е. С. (2011). Безопасность критических информационных инфраструктур в международном гуманитарном праве. *Вестник МГИМО-Университета*, № 4, с. 154–162.

28. Крутских, А. В. (2007). К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*, № 1 (5), с. 28–37.

29. Федоров, А. В., Зиновьева, Е. С. (2017). Международная информационная безопасность: политическая теория и дипломатическая практика. Москва: МГИМО, 360 с.

30. Greenberg, L. T., Goodman, S. E., Soo Hoo, K. J. (1997). Information Warfare and International Law. Washington. National Defense University Press, 1997.

31. Солодка, О. М. (2020) Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*, № 1 (32)/2020. URL: http://il.ippi.org.ua/article/view/200311

32. Настюк, В. Я., Бєлєвцева, В. В. Правові засади міжнародного співробітництва щодо протидії інформаційним правопорушенням. *Правова інформатика*, № 2 (42)/2014. URL: http://ippi.org.ua/sites/default/files/14nvypip.pdf

33. Кісілевич-Чорнойван, О. М. (2009). Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*, № 8, с. 11–18. URL: http://nbuv.gov.ua/UJRN/utp_2009_8_2

34. Фролова, О. (2019). Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні відносини*, вип. 46, с. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13

35. Фролова, О. М. (2018). Роль ООН в системі міжнародної інформаційної безпеки. *Електронне видання Інституту міжнародних відносин «Міжнародні відносини. Серія: Політичні науки»*, № 18.

36. Костирєв, А. (2010). Політико-правові проблеми розбудови системи міжнародної інформаційної безпеки в умовах глобалізації. *Сучасна українська політика. Політики і політологи про неї.* Київ, вип. 21, с. 234–246.

37. Kopiika, M. (2020). Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя*, 1–2020, с. 102–109. URL: https://jpl.donnu.edu.ua/article/view/7967/7967

38. Романчук, Ю. В. (2009). Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти. автореф. дис. ... канд. політ. наук: 23.00.04. НАН України. Ін-т світ. економіки і міжнар. відносин. Київ, 20 с.

39. Міжнародна інформаційна безпека: теорія і практика: підручник / Макаренко Є. А., Рижков М. М., Ожеван М. А. та ін. Київ. Центр вільної преси, 2016, 418 с.

40. The Freedom of Information Act. U.S. Department of State. URL: https://foia.state.gov/learn/foia.aspx

41. Privacy Act of 1974. U.S. Department of Justice. URL: https://www.justice.gov/opcl/privacy-act-1974

42. Committee on National Security Systems: National Information Assurance (IA) Glossary, *CNSS Instruction*, No. 4009, 26 April 2010.

43. ISACA. (2008). Glossary of terms. URL: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

44. Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions *«Network and Information Security: Proposal for A European Policy Approach»*, Brussels, 6.6.2001. COM (2001) 298 final.

45. Japan Cybersecurity Strategy. *Information Security policy Council*, 2013. URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

46. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству. Принята 15 октября 2003 года. UN. URL: https://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml

47. DEEP: Cybersecurity – A Generic Reference curriculum. NATO. URL: https://www.nato.int/cps/en/natohq/topics_157591.htm

48. Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895) Совет безопасности РФ. URL: http://www.scrf.gov.ru/documents/5.html

49. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

50. Канев, Сергей (2014). Чебурашка, или Хорошими делами прославиться нельзя. *Новая Газета*, 5 мая 2014. URL: https://novayagazeta.ru/articles/2014/05/05/59473-cheburashka-ili-horoshimi-delami-proslavitsya-nelzya

51. Принят закон о «суверенном интернете». Государственная Дума Федерального собрания Российской Федерации. 16.04.2009. URL: http://duma.gov.ru/news/44551/

52. Основы государственной политики в области международной информационной безопасности на период до 2020 года. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/

53. Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). URL: http://www.scrf.gov.ru/security/information/document114/

54. Convention on International Information Security. The Ministry of Foreign Affairs of the Russian Federation. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

55. 2006–2020 年国家信息化发展战略 (2006–2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè). 08.05.2005. URL: https://bit.ly/3FsA8VK

56. 中华人民共和国网络安全法 (Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ). 07.11.2016. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

57. Yan Luo, Zhijing Yu, Nicholas Shepherd (2021) Cybersecurity risk classification under China's multi-level protection scheme. Practical Law. Thomson Reuters. URL: https://uk.practicallaw.thomsonreuters.com/w-022-3160?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true

58. 汪玉凯: 中央网络安全与信息化领导小组的由来及其影响 (Wāngyùkǎi: Zhōngyāng wǎngluò ānquán yǔ xìnxī huà lǐngdǎo xiǎozǔ de yóulái jí qí yǐngxiǎng). Baidu.com. 06.03.2014. URL: https://wenku.baidu.com/view/0c29475252d380eb62946d86.html.

59. Манойло, А. В. (2003). Государственная информационная политика в особых условиях: монография. Москва: МИФИ, 388 с.

60. Ryjov, Alexander P., Mikhalevich, Igor F. (2020). Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures. *In Handbook of Research on Cyber Crime and Information Privacy*, p. 310–337.

61. Statement of acting chairwoman Rosenworcel on Department of Justice decision to withdraw lawsuit to block California net neutrality law. URL: https://docs.fcc.gov/public/attachments/DOC-369799A1.pdf

62. REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015. laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2

63. Правительство РФ не видит необходимости в законодательном закреплении сетевого нейтралитета. Роскомсвобода, 29 октября 2018. URL: https://roskomsvoboda.org/42667/

64. Hu, Henry L. (2011). The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration. The China Quarterly, 207 (207), 523–540.

65. Global Freedom Status. Freedom House. https://freedomhouse.org/explore-the-map?type=fiw&year=2021.

REFERENCES

1. Wenger, A. (2001). The Internet and the Changing Face of International Relations and Security. *Information and Security*, № 7, p. 5–11.

2. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. Ed by G. Giacomello. Bloomsbury Publishing USA, 2014.

3. Hansen, L., Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, № 4, p. 1155–1175.

4. Tikk-Ringas, E. (2015). Evolution of the Cyber Domain: The Implications for National and Global Security. London. *Routledge, for the International Institute for Strategic Studies*, 212 p.

5. Kucheryavyj, M. M. (2013). Global'noe informacionnoe obshchestvo i problemy bezopasnosti. *Vlast'. Obshchenacional'nyj nauchno-politicheskij zhurnal*, № 9 (sentyabr'), p. 89–92.

6. Global'naya bezopasnost': innovacionnye metody analiza konfliktov/pod red. A. I. Smirnova. M. Obshchestvo «Znanie» Rossii, 2011, 272 p.

7. Shvec D. Yu. (2005) Informacionnaya bezopasnost' Rossijskoj Federacii v sovremennyh mezhdunarodnyh otnosheniyah. avtoref. diss. … kandidata sociologicheskih nauk. Moskva: MGIMO (U) MID Rossii.

8. Bykov, I. A. (2008). Upravlenie Internetom kak odna iz problem sovremennyh mezhdunarodnyh otnoshenij. *Politeks*, № 2. URL: https://cyberleninka.ru/article/n/upravlenie-internetom-kak-odna-iz-problem-sovremennyh-mezhdunarodnyh-otnosheniy (data obrashcheniya: 18.11.2021).

9. Yakushev, M. V. (1999). Informacionnoe obshchestvo i pravovoe regulirovanie: novye problemy teorii i praktiki. *Informacionnoe obshchestvo*, № 1. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e09339699c32568b1003ab653

10. Kurbalija, Jovan (2014). An Introduction to Internet Governance. DiploFoundation. 206 p.

11. Balzacq, T., Cavelty, M. D. (2016). A theory of actor-network for cyber-security, *European Journal of International Security*, № 2, p. 176–198.

12. Internet Governance: A Grand Collaboration/ed. by D. MacLean. New-York. UN ICT Task Force Series, 2005, 393 p.

13. Hofmann, J. (2005). Internet Governance: A Regulative Idea in Flux. Social Science Research Centre. Berlin, 2005. URL: http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf

14. Libicki, M. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation.

15. Molander, Roger C., Riddile, Andrew, Wilson, Peter A. (1996). Strategic Information Warfare. A New Face of War. RAND. MR-661-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR661.html

16. Szafranski, R. (1995). A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*, № 1.

17. Anichkina, T. B. (2007). O nekotoryh priemah informacionnoj vojny SSHA. *SSHA-Kanada: ekonomika, politika, kul'tura*, № 7, p. 123–127.

18. Panarin, I. (2006). Informacionnaya vojna i geopolitika. Pokolenie, 560 p.

19. Turonok, S. G. (2003). Informacionno-kommunikativnaya revolyuciya i novyj spektr voenno-politicheskih konfliktov. *Politicheskie issledovaniya*, № 1, p. 24–38.

20. Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies*, № 5, p. 689–711.

21. Nye, J. (2011). The future of power. New-York. Basic Books, 300 p.

22. Deibert, R. (2015). Trajectories for Future Cybersecurity Research. The Oxford Handbook of International Security/ed. by A. Gheciu and W. C. Wohlforth. – Oxford: Oxford University Perss, p. 531–556.

23. Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, vol. 39, № 3, p. 7–47.

24. Farrell, H. (2015). Promoting Norms for Cyberspace. New York: Council on Foreign Relations.

25. Finnemore, M. (2011). Cultivating International Cyber Norms. America's Cyber Future: Security and Prosperity in the Information Age/ed. by K. Lord, T. Sharp. – Washington, DC: Center for a New American Security, 2011, p. 89–101.

26. Tallinn Manual on the International Law Applicable to Cyber Warfare/ed. by M.Schmitt. New York: Cambridge University Press, 2013, 282 p.

27. Korotkov, A. V., Zinov'eva, E. S. (2011). Bezopasnost' kriticheskih informacionnyh infrastruktur v mezhdunarodnom gumanitarnom prave. *Vestnik MGIMO-Universiteta*, № 4, p. 154. New York, 162.

28. Krutskih, A. V. (2007). K politiko-pravovym osnovaniyam global'noj informacionnoj bezopasnosti. *Mezhdunarodnye processy*, № 1 (5), p. 28–37.

29. Fedorov, A. V., Zinov'eva, E. S. (2017). Mezhdunarodnaya informacionnaya bezopasnost': politicheskaya teoriya i diplomaticheskaya praktika. Moskva: MGIMO, 360 p.

30. Greenberg, L. T., Goodman, S. E., Soo Hoo, K. J. (1997). Information Warfare and International Law. Washington: National Defense University Press.

31. Solodka, O. M. (2020). Zabezpechennia informatsiinoho suverenitetu derzhavy: pravovyi dyskurs. *Informatsiia i pravo*, № 1 (32). URL: http://il.ippi.org.ua/article/view/200311

32. Nastiuk, V. Ia., Bielievtseva, V. V. (2014). Pravovi zasady mizhnarodnoho spivrobitnytstva shchodo protydii informatsiinym pravoporushenniam. *Pravova informatyka*, № 2(42). URL: http://ippi.org.ua/sites/default/files/14nvypip.pdf

33. Kisilevych-Chornoivan, O. M. (2009) Informatsiina bezpeka ta mizhnarodna informatsiina bezpeka: problema vyznachennia poniat. *Yur Yurysprudentsiia: teoriia i praktyka,* № 8, p. 11–18. URL: http://nbuv.gov.ua/UJRN/utp_2009_8_2

34. Frolova, O. (2019). Mizhnarodne spivrobitnytstvo v haluzi zabezpechennia informatsiinoi bezpeky. *Visnyk Lvivskoho universytetu. Seriia: Mizhnarodni vidnosyny*, vyp. 46, p. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13

35. Frolova, O. M. (2018). Rol OON v systemi mizhnarodnoi informatsiinoi bezpeky. *Elektronne vydannia Instytutu mizhnarodnykh vidnosyn «Mizhnarodni vidnosyny. Seriia: Politychni nauky»*, № 18.

36. Kostyriev, A. (2010). Polityko-pravovi problemy rozbudovy systemy mizhnarodnoi informatsiinoi bezpeky v umovakh hlobalizatsii. Suchasna ukrainska polityka. *Polityky i politolohy pro nei.* Kyiv, vyp. 21, p. 234–246.

37. Kopiika, M. (2020) Modernizatsiia polityky mizhnarodnykh orhanizatsii u sferi informatsiinoi bezpeky. *Politychne zhyttia*, 1, p. 102–109. URL: https://jpl.donnu.edu.ua/article/view/7967/7967

38. Romanchuk, Yu. V. (2009). Mizhnarodne spivrobitnytstvo u sferi informatsiinoi bezpeky: kontseptualnyi ta rehuliatyvnyi aspekty. Avtoref. dys... kand. polit. nauk: 23.00.04. NAN Ukrainy. In-t svit. ekonomiky i mizhnar. vidnosyn. Kyiv, 20 p.

39. Mizhnarodna informatsiina bezpeka: teoriia i praktyka/Makarenko Ye. A., Ryzhkov M. M., Ozhevan M. A., Kuchmii O. P., Frolova O. M. Pidruchnyk. Kyiv: Tsentr vilnoi presy, 2016, 418 p.

40. The Freedom of Information Act. U.S. Department of State. URL: https://foia.state.gov/learn/foia.aspx

41. Privacy Act of 1974. U.S. Department of Justice. URL: https://www.justice.gov/opcl/privacy-act-1974

42. Committee on National Security Systems: National Information Assurance (IA) Glossary, *CNSS Instruction*, No. 4009, 26 April 2010.

43. ISACA (2008). Glossary of terms. URL: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

44. Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001, COM (2001)298 final.

45. Japan Cybersecurity Strategy. Information Security policy Council, 2013. URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

46. Rekomendaciya o razvitii i ispol'zovanii mnogoyazychiya i vseobshchem dostupe k kiberprostranstvu. Prinyata 15 oktyabrya 2003 goda. UN. URL: https://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml

47. DEEP: Cybersecurity – A Generic Reference curriculum. NATO. URL: https://www.nato.int/cps/en/natohq/topics_157591.htm

48. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utverzhdena Prezidentom Rossijskoj Federacii V. Putinym 9 sentyabrya 2000 g., № Pr-1895) Sovet bezopasnosti RF. URL: http://www.scrf.gov.ru/documents/5.html

49. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. Utverzhdena Ukazom Prezidenta Rossijskoj Federacii ot 5 dekabrya 2016 g. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

50. Kanev, Sergej (2014). CHeburashka, ili Horoshimi delami proslavit'sya nel'zya. *Novaya Gazeta.* 5 maya. URL: https://novayagazeta.ru/articles/2014/05/05/59473-cheburashka-ili-horoshimi-delami-proslavitsya-nelzya

51. Prinyat zakon o «suverennom internete». Gosudarstvennaya Duma Federal'nogo sobraniya Rossijskoj Federacii. 16.04.2009. URL: http://duma.gov.ru/news/44551/

52. Osnovy gosudarstvennoj politiki v oblasti mezhdunarodnoj informacionnoj bezopasnosti na period do 2020 goda. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/

53. Osnovy gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti (Utverzhdeny Ukazom Prezidenta Rossijskoj Federacii ot 12 aprelya 2021, № 213). URL: http://www.scrf.gov.ru/security/information/document114/

54. Convention on International Information Security. The Ministry of Foreign Affairs of the Russian Federation. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

55. 2006–2020 年国家信息化发展战略 (2006–2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè). 08.05.2005. URL: https://bit.ly/3FsA8VK

56. 中华人民共和国网络安全法 (Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ). 07.11.2016. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

57. Yan Luo, Zhijing Yu, Nicholas Shepherd (2021) Cybersecurity risk classification under China's multi-level protection scheme. Practical Law. Thomson Reuters. URL: https://uk.practicallaw.thomsonreuters.com/w-022-3160?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true

58. 汪玉凯: 中央网络安全与信息化领导小组的由来及其影响 (Wāngyùkǎi: Zhōngyāng wǎngluò ānquán yǔ xìnxī huà lǐngdǎo xiǎozǔ de yóulái jí qí yǐngxiǎng). Baidu.com. 06.03.2014. URL: https://wenku.baidu.com/view/0c29475252d380eb62946d86.html.

59. Manojlo, A. V. (2003). Gosudarstvennaya informacionnaya politika v osobyh usloviyah: Monografiya. Moskva, MIFI. 388 p.

60. Ryjov, Alexander P., Mikhalevich, Igor F. (2020). Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures. *In Handbook of Research on Cyber Crime and Information Privacy*, p. 310–337.

61. Statement of acting chairwoman Rosenworcel on Department of Justice decision to withdraw lawsuit to block California net neutrality law. URL: https://docs.fcc.gov/public/attachments/DOC-369799A1.pdf

62. REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015. laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2

63. Pravitel'stvo RF ne vidit neobhodimosti v zakonodatel'nom zakreplenii setevogo nejtraliteta. *Roskomsvoboda*, 29 October 2018. URL: https://roskomsvoboda.org/42667/

64. Hu, Henry L. (2011). The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration. The China Quarterly, 207 (207), 523–540.

65. Global Freedom Status. Freedom House. https://freedomhouse.org/explore-the-map?type=fiw&year=2021.

Матеріал надійшов до редакції 14.10.2022 р.