DOI 10.31558/2519-2949.2020.1.15
УДК 327.5+351.746.1

ORCID ID: https://orcid.org/0000-0003-0306-1362
Копійка М. В., Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка

МОДЕРНІЗАЦІЯ ПОЛІТИКИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стаття присвячена аналізу модернізації політики міжнародних організацій у сфері інформаційної безпеки з огляду на появу нових гібридних загроз для міжнародного миру, оскільки проблеми глобальної безпеки посідають особливе місце в структурі міжнародної політики, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світопорядку, навіть саме існування цивілізації. Наразі проблема забезпечення інформаційної безпеки на міжнародному рівні полягає у прагненні окремих світових акторів контролювати політичні процеси на значних територіях із застосуванням інформаційних та кібероперацій, що спричинює проблему інформаційного дисбалансу сил і порушення національного інформаційного суверенітету. Аналіз стратегій міжнародного співробітництва у сфері інформаційної безпеки свідчить про спільні і відмінні підходи до трансформації політичної діяльності міжнародних організацій, що зумовлюються політичними позиціями акторів, різними пріоритетами забезпечення інформаційної безпеки та різним рівнем їх інформаційного розвитку.

Практичне забезпечення інформаційної безпеки у форматі міжнародних організацій визначається стратегічною спрямованістю загроз щодо критично важливих систем життєдіяльності світового співтовариства, використанням інформаційних ресурсів як зброї масового ураження, необхідністю створення міжнародних механізмів протидії і попередження глобального протистояння, непередбачуваного за своїми наслідками Тенденції зрощування глобальних і регіональних проблем вплинули на можливості міжнародних акторів визначати напрями і стратегії політичних змін на видиму перспективу, обумовили залучення потужного механізму міжнародних інститутів для розв'язання проблем світового розвитку. Гібридний характер інформаційних загроз зумовив зміну підходів міжнародних організацій до політики у сфері інформаційної безпеки і формування нових структур для протидії сучасним викликам для підтримання миру і стабільності.

Ключові слова: *міжнародні організації, інформаційна безпека, кібербезпека, інформаційні загрози, центри протидії, ООН, НАТО, ОБСЄ, БРІКС.*

*Постановка проблеми***.** Докорінні зміни політики міжнародних організацій щодо інформаційної безпеки, викликані переосмислення концепту забезпечення миру і стабільності у XXI ст., швидкоплинним розвитком високих технологій та їх визнанням технологіями подвійного використання, появою нових загроз для життєдіяльності світової спільноти, зумовили модернізацію базових засад діяльності міжнародних інститутів, які відповідають за безпеку, а також врахування в нових доктринах міжнародної безпеки інформаційної складової як невід'ємної частини стратегічного планування. Міжнародне співробітництво у сфері інформаційної безпеки потребує вироблення міжнародних стратегій з проблем глобальних війн «четвертого покоління» (4GW), вимагає пошуку спільних рішень щодо протидії сучасним інформаційним та кіберзагрозам, інформаційному тероризму та кіберзлочинності. З огляду на визнання ключовою проблемою забезпечення інформаційної безпеки у глобальному вимірі відбувається модернізація політики міжнародних урядових і неурядових організацій, які відіграють пріоритетну роль у міждержавній взаємодії, оскільки сучасна міжнародна система формується під впливом таких чинників, як конкуренція за лідерство у глобальному управлінні, діджиталізація

економіки та врегулювання сучасних гібридних конфліктів з використанням інноваційних технологій і деструктивних впливів.

Формулювання цілей статті. Мета статті полягає у дослідженні сучасного концепту інформаційної безпеки як ключового чинника модернізації політики міжнародних організацій у глобальному середовищі.

Аналіз останніх досліджень і публікацій. До вивчення проблеми інформаційної безпеки у міжнародному вимірі зверталися такі відомі зарубіжні фахівці, як М.Лібіцкі [1], Ф.Хоффман [2], Дж.Най-мол.[3], А.Себровскі, Дж.Гарстка [4] тощо, які розробили новітні теорії сили, теорії інформаційних війн нового покоління та практики використання інформаційних озброєнь у міжнародних конфліктах. У наукових працях також було виявлено спільні і відмінні характеристики інформаційної безпеки, які складаються в системі глобальних і регіональних відносин, проаналізовано інструментарій інформаційних та кіберзагроз для системи міжнародної безпеки, розглянуто міжнародне співробітництво щодо інформаційної безпеки на рівні міжнародних організацій і провідних держав світу, з'ясовано інституційні засади міжнародної інформаційної безпеки.

Вітчизняні науковці О.Кучмій [5] Є.Макаренко [5], М.Рижков [5], О.Фролова [5], Г.Почепцов [6], М.Ожеван [7] тощо розвинули теоретичні положення щодо проблеми міжнародної взаємодії у сфері інформаційної безпеки, визначили чинники політичної діяльності міжнародних інституцій в умовах глобальних зрушень, охарактеризували міжнародні механізми протидії новим викликам для системи міжнародної безпеки,

Виділення невирішених раніше частин загальної проблеми. Сучасні виклики та інтегровані загрози для підтримання миру і стабільності спричинили появу нових підходів до практичних засад міжнародного співробітництва у сфері інформаційної безпеки. Міжнародне співтовариство дійшло згоди, що лише спільними зусиллями та на основі міжнародного права можливо вирішити безпекові проблеми глобального інформаційного середовища в контексті протидії новітнім інформаційним загрозам. Відтак очевидною є необхідність дослідження політики інформаційної безпеки міжнародних організацій, запроваджених упродовж останнього часу, практичного розгляду нових документів і рішень щодо їх інституційного забезпечення та імплементації у діяльності держав-учасниць.

Виклад основного матеріалу й обґрунтування результатів дослідження. Політичні рішення щодо міжнародної інформаційної безпеки, що приймаються у форматі міжнародних організацій, зокрема ООН, НАТО, ОБСЄ і БРІКС, виступають керівними принципами діяльності багатосторонніх механізмів за широкого представництва і всеосяжного врахування позицій та інтересів усіх міжнародних акторів.

Модернізація політики інформаційної безпеки на рівні ООН зумовлена окресленням нових чинників відповідальної поведінки держав, приватного сектора, наукових кіл і організацій громадянського суспільства у кіберпросторі, яка могла б сприяти підвищенню ефективності міжнародного співробітництва. Варто зазначити, що питання міжнародної інформаційної безпеки упродовж 1998-2015 рр. постійно обговорювалось на ГА ООН з метою розробки відповідного міжнародного документа на основі резолюцій «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» та «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки», в яких містилися положення про подвійне використання високих технологій як у цивільній, так і у воєнній сферах, про застосування досягнень науки і техніки у модернізації сучасних озброєнь, про важливість протидії деструктивним впливам [5].

Гостре обговорення проекту Конвенції про міжнародну інформаційну безпеку продемонструвало різні позиції держав щодо визначення понять, бачення потенційних інформаційних загроз та інституційного забезпечення міжнародного співробітництва у межах міжнародної організації. Для узгодження підходів до формування документа на 60 сесії ГА ООН була створена Група урядових експертів, які мали здійснити компетентний аналіз проблем у сфері міжнародної інформаційної безпеки, розробити міжнародні принципи регулювання комунікаційних мереж з огляду на те, що інноваційні технології можуть бути використані для руйнування базових систем забезпечення життєдіяльності держав і спільнот. Проте конкуренція підходів США і Росії до базових засад документа про інформаційну безпеку зумовила його несхвалення і переведення дискусії на подальшу перспективу [8].

Наразі, враховуючи поширення кіберзагроз, ГА ООН більшістю голосів ухвалила нову резолюцію «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної

безпеки» (2019), в якій підтверджується необхідність створення відкритого, безпечного, стабільного, доступного і мирного інформаційно – комунікаційного середовища, встановлення довірчих відносин між державами, розширення можливостей держав щодо співпраці і заохочення використання високих технологій, що сприятимуть зменшенню ризику виникнення конфліктів, і яка є суттєво важливою для забезпечення міжнародної безпеки. Особливо відзначалося, що хоча головна відповідальність за забезпечення безпеки і мирного інформаційно-комунікаційного середовища лежить на державах, визначення механізмів участі приватного сектора, наукових кіл і організацій громадянського суспільства відповідно до обставин могло б сприяти підвищенню ефективності міжнародного співробітництва. Практично було на рівні ООН було створено новий формат Групи урядових експертів на основі справедливого географічного представництва держав, які таким чином можуть зробити важливий внесок у зміцнення міжнародної інформаційної безпеки [10], [11].

Найбільш впливовою міжнародною організацією, що модернізувала політику щодо інформаційної безпеки, вважається НАТО, яка, враховуючи розуміння кіберпростору як середовище інформаційного протиборства, визначила саме кібербезпеку як основний пріоритет своєї діяльності. Організація заснувала передові центри НАТО у країнах-членах як багатонаціональні інститути для розробки доктрини кібербезпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії кіберзагрозам, обміну досвідом кіберзахисту фахівців країн-членів і країн-партнерів, як протидіяти кіберзагрозам. Наразі Центр кібербезпеки НАТО функціонує в Естонії, оскільки створення центру відбулося саме за ініціативою естонської влади і перших країн-спонсорів, які уклали меморандум про взаєморозуміння щодо діяльності та акредитації Центру. Слід підкреслити, що Центр не є підрозділом військового командування або структури збройних сил НАТО, а персонал та фінансування забезпечуються державами-спонсорами та державами-учасниками [11].

Експерти Центру спільно з Організацією Червоного Хреста та Кібернетичним командуванням США представили доповідь «Керівні принципи міжнародного права, що можуть бути застосовані під час кібернетичних війн» та «Талліннські керівні принципи 2.0», які вважаються базовими засадами щодо ведення кібервійн і відповідають положенням сучасного міжнародного права про регулювання операцій у кіберпросторі, а держави несуть відповідальність за кібератаки проти інших держав, які ведуться з їх території. У документі йдеться про заборону застосування сили в кіберпросторі, тому що кібератаки призводять до руйнування інфраструктури, цифрових даних та систем життєзабезпечення держав, залякують цивільне населення і вважаються військовими злочинами. Відтак кібервійни дозволяється вважати «збройними конфліктами», і застосування контрзаходів у відповідь на кібератаки є законним. Зазначимо, що доповідь експертів є незалежною думкою авторів і на відміну від офіційних документів НАТО має рекомендаційний характер [12].

Разом з тим у документах організації стверджується, що кіберзагрози для безпеки НАТО «стають все частішими й складнішими, більш руйнівними та примусовими, тому керівництво НАТО, держави-члени та союзні держави покладаються на колективну кібероборону задля виконання основних завдань Альянсу та оперативного управління кризовими ситуаціями. Таким чином, кібербезпека стала одним з провідних пріоритетів для трансатлантичної організації з огляду на те, що «…гібридні атаки можуть зашкодити військовій і цивільній сфері життєдіяльності країн-учасниць, тому заходи, схвалені упродовж останніх років, сприятимуть ефективному забезпеченню захисту НАТО від кіберзагроз». Основні принципи щодо кібербезпеки Альянсу були зафіксовані у положеннях 2019 р., в яких підтверджено, що: кібербезпека вважається складовою основних завдань колективної оборони НАТО, що у кіберпросторі застосовуються принципи міжнародного права що кібербезпека спрямована на захист власних мереж організації та підвищення її обороноздатності.

Союзники підтвердили оборонний мандат НАТО й визнали кіберпростір середовищем операцій, в якому НАТО має ефективно захищатися, як це відбувається в інших фізичних середовищах протиборства. Командам НАТО з питань швидкого реагування на кіберзагрози наказано надавати допомогу союзникам щодо протидії кібератакам, крім того для захисту держав-членів НАТО можуть залучатися національні підрозділи кібербезпеки для проведення спеціальних операцій. У 2019 р. було схвалено рекомендації НАТО, що містять низку інструментів для подальшого зміцнення здатності НАТО реагувати на агресивні кібератаки, для активізації співпраці з діловими колами і приватним сектором у сфері в кіберпромисловості та надання можливостей скористатися кіберпростором союзникам на основі передбачуваних та безпечних норм»[13], [14].

ОБСЄ як одна зі структур з підтримання безпеки та стабільності, що охоплює Європу, Північну Америку та пострадянські республіки, вважається міжнародним форумом для обговорення проблем сучасної безпеки. Цей форум був започаткований як міжнародний інститут для підтримання безпеки, прав людини, фундаментальних свобод, демократії, захисту професійної діяльності мас-медіа у зонах збройних конфліктів тощо. Модернізація політики організації виявилася необхідною з огляду на появу нових загроз гібридних конфліктів, вагомою складовою яких стали спеціальні інформаційні операції і деструктивні впливи.

У порядку денному організації було сформульовано пропозиції щодо основних напрямів роботи ОБСЄ з питань формування системи міжнародної інформаційної безпеки, серед яких: «визначення понять у сфері міжнародної інформаційної безпеки; створення ефективних механізмів попередження й знешкодження загроз з використанням високих технологій; використання чинних норм міжнародного права для протидії інформаційним загрозам; створення системи виявлення джерел інформаційних загроз; активізація міжнародних зусиль для безпеки функціонування мережі Інтернет; підвищення довіри до глобальної інформаційної інфраструктури на основі міжнародного управління нею тощо. Водночас, на погляд представників ОБСЄ, найбільшої уваги у сучасному світі потребують кіберзагрози, тому організація закликала усі зацікавлені сторони до пошуку рішень проблем у сфері кібербезпеки та досягнення загального й ефективного регулювання кіберпростору на основі норм і принципів міжнародного права.

Для вироблення загального підходу ОБСЄ до проблем кібербезпеки та визначення ролі ОБСЄ у цьому процесі у Відні 9-10 травня 2011р. було проведено конференцію «Загальний підхід до кібербезпеки: визначення майбутньої ролі ОБСЄ», на якій розглядалися форми і методи протиправного використання кіберпростору, аналізувалися відповідні контрзаходи з боку міжнародних і регіональних організацій, характеризувалися кібервпливи на безпеку в регіоні ОБСЄ. Йшлося також про визначення потенціалу ОБСЄ для застосування всеосяжного підходу до кібербезпеки, в тому числі через обмін досвідом між країнами регіону, та можливу розробку норм, що регулюють поведінку держав у кіберпросторі; про можливість ухвалення рішень, спрямованих на зміцнення кібербезпеки в регіоні. У 2013 р. ОБСЄ прийняла інноваційні рекомендації про «заходи щодо зміцнення довіри» у сфері кібербезпеки, спрямовані на підвищення прозорості та забезпечення безпеки в регіоні, які передбачали взаємодію з приватним сектором і провайдерами найважливішої інфраструктури, а також спільні підходи до управління кібербезпекою [15].

Австрійська конференція ОБСЄ «Кібербезпека критичної інфраструктури: зміцнення формування довіри в ОБСЄ», що відбулася 2017 р., сприяла дискусії держав-учасниць організації щодо вирішення найбільш гострих проблем безпеки ІКТ, обміну найкращими практиками для ефективного та своєчасного реагування на критичні інциденти. До спільних заходів було віднесено: подолання терористичної та злочинної діяльності у кіберпросторі відповідно до зобов'язань ОБСЄ; захист критичної інфраструктури від шкідливої діяльності у галузі ІКТ; захист прав людини в інтернеті на засадах чинного міжнародного права. Братиславська конференція ОБСЄ «Кібербезпека та безпека в галузі ІКТ для безпечного майбутнього: роль ОБСЄ у сприянні регіональній кіберстабільності» (2019 р.) передбачала створення платформи для представників громадського, приватного та неурядового секторів з усього регіону ОБСЄ для проведення всебічного діалогу з питань безпеки ІКТ на глобальному, регіональному та національному рівнях.

При цьому було враховано резолюцію Генеральної Асамблеї ООН A / RES / 73/266 про запровадження регіональних консультацій між державами-учасницями ОБСЄ та новоствореною групою урядових експертів з питань розвитку інформаційних та комунікаційних технологій у контексті міжнародного миру та безпеки. Інтерактивні дискусії у форматі ОБСЄ охопили питання багатосторонньої кібердипломатії, розвитку регіональної кібербезпеки як рушійної сили глобального прогресу, впливу штучного інтелекту на безпеку ІКТ та захист критичної інфраструктури. На конференції наголошувалося, що інформаційно-комунікаційні технології у сучасному світі стали головним рушієм економічного та соціального зростання, а також зумовили новий вимір міжнародних відносин, оскільки загрози у кіберпросторі збільшили потенціал напруженості між державами через неправомірне використання мереж, кібератаки і порушення конфіденційності. Основна увага організації була спрямована на розроблення заходів довіри між державами-учасницями, щоб зменшити ризики конфліктів, пов'язаних із використанням ІКТ [16], [17]. Зазначимо, що в рамках ОБСЄ проблему міжнародної інформаційної безпеки доцільно було б конкретизувати через дослідницькі проекти, аналітичні експертні оцінки та відповідні програми міжнародної організації.

Формат співпраці неформального об'єднання БРІКС у сфері міжнародної безпеки відбувається у рамках щорічних самітів, неформальних зустрічей глав держав і урядів країн-учасниць, протокольних зустрічей Високих представників з питань національної безпеки та робочої групи з питань міжнародної інформаційної безпеки. Активізація співробітництва у сфері інформаційної безпеки, як зазначається в офіційних документах організації, засвідчує, що проблема протидії новим високотехнологічним озброєнням залежить не лише від дій міжнародних організацій та національних інститутів, до компетенції яких віднесено загальні завдання забезпечення інформаційної безпеки, а й від координації безпекової політики та міжнародного співробітництва на багатосторонній основі. У попередні роки стратегію інформаційної безпеки БРІКС пов'язували з підтримкою проекту РФ та Групи експертів ООН, яку очолював представник Росії, щодо запровадження саме російських пропозицій у документ з міжнародної інформаційної безпеки. Інші пропозиції країни БРІКС відхиляли і завжди голосували «проти».

Водночас стрімкий прогрес інформаційно-комунікаційних технологій у країнах БРІКС, зокрема у Китаї та Індії, спричинив суттєву модернізацію політики інформаційної безпеки об'єднання, яка полягає у визнанні важливості забезпечення кібербезпеки та інформаційного суверенітету країн-учасниць. Дослідження показали, що країни БРІКС для захисту інформаційного суверенітету розробляють законодавство про інформаційний суверенітет, розглядають положення про нові стандарти захисту даних, їх конфіденційність та запровадження інструментів для обмеження доступу зарубіжних технологічних компаній до національного кіберсередовища. Повна довіра до іноземних технологій, як зазначають високопосадовці країн-учасниць БРІКС, може вплинути на захист персональних даних, спричинити загрози маніпулювання масовою свідомістю та порушення систем життєдіяльності держав.

Уряди країн БРІКС також усвідомлюють, що масове використання послуг мережі Інтернет та соціальних медіаплатформ громадянами об'єднання може загрожувати через хакерські атаки політичним режимам і національній безпеці країн, які вкладають значні інвестиції у програми діджиталізації економіки і промисловості, враховуючи, що жорсткі стандарти кібербезпеки будуть ключовими для захисту інтелектуального потенціалу кожної країни БРІКС. Зокрема, йдеться про наполягання Індії зберігати персональні дані власних громадян лише на комп'ютерних ресурсах країни, про ухвалення законодавства про інформаційний суверенітет в Росії, затвердження у 2018 р. нового Загального закону про захист даних, забезпечення комп'ютеризації урядових операцій, впровадження технологій «Інтернету речей» для автоматизації промисловості у Бразилії. Крім того, на погляд експертів організації, країни БРІКС одночасно є одними з країн, з яких походить більшість кібератак, і країнами, проти яких найчастіше здійснюються кібератаки. Така ситуація виводить проблему кібербезпеки перший план порядку денного країн-учасниць БРІКС [18].

Нова програма дій неформальної організації «Від BRICS до CyberBRICS: Нове співробітництво у сфері кібербезпеки» обговорювалася на зустрічі міністрів з питань комунікаційного розвитку країн БРІКС, що відбулася у Бразилії в серпні 2019 р. Під час зустрічі було оприлюднено спільну декларацію, в якій підкреслюється стратегічний інтерес партнерства БРІКС щодо нових цифрових інфраструктур, технологій 5G, Інтернету речей та кібербезпеки. Урядовці підтвердили, що сучасна інфраструктура, ефективне управління кібербезпекою, зокрема встановлення стандартів захисту даних, є вирішальними ресурсами для інклюзивного та сталого розвитку країн БРІКС. Цифрова трансформація на рівні політики БРІКС визнана важливим елементом майбутнього економіки та суспільства країн-учасниць, і саме тому розробка та реалізація стратегій діджиталізації, що впливає на конкурентоспроможність країн об'єднання на міжнародному рівні, спрямована на створення нових потужностей для співпраці країн БРІКС у різних сферах: від традиційних цифрових технологій до інтелектуальних технологій штучного інтелекту й робототехніки, які визначають потенціал перспективного розвитку учасників організації.

Разом з тим наголошувалося, що Китай, безумовно, є країною з найбільш системним підходом до інновацій, інвестуючи значні кошти в технології 5G, оскільки він наразі є світовим лідером із поширення таких технологій у сфері телекомунікацій, а також у забезпеченні кібербезпеки. Так, у Китаї нещодавно було ухвалено узгоджене за нормами законодавство про кібербезпеку, електронну комерцію та стандарти захисту даних. Натомість Бразилія лише нещодавно почала реалізовувати свою однорічну Стратегію цифрової трансформації, в якій відсутні положення про кібербезпеку, хоча урядові інституції працюють над її розробкою. Можна стверджувати, що у такому складному контексті цифрова трансформація може принести як великі переваги, так і створити великі ризики.

Фахівці зазначають, що численні взаємопов'язані пристрої, які управляються через мережі 5G, мають потенціал значно покращити робототехніку, промислову автоматизацію, «розумне» землеробство та забезпечити значне підвищення ефективності завдяки потужним можливостям збирання та обробки даних. Також враховується той факт, що половина населення БРІКС вже підключена до інтернету, генеруючи неймовірну кількість даних. Практично такі досягнення, підкреслюється у дослідженнях, революціонізують діяльність в інтернеті та в режимі офлайн, надають безпрецедентні можливості, але й створюють нові багатогранні загрози, оскільки взаємозв'язок Інтернету речей потребує найвищого рівня безпеки, щоб уникнути злому, витоку даних та перетворення цифрових сподівань БРІКС у в потенційні проблеми.

У новій програмі дій також порушується питання про необхідність спільної співпраці та порівняльної перспективи політики інформаційної безпеки країн БРІКС, які є важливими не лише для взаєморозуміння та поваги до позицій кожної країни, але й для того, щоб розробити сумісні технології та правила, що сприятимуть доступу до інноваційних послуг та продуктів, забезпечуючи при цьому захист прав користувачів. Країни БРІКС можуть мати різні позиції у контексті чутливості і вразливості певної проблематики, але їх пріоритети та цілі часто дуже схожі за основними ідеями. У цьому контексті реалізація потужної ініціативи щодо співпраці з багатьма зацікавленими сторонами, у форматі якої уряди країн БРІКС можуть вести діалог з науковцями, приватним сектором та представниками громадянського суспільства, отримуючи вклад та відгуки стосовно різних аспектів їхньої політики в галузі кібербезпеки, була б вигідною стратегією для всіх учасниць об'єднання.

Для початку, вважають експерти, уряди країн-членів БРІКС, які протягом останніх років послідовно наголошували на значенні посилення співпраці в галузі досліджень та технологічного розвитку, могли б підтримати створення механізму співпраці аналітичних центрів БРІКС з питань кібербезпеки. Як показує новаторський досвід проекту CyberBRICS, аналіз існуючої цифрової політики має першочергове значення для виявлення передової практики та пропонування стійких та справедливих рішень. Бразильське ротаційне головування в БРІКС, за оцінкою країн-учасниць організації, надав унікальну можливість сформулювати позитивний та інноваційний порядок денний, підкреслюючи переваги вдосконалення співпраці у сфері цифрової політики в цілому та кібербезпеки зокрема. Таким чином, пріоритети співробітництва країн БРІКС в сфері інформаційної безпеки засвідчили, що ефективність боротьби з новими високотехнологічними озброєннями залежить не тільки від заходів, що здійснюються на рівні національних інститутів і регіональних організацій, на які покладено спільні завдання забезпечення інформаційної безпеки, але і від координації співробітництва держав на багатосторонній основі [19].

Висновки та перспективи подальших досліджень. Трансформація інформаційної парадигми глобального розвитку, яка є відображенням нових закономірностей формування сучасної системи міжнародних відносин, свідчить про новації міжнародного співробітництва у сфері інформації і комунікації і відповідно потребує вдосконалення політики щодо забезпечення міжнародного миру і стабільності. Модернізація політики міжнародних організацій щодо інформаційної безпеки визначається їх можливостями забезпечити багатосторонній діалог міжнародних акторів, врахувати різні позиції суб'єктів глобального управління з протидії новітнім інформаційним загрозам та виступати згідно зі статутними повноваженнями як універсальні міжнародні платформи для формування консенсусу у вирішенні актуальних безпекових проблем.

Бібліографічний список:

1. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare / M.C.Libicki. – Cambridge: Cambridge University Press, 2007. – 336 p.
2. Hoffman F. Hybrid vs Compound /Frank G. Hoffman // Small Wars Journal. – 2009. – October. URL.: http://smallwarsjournal.com /blog/journal/docs–temp/189–hoffman.pdf.
3. Nye J.S. Cyber Power / Joseph S. Nye. – Cambridge: Pub. by Belfer Center for Science and International Affairs, 2010. – 26 p.
4. Cebrovski A., Garstka J. Network–Centric Warfare: Its Origin and Future / A. Cebrovski, J.Garstka // Proceedings. – 1998. – January. URL.: http:// www. kinection. com/ ncoic/ ncw _origin_future.pdf
5. Міжнародна інформаційна безпека: теорія і практика//Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М./Підручник. – Київ: Центр вільної преси, 2016. – 418 с.
6. Почепцов Г. Гибридная война: информационная составляющая / Г.Почепцов. URL.: http://psyfactor.org/ psyops/hybridwar5.htm

7. Ожеван М.А.Глобальна війна гранд-наративів у сучасну добу // Стратегічні комунікації в міжнародних відносинах. Монографія. – К. : Вадекс, 2019. – 442 с.
8. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/ GEN/ N13/371/66/ PDF/N1337166. pdf?OpenElement
9. Resolution adopted by the General Assembly on 12 December 2019 [on the report of the First Committee (A/74/363)] 74/29. Developments in the field of information and telecommunications in the context of international security. URL: https://undocs.org/en/A/RES/74/29
10. Developments in the field of information and telecommunications in the context of international security. URL: https://www.un.org/disarmament/ict-security/Prevention of an arms race in outer space https://undocs.org/en/A/RES/74/32
11. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://www.cybersecurityintelligence.com/ nato-cooperative-cyber-defence-centre-ccdcoe-395.html
12. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched // NATOCCDCOE. – 2017. URL: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html.
13. A cyber-security framework fordevelopment, defense and innovation at NATO. URL: https://innovation-entrepreneurship.springeropen.com/track/pdf/10.1186/s13731-019-0105-z
14. Brent L. NATO's role in cyberspace. URL: https://www. nato.int/docu/ review/articles/2019/02/12/ natos-role-in-cyberspace/index.html
15. Organization for Security and Co-operation in Europe – OSCE. URL: https://www.osce.org/whatistheosce
16. Austrian OSCE Chairmanship Conference on Cyber Security. URL: https://www.osce.org/event/austrian-cyber-security-2017
17. Cyber/ICT Security for a safer future: The OSCE's role in fostering regional cyber stability. URL: https://polis.Osce.org/cyberict-security-safer-future-osces-role-fostering-regional-cyber-stability
18. Belli L. BRICS countries to build digital sovereignty. URL: https://www.opendemocracy.net/en/hri-2/ brics-countries-build-digital-sovereignty/
19. From BRICS to CyberBRICS: New Cybersecurity Cooperation. URL: http://www.chinatoday.com.cn/ ctenglish/2018/tpxw/201911/t20191113_800184922.html

References:

1. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare / M.C.Libicki. – Cambridge: Cambridge University Press, 2007. – 336 p.
2. Hoffman F. Hybrid vs Compound /Frank G. Hoffman // Small Wars Journal. – 2009. – October. URL.: http://smallwarsjournal.com /blog/journal/docs–temp/189–hoffman.pdf.
3. Nye J.S. Cyber Power / Joseph S. Nye. – Cambridge: Pub. by Belfer Center for Science and International Affairs, 2010. – 26 p.
4. Cebrovski A., Garstka J. Network–Centric Warfare: Its Origin and Future / A. Cebrovski, J.Garstka // Proceedings. – 1998. – January. URL: http:// www. kinection.com/ncoic/ncw_origin_future.pdf
5. Mizhnarodna informatsiyna bezpeka: teoriya i praktyka. Pidruchnyk // Makarenko YE.A, Ryzhkov M.M., Ozhevan M.M., Kuchmiy O.P., Frolova O.M. – K.: «Tsentr vil′noyi presy», 2016. – 418 p.
6. Pocheptsov H. Hybrydnaya voyna: ynformatsyonnaya sostavlyayushchaya / H.Pocheptsov. URL: http://psyfactor.org/psyops/hybridwar5.htm
7. Ozhevan M.A.Hlobal′na viyna hrand-naratyviv u suchasnu dobu // Stratehichni komunikatsiyi v mizhnarodnykh vidnosynakh. Monohrafiya. – K. : Vadeks, 2019. – 442 s.
8. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/ GEN/N13/371/66/PDF/N1337166.pdf?OpenElement
9. Resolution adopted by the General Assembly on 12 December 2019 [on the report of the First Committee (A/74/363)] 74/29. Developments in the field of information and telecommunications in the context of international security. URL: https://undocs.org/en/A/RES/74/29
10. Developments in the field of information and telecommunications in the context of international security. URL: https://www.un.org/disarmament/ict-security/Prevention of an arms race in outer space https://undocs.org/en/A/RES/74/32
11. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://www.cybersecurityintelligence.com/ nato-cooperative-cyber-defence-centre-ccdcoe-395.html
12. Strategic Communications Centre of Excellence. URL: https://www.stratcomcoe.org/about-us
13. A cyber-security framework fordevelopment, defense and innovation at NATO. URL: https://innovation-entrepreneurship.springeropen.com/track/pdf/10.1186/s13731-019-0105-z
14. Brent L. NATO's role in cyberspace. URL: https://www.nato.int/docu/review/articles/2019/02/12/ natos-role-in-cyberspace/index.html
15. Organization for Security and Co-operation in Europe – OSCE. URL: https://www.osce.org/whatistheosce

16. Austrian OSCE Chairmanship Conference on Cyber Security. URL: https://www.osce.org/event/austrian-cyber-security-2017

17. Cyber/ICT Security for a safer future: The OSCE's role in fostering regional cyber stability. URL: https://polis.Osce.org/cyberict-security-safer-future-osces-role-fostering-regional-cyber-stability

18. Belli L. BRICS countries to build digital sovereignty. URL: https://www.opendemocracy.net/en/hri-2/brics-countries-build-digital-sovereignty/

19. From BRICS to CyberBRICS: New Cybersecurity Cooperation. URL: http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html

Kopiika M. V. Modernization of the policy of the international organizations in information security

The article analyses the modernization of international organizations' policy in information security in view of the emergence of new hybrid threats for international peace because global security issues occupy a special place in the structure of international policy, identify the contradictions of the current stage of international development and reached such a level and severity that can endanger the maintenance of world order, even the existence of civilization. Nowadays, the issue of information security at the international level consists in the striving some global actors to control political processes in large territories with using information and cyber operations that cause the problem of information imbalance of forces and violation of national information sovereignty. The analysis of the strategies of international cooperation in information security shows common and different approaches to the transformation of political activities of international organizations that depends on the political positions of the actors, different priorities of providing information security and different level of their information development.

The practical provision of information security in the format of international organizations has been determined by the strategic focus of threats on the critical life systems of the world community, the use of information resources as a weapon of mass destruction, the need to create international mechanisms of counteraction and prevent global confrontation, unforeseen in its consequences. Trends of global and regional issues have influenced on the ability of international actors to determine the directions and strategies of political changes in the future, as well as led to the involvement of a powerful mechanism of international institutions for solving the problems of world development. The hybrid nature of information threats has led to a transformation of the international organizations' approaches to information security and the establishment of new structures for countering modern challenges to maintain peace and stability.

Key words: *international organizations, information security, cybersecurity, information threats, centers of counteraction, UN, NATO, OSCE, BRICS.*