УДК 327.5 (73+520)

ПРІОРИТЕТИ СПІВРОБІТНИЦТВО ЯПОНІЇ ЗІ США У СФЕРІ КІБЕРБЕЗПЕКИ

PRIORITIES OF COLLABORATION OF JAPAN ARE FROM THE USA IN THE FIELD OF CYBERSECURITY

Сябро А. В.,
аспірантка кафедри міжнародної інформації,
Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка (Київ, Україна),
e-mail: siabro_anastasiia@ukr.net

Syabro A. V.,
postgraduate student, International Information Institute of International Relations of the Kyiv National University named after Taras Shevchenko (Kyiv, Ukraine), e-mail: siabro_anastasiia@ukr.net

У статті досліджено еволюцію пріоритетів співробітництва Японії зі США у сфері безпеки та оборони. Проаналізовано сучасні виклики та загрози для регіональної системи безпеки АТР. Визначено передумови включення до пріоритетів двостороннього співробітництва питань кібербезпеки. Доведено актуальність японсько-американського альянсу у сфері безпеки для протистояння новим типам загроз в умовах зростання кібермогутності основних геополітичних опонентів Японії та США – КНДР, КНР та РФ, які активно використовують методи інформаційного протиборства та завдають удари по критично важливим елементам інфраструктури країн регіону. Це обумовило потребу вироблення спеціальних політико-правових механізмів двостороннього співробітництва та створення двосторонніх робочих груп, які розглядають широкий спектр питань співпраці обох країн у сфері кібербезпеки. У статті доведено, що співробітництво Японії зі США у сфері кібербезпеки є запорукою підтримання миру і безпеки в АТР.

Ключові слова. *Регіональна безпека, АТР, кібербезпека, кібератака, кіберзлочинність, Кібердіалог Японія-США, Сили самооборони, Японія, США, Північна Корея, Китай, Росія.*

This article explores the evolution of security and defense priorities of Japan's and the US cooperation. Modern challenges and threats to the regional security system of the APR are analyzed. The preconditions for inclusion in the priorities of bilateral cooperation on cybersecurity are identified. It is proved the relevance of the US-Japan security alliance counteraction to new types of threats in the context of the growing cyberpower of major geopolitical opponents of Japan and the US - the DPRK, the PRC and the Russian Federation - which actively use methods of information warfare and strike at critical elements of the infrastructure of countries in the region. This necessitated the development of specific political and legal mechanisms for bilateral cooperation and the creation of bilateral working groups that address a wide range of issues of cooperation between the two countries in the field of cybersecurity. The article proves that Japan's cooperation with the United States in cybersecurity is the key to maintaining peace and security in the Asia-Pacific region.

Keywords: *Regional security, Asia-Pacific region, cybersecurity, cyberattack, cybercrime, Japan-US Cyber Dialogue, Self-Defense Forces, Japan, USA, North Korea, China, Russia.*

Постановка проблеми. В умовах появи сучасних викликів і загроз для системи підтримання міжнародного миру і безпеки для багатьох акторів міжнародних відносин виникає потреба перегляду існуючих механізмів співробітництва, відповідно до нових умов. Важливим чинником трансформації середовища безпеки виступає науково-технологічний прогрес, що призвів до чергового витка гонки озброєнь та появи нових методів протиборства з використанням високих технологій та наукових досягнень. Таким чином протистояння держав переміщується у віртуальний простір, де використовується так звана інформаційна зброя, а можливості самої держави визначаються її інноваційним потенціалом та рівнем інформаційно-технологічного розвитку.

Враховуючи особливості сучасного розвитку країн Азійсько-Тихоокеанського регіону, проблема інформаційної безпеки є надзвичайно актуальною і потребує вироблення ефективних механізмів для її вирішення, особливо в умовах включення у глобальне інформаційне протистояння таких держав, як Китай та Північна Корея. В цих умовах Японія та США змушені переглядати нині діючу стратегію співробітництва у сфері безпеки та оборони, надаючи особливої уваги питанням кібербезпеки.

Аналіз останніх досліджень і публікацій. Дослідження проблеми кібербезпеки як нового пріоритету двостороннього співробітництва Японії та США обумовлює звернення до наукових праць фахівців з питань інформаційного протиборства. Так, загальні проблеми кібербезпеки досліджено у роботах Зб. Бжезинського, М. Лібіцкі, Дж. Ная, О. Тоффлера, О. Манойла, Д.Дубова, О.Зернецької, О.Литвиненка, О.Ожевана, В. Петрова, Г. Почепцова, Є.Макаренко та ін. Праці М. Цучія , Дж. А. Льюіса, Ф.-С. Геді, П. Калландера, К. В. Х'юза, Л. Уеллса, Р. Репка, Д.Херста, С.В. Гарольда, Ю. Ітo та ін. присвячені окремим питанням співробітництва Японії та США у сфері кібербезпеки. Водночас, проблема еволюції пріоритетів двостороннього співробітництва у контексті геополітичних зрушень розглянуто фрагментарно, переважно з позиції спільних кіберзагроз та пошуку оптимальних практичних механізмів для оперативного реагування на них.

Мета дослідження полягає у визначенні чинників, що впливають на перегляд стратегії співробітництва Японії та США у сфері безпеки, з'ясуванні базових пріоритетів співробітництва держав у сфері кібербезпеки та аналізі потенційних наслідків такого співробітництва для архітектури регіональної інформаційної безпеки АТР.

Виклад основного матеріалу. Співробітництво Японії зі США у сфері безпеки розпочалося з 50-х рр. XX ст. За майже 60 років співпраці відбулися суттєві зміни як у системі підтримання міжнародного миру і безпеки, так й в рамках архітектури безпеки АТР, що вплинуло на характер та особливості японсько-американського двостороннього співробітництва, яке від самого початку мало асиметричний характер. Завершення періоду «холодної війни» та поява нових загроз для архітектури безпеки АТР обумовили виникнення потреби перегляду існуючих пріоритетів двостороннього співробітництва, а до порядку денного увійшли питання, пов'язані з використанням досягнень науки та технологій у контексті безпеки регіону. Так, найбільш суттєві зміни почали відбуватися з прискоренням процесів модернізації країн регіону, що було обумовлено науково-технологічним розвитком та появою можливості доступу до продуктів інноваційної діяльності країн Заходу. Відтоді став очевидним факт подвійного характеру високих

технологій, які можуть бути використані як для підвищення темпів економічного зростання, так й для завдання потужного удару по будь-якій країні незалежно від відстані або кордонів за допомогою різноманітних інформаційних озброєнь або досягнень сучасної науки.

Основними проблемами кібербезпеки регіону стали шпигунство та злочинність, що фінансуються державами, зростання наступальних військових кіберможливостей та використання кібермогутності як нового інструменту політичного примусу. Тому уряди держав АТР включили питання кібербезпеки як складову національної стратегії безпеки. Особливого значення питання кібербезпеки мають для Японії та Сполучених Штатів, оскільки Північна Азія є своєрідною «точкою спалаху» для кібербезпеки. Основними супротивниками у сфері кібербезпеки Японії та США виступають Китай, Північна Корея та Росія. Зокрема, Росія та Китай витрачають на кібердіяльність значно більше, ніж Японія; а Північна Корея, незважаючи на недостатньо високий рівень розвитку кіберсередовища, володіє більш потужними кіберсилами, ніж Японія. У той же час Китай і Росія є світовими лідерами в галузі кіберможливостей як для шпигунства, так і для нападу. Їх діяльність поширюється на світовий інформаційний простір. А тому перед Японією постала важлива проблема – удосконалення своєї системи кібербезпеки, як для власного захисту, так й для повноцінного партнерства зі Сполученими Штатами у сфері безпеки та оборони [6].

Слід зазначити, що на думку експертів, стратегія кібербезпеки має сенс лише тоді, коли вона вбудована в більш широкий геополітичний контекст. Використання кіберможливостей дозволяє країнам застосовувати нові інструменти для шпигунства, примусу, нападу, але у спосіб, що відповідає їхнім стратегічним цілям. Тому, такі держави, як Японія змушені шукати більш дієві механізми захисту кіберпростору. А оскільки розбудова глобальної інформаційної інфраструктури суттєво скорочує відставань між країнами і регіонами світу, Токіо опиняється лише в декількох секундах від Пекіна. При цьому дві країни-сусіди – Росія та Китай – активно застосовують методи кібершпигунства і мають добре розвинені можливості здійснювати військові кібератака, а Північна Корея – постійно використовує кібератаки для завдання удару по Південній Кореї та США. Найбільш небезпечними кібератаками є ті, що завдають фізичної шкоди, наприклад, удар по ядерних об'єктах Ірану за допомогою вірусу Stuxnet. І хоча на використання таких технологій здатні лише декілька країн, але ймовірно, що Росія має цю спроможність, Китай, можливо, вже володіє нею, а Іран та Північна Корея прагнуть її придбати [6].

У 2014-2015 рр. потреба включення питань кібербезпеки до пріоритетів двостороннього співробітництва Японії та США була підтверджена серією кібератак, які продемонстрували не тільки вразливість приватного інтернет-простору, а й довели факт зростання кібермогутності одного з головних суперників США – КНДР. Зокрема, у 2014 р. відбулася масштабна хакерська атака на сервери компанії Sony Pictures Entertainment. Внаслідок інциденту було викрадено та згодом оприлюднено або знищено персональні данні співробітників, їх родин, а також інформацію комерційного характеру та цифрові копії кінопродукції компанії. В результаті проведеного розслідування ФБР дійшло висновків, що джерелом небезпеки була Північна Корея. Найбільш вірогідною ціллю нападу було названо комедійну стрічку «Інтерв'ю», в якій йшлося про змову з метою вбивства лідера КНДР Кім Чен Ина [5]. Як зауважило видання The Washington Post, це був перший випадок, коли США звинувачують у здійсненні кібератаки іноземну державу [13]. Але занепокоєння викликав й той факт, що атакована компанія Sony Pictures Entertainment хоча і є сьогодні американською, але бренд належить Японії, яка географічно значно ближче до Північної Кореї, що може призвести до непередбачуваних наслідків для системи кібербезпеки в Азійсько-Тихоокеанському регіоні. Тому, враховуючи, які погрози лунали від офіційних представників КНДР, показ фільму «Інтерв'ю» було вирішено відмінити, щоб не спровокувати ескалацію конфлікту або не допустити нові хвилі атак на інші об'єкти [17]. Найважливішим наслідком цього кіберінциденту стало усвідомлення того, що напади на країни-союзники США в АТР можуть використовуватися для спекуляцій або приховування справжніх цілей держави-ініціатора агресії. Наприклад, КНР або РФ не можуть напряму здійснювати атаки на цивільні цілі на американській території, оскільки уникають ескалації конфліктів внаслідок прямої агресії (хоча Іран та Північна Корея можуть й не виявляти такої стриманості). Напад на Sony Pictures Entertainment продемонстрував не тільки збільшення кібермогутності КНДР, а й можливостей завдавати ударів по кіберпростору США. Водночас став очевидним й факт збільшення можливостей США ідентифікувати загрози та їх джерела, поєднуючи методи розвідки та криміналістики, що не завжди доступно для приватного сектору. І хоча Північна Корея відтепер була змушена діяти більш обережно, усвідомлюючи небезпеку бути ідентифікованою як джерело кібератаки, вона продемонструвала свої можливості завдавати удари по стратегічним об'єктам та критично важливим елементам національної інформаційної інфраструктури Японії та США [6].

Для Японії цей кіберінцидент був не першим. У 2000 р. відбулася масштабна кібератака на урядові структури Японії, у 2011 р. об'єктом кібернападу було обрано комп'ютерну мережу компанії Mitsubishi Heavy Industries Ltd., а вже у травні 2015 р. відбулася чергова атака на сервери Японської пенсійної служби. Але більшість кібератак, про які було офіційно заявлено, насправді є видами кіберзлочинності, актами кібершпигунства або кіберсаботажу, що можна назвати скоріше «зброєю масового занепокоєння», оскільки вона не призводить до реальних фізичних або матеріальних втрат. Водночас це не означає, що таких наслідків не може бути у майбутньому [17].

Внаслідок збільшення масштабів кібератак на критично-важливі елементи інфраструктури Японії та США, джерелами яких виступали інші держави регіону, стала очевидною потреба перегляду не тільки національних стратегій у сфері кібербезпеки обох країн, а й пріоритетів двостороннього співробітництва держав та включення проблеми кібербезпеки до базових аспектів взаємодії [6]. Так, під час зустрічі прем'єр-міністра С. Абе з президентом Б. Обамою у квітні 2015 р. було узгоджено позиції обох країн з питань кібербезпеки, вирішення яких можливе за умови гарантії забезпечення безпечного та стабільного використання кіберпростору на основі вільного потоку інформації та відкритого Інтернету [16]. В оновленому документі «Керівні принципи співробітництва Японії та США у сфері оборони» (2015 р.) було представлено базові підходи японсько-американського співробітництва у сфері кібербезпеки як нової ключової сфери співпраці [9]. У документі, зокрема, зазначалося, що для забезпечення безпечного та стабільного використання кіберпростору обидва уряди мають систематично обмінюватися інформацією про загрози та вразливості в кіберпросторі; надавати інформацію про розвиток різних можливостей у кіберпросторі, включаючи обмін найкращими практиками щодо навчання та освіти у сфері кібербезпеки; виробити ефективні механізми співпраці у сфері захисту критичної інфраструктури, у тому числі тих її складових, що забезпечують ефективну діяльність служб спеціального призначення, Збройних сил або Сил самооборони, а також співпраця с приватним сектором, наприклад, у сфері надання необхідної для кібербезпеки інформації [7]. При цьому як Сили самооборони, так й Збройні сили США мають забезпечувати контроль за своїми мережами та системами, обмінюватися досвідом з питань забезпечення кібербезпеки, підтримувати стійкість своїх мереж для досягнення цілей своєї діяльності, сприяти удосконаленню національних систем кібербезпеки, проводити двосторонні навчання для забезпечення ефективної співпраці з питань кібербезпеки в різних ситуаціях. У разі кіберінцидентів, спрямованих проти японської держави, елементів її критичної інфраструктури або мереж служб, що використовуються Силами самооборони та Збройними силами США у Японії, остання буде нести основну відповідальність за реагування, а США, спираючись на тісну двосторонню координацію, надаватиме відповідну підтримку [7].

Слід зазначити, що Міністерство оборони Японії та Міністерство оборони США чітко так й не визначили, які саме кіберінциденти підпадають під дії у відповідь, наприклад, використання Сил самооборони Японії та Збройні сили США як відповідь на кібератаку. Водночас є посилання на Таллінський посібник, в якому чітко проведено межу між різновидами кібератак. Так, найбільш небезпечними «атаками» вважаються такі кібероперації, що можуть завдати шкоду фізичному здоров'ю людей або призвести до пошкодження майна, а отже можуть потрапити під дію права на самозахист. Кібератаки, які не призвели до загибелі людей або фізичної шкоди майну, більш точно можуть бути охарактеризовані як кіберзлочини, кібершпигунство або кіберсаботаж, і не можуть призвести до розгортання Сил самооборони чи Збройних сил США у відповідь, а реагувати на події мають правоохоронні структури та організації [7]. Одним з найбільш вірогідних сценаріїв – це кібератака на системи командування та управління, що використовується Силами самооборони Японії. Якщо контроль над системою буде втрачено, а супротивник використає цю ситуацію для переміщення збройних сил, Японія може розглянути можливість використання кібернетичної контратаки у відповідь. Але дії повинні бути зваженими, щоб не допустити переростання інциденту у фізичний конфлікт чи війну.

У той же час виникає дилема, чи можна вважати кібервторгнення аналогом вторгнення у повітряний простір чи територіальні води. З погляду розташування даних, надзвичайно важко виявити національні кордони кіберпростору. Однак, коли йдеться про кіберпростір з погляду географічного розташування критичних елементів інфраструктури, визначити такі кордони та правову юрисдикцію стає можливим. Отже, якщо ідентифіковано кібератаку, що завдає шкоду фізичним об'єктам у межах національних кордонів, держава може оперативно реагувати на загрозу.

Водночас Міністерство оборони Японії та Сили самооборони не можуть розглядати застосування активних «наступальних» заходів у кіберпросторі через статтю 9 Конституції Японії, оскільки використання зброї навіть для проведення первинних контратак ускладнене чинними законодавчими рамками. Але, якщо держава доведе причетність зарубіжних країн до кібернападу, вона отримає можливість зупинити їх за допомогою кіберзаходів (не використовуючи військові сили). Тому активні «захисні» заходи в кіберпросторі знаходяться в межах доступних варіантів. Водночас, на думку експертів [1], в умовах постійного зростання масштабів кіберзагроз, можливості допомогти іншим країнам у сфері захисту критично важливих елементів національної інформаційної інфраструктури навіть у США стають надзвичайно обмеженими. Тому найефективнішим є, наприклад, сприяння та допомога Японії розвивати власну систему кібербезпеки.

Для реалізації завдань двостороннього співробітництва у сфері кібербезпеки Японія і США створили низку як загальних, так й спеціальних механізмів. Наприклад, загальні питання ролі і значення кібербезпеки у системі двостороннього співробітництва у сфері безпеки і оборони розглядаються в рамках спеціальних зустрічей між Японією і США, а також роботи Консультативного комітету з питань безпеки Японії та США («Зустріч 2 + 2»). Для вирішення практичних завдань співробітництва у сфері кібербезпеки було ініційовано створення двостороннього стратегічного Кібердіалогу Японія-США, Діалогу з питань політичного співробітництва між Японією та США в галузі Інтернет-економіки, Робочих груп, наприклад, з питань кіберзахисту між Міністерством оборони Японії та Міністерством оборони США [17].

Двосторонні зустрічі в рамках Кібердіалогу

відбувалися щороку з 2013 р по 2018 р. Основною метою зустрічі представників Японії та США було визначено проведення двосторонніх консультацій на найвищому рівні щодо обміну інформацією про кіберзагрози, стандартизації підходів до проблеми розробки міжнародної кіберполітики, порівняння національних кіберстратегій, співпраці у сфері захисту критичної інфраструктури тощо. Практика проведення зустрічі в рамках Кібердіалогу Японії та США уможливила не тільки поглиблення двосторонньої співпраці з широкого кола питань кібербезпеки, а й зміцнила японсько-американський альянс в цілому. Досягнути успіхів вдалося завдяки реалізації таких завдань: забезпечення ефективного обміну інформацією з різноманітних проблем кібербезпеки, що становлять взаємний інтерес, обговорення та реалізація усіх можливих заходів співробітництва в зазначеній сфері; участь у міжнародних кіберфорумах для досягнення базових цілей співробітництва, особливо з питань застосування норм відповідальної поведінки держави в кіберпросторі; розробка практичних заходів щодо зміцнення довіри та впровадження національних кіберстратегій урядами обох держав з метою зменшення кількості ризиків в кіберпросторі; збереження відкритості та сумісності на основі багатостороннього підходу до управління Інтернетом; координація співпраці в галузі кібербезпеки з третіми країнами; впровадження ефективних механізмів співпраці між урядами та приватним сектором для забезпечення безпеки критичних елементів інфраструктури; закріплення ролі і значення системи кіберзахисту в національних стратегіях безпеки і оборони, а також обговорення та подальше включення нових напрямків двостороннього співробітництва в галузі кіберзахисту [8]

Під час проведення зустрічей в рамках Кібердіалогу було визначено основні складові спільного підходу урядів Японії та США до проблеми кіберполітики з метою впровадження ефективної системи кіберполітики. Представники обох країн обговорювали питання співробітництва за такими напрямами: захист критичної інфраструктури держав, розбудова потенціалу у сфері протидії викликам і загрозам у кіберпросторі, протидія зростанню кіберзлочинності та пошук ефективних механізмів запобігання виникненню та поширенню феномену, проблеми забезпечення пріоритетів національної безпеки в кіберпросторі, формування кіберпотенціалу та вироблення спільних підходів у питаннях міжнародної стратегії забезпечення кібербезпеки. Як зазначалося в офіційних заявах представників Японії та США за результатами проведення зустрічей, Кібердіалог має поглибити спільне розуміння відповідних організацій, політики та операційної архітектури, а також визначити можливості для зміцнення механізмів двостороннього співробітництва у подальшому [8; 10-12; 18; 19]. Слід також відзначити, що під час зустрічей особливу увагу представники обох країн приділяли питанню розвитку національної системи кібербезпеки Японії та США. На думку урядовців, ефективне двостороннє співробітництво можливе лише за умови високого рівня національних стандартів забезпечення безпеки в інформаційному середовищі [11].

Підкреслимо, що П'ятий Кібердіалог між Японією та США відбувся у липні 2017 року після зустрічі між прем'єр-міністром С. Абе та президентом Д. Трампом, на якій представники обох держав підтвердили наміри розширювати двостороннє співробітництво в галузі кібербезпеки. Водночас занепокоєння викликала сама позиція Д. Трампа, який заявив про наміри згортати присутність США у АТР. Це викликало хвилю коментарів від урядовців та експертів, які застерігали, що це призведе до появи суттєвих викликів для системи безпеки регіону та країн-союзників США – Японії та Південної Кореї, які намагатимуться шукати інших геополітичних партнерів, що замінять «американську парасолю». Отже такий крок може призвести до неоднозначних геополітичних та безпекових наслідків, що усвідомлює і Японія, і США. Система альянсів, створена США після Другої світової війни, стала основою для просування та захисту інтересів Америки в регіоні, Японія ж відігравала основну роль у цьому процесі. Водночас Д. Трамп постійно зазначає, що США несуть набагато більше витрат, ніж інші учасники альянсів, незважаючи на двосторонню зацікавленість у підтримці співробітництва. Тому, на думку експертів, задля збереження зацікавленості США у продовженні двостороннього співробітництва, Японії слід розширювати свою участь в альянсі як на рівні фінансування, так й на рівні підвищення технічної спроможності у сфері безпеки та оборони. У контексті кібербезпеки йдеться про підвищення стандартів захисту національного інформаційного простору та удосконалення системи швидкого реагування на кіберінциденти, а також пошук та надання оперативної інформації, що є важливою для забезпечення кібербезпеки обох країн [15].

Під час чергової зустрічі Консультативного комітету з питань безпеки Японії та США у форматі «2+2» 19 квітня 2019 р. у Вашингтоні обговорювалися питання кібербезпеки як однієї з пріоритетних сфер двостороннього співробітництва. США підтвердили свою готовність виконувати зобов'язання надавати допомогу у випадку серйозних кіберінцидентів, спрямованих проти Японії [2]. Представники обох країн висловили чітку позицію щодо посилення співпраці у сфері кібербезпеки, включаючи можливості стримування та реагування, оскільки зростання нових типів загроз обумовлює потребу поєднання зусиль задля забезпечення переваг Альянсу у вирішенні питань безпеки в рамках АТР. Але для досягнення результату необхідно, щоб кожна країна відповідала за розвиток відповідних можливостей для захисту своїх національних мереж та критичної інфраструктури [2].

Учасники зустрічі також обговорили можливості застосування Статті 5 Договору про безпеку у випадку кібератаки. Так, як зазначалося у підсумковій спільній заяві за результатами зустрічі, кібератака може за певних обставин розглядатися як збройний напад відповідно до Статті 5 Договору, але рішення щодо застосування зазначеної статті

до конкретної кібератаки буде ухвалюватися у кожному конкретному випадку шляхом двосторонніх політичних консультацій. Такий крок є відповіддю на нові загрози, пов'язані із швидким технологічним прогресом КНР та Росії. Зокрема, М.Помпео виступив з критикою на адресу саме Китаю, який суттєво активізував свою діяльність у кіберпросторі, оскільки у геополітичній конкуренції часто кидає виклик існуючим міжнародним нормам і принципам саме завдяки використанню нових засобів протиборства, наприклад, кіберзброї, кібершпигунства або кіберсаботажу [4]. Тому саме такі альянси, як той, що створили Японія і США, є запорукою миру і безпеки в АТР. Водночас деякі експерти попередили про складність у встановленні та доведенні причетності інших держав до здійснення кібератаки. Так, Т. Кавагучі, старший науковий співробітник компанії Tokio Marine & Nichido Risk Consulting Co., заявив, що для того, щоб Японія та США відповіли на атаку спільно, потрібно здійснити ідентифікацію нападника, але це зробити вкрай важко, тому ймовірно буде потрібно ухвалювати саме політичне рішення [2].

Під час прес-конференції після зустрічі на саміту G20 в Осаці у липні 2019 р. Д. Трамп знову заявив, що договір між Японією та США 1960 р. є «несправедливим» і потребує зміни. Водночас президент США зазначив, що не прагне виходу з пакту, але вважає, що його слід переглянути, відповідно до сучасних умов. Важливим чинником в цьому процесі є збільшення ролі Японії у реалізації основних цілей і завдань Договору про безпеку [14]. Як зазначають експерти, такі заяви можуть бути пов'язані з прагненням США змусити не тільки збільшити масштаби участі в реалізації пріоритетів співробітництва у сфері безпеки, але й спонукати Японію до поступок у двосторонніх торгових переговорах щодо збільшення обсягів закупівель американської оборонної техніки [3]. Для самої ж Японії пропонується використати Олімпіаду 2020 для того, щоб питання безпеки не тільки не стали другорядним фактором двостороннього співробітництва, а навпаки, перетворилися на пріоритет сучасної політики у сфері безпеки та оборони. Особливу роль має відграти питання посилення заходів у сфері кібербезпеки [20]

Висновки. Потужні геополітичні трансформації та непередбачуваність використання результатів інформаційного та науково-технічного прогресу, призвели до появи нових викликів та загроз для системи підтримання міжнародного миру і безпеки. Під впливом цих факторів відбувається швидка трансформація середовища безпеки як на глобальному, так й на регіональному рівнях. Тому перед японсько-американським альянсом у сфері безпеки постали нові завдання, що вплинули на перегляд пріоритетів двостороннього співробітництва у сфері безпеки і оборони та обумовили включення до порядку денного проблеми кібербезпеки. Ситуація ускладнюється й тим фактом, що потенційні супротивники обох держав активно нарощують кіберпотугу і використовують різноманітні види і типи кібератак для завдання потужного удару як по регіональній системі безпеки, так й по її ключовим акторам. Тому й Японія, й США висловили занепокоєння зростанням потенційного руйнівного впливу кібератак на критичні елементи інфраструктури держав, що може мати негативні наслідки для всіх держав АТР. Отже питання кібербезпеки набувають дедалі більшої актуальності, про що свідчить постійна увага представників обох країн до їх вирішення в рамках реалізації програм двостороннього співробітництва у сфері безпеки та оборони.

Список використаних джерел

1. Davis, J.S., Libicki, M.C., Johnson, S.E., Kumar, J., Watson, M., Karode A., 2016. *A Framework for Programming and Budgeting for Cybersecurity*. [online] Santa Monica, Calif.: RAND Corporation. Available at: <https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL186/RAND_TL186.pdf > [Accessed 16 October 2019].
2. Hurst, D., 2019. 'Japan, US Beef up Their Cyber Alliance', *The Diplomat* [online] 26 April. Available at: <https://thediplomat.com/2019/04/japan-us-beef-up-their-cyber-alliance/> [Accessed 16 October 2019].
3. Japan braced for more security treaty talks with U.S*., The Asahi Shimbun* [online] 30 June. Available at: <http://www.asahi.com/ajw/articles/AJ201906300030.html> [Accessed 16 October 2019].
4. Jiji, K., 2019. 'U.S. to defend Japan from cyberattack under security pact', *The Japan Times* [online] 04 April. Available at: <https://www.japantimes.co.jp/news/2019/04/20/national/politics-diplomacy/first-japan-u-s-say-security-treaty-cover-cyberattacks/#.XZ2HCv9X-qHv> [Accessed 16 October 2019].
5. Kelley, M.B., 2014. 'Here's The Full FBI Statement Calling Out North Korea For The Sony Hack', *Business insider* [online] 19 December. Available at: <https://www.businessinsider.com/heres-the-full-fbi-statement-calling-out-north-korea-for-the-sony-hack-2014-12> [Accessed 16 October 2019]
6. Lewis, J.A., 2015. *U.S.-Japan Cooperation in Cybersecurity A Report of the CSIS Strategic Technologies Program* [online] Center for Strategic and International Studies. Available at: <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf> [Accessed 16 October 2019].
7. Libicki, M.C., 2016. 'U.S.-Japanese Cooperation in Cyberspace: Potential and Limitations'. In: Harold, S.W., Libicki, M.C., Tsuchiya, M., Ito, Y., Cliff, R., Jimbo, K., Tatsumi, Y. *U.S.–Japan Alliance Conference. Strengthening Strategic Cooperation* [online], pp.6-15. Available at: <https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF351/RAND_CF351.pdf> [Accessed 16 October 2019].
8. Ministry of Foreign Affairs of Japan, 2013. *Joint Statement Japan-U.S. Cyber Dialogue* [online] (10 May). Available at: <https://www.mofa.go.jp/region/page22e_000001.html> [Accessed 16 October 2019].
9. Ministry of Foreign Affairs of Japan, 2015. *The Guidelines for Japan-U.S. Defense Cooperation* (April 27) [online]. Available at: <https://www.mofa.go.jp/files/000078188.pdf> [Accessed 16 October 2019].
10. Ministry of Foreign Affairs of Japan, 2016. *The 4th Japan-US Cyber Dialogue* [online] (July 27). Available at: <https://www.mofa.go.jp/press/release/press4e_001218.html> [Accessed 16 October 2019].
11. Ministry of Foreign Affairs of Japan, 2017. *The 5th Japan-U.S. Cyber Dialogue* [online] (July 24). Available at: <https://www.mofa.go.jp/press/release/press3e_000115.html> [Accessed 16 October 2019].
12. Ministry of Foreign Affairs of Japan, 2018. *The 6th Japan-US Cyber Dialogue* [online] (July 25). Available at: <https://www.mofa.go.jp/press/release/press4e_002116.html> [Accessed 16 October 2019].

13. Peterson, A., 2014. 'The Sony Pictures hack, explained', *The Washington Post* [online] 18 December. Available at: <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/> [Accessed 16 October 2019]

14. Sieg, L., 2019. '*Trump's criticism of U.S.-Japan security pact could be headache for Abe*' [online]. Reuters. Available at: <https://www.reuters.com/article/us-japan-usa-security-analysis/trumps-criticism-of-us-japan-security-pact-could-be-headache-for-abe-idUSKCN1TW1XH> [Accessed 16 October 2019].

15. Solomon, R., 2018. 'Japan must do more to support its alliance with the U.S.', *The Japan Times* [online] 11 September. Available at: <https://www.japantimes.co.jp/opinion/2018/09/11/commentary/japan-commentary/japan-must-support-alliance-u-s/#.XZ6kdf9XqHv> [Accessed 16 October 2019].

16. Tatsumi, Y., 2015. '4 Takeaways From the New US-Japan Defense Guidelines. What's new about the Guidelines, and what that actually means for U.S.-Japan cooperation moving forward', *The Diplomat* [online] 29 April. Available at: <https://thediplomat.com/2015/04/4-takeaways-from-the-new-us-japan-defense-guidelines/> [Accessed 16 October 2019].

17. Tsuchiya, M., 2016. 'Japan-U.S. Cooperation on Cybersecurity'. In: Harold, S.W., Libicki, M.C., Tsuchiya, M., Ito, Y., Cliff, R., Jimbo, K., Tatsumi, Y. *U.S.–Japan Alliance Conference. Strengthening Strategic Cooperation* [online], pp.16-25. Available at: <https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF351/RAND_CF351.pdf> [Accessed 16 October 2019].

18. U.S. Department of State. Diplomacy in Action, 2014. *The Second US-Japan Cyber Dialogue. Media Note* [online] (April 10)]. Available at: < https://2009-2017.state.gov/r/pa/prs/ps/2014/04/224648.htm> [Accessed 16 October 2019].

19. U.S. Department of State. Diplomacy in Action, 2015. *The Third U.S.-Japan Cyber Dialogue. Media Note* [online] (July 17). Available at: <https://2009-2017.state.gov/r/pa/prs/ps/2015/07/245032.htm> [Accessed 16 October 2019].

20. Wells, L., Tsuchiya, M., Repko, R., 2017. *Improving Cybersecurity Cooperation between the Governments of the United States and Japan* [online] Sasakawa Peace Foundation USA. Available at: <https://spfusa.org/wp-content/uploads/2017/02/Improved-Cybersecurity-cooperation.pdf> [Accessed 16 October 2019].