

УДК 327.7 : 004.738.5 (540+520+510)

## **ПОЗИЦІЇ ДЕРЖАВ АЗІЙСЬКО-ТИХООКЕАНСЬКОГО РЕГІОНУ ЩОДО УХВАЛЕННЯ РЕЗОЛЮЦІЙ З ПИТАНЬ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РАМКАХ ООН**

## **POSITIONS OF STATES OF THE ASIA-PACIFIC REGION REGARDING THE ADOPTION OF RESOLUTIONS ON INTERNATIONAL INFORMATION SECURITY ISSUES WITHIN THE FRAMES OF THE UN**

## **ПОЗИЦИИ ГОСУДАРСТВ АЗИАТСКО-ТИХООКЕАНСКОГО РЕГИОНА КАСАТЕЛЬНО ПРИНЯТИЯ РЕЗОЛЮЦИИ ПО ВПРОСАМ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ООН**

### **Рижков М.М.**

Доктор політичних наук, професор, завідувач кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка. E-mail: rnn253@gmail.com

### **Сябро А.І.**

Аспірант кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка. E-mail: siabro.anastasiia@gmail.com

### **Ryzhkov Mykola M.**

Doctor of Science (Political Science), Professor, Head of the Chair of International Information of the Institute of International Relations, Taras Shevchenko National University of Kyiv. E-mail: rnn253@gmail.com

### **Siabro Anastasiia I.**

Graduate student of the Institute of International Relations of the Kyiv National Taras Shevchenko University. E-mail: siabro.anastasiia@gmail.com

### **Рыжков М.М.**

Доктор политических наук, профессор, заведующий кафедры международной информации Института международных отношений Киевского национального университета имени Тараса Шевченко. E-mail: rnn253@gmail.com

### **Сябро А.И.**

Аспірант кафедри міжнародної інформації Інститута міжнародних відносин Київського національного університету імені Тараса Шевченко. E-mail: siabro.anastasiia@gmail.com

**Анотація.** *Досягнення у сфері інформатизації та телекомунікацій виступають суттєвою складовою процесу трансформації міжнародної системи миру і безпеки. У статті відзначено, що зміни мають подвійний характер наслідків. З одного боку, нові технології стають важливою складовою стратегії модернізації суспільства в країнах, що розвиваються, з другого – можуть використовуватися для модернізації озброєнь або створення нових засобів протидії у сучасних міжнародних відносинах. Найбільш актуальним питання використання інформаційних технологій постає перед країнами АТР. У статті розглянуто процес обговорення нових викликів та загроз для міжнародної безпеки, що виникають внаслідок розвитку та широкого впровадження інформаційно-комунікаційних технологій. Досліджено позиції держав щодо ухвалення резолюції у сфері міжнародної інформаційної безпеки на прикладі Японії, Індії та Китаю. У статті показано, що позиції держав мають як спільні, так й відмінні риси. Так, Японія та Індія прагнуть досягнути збалансованої системи міжнародної інформаційної безпеки, яка одночасно повинна мати механізми запобігання виникненню*

загроз в інформаційній та науково-технологічній сферах та гарантувати продовження науково-технологічного розвитку, що є важливою складовою сучасних стратегій розвитку і модернізації багатьох країн світу. Китай виступив із позицією жорсткого регулювання питань міжнародної інформаційної безпеки та вироблення відповідних правил поведінки держав у кіберпросторі.

**Ключові слова:** міжнародна безпека, інформаційна безпека, міжнародне співробітництво, інформаційні виклики і загрози, ООН, національна стратегія кібербезпеки, Японія, Індія, Китай.

**Abstract.** *Achievements in the sphere of automatization and telecommunication are an essential component of transformation of the international peace and security system. This article presents, that consequences of changes are of a dual character. On the one hand, new technologies are becoming an important component of society modernization strategies in developing countries, on the other hand, they can be used for armament modernization or creation of new means of confrontation in modern international relations. APR countries face the most relevant issue of information technologies usage. The article deals with the process of discussion of new challenges and threats to international security, emerging as a result of development and large-scale implementation of information-communication technologies. Positions of states regarding the adoption of resolution in the sphere of international information security were studied through examples of Japan, India, and China. It is proved in the article, that information technologies have become an important component of the security system in the world. Technologies usage may lead to steady international development as well as to information arms race. That is why working out a common position on international information security issues is of crucial importance. It is within the framework of the UN, that different states of the world are given an opportunity to express their visions of the problem of international information security and work out common approaches to its solution. The article shows, that states' positions have similar as well as different features. For instance, all states express concern regarding possible limitation of technology transfer for the establishment of a more controlled international political environment. But states' positions have major differences as to mechanisms of information security provision. Thus, Japan and India strive to achieve a balanced system of international information security, which should at the same time have preventive mechanisms against the emergence of threats in the information and science and technology spheres and guarantee continuation of scientific-technological development, which is a crucial component of development and modernization strategies in many countries of the world. China came forward with position of strong regulation of international information security issues and suggested framing of corresponding regulations of the states' conduct in the cyberspace.*

**Key words:** *international security, information security, international cooperation, information challenges and threats, UN, national cyber security strategy, Japan, India, China.*

**Аннотация.** *Достижения в сфере информатизации и телекоммуникаций выступают существенной составляющей процесса трансформации международной системы мира и безопасности. В статье отмечено, что изменения имеют двойственный характер последствий. С одной стороны, новые технологии становятся важной составляющей стратегии модернизации общества в развивающихся странах, с другой - могут использоваться для модернизации вооружений или создание новых средств противоборства в современных международных отношениях. Наиболее актуальным вопросом использования информационных технологий предстает перед странами АТР. В статье рассмотрен процесс обсуждения новых вызовов и угроз международной безопасности, возникающих в результате развития и широкого внедрения информационно-*

коммуникационных технологий. Исследована позиции государств по принятию резолюции в сфере международной информационной безопасности на примере Японии, Индии и Китая. В статье показано, что позиции государств имеют как общие, так и отличительные черты. Так, Япония и Индия стремятся достичь сбалансированной системы международной информационной безопасности, которая одновременно должна иметь механизмы предотвращения возникновения угроз в информационной и научно-технологической сферах, гарантировать продолжение научно-технологического развития, что является важной составляющей современных стратегий развития и модернизации многие страны мира. Китай выступил с позиции жесткого регулирования вопросов международной информационной безопасности и выработки соответствующих правил поведения государств в киберпространстве.

**Ключевые слова:** международная безопасность, информационная безопасность, международное сотрудничество, информационные вызовы и угрозы, ООН, национальная стратегия кибербезопасности, Япония, Индия, Китай.

**Постановка проблеми.** Проблема інформаційної безпеки постає як нагальна у формуванні сучасної системи міжнародного миру і безпеки. Процеси бурхливого інформаційного та науково-технологічного розвитку створюють не тільки нові можливості для вирішення найбільш актуальних проблем сучасності – економічного розвитку та подолання диспропорцій між країнам, відновлення екологічного балансу та впровадження нових джерел енергії, формування громадянського суспільства тощо. Водночас, як свідчать чисельні дослідження практики застосування високих технологій, вони дедалі частіше використовуються як технології подвійного призначення. Впровадження обмежувальних механізмів можуть спричинити порушення міжнародних зобов'язань, спрямованих на розвиток науково-технологічного співробітництва з метою допомоги країнам, що розвиваються. Отже, виникає потреба вироблення нових механізмів регулювання обміну знаннями та технологіями, які не тільки не зруйнували б досягнутий прогрес у сфері науково-технологічного співробітництва, але й допомогли виробити на основі консенсусу між усіма учасниками процесу ефективні механізми формування системи міжнародної інформаційної безпеки. В цьому контексті важливим є дослідження досвіду провідних країн АТР, які, з одного боку, демонструють високі темпи інформаційного та технологічного зростання, формування системи інновацій, становленні інформаційної індустрії та впровадження нових інформаційних продуктів та послуг, що неможливо було б досягнути без реалізації стратегій співробітництва у галузі інформаційно-комунікаційного та науково-технологічного розвитку. З другого боку, окремі країни регіону виступають міжнародними акторами, що спричиняють виникнення сучасних викликів і загроз на основі використання високих технологій та наукових досягнень.

**Мета статті.** Дослідити особливості трансформації позицій провідних держав АТР щодо ухвалення резолюції ГА ООН «Досягнення науки і техніки та їх вплив на міжнародну безпеку», яка є основою для вироблення фундаментальних принципів міжнародної інформаційної безпеки, і виявити особливості бачення **Японією, Індією та Китаєм** базових міжнародних механізмів регулювання використання інформаційних технологій у контексті міжнародної безпеки.

**Аналіз останніх досліджень і публікацій.** Вивчення проблеми ухвалення резолюції з питань міжнародної інформаційної безпеки переважно здійснюється в рамках правових теорій, що стосуються вироблення міжнародних норм у сфері безпеки. Водночас зосередження тільки на правових аспектах не дозволяє виявити причини розбіжностей в оцінці інформаційних загроз для міжнародної безпеки та політичної позиції окремих держав, що можуть пов'язувати підтримку певних міжнародних документів з питаннями національного інформаційного суверенітету та національної інформаційної безпеки. Так, загальні питання міжнародної інформаційної безпеки

розглядаються у роботах відомих зарубіжних та вітчизняних авторів – Р. Армітіджа, Зб. Бжезинського, М. Лібіцкі, Дж. Ная, У. Оуенса, О. Тоффлера, В. Дергачова, О. Манойла, С. Расторгуєва, Д. Дубова, О. Зернецької, О. Литвиненка, О. Ожевана, В. Петрова, Г. Почепцова, О. Сосніна, та ін. Суттєвий внесок у дослідження проблеми ухвалення міжнародних документів у сфері інформаційної безпеки здійснили Р. Гурвітц, Б. Світманн, С. Бойко, Р. Болгов, О. Демідов, І. Кванталіані, А. Крутських, О. Лобанова, Д. Маркар'ян, О. Маслакова, Н. Ромашкіна, Ю. Томілова, В. Шерстюк, Є. Макаренко, Ю. Романчук, О. Фролова та ін. У той же час дослідження, присвячені висвітленню позиції держав АТР щодо ухвалення резолюцій ГА ООН у сфері інформаційної безпеки мають фрагментарний характер і переважно розглядаються крізь призму протистояння двох геополітичних лідерів – США та РФ.

**Виділення невирішених раніше частин загальної проблеми.** Країни АТР в сучасній системі міжнародних відносин виступають дієвими акторами, що можуть активно впливати на формування пріоритетів міжнародного співробітництва. В умовах формування глобального суспільства знань саме ці країни демонструють високі темпи інформаційного і науково-технологічного розвитку. Водночас, з погляду забезпечення безпеки, країни лідери – Японія, Китай та Індія – мають різний рівень готовності до викликів та загроз інформаційної доби. Так, якщо Японія визнається однією з найбільш захищених держав світу в інформаційній сфері, то Індія, незважаючи на потужний інформаційний, науковий та технологічний потенціал, на жаль не вважається зразком безпеки та захисту національного інформаційного простору, хоча й має достатньо розгалужену правову базу. Китай має особливий статус у сфері інформаційної безпеки, оскільки вважається геополітичним опонентом та традиційним супротивником для США в глобальному інформаційному просторі. Так, КНР, як один з лідерів інформаційного та науково-технологічного розвитку світу, має значний потенціал для розбудови інформаційного суспільства. Але, як свідчить практика, Китай все ще посідає провідні позиції серед країн, які виробляють і масово використовують продукти піратської індустрії у сфері сучасних технологій, вдаючись до промислового шпигунства та хакерських атак. Крім того, за даними аналітичних центрів часто саме КНР виступає як фактор небезпеки та дестабілізації у сфері інформаційної безпеки, оскільки вдається до методів кібершпигунства та кібератак на урядові та безпекові структури провідних держав світу, зокрема, США, для тиску на уряди та систему ухвалення рішень.

Незважаючи на такі розбіжності у характеристиках рівня розвитку системи національної безпеки, Японія, Індія і Китай є активними учасниками процесу вироблення міжнародних норм і принципів у сфері інформаційної безпеки, мають свою позицію щодо окремих питань та виступають з різноманітними ініціативами в рамках діяльності міжнародних організацій, зокрема, ООН. Таким чином, дослідження позиції цих країн щодо ухвалення резолюції «Досягнення науки і техніки та їх вплив на міжнародну безпеку» дозволяє виявити спільні проблеми і бачення шляхів їх вирішення як для країн регіону, так й світу в цілому. Водночас, вивчення позиції держав дозволяє виявити унікальні риси національних підходів щодо формування національної системи інформаційної безпеки, яку доцільно розглядати крізь призму комплексного аналізу політичних, правових та інформаційних факторів.

**Виклад основного матеріалу дослідження.** В умовах розбудови глобального інформаційного суспільства та подальшого бурхливого науково-технологічного розвитку питання інформаційної безпеки набувають дедалі більшого значення як для глобальної системи підтримання миру і стабільності, так й для системи національної безпеки всіх держав світу. З одного боку, новітні досягнення у сфері науки і технологій відкривають широкі можливості і набувають все більшого значення для реалізації стратегії модернізації суспільства, появи нових моделей економічної діяльності, розв'язання проблем соціально-економічного характеру, трансформації політичної

діяльності та гуманітарного розвитку, а з другого, – містять колосальний руйнівний потенціал, оскільки виступають як новітні загрози для міжнародного миру і безпеки. Саме тому ООН сьогодні є важливим міжнародним інститутом, в рамках діяльності якого країни намагаються обговорити та виробити спільну позицію з питань регулювання проблеми міжнародної інформаційної безпеки.

Зазначимо, що питання використання досягнень науки і техніки у військових цілях обговорюються в рамках засідання Першого комітету з кінця 1980-х-початку 1990-х рр. Так, у 1988 р. представник Індії вніс проект резолюції на розгляд Першого комітету Генеральної Асамблеї, зауваживши при цьому, що подальше зростання обсягів фінансування розробки нових систем озброєння можна порівняти з дозованим використанням вибухової ядерної сили. Мініатюризація і розширення масштабів електронно-обчислювальних операцій за допомогою мікроелектронних пристроїв, а також нові паливні та лазерні технології змінюють середовище безпеки. Тому необхідно розпочати роботу над виробленням консолідованої позиції з відповідних проблем, щоб зробити можливими спільні зусилля з їх вирішення [1].

7 грудня 1988 було прийнято першу резолюцію A/43/77 «Досягнення науки і техніки та їх вплив на міжнародну безпеку» (за – 129 голосів, проти – 7, утрималися – 14). У документі Генеральному секретарю було доручено стежити за досягненнями науки і техніки, особливо за тими, які мали потенційне військове застосування, і здійснювати оцінку їх впливу на міжнародну безпеку, за результатами чого представити 49-й сесії в 1990 році Генеральній Асамблеї відповідну доповідь. Основними аспектами технічних досягнень, що були висвітлені у доповіді, стосувалися ядерної технології, космонавтики, матеріалознавства, інформатики і біотехнологій. З метою сприяння проведенню дослідження були залучені профільні експерти для подачі індивідуальних звітів про оцінку впливу і військовий потенціал досягнень у відповідних сферах [2]. У доповіді, зокрема, зазначалося, що сучасні технології мають сприяти подальшому розвитку світової спільноти, а не заважати позитивним тенденціям у міжнародних відносинах, пов'язаними із реалізацією Договору між СРСР та США про ліквідацію ракет середньої та малої дальності (1997-1988 рр.). Модернізація та якісне удосконалення систем ядерного та звичайних озброєнь є наслідком впровадження досягнень науки і техніки, що призведе не тільки до збільшення радіусу їх дії, підвищення точності та посилення дії ураження, а й до появи нових видів озброєнь. Викликав занепокоєння й той факт, що значна частина сучасних технологій не використовується для подолання багатьох проблем, що постають перед світовою спільнотою, наприклад, збалансованого міжнародного соціально-економічного розвитку та подолання розриву між розвиненими країнами та країнами, що розвиваються. Водночас зростає ризик неконтрольованої розробки та купівлі ядерної, хімічної та біологічної зброї країнами, які не є учасниками існуючих угод у сфері скорочення озброєнь. У резолюції 45/60 «Досягнення науки і техніки та їх вплив на міжнародну безпеку» Генеральна Асамблея прийняла до відома доповідь і висловила свою згоду з тим, що міжнародне співтовариство має уважно стежити за змінами технологій, оскільки питання підтримання міжнародної системи миру і безпеки були і залишаються головним пріоритетом діяльності ООН [3].

З того часу було оприлюднено цілу низку доповідей Комітету та ухвалено резолюції, в яких постійно наголошується на таких проблемах, як: досягнення науки і техніки та їх вплив на міжнародну безпеку, наука і техніка для роззброєння, роль науки і техніки для галузей, пов'язаних з безпекою і роззброєнням, а також передача технологій, що мають військове призначення [4]. Так, у щорічній Доповіді комісії з питань роззброєння (1991 р.) зазначалося, що використання нових технологій у військовій сфері може призвести до якісно нової гонки озброєнь (наприклад, модернізації зброї масового ураження), що є неприпустимим, оскільки призводить до негативізації наслідків науково-технологічного прогресу, результати якого можуть і

мають бути використані передусім в мирних цілях, зокрема, задля подальшого соціально-економічного розвитку. У документі також підкреслюється, що сучасні технології мають подвійний характер використання. Отже, встановлення контролю та певних обмежень на використання результатів науково-технологічного розвитку не повинно обмежувати можливості використання високотехнологічних продуктів, послуг та «ноу-хау» в мирних цілях. Суттєву роль у досягненні міжнародного миру і безпеки було відведено співробітництву, спрямованому на спільне використання досягнень науки і техніки для контролю над озброєннями та роззброєнням [4].

Важливим кроком на шляху до вироблення міжнародних норм і принципів у сфері інформаційної безпеки, які б стали основою для подальшої співпраці з метою забезпечення миру і безпеки, стало обговорення і ухвалення резолюцій на 53-й сесії Генеральної Асамблеї ООН – «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» [5] та «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» [6]. Так, у першому документі йшлося про подвійну природу науково-технологічних досягнень і зазначалося, що досягнення науки і техніки сьогодні використовуються як у цивільній, так й у воєнній сферах. Водночас підкреслювалася потреба подальшого науково-технологічного прогресу, який слід використовувати задля поступального розвитку усього людства, сприяючи стійкому економічному і соціальному розвитку усіх держав та гарантуючи міжнародну безпеку. Тому вкрай важливим є сприяння розвитку міжнародного співробітництва у сфері використання досягнень науки і техніки на основі передачі «ноу-хау», послуг, нових знань та обміну ними в мирних цілях. При цьому передача високих технологій та сучасних наукових розробок подвійного призначення в умовах відсутності дієвих міжнародно-правових механізмів регулювання цієї діяльності здатні спричинити негативний вплив на систему міжнародної безпеки, оскільки можуть призвести до швидкої модернізації сучасних систем озброєнь, зокрема, зброї масового ураження [5].

У резолюції «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» також підтверджується подвійний характер використання досягнень науки і техніки. З одного боку, ці досягнення відкривають широкі можливості для подальшого розвитку цивілізації, розширюють напрями і сфери взаємодії задля добробуту всіх держав, збільшують конструктивний потенціал людства, а тому поширення і використання інформаційних технологій та результатів наукового розвитку торкаються інтересів усього міжнародного співтовариства. З другого, – ці інноваційні технології і засоби можуть бути використані з метою, що суперечить задачам забезпечення міжнародної стабільності і безпеки, можуть негативно вплинути на безпеку усіх держав світу. Тому для попередження неправомірного використання технологій або інформаційних ресурсів зі злочинними чи терористичними намірами держави повинні на міжнародному рівні розглянути питання реальних і потенційних загроз у сфері інформаційної безпеки, розробити загальні принципи, спрямовані на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем і мереж, дати оцінку проблемі інформаційної безпеки та представити власну позицію з актуальних питань інформаційної безпеки. Таким чином держави отримали можливість оприлюднювати бачення шляхів вирішення проблем у сфері інформаційної безпеки, відповідно до національної стратегії і практики її реалізації. Відтоді Генеральний секретар щорічно представляє Генеральній Асамблеї доповідь, що містить позиції держав-членів ООН з даної проблематики [6].

Враховуючи високі темпи інформатизації та проникнення сучасних технологій, а також включення у глобальну систему інноваційного розвитку, для країн АТР проблема інформаційної безпеки набула критичного значення. Тому, починаючи з 53-ої сесії Генеральної Асамблеї ООН провідні держави регіону (Японія, Індія, КНР, Південна Корея та Сінгапур) регулярно представляють свою позицію щодо проблеми використання досягнень науки і техніки у контексті міжнародної безпеки.

Так, Японія представляла свою позицію вперше у 2013 р. У відповіді держави, зокрема, зазначалося, що вона визнає роль і значення кіберпростору як базової інфраструктури для соціально-економічної діяльності державного і приватного секторів. Інформатизація сприяє економічному зростанню, забезпеченню зайнятості та розвитку, а також зміцненню демократії та захисту прав людини шляхом забезпечення свободи інформаційних потоків і свободи вираження думок [7]. Отже доступ до кіберпростору має важливе значення для життя людей в усьому світі. У той же час у зв'язку з інформаційним та науково-технологічним розвитком виникає потреба вироблення більш досконалих механізмів захисту недоторканності особистого життя і прав інтелектуальної власності, а також формування безпечного кіберсередовища з метою використання всіх благ, що ним забезпечуються. Як підкреслюється у документі, кібератаки відбуваються в усьому світі і стають транснаціональною глобальною загрозою, тому країни окремо не в змозі протистояти кіберзлочинам та кібератакам, кількість яких постійно зростає, а більш ефективним є налагодження взаємодії в рамках міжнародного співтовариства, в тому числі між відповідними державами та зацікавленими сторонами [7].

Позиція Японії також містила інформацію про ініціативи самої держави, спрямовані на зміцнення системи інформаційної безпеки та зміцнення потенціалу протистояння кібератакам. Так, в ухваленій Стратегії кібербезпеки Японії на 2013-2015 рр. підкреслюється, що задля забезпечення безпеки і миру японського народу необхідно вжити такі заходи: сприяння обміну в рамках партнерства між державними і приватними структурами інформацією про кібернапади; вдосконалення підготовки співробітників з питань забезпечення безпеки не тільки для урядових установ і промисловості, але й для всіх японських громадян; підвищення обізнаності про кібербезпеку; зміцнення потенціалу з протидії кібернападам в рамках міжнародного співробітництва та розширення внеску держави в розробку міжнародних норм, що стосуються кібербезпеки. Японія вважає, що діючі міжнародно-правові норми, включаючи Статут ООН і норми міжнародного гуманітарного права, можна застосовувати й до кіберпростору. Разом з тим, з огляду на унікальні особливості інформаційно-комунікаційних і мережних технологій, необхідно продовжувати практику обговорення питань про застосування окремих норм і принципів у сфері інформаційної безпеки [8].

У 2016 р. та 2017 р. під час обговорення питання щодо ухвалення резолюції «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» у доповіді Генерального секретаря було також включено позицію Японії щодо проблеми інформаційної безпеки [9-10]. Так, у відповідях 2016 р і 2017 р. наголошувалося, що зусилля Японія у сфері забезпечення інформаційної безпеки базуються на таких принципах, як: свобода інформаційних потоків, верховенство права, відкритість, самоврядування та залучення усіх зацікавлених сторін, які окреслені у Стратегії забезпечення кібербезпеки Японії 2015 року [11]. Пріоритетними напрямками діяльності держави в означеній сфері є: заохочення верховенства права в кіберпросторі, заходи зміцнення довіри і нарощування потенціалу. Щодо заохочення верховенства права, Японія бере активну участь в міжнародних дискусіях, спрямованих на формування загального розуміння того, що діючі норми міжнародного права повинні застосовуватися й у кіберпросторі, а також при розробці необов'язкових і добровільних норм відповідальної поведінки держав як основи для забезпечення стабільності і передбачуваності міжнародного співтовариства. Разом з тим з урахуванням унікальних особливостей інформаційно-комунікаційних технологій необхідно подальше прояснення питання про те, як будуть застосовуватися окремі норми і принципи [10].

Для просування заходів щодо зміцнення довіри потрібно забезпечити транспарентність і обмін інформацією. Проте рівень вжитих заходів варіюється від

держави до держави, оскільки кожна з них має право визначати рівень, який відповідає її можливостям та національним інтересам. Тому Японія бере активну участь в діяльності із зміцнення довіри в рамках двостороннього діалогу та багатосторонніх механізмів, таких, наприклад, як АТЕС та АСЕАН, що дає можливість виробити спільні підходи до вирішення проблеми із усіма зацікавленими країнами регіону.

На думку представників Японії, доцільно впроваджувати такі заходи, які могли б бути прийняті міжнародним співтовариством для зміцнення інформаційної безпеки на глобальному рівні. Наприклад, щодо заохочення верховенства права, то Японія наполягає на необхідності продовження обговорень з приводу вироблення норм міжнародного права, що відносяться до мирного часу, законів, що стосуються права на самозахист, і норм міжнародного гуманітарного права, а також розробки добровільних норм в рамках подальшої роботи Групи урядових експертів з питань інформаційної безпеки. Що стосується зміцнення довіри і нарощування потенціалу, то особливо важливим є заохочення виконання рекомендацій, що містяться в доповідях експертних груп, кожною державою або регіоном [10].

У відповіді Японії на 73-ій сесії Генеральної Асамблеї ООН у 2018 р. зазначалося, що держава вітає прийняття резолюції 72/28 про роль науки і техніки в контексті міжнародної безпеки та роззброєння і сподівається, що здійснення даної ініціативи поглибить розуміння міжнародним співтовариством цієї нової, багатогранної, складної, глобальної і дуже важливої теми [12]. Важливість теми визнається також усіма державами-членами ООН, проте її багатогранність і багатоаспектність потребує подальшого більш глибокого вивчення. При цьому, зазначається у позиції Японії, варто брати до уваги наступне:

- необхідно здійснити структурний аналіз і оцінку поточної ситуації щодо використання новітніх технологій та їх можливого впливу на міжнародну безпеку і роззброєння з тим, щоб можна було визначити сфери, в яких необхідні узгоджені, термінові і результативні міжнародні дії;

- одним з ключових наскрізних питань, пов'язаних з даною темою, є питання про можливе неправомірне використання нових технологій подвійного призначення та зловживання ними, але усуненню цієї загрози не повинне перешкоджати подальшому розвитку науки і техніки;

- потрібно нарощувати потенціал і розробляти необхідні технології у сфері попередження, виявлення і вивчення нових видів загроз, зокрема пов'язаних із застосуванням біологічних і хімічних речовин або високих технологій;

- необхідно дотримуватися міждисциплінарного підходу, оскільки науковий прогрес породжує низку взаємозв'язків, в тому числі між кібербезпекою і дискусією з питань управління штучним інтелектом;

- передачу товарів і технологій подвійного призначення, які можуть бути використані для виробництва зброї масового ураження або звичайних озброєнь і таким чином мати наслідки для міжнародної безпеки, роззброєння та нерозповсюдження, слід контролювати у відповідності з керівними принципами, покладеними в основу режимів контролю за експортом;

- необхідно залучати до участі усі зацікавлені сторони і налагодити тісну співпрацю між політичними, науковими, промисловими колами та громадянським суспільством [12].

Показовим у даному контексті є проведення за ініціативи Японії разом з Центром Генрі Л. Стімсона 23 березня 2018 року в Нью-Йорку Восьмої наради з питань безпеки в форматі «круглого столу», присвяченої темі «Управління передовими технологіями» [12]. На цій нараді експерти держав-членів ООН і представники допоміжних органів Ради Безпеки, науково-дослідних центрів, промисловості та академічних кіл обговорили наслідки розвитку технологій для міжнародної безпеки, а Генеральний секретар наголосив на необхідності максимізувати користь від технічної революції, при



цьому усуваючи і пом'якшуючи пов'язані з нею ризики. Японія сповнена рішучості продовжувати такого роду дискусії, залучаючи до участі в них усі зацікавлені сторони.

Іншою країною-лідером науково-технологічного розвитку АТР, що взяла участь в обговоренні питання про досягнення науки і техніки та їх вплив на міжнародну безпеку, була Індія, яка представила свою позицію у 2016 р. та у 2018 р. [9; 12]. Зазначимо, що з'ясування позиції держави щодо ухвалення резолюції є показовою, оскільки Індія, на жаль, демонструє неготовність ефективно протистояти кіберзагрозам. Так, напочатку 2019 р. британською компанією Comptitech було представлено рейтинг кібербезпеки 60 країн світу, що базується на аналізі таких критеріїв: відсоток стаціонарних комп'ютерів, заражених шкідливим програмним забезпеченням, відсоток заражених мобільних пристроїв, кількість атак троянів-банкерів, частка віддалених telnet-атак, частка атак кріптомайнерів, готовність країни до кібератаки, актуальність законодавства. Законодавство також оцінювалося окремо за такими категоріями: конфіденційність, національна стратегія, оборона, захист інформації, критична інфраструктура, торгівля і злочинність [13]. Так, дослідження показало, що найбільш підготовленою до кіберзагроз країною не тільки в Азійсько-тихоокеанському регіоні, а й у світі в цілому є Японія. Водночас Індія, незважаючи на суттєві досягнення у сфері законодавства, за всіма іншими критеріями оцінки ефективності кібербезпеки посідає 15-ту позицію серед найменш захищених країн світу.

Усвідомлюючи потребу у виробленні міжнародних норм і принципів регулювання сфери кібербезпеки, Індія у 2016 р. у своїй позиції наголошувала на зростанні актуальності безпекових факторів, особливо у контексті впливу інформаційних технологій на економічне зростання та соціальну згуртованість країни [9]. Як підкреслюється у позиції держави, яку було представлено в рамках доповіді Генерального секретаря, розвиток сектору ІКТ супроводжується зростанням кіберзагроз (кібернападів, кіберзлочинів, кібертероризму, шпигунства і відмивання грошей), а також віртуалізацією діяльності терористичних угруповань (наприклад, ІДІЛ), які активно використовують Інтернет і соціальні мережі для вербування нових членів, мобілізації коштів, пропаганди і радикалізації діяльності. Серйозне занепокоєння також викликає використання соціальних мереж, які, з одного боку, відкривають величезні можливості для взаємодії, а з другого, – можуть використовуватися в неправомірних цілях для посилення етнічної і соціальної роз'єднаності. В таких умовах надзвичайно важливим є вироблення загальної позиції міжнародної спільноти щодо поведінки держав в кіберпросторі та вживання заходів із зміцнення довіри і безпеки відповідно до рекомендацій, представлених в доповіді Групи урядових експертів ООН 2015 року.

У відповіді країни, представленої в доповіді Генерального секретаря ООН на 73-й сесії, зауважувалося, що саме Індія (у співавторстві з 18 іншими країнами – Австрією, Анголою, Бангладеш, Бразилією, Бутаном, Німеччиною, Іспанією, Італією, Канадою, Маврикієм, Нідерландами, Парагваєм, Сьєрра Леоне, Фінляндією, Хорватією, Чорногорією, Швейцарією і Швецією) підготувала проект резолюції 72/28 ГА ООН про роль науки і техніки в контексті міжнародної безпеки та роззброєння, яка була прийнята Першим комітетом в 2017 році на сімдесят другій сесії ГА, а згодом – Асамблеєю на основі консенсусу. У документі, зокрема, зазначалося, що активний розвиток науки і техніки є характерною рисою XXI століття. Сьогодні з'являються нові галузі технологій, а в існуючих сферах відкриваються нові можливості для міждисциплінарного співробітництва. Крім того, збільшилася кількість міжнародних суб'єктів, що беруть участь в розробці технологій, водночас, починає змінюватися роль урядів, приватного сектора і установ в сфері досліджень і розробок. Слід зазначити, що чимало країн, що розвиваються, використовують переваги технологій, особливо цифрових технологій, для прискорення темпів економічного розвитку. Це призводить до актуалізації питання міжнародного співробітництва в сфері «великої науки»,

оскільки окремо країни часто не в змозі задовольнити свої потреби в фінансових і людських ресурсах [12].

Отже Індія у своїй позиції підкреслює позитивний потенціал науки і техніки у вирішенні найбільш складних світових проблем – подолання диспропорцій економічного та соціального розвитку, збереження екологічного балансу, виробництво чистої і недорогої енергії, що уможливить реалізацію пріоритетів Порядку денного в галузі сталого розвитку на період до 2030 року. Разом з тим країна висловила занепокоєння щодо впливу новітніх технологій на систему розбросення і міжнародну безпеку. Потенційні переваги і ризики, пов'язані з новими технологіями, такими, наприклад, як синтетична біологія або редагування генома, з розмиванням межі між традиційними галузями науки і техніки, з появою нових можливостей застосування вже існуючих технологій та технологій, що тільки розробляються, зі зближенням наукових галузей, зокрема, хімії та біології, можливості застосування штучного інтелекту і автономних систем в звичайному озброєнні, збільшенням масштабів наслідків застосування кіберзброї державними та недержавними акторами, виникненням потреби звернення до питань космічної безпеки з урахуванням нових технічних досягнень, які стирають різницю між космічним і навколосезним просторами, а також з урахуванням ролі приватного сектора в космічній діяльності, обумовлюють зростання потреби розширення та удосконалення механізмів міжнародного співробітництва. Проблема ускладнюється й тим, що новітні технології можуть використовуватися терористичними та злочинними угрупованнями або стати поштовхом до початку нової гонки озброєнь, що призведе до збільшення масштабів поширення зброї масового ураження, порушення норм діючого міжнародного гуманітарного права, а також порушення етичних норм і прав людини [12].

У підсумку Індія виступила з низкою пропозицій для країн-членів ООН щодо удосконалення міжнародних механізмів регулювання використання досягнень науки і техніки у сфері міжнародної безпеки, зокрема, виробити механізми відстеження та картування останніх науково-технічних досягнень, у тому числі, у сфері ІКТ, продовжити працювати над проблемою використанням таких технологій у військових цілях, зміцнити партнерські відносини з представниками промисловості, наукових кіл і громадянського суспільства задля обговорення і вирішення проблем інформаційної безпеки тощо [12].

Показовою у контексті досліджуваної теми є позиція КНР, яка не тільки окреслює загальні тенденції у сфері інформаційного розвитку та його впливу на міжнародну безпеку, а й містить низку пропозицій, які було неоднозначно сприйнято світовою спільнотою. Так, своє ставлення до проблеми міжнародної інформаційної безпеки країна представила уперше у 2004 році [14]. У позиції країни, зокрема, зазначалося, що бурхливий розвиток інформатики та телекомунікацій є важливою особливістю науково-технічного прогресу. У сучасних умовах, коли суттєво зросли масштаби загроз для міжнародної безпеки, з'явилися нетрадиційні чинники безпеки, поширюється у глобальних масштабах міжнародний тероризм та злочинність, які активно використовують сучасні інформаційно-комунікаційні технології та мережі, забезпечення інформаційної безпеки перетворилося на першочергове завдання для міжнародної спільноти. Тому Китай висловив підтримку міжнародним зусиллям, спрямованим на забезпечення і зміцнення інформаційної безпеки всіх країн, та створення Групи урядових експертів ООН для обговорення і розгляду питань інформаційної безпеки.

У 2006 році Китай у своєму баченні підкреслив, що проблема інформаційної безпеки перетворилася на фундаментальний фактор, який впливає як на загальну безпеку держав світу, так й на систему глобальної безпеки та стабільності. Для вирішення цієї проблеми необхідна спільна відповідальність міжнародного співтовариства [15].

На думку КНР, проблема інформаційної безпеки – це не тільки ризики, обумовлені слабкістю базової інформаційної інфраструктури, але й політичні, економічні, військові, соціальні, культурні і багато інших проблем, які виникають в результаті несанкціонованого використання інформаційних технологій. Тому при розгляді проблеми інформаційної безпеки цим двом чинникам слід приділяти однакову увагу.

Як підкреслюється у позиції держави, інформаційні технології повинні використовуватися відповідно до цілей Статуту ООН та основних принципів міжнародних відносин. Так, безперешкодний потік інформації слід гарантувати з урахуванням необхідності забезпечення національного суверенітету і безпеки, а також поваги існуючих між країнами історичних, культурних і політичних відмінностей. Водночас, кожна країна має право на використання свого власного кіберпростору відповідно до свого внутрішнього законодавства та потреб інформаційного розвитку. У свою чергу, міжнародне співтовариство має активізувати свою співпрацю в проведенні досліджень щодо використання інформаційних технологій з огляду на те, що актуальною залишається проблема асиметрії інформаційного розвитку країн, а отже не всі можуть скористатися перевагами вільного поширення інформаційних технологій [15].

Як неодноразово підкреслювалося у позиції КНР, найбільш ефективним міжнародним форумом для обговорення проблеми інформаційної безпеки є ООН. І хоча Група урядових експертів з інформаційної безпеки не змогла домогтися в 2005 році істотних результатів, проте експерти різних країн провели широкий обмін думками і запропонували різноманітні варіанти рішень з цілого комплексу питань, що стосуються інформаційної безпеки, заклавши тим самим міцний фундамент для подальших обговорень міжнародною спільнотою зазначених проблем та пошуку шляхів їх вирішення. У зв'язку з цим Китай підтримав ідею відновлення роботи Групи урядових експертів у 2009 році для проведення детального та всеосяжного дослідження загроз і проблем у сфері інформаційної безпеки, а також для розробки відповідних програм і політики для їх нейтралізації. Китай же, як й раніше, буде і надалі підтримувати міжнародні зусилля, спрямовані на вирішення проблеми інформаційної безпеки, і брати участь в міжнародних ініціативах [15].

У 2007 році Китай в черговий раз представив свою позицію щодо проблеми міжнародної інформаційної безпеки. Так, у документі зазначалося, що питання інформаційної безпеки є вкрай актуальними для держави, тому Китай розробив і поступово реалізує власну національну стратегію у сфері інформаційної безпеки. Наприклад, було ухвалено низку законів та розроблено стандарти в галузі регулювання інформаційної безпеки, вжито заходів із розширення контролю за випадками порушень інформаційної безпеки, вдосконалено механізми координації і управління у сфері інформаційної безпеки, запроваджено дослідження з питань технологій забезпечення інформаційної безпеки і створення системи реагування на загрози безпеці національних інформаційних мереж, що суттєво поліпшило систему безпеки мережевої інфраструктури держави і базових інформаційних систем. Китай також бере активну участь у міжнародному співробітництві в галузі інформаційної безпеки, зокрема, в рамках Шанхайської організації співробітництва. Так за участі китайської держави в рамках організації було розроблено та ухвалено Заяву з питань міжнародної інформаційної безпеки, що передбачала створення Групи експертів держав-членів з міжнародної інформаційної безпеки [16; 17].

2008 року Китай знову виступив із власним баченням проблеми міжнародної інформаційної безпеки, розширивши свою позицію з цього питання. Так, з одного боку, держава визнала об'єктивні переваги, що надає масове впровадження інформаційно-комунікаційних технологій для соціально-економічного розвитку країн світу, а з другого, – висловила переконання, що подальший процес глобальної комп'ютеризації

обумовлює виникнення небезпеки неправомірного використання результатів цього процесу, що потенційно може завдати шкоди безпеці як окремих країн і регіонів, так й світу в цілому. Серед небезпек, що виникають внаслідок інформаційного розвитку, було визначено розробку і застосування інформаційної зброї, інформаційну злочинність, інформаційний тероризм, використання лідерських позицій у сфері інформатизації на шкоду інтересам і безпеці інших країн, а також поширення інформації, що руйнує політичні, економічні, соціальні системи і духовно-культурне середовище інших країн. Отже, як стверджує КНР, світова спільнота повинна зміцнити підходи до співпраці в цій галузі і вжити спільних заходів для вирішення окреслених проблем. У своїй позиції Китай також поінформував про позитивні зрушення у сфері формування національної системи інформаційної безпеки. Так, серед переваг було визначено удосконалення законодавчої бази, розробку положень і стандартів у сфері інформаційної безпеки, досягнення у сфері боротьби зі злочинним використанням інформаційних технологій та мереж, удосконалення механізмів інвестування у сектор інформаційної безпеки, створення системи оперативного реагування тощо [18].

**Висновки.** Як свідчить аналіз позиції провідних держав АТР щодо ухвалення резолюції ГА ООН «Досягнення науки і техніки та їх вплив на міжнародну безпеку», проблема інформаційної безпеки виступає суттєвим фактором їх поступального розвитку. Отже, вироблення міжнародних норм і принципів, які б відповідали сучасному стану системи міжнародного миру і безпеки, визначаються як життєво необхідні, оскільки дозволяють не тільки продовжувати використовувати науково-технологічне співробітництво для реалізації програм модернізації суспільства, збільшення темпів соціально-економічного розвитку, але й виробити правила поведінки держав задля ефективної протидії виникненню викликів та загроз у сфері інформаційної безпеки.

Водночас, позиції держав суттєво відрізняються, оскільки кожна з них містить унікальні характеристики національної інформаційної безпеки і відповідно – власне бачення пріоритетів міжнародного співробітництва в цій сфері. Так, якщо Японія переважно зорієнтована на збереження балансу між міжнародним технологічним трансфером та національними пріоритетами у сфері інформаційної безпеки, то Індія переважно зорієнтована на вирішення проблеми збереження існуючих механізмів науково-технологічного співробітництва як важливої передумови подальшого соціально-економічного розвитку. Китай же, як потенційний супротивник у сфері інформаційної безпеки для США та країн Заходу, виступає переважно на захист стратегічних ініціатив таких акторів, як Російська Федерація, намагаючись досягнути переваги у вирішенні питання розробки правил поведінки держав задля утворення ефективної системи міжнародної інформаційної безпеки.

#### **Список використаних джерел**

1. Current developments in science and technology and their potential impact on international security and disarmament efforts. Report of the Secretary-General [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/73/177>.
2. Scientific and technological developments and their imract on international security. Report of the Secretary-General. [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/45/568>.
3. Scientific and technological developments and their imract on international security. Resolution adopted by the General Assembly (A/45/60). [Електронний ресурс]. – Режим доступу: <https://undocs.org/en/A/RES/45/60>.
4. Report of the Disarmament Comission General Assembly Official Records: Forty-Sixth Session Supplement. No. 42. [Електронний ресурс]. – Режим доступу: <https://undocs.org/pdf?symbol=en/A/46/42>.

5. Role of science and technology in the context of international security and disarmament Resolution adopted by the General Assembly (A/53/73). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/RES/53/73>.
6. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly (A/53/70). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/RES/53/70>.
7. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/68/156/Add.1). [Електронний ресурс]. – Режим доступу: [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/156/Add.1&Lang=E](https://www.un.org/ga/search/view_doc.asp?symbol=A/68/156/Add.1&Lang=E).
8. Japan's National Security Strategy (December 17, 2013). [Електронний ресурс]. – Режим доступу: <https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf>.
9. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/71/172) [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/71/172>
10. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (72/315) [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/72/315>
11. Cybersecurity Strategy (September 4, 2015). Cabinet Decision. The Government of Japan [Електронний ресурс]. – Режим доступу: <https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>.
12. Current developments in science and technology and their potential impact on international security and disarmament efforts. Report of the Secretary-General (A/73/177). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/73/177>
13. Moody R. Which countries have the worst (and best) cybersecurity? / Rebecca Moody. [Електронний ресурс]. – Режим доступу: <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>
14. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/59/116). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/59/116>.
15. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/61/161). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/61/161>.
16. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/ 62/98). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/62/98>
17. SCO members sign statement on international information security (June 15, 2006) [Електронний ресурс]. – Режим доступу: [http://www.gov.cn/misc/2006-06/15/content\\_311225.htm](http://www.gov.cn/misc/2006-06/15/content_311225.htm)
18. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/63/139). [Електронний ресурс]. – Режим доступу: <https://undocs.org/A/63/139>.

## References

1. Current developments in science and technology and their potential impact on international security and disarmament efforts. Report of the Secretary-General Available at: <<https://undocs.org/A/73/177>>
2. Scientific and technological developments and their impact on international security. Report of the Secretary-General. Available at: <<https://undocs.org/A/45/568>>.
3. Scientific and technological developments and their impact on international security. Resolution adopted by the General Assembly (A/45/60). [Available at: <<https://undocs.org/en/A/RES/45/60>>.

4. Report of the Disarmament Commission General Assembly Official Records: Forty-Sixth Session Supplement. No. 42. Available at: <<https://undocs.org/pdf?symbol=en/A/46/42>>.
5. Role of science and technology in the context of international security and disarmament Resolution adopted by the General Assembly (A/53/73). Available at: <<https://undocs.org/A/RES/53/73>>.
6. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly (A/53/70). Available at: <<https://undocs.org/A/RES/53/70>>
7. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/68/156/Add.1). Available at: <[https://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/156/Add.1&Lang=E](https://www.un.org/ga/search/view_doc.asp?symbol=A/68/156/Add.1&Lang=E)>
8. Japan's National Security Strategy (December 17, 2013). Available at: <<https://www.cas.go.jp/jp/siryoku/131217anzenhoshou/nss-e.pdf>>
9. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/71/172) Available at: <<https://undocs.org/A/71/172>>
10. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (72/315) Available at: <<https://undocs.org/A/72/315>>
11. Cybersecurity Strategy (September 4, 2015). Cabinet Decision. The Government of Japan Available at: <<https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>>.
12. Current developments in science and technology and their potential impact on international security and disarmament efforts. Report of the Secretary-General (A/73/177). Available at: <<https://undocs.org/A/73/177>>
13. Moody R. Which countries have the worst (and best) cybersecurity? / Rebecca Moody. Available at: <<https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>>
14. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/59/116). Available at: <<https://undocs.org/A/59/116>>.
15. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/61/161). Available at: <<https://undocs.org/A/61/161>>.
16. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/ 62/98). Available at: <<https://undocs.org/A/62/98>>
17. SCO members sign statement on international information security (June 15, 2006) Available at: <[http://www.gov.cn/misc/2006-06/15/content\\_311225.htm](http://www.gov.cn/misc/2006-06/15/content_311225.htm)>
18. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A/63/139). Available at: <<https://undocs.org/A/63/139>>.