Кириченко І.О.*

СПІВРОБІТНИЦТВО ОРГАНІЗАЦІЇ АМЕРИКАНСЬКИХ ДЕРЖАВ ТА СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

The article views the problem of guaranteeing of information security within the framework of collaboration of Organization of American States and new president of the USA B.Obama; basic threats are selected in the field of information security. Was made a conclusion that the collaboration of regional organization of OAS lies in support of American strategy of creation of global culture of cybersecurity.

У сучасному світі нові тенденції міжнародного розвитку, вплив високих технологій на глобальну інтеграцію зумовлюють необхідність вирішення актуальних проблем життєдіяльності людства, узгодження нових міжнародних принципів взаємодії та правил поведінки акторів міжнародних відносин у сфері безпеки. Глобальною проблемою сучасності, до якої привернуто увагу авторитетних міжнародних організацій, політичних лідерів, науковців з питань геополітики та міжнародного правопорядку, світової громадськості, є проблема об'єктивного ускладнення структури міжнародних відносин і підтримання сталого миру, попередження конфліктів, уникнення нової гонки озброєнь з використанням новітніх науково-технологічних досягнень.

Проблеми глобальної безпеки визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світового порядку, навіть саме існування цивілізації. Глобальна безпека як чинник міжнародних відносин, вплив якого має універсальний характер і врахування якого в діяльності міжнародного співтовариства та в зовнішній політиці окремих держав призводить до радикальних змін у поведінці акторів міжнародних відносин, до трансформації самої сутності проблеми безпеки після закінчення «холодної війни» і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах міжнародної безпеки інформаційної складової.

У площині можливостей забезпечення глобальної безпеки постають міжнародні об'єднавчі процеси, глобальне поширення принципів демократії, вдосконалення норм економічної кооперації, інтегральне усвідомлення світовою спільнотою відповідальності за прогресивний розвиток світу. Міжнародне співтовариство визнало факт існування глобальної проблеми міжнародної інформаційної безпеки, у системі якої ключове значення має фундаментальна проблема обмеження військового застосування досягнень науки й техніки.

До нових міжнародних реалій безпеки відносять якісно нове бачення архітектури міжнародної безпеки під впливом подвійного використання інформаційно-комунікаційних технологій, маніпулювання, викривлення інформаційної реальності, деструктивне використання соціальних комунікацій, невизначеність правового поля інформаційної безпеки, інформаційний тероризм. Невизначеність регулятивних механізмів політики міжнародної інформаційної безпеки зумовлює потребу розвитку різноманітних норм галузевого права, що регулюють інформаційні

* аспірантка відділу трансатлантичних досліджень Інституту світової економіки і міжнародних відносин НАН України

Науковий керівник: проф. Макаренко Є.А.

правовідносини у всіх без винятку сферах життєдіяльності суспільства, тому до правотворчого процесу з проблематики міжнародної інформаційної безпеки інтенсивно залучені інституції ООН, міжнародні субрегіональні та регіональні організації, фахівці-міжнародники.

З огляду на реалії сучасної геополітики політичні еліти, демократичні інститути і міжнародна спільнота постали перед наслідками поглиблення і розширення глобалізаційних процесів та необхідністю перегляду концептуальних і практичних підходів до забезпечення міжнародної безпеки з урахуванням впливу інформаційного чинника на світову систему. Відтак, стратегії міжнародного співробітництва у сфері інформаційної безпеки впливають на формування нової системи підтримання міжнародного миру і сталого розвитку, на доктрини безпеки та оборони акторів міжнародних відносин, на функціонування механізмів протидії інформаційним загрозам.

Важливість і значущість дослідження проблеми міжнародного співробітництва у сфері інформаційної безпеки зумовлює підвищений інтерес до неї з боку багатьох вітчизняних й зарубіжних науковців-політологів, дослідження яких присвячено аналізу безпекових концепцій в умовах глобалізації міжнародної політичної системи. Особливий внесок в осмислення інформаційної безпеки як політичної категорії належить таким відомим науковцям, як І.Валлерстайн, Б.Дженкінс, Р.Кеохейн, М.Лібікі, Дж.Най, Г.Шіллер, А.Крутських, О.Леонов, В.Лісічкін, І.Панарін, С.Расторгуєв, О.Гребініченко, А.Гуцал, В.Ліпкан, О.Литвиненко, Є.Макаренко, М.Ожеван, Г.Почепцова, О.Соснін та ін.

Проблеми інформаційної безпеки входять до компетенції регіональної міжнародної організації – Організації Американських Держав (ОАД), в рамках якої активно просувається ініціатива США щодо створення глобальної культури кібербезпеки, ведеться робота з питань протидії тероризмові, в тому числі інформаційному. Генеральна Асамблея ОАД у 2003 році прийняла резолюцію «Розробка міжамериканської стратегії щодо боротьби із загрозами для кібербезпеки» [1]. Рекомендації щодо проекту стратегії було розроблено Міжамериканською комісією з питань зв'язку, Міжамериканським комітетом боротьби з тероризмом, Нарадою міністрів юстиції і міністрів або генеральних прокурорів Північної і Південної Америки та її Групою урядових експертів з проблеми кіберзлочинності.

Внаслідок прийняття резолюції в Буенос-Айресі (28-29 липня 2003 р.) була проведена Конференція ОАД з питань кібербезпеки, яка визнала, що серйозність інформаційних загроз критичним інформаційним системам, структурам, і, загалом, економіці країн у всьому світі потребує активної координації діяльності державного і приватного секторів, тобто фактично – впровадження основного принципу культури кібербезпеки. На Спеціальній конференції з питань безпеки в Мехіко (28-29 жовтня 2003 р.) держави-члени ОАД заявили про свій намір прийняти і виконувати стратегію кібербезпеки, яка повинна бути спрямована на прийняття необхідних заходів щодо попередження і реагування на кібератаки незалежно від їх джерела, боротьбу з кіберзагрозами і кіберзлочинністю, криміналізації атак у кіберпросторі, захисту критично важливих інфраструктур і мережевих систем.

Підсумком цієї діяльності було прийняття ГА ОАД в червні 2004 року Багатосторонньої міжамериканської стратегії щодо боротьби із загрозами кібербезпеки: багатоаспектний і міждисциплінарний підхід до створення культури кібербезпеки [2], яка передбачає імплементацію принципів культури кібербезпеки, аналогічних викладеним у резолюції ГА ООН 57/239 «Про створення глобальної культури кібербезпеки», створення Міжамериканської мережі груп реагування на надзвичайні ситуації в комп'ютерній галузі, визначення і прийняття єдиних стандартів у цій галузі, модернізацію нормативно-правової бази щодо боротьби з кіберзлочинністю. У документі державам-членам ОАД рекомендується оцінити доцільність застосування принципів Європейської Конвенції про кіберзлочинність і розглянути можливість приєднання до цієї угоди. Слід підкреслити, що США, які активно ви-

ступають із закликом до всіх країн приєднатися до цієї Конвенції як модельного інструменту у боротьбі з кіберзлочинами, на практиці її не ратифікували, і, отже, не пов'язані жодними зобов'язаннями, що передбачаються документом.

Сучасна стратегія інформаційної безпеки ОАД пов'язана з концепціями інформаційного протиборства нового президента Б.Обами та новими пріоритетними напрямами у сфері міжнародної безпеки. Саме у форматі «інформаційної парадигми» політичний лідер Америки намагається позиціонувати риси, характерні як для ліберально-демократичної, так і консервативно-республіканської ідеології. Інформаційні переваги держави, на думку аналітиків адміністрації Б.Обами, спроможні зберегти елементи досягнутої у попередній докризовий період стабільності та забезпечити посткризовий розвиток, зробити більш прогнозованим перебіг соціальних конфліктів та надати конструктивного характеру розв'язанню подібних конфліктів, уберегти суспільство від само руйнації [3]. Відповідно, нова стратегія інформаційної безпеки США позначена виразними поворотом до мілітаризації, яка означає більш тісну координацією під егідою військових (Білого Дому та Пентагону) політики у сфері «кібербезпеки», а також військових й невійськових аспектів психологічних й інформаційних операцій.

Як зазначають зарубіжні і вітчизняні фахівці з питань інформаційної безпеки, з огляду на світову кризу, у зовнішній політиці Б.Обами набуває декларативного змісту традиційно притаманна Демократичній партії США ідеологема «просування демократії й захисту прав людини» [4]. Це, зокрема, означає, що в інтересах боротьби з кризовими явищами у світовій економіці та політиці Б.Обама та керівник американської дипломатії Г.Клінтон готові будуть піти на певні політичні компроміси з керівниками Росії й Китаю аж до мовчазної згоди на закріплення за цими та іншим потужними державними утвореннями «сфер відповідальності» за підтримання регіональної безпеки й стабільності [4].

Б.Обама ще під час останньої президентської виборчої кампанії критикував Дж.Буша-молодшого за неувагу до питань захисту «чутливої» інформації у комп'ютерних мережах, а «кібератаки» (хакерські атаки) на національні інформаційні мережі прирівнював до нападів на США із використанням атомної та бактеріологічної зброї. Не меншого значення проблемам інформаційної безпеки США відводив інший кандидат на пост президента США, – Дж.Маккейн, який підкреслював, що інформаційні операції перетворилися на головний метод ведення сучасної війни.

Уже як президент США Б.Обама підтримав й розвинув ідею Дж.Буша-молодшого, проголошену 8 січня 2008 р. під назвою «Комплексна національна ініціатива з кібербезпеки» [5] і доручив координацію «ініціативи з кібербезпеки» Департаменту внутрішньої безпеки, де існує відповідна Служба швидкого реагування на комп'ютерні інциденти, а Службі кібербезпеки Білого Дому, якій у лютому 2009 р. було відведено два місяці для підготовки Федерального плану налагодження моніторингу кібератак (умовна назва «Ейнштейн») вартістю 6 млрд. доларів США. Варто зазначити, що у перспективі до 2013 року, державні витрати США на забезпечення «високотехнологічної безпеки» зростуть на 44% – від 7,4 млрд. доларів у 2008 фінансовому році до 10,7 млрд. – у 2009 фінансовому році. Програму кібербезпеки запропоновано для реалізації компаніям Lockheed Martin, Boeing, Raytheon, Symantec і Mcafee, які надають необхідні ресурси для розгортання діяльності у відносно новому для себе напрямі забезпечення кібербезпеки. Так, компанія Boeing ще в серпні 2008 року створила спеціальний кібернетичний підрозділ не лише для внутрішніх потреб, але й для виконання зовнішніх контрактів [4].

У стратегічному плані з кібербезпеки Буша-Обами йдеться ймовірно не лише про заходи превентивно-оборонного характеру, але й про наступальну «інформаційну зброю» (перехоплення повідомлень на лінях зв'язку включно з Інтернетом, руйнування чужих інформаційних систем, зовнішні інформаційно-психологічні

впливи), оскільки план є конфіденційним, а у відкриту пресу потрапляють лише його фрагменти. Принциповою новизною ініціативи кібербезпеки можна вважати таку мілітаризацію питань інформаційної безпеки, яка означає залучення до програми обороноздатності держави Національної агенції безпеки, по суті військової структури за своїм характером. До січня 2008 року питання інформаційної безпеки у США розглядалися як суто технічні завдання для цивільних фахівців, а упродовж останніх 20-ти років вони були віднесені до компетенції Національного інституту стандартів та технологій.

Ідейні підходи нового президента США щодо «інформаційних озброєнь» істотно зближує позиції Америки й Росії, яка з 1998 року постійно ставить в Першому комітеті Генеральної Асамблеї ООН (займається проблемами нерозповсюдження зброї масового ураження) питання щодо «інформаційної зброї» як зброї масового ураження, наражаючись на вето США та їх союзників, які відмовлялися визнавати реальність існування «інформаційних озброєнь».

На думку нового директора Національної розвідки США адмірала Д.Блера, головними суб'єктами атак на американські інформаційні системи є Росія й Китай, на другому місці – структури організованої злочинності, метою яких є виведення інформаційних систем з ладу або істотне уповільнення їх роботи, щоб створити перешкоди для правоохоронних органів США. У відповідь на подібні кібератаки американці мають намір зменшити число порталів, які сполучають урядові сервери з Інтернетом – від 4 500 до 2 500. Тенденція до скорочення «точок доступу» до федеральної урядової інформаційної мережі в інтересах інформаційної безпеки не є чимось принципово новим, оскільки така політика проводилася протягом останніх двох років і також має свої негативи, тобто звужує можливості електронного урядування.

Поширення зброї масового ураження, прагнення екстремістських та терористичних груп одержати до неї доступ, революція у військовій справі, заснована на високих інформаційних технологіях, висока уразливість сучасних суспільств до медіа-впливів у своїй сукупності та у поєднанні з викликами тотальної цивілізаційної кризи вимагають від держави, щоб вона повною мірою скористалась монополією на застосування «інформаційних озброєнь», що враховано у новій стратегії інформаційної безпеки США.

Водночас, враховуючи різновекторність інформаційних загроз, Пентагон збирається істотно збільшити витрати на «психологічні операції» та «зв'язки з громадськістю» з метою просування національних інтересів США у міжнародному співтоваристві. За підрахунками Associated Press, подібні витрати за останні п'ять років зросли на 63% й досягли у 2009 р. 4, 7 млрд. доларів США (1% від військового бюджету). З них 489 млн. доларів США заплановано на «психологічні операції» поза межами держави. Йдеться про психологічну обробку світової спільноти з дотриманням вимог конфіденційності «цільових зарубіжних аудиторій». Дослідники проблем кібербезпеки наголошують, що штат військових пропагандистів уже майже зрівнявся з аналогічним штатом фахівців з публічної дипломатії у Державному департаменті (27 000 проти 30 000). У лютому 2009 р. військове командування США встановило для збройних сил новий польовий статут (field manual) із проведення інформаційних операцій, де вказується на умови їх ефективного поєднання зі звичайними (традиційними) видами озброєнь [4].

30 жовтня 2003 р. тодішній міністр оборони Д.Рамсфелд підписав секретний план «Дорожня карта інформаційних операцій» [6], у якому містилося положення про те, що «інформація, призначена для зарубіжної аудиторії, повинна спочатку апробуватися на внутрішній аудиторії», що скандал у пресі, оскільки у США від 1948 р. американському урядові законом забороняється здійснювати психологічний вплив на масову свідомість американської держави. В результаті Офіс стратегічних впливів, створений Д.Рамсфелдом для реалізації зазначеної «дорожньої карти», за наполяганням Конгресу було ліквідовано, а за новою стратегією кібербе-

зпеки адміністрація Б.Обами висловилася за фактичне відновлення цього підрозділу Пентагону під назвою Офісу стратегічних комунікацій, який поєднуватиме функціональні завдання підтримання «зв'язків з громадськістю» й проведення інформаційних та психологічних операцій [4]. Відтак, радники Б.Обами рекомендують президентові об'єднати зусилля держав-членів ОАД для створення ефективної регіональної системи протиборства з інформаційними загрозами і, зокрема, з інформаційним тероризмом.

Таким чином, позиція регіональної організації ОАД щодо співробітництва в сфері інформаційної безпеки полягає у підтримці американської стратегії створення глобальної культури кібербезпеки і спрямована на практичні заходи, що стосуються попередження і реагування на кібератаки незалежно від їхніх джерел, боротьбу з кіберзагрозами і кіберзлочинністю, захист критично важливих інфраструктур і мережевих систем.

Список використаних джерел

1. Development of an Inter-American strategy to combat threats to Cybersecurity (Resolution adopted at the fourth plenary session, held on June 10, 2003) [Electronic resource]. – Access mode: http://www.oas.org/juridico/english/ga03/agres_1939.htm.
2. Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity (2004) [Electronic resource]. – Access mode: http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.
3. Jose K. Obama Adds «Cyber Security» to National Defense Plan [Electronic resource] / Katharine Jose. – Access mode: http://www.observer.com/2008/politics/obama-adds-cyber-security-national-defense-plan
4. Інформаційна безпека: контрманіпулятивні стратегії. Навчальний посібник / [Макаренко Є.А., Рижков М.М. та ін.]. – К.: Центр вільної преси, 2009. – 286 с.
5. Rollins J. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations CRS. Report Prepared for Members and Committees of Congress (March 10, 2009) [Electronic resource] / J.Rollins, A.C.Henning. – Access mode:http://www.boozallen.com/media/file/Cybersecurity_in_Federal_Government.pdf.
6. The Information Operations Roadmap [Electronic resource]. – Access mode: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_01_06_psyops.pdf.