

УДК 930:341.17ШОС:004.056](094)

DOI 10.24919/2519-058x.4.111226

Ольга ГАПЕЄВА,

orcid.org/0000-0002-3145-7025

*кандидат історичних наук, старший науковий співробітник,
докторант Національної академії сухопутних військ
імені гетьмана Петра Сагайдачного,
(Україна, Львів) o.gapeewa@gmail.com*

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА – КЛЮЧОВИЙ НАПРЯМ ДІЯЛЬНОСТІ ШАНХАЙСЬКОЇ ОРГАНІЗАЦІЇ СПІВРОБІТНИЦТВА: 2006 – 2017 рр.

У статті розглянуто основні напрями діяльності ШОС щодо забезпечення міжнародної інформаційної безпеки в історичній ретроспективі, досліджено діяльність та законодавчі ініціативи Російської Федерації як учасниці ШОС з питання, що вивчається.

Встановлено, що концептуальні документи з інформаційної безпеки, які поширюються на міжнародному рівні від імені ШОС, відповідають національним інтересам Російської Федерації та містять окремі положення російських доктринальних документів з інформаційної безпеки.

Ключові слова: *інформаційна безпека, інформаційний простір, міжнародна інформаційна безпека, Шанхайська організація співробітництва.*

Лім. 26.

Olha HAPERYEVA,

*PhD (History), Senior researcher, doctoral student,
National Army Academy named after Hetman Petro Sahaidachny,
(Ukraine, Lviv) o.gapeewa@gmail.com*

INTERNATIONAL INFORMATION SECURITY AS AN IMPORTANT DIRECTION OF THE SHANGHAI COOPERATION ORGANIZATION ACTIVITIES: 2006 – 2017

The article deals with researches of the Shanghai Cooperation Organization (SCO) activities in the area of international information security and analysis of the legislative initiatives of the Russian Federation as a member country of the SCO in the historical retrospective.

The resource base of the article is the official documents posted on the Shanghai Cooperation Organization web site (<https://rus.sectsc.org/>), the Ministry of Foreign Affairs of the Russian Federation (<https://www.mid.ru>) and other web sites of member countries of organization.

The article is based on the problematic-chronological principle.

It was determined that the cooperation of the SCO's member countries in the area of information security de facto began on June 16, 2009 by signing the Yekaterinburg Declaration of cooperation in information security providing. According to paragraph 7 of this document, the relevance of international information security providing is identified as an important element of the overall international security system.

The Russian Federation's initiatives in the area of international information security were continued in Yekaterinburg (September 2011). The Russian experts presented a draft concept of the IIB Collaboration Convention as an alternative to the 2001 Budapest Council of Europe Convention concerning cybercrime.

On September 12, 2011 United Nations Permanent Representatives of Russia, China, Tajikistan and Uzbekistan sent a joint letter to UN Secretary General with a request to extend the draft «Rules of Conduct in the Field of International Information Security» adopted at the Shanghai Cooperation Organization Summit in Astana on June 2011 as an official document of the United Nations General Assembly. The main task of the Rules» was to develop a code of responsible behavior of countries in the international information security, taking into account military-political, criminal and terrorist challenges and threats.

However, due to discrepancies in terms of terminology and models of international information security between the Russian Federation and Western countries, the document was not adopted until present. One of the document provisions is the prohibition – «to use ICT and information and communication networks for interference in the internal affairs of other countries with purpose to undermine their political, economic and social stability».

The author concludes that Russia plays a dominant role in the field of international information security within the framework of the SCO, which promotes the name of this regional organization of legislative initiatives related to its national interests. The development of draft international legal documents concerning international information security is carried out by powerful research organizations and institutions of the Russian Federation and, on some issues, duplicates Russian doctrinal documents.

In further research, the author is going to consider the historical process of creating national information security systems in the countries of the Central Asian region - the republics of the former USSR – and to analyze the content of information campaigns conducted by the Russian Federation in these countries.

Key words: *information security, information space, international information security, Shanghai Cooperation Organization.*

Ref. 26.

Ольга ГАПЕЕВА,

*кандидат исторических наук, старший научный сотрудник,
докторант Национальной академии сухопутных войск
имени гетмана Петра Сагайдачного,
(Украина, Львов) o.gapeewa@gmail.com*

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – КЛЮЧЕВОЕ НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА: 2006 – 2017 гг.

В статье рассмотрены основные направления деятельности ШОС по обеспечению международной информационной безопасности в исторической ретроспективе, исследованы деятельность и законодательные инициативы Российской Федерации как участницы ШОС по изучаемому вопросу.

Установлено, что концептуальные документы по информационной безопасности, которые распространяются на международном уровне от имени ШОС, отвечают национальным интересам Российской Федерации и содержат отдельные положения российских доктринальных документов по информационной безопасности.

Ключевые слова: *информационная безопасность, информационное пространство, международная информационная безопасность, Шанхайская организация сотрудничества.*

Лит. 26.

Постановка проблеми. Після розпаду СРСР та ліквідації структур, діяльність яких була спрямована на захист інформації, забезпечення інформаційної безпеки на пострадянському просторі набуло актуальності й стало одним з ключових напрямів діяльності регіональних міжнародних організацій: Співдружності Незалежних Держав (далі – СНД), Шанхайської організації співробітництва (далі – ШОС), Союзної держави Росії та Білорусі і військово-політичної міжнародної організації – Організації Договору про колективну безпеку (далі – ОДКБ). Так, у військовій галузі співпраці держав-учасниць СНД було прийнято найбільшу кількість нормативно-правових документів, пов'язаних із забезпеченням інформаційної безпеки та міждержавним інформаційним обміном. Об'єктивно це пояснюється існуванням перехідної структури – Об'єднаних збройних сил СНД, на яку покладались завдання збереження єдиної системи управління військами та реформування Збройних Сил колишнього СРСР. Проте розробка й прийняття інших законодавчих актів щодо формування спільного інформаційного простору держав-учасниць Співдружності здійснювались зі значним запізненням, а їхній зміст не завжди відповідав геополітичним реаліям. Також поза сферою нормативно-правового врегулювання залишились питання проведення інформаційно-психологічних операцій та інформаційних кампаній [4; 5].

Одним із напрямів діяльності ОДКБ є захист спільного інформаційного простору, удосконалення й уніфікація законодавства держав-членів у галузі інформаційної безпеки, організація спільної протидії загрозам в інформаційній сфері. З цієї метою було створено низку інформаційно-аналітичних структур із залученням зацікавлених міністерств, відомств, організацій, наукових установ. Одним з перспективних напрямів діяльності ОДКБ є навчання фахівців відповідних спеціальностей (журналістів, фахівців з міжнародних відносин та економічних спеціальностей)

з основ планування, ведення інформаційно-психологічних операцій та протидії їм. Окремо слід вказати на підготовку фахівців із захисту інформації у цивільних вишах та підготовку військових фахівців. Цікавим також є досвід проведення спільних операцій постійної дії у інтернет-сегментах держав-учасниць Договору та у спільному інформаційному просторі на зразок операції «ПРОКСІ», що проводилася у Киргизстані навесні 2010 р. Зауважимо, що рішенням Ради колективної безпеки ОДКБ від 23 грудня 2014 р. був створений Консультаційний координаційний центр ОДКБ з питань реагування на комп'ютерні інциденти, а 10 квітня 2015 р. відбулося перше засідання Ради Консультаційного координаційного центру (ККЦ) ОДКБ, на якому Головою Ради було обрано представника Російської Федерації (далі – РФ). [6].

Інформаційна політика та інформаційна безпека є основними складовими діяльності Союзної держави Росії та Білорусі. Для цих країн надзвичайно важливим є об'єднання спільних зусиль та взаємодія у сфері захисту інформаційного простору і протидії деструктивним впливам.

Враховуючи, що чотири республіки колишнього СРСР: Республіка Казахстан, Республіка Таджикистан, Киргизька Республіка та Республіка Узбекистан є державами-членами Шанхайської організації співробітництва (далі – ШОС), *метою статті* є дослідження в історичній ретроспективі діяльності цієї впливової регіональної організації у галузі забезпечення міжнародної інформаційної безпеки та аналіз законодавчих ініціатив Російської Федерації як держави-члена ШОС з питання, що досліджується.

Аналіз останніх досліджень і публікацій. У наших попередніх наукових студіях було визначено основні напрями діяльності ОДКБ і СНГ щодо становлення системи керівних органів в галузі інформаційної безпеки; проаналізовано зміст основних нормативно-правових документів та порядок їх розробки й затвердження, з'ясовано основні заходи щодо забезпечення інформаційної безпеки та їх результативність, узагальнено досвід підготовки фахівців [4; 5; 6]. Окреме дослідження присвячено історіографічному аналізу проблематики інформаційної безпеки на пострадянському просторі [7].

Діяльність ШОС у сфері забезпечення інформаційної безпеки є предметом наукових розвідок зарубіжних та українських вчених. Зокрема, велику увагу дослідженню цієї проблематики приділяють фахівці Національного дослідницького інституту світової економіки та міжнародних відносин імені Є.М. Примакова НАН РФ, Російського інституту стратегічних досліджень, ППР-центру (провідної неурядової організації, що спеціалізується на дослідженні проблем забезпечення міжнародної інформаційної безпеки), Інституту проблем інформаційної безпеки Московського державного університету ім. М.В. Ломоносова, а також політологи: Н. Ромашкіна, О. Демидов, О. Федоров, О. Бедрицький, А. Крутських, А. Стрельцов. Зауважимо, що попри ґрунтовний аналіз проблематики міжнародної інформаційної безпеки та пошуку шляхів взаєморозуміння у цій сфері між РФ та США, роботи російських дослідників мають виражений пропагандистський характер: автори наголошують на «миротворчих» ініціативах РФ у цьому напрямку, акцентують увагу на внесок російських експертів у розробку низки законодавчих документів [9]. Серед українських науковців діяльність ШОС досліджували: Є. Дьякова, О. Грицун, Є. Макаренко [8; 12; 17].

Основою джерельної бази цієї студії є офіційні документи, розміщені на інтернет-порталі Шанхайської організації співробітництва (<https://rus.sectso.org/>), Міністерства закордонних справ Російської Федерації (<https://www.mid.ru>), аналітичні огляди, виступи та інтерв'ю провідних фахівців у сфері інформаційної безпеки.

Виклад основного матеріалу. Перш ніж розпочати висвітлення основних напрямів діяльності Шанхайської організації співробітництва з питання, що досліджується, зауважимо, що на міжнародному рівні дотепер відсутній єдиний понятійний апарат з інформаційної безпеки. Не зазнали успіху й спроби держав-учасниць ОДКБ розробити термінологію з цього питання та уніфікувати нормативно-правову базу. Щоправда, у 2014 р. було презентовано Словник-довідник з інформаційної безпеки для парламентської асамблеї ОДКБ, виданий у Санкт-Петербурзі, проте суттєвих зрушень у цьому напрямку не відбулось [9].

Слід також додати, що РФ – держава-учасник більшості інтеграційних утворень на пострадянському просторі – тривалий час є ініціатором обговорення тріади питань щодо безпеки інформаційного простору: запобігання милітаризації інформаційної сфери, протидія екстремізму й теро-

ризму, кримінальні злочини із застосуванням можливостей сучасних інформаційно-комунікаційних технологій. Відповідно, більшість документів з інформаційної безпеки, що «просуваються» від імені ШОС та інших регіональних організацій, містять положення, які відповідають поглядам РФ у цій сфері та її національним інтересам.

ШОС, створена у 2001 р. у м. Шанхаї, з червня 2017 р. об'єднує 8 країн: Республіку Казахстан, Китайську народну республіку, Російську Федерацію, Киргизьку Республіку, Республіку Узбекистан, Республіку Таджикистан, Ісламську Республіку Пакистан та Республіку Індія. Існують угоди про партнерство ШОС з ООН, СНД, ОДКБ. Серед республік колишнього СРСР, які є учасниками інших інтеграційних утворень, Республіка Білорусь з 2015 р. має статус держави-спостерігача у ШОС.

Чому саме ШОС стала своєрідним «рупором» РФ у напрямі забезпечення міжнародної інформаційної безпеки (далі – МІБ)? Низка законодавчих ініціатив РФ у цій сфері, запропонованих на розгляд Генеральної Асамблеї ООН протягом 1998 – 2004 рр., не отримала підтримки; виникли розбіжності між поглядами російських фахівців та фахівців зі США і Великобританії (т. зв. «три моделі інформаційної безпеки») [2]; Саме тому РФ була змушена «...перенести акценти на регіональний рівень» [2, 122].

Щодо іншої міжнародної організації – ОДКБ – створення власної системи інформаційної безпеки у її рамках розпочалось у листопаді 2006 р., а відповідна Програма спільних дій, прийнята Рішенням Ради колективної безпеки ОДКБ, була затверджена лише у 2008 р. [6].

Розглянемо діяльність ШОС щодо забезпечення міжнародної інформаційної безпеки за проблемно-хронологічним принципом. Так, 16 серпня 2007 р. у м. Бішкек відбулося чергове засідання голів держав-членів організації, за підсумками якого було опубліковано Спільне комюніке: лідери шістьох країн підписали Бішкекську декларацію і затвердили «План дій держав-членів ШОС щодо забезпечення міжнародної інформаційної безпеки», підготовлений з ініціативи РФ, у якому зафіксовано наміри сторін протистояти викликам і загрозам в інформаційній сфері з врахуванням спільних поглядів на проблему [24].

У жовтні 2007 р. у Пекіні відбулося засідання Групи експертів держав-членів ШОС з проблем міжнародної інформаційної безпеки, де було ухвалено рішення про офіційне утворення групи й узгодження засад її діяльності. Головою групи було обрано представника РФ як держави, що ініціювала розгляд питань міжнародної інформаційної безпеки у рамках ШОС. Групі було доручено відпрацювати План дій та визначити шляхи й засоби розв'язання проблематики забезпечення МІБ у рамках ШОС [18].

Співпраця держав-учасниць ШОС у галузі інформаційної безпеки *de facto* розпочалась 16 червня 2009 р. з моменту підписання Єкатеринбурзької декларації про співпрацю у забезпеченні інформаційної безпеки. Відповідно до пункту 7 цього документа, актуальність забезпечення міжнародної інформаційної безпеки визначена ключовим елементом загальної системи міжнародної безпеки [13]. Наступним кроком у цьому напрямі стало підписання Угоди між урядами держав-членів ШОС щодо співробітництва у галузі забезпечення міжнародної інформаційної безпеки, яка вступила у дію лише 5 червня 2012 р. [25].

Зокрема, у п. 1 Угоди визначено загрози у галузі забезпечення міжнародної інформаційної безпеки; основні напрями, форми й механізми співробітництва та засади захисту інформації. Цікавими для нашого дослідження є зміст додатків до Угоди. У додатку 1 запропоновано Перелік основних понять у галузі забезпечення МІБ: «інформаційна безпека», «міжнародна інформаційна безпека»; «інформаційна війна», «інформаційні ресурси», «інформаційна зброя», «неправомірне використання інформаційних ресурсів», тощо. Як зауважує О. Демидов, ці поняття «... використовуються майже в тій формі, в якій вони існують у національному законодавстві РФ» [9, 137].

У додатку 2 міститься Перелік основних загроз у сфері забезпечення міжнародної інформаційної безпеки, їхніх витоків та ознак, а саме:

- розробка та застосування інформаційної зброї, підготовка і ведення інформаційної війни;
- інформаційний тероризм;
- інформаційна злочинність;

- використання домінуючого положення в інформаційному просторі на шкоду інтересам і безпеці інших держав;
- поширення інформації, яка завдає шкоду суспільно-політичній та соціально-економічній системі, духовній, моральній і культурній середовищі інших держав;
- загрози безпечного, стабільного функціонування глобальних і національних інформаційних інфраструктур, що мають природний і (або) техногенний характер [25]. Угоду ратифікували чотири держави-члени ШОС: РФ, КНР, Казахстан і Таджикистан.

Після підписання Угоди Голови держав-членів ШОС виступили зі спільною Заявою з міжнародної інформаційної безпеки [14]. Зокрема, у документі висловлювалася стурбованість використанням ІКТ у злочинних, терористичних та військово-політичних цілях, несумісних із забезпеченням міжнародної безпеки. Голови держав заявили про спільні погляди на проблеми, пов'язані з міжнародною інформаційною безпекою, та про намір об'єднати зусилля в рамках ШОС з метою протистояння цим загрозам. Тобто, «...коли на рівні ООН процес просування ідеї забезпечення інформаційної безпеки почав заходити у глухий кут, країни ШОС заклали основу регіонального співробітництва у цій сфері» [2, 123].

Слід заважити, що ініціативи РФ у сфері забезпечення МІБ було продовжено у Єкатеринбурзі (вересень 2011 р.), коли на Другій зустрічі високих представників ШОС російськими експертами було презентовано проект концепції Конвенції про забезпечення МІБ, відпрацьований за участі Ради безпеки РФ, Інституту проблем інформаційної безпеки МДУ ім. М. В. Ломоносова та низки федеральних органів РФ, як своєрідну альтернативу Будапештській конвенції Ради Європи 2001 р. щодо боротьби із кіберзлочинністю [16].

У проекті Конвенції запропоновано варіант 20 основних термінів з інформаційної безпеки, визначено перелік загроз в інформаційному просторі, принципи забезпечення МІБ, заходи щодо запобігання та врегулювання воєнних конфліктів у інформаційному просторі, а також низка питань правничого характеру щодо ратифікації і денонсації Конвенції. Зауважимо, що РФ очікувала підписання проекту цього документа ще у 2012 р., проте його (документа) положення суттєво відрізнялись від положень Стратегії операцій у кіберпросторі Міністерства оборони США (The 2011 U.S. Department of Defense Strategy for Operating in Cyberspace), яка дозволяє активно протидіяти кіберопераціям та застосовувати кіберзброю у відповідь.

Під час обговорення Конвенції деякі експерти зауважили, що більшість запропонованих термінів були запозичені з Доктрини інформаційної безпеки РФ у редакції 2000 р. та втратили актуальність. Крім цього, запропонована термінологія потребувала доопрацювання, зокрема, з урахуванням сучасного стану кібершпіонажу та ігноруванням інтересів всіх учасників інформаційного обміну [21].

12 вересня 2011 р. Постійні представники Росії, Китаю, Таджикистану і Узбекистану при ООН направили спільний лист Генеральному Секретареві ООН Пан Гі Муну з проханням поширити проект «Правил поведінки в галузі забезпечення міжнародної інформаційної безпеки», прийнятий на саміті Шанхайської організації співробітництва в Астані у червні 2011 р., як офіційний документ Генеральної Асамблеї ООН. Головним завданням «Правил» стало вироблення кодексу відповідальної поведінки держав у сфері міжнародної інформаційної безпеки з урахуванням військово-політичних, кримінальних і терористичних викликів і загроз. Документ передбачає «... протидію використанню інформаційних і телекомунікаційних технологій в цілях, не сумісних з завданнями забезпечення міжнародної стабільності, миру і безпеки, дотримання прав і свобод людини в інформаційному просторі, повагу суверенітету, територіальної цілісності та політичної незалежності усіх держав, а також створення багатостороннього прозорого і демократичного міжнародного механізму регулювання мережі Інтернет» [22]. РФ закликала всі зацікавлені сторони брати активну участь у дискусіях з цього питання. «Ми переконані, що ця ініціатива стане першим кроком на шляху до вироблення універсального документа ООН, який буде націлений на комплексне забезпечення міжнародної інформаційної безпеки, максимально враховуючи інтереси світової спільноти» [22].

Проте просування від імені ШОС «Правил» знову виявилось невдалим. У вересні 2014 р. за підсумками чергового саміту ШОС, було підписано Душанбінську декларацію Голів держав-чле-

нів ШОС. Так, п. 5. Декларації зобов'язує держави-члени ШОС активізувати зусилля щодо створення «...мирного, безпечного, справедливого і відкритого інформаційного простору, ґрунтуючись на принципах поваги державного суверенітету і невтручання у внутрішні справи інших країн» [11].

З цієї метою в січні 2015 р. було запропоновано нову редакцію «Правил» від імені держав-членів ШОС як офіційний документ ООН. Голови держав-членів ШОС закликали до розробки відповідного міжнародно-правового документа центральної координуючої ролі ООН; підтвердили зобов'язання не застосовувати інформаційно-комунікаційні технології з метою порушення міжнародного миру і безпеки, а також для втручання у внутрішні справи інших держав і підризу їхньої політичної, економічної і соціальної стабільності; утримуватися від застосування сили або загрози силою у ході розв'язання міжнародних спорів, що виникають у цифровій сфері [19].

У червні 2015 р. за підсумками засідання Групи урядових експертів (ГУЕ) ООН з міжнародної інформаційної безпеки було визнано, що до сфери використання інформаційно-комунікаційних технологій застосовується міжнародне право, однак у разі необхідності воно може бути доповнене, у тому числі за рахунок прийняття нових норм. Прийнята більшістю доповідь була спрямована генсеку ООН для подання на майбутній 70-ї сесії Генасамблеї організації [20].

«...Особливістю ініціативи ШОС є її миротворчий характер. Якщо концепції західних держав передбачають регулювання кібервійн, цей документ передбачає запобігання конфліктам в інформаційній сфері», – інформує МЗС РФ [19].

Цікавого є й зміна підходів російських представників – т.зв. «тактика» малих кроків». Оскільки досягти домовленості у розв'язання глобальних питань не вдалося, йдеться про пошук порозуміння «малими кроками». Зокрема, про підписання угод про безпеку банківської сфери та об'єктів критичної інфраструктури [10].

В Астанинській Декларації глав держав – членів Шанхайської організації співробітництва, прийнятій 9 червня 2017 р., голови держав-членів ШОС висловили підтримку виробленню у рамках ООН універсального кодексу правил, принципів і норм відповідальної поведінки держав в інформаційному просторі і розглядають нову редакцію «Правил поведінки в галузі забезпечення міжнародної інформаційної безпеки», поширену в січні 2015 р. від імені держав – членів ШОС, як офіційний документ ООН, важливий крок у цьому напрямі [1].

У контексті вищевикладеного виникає питання: якої оцінки заслуговують «миротворчі» заходи РФ в Естонії (2007), Грузії (2008), кібертаки на сайти державних органів влади й управління України, втручання у виборчі процеси західних держав? РФ, як ініціатор і розробник міжнародних правових документів з питань інформаційної безпеки, сама грубо порушує закладені в них принципи і норми поведінки.

Слід зауважити, що ініціатива РФ, поширена від імені ШОС у 2016 – 2017 рр. щодо вироблення у рамках роботи Групи урядових експертів ООН доповіді, основою якої мали стати вищевказані «Правила» та пропозиції щодо прийняття ГА ООН резолюції та яка мала закріпити ці правила, була заблокована західними країнами у червні 2017 р. [3].

Проте у 2017 р. було підписано Стратегію розвитку ШОС до 2025 р. Зокрема, держави-члени, спираючись на міждержавну Угоду про співробітництво в галузі забезпечення міжнародної інформаційної безпеки від 2009 р. та інші документи, підтвердили наміри щодо співробітництва у сфері контролю за інформаційним простором, удосконалення механізму співробітництва у боротьбі проти використання ІКТ у терористичних цілях і протидії кіберзагрозам. Держави-члени ШОС висловили готовність продовжити роботу з прийняття ООН «Правил поведінки в галузі забезпечення міжнародної інформаційної безпеки», формування єдиного міжнародного регулювання сфери ІКТ, розвивати співробітництво на цьому напрямі, підвищенні кваліфікації профільних спеціалістів [26]. Так, у червні 2017 р. відбулася Перша Міжнародна конференція з інформаційної безпеки в рамках ІХ міжнародного ІТ-Форуму у Ханті-Мансійську, за участю країн ШОС і БРИКС, до якої приєдналися і країни ОДКБ. За результатами роботи конференції прийнято пропозицію: сформувати Югорський міжнародний експертний клуб з інформаційної безпеки, як «площадку для роботи з зарубіжними ЗМІ, починаючи з постійних звинувачень на адресу РФ у хакерських атаках» [15].

Як зауважив спеціальний представник президента РФ Андрій Крутських: «Не всі держави поділяють наш миротворчий підхід... проте Росія має намір продовжувати процес перемовин. У найближчій перспективі міжнародні норми поведінки завдяки зусиллям учасників ОДКБ, БРИКС та ШОС почнуть отримувати конкретні риси» [23].

Висновки. Домінуючу роль у сфері забезпечення міжнародної інформаційної безпеки у ШОС відіграє РФ, яка просуває він імені цієї регіональної організації законодавчі ініціативи, пов'язані з її національними інтересами, які за окремими позиціями дублюють російські доктринальні документи. Розробка документів міжнародно-правового характеру, поданих від ШОС, здійснюється потужними науково-дослідними організаціями й установами РФ.

У наших подальших дослідженнях ми плануємо розглянути процес формування національних систем інформаційної безпеки у державах Центрально-Азійського регіону – республіках колишнього СРСР та проаналізувати зміст інформаційних кампаній, що проводяться РФ у цих державах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Астанинская декларация глав государств-членов Шанхайской организации сотрудничества. – [Электронный ресурс]. – Режим доступа: <http://kremlin.ru/supplement/5206>.
2. Бедрицкий А. В. Международные договоренности по киберпространству: возможен ли консенсус / А. В. Бедрицкий // Проблемы национальной стратегии. – 2012. – № 4(13). – С. 119–136.
3. Выступление заместителя Секретаря Совета Безопасности Российской Федерации О. В. Храмова на Саммите по вопросам кибербезопасности (28 июня 2017 г., г. Тель-Авив, Государство Израиль). – [Электронный ресурс]. – Режим доступа: <http://www.scrf.gov.ru/news/allnews/2242/>
4. Гапеева О. Л. Інформаційна безпека на пострадянському просторі: системно-історичний аналіз / О. Л. Гапеева // Грані. Науково-теоретичний альманах. – №140 (2016). – С. 93–99.
5. Гапеева О. Л. Діяльність ОДКБ у сфері інформаційної безпеки: історична ретроспектива / О. Л. Гапеева // Військово-історичний меридіан: електронне видання. – № 14 (2016). – [Електронний ресурс]. – Режим доступа: http://vim.gov.ua/images/sbor/vim_14_2016-135-145.pdf
6. Гапеева О. Л. Інформаційна політика СНД та ОДКБ: історико-правовий аспект / О. Л. Гапеев // Гілея. – № 117. – С. 90–93.
7. Гапеева О. Л. Історіографічний аналіз проблематики інформаційної безпеки на пострадянському просторі / О. Гапеева // Historical and Cultural Studies. – 2016. – Vol. 3. – С. 37–41.
8. Грицун О. Регулювання питань міжнародної інформаційної безпеки в межах міжнародних організацій / О. Грицун. – [Електронний ресурс]. – Режим доступа: <http://aw.journalsofznu.zp.ua/archive/visnik-4-2014-1/24.pdf>
9. Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы / О. Демидов. – [Электронный ресурс]. – Режим доступа: <http://mail.pircenter.org/media/content/files/10/13559089230.pdf>
10. Демидов О. Игра про правила / О. Демидов, Е. Черненко // Россия в глобальной политике. – 2015. – № 4. – [Электронный ресурс]. – Режим доступа: <http://www.globalaffairs.ru/number/igra-pro-pravila-17640>
11. Душанбинская декларация глав государств – членов Шанхайской организации сотрудничества. – [Электронный ресурс]. – Режим доступа: <http://kremlin.ru/supplement/4750>.
12. Дьякова Є. Україна та Шанхайська організація співробітництва, перспективи співпраці / Є. Дьякова. – [Електронний ресурс]. – Режим доступа: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?...2...
13. Екатеринбургская декларация Глав государств-членов Шанхайской организации сотрудничества. – [Электронный ресурс]. – Режим доступа: http://repository.un.org/bitstream/handle/11176/171971/a_63_924-ru.pdf?sequence=5&isallowed=y.
14. Заявление глав государств-членов ШОС по международной информационной безопасности. – [Электронный ресурс]. – Режим доступа: <http://infoshos.ru/ru/?id=94/>
15. Инфофорум-Югра. [Электронный ресурс]. – Режим доступа: <https://infoforum.ru/conference/conference/view/id/36>
16. Конвенция об обеспечении международной информационной безопасности (концепция). – [Электронный ресурс]. – Режим доступа: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/crtickb6bz29/content/id/191666
17. Макаренко Є. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст / Є. Макаренко // Актуальні проблеми міжнародних відносин. – 2011. – випуск 102 (частина I). – С. 51–62.

18. О заседании в Пекине группы экспертов государств-членов ШОС по международной информационной безопасности. – [Электронный ресурс]. – Режим доступа: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/uscutiw2po53/content/id/389112
19. Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности». – [Электронный ресурс]. – Режим доступа: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/uscutiw2po53/content/id/916241.
20. Об итогах заключительного заседания Группы правительственных экспертов ООН по международной информационной безопасности. – [Электронный ресурс]. – Режим доступа: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1525144
21. Понятие свободы не абсолютно. – [Электронный ресурс]. – Режим доступа: <https://www.gazeta.ru/business/2012/02/09/3994965.shtml>.
22. Правила поведения в области обеспечения международной информационной безопасности. – [Электронный ресурс]. – Режим доступа: <https://rus.rusemb.org.uk/policycontact/6>.
23. СМИ: РФ предложит ООН принять правила поведения в киберпространстве. – [Электронный ресурс]. – <https://hitech.vesti.ru/article/674623/>
24. Совместное коммюнике по итогам заседания Совета глав государств-участников ШОС от 18 августа 2007 г. – [Электронный ресурс]. – Режим доступа: <http://www.fmprc.gov.cn/rus/wjdt/gb/t353700.shtml>
25. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. – [Электронный ресурс]. – Режим доступа: <https://ccdcoe.org/sites/default/files/documents/sco-090616-isagreementrussian.pdf>
26. Стратегия развития Шанхайской организации сотрудничества до 2025 года – [Электронный ресурс]. – Режим доступа: <http://infoshos.ru/ru/?id=125>

REFERENCES

1. Astaninskaya deklaraciya glav gosudarstv-chlenov SHanhajskoj organizacii sotrudnichestva. – [Elektronnij resurs]. – Rezhim dostupu: <http://kremlin.ru/supplement/5206>.
2. Bedrickij A.V. Mezhdunarodnye dogovorenosti po kiberprostranstvu: vozmozhen li konsensus / A.V. Bedric'kij // Problemy nacional'noj strategii. – 2012. – № 4(13). – S. 119–136.
3. Vystuplenie zamestitelya Sekretarya Soveta Bezopasnosti Rossijskoj Federacii O. V. Hramova na Sammite po voprosam kiberbezopasnosti (28 iyunya 2017 g., g.Tel'-Aviv, Gosudarstvo Izrail'). – [Elektronnij resurs]. – Rezhim dostupu: <http://www.scrf.gov.ru/news/allnews/2242/>
4. Gapeeva O. L. Informacijna bezpeka na postradyans'komu prostori: sistemno-istorichnij analiz / O. L. Gapeeva // Grani. Naukovo-teoretichnij al'manah. – №140 (2016). – S. 93–99.
5. Gapeeva O. L. Diyal'nist' ODKB u sferi informacijnoi bezpeki: istorichna retrospektiva / O. L. Gapeeva // Vijs'kovo-istorichnij meridian: elektronne vidannya. – № 14 (2016). – [Elektronnij resurs]. – Rezhim dostupu: http://vim.gov.ua/images/sbor/vim_14_2016-135-145.pdf
6. Gapeeva O. L. Informacijna politika SND ta ODKB: istoriko-pravovij aspekt / O. L. Gapee // Gileya. – № 117. – С. 90–93.
7. Gapeeva O. L. Istoriografichnij analiz problematiki informacijnoi bezpeki na postradyans'komu prostori / O. Gapeeva // Historical and Cultural Studies. – 2016. – Vol. 3. – S. 37–41.
8. Gricun O. Regulyuvannya pitan' mizhnarodnoi informacijnoi bezpeki v mezhah mizhnarodnih organizacij / O. Gricun. – [Elektronnij resurs]. – Rezhim dostupu: <http://aw.journalsofznu.zp.ua/archive/visnik-4-2014-1/24.pdf>
9. Demidov O. Obespechenie mezhdunarodnoj informacionnoj bezopasnosti i rossijskie nacional'nye interesy / O. Demidov. – [Elektronnij resurs]. – Rezhim dostupu: <http://mail.pircenter.org/media/content/files/10/13559089230.pdf>
10. Demidov O. Igra pro pravila / O. Demidov, E. CHernenko // Rossiya v global'noj politike. – 2015. – № 4. – [Elektronnij resurs]. – Rezhim dostupu: <http://www.globalaffairs.ru/number/igra-pro-pravila-17640>
11. Dushanbinskaya deklaraciya glav gosudarstv – chlenov SHanhajskoj organizacii sotrudnichestva. – [Elektronnij resurs]. – Rezhim dostupu: <http://kremlin.ru/supplement/4750>.
12. D'yakova E. Ukraïna ta SHanhajs'ka organizaciya spivrobotnictva, perspektivi spivpraci / E. D'yakova. – [Elektronnij resurs]. – Rezhim dostupu: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?...2...
13. Ekaterinburgskaya deklaraciya Glav gosudarstv-chlenov SHanhajskoj organizacii sotrudnichestva. – [Elektronnij resurs]. – Rezhim dostupu: http://repository.un.org/bitstream/handle/11176/171971/a_63_924-ru.pdf?sequence=5&isallowed=y.
14. Zayavlenie glav gosudarstv-chlenov SHOS po mezhdunarodnoj informacionnoj bezopasnosti. – [Elektronnij resurs]. – Rezhim dostupu: <http://infoshos.ru/ru/?id=94/>

15. Infoforum-YUgra. – [Elektronnij resurs]. – Rezhim dostupu: <https://infoforum.ru/conference/conference/view/id/36>
16. Konvenciya ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (konceptiya). – [Elektronnij resurs]. – Rezhim dostupu: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/cptickb6bz29/content/id/191666
17. Makarenko Є. Mizhnarodne spivrobitnictvo u sferi informacijnoї bezpeki: regional'nij kontekst/ Є. Makarenko // Aktual'ni problemi mizhnarodnih vidnosin. – 2011. – vipusk 102 (chastina I). – S. 51–62.
18. O zasedanii v Pekine grupy ehkspertov gosudarstv-chlenov SHOS po mezhdunarodnoj informacionnoj bezopasnosti. – [Elektronnij resurs]. – Rezhim dostupu: http://www.mid.ru/mezhdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/uscutiw2po53/content/id/389112
19. Ob iniciative stran-chlenov SHOS «Pravila povedeniya v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti». – [Elektronnij resurs]. – Rezhim dostupu: http://www.mid.ru/mezhdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/uscutiw2po53/content/id/916241.
20. Ob itogah zaklyuchitel'nogo zasedaniya Gruppy pravitel'stvennyh ehkspertov OON po mezhdunarodnoj informacionnoj bezopasnosti. – [Elektronnij resurs]. – Rezhim dostupu: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1525144
21. Ponyatie svobody ne absolyutno. – [Elektronnij resurs]. – Rezhim dostupu: <https://www.gazeta.ru/business/2012/02/09/3994965.shtml>.
22. Pravila povedeniya v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti. – [Elektronnij resurs]. – Rezhim dostupu: <https://rus.rusemb.org.uk/policycontact/6>.
23. SMI: RF predlozhit OON prinyat' pravila povedeniya v kiberprostranstve. – [Elektronnij resurs]. – <https://hitech.vesti.ru/article/674623/>
24. Sovmestnoe kommyunike po itogam zasedaniya Soveta glav gosudarstv-uchastnikov SHOS ot 18 avgusta 2007 g. – [Elektronnij resurs]. – Rezhim dostupu: <http://www.fmprc.gov.cn/rus/wjdt/gb/t353700.shtml>
25. Soglashenie mezhdru pravitel'stvami gosudarstv-chlenov SHanhajskoj organizacii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti. – [Elektronnij resurs]. – Rezhim dostupu: <https://ccdcoe.org/sites/default/files/documents/sco-090616-iisagreementrussian.pdf>
26. Strategiya razvitiya SHanhajskoj organizacii sotrudnichestva do 2025 goda – [Elektronnij resurs]. – Rezhim dostupu: <http://infoshos.ru/ru/?id=125>

Стаття надійшла до редакції 21.09.2017 р.