УДК 321.01

РОЛЬ І МІСЦЕ РФ У ГЛОБАЛЬНОМУ ГЕОПОЛІТИЧНОМУ КІБЕРСУПЕРНИЦТВІ

Дубов Дмитро Володимирович,
кандидат політичних наук, старший науковий співробітник

З'ясовано роль і місце РФ у глобальному суперництві геополітичних гравців, дана оцінка пріоритетів Росії у сфері міжнародної інформаційної безпеки. Зазначено, що РФ побудувала «інформаційно закриту» модель суспільства та продовжує агресивні дії в кіберпросторі. Зроблено висновок, що зусилля Росії щодо впорядкування на міжнародному рівні питань «міжнародної інформаційної безпеки» мають на меті легітимацію власної рестриктивної політики.

Ключові слова: **Російська Федерація, кіберпростір, кіберпотенціал, суперництво, США, міжнародна інформаційна безпека.**

Агресія РФ проти України в межах «гібридної війни», розв'язаної на сході України, а також фактична спроба Росії за рахунок цього протистояння демонтувати чинну міжнародну систему безпеки, зумовлює зростання уваги до всіх елементів безпекової політики РФ з боку інших гравців. Не є винятком і політика Росії щодо національного та міжнародного кіберпростору, вона намагається використати його у власних інтересах, формуючи при цьому інформаційно-закриту модель суспільства і намагаючись нав'язати таку ж модель усьому світу.

При цьому, незважаючи на очевидне неприйняття на термінологічному рівні Росією поняття «кіберпростір» чи «кібербезпека» (замінюючи його більш традиційними «інформаційний простір», «інформаційна безпека» та «міжнародна інформаційна безпека»), вона все більшу увагу починає приділяти саме цьому технічному складнику.

Зважаючи на те, що політичні амбіції російського керівництва виходять за межі регіональних протиборств і зростають до глобальних геополітичних протистоянь, цікавим і важливим є визначення тієї ролі, яку Росія відіграє саме в глобальному геполітичному суперництві, яке нині сформоване навколо двох найбільших гравців – США та КНР.

Мета даної статті – з'ясувати роль та місце РФ у глобальному суперництві геополітичних гравців та оцінити пріоритети Росії у сфері міжнародної інформаційної безпеки.

Росія та її військовий потенціал завжди були у фокусі уваги значної кількості дослідників-безпекознавців. Кіберскладник цього потенціалу вивчали як західні фахівці Г. Раттрей [5], К. Байлон [3], В. Ешмор [9], Дж. Катон [8], так і російські дослідники та експерти - О. Демидов [7], О. Черненко [33], А. Лукацький [16], А. Куликова [17].

В Україні ж російські можливості використання кіберпростору залишаються, зазвичай, поза межами кібербезпекових досліджень.

Поточний стан військово-політичної ситуації у світі, пов'язаний із агресією Росії проти України та загальним міжнародним загостренням відносин на цьому тлі, безумовно, актуалізує і питання політики Ф щодо кібербезпекової теми.

Однак слід зазначити, що, на нашу думку, навіть незважаючи на глобальну занепокоєність діями РФ та її спробами тотально демонтувати систему міжнародної безпеки, у глобальному геополітичному сенсі це не вивело Росію в число реальних геополітичних гравців. Показово, що навіть після подій в Україні, наприклад, американська військова думка майже не відреагувала[1] на цю ситуацію та не збільшила кількості рефлексій ситуації, що склалась.

Сам факт того, що РФ розпочала збройну агресію з використанням методів середини XX ст., її виключення з боку міжнародних гравців із низки світових економічних процесів (введення санкцій), свідчить про те, що Росія настільки слабо інтегрована до глобальної системи міжнародних відносин, що її виключення з цієї системи хоч і створює певні складнощі, однак не є критичним. Малоймовірно, що аналогічні дії можливі стосовно інших геополітичних гравців (передусім США та КНР). Відповідно, РФ, незважаючи на своє бажання відігравати істотнішу роль на міжнародній арені, все ще залишається другорядним гравцем, який лише створює тло для реального стратегічного суперництва інших учасників міжнародного процесу. Майже аналогічною є ситуація й з роллю Росії у глобальному кібербезпековому суперництві – вона залишається гравцем «другого ешелону», дедалі частіше виступаючи сателітом Китаю, однак не його повноцінним партнером. Це

[1]Відповідну тенденцію засвідчує моніторинг автором дослідження профільних американських журналів та наукових баз за травень 2014 – лютий 2015 рр.

спричинює і поступове збільшення ступеня залежності РФ від КНР в економічному сенсі.

У своїй політиці щодо майбутнього кіберпростору РФ, так само як і КНР, робить істотний акцент не стільки на технічний, скільки на контентний складник. Формуючи, вочевидь, закриту інформаційну систему у своїй країні, російське керівництво намагається встановити пріоритетний контроль за внутрішніми інформаційними потоками. В тих аспектах власної політики у сфері інформаційної безпеки, де потрібні лише дії уряду для вирішення тих чи інших завдань (посилення відповідальності за публікації в мережі Інтернет, глобальний моніторинг національного сегменту Мережі, можливість відключати сайти, що знаходяться в російському сегменті Інтернету тощо) РФ досягла досить істотних результатів.

Розбудова сучасної російської інформаційної моделі та її кіберспроможності

Власне, чинну російську інформаційну модель було побудовано завдяки зусиллям В. Суркова (високопосадовця Адміністрації Президента РФ з 1999 по 2011 рр.), якому, на думку експертів [30], «завдячує» своїм існуванням той російський інформаційний простір, який ми можемо спостерігати останні 10 років із тотальною пропагандою, знищенням опозиційних видань, контрольованою опозицією та підтримкою (як проплаченою, так і щирою) будь яких дій влади з боку населення.

Після часткового усунення у 2011 р. В. Суркова від питань інформаційної політики російські ініціативи у сфері «захисту інформаційного простору» стали більш жорсткими та прямолінійними. Починаючи з 2012 р. можна однозначно говорити про перехід від м'яких (непрямих) методів контролю за інформпростором до значно жорсткіших (прямих). І левова частка з них була спрямована на посилення контролю держави за мережею Інтернет.

Лише у 2013–2014 рр. було проголошено принаймні декілька ініціатив, які сприяють сегментуванню глобальної Мережі та збільшенню контрольованості російського сегменту російською владою. Наприклад, це створення «національного інтернету» – ця ідея з'являється все частіше, починаючи від заяви сенатора Ради Федерації М. Кавджарадзе про створення «Чебурашки» і до ідеї «більш патріотичного інтернету», озвученої вже у 2015 р. в офіційній заяві Російського військово-історичного товариства [26]. Сюди ж можна додати діяльність з обмеження розповсюдження в Мережі певних видів контенту (передусім – опозиційного характеру чи такого, що не вписується до панівної пропагандистської державної парадигми) державною структурою «Роскомнадзор», впровадження обмежень на анонімний доступ до публічних точок Wi-Fi, випадки переслідування людей за розповсюдження в Інтернеті ідей, які дисонують із панівною ідеологічною концепцією РФ (наприклад щодо анексії Криму чи агресії РФ проти України) [32].

Тобто тренд до побудови масштабного інформаційного (а разом із ним і цифрового) муру є більш ніж однозначним.

Однак якщо в сенсі «закриття» власного інформаційного простору від викликів панівній політичній системі та її очільникам з боку опозиційного контенту зусилля російської влади більш-менш очевидні, то кіберскладник залишається все ще не завжди структурованим.

Водночас не можна сказати, що РФ ставиться до питань кібербезпеки неуважно. До останнього часу загрозами в цій сфері опікувалися переважно Міністерство внутрішніх справ РФ (Управління «К»), Федеральна служба безпеки РФ (Центр інформаційної безпеки), а також у межах окремих завдань – Федеральна служба охорони та Міністерство інформації РФ. Однак, як зазначають російські експерти [7], все ще спостерігається величезний розрив між США та Росією у можливостях здійснювати кібератаки, а відтак – і в їх кіберпотенціалах. Хоча, на думку тих самих експертів, цей розрив поступово зменшується.

У 2014 р. на тлі посилення західних санкцій проти РФ за агресію щодо України в РФ було проведено одразу декілька заходів, що можна назвати «кібернавчаннями». Один блок був присвячений сценарію можливості відключення РФ від глобальної Мережі. З цією метою в липні 2014 р. на базі Міністерства зв'язку та масових комунікацій було проведено навчання за участі Міністерства оборони, Федеральної служби безпеки, Федеральної служби охорони, Міністерства внутрішніх справ, ОАО «Ростелеком», Координаційного центру національного домену мережі «Інтернет», Технічного центру «Інтернет» (*MSK–IX*) [25].

Крім того, були заявлені плани і про військові кібернавчання в межах комплексних навчань Колективних сил оперативного реагування ОДКБ «Взаємодія–2014» [14]. На них планувалося відпрацювати питання забезпечення кібернетичної безпеки власних інформаційних систем, а також технічної взаємодії при реагуванні на дії інформаційних систем супротивників ОДКБ. Відомості про результати таких навчань відсутні.

Також у 2014 р. було заявлено про створення у структурі Міністерства оборони РФ військ інформаційних операцій [21]. Їх основне завдання – захист російських воєнних систем управління та зв'язку від кібертероризму та надійне закриття інформації, що в них циркулює, від імовірного супротивника. Передбачається, що до складу цих військ увійдуть частини у військових округах і на флотах, які забезпечені висококваліфікованими спеціалістами: математиками, програмістами, інженерами, криптографами,

зв'язківцями, офіцерами радіоелектронного протиборства, перекладачами та іншими.

Слід зазначити, що ще всередині 2013 р. були створені т. зв. наукові роти у складі ЗС РФ. Їх формальне завдання – виконання конкретних науково-прикладних задач відповідно до наказів та в інтересах органів воєнного управління [28]. Завдання цим військовослужбовцям ставляться, виходячи з потреб і профілю військових частин, на базі яких вони знаходяться, та підприємств ВПК [27]. Однак принаймні частина таких рот уже працює за напрямом «нові інформаційні технології», причому, як наголосив очільник Міноборони РФ С. Шойгу, міністерство розпочинає велику програму пошуку програмістів, оскільки «обсяги програмного продукту, який нам необхідний у найближчі 5 років, ми переведемо в конкретні, осяжні обсяги та цифри» [27]. Фактично ж, наукові роти мають стати основною науково-технічною базою для військ інформаційних операцій.

Занепокоєність РФ кібербезпековим складником зрозуміла. Виступаючи 7 квітня 2014 р. перед співробітниками ФСБ, В. Путін зазначив, що істотний акцент має бути зроблено на захисті інформаційної інфраструктури, оскільки лише у 2013 р. було попереджено більш ніж 9 млн спрямованих впливів на сайти та інформаційні системи російських органів державної влади [13].

У 2013 р. указом президента РФ [36] ФСБ було поставлено завдання створити державну систему виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси Росії.

За даними окремих російських фахівців, завдяки цій системі вже було виявлено три кібер-агентурні мережі, що дало змогу попередити крадіжку 2 млн сторінок секретної інформації [35]. Так само РФ опікується проблемою виявлення та знешкодження «закладок» у програмних і технічних складниках інформаційних технологій, що використовуються державою.

Незважаючи на увагу російської держави до зазначеної теми, на рівні стратегічних документів питання кібербезпеки все ще залишається неузгодженим і принципово не вирішеним. Ще в січні 2014 р. для публічного обговорення був запропонований проект концепції Стратегії кібербезпеки Російської Федерації [24], однак до її прийняття справа так і не дійшла[2]. Фактично і нині в цьому сенсі РФ користується прийнятою ще в 2000 р. Доктриною інформаційної безпеки РФ [19], де в розділі «Види загроз інформаційній безпеці Російській Федерації» прописано блоки проблем, що традиційно відносяться до кібербезпекових (блок питань, що винесено в підпункт «Загрози безпеці інформаційних і телекомунікаційних засобів та систем, як уже розгорнутих, так і створюваних на території Росії»).

[2] Станом на лютий 2015 р.

Ставлення країн Заходу до потенційних російських кіберзагроз

Загалом РФ залишається досить впливовим гравцем у світовому кіберпросторі, на що західні посадовці та експерти регулярно звертають увагу. Однак слід зазначити, що в західних країнах не існує чіткого та зрозумілого відношення до кіберзагроз, що виходять саме з Росії. На противагу ситуації з КНР, яка майже в усіх документах та звітах ідентифікується як потужний самостійний гравець у кіберпросторі, потенціал РФ оцінюється неоднозначно.

Переважно небезпека Росії в кіберпросторі визнається виходячи з двох факторів. По-перше, це досвід двох відомих кіберпротистоянь – в Естонії 2007 р. та у Грузії 2008 р.. З точку зору реальної небезпеки (особливо для об'єктів критичної інфраструктури) частково небезпечною була лише атака на Естонію. Здебільшого це були класичні DDoS-атаки, які не можуть спричинити реальної загрози інформаційним системам. По-друге, це висока активність російських хакерів саме як кіберзлочинців, що ставлять за мету особисте збагачення. Виходячи переважно з цього, західні експерти [4] вказують, що кіберзагрози з боку Росії можуть бути досить істотними. Крім того, часто Росія називається однією з 5 країн (поряд із США, Китаєм, Великою Британією та Францією), яка володіє найвищим потенціалом кібермогутності та кіберспроможності у світі.

Двозначним є відношення США до потенційної російської кіберзагрози. З одного боку, майже всі кібербезпекові документи (особливо, матеріали слухань, дослідження чи позиційні документи силових відомств) містять згадування про події в Естонії та Грузії, зазначаючи роль Росії в них, тим самим вказуючи на кіберпротенціал РФ. Однак на рівні офіційних документів (передусім стратегічного характеру) США не розглядають Росію як потужне джерело кібернебезпек. Принаймні такого рівня, що це заслуговувало б на спеціальну увагу при формування механізмів кіберстримування. Наприклад, в оновленій Стратегії національної безпеки США від 6-го лютого 2015 р. [11], незважаючи на широке висвітлення кібербезпекової тематики (включно з окремим пунктом щодо кібербезпеки), Росія (на відміну від КНР) не згадується як потенційна кіберзагроза для США.

У червні 2013 р. міністр оборони США Ч. Хейгел у ґрунтовному виступі з питань стратегічних викликів безпеці США та її стратегічних інтересів у цій царині фактично не згадував про кіберзагрози з боку Росії безпеці США, зазначаючи при цьому, що є об'єктивна необхідність посилити увагу до нових викликів у сфері інформаційних технологій в Азійсько-Тихоокеанському регіоні [2]. Часткове пояснення такої позиції США можна побачити у заявах очільників розвідувальних відомств. Так, наприкінці 2013 р. голова Національної розвідки Дж. Клеппер зазна-

чив, що хоча США і визнають Китай і Росію «просунутими кібератакорами», однак не очікують з їх боку будь-яких «руйнівних» атак [10].

Однак на рівні прогнозних документів, а тим більше досить регулярних парламентських і комітетських слухань з кібербезпекової тематики у США, Росія постійно фігурує як одна із загроз кібербезпеці Сполучених Штатів.

При цьому в межах окремих слухань чи дослідницьких матеріалів вказується на те, що російські агресивні зусилля в кіберпросторі мають певний результат і впливають на американську систему кібербезпеки вже зараз. Зокрема, у звіті [6] про слухання в Комітеті з розвідки (*U.S. House permanent select committee on intelligence*) вказується, що троянські віруси, ідентифіковані як російські, дали змогу хакерам отримати доступ до систем управління деяких об'єктів критичної інфраструктури США, а самі віруси вповні могли бути використані для відключення життєво важливої інфраструктури, пов'язаної з нафтою та газом, електромережами чи водопостачанням.

В інтерв'ю у лютому 2014 р., присвяченому сучасним технологіям та кібербезпеці, президент США Б. Обама зазначив, що вважає Китай і Росію одними із загроз кібербезпеці США, а потенціал цих країн у даній сфері він розглядає як досить потужний [12].

Незважаючи все це, навіть у тих випадках, коли США активно визнають Росію як помітного гравця у світовому кіберпросторі, це визнання тісно пов'язане з КНР. Досить показово, що і Міністерство оборони США розглядає російську кібербезпекову тему не окремо, а виключно в контексті китайської. Зокрема в межах таких документів, як *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*. У звіті за 2014 р. кібербезпековий складник китайської міці та зусиль КНР щодо глобального кіберпростору розглядається саме разом із Росією. Серед іншого вказується, що Китай підтримує ініціативи Росії зі встановлення більшого контролю урядів за кіберпростором.

Слід визнати, що такий підхід американських аналітиків багато в чому виправданий, особливо із сьогоднішніх позицій. Зокрема, більшість зовнішньополітичних ініціатив РФ не реалізується без участі КНР, при цьому очевидно, що більшою мірою саме від КНР залежить, наскільки успішно (та чи взагалі буде) розвиватися та чи інша ініціатива. Такий рівень двосторонньої співпраці планується закріпити через підписання китайсько-російської угоди щодо співробітництва у сфері міжнародної інформаційної безпеки [33]. Предметом угоди має стати посилення заходів довіри та попередження перетворення кіберінцидентів у повномасштабний конфлікт, співробітництво у сфері забезпечення національних сегментів Інтернету й посилення взаємодії двох країн на міжнародних майданчиках з даної тематики.

Цей договір має стати і своєрідною відповіддю на заморожування відносин між РФ і США та стрімкою переорієнтацією Росії на східний вектор співробітництва. Фактично ж ця угода замінить (неформально) підписані в 2013 р. угоди між США та РФ з того ж питання, які були фактично призупинені в 2014 р. після агресії Росії проти України.

Заходи РФ щодо розбудови власної кібермогутності

Зважаючи на істотний рівень закритості інформації безпекового характеру в РФ (в т.ч. – у сфері кібербезпеки), оцінити реальні можливості РФ здійснювати масштабні заходи в кіберпросторі досить складно. Однак, судячи з окремих публічних дискусій, РФ дійсно зацікавлена у розбудові власної кібермогутності, а відтак – у спроможності використовувати кіберпростір у своїх інтересах (в т.ч. – військових). Зокрема, це можна побачити з широкої публічної дискусії в РФ із проблеми утвердження «цифрового суверенітету» держави в сучасному світі. Причому як взірець власника такого суверенітету обрано КНР.

Загалом обговорення триває, вочевидь, відштовхуючись від ідей «інформаційного суверенітету» І. Ашманова [20], який вважає необхідним зосередити увагу на налагодженні власного виробництва як технологічного, так і контентного (програмного) складника кіберпростору. Однак зусилля в цьому напрямі все ще розфокусовані та нескоординовані, а результати – неоднозначні.

Наприклад, малоймовірно, що нині РФ дійсно готова для розробки повноцінної власної операційної системи, хоча такі завдання і ставляться. Кращі результати РФ спостерігаються у сфері побудови власних мікропроцесорів (у квітні 2014 р. було заявлено про готовність запустити у серію виробництво мікропроцесорів «Ельбрус-4» компанії МЦСТ), однак це швидше епізодичні здобутки. Особливо яскраво це проявляється на фоні розробок різноманітних національних «планшетів», «телефонів» тощо. Після презентацій подібних продуктів часто ставало очевидним, що «національними» вони можуть вважатися досить умовно – вони або вироблені в інших країнах (оскільки РФ не має необхідних ресурсів), або використовують традиційні програмні платформи, що робить їх звичайними «не національними» продуктами.

Низка роздумів як експертів, так і політиків з приводу «цифрового суверенітету в Росії» дає змогу зробити висновок, що ними не враховується (або не акцентується увага) об'єктивна різниця у показниках розвитку двох суспільств (РФ та КНР), різних ціннісних характеристиках. Наприклад, розвинутий «цифровий» (кібернетичний) складник майже неможливий без істотних вкладень у науку, дослідження та інновації. Однак у 2014 р. ці показники розділилися наступним чином: США залишаються недосяж-

ним лідером – більше 465 млрд дол. [1], тоді як ЄС загалом – 351 млрд, КНР – 284, Російська Федерація – 40 млрд. Тобто РФ відстає від КНР щонайменше у 6 разів. До цього ж можна додати очевидну неефективність чинної економічної моделі РФ (її залежність від цін на енергоносії), а також неможливість «імпортувати» східноазійський тип відносин між державою та громадянами, що багато в чому є запорукою успішності реалізації Китаєм власної політики в інформаційному та кіберпросторі.

Слід зазначити, що ідея якнайшвидшого встановлення «цифрового суверенітету» переважно дискутується наближеними до владних структур експертами, або чиновниками та політиками. І ця дискусія багато в чому є тенденційною та не підкріпленою реальними можливостями країни. Як слушно зауважує знаний російський експерт з інформаційної безпеки А. Лукатський, запропоновані підходи до побудови «цифрового суверенітету» є малоперспективними, а подекуди і шкідливими для держави, оскільки більшою мірою є демагогічними, ніж реальними [16]. Остання думка підтверджується й тими заходами фіктивного «імпортозаміщення» у сфері ІТ, які відбувалися в РФ протягом 2014 р. Наприклад, за даними журналістів, в Міноборони РФ це набуло вигляду класичного «потьомкінського села»: логотипи іноземних торгових марок на службових телефонах закрили наліпками «Воєнтелекому» на вимогу міністра С. Шойгу [34].

На нашу думку, Російська Федерація стає заручницею власного малоперспективного підходу до проблеми – вона намагається реалізувати концепцію «цифрового суверенітету» через переліки об'єктів (продуктів) імпортозаміщення, а не через створення механізмів. А саме останнім шляхом і йде КНР, хоча на перший погляд видається, що стратегії КНР та РФ однакові. Наприклад, у той час, як уряд РФ ставить завдання створити «національний планшет», КНР стимулює розвиток транснаціональних китайських ІТ-ТНК, які змогли б подібну ідею реалізувати. І цей підхід є значно перспективнішим і стратегічно правильним. І це стосується майже всього спектра згаданого цифрового суверенітету.

Позиція РФ на міжнародній арені

Однак якщо внутрішні зусилля РФ, спрямовані на убезпечення від загроз з кіберпростору (технічних і політичних) мають дещо фрагментарний вигляд, а подекуди є надмірними, то позиція на міжнародній арені є більш цілісною й продуманою.

Своє загальне бачення зовнішніх інформаційних загроз і стратегічних пріоритетів РФ виклала у двох базових документах: оновлена «Воєнна доктрина Російської Федерації» (від грудня 2014 р.) [15] та в «Основах державної політики Російської Федерації у сфері міжнародної інформаційної безпеки на період до 2020 року» (2013 р.) [29].

Воєнна доктрина у п. 12 серед зовнішніх загроз виділяє використання інформаційних і комунікаційних технологій у воєнно-політичних цілях для нейтралізації дій, що суперечать міжнародному праву, спрямованих проти суверенітету, політичної незалежності, територіальної цілісності держав та становлять загрозу міжнародному миру, безпеці, глобальній та регіональній стабільності. Відповідно симетричною відповіддю на цю загрозу є п. 21(у), у якому планується створювати умови, спрямовані на недопущення реалізації зазначених загроз. Крім того, п. 46(в) прямо вказує на те, що РФ не збирається обмежуватися виключно оборонними заходами, а планує розвивати сили та засоби інформаційного протиборства.

Другий документ («Основи державної політики...») концептуально викладає розуміння РФ того, якою взагалі має бути міжнародна політика стосовно глобального інформаційного простору й міжнародної інформаційної безпеки. Під останньою мається на увазі «такий стан глобального інформаційного простору, при якому виключені можливості порушення прав особи, суспільства та прав держав в інформаційній сфері, а також деструктивного та протиправного впливу на елементи національної критичної інформаційної інфраструктури». Серед пріоритетних завдань, які цей документ визначає як ключові, варто звернути увагу на два з них, які й формують принципову відмінність у позиціях США та країн Заходу, з одного боку, та альянсу РФ-КНР – з іншого: створення умов для протидії загрозам використання інформаційно-комунікативних технологій з метою втручання у внутрішні справи суверенних держав і створення умов для забезпечення технологічного суверенітету держав у сфері інформаційно-комунікаційних технологій та подолання інформаційної нерівності між розвиненими країнами й тими, що розвиваються.

Перше – це постійна занепокоєність РФ щодо можливості організації на її території іноземними спецслужбами «кольорової революції» (а російське як військове, так і політичне керівництво держави повністю впевнене, що всі «кольорові революції» інспіровані іноземними спецслужбами).

Друге – приховане звинувачення країн Заходу в тому, що вони штучно стримують технологічний розвиток інших країн, не даючи їм набути необхідної «технологічної суверенності» (цифрового суверенітету). Щоправда, тут позиції РФ виглядають продуманішими та підкріплені прикладами реальних кроків розвинутих країн у дусі сучасного неоколоніалізму.

Метою ж «Основ державної політики Російської Федерації у сфері міжнародної інформаційної безпеки на період до 2020 року» є, передусім, просування на міжнародній арені російської ініціативи розробки та прийняття державами-членами ООН Конвенції із забезпечення міжнародної інформаційної безпеки.

Варто зазначити, що РФ досить послідовно обстоює більшість із цих тез на міжнародному рівні й почала це робити ще на початку 90-х років. Зокрема, перша цілісна спроба ініціювати міжнародний договір (конвенцію) з протидії використання інформаційного простору з ворожими цілями належить саме РФ: у 1993 р. для розгляду у структурах ООН було підготовлено проект «Конвенції про заборону воєнного чи іншого ворожого використання методів та засобів впливу на інфосферу» [22]. Цей перший проект складався всього з 10 статей, з яких 5 були взагалі технічними [18].

Перші спроби були, вочевидь, невдалими і залишалися такими принаймні до 2009 р., коли РФ запропонувала одразу кілька нових документів.

Перший – Конвенція про забезпечення міжнародної інформаційної безпеки (КЗМІБ) [23], концепцію якої було представлено російською стороною під час Другої міжнародної зустрічі високих представників, що курують питання безпеки (20–21 вересня 2011 р., Єкатеринбург)[3], є значно більшою за обсягом, ніж Правила, і ґрунтовніше висвітлює те, що було лише контурно й частково окреслено китайсько-російським документом. Зокрема, в КЗМІБ, так само, як і у Правилах, акцентовано увагу на тому, що всі питання, пов'язані з державною політикою щодо мережі Інтернет, є суверенним правом держав. Крім того, з-поміж загроз у сфері міжнародної інформаційної безпеки виокремлені:

- неправомірне використання інформаційних ресурсів іншої держави без узгодження з державою, в інформаційному просторі якої ці ресурси розміщені;
- діяльність в інформаційному просторі з метою підриву політичної, економічної та соціальної системи іншої держави, психологічний вплив на населення, що дестабілізує суспільство;
- маніпулювання інформаційними потоками в інформаційному просторі інших держав, дезінформація та приховування інформації з метою викривлення психологічного та духовного середовища суспільства, ерозія традиційних культурних, моральних, етичних та естетичних цінностей;
- протидія доступу до новітніх інформаційно-комунікативних технологій, створення умов технологічної залежності у сфері інформатизації на шкоду іншим державам[4];
- інформаційна експансія, набуття контролю над національними інформаційними ресурсами іншої держави.

Документ, запропонований РФ для розгляду та обговорення ООН, не суперечить китайським підходам до інформаційної та кібербезпеки та відверто опонує аналогічним американським документам і підходам. Можна припустити, що Росія та Китай активно консультувалися щодо своїх позицій, погоджували їх. Але, незважаючи на досить потужний супровід зазначеної ініціативи російським зовнішньополітичним відомством, вона так і не перетворилася на базу домовленостей між основними геополітичними гравцями, включно зі США та їх союзниками.

Другий – спільна ініціатива 4-х країн з утвердження на міжнародному рівні «правил для Інтернету»: «Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки». Базовий варіант Правил було внесено у вересні 2011 р., а оновлений варіант (цього разу до країн, що вносили документ, додалися Казахстан і Киргизстан) – 13-го січня 2015 р. [31].

Оновлений варіант майже не містить принципових змін щодо до першого. Частково доповнено преамбулу документа, де з'явилися відсилання до звітів Групи урядових експертів (створеної на основі Резолюції 66/24 у 2012 р.), зокрема від 2013 р.

Загалом документ став більш предметним і жорстким щодо бажань його ініціаторів. Замість розмитих формулювань попередньої редакції, нові тези не залишають двозначних розумінь кінцевої мети авторів. Так, замість загальних формулювань про необхідність не використовувати ІКТ для актів агресії, загроз міжнародному миру, розповсюдження інформаційної зброї та іншого, чітко вказано, що одним із зобов'язань підписантів є невикористання «інформаційно-комунікаційних технологій та інформаційно-комунікаційних мереж для втручання в справи інших держав і з метою підриву політичної, економічної та соціальної стабільності», а також можливість держав обмежувати права громадян на інформацію. Причому останній пункт (незважаючи на наявні уточнення причин таких обмежень) сформульований достатньо широко, що дасть змогу включити туди майже будь-що.

Цікавим є й уточнення норми щодо управління Інтернетом. Якщо в проекті документа від 2011 р. ця теза була прописана ширше, то в новій редакції прямо вказується на те, що вирішальну роль в управлінні мережею мають відігравати виключно держави. Це, вочевидь, суперечить т.зв. мультистейкхолдерському підходу, якого дотримується США та пов'язані з ним гравці (як державні, так і недержавні), а отже, є ще однією з причин відсутності компромісу з цього питання.

Загалом логіка і суть оновленого проекту Правил не лише не змінилися порівняно з попе-

[3]Учасниками є 52 країни. Рівень представництва – вищі особи, які відповідають за координування діяльності правоохоронних структур.

[4]Хоча цей пункт кореспондує з тезами американської Стратегії кіберпростору, він має у російській версії принципово інший зміст. США, заперечуючи «обмеження доступу до технологій», мають на увазі обмеження урядами доступу до ІКТ для населення, тоді як РФ, вочевидь, має на увазі формальні та неформальні міждержавні обмеження. Зокрема обмеження, пов'язані із сумнозвісною поправкою Джексона-Веніка чи правилами, встановленими за років «холодної війни» (1949 р.) Координаційним комітетом з експортного контролю (*Coordinating Committee for Multilateral Export Controls, CoCom*), які згодом трансформувалися на Вассенарські домовленості (1996 р.)

реднім, однак стали чіткішими та зрозумілішими щодо основних світоглядних позицій його ініціаторів. Крім того, цей документ очікувано розроблений у руслі російських «Основ державної політики Російської Федерації у сфері міжнародної інформаційної безпеки на період до 2020 року» та є для РФ проміжним етапом підготовки до внесення на обговорення проекту Конвенції про забезпечення міжнародної інформаційної безпеки (швидше за все – також оновленої версії).

Однак малоймовірно, що консенсус із цього питання буде знайдено і російські ініціативи зможуть просунутися далі проектів документів (на що звертають увагу і російські експерти [17]). Як слушно зазначають дослідники [3], принципова незгода Заходу із російським підходом до розуміння поняття «інформаційна безпека» та «міжнародна інформаційна безпека», коли в них включаються, крім технічних питань, ще й «контентні» (використання соцмереж, заходи з обмеження інформаційних прав людини, питання політичної та соціальної стабільності тощо), робить досягнення консенсусу неможливим. Однак схоже на те, що РФ і не ставить перед собою реальної мети досягти такого консенсусу, а завданням як самих ініціатив, так і низки внутрішніх документів у сфері регулювання внутрішньоросійського інформаційного простору є своєрідна легітимація власної рестриктивної політики з посиланням на те, що країни Заходу не бажають чути російські аргументи щодо актуальних загроз, які походять з кіберпростору.

Висновки для України

Подібний стратегічний вектор політики РФ щодо глобального кіберпростору (легітимація рестриктивної політики, а потенційно – використання кіберпростору у воєнних цілях) безпосередньо стосується і України, яка може стати своєрідним полігоном використання Росією власних кіберозброєнь та оновлених кіберпотужностей. Відповідно, Україна не може собі дозволити сприймати озвучені РФ плани нарощування свого кіберпотенціалу виключно у форматі «спостереження» та «констатації» – Україна має чітко визначитися з власною стратегією як щодо національного, так і глобального кіберпростору, своїх можливостей використання його у власних інтересах та протидії спробам сторонніх гравців використати його проти національних інтересів України. Це, своєю чергою, буде неможливим без дієвої системи кібернетичної безпеки держави, взаємоузгодженої діяльності всіх основних відомств сектору безпеки та оборони, формування нового типу взаємовідносин між державою та приватним сектором, а також нормативно-правового унормування питань, пов'язаних із кібербезпекою України.

Список використаних джерел

1. *2014 global* R&D funding forecast [Електронний ресурс]. – Режим доступу: http://www.battelle.org/docs/tpp/2014_global_rd_funding_forecast.pdf?sfvrsn=4

2. *As Delivered* by Secretary of Defense Chuck Hagel, Omaha, Nebraska, Wednesday, June 19, 2013 [Електронний ресурс]. – Режим доступу: http://www.defense.gov/speeches/speech.aspx?speechid=1791

3. *Baylon C.* Overview: Common Challenges in Cyber Security and Space Security – Contributing to an Escalatory Cycle of Militarization? / Chatham House. Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives [Електронний ресурс]. – Режим доступу: http://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSpaceSecurityBaylonUpdate.pdf

4. *Cyber* defence in the EU. Preparing for cyber warfare? [Електронний ресурс]. – Режим доступу: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

5. *Cyberpower* and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. – Washington, D.C.: Potomac Books, 2009. – 642 p.

6. *Cybersecurity* threats: the way forward [Електронний ресурс]. – Режим доступу: http://intelligence.house.gov/hearing/cybersecurity-threats-way-forward

7. *Demidov O.* Russia's Information Security Policy / Chatham House. Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives [Електронний ресурс]. – Режим доступу: http://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSpaceSecurityBaylonUpdate.pdf

8. *Distinguishing* acts of war in cyberspace: assessment criteria policy considerations, and response implications / Jeffrey L. Caton [Електронний ресурс]. – Режим доступу: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1229

9. *Impact* of Alleged Russian Cyber Attacks / William C. Ashmore // School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas. – 58 p. [Електронний ресурс].– Режим доступу: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-027.pdf

10. *Spy* Chief Says Little Danger of Cyber 'Pearl Harbor' in Next Two Years / Kim Zetter [Електронний ресурс]. – Режим доступу: http://www.wired.com/2013/03/no-cyber-pearl-harbor/

11. *USA* National Security Strategy 2015 [Електронний ресурс]. – Режим доступу: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf

12. *White* House. Red Chair. Obama Meets Swisher [Електронний ресурс]. – Режим доступу: http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/

13. *Алексей* Соколов займется информационной безопасностью России [Електронний ресурс]. – Режим доступу: http://www.eurasian-defence.ru/node/30517

14. *В Карагандинской* области пройдут киберучения «Взаимодействие-2014» [Електронний ресурс]. – Режим доступу: http://www.inf74.ru/news/v-karagandinskoy-oblasti-proydut-kiberucheniya-vzaimodeystvie-2014/

15. *Военная д*октрина Российской Федерации [Електронний ресурс]. – Режим доступу: http://www.rg.ru/pril/article/106/65/05/Voennaia_doktrina_RF.pdf

16. *Возможен* ли в России цифровой суверенитет / Алексей Лукатский [Електронний ресурс]. – Режим доступу: http://lukatsky.blogspot.com/2013/03/blog-post_18.html

17. *Возможна* ли гонка кибервооружений между Россией и США? / Александра Куликова [Електронний ресурс]. – Режим доступу: http://pircenter.org/media/content/files/13/14243529940.pdf

18. *Глобальное* информационное пространство и его место в современном международном праве / А. Иванов // Полхуновский вестинк. – 2005. –№ 1 [Електронний ресурс]. – Режим доступу: http://www.facebook.com/l.php?u=http%3A%2F%2Fnew.elib.altstu.ru%2Fjournal%2Fshow%2F100401&h=GAQFxcMtV

19. *Доктрина* информационной безопасности Российской Федерации [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/5.html

20. *Информационный* суверенитет – новая реальность / Игорь Ашманов [Електронний ресурс]. – Режим доступу: http://iforum.ua/docs/biz/

21. *Источник* в Минобороны: в Вооруженных силах РФ созданы войска информационных операций [Електронний ресурс]. – Режим доступу: http://tass.ru/politika/1179830

22. *Конвенция* о запрещении военного или любого юного враждебного использования методов и средств воздействия на инфосферу (первая редакция) [Електронний ресурс]. – Режим доступу: https://scontent.xx.fbcdn.net/hphotos-xap1/v/t1.0-9/10672229_712367012176244_8665293358022848638_n.jpg?oh=cb8a677919121b3b910b271669cc2100&oe=555D4B14

23. *Конвенция* об обеспечении международной информационной безопасности (концепция) / Министерство иностранных дел РФ [Електронний ресурс]. – Режим доступу: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

24. *Концепция* стратегии кибербезопасности Российской Федерации [Електронний ресурс]. – Режим доступу: http://council.gov.ru/press-center/discussions/38324/

25. *Минкомсвязь*, ФСБ и Минобороны провели учения по защите российского сегмента интернета [Електронний ресурс]. – Режим доступу: http://www.minsvyaz.ru/ru/events/31441/

26. *Михалков* и Пореченков создадут в России «патриотический интернет» [Електронний ресурс]. – Режим доступу: http://timeua.com/news/2/31214.html

27. *Научные* роты. Специальный репортаж В. Акиньшина [Електронний ресурс]. – Режим доступу: http://www.vesti.ru/doc.html?id=1105336

28. *Об утверждении* Положения о научных ротах Вооруженных Сил Российской Федерации [Електронний ресурс]. – Режим доступу: http://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fguap.ru%2Fguap%2Fdep07%2F2014%2Finstr_otb.doc&ei=banhVPjNGcXzUoblgvgO&usg=AFQjCNF3wjb6-kM76ZsCj5mqNurfUbQYLg&sig2=yNerljxnNrYiEzxPbvpjKw*&bvm=bv.85970519,d.d24&cad=rja*

29. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/114.html

30. *Дугин А.* Первые мысли об уходе Суркова. Good bye, golden boy / Александр Дугин [Електронний ресурс]. – Режим доступу: http://evrazia.org/article/1876

31. *Письмо* постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря [Електронний ресурс]. – Режим доступу: http://www.mid.ru/bdomp/ns-dmo.nsf/c85969b2329a429944257d5600225ebb/44257b100055f7e6c3257db4004192e4/$FILE/A%2069%20723%20Ru.pdf

32. *Россиянку,* которая распространяла украинские новости в соцсетях, следственный комитет РФ записал в «Правый сектор» [Електронний ресурс]. – Режим доступу: http://ru.tsn.ua/svit/rossiyanku-kotoraya-rasprostranyala-ukrainskie-novosti-v-socsetyah-sledstvennyy-komitet-rf-zapisal-v-pravyy-sektor-404252.html

33. *Черненко Е.* Русский с китайцем большие братья навек / Елена Черненко [Електронний ресурс]. – Режим доступу: http://www.kommersant.ru/doc/2608311

34. *Рожков Р.* Семь бед — один рунет / Роман Рожков [Електронний ресурс]. – Режим доступу: http://www.kommersant.ru/doc/2640958

35. *Птичкин С.* Троянский код / Сергей Птичкин [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2014/11/21/kod.html

36. *О создании* государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : указ Президента Российской Федерации от 15 января 2013 г. № 31 [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html