УДК 327.8 : 15

ДЕРЖАВНІ АКТОРИ У СИСТЕМІ РОСІЙСЬКОГО ЗОВНІШНЬОПОЛІТИЧНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ

Надіслано:
26.03.2019
Рецензовано:
04.04.2019
Прийнято:
03.05.2019

Демартино Андрій Павлович
кандидат історичних наук, докторант,
Інститут держави і права імені В. М. Корецького НАН України
м. Київ, Україна
ORCID: 0000-0002-2647-0129
andrede17@gmail.com

У статті досліджується рольова і структурна функція центральних органів державної влади, що є ключовими елементами російської системи інформаційного впливу на міжнародній арені. Аналізуються основні актори, що представляють державний сектор в рамках зовнішньої стратегії Кремля, їхні основні характеристики та вплив на процес прийняття і реалізації рішень вищого політичного керівництва Росії.

В умовах російської агресії проти України, що триває з 2014 р., інформаційна та кібервійна є однією з ключових стратегій Кремля, спрямованих на знищення української державності та деморалізацію українського суспільства.

У дослідженні було використано системний та структурно-функціональний аналіз. Зокрема, визначено коло ключових державних акторів, досліджено їх рольову функцію та структурний вплив в системі центральних органів державної влади РФ на підготовку відповідних зовнішньополітичних, організаційних та управлінських рішень і заходів для забезпечення російської інформаційної агресії на міжнародній арені. Це також дало змогу визначити масштаб і специфіку залучення вищого політичного керівництва Росії до реалізації основних напрямів та інструментів інформаційного впливу Москви РФ за кордоном. Насамперед. Це все має велике значення для забезпечення національної безпеки, зокрема для підготовки відповідних зовнішньополітичних, організаційних та управлінських рішень і заходів для захисту від інформаційного впливу противника.

Аналіз практики застосування Росією проти своїх сусідів технологій інформаційної та гібридної війни свідчить про те, що Москва для зміцнення свого впливу назовні комплексно використовує широкий спектр як державних органів, так і неурядових акторів, що діють як єдиний механізм за єдиним сценарієм в системі централізованого керівництва.

Ключові слова: інформація; технології; безпека; агресія; кібервійна.

***Demartyno Andrii**, Candidate of Historical Sciences, Doctoral Student, V. M. Koretskyi Institute of State and Law of the National Academy of Sciences of Ukraine, Kyiv, Ukraine*

State players in the system of Russian external foreign policy information influence

The article investigates the role and structural function of the central public authorities, which are the key elements of the Russian system of information influence in the international arena. The major players representing state sector in the framework of the Kremlin's foreign strategy, their main characteristics and impact on the process of deciding and implementation of decisions of the highest political leadership of Russia have been analyzed.

In the context of the Russian aggression against Ukraine, which has been continuing since 2014, information and cyber warfare is one of the key Kremlin strategies aimed at the destruction of Ukrainian statehood and demoralization of Ukrainian society.

The study has applied systemic and structural-functional analysis. In particular, it has identified a range of key state players, and investigated their role function and structural influence on the development of relevant foreign policy, organizational and managerial decisions and measures on support of the Russian information aggression in the international arena in the system of central bodies of state power of the Russian Federation. It has also provided the opportunity to determine the scale and specific features of the involvement of the highest political leadership of Russia in the implementation of the main directions and tools of information influence of Moscow, Russian Federation, abroad. All these facts, in turn, are of great importance for ensuring national security, in particular in the development of appropriate foreign policy, organizational and managerial decisions and protective measures against the information impact of the enemy.

The analysis of the practice of Russia's information and hybrid warfare technologies application against its neighbours shows that Moscow has been taking advantage of a wide range of both state bodies and non-governmental players to strengthen its influence abroad, operating as a single mechanism under a single scenario in the centralized management system.

Key words: information; technology; security; aggression; cyber warfare.

Демартино Андрей Павлович*, кандидат исторических наук, докторант, Институт государства и права имени М. М. Корецкого НАН Украины, г. Киев, Украина*

Государственные акторы в системе российского внешнеполитического информационного воздействия

В статье исследуется ролевая и структурная функция центральных органов государственной власти, которые являются ключевыми элементами российской системы информационного влияния на международной арене. Анализируются основные акторы, представляющие государственный сектор в рамках внешней стратегии Кремля, их основные характеристики и влияние на процесс принятия и реализации решений высшего политического руководства России.

В условиях российской агрессии против Украины, которая длится с 2014 г., информационная и кибервойна является одной из ключевых стратегий Кремля, направленных на уничтожение украинской государственности и деморализацию украинского общества.

В исследовании были использованы системный и структурно-функциональный анализ. В частности, определён круг ключевых государственных акторов, исследованы их ролевую функцию и структурное влияние в системе центральных органов государственной власти РФ на подготовку соответствующих внешнеполитических, организационных и управленческих решений и мероприятий по обеспечению российской информационной агрессии на международной арене. Это также позволило определить масштаб и специфику привлечения высшего политического руководства России к реализации основных направлений и инструментов информационного влияния Москвы РФ за рубежом. Все это в свою очередь имеет большое значение для обеспечения национальной безопасности, в частности при подготовке соответствующих внешнеполитических, организационных и управленческих решений и мер по защите от информационного воздействия противника.

Анализ практики применения Россией против своих соседей технологий информационной и гибридной войны свидетельствует о том, что Москва для укрепления своего внешнего влияния комплексно использует широкий спектр как государственных органов, так и неправительственных акторов, действуют как единый механизм по единому сценарию в системе централизованного руководства.

Ключевые слова: информация; технологии; безопасность; агрессия; кибервойна.

Вступ

В умовах російської агресії проти України, що триває з 2014 р., інформаційна війна в кіберпросторі, ЗМІ та соціальних мережах є однією з ключових стратегій Кремля, спрямованих на знищення нашої державності та деморалізацію українського суспільства. У зв'язку з цим, виникає нагальна і досить актуальна потреба у вивченні ролі й місця основних державних акторів, що визначають напрями та інструменти реалізації інформаційного впливу Москви. Усе це має велике значення для забезпечення національної безпеки, зокрема при підготовці відповідних зовнішньополітичних, організаційних та управлінських рішень і заходів по захисту від інформаційного впливу противника.

Аналіз останніх досліджень і публікацій

Наукових праць, в яких досліджується специфіка роботи російських органів центральної влади у сфері зовнішнього інформаційного впливу, зовсім не багато. Останнє обумовлено тим, що значна частина змістовних матеріалів з даної проблематики часто-густо має конфіденційний або навіть засекречений характер. Крім того, в умовах гібридної війни Кремль постійно залучає нові технології і розширює існуючий арсенал засобів ведення інформаційного протиборства, що додатково збільшує потребу у своєчасному аналізі та систематизації російської діяльності в цій сфері. Зокрема, у працях С. Канєва, О. Мєльнікової, Р. Рудомського, М. Барабанова, Д. Туровського, А. Благовєщєнського та ін. досліджуються особливості діяльності основнихдержавних акторів, що забезпечують інформаційний вплив Росії за кордоном.

Виділення невирішених раніше частин загальної проблеми

Комплексне дослідження функціонування російської «інформаційної машини» зовнішньополітичного впливу, як цілісного механізму з точки зори основних державних акторів, що визначають напрями та інструменти реалізації інформаційного впливу Москви.

Формулювання цілей статті

Дослідити рольову і структурну функцію центральних органів державної влади РФ, що є ключовими елементами інформаційного впливу Москви на міжнародній арені, систематизувати їхні основні характеристики та з'ясувати специфіку реалізації рішень вищого політичного керівництва Росії у цій сфері.

У цій статті автором буде розглянуто діяльність лише державних російських акторів, безпосередньо задіяних зовнішній інформаційній стратегії, яку Кремль веде на міжнародній арені. Масштаби інформаційної агресії РФ дозволяють говорити про те, що існує цілісна державна машина інформаційної війни.

Виклад основного матеріалу дослідження

Аналіз практики застосування Росією проти своїх сусідів технологій інформаційної і гібридної війни свідчить про те, що Москва для зміцнення свого впливу назовні комплексно використовує широкий спектр як державних органів, так і неурядових акторів, що діють як єдиний механізм за єдиним сценарієм.

У Росії до державних органів, що контролюють діяльність в інформаційній сфері, та мають специфіку роботи, пов'язану з міжнародними відносинами і безпекою, належать:

– Рада безпеки Росії та Адміністрація Президента РФ;

– Міністерство закордонних справ РФ;

– Іномовні ЗМІ, що фінансуються з федерального бюджету;

– Федеральна служба безпеки Російської Федерації (ФСБ Росії) та Служба зовнішньої розвідки РФ;

– Міністерство оборони Російської Федерації (Міноборони Росії).

Рада безпеки Росії

Рада безпеки РФ утворена указом президента від 3 червня 1992 р. є конституційним дорадчим органом. Здійснює підготовку рішень президента з питань забезпечення безпеки, організації оборони, військового будівництва, військово-технічного співробітництва з іноземними державами, а також з інших питань, пов'язаних із захистом конституційного ладу, незалежності та територіальної цілісності РФ. Діяльність здійснюється у формі засідань і нарад.

Вага і значення цього органу визначається тим, що згідно Конституції РФ Президент «формує і очолює Раду безпеки Російської Федерації, статус якої визначається федеральним законом». Крім нього до складу ради за посадою входять 12 постійних членів, включаючи секретаря Радбезу, і 18 членів, які призначаються президентом за поданням секретаря. Основними робочими органами є наукова рада та сім міжвідомчих комісій (з проблем СНД, по військової безпеки, з інформаційної безпеки та ін.). Апарат Радбезу, очолюваний секретарем, є самостійним підрозділом адміністрації президента.

У 2011 р. указом № 590 президента Дмитра Медведєва повноваження Радбезу і його секретаря були істотно розширені. Відомство, яке очолює Микола Патрушев отримало право не тільки на «формування державної політики в галузі забезпечення національної безпеки», але й рішення Радбезу, згідно з указом, стали обов'язковими для виконання всіма міністерствами і відомствами. Відтоді Радбез також бере участь у «формуванні кадрової політики», «організовує контроль за цільовим витрачанням бюджетних асигнувань, передбачених у федеральному бюджеті на відповідний рік на фінансування витрат по забезпеченню національної оборони, національної

безпеки та правоохоронної діяльності», а уряд, Рада Федерації і Держдума зобов'язані щорічно подавати звіт про виконану роботу (Kanev, 2016).

Починаючи з 2013 р. Рада безпеки по суті стала основним центром прийняття стратегічних рішень в системі влади РФ. Вона перетворилася в щось на зразок «тіньового уряду», що має істотний вплив на основні напрями державної політики. Однак формально порушень тут немає. З точки зору права – це орган дорадчий і обговорювати він може все що завгодно, щоб забезпечити умови «для здійснення Президентом Російської Федерації повноважень в галузі забезпечення національної безпеки».

З погляду автора, саме Рада безпеки РФ є тим ключовим органом, що розглядає і приймає політичні рішення щодо початку інформаційної кампанії (війни, агресії, атаки) стосовно конкретної країни або недержавної організації. Зокрема, секретар Ради Безпеки РФ Микола Патрушев, характеризуючи її діяльність за останні 25 років, зазначав: «Кожне засідання або нараду Ради безпеки під головуванням президента Росії присвячено найбільш актуальним проблемам… У відповідь на розв'язання Грузією війни в Південній Осетії в серпні 2008 р. Рада безпеки РФ прийняла рішення про примус до миру Грузії, визнання незалежності Абхазії і Південної Осетії та надання допомоги в становленні їх державності. Серед пріоритетів залишалися питання протидії міжнародному тероризму, зокрема з урахуванням негативного розвитку ситуації в Сирії, Ємені, Іраку, Лівії, загроз, що виходять з афгано-пакистанської зони нестабільності. Вплив цих факторів додатково враховувався при підготовці пропозицій щодо розвитку співробітництва з державами-учасниками СНД, в процесі вироблення заходів для забезпечення безпеки Олімпійських та Параолімпійських ігор в Сочі та інших великих спортивних змаганнь» (Voynyi miry, 2017).

Адміністрація Президента Російської Федерації

Таким чином, Рада безпеки РФ є ключовим органом легітимізації політичних рішень в сфері реалізації заходів зовнішньополітичного інформаційного впливу. У цьому контексті виконавчим і контролюючим органом реалізації затверджених стратегій виступає Адміністрація Президента Російської Федерації (далі – АП РФ), яка в той же час виконує функції оперативного інформаційного реагування.

АП РФ є державним органом, сформованим відповідно до пункту «і» статті 83 Конституції Російської Федерації, який забезпечує діяльність Президента Російської Федерації і здійснює контроль за виконанням рішень Президента Російської Федерації.

Згідно «Положення про Адміністрацію Президента Російської Федерації», затвердженого Указом Президента РФ від 6 квітня 2004 р. № 490

«Про Адміністрацію Президента Російської Федерації», цей орган створений для (Polozhenie ob Administratsii Prezidenta, 2004):

– забезпечення реалізації Президентом Російської Федерації повноважень глави держави;

– здійснення контролю за виконанням рішень Президента Російської Федерації;

– підготовки пропозицій Президентові Російської Федерації щодо заходів, спрямованих на охорону суверенітету Російської Федерації, її незалежності та державної цілісності;

– сприяння Президентові Російської Федерації у визначенні основних напрямів внутрішньої і зовнішньої політики держави;

– розробки загальної стратегії зовнішньої політики Російської Федерації, забезпечення реалізації Президентом Російської Федерації його повноважень для керівництва зовнішньою політикою Російської Федерації;

– сприяння Президентові Російської Федерації в забезпеченні узгодженого функціонування і взаємодії органів державної влади тощо.

На думку російського дослідника зовнішньої і внутрішньої політики Кремля Юрія Федорова, автора видання «Гібридна війна по-російськи», АП РФ здійснює загальну координацію російської зовнішньополітичною пропагандою, включаючи виділення коштів (Fedorov, 2016, p.146). За його думкою, ключову роль в цьому процесі відігравали (станом на 2016 рік):

– Перший заступник Керівника Адміністрації Президента (Олексій Громов) та заступник Керівника Адміністрації Президента – прес-секретар Президента (Дмитро Пєсков), які спрямовують діяльність Управління у зв'язках з громадськістю і масових комунікацій АП.

– Помічник Президента РФ з питань зовнішньої політики Юрій Ушаков, який координує діяльність Управління Президента із зовнішньої політики.

– Помічник Путіна Владислав Сурков, який здійснює керівництво діяльністю Управління Президента з прикордонного співробітництва, що забезпечує діяльність Президента з питань прикордонного співробітництва з Республікою Абхазія, Республікою Південна Осетія і Україною та з іншими суміжними державами, а також Управління Президента з міжрегіональних і культурних зв'язків із зарубіжними країнами.

Міністерство закордонних справ Росії

Відповідно до Указу Президента РФ від 8 листопада 2011 р. «Про координуючу роль Міністерства закордонних справ Російської Федерації (МЗС РФ – далі) в проведенні єдиної зовнішньополітичної лінії Російської Федерації», МЗС Росії є головним органом у системі федеральних органів виконавчої влади у сфері відносин з іноземними державами і міжнародними

організаціями. Міністерство координує проведення єдиної зовнішньополітичної лінії Російської Федерації.

Саме МЗС РФ є ключовим органом, що політично, ідеологічно і пропагандистські використовує офіційну трибуну міжнародних організацій (ООН, ОБСЄ, Ради Європи тощо), відпрацьовує майданчики глобальних і регіональних форумів (саміти «двадцятки», БРИКС, ШОС, СНД та ін.) та міжнародних конференцій. Крім того, координуюча роль МЗС поширюється на сферу інформаційного супроводу зовнішньої політики держави. Цю функцію здійснює діючий в рамках МЗС Департамент інформації та друку (ДІД) МЗС.

Основним джерелом офіційної зовнішньополітичної інформації є Інтернеті-портал МЗС Росії, що містить весь спектр інформаційних матеріалів Міністерства: офіційні документи, заяви, коментарі, інформацію про підсумки переговорів, огляди преси, моніторинги тощо.

МЗС Росії має свої сторінки в соціальних мережах Twitter, Youtube, Facebook, Flickr із загальною кількістю підписників понад 700 тисяч. Облікові записи в Twitter зареєстрували 135 закордонних установ МЗС Росії, 8 з них мають також іншомовну версію (на мові країни перебування). Одним з інструментів інформаційної роботи є соціальна мережа Storify, що використовується для аналізу, збору інформації та оцінки ефективності роботи закордонних установ по конкретним заходам (саміт ШОС, БРІКС і ін.). Крім офіційних акаунтів МЗС РФ, деякі представники Міністерства з числа вищого керівництва мають персональні сторінки, на яких також ведеться активне обговорення питань міжнародної політики (Melnikova, 2015).

Сьогодні інформаційну стратегію МЗС РФ можна визначити як агресивну інформаційну присутність, спрямовану на максимальне розширення російської присутності у світовому інформаційному полі. З метою реалізації цього завдання, створюються власні системи засобів впливу на зарубіжну аудиторію, включаючи використання новітніх можливостей інформаційних технологій.

Іномовні ЗМІ, що фінансуються з федерального бюджету

До інструментів зовнішньополітичного впливу, які створені і утримуються коштом російського уряду є – *Телеканал «Росія сьогодні».* У 2005 р. телеканал «Росія сьогодні» («RussiaToday», RT) розпочав іноземне мовлення з метою висвітлення за кордоном державної політики Російської Федерації, подій внутрішнього життя країни та міжнародних тем в дусі відповідності пріоритетів Кремля. Телеканал був заснований агентством «РИА Новости» через його дочірню організацію «ТВ-Новости». Головним редактором було призначено журналістку Маргариту Симоньян.

В основу діяльності телеканалу покладено механізм глобального виробництва актуальних новинних інформаційних повідомлень, що забезпечує

розширення інформаційної присутності Росії за кордоном. RT складається з чотирьох цілодобових інформаційних телеканалів, що ведуть мовлення з Москви у більш ніж 100 країнах світу англійською, арабською, іспанською і французькою мовами, телеканалів RT America і RT UK, що виходять в ефір з власних студій у Вашингтоні та Лондоні відповідно, документального каналу RTД, а також глобального новинного відео агентства Ruptly, що пропонує ексклюзивні матеріали іншим телеканалам.

Основним є телеканал англійською мовою RT International – перший російський інформаційний телеканал, який веде цілодобове мовлення англійською мовою. RT цілодобово доступний 700 мільйонам глядачів по всьому світу (RussiaToday, 2019).

За час свого існування телеканалу вдалося стати досить великим виробником новинний продукції. За словами міністра закордонних справ Сергія Лаврова, телеканал «RussiaToday» – дійсно вдалий проект і ефективний засіб масової інформації, який за популярністю можна порівняти з Сі-Ен-Ен, Бі-Бі-Сі і багатьма іншими провідними телеканалами США і Європи, але представляє альтернативну їм точку зору на події в світі (Vystuplenie i otvety na voprosy, 2014).

На думку відомого російського Савіка Шустера, глобальна мережа RussiaToday– головна зброя російської влади у інформаційній боротьбі.

RT фінансується з федерального бюджету РФ. Бюджет RussiaToday на 2012 р. становив €275 млн, а у 2014 – вже 500 млн доларів. Цей канал станом на 2012 р. посів перше місце у світі за розмірами державних витрат на одного працівника, які сягнули $183 тис. на людину(Rosijsko-ukrayinskainformacijnavijna,2019).

Федеральна служба безпеки Російської Федерації (ФСБ Росії)

Аналіз відкритих джерел інформації дає підстави стверджувати, що назовні РФ у структурі ФСБ інформаційні операції здійснюють принаймні два підрозділи.

Перший – 5-а Служба (Служба оперативної інформації і міжнародних зв'язків) ФСБ Росії. З 2009-го її керівником є генерал-полковник Сергій Беседа.

За даними Інтернет-видань, цей підрозділ було створено для того, щоб повернути «федералам» власні органи зовнішньої розвідки, які після ліквідації КДБ перейшли до Служби зовнішньої розвідки Росії. Ця Служба займається зовнішньою розвідувальною діяльністю, зокрема в країнах ближнього зарубіжжя. Керівництво і співробітники підрозділу неодноразово були помічені в Абхазії, Придністров'ї, Молдові, а також в Україні (Rudomskiy, 2017).

Зокрема, за інформацією групи «Інформаційний Опір», 20 лютого 2014 р. генерал-полковник Сергій Беседа разом з групою співробітників ФСБ прибув

в Україну після розстрілу Майдану для впливу на тоді ще президента України Віктора Януковича. За однією з версій, саме ці людини стояли за організацією сепаратистського з'їзду в Харкові і втечею Януковича до Росії (General FSB Beseda, 2014).

За даними порталу «Грузія Online», начальник 5-ої служби ФСБ РФ був причетний до дестабілізації ситуації в Грузії в 2008-му і 2010-му рр. Зокрема, згідно однієї з версій, озвучених на порталі, під керівництвом Беседи була створена опозиційна Михайлу Саакашвілі «Грузинська партія», за що Кремль передав її співголові Іраклію Окруашвілі близько 30 мільйонів доларів. Згідно зі сценарієм, розписаним в ФСБ, прокремлівський лідер Окруашвілі повинен був прийти до влади в Тбілісі після відділення Цхінвалі(Rudomskiy, 2017).

За повідомленнями ЗМІ, однією зі складових військових формувань бойовиків на Донбасі є армія, яка знаходиться під контролем ФСБ Росії, її керівництвом займається згадуваний вище генерал-полковник ФСБ Сергій Беседа (Rudomskiy, 2017).

Другий підрозділ – Центр інформаційної безпеки ФСБ Росії (ЦІБ ФСБ, 18-й центр), спеціалізований підрозділ ФСБ, що займається забезпеченням інформаційної безпеки Росії.

Центр створений на основі Управління комп'ютерної та інформаційної безпеки департаменту контррозвідки ФСБ і входить до складу служби контррозвідки ФСБ. Офіційно ЦІБ розслідує злочини в галузі електронної комерції та незаконного поширення персональних даних.

Зокрема, саме в Центрі інформаційної безпеки ФСБ Росії були створені підрозділи для дій в соціальних мережах в Україні. Про діяльність цієї структури дуже мало інформації у відкритих джерелах. Але в серпні 2014 р., під час загострення ситуації в АТО, глава Служби безпеки України Валентин Наливайченко оголосив наступні дані: «18-й спеціальний центр ФСБ Росії працює як спеціальний заклад, де цілодобово майже 1,5 тис. осіб в соціальних мережах через роботизовані системи розсилки повідомлень цілеспрямовано останні три доби розсилають повідомлення і тексти панічного характеру»(Poltory tyisyachi sotrudnikov FSB, 2014).

У відкритих джерелах багато писалося про інформаційні та кібератаки, що здійснювалися хакерськими групами під егідою 18-го центру в інших країнах, але про це буде написано далі в розділі, присвяченому хакерам, яких асоціюють з Росією.

Служба зовнішньої розвідки Російської Федерації

Служба зовнішньої розвідки (СЗР) Росії є складовою частиною сил забезпечення безпеки держави від зовнішніх загроз.

Діяльність СЗР будується на базі федерального закону «Про зовнішню розвідку» № 5-ФЗ від 10 січня 1996 р. (з наступними змінами). Так, у ст. 11.

«Сфери діяльності органів зовнішньої розвідки Російської Федерації» зазначається: «Розвідувальна діяльність у межах своїх повноважень здійснюється: 1) Службою зовнішньої розвідки Російської Федерації – в політичній, економічній, військово-стратегічній, науково-технічній та екологічній сферах, у сфері шифрованого, засекреченого та інших видів спеціального зв'язку з використанням радіоелектронних засобів і методів за межами Російської Федерації, а також в сфері забезпечення безпеки установ Російської Федерації, що знаходяться за межами території Російської Федерації, і відряджених за межі території Російської Федерації громадян Російської Федерації, що мають за родом своєї діяльності допуск до відомостей, що становлять державну таємницю»(Sluzhba vneshney razvedki Rossii, 2012).

Також у законі чітко зазначено, що розвідувальна діяльність органів ФСБ здійснюється у взаємодії з органами зовнішньої розвідки Російської Федерації і відповідно до Федерального закону «Про федеральну службу безпеки».

Загальне керівництво Службою зовнішньої розвідки РФ здійснює президент РФ. Він призначає директора служби зовнішньої розвідки.

Сучасна організаційна структура СЗР РФ включає оперативні, аналітичні, функціональні підрозділи (управління, служби, самостійні відділи).

Враховуючи специфіку відомства у відкритих джерелах дуже мало інформації про діяльність СЗР РФ на ниві інформаційної війни. Натомість у ЗМІ повідомлялося про те, що СЗР Росії проводила закриті тендери на розробку методик «формування громадської думки» через соціальні мережі. Технічне завдання звучало як «розробка спеціального програмного комплексу автоматизованого розповсюдження інформації у великих соціальних мережах та організації інформаційної підтримки заходів по підготовленим сценаріями впливу на задану масову аудиторію соціальних мереж» (Cooper, 2015).

Міністерство оборони Російської Федерації

Хоча у 2008 р. під час грузино-російського конфлікту збройним силам РФ вдалось достатньо швидку придушити опір грузинської армії, разом з тим отриманий досвід став серйозним сигналом для Кремля щодо необхідності серйозних змін у військовій сфері. Тому, за результатами бойових дій в Грузії, політичним керівництво Росії восени 2008 р. було прийнято рішення про здійснення нового етапу радикальної військової реформи, що мало на меті прискорене приведення збройних сил до «нового вигляду», орієнтованого насамперед на участь в локальних конфліктах на території колишнього СРСР (Barabanov 2014).

14 жовтня 2008 р. міністр оборони Російської Федерації Анатолій Сердюков публічно оголосив про початок реалізації заходів з докорінного реформування російської військової системи. У 2010 р. було

підготовлено і прийнято масштабну програму озброєнь до 2020 р., яку підписав і затвердив президент РФ Дмитро Медведєв. Програма передбачала виділення 20,7 трлн рублів на нове, модернізоване озброєння і військову техніку, а також на науково-дослідні та дослідно-конструкторські роботи (Spisok stran po voennyim rashodam, 2019). У 2014 р. за сумарними асигнуваннями на армію Росія увійшла до трійки світових лідерів (Istochnik v Minoboronyi, 2014).

Наприкінці грудня 2011 р. Міноборони представило вже згадуваний документ під назвою «Концептуальні погляди на діяльність Збройних сил РФ в інформаційному просторі», де вперше визначався порядок дій ЗС Росії в умовах сучасної інформаційної війни, а також задані пріоритети інформаційного висвітлення і супроводу конфліктів, прописані завдання взаємодії ВС з медіа і громадськістю тощо.

Відповідно вже у березні 2012 р. віце-прем'єр РФ Дмитро Рогозін одним з перших російських високопосадовців озвучив тезу про необхідність створення в російській армії структури, аналогічної кіберкомандуванню в збройних силах США.

Влітку 2013 р. в російських ЗМІ повідомлялося про те, що вже до кінця року в російській армії з'явиться новий рід військ, який буде відповідати за інформаційну безпеку країни. Основні завдання цих військ: моніторинг і обробка інформації, що надходить ззовні, а також боротьба з кіберзагрозами. Офіцери, яких готують для служби в цих військах, в обов'язковому порядку повинні будуть пройти лінгвістичну підготовку, тобто вивчити іноземну мову, в першу чергу англійську (Blagoveschenskiy, 2013).

Також у 2013 р. Міноборони РФ оголосило про «велике полювання» на програмістів, які закінчують навчання в цивільних вузах, щоб залучити їх в наукові роти, які планувалося створити в якості підрозділів кібервійськ. Як заявив керівник міністерства Сергій Шойгу, з появою наукових рот може з'явитися «нове покоління людей, які будуть рухати військову науку»(Turovskiy, 2016).

12 травня 2014 р. Федеральне державне унітарне підприємство «Інформаційне телеграфне агентство Росії (ІТАР-ТАСС)» повідомило, що війська інформаційних операцій сформовані в Збройних силах Росії. Їх головне призначення – захист російських військових систем управління і зв'язку від кібертероризму та дій ймовірного противника. Як повідомило джерело агентства в Міноборони РФ: «Ідея створення такої структури, призначеної для кібернетичного та інформаційного протиборства з вірогідним противником, опрацьовувалася не один рік. Торішні викриття екс-співробітника ЦРУ Едварда Сноудена щодо глобального електронного стеження з боку АНБ США тільки прискорили процес прийняття рішення. До складу військ інформаційних операцій увійдуть частини і підрозділи у військових округах і на флотах,

укомплектовані висококваліфікованими фахівцями: математиками, програмістами, інженерами, криптографами, зв'язківцями, офіцерами радіоелектронної боротьби, перекладачами та іншими. Керівником нової структури призначено воєначальника в генеральському званні»(V internet vveli kibervoyska, 2017).

За повідомленнями російських ЗМІ ці війська формувалися у форматі «наукових рот» у військових частинах по всій країні. Набирали туди випускників технічних вузів – математиків, програмістів, криптографів, інженерів. В анкеті для вступу просили вказати знання мов програмування, програмних алгоритмів. Зокрема, Новосибірський державний технічний університет оголошував серед студентів набір в наукову роту ЦНДІ Міністерства оборони РФ в Сергієвому Посаді для участі в «застосуванні супер комп'ютерних технологій». У вересні 2015 р. при Міноборони відкрилася кадетська школа IT-технологій, а трьома місяцями пізніше Військову академію зв'язку закінчили перші випускники наукової роти «спецназу інформаційної безпеки»(Turovskiy, 2016).

Крім студентів Міноборони залучало хакерів, що мали проблеми із законом. Один з керівників кібердослідницької компанії Crowdstrike Дмитро Альперович фактично підтвердив цю інформацію: «Коли помічають когось технічно підкованого в російському підпіллі, на нього заводиться кримінальна справа, потім він просто зникає»(Turovskiy, 2016).

22 лютого 2017 р. міністр оборони Росії Сергій Шойгу під час свого виступу на засіданні Держдуми офіційно підтвердив існування в країні військ інформаційних операцій. За даними експертів зі спеціалізованої кампанії з інформаційної безпеки Zecurion Analytics, Росія входить в топ-5 країн за чисельністю і фінансуванням кібервійськ. Так, чисельність оцінюється приблизно в 1 тис. осіб, на фінансування яких щорічно може відводитися близько $ 300 млн. Основними напрямками діяльності кібервійськ в Zecurion називають шпигунство, кібератаки та інформаційні війни, які включають різні засоби впливу на настрій і поведінку населення країн. При цьому чим більше розвинена країна, тим вразливіша вона для кібератак. Зокрема, керівник аналітичного центру Zecurion Володимир Ульянов зазначав: «Залежність різних пристроїв і устаткування від інтернету буде тільки зростати. У результаті буде збільшуватися вразливість окремих користувачів, їх гаджетів, машин, а також систем і інфраструктури країн» (Polozhenieob AdministratsiiPrezidenta, 2004).

Висновки

У повній відповідності до російської концепції інформаційної та гібридної війни, Кремль створив мережу державних органів, які є частиною цілісного механізму зовнішнього впливу на будь-яку країну (міжнародну урядову чи нерядову організацію), що передбачає комплексне застосування

усіх засобів – від кібератак у мережах і інформаційної війни – до ведення бойових дій, які підтримуються операціями з розповсюдження хаосу і безладу всередині країни ворога. Поява інтернету, зокрема, соціальних мереж, надала Кремлю прямий доступ до населення його супротивників, минаючи воротарів, роль яких раніше грали ЗМІ.

Як складові частини російської стратегії зовнішнього впливу та гібридної війни державні органи відповідають за прийняття політичних рішень та офіційну реакцію РФ на міжнародній арені. Жодна з інформаційних чи кібератак, які розпочинав Кремль – Естонія (2007), Грузія (2008), Україна (з 2014), Сирія (з 2015), як і багато інших випадків, не обходилися без участі державних органів, які спочатку санкціонували кожну інформаційну агресію, а потім супроводжували її на офіційному рівні.

Масштаби інформаційної агресії дозволяють говорити про те, що в Росії існує цілісна державна машина інформаційної війни. І за рівнем оснащення, фінансування кібератак та інформаційних війн Російська Федерація входить в топ-5 країн.

References:

1. Barabanov, M. (2014). 'Ispytanie «novogo oblika». Ukrainskij konflikt i voennaja reforma v Rossii' [The test of the "new look". Ukrainian conflict and military reform in Russia]. *Rossija v global'noj politike* [Russia in global politics], [online], no. 5. Available at: http://www.globalaffairs.ru/number/Ispytanie-novogo-oblika-17097 [Accessed 10 February 2019].

2. Blagoveschenskiy, A. (2013). 'V 2013 godu Rossii pojavjatsja svoi kibervojska' [In 2013, Russia will have its own cyber warfare]. RG.ru, [online]. Available at: https://rg.ru/2013/07/05/cyberwar-site-anons.html [Accessed 11 February 2019].

3. Cooper, J. (2015). Voennoe lico "Voinstvennoj Rossii" [The military face of "militant Russia"]. *Rossija v global'noj politike* [Russia in global politics], [online], no. 6. Available at:http://www.globalaffairs.ru/number/Voennoe-litco-Voinstvennoi-Rossii-17830 [Accessed 14 February 2019].

4. Egorov, I. (2017). 'Vojny i miry. Nikolaj Patrushev: ob Ukraine i SShA, kiberatakah, Sirii i roli Sovbeza v istorii Rossii' [Wars and worlds. Nikolay Patrushev: about Ukraine and the USA, cyber attacks, Syria and the role of the Security Council in the history of Russia]. *Rossijskaja gazeta* [Russian newspaper], online, no. 107 (7273). Available at: https://rg.ru/2017/05/18/nikolaj-patrushev-ob-ukraine-i-ssha-kiberatakah-sirii.html [Accessed 28 January 2019].

5. *Federal'nyj Zakon «O vneshnej razvedke»: ot 10.01.1996 № 5-FZ* [Federal Law "On Foreign Intelligence" from January 10, 1996 No. 5-FL], [online]. Available

at:http://pravo.gov.ru/proxy/ips/?docbody=&nd=102039044 [Accessed 13 February 2019].

6. Fedorov, Yu. (2016*). "Hybrid" War à la Russe: "Gibridnaja" vojna po-russki.* Kyiv: TOV "Biznespoligraf".

7. General FSB Beseda priezzhal k Janukovichu posle rasstrela Majdana stimulirovat' separatism [The FSB General Conversation came to Yanukovych after the execution of the Maidan to stimulate separatism]. (2014). *Crime.in.ua,* [online]. Available at: http://crime.in.ua/news/20140406/beseda [Accessed 13 February 2019].

8. Informagentstvo "Sputnik" [News agency "Sputnik"]. *Wikipedia*, [online]. Available at: https://ru.wikipedia.org/wiki/Sputnik [Accessed 12 February 2019].

9. Istochnik v Minoborony: v Vooruzhennyh silah RF sozdany vojska informacionnyh operacij [Source in the Ministry of Defense: troops of information operations created in the Armed Forces of the Russian Federation]. (2014). *TASS*, [online]. (ITAR-TASS). Available at: https://tass.ru/politika/1179830 [Accessed 15 February 2019].

10. Kanev, S. (2016). 'Smotryaschie ot prezidenta' [Watchers from the president]. *The New Times*, [online], no. 11 (402). Available at: https://newtimes.ru/stati/temyi/02436cd5b5fbf254ceb4c06379300ab7-smotryashue-ot-prezudenta.html [Accessed 23 January 2019].

11. Mandro, I., Giber, N. (2017). 'Novyj arsenal firmy «Rossija»' [New Arsenal of the Russia Company]. *InoSMI,* [online]. Available at: http://inosmi.ru/politic/20170307/238837275.html [Accessed 03 March 2019].

12. Mel'nikova, O. A. (2015). 'Osnovnye zadachi informacionnogo obespechenija vneshnepoliticheskoj dejatel'nosti' [The main objectives of the information support of foreign policy activities]. *Vestnik MGIMO-Universiteta* [Bulletin of Moscow State Institute of International Relations-University], no. 2 (41), p. 95.

13. Poltory tysjachi sotrudnikov FSB kruglosutochno sejut paniku v socsetjah sredi ukraincev [One and a half thousand FSB employees around the clock sow panic on social networks among Ukrainians]. (2014). O*bozrevatel* [Observer], [online]. Available at: https://www.obozrevatel.com/politics/28351-poltoryi-tyisyachi-sotrudnikov-fsb-kruglosutochno-seyut-paniku-v-sotsialnyih-setyah.htm [Accessed 13 February 2019].

14. Rosiisko-ukrainska informatsiina viina [Russian-Ukrainian information warfare]. *Wikipedia*, [online]. Available at: https://uk.wikipedia.org/wiki/Rosijs`ko-ukrayins`ka_informacijna_vijna [Accessed 12 February 2019].

15. Rossija segodnja [Rossiya Segodnya]. *Wikipedia*, [online]. Available at: https://ru.wikipedia.org/wiki/Rossy`ya_segodnya [Accessed 12 February 2019].

16. Rudomskiy, R. (2017). 'Kurator okkupirovannogo Donbassa ot FSB. Chto izvestno pro Sergeja Besedu' [Curator of the occupied Donbass from the FSB. What is

known about Sergey Beseda]. *Depo.ua,* [online]. Available at: https://www.depo.ua/rus/war/kh/kurator-okupovanogo-donbasu-vid-fsb-scho-vidomo-pro-sergiya-besidu-20171026664368 [Accessed 05 March 2019].

17. Russia Today. *Wikipedia*, [online]. Available at: https://ru.wikipedia.org/wiki/RT [Accessed 12 February 2019].

18. Sluzhba vneshnej razvedki Rossii sozdaet botov dlja social'nyh setej za 30 mln. Rublej [The Foreign Intelligence Service of Russia creates bots for social networks for 30 million rubles]. (2012). *Habr.* [online]. Available at: https://habr.com/post/150269 [Accessed 14 February 2019].

19. Spisok stran po voennym rashodam [List of countries by military expenditures]. *Wikipedia,* [online]. Available at: https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D1%81%D1%82%D1%80%D0%B0%D0%BD_%D0%BF%D0%BE_%D0%B2%D0%BE%D0%B5%D0%BD%D0%BD%D1%8B%D0%BC_%D1%80%D0%B0%D1%81%D1%85%D0%BE%D0%B4%D0%B0%D0%BC [Accessed 13 February 2019].

20. Turovskiy, D. (2016). 'Rossijskie vooruzhennye kibersily. Kak gosudarstvo sozdaet voennye otrjady hakerov' [Russian armed cyber forces. How the state creates military units of hackers]. *Meduza*, [online]. Available at: https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily [Accessed 10 February 2019].

21. Ukaz Prezidenta RF "Ob utverzhdenii Polozhenija ob Administracii Prezidenta Rossijskoj Federacii" ot 06.04.2004 N 490 [Presidential Decree "On the approval of the Regulations on the Administration of the President of the Russian Federation" from 06.04.2004 N 490]. *President Rossii* [The President of Russia], [online]. Available at: http://kremlin.ru/acts/bank/20769 [Accessed 17 February 2019].

22. V internet vveli kibervojska. Analitiki ocenili kolichestvo hakerov na gossluzhbe [A cyber war was entered on the Internet. Analysts estimated the number of hackers in the civil service]. (2017). *Kommersant,* [online], no. 2. Available at: https://www.kommersant.ru/doc/3187320 [Accessed 15 February 2019].

23. Vystuplenie i otvety na voprosy Ministra inostrannyh del Rossii S. V. Lavrova v hode diskussii v ramkah Molodezhnogo obrazovatel'nogo foruma. Seliger, 27 avgusta 2014 goda. (2014). *Ministerstvo inostrannyh del Rossii* [Ministry of Foreign Affairs of Russia], [online]. Available at: http://www.mid.ru/brp_4.nsf/0/7cf0446902f9584544257d4 10064d1c8 [Accessed 11 February 2019].