УДК 327.8:15

А. П. ДЕМАРТИНО

ІНТЕРНЕТ В РОСІЙСЬКІЙ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ ВІЙНИ

Досліджуються особливості російських підходів до використання мережі Інтернет в умовах інформаційної війни та нового позиціонування Росії на зовнішній арені. Аналізуються ключові мотиви і фактори, що визначають російське бачення ролі і місця кібервійни в рамках зовнішньої агресії Кремля. Систематизовано документальні та доктринальні основи російської концепції інформаційної війни.

Ключові слова: *інформаційна війна, кібератаки, «доктрина Герасимова», гібридна війна.*

Демартино А. П. **Интернет в российской концепции информационной войны**

Исследуются особенности российских подходов к использованию сети Интернет в условиях информационной войны и нового позиционирования России на внешней арене. Анализируются ключевые мотивы и факторы, определяющие российское видение роли и места кибервойны в рамках внешней агрессии Кремля. Систематизированы документальные и доктринальные основы российской концепции информационной войны.

Ключевые слова: *информационная война, кибератаки, «доктрина Герасимова», гибридная война.*

Demartyno Andrii**. Internet in the Russian concept of information warfare**

In this article, the peculiarities of Russian approaches to the use of the Internet in the conditions of information warfare and the new positioning of Russia in the foreign arena are studied. The key motives and factors that determine Russia's vision of the role and place of cyberwar within the framework of the Kremlin's foreign aggression are analyzed. The documentary and doctrinal foundations of the Russian concept of information warfare are systematized.

Key words: *information war, cyberattacks, «Gerasimov's doctrine», hybrid war.*

В умовах російської агресії проти України, що триває з 2014 року, Кремль надзвичайно активно використовує соціальні мережі та Інтернет в рамках інформаційної війни як однієї з

© *ДЕМАРТИНО Андрій Павлович* – кандидат історичних наук, докторант Інституту держави і права ім. В. М. Корецького НАН України

ключових стратегій, спрямованих на знищення нашої державності та деморалізацію українського суспільства.

Комплекс заходів, який реалізується російським керівництвом для вирішення своїх зовнішньополітичних завдань з використанням можливості Інтернету, можна визначити, як кібервійна.

У зв'язку з цим виникає нагальна і досить актуальна потреба у вивченні основних засад, мотивів, факторів і складових, що визначають російське бачення ролі й місця кібервійни в рамках зовнішньої агресії РФ. Все це має велике значення для забезпечення національної безпеки, зокрема для розробки відповідних методів захисту українських інформаційно-технічних і соціальних систем від інформаційного впливу противника.

Наукових праць, в яких досліджуються російські особливості ведення кібервійни в рамках інформаційного протиборства досить багато. Натомість Кремль постійно вдосконалює і розширює засоби і методи застосування своєї інформаційної зброї, що обумовлює необхідність постійного аналізу та систематизації його дій у кіберпросторі, ЗМІ та соціальних мережах. Зокрема, в публікаціях російських і західних дослідників[1] розглядаються основні підходи до питання ведення Росією інформаційної війни, залучення нею нових технологій і розширення існуючого арсеналу засобів ведення інформаційного протиборства.

Основна мета даної статті полягає в тому, щоб дослідити еволюцію російських підходів до використання соціальних мереж та Інтернету в рамках інформаційної війни та нового позиціонування Росії на зовнішній арені, а також проаналізувати ключові мотиви і фактори, що визначають російське бачення ролі і місця кібервійни в рамках зовнішньої агресії Кремля.

У західній літературі поширено вживання терміну «кібервійна» (Cyberwar або Cyberwarfare), утворений від слова cyber, що означає «пов'язаний з комп'ютерами та інтернетом», та слова «war, warfare», що означає «війна, воєнні дії». Так, експерти з безпеки уряду США Річард А. Кларк та Роберт Нейк у

своїй книзі «Кібервійна» дають таке визначення цьому поняттю – «дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування»[2]. В цілому західні фахівці розглядають кібервійну як окремий вид протиборства, що відбувається в Інтернеті або комп'ютерних мережах. Зокрема британський журнал Економіст описує кібервійну як «п'яту область війни, після землі, моря, повітря і космосу»[3].

На відміну від західних колег більшість російських теоретиків і практиків не розглядають кібервійну як окрему сферу протиборства, натомість концептуалізують в рамках більш широкого поняття – інформаційної війни, яка окрім операцій в комп'ютерних мережах, включає також електронні та медіа-війни, психологічні та інформаційні операції тощо. Так, дослідник Олександр Капто у відомій статті «Кібервійна: генезис і доктринальні межі» зазначає: «Кібервійна – один з нових видів війни, заснований на сучасних технологіях. Це не самостійний вид протиборства, кібервійна завжди є складовою частиною інформаційної війни, і в цілому виступає елементом повномасштабної військової кампанії, що включає як нещодавно виниклі, так і більш звичні способи боротьби. Кібервійна не існує поза традиційною війною, хоча конкретні кібероперації можуть проводитися (і нині проводяться в багатьох регіонах планети)»[4].

Такий більш широкий підхід обумовлений тим, що переважна частина російських фахівців і урядовців переконані, що Москва перебуває в постійній, екзистенційній боротьбі з внутрішніми та зовнішніми силами, які прагнуть кинути виклик її політичній владі. Зокрема, секретар Ради Безпеки РФ Микола Патрушев в своєму інтерв'ю на запитання кореспондента «Те, що відбувається на Україні – один з яскравих прикладів наслідків «кольорових революцій», інспірованих Заходом по всьому світу. Чи слід очікувати подібних дій стосовно Росії?» надав таку відповідь: «Ви маєте рацію, «кольорові революції» – це вже традиційний інструмент політики окремих країн, націленої на руйнування державності і втрату суверенітету під при-

водом демократизації. Насправді ж країна, де відбувається «кольорова революція», майже завжди занурюється в хаос і переходить під зовнішнє управління. Західні технологи не відмовилися від планів реалізації «кольорових сценаріїв» і в нашій країні. При цьому вони не соромляться у виборі методів нагнітання протестних настроїв – від спекуляції на тимчасових труднощах соціально-економічного характеру до відвертої брехні»[5].

Відповідно владна еліта Росії розглядає Інтернет і вільний потік інформації, яку він породжує, як безпекову загрозу, тобто таку, що має більший пріоритет і тенденцію до стратегічного та довгострокового характеру.

Це цілком простежується і в історичній ретроспективі. Адже до 2007-2008 років, вище російське політичне керівництво, спочатку в особі Бориса Єльцина, а потім і Володимира Путіна, було переважно сконцентровано на внутрішньополітичних аспектах консолідації власної влади. Зокрема, у 1999-2003 роках відбувся погром недержавних ЗМІ в рамках зачищення російського інформаційного поля від впливу олігархів, що завершилося так званим «одержавленням медіа» в Росії, які фактично опинилися під тотальним контролем «путінського режиму».

Якісно нові зміни у політиці Кремля в інформаційній сфері були започатковані відомою промовою Президента Росії Володимира Путіна на Мюнхенській конференції з безпеки 2007 року. По суті було заявлено нове позиціонування Кремля в міжнародній системі, обумовлене свідомою відмовою як від інтеграції у систему західних демократій, так і від розбудови в Росії демократичної правової держави.

Після Мюнхена «путінському режиму» вдалося не тільки поставити під повний контроль практично усі ЗМІ РФ, а й створити державну машину тотальної пропаганди та інформації, яка повністю формує інформаційний порядок денний російського суспільства. Варто зазначити, що «нова цензура» не просто виключає з інформаційної повістки реальні події. Вона підміняє їх імітаційними повідомленнями, які повинні створювати у гля-

дачів відчуття залежності від головного героя сюжетів. Щоденно на різних рівнях через телевізійні, друковані та інші ЗМІ Кремль цілеспрямовано «промиває мізки» росіян і формує потрібні настрої населення. Система пропаганди працює таким чином, щоб значна більшість суспільства завжди підтримувала відповідні ідеї влади незалежно від того, яку власну думку ця більшість мала вчора або має сьогодні.

З початку 2010-х рр. ця система зазнала певної еволюції і розширила зону свого впливу – з традиційних ЗМІ на «нові медіа», з мовного сектора – в інтерактивний, з внутрішньої повістки – в міжнародну[6].

З 2007 року ескалації конфліктів Росії з іншими країнами почали збігатися у часі з кібератаками на опонентів російського уряду. Відбувалися вони за схожим сценарієм: паралельно з тим, як йшли військові дії, мітинги або переговори, невідомі люди проводили DDoS-атаки на державні сайти, зламували поштові скриньки політиків і їх сайти, викладали на них образливі зображення, а також передавали компромат близьким до російської влади ЗМІ. Останні інтенсивно розкручували «скандальні» сюжети, з приводу яких потім з'являлися офіційні реакції російського МЗС, Держдуми, Президента тощо.

Вперше це сталося з Естонією навесні 2007 року. Національна дискусія навколо перенесення з центру Таллінна на військове кладовище пам'ятника радянським солдатам, загиблим у Другій світовій війні, переросла в міжнародний конфлікт. Саме тоді російські хакери атакували сайти президента, прем'єр-міністра, держустанов, банків – вони перестали на кілька тижнів відкриватися через DDoS-атаки. У доповіді Elliot School of International Affairs ці атаки назвали «першою світовою кібервійною»[7].

У 2008 році історія повторилася під час військового конфлікту з Грузією, протягом якого Росія активно використовувала кібератаки та фейкові новини для впливу на грузинські структури влади та суспільство[8]. З 2010-х подібні атаки стали відбуватися ще частіше – і для них вибиралися все більш серйозні цілі. В різному ступені їх відчули на собі Україна в

2014 році, Німеччина в 2015 році, Сполучені Штати в 2016 році. Під прицілом були і Організація з безпеки і співробітництва в Європі (ОБСЄ), НАТО, Європейський союз. Міжнародна редакція французького телеканалу TV5 також піддалася хакерській атаці через поширення інформації, яку Москва визнала негативною[9].

Нові інформаційні можливості були узагальнені та концептуалізовані на офіційному рівні. Відповідно до оновленої Військової доктрини Російської Федерації (2010), однією з особливостей сучасних військових конфліктів є «попередня реалізація заходів інформаційної війни з метою досягнення політичних цілей без використання військової сили, а згодом і в інтересах формування сприятливої реакції світової спільноти на використання військової сили»[10]. По суті визнавалося, що інструменти інформаційної війни можуть, фактично, бути використані до початку військових операцій з метою досягнення цілей держави без застосування сили або, якщо сила буде застосовуватися, то таким чином, щоб дезорієнтувати та деморалізувати супротивника та забезпечити, щоб держава могла виправдати свої дії в очах громадськості.

У кінці грудня 2011 р. Міністерство оборони представило документ під назвою «Концептуальні підходи щодо діяльності Збройних сил РФ в інформаційному просторі». Ключовою новинкою документа стало те, що цей простір вперше було віднесено до потенційних театрів військових дій і відзначено в якості однієї з основних загроз національної безпеки. В ньому зокрема зазначалося, що високі темпи розвитку інформаційних систем різного призначення, комп'ютерних мереж типу Інтернет та електронних ЗМІ призвели до формування глобального інформаційного простору. І поряд з сухопутним, морським, повітряним і космічним простором, інформаційне середовище в арміях найбільш розвинених країн стало активно використовуватися для розв'язання широкого кола військових завдань. Внаслідок уразливості інформаційно-комунікаційних систем від радіоелектронних та програмно-апаратних впливів у світі виникла і швидко поширюється інформаційна зброя,

що володіє «транскордонними атакуючими факторами, різко зросла роль інформаційної війни». Відповідно Російська Федерація, що стрімко розвивається шляхом інформатизації всіх сфер життєдіяльності суспільства, постала перед новою серйозною загрозою, що виходить з глобального інформаційного простору[11].

Крім того, істотним нововведенням стало те, що Москва розширила на цю сферу можливість, «в умовах ескалації конфлікту в інформаційному просторі», скористатися правом на індивідуальну або колективну самооборону з застосуванням будь-яких методів і засобів.

Суттєві новації були внесені в «Концепцію зовнішньополітичного курсу Російської Федерації» (2013 рік[12]), де мова йшла про принципову зміну політичного курсу РФ на зовнішній арені. Так, Кремль відмовився від інтеграції в західні структури, натомість взяв курс на збереження незалежності Росії і співпрацю з партнерами на Сході та Півдні. Мета приєднання російської національної економіки до світового ринку була замінена на забезпечення реіндустріалізації країни, що мала закласти основи російської економічної незалежності, і створити власну економічну асоціацію. Вакуум в ідеології зовнішньої політики Росії був заповнений ідеєю формування «російського миру» і пріоритетами захисту традиційних християнських цінностей[13].

Після «мюнхенської промови» та війни з Грузією російські експерти також почали адаптувати існуючі концепції інформаційної війни до нового політичного курсу Кремля. 15 жовтня 2008 року в російській газеті «Військово-промисловий кур'єр» була опублікована стаття «Система інформаційного протиборства», написана професором Дипломатичної академії МЗС Росії Ігорем Панаріним.

Аналізуючи наслідки вторгнення російських військ до Грузії, Ігор Панарін доходить висновку, що з інформаційної точки зору Росія програла цю війну, оскільки Захід не зрозумів і не підтримав фактичне захоплення нею двох регіонів іншої країни. Професор зазначає, що головною проблемою стала

«явна недооцінка ролі інформаційного протиборства сучасною російською політичною елітою в умовах посилення глобальної економічної та геополітичної конкуренції в світі»[14].

Відповідно для того, щоб Росія могла вигравати інформаційні війни, Ігор Панарін пропонує створити спеціальні організаційно-управлінські та аналітичні структури як для протидії інформаційній агресії, так і для розробки та проведення інформаційних операцій (оборонних і наступальних). Зокрема, він запропонував наступні кроки.

1. Створити єдиний державний орган, що буде координувати діяльність інформаційно-аналітичних підрозділів ключових відомств.

2. Створити зовнішньополітичний державний медіахолдинг (ВГТРК, Russia Today, «Голос Росії», «Маяк», РІА Новини і так далі), який доцільно підпорядкувати МЗС Росії.

Ігор Панарін зазначає, що Росії необхідно відновити свій потенціал механізму зовнішньополітичної пропаганди, який був ґрунтовно зруйнований в 90-і роки. Втім, він відзначив, що цей провал був усвідомлений російським керівництвом і з приходом до влади президента В. Путіна почалося поступове впевнене відновлення втрачених позицій. Ключовим кроком у цьому напрямку є створення в 2006 році супутникового телеканалу Russia Today.

3. Створити державний інтернет-холдинг з виробництва книг, відеофільмів, відеоігор тощо для активного поширення в мережі Інтернет.

4. Створити інформаційний антикризовий центр, що буде керувати інформаційними потоками через налагодження конструктивної співпраці із ЗМІ.

5. Сформувати систему інформаційної протидії, що включатиме ресурси як держави, так і великого бізнесу, інститутів громадянського суспільства.

6. Запустити мережу неурядових організацій Росії, що діють на території країн СНД, ЄС, США (за американською моделлю – в Росії діють численні американські неурядові організації, що фінансуються урядом США).

7. Організувати систему підготовки кадрів для ведення інформаційного протиборства.

Підсумовуючи свій аналіз і пропозиції, І. Панарін зазначив, що потрібно значно посилити фінансування програм інформаційного протиборства. Заходи інформаційного протиборства повинні фінансуватися за принципом головного пріоритету. Він наголосив, що сьогодні фінансування програм інформаційного протиборства більш важливе, ніж фінансування програм ядерного стримування. Інформаційна зброя є більш небезпечною для Росії, ніж зброя ядерна. І це необхідно визнати політичній еліті Росії[15].

На думку російських фахівців, які досліджують проблеми військових конфліктів, досягнення мети в війнах майбутнього буде неможливим без завоювання інформаційної переваги над противником. Так, старший науковий співробітник Військової академії Генерального штабу Збройних Сил РФ (ВАГШ), доктор військових наук Геннадій Нальотов вважає, що в сучасних умовах передові технології зруйнували класичний тип війни. Війни нової доби інформаційних та інших високих технологій за своїм характером будуть принципово відрізнятися від війн минулого століття[16].

Начальник кафедри військового мистецтва ВАГШ генерал-майор Сергій Кураленко в статті «Тенденції зміни характеру збройної боротьби у воєнних конфліктах першої половини XXI століття» зазначив, що розвиток інформаційних технологій призвів до значних змін в способах ведення війни і обумовив формування нового виду збройних сил – до створення кібервійськ. Зараз збройна боротьба має об'ємний характер і включає повітряно-космічну, морську, наземну і, найголовніше, нову сферу – інформаційну. А питання, де і в якій сфері буде вирішуватися результат війни і відповідно яка зі сфер буде визначальною, залежить від умов військових дій і протиборчих сторін[17].

У рамках законодавчих та доктринальних перетворень слід також згадати так звану «Доктрину Герасимова» – концепцію «війни нового покоління», яку представив начальник Головного

управління ВС Росії Валерій Герасимов у доповіді про гібридну війну в Академії військових наук у лютому 2013 року. Основні тези його доповіді були опубліковані в статті «Цінність науки в передбаченні» в газеті «Військово-промисловий кур'єр»[18].

В. Герасимов пише: «Самі поняття «правил війни» істотно змінилися. Зросла роль невійськових способів в досягненні політичних і стратегічних цілей, які в деяких випадках за своєю ефективністю значно перевершили силу зброї. Акцент у застосуванні методів протиборства зміщується в бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів, реалізованих із задіянням протестного потенціалу населення. Все це доповнюється військовими заходами прихованого характеру, в тому числі реалізацією заходів інформаційного протиборства і діями сил спеціальних операцій. До відкритого застосування сили, часто під виглядом миротворчої діяльності та кризового врегулювання, переходять тільки на якомусь етапі, в основному для досягнення остаточного успіху в конфлікті»[19].

Новація «доктрини Герасимова» полягає в тому, що інформаційна складова була виділена в якості одного з ключових місць в системі ведення нелінійних дій і стала, поряд з військовою міццю, однією із складових проведення гібридних операцій.

У своїй подальшій програмній статті «З досвіду Сирії», опублікованій у випуску газети «Військово-промисловий кур'єр» за 9 березня 2016 року, Валерій Герасимов особливо це підкреслює: «В той же час все більше очевидним є те, що розвиток засобів збройної боротьби є далеко не єдиною причиною вдосконалення форм і способів застосування угруповань військ і сил.

У сучасних конфліктах все частіше акцент у застосуванні методів боротьби зміщується в бік комплексного застосування політичних, економічних, інформаційних та інших невійськових заходів, реалізованих з опорою на військову силу. Це так звані гібридні методи. Їх зміст полягає в маніпуляції протестним потенціалом населення в поєднанні з іншими невійськовими засобами. Важливого значення при цьому набуває масо-

ваний, цілеспрямований вплив на свідомість громадян держав – об'єктів агресії за допомогою глобальної мережі Інтернет. Інформаційні ресурси стали одним з найефективніших видів зброї. Широке їх використання дозволяє в лічені дні розгойдати ситуацію в країні зсередини»[20].

Уже з урахуванням російського досвіду в Сирії В. Герасимов робить висновок, що поєднання традиційних і гібридних методів вже зараз є характерною рисою будь-якого збройного конфлікту. При цьому якщо другі можуть використовуватися і без відкритого застосування військової сили, то класичні бойові дії без гібридних – вже ні.

Таким чином, російська концепція «гібридної війни» – це сучасна цілісна стратегія 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» / посередників, роль яких раніше грали ЗМІ. Використовуючи кібератаки і так звані фальшиві облікові записи в соціальних мережах, або так званих ботів, як зброю, Росія розпалює існуючі релігійні, соціальні, етнічні та інші суперечності для того, щоб принести дезінформацію в новини країни-супротивника, поширити в ній пропаганду, замаскована під «альтернативні» новини RT і «Супутника» тощо і, як наслідок, подавити волю керівництва країни і населення та їхню здатність чинити опір агресії.

По суті російські теоретики і практики розробили гнучку стратегію застосування так званої «гібридної війни», що складається з таких взаємопов'язаних і взаємодоповнюючих елементів як: політичне рішення (визначення цілі/проблеми); інформаційний привід або кібератака (створення проблеми); залучення ЗМІ (розкрутка проблеми); реакція офіційних державних органів (вимога розв'язати певним чином проблемне питання); застосування військових підрозділів (збройних сил РФ, «зеле-

них чоловічків», «апалченців», «добровольців», приватних військових компаній тощо).

Черговість реалізації цих елементів може змінюватися або застосовуватися одночасно. Але відтепер керівництво кожної країни (міжнародної урядової чи нерядової організації) розуміє, що зіткнувшись з інформаційною атакою Росії, воно потенційно може отримати повний спектр зовнішньої агресії аж до застосування військових підрозділів.

Варто відзначити, що гібридні військові дії Росії також спираються на глибокий аналіз попередніх змін влади, що відбулися у багатьох країнах у рамках так званих «кольорових революцій», на багатий досвід діяльності хакерських і терористичних груп, на добре відпрацьовану систему пропаганди та маніпуляцій тощо.

З огляду на дату оприлюднення першої доповіді В. Герасимова і наступні дії Росії у Криму та на Донбасі, багато західних експертів схильні пов'язувати ці події і прямо вказують на застосування відповідної доктрини щодо України[21].

Проти Києва Москва застосувала практично максимальний набір засобів в рамках «доктрини Герасимова». Засоби, які використовують росіяни в цій війні, носять гібридний характер: використання соцмереж для формування громадської думки серед українського населення; поширення не правдивих або фейкових новин для пропаганди, що розпалює ворожнечу в національній культурі; ведення психологічної війни проти українських військових і суспільства; операції спецслужб; кібератаки; підривні дії і диверсії; підтримка збройного опору українській владі, включно з веденням активних бойових дій за участю збройних сил РФ і «гібридних військ» («добровольці», «апалченці», представники приватних військових компаній тощо).

Американський аналітик Майкл Голловей в статті «Як Росія перетворила соцмедіа в Криму на зброю» зазначав, що Крим став випробувальним майданчиком для російських інформаційних операцій, що продемонструвало світу потужність військового використання соціальних медіа. Автор

писав: «Під час анексії Криму, російський уряд витратив більш ніж 19 млн доларів на фінансування роботи 600 осіб, які постійно коментували статті, писали блоги і проводили діяльність в соціальних медіа. Їх метою було змінити думку громадськості та міжнародної спільноти, перекрити голоси дисидентів в онлайн медіа, створити враження, що населення підтримує анексію»[22].

Таким чином, можемо констатувати, що російський владний режим приділяє надзвичайно велику увагу інформаційній сфері, як одному з ключових чинників контролю та збереження політичної влади.

При цьому, Кремль виявляє високу ступень гнучкості і адаптивності в питанні вдосконалення механізмів контролю інформаційного поля, як всередині країни так і за її межами. Російськими фахівцями постійно відслідковується і впроваджується в роботу самі останні світові технології і наукові розробки.

Російська владна концепція контрою за станом громадської думки і впливу на неї має стратегічний і довгостроковий характер. На Заході, на відміну від Росії, питанню інформаційної безпеки тривалий час не приділялось належної уваги, аж до подій, пов'язаних зі спробами втручання «російських хакерів» в президентські вибори в США 2016 року.

Внутрішня ґенеза російської влади по формуванню підходів до питань роботи з інформаційною сферою мала декілька етапів.

До середини 2000-х років Кремль був переважно концентрований на внутрішньополітичних аспектах консолідації власної влади. Зачищення російського інформаційного поля від впливу олігархів призвело до погрому недержавних ЗМІ в рамках і так званим «одержавленням медіа». ЗМІ фактично опинилися під тотальним контролем «путінського режиму».

Наступний етап настав після економічного зміцнення Російської Федерації пов'язаного з високими цінами на енергоносії і новим позиціонування російським керівництвом місця та ролі Росії у світі.

Започаткований В. Путіним у Мюнхені у 2008 році новий курс призвів до переосмислення російських стратегії щодо інформаційної безпеки як всередині країни, так і назовні.

Наслідком цього стало побудова всередині РФ тотальної системи «нової цензури», що виключає з інформаційної повістки реальні події замінюючи їх імітаційними повідомленнями, так званими фейками.

Для зовнішньополітичних потреб російськими теоретиками і практиками була розроблена концепція інформаційної війни. Кібератаки на Естонію у 2007 році, а потім інформаційна та військова війна у Грузії (2008), Україні (з 2014), Сирії (з 2015), як і багато інших випадків свідчать про те, що Кремль веде інформаційний наступ на всіх стратегічних рівнях, практично у глобальному масштабі.

Очевидно, що Москва намагається враховувати усі особливості країни, проти якої ведеться регіональна інформаційна війна. Вона, як правило, вибудовується заздалегідь за рахунок підготовлених і продуманих інформаційних кампаній, для яких розробляються сценарії і комплексно залучається широкий спектр державних органів.

Зміни в інформаційних стратегіях російської влади знаходять своє достатньо повне відображення у різного виду офіційних документах – доктринах, концепціях. Головна новація, яка фіксується на державному рівні, це визнання інформаційного простору як самостійного і повноцінного театрів військових дій, для захисту якого Росія має використовувати всі доступні методи і засоби.

1. *Кантор А. С.* Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. 2013. Т. 83. № 7. С. 616; *Войны* и миры. Николай Патрушев: об Украине и США, кибератаках, Сирии и роли Совбеза в истории России // Российская газета. 18.05.2017. URL: https://rg.ru/2017/05/18/nikolaj-patrushev-ob-ukraine-i-ssha-kiberatakah-sirii.html; Туровский Д. Российские вооруженные киберсилы. Как государство создает военные отряды хакеров // Meduza. 7 ноября 2016. URL: https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily; *Blank, Stephen J.* Information Warfare a la Russe // Cyberspace: Malevolent

Actors, Criminal Opportunities, and Strategic Competition. – Phil Williams and Dighton Fiddner. Strategic Studies Institute and U.S. Army War College Press. August 2016. P. 219–220; *Мандро Изабель, Гибер Натали.* Новый арсенал фирмы «Россия». Цикл «Информационные войны Кремля» о том, как Москва разрабатывала и реализовала стратегию «гибридного» конфликта в информационной сфере и интернете. 07.03.2017. URL: «http://inosmi.ru/politic/20170307/238837275.html»; *Bratersky Maxim.* Transformation of Russia's Foreign Policy. 7 june 2014. URL: «http://eng.globalaffairs.ru/number/Transformation-of-Russias-Foreign-Policy—16706»; *Панарин И.* Система информационного противоборства // Военно-промышленный курьер. 2008. № 41 (257). URL: https://www.vpk-news.ru/issues/257; *Налетов Г. А.* К вопросу о разработке концепции нетрадиционных войн и вооружённых конфликтов // Вестник Академии военных наук. 2012. № 1. С. 31; *Кураленко С. В.* Тенденции изменения характера вооруженной борьбы в военных конфликтах первой половины XXI века // Военная мысль. 2012. № 11. С. 40–46; *Герасимов В. В.* Ценность науки в предвидении // Военно-промышленный курьер. 2013. № 8 (476). URL: «http://www.vpk-news.ru/articles/14632»; *Герасимов В. В.* По опыту Сирии // Военно-промышленный курьер. 2016. № 9 (624). URL: «http://vpk-news.ru/articles/29579»; *Martin N. Murphy.* Understanding Russia's Concept for Total War in Europe. The Heritage Foundation, 12.09.2016; *Sam Jones.* Ukraine: Russia's new art of war. Financial Times, 28.08.2014; *Holloway M.* How Russia Weaponized Social Media in Crimea. Realcleardefense. 10.05.2017. URL: «http://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html **2.** *Clarke Richard A., Knake Robert.* Cyber War. The Next Threat to National Security and What to Do About It. Harper Collins. 2010. P. 6. **3.** *Cyberwar:* War in the Fifth Domain // The Economist. 2010. URL: https://www.economist.com/leaders/2010/07/01/cyberwar?story_id=16481504&source=features_box1 **4.** *Kanto A. C.* Цит. работа. С. 616. **5.** *Войны* и миры. Николай Патрушев: об Украине и США, кибератаках, Сирии и роли Совбеза в истории России // Российская газета. 18.05.2017. URL: https://rg.ru/2017/05/18/nikolaj-patrushev-ob-ukraine-i-ssha-kiberatakah-sirii.html. **6.** *Василий Гатов.* Путин, марьиванна и «украинцы в телевизоре». От КПСС до Путина: каков был путь к новой цензуре и новой медиареальности в России. 10 февраля 2015. https://www.svoboda.org/a/26840571.html. **7.** *Туровский Д.* Российские вооруженные киберсилы. Как государство создает военные отряды хакеров. Meduza. 7 ноября 2016. URL: https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily. **8.** *Blan Stephen J.* Information Warfare a la Russe // Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition. – Phil Williams and Dighton Fiddner. Strategic Studies Institute and U.S. Army War

College Press. August 2016. P. 219–220. **9.** *Мандро Изабель, Гибер Натали.* Новый арсенал фирмы «Россия». Цикл «Информационные войны Кремля» о том, как Москва разрабатывала и реализовала стратегию «гибридного» конфликта в информационной сфере и интернете. 07.03.2017. URL: «http://inosmi.ru/politic/20170307/238837275.html». **10.** *Военная* доктрина Российской Федерации. 5 февраля 2010 года. URL: http://kremlin.ru/supplement/461. **11.** *Концептуальные* взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. 2011. URL: «http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle». **12.** *Концепция* внешней политики Российской Федерации (Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. (в соответствии с Указом Президента Российской Федерации от 30 ноября 2016 года № 640 утратила силу). URL: «http://www.mid.ru/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/122186». **13.** *Bratersky Maxim.* Transformation of Russia's Foreign Policy. 7 june 2014. URL: «http://eng.globalaffairs.ru/number/Transformation-of-Russias-Foreign-Policy—16706». **14.** *Панарин И.* Система информационного противоборства // Военно-промышленный курьер. 2008. № 41 (257). URL: «https://www.vpk-news.ru/issues/257». **15.** Там же. **16.** *Налетов Г. А.* К вопросу о разработке концепции нетрадиционных войн и вооружённых конфликтов // Вестник Академии военных наук. 2012. № 1. С. 31. **17.** *Кураленко С. В.* Тенденции изменения характера вооруженной борьбы в военных конфликтах первой половины XXI века // Военная мысль. 2012. № 11. С. 40–46. **18.** *Герасимов В. В.* Ценность науки в предвидении // Военно-промышленный курьер. 2013. № 8 (476). URL: http://www.vpk-news.ru/articles/14632. **19.** Там же. **20.** Герасимов В. В. По опыту Сирии // Военно-промышленный курьер. 09.03.2016. № 9 (624). URL: «http://vpk-news.ru/articles/29579». **21.** *Martin N. Murphy.* Understanding Russia's Concept for Total War in Europe. The Heritage Foundation, 12.09.2016; *Sam Jones.* Ukraine: Russia's new art of war. Financial Times, 28.08.2014. **22.** *Holloway M.* How Russia Weaponized Social Media in Crimea. Realcleardefense. 10.05.2017. URL: «http://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html.

***Demartyno Andrii*. Internet in the Russian concept of information warfare**

In this article, the peculiarities of Russian approaches to the use of the Internet in the conditions of information warfare and the new positioning of Russia in the foreign arena are studied. The key motives and factors that determine Russia's vision of the role and place of cyberwar within the framework of the Kremlin's foreign aggression are analyzed. The documentary and doctrinal foundations of the Russian concept of information warfare are systematized.

In the context of Russian aggression against Ukraine, which lasts from 2014, information warfare is one of the key Kremlin's strategies aimed at the destruction of statehood and the demoralization of Ukrainian society. In connection with this, there is an urgent and very urgent need to study the main motives, factors and components that determine the Russian vision of the role and place of information warfare within the framework of foreign aggression of the Russian Federation. All this is of great importance for ensuring national security, in particular for developing appropriate methods for protecting Ukrainian information and technical and social systems from the enemy's informational influence. The main purpose of this article is to investigate the evolution of Russian approaches to information warfare in the face of Russia's new positioning in the foreign arena, as well as to analyze key motives and factors that determine Russia's vision of the role and place of the information warfare within the framework of the Kremlin's foreign aggression.

Unlike Western colleagues, most Russian theorists and practitioners do not regard cyberwar as a separate controversy, but instead conceptualize it as part of a broader notion of information warfare that includes electronic and media wars, psychological and information operations, besides operations in computer networks. etc. Such a broader approach is due to the fact that the vast majority of Russian specialists and government officials are convinced that Moscow is in a constant, existential struggle with internal and external forces that seek to challenge its political power. Accordingly, Russia's ruling elite is considering the Internet and the free flow of information it generates as a security threat, that is, having a higher priority and a tendency towards a strategic and long-term nature.

Qualitatively new changes in the Kremlin's policy in the information sphere were initiated by Putin's famous speech at the Munich Security Conference of 2007. In essence, the Kremlin's new positioning in the international system was declared, due to a deliberate denial of both integration into the system of Western democracies, and the development of a democratic state under the rule of law in Russia. After Munich, the Putin regime managed not only to put almost all Russian media out of control, but also to create a state machine of total propaganda and information that completely forms the information agenda of Russian society. It should be noted that the «new censorship» does not simply exclude real events from the newsletter. It replaces them with imitation messages, which should create a feeling of dependency on the main character of the plot. Every day, at various levels through television, print and other media, the Kremlin deliberately flushes the brains of Russians and shapes the mood of the population. The propaganda system works in such a way that a large majority of the society has always supported the relevant ideas of the authorities, regardless of what their majority thought was yesterday or today.

Key words: information war, cyberattacks, «Gerasimov's doctrine», hybrid war.