**ІНФОРМАЦІЙНА БЕЗПЕКА В ЛАТИНСЬКІЙ АМЕРИЦІ**

Багато латиноамериканських компаній не готові захищати дані й відстають від своїх міжнародних колег щодо прийняття кіберстрахування. Кіберзлочинність становить величезну загрозу для їхньої економіки. Держави відчувають стрімке зростання цифрових технологій. Хоча це може розглядатися як позитивна зміна – воно відкриває багато можливостей і для кіберзлочинців.

У цій галузі є лише кілька країн, які прийняли законодавство про кібербезпеку. Існують також підприємства, які піклуються про кібербезпеку, вони повільно виходять на ринок країн Латинської Америки. Ізраїльські компанії є великими постачальниками послуг урегіоні.

Шпигунство – одна зі стратегій, що передбачає втручання у внутрішню політику держав Латинської Америки. Однак є й інші стратегії, які видаються «непрямими», а, утім, можуть надто впливати на політичні сценарії, як-от кібербезпека на виборах.

Три з п‟яти латиноамериканських підприємств зазнали кібератак. Найвищий показник виявився в Перу, за ним – Мексика, Аргентина, Бразилія та Колумбія. Зазвичай, головною причиною є шкідливий код. Однак у 2018 р. вірус-вимагач забрав корону собі. Зростання кількості злочинів, що вимагають викупу, пов‟язане з тим, що для зловмисників це найдешевший спосіб просування й сприяння нападам.

Для запобігання майбутнім масовим атакам країни Латинської Америки та Карибського басейну почали створювати власні стратегії кібербезпеки. Чилі й Мексика опублікували свої стратегії кібербезпеки у 2017 р. та врахували широкий спектр аспектів кіберзлочинності для подолання ризиків кібербезпеки задля створення всеосяжної системи.

У разі кібербезпеки, як і в усіх галузях, співпраця відіграє принципову роль. Латиноамериканські країни співпрацюють для створення кращих зв‟язків щодо кібербезпеки. Однією з платформ, які використовувались для побудови таких партнерств, був XIII саміт Тихоокеанського альянсу, що відбувся в Мексиці.

Організація американських держав уже понад 10 років займається однією з основних проблем кібербезпеки та кіберзлочинності, заохочуючи й підтримуючи роботу держав-членів щодо посилення їх спроможності стосовно захисту людей, економіки та критичної інфраструктури регіону від кіберзлочинності й інших кібератак чи інцидентів.

**Ключові слова:** інформаційний простір, інформаційна безпека, кібератака, кібербезпека, кіберзлочинність, Латинська Америка, Бразилія, Мексика, Чилі.

УДК 316.485.26:316.776.23(470)

**Тихомирова Євгенія,**
доктор політичних наук, професор,
Східноєвропейський національний університет імені Лесі Українки,
Луцьк, Україна, teb53@ukr.net
https://orcid.org/0000-0002-5017-5875

# РОСІЙСЬКА ІНФОРМАЦІЙНА ВІЙНА: ТЕОРЕТИЧНІ ТА ПРАКТИЧНО-ПРИКЛАДНІ АСПЕКТИ

*У статті розглянуто проблему наростання інформаційної війни, що виникла внаслідок агресивної політики Росії та створила небезпеку як сучасному європейському, так і українському інформаційному простору. Посилаючись на аналіз результатів наукових досліджень, за допомогою яких вивчались окремі теоретичні та практично прикладні аспекти цієї війни, говоримо про сутність досліджуваної проблеми й потребу її розв'язання.*

*Мета даної публікації – 1) проаналізувати термін «російська інформаційна війна» (трактується як комплекс заходів, здійснюваних урядовими та неурядовими організаціями Росії, передусім в інформаційному просторі України й Росії, інших країн світу); 2) виокремити місце інформаційної війни в російській геополітичній доктрині, котра розглядається як система офіційно прийнятих у державі поглядів на розвиток світових процесів, міжнародну систему безпеки, утвердження геополітичних інтересів і пріоритетів РФ у сучасному світі, їх реалізація та захист; 3) охарактеризувати особливості російських військ для «інформаційних операцій», спеціальних підрозділів для ведення інформаційної боротьби в*

*Інтернеті; 4) діяльність російської фабрики тролів у Санкт-Петербурзі (ідеться про контору під назвою «Агентство інтернет-досліджень», що цілодобово працює в Петербурзі); 5) дослідити проблеми запобігання дезінформації Кремля.*
***Ключові слова:*** *інформаційна війна, дезінформація, російські війська для «інформаційних операцій», російська геополітична доктрина, російська фабрика тролів.*

## 1. ВСТУП

**Постановка наукової проблеми та її значення.** Актуальність проблеми, яку досліджуємо в цій статті, зумовлено наростанням інформаційних загроз, що створили небезпеку сучасному європейському та українському інформаційному простору внаслідок агресивної інформаційної політики Росії.

Як відомо, поняття «інформаційна війна» увів у науковий обіг американський дослідник М. Маклюен, який проголосив тезу «Істинно тотальна війна – це війна за допомогою інформації» [16]. На його думку, на сучасному етапі економічні зв'язки й відносини все більше набувають форми обміну знаннями, а не товарами. А засоби масової комунікації саме є новими «природними ресурсами», що збільшують багатства суспільства. Тобто боротьба за капітал, простори для збуту відходять на другий план, а головним зараз стає доступ до інформаційних ресурсів, знань, що приводить до того, що війни ведуться більше в інформаційному просторі та за допомогою інформаційних видів озброєнь [9].

**Аналіз останніх досліджень і публікацій.** Існує велика кількість українських досліджень та публікацій на тему російської інформаційної війни проти України й застосування під час її ведення новітніх технічних можливостей та маніпулятивних технологій. Серед них – праці М. Бучина і Ю. Курус, І. Валюшко, Ю. Горбань, Є. Магди, Я. Малика, В. Панченко, Г. Сасина та Т. Черненко [3; 4; 6; 17; 8; 9; 12; 13; 15].

**Мета публікації.** Метою статті є спроба проаналізувати термін «російська інформаційна війна», виокремити місце інформаційної війни в російській геополітичній доктрині, охарактеризувати особливості російських військ для «інформаційних операцій», діяльність російської фабрики тролів у Санкт-Петербурзі та проблеми запобігання дезінформації Кремля.

**Методика дослідження.** В основу методології дослідження покладено інституціоналізм. Російську інформаційну війну трактовано нами як комплекс заходів, здійснюваних урядовими й неурядовими організаціями Росії, передусім, як в інформаційному просторі України та Росії, так і інших країн світу.

## 2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Почавшись у часи розпаду СРСР, російська інформаційна війна проходить протягом усієї незалежності України. Особливо інтенсивно вона почалася проти Майдану наприкінці 2013 р., перетворившись у масштабну гібридну війну з уведенням російських військ на територію Криму й Донбасу. Інформаційна війна путінської Росії проти України призвела до того, що більшість опитаних росіян готові воювати з українцями. Вірусом ненависті заражені насамперед молоді люди, які ніколи не були в Україні та не мають контактів із її громадянами. Старших людей лякають «бандерівцями-головорізами, які прийшли до влади». Це результат планомірної тотальної брехні, що розробляється ідеологами Кремля, транслюється по телебаченню. Щороку Росія витрачає проти України на інформаційну війну до 4 млрд дол., В. Філіпчук на «круглому столі» на тему «Як виграти інформаційну війну?» зазначив, що Росія веде структуровану інформаційну війну, що є *складовою частиною геополітичної доктрини РФ* та її гібридної війни [7].

«Доктрина РФ – це система офіційно прийнятих у державі поглядів на розвиток світових процесів, міжнародну систему безпеки, утвердження геополітичних інтересів і пріоритетів РФ у сучасному світі, їх реалізація й захист» [5]. До правової бази геополітичної доктрини РФ потрібно відносити конституцію РФ, що передбачає прийняття федеральних законів, інших нормативних правових актів країни, що регулюють діяльність федеральних органів державної влади у сфері зовнішньої та внутрішньої політики й функціонування системи правового захисту національних інтересів, Воєнну доктрину, Стратегію національної безпеки РФ, Доктрини інформаційної безпеки 2000 і 2016 рр., норми міжнародного права й міжнародні договори країни. Провідний геополітичний інтерес РФ у контексті

геополітичної доктрини – збереження та безпечний розвиток світових цивілізацій, народів і держав у цілому.

Як зазначено у Воєнній доктрині РФ, намітилася тенденція зміщення військових небезпек і воєнних загроз в інформаційний простір та внутрішню сферу РФ. До основних зовнішніх військових загроз поряд з іншими віднесено «використання інформаційних та комунікаційних технологій у військово-політичних цілях для здійснення дій, що суперечать міжнародному праву, спрямованих проти суверенітету, політичної незалежності, територіальної цілісності держав і становлять загрозу міжнародному миру, безпеки, глобальної й регіональної стабільності». А до внутрішніх військових небезпек входять «діяльність з інформаційного впливу на населення, передусім на молодих громадян країни, що має на меті підрив історичних, духовних і патріотичних традицій у сфері захисту Вітчизни»[5].

За своїм призначенням, Доктрина інформаційної безпеки є документом стратегічного планування у сфері забезпечення національної безпеки поряд зі Стратегією національної безпеки РФ. Крім того, вона слугує основою для формування державної політики в галузі забезпечення інформаційної безпеки. Нова редакція Доктрини інформаційної безпеки РФ [11] визначає пріоритети безпеки держави в інформаційній сфері, серед яких – застосування інформаційних технологій в інтересах збереження культурних, історичних та духовно-моральних цінностей, що може означати створення нових і підтримку наявних інформаційних джерел (радіостанцій, друкованих й електронних видань, сайтів) із відповідним тематичним наповненням; залучення різних організацій і наукових установ (у т. ч. приватних) для розробки та виробництва інформаційних, програмних й електронних продуктів у державних цілях; розвиток каналів доведення інформації до російської та міжнародної громадськості про офіційну позицію Росії, що на практиці означає збільшення фінансування контрольованих Кремлем телевізійних каналів, друкованих й електронних засобів інформування; використання Росією з метою реалізації своєї політики суб'єктів міжнародної інформаційної політики із залученням міжнародних організацій. Ще одним важливим моментом Доктрини є наявність у силових структурах Росії, а також в «інших військових формуваннях й органах *сил і засобів інформаційного протиборства*» [10, 11].

Сьогодні традиційні концепції ведення війни набувають глибоких змін. На зміну стратегіям ведення війни на виснаження та знищення приходять концепції непрямих дій, гібридної війни, стратегічного паралічу й інші, які враховують нові фактори уразливості сторін. У цих концепціях виділяються три сфери ведення війни: фізична, ментальна і моральна. За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Реалізація національних інтересів в інформаційній сфері спрямована на формування безпечного середовища оборони достовірної інформації й стійкої розбіжності інформаційної інфраструктури задля забезпечення конституційних прав і свобод людини й громадянської безпеки. Сучасні інформаційні технології дають змогу державам реалізовувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів.

Головною особливістю Воєнної доктрини (ВД) РФ 2014 р. є визначення місця інформаційної війни в домінуючих позиціях сучасного воєнного протистояння. Росія визнала, що інформація – це зброя, якою досягаються перемоги. Поряд із традиційними засобами ураження інформаційна зброя отримала визнання російського військового й політичного керівництва. Величезну увагу приділено інформаційному впливу через Інтернет «вплив у глобальному інформаційному просторі на противника, на всю глибину його території». Із цією метою в російських силових структурах створено *спеціальні підрозділи для ведення інформаційної боротьби в Інтернеті*, аналог американських кіберкоманд (Cyber Command), підвідомчих Міноборони США, що займаються військовими кіберопераціями й захистом американських комп'ютерних мереж. Їхню діяльність спрямовано на програмно-комп'ютерний захист і проникнення в закриті інформаційні мережі інших держав. Характерно, що, наголошуючи на загрозах від НАТО, ВД РФ 2014 р. не розглядає нарощування збройної могутності східними сусідами РФ. Фахівці говорять про неприкриту однобокість в оцінці воєнних загроз, оскільки до уваги не взято територіальні претензії та воєнні приготування Японії, а також створення інфраструктури Китаєм уздовж російського кордону.

У Збройних силах РФ у 2017 р. сформовано новий вид військ – *«війська інформаційних операцій»*. Аналітики вказували, що основними завданнями російських кібервійськ стануть «обробка інформації,

що надходить ззовні, а також боротьба з кіберзагрозами»; кожен, хто працює в ротах, повинен пройти лінгвістичну підготовку і вивчити англійську мову. Їхня головна мета – займатися контрпропагандою. Про це розповідав у свій час глава Міністерства оборони Росії С.Шойгу під час виступу в Державній думі РФ. «Сформовано війська інформаційних операцій, які є більш ефективними та сильнішими», – заявив він, відповідаючи на питання щодо необхідності відновити роботу управління, яке б мало займатися пропагандою. «Пропаганда – це не просто провокативна інформація. Вона має бути розумною, грамотною, ефективною та конкретною», – наголосив міністр [14]. Вважають, що першим, хто заговорив про необхідність створення в російських збройних силах кіберкомандування, був віце-прем'єр-міністр Д. Рогозін. Це було ще в березні 2012 р. У той самий час на сайті Міністерства закордонних справ Російської Федерації з'явився розділ, у якому нібито зовнішньополітичне відомство публікуватиме виявлену неправдиву інформацію, яку було скеровано проти Росії. Як відомо, на сьогодні РФ веде інформаційну війну проти всієї Європи, а не лише проти України.

Армія США видала «*Посібник із російської військової справи нового покоління*» (*Russian New Generation Warfare Handbook*), призначений для підвищення інформованості американських військових про тактику Росії в гібридній війні. Посібник опубліковано в грудні 2016 р. для внутрішнього користування, але він не є засекреченим. Авторами книги вказано Армію США та Групу з асиметричної війни. У керівництві вивчено російську гібридну військову тактику, що застосовувалася в Криму й на Донбасі. «Поки американська армія билася в Іраку та Афганістані, вона досягла найвищого тактичного рівня протиборчої сили нашої ери. Однак вороги Америки не відпочивали. Росія спостерігала трансформацію американської армії та почала трансформацію своєї власної», – ідеться в передмові до видання[18].

У цьому посібнику констатовано, що під час грузинської й української криз Росія розробила новий підхід до своїх операції, які широко називають російською війною нового покоління. Російські інформаційні операції спеціально орієнтовані на сегменти супротивника, які реагують на російські наративи. Це змушує деяких місцевих жителів боротися за обіцяне російською стороною майбутнє. Фактично кримські групи самооборони та сепаратисти на сході України, котрі борються за «Новоросію», є прикладами цього. Інформаційні операції (ІО) ключові у військовій доктрині Росії. Автократична структура Росії означає, що їхні зусилля ІО однозначно вкладено з тактичного до стратегічного рівня. Певні ключові теми (захист від корупції, західні цінності, захист російської мови й т. ін.) є базою для російських повідомлень. Українські солдати отримували текстові повідомлення на їхні телефони з погрозами проти їхніх сімей і точну інформацію про місцезнаходження сім'ї. Така тактика чинить надзвичайно негативний психологічний вплив на молодих солдатів, котрі перебувають поза прямими контактами зі своїми близькими.

Як зазначають експерти, це новий рід військ, що підпорядковується начальнику військ зв'язку. Вони діють в інформаційному просторі, примушуючи протистояти в інформаційних мережах управління військами й зброєю. Зрозуміло, що в цьому випадку вони використовують усі засоби радіоелектронної боротьби, які є. За даними Zecurion, Росія вступає в топ-5 країн за чисельністю та фінансованістю кібервійськ. Основними напрямами діяльності кібервійськ у Zecurion називаються шпіонаж, кібератаки й інформаційні війни, які «включають різні засоби впливу на настрої та поведінку населення країн». При цьому, чим більше розвинена країна, тим вразливіша вона для кібератак.

«Залежність різних пристроїв й обладнання від Інтернету буде тільки зростати. У результаті, збільшиться вразливість окремих користувачів, їхніх гаджетів, машин, а також системних й інфраструктурних країн [19].

Аналітики вважають, що створена структура займеться «потужними геополітичними аналізами, які виявлятимуть напрями інформаційних ударів: наступальних, оборонних, об'єкти цих ударів, готових контрударів». Тепер потрібно зробити командуючих елементами операції, штаб для їхніх організацій. Усе відбувається, як на звичайній війні. Це можуть бути великі аналітики, відомі представники журналістського співтовариства. Вважають, що в таких спецслужб є кілька напрямів: первинне – чисто пропагандистське (пропаганда та контрпропаганда), інші – чисто оперативні, щоб відключити увагу противника або щоб дати недостовірну інформацію. Особливість таких військ у тому, що вони є саме в армії, відносять до розвідувального управління[18].

Значну частину постів і коментарів на Інтернет-форумах стосовно політики залишають професійні тролі, які отримують за участь у дискусіях зарплату. Найвідоміша *«фабрика тролів»* – контора під

назвою «*Агентство інтернет-досліджень*», – цілодобово працює в Петербурзі. «Кремлеботи», «російські Тролі», «ольгінські Тролі» – ці та інші назви міцно закріпилися за фейковими акаунтами в соціальних мережах, що проводять російську пропаганду на просторах Інтернету. На перший погляд, вони мало відрізняються від реальних людей, такої собі «диванної сотні росіян», проте насправді «кремлеботи» є зброєю в гібридній війні: впливають на суспільну думку, утручаються в хід виборів, підтримують сепаратистські референдуми, поширюють ідеї «руського світу» та зводять нанівець невигідні Кремлю дискусії – як опозиційні, так і провладній.

Це справжня фабрика, де існують виробничі норми, під час виконання норми ти заробляєш 45 тис. А норма – це 135 коментарів за зміну, що триває 12 год. Там є ще відділ «Живого журналу», відділ новин, відділ, де роблять всякі картинки, демотиватори, відділ, де роблять відео. У кожного – свій кабінет, столи з комп'ютерами, особливо там по кабінетах не «шастає» ніхто, усі сидять на своїх місцях. Існує денна й нічна зміна – два дні через два. Спеціальні люди на певному форумі пишуть якусь новину, а завдання тролів – її коментувати. Причому коментується це таким чином: тролі поділено на трійки, один із них – «злодій», тобто той, який пише, що нібито не згоден із тим, що написано на цьому форумі, лає владу, щоб надати якусь достовірність тому, що відбувається. Решта двоє вступають у дискусію з ним: ні, ви не маєте рації, усе абсолютно правильно. Причому один повинен забезпечити якийсь коментар картинкою, що підходить за змістом, а інший – посиланням на свою правоту: лиходій, картинка, посилання. Коментар повинен бути обсягом не менше ніж 200 знаків. Головне завдання фабрики – писати на відвідувані форуми, зокрема на форуми ідеологічних ворогів. Тема України превалює, тому особливу увагу «тролів» прикута до України. Вважають, що основною метою діяльності «Агентства Інтернет-досліджень» є поширення дезінформації про події у світі, зокрема в Україні та США, «дискредитувати Україну й просто негативно висловлюватися про українців. Є відділ української мови, відділ англійської мови, окремі люди працюють у соціальних мережах, зокрема на Фейсбуці. Оскільки політолог не може охопити всю картину світу, тут дається завдання – писати про це. А як писати – неважливо, хвалити або лаяти, головне, вставляти це ключове слово – тег. Потім увели щось типу політінформації, тобто заходить юнак, який на порядок денний каже, про що писати, щоб трошки хоча б розкрити тему. У цього хлопця рівень украй низький, тому виглядає все абсурдно. До речі, був іспит з ідеології. Там ставлять 15–20 питань, на які треба відповісти. Той, хто не відповідає, перездає, хто взагалі нездатний – того звільняють [1].

Дослідники стверджують, що десь за 8 років у датасеті з «Фабрики тролів» маємо 774 957 твітів про Україну, які згенерували 1369 акаунтів. До анексії Криму твіттер-боти майже не проявляли активність. Більш масово акаунти з вибірки стали твітити вже в кінці травня 2014-го. Наступні півроку кількість твітів не падала нижче ніж 115 на день. Справжній «твіттер-шторм» відбувся 18 липня 2014 р. – на наступний день після катастрофи літака МН-17. У той день акаунти «натвітили» понад 44 000 повідомлень, а на наступний – понад 25 000. Тоді 297 акаунтів просували інформацію про нібито винуватість України у збитті Боїнгу за допомогою хештегів #ПровокацияКиева (22,3 тис. згадок), #КиевСбилБоинг (22,1 тис.) та #КиевСкажиПравду (21,9 тис.). Більше ніж 200 акаунтами керували централізовано. Крім того, що сам твіттер пов'язує всі акаунти з датасету з «Агентством Інтернет-досліджень». Протягом липня спостерігали дивну активність кількох клієнт-сервісів для роботи з твіттером. Наприклад, за допомогою програми, яка має маркування «twisofter», твітили лише протягом 16–19 липня 2014 р. Найбільше публікацій зроблено 18 та 19 липня – 19,3 та 11,2 тис. твітів (або 43 % і 40 % від загальної кількості у цей день). Така ж історія із сервісом із маркуванням «token_app». Жодної згадки про ці сервіси в пошукових системах не знайдено, а отже, існує ймовірність, що ці клієнт-сервіси створено лише під конкретне завдання [2].

Аналітики зазначають, що дії України щодо нейтралізації інформаційних загроз із боку Росії треба виконувати на трьох рівнях: перший – геополітичний (полягає у впливі на інформаційного агресора та обмеженні інтенсивності й сили його нападу); другий – стан, що охоплює захист цілісності, ефективності та дієздатності системи управління, інформаційної інфраструктури, інформаційних ресурсів; третій – рівень громадськості, спрямований на захист стабільності й послідовності розвитку соціальних та політичних відносин, свідомості громадян, цілісності кожної людини.

Серед механізмів протидії інформаційній війні Росії проти України дослідники виокремлюють дві групи заходів – нормативно-правові й інституційні. До першої відносять законодавчі акти України, серед яких провідну роль у протидії інформаційній агресії Росії відіграє Доктрина інформаційної

безпеки України. Серед другої групи механізмів – державні та недержавні інституції, діяльність яких спрямовано на формування й реалізацію інформаційної безпеки України, а також міжнародні структури, діяльність котрих націлено на нейтралізацію інформаційного впливу з боку Росії. Протидіяти впливу в Україні дезінформації Кремля мають насамперед державні інститути. Серед вітчизняних інституційних механізмів протидії російській інформаційній важливе місце, на думку науковців, відведено Раді національної безпеки і оборони України, Кабінету Міністрів України, Міністерству інформаційної політики України, Міністерству закордонних справ України, Міністерству оборони України, кіберполіції та ін. [3]

Значну увагу потрібно звертати на такі механізми протидії інформаційній війні Росії проти України, як заборона російських сайтів і соціальних мереж, а також запровадження квот на українську мову в мас-медіа. Насамперед, через створення єдиного центру протидії російської пропаганди в соціальних мережах, що об‟єднав би урядові й громадські організації. Наступний крок полягає в широкому інформуванні користувачів соціальних мереж щодо інформаційної «гігієни», методології виявлення, ідентифікації російських тролів. Також доцільним було б створення єдиного обліку ідентифікованих «кремлеботів» та спеціальних програм і додатків, які б допомагали ідентифікувати «тролів» серед користувачів. Активна співпраця з менеджментом самих соціальних мереж у площині протидії «тролям» сприятиме їх швидкому блокуванню. Одним із найважливіших інструментів у боротьбі з діяльністю Росії в соціальних мережах є активна контрпропаганда на державному рівні.

## 3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, наростання російської інформаційної війни здійснювалося внаслідок агресивної політики Росії, що створила небезпеку як на сучасному європейському, так і українському інформаційному просторі. Інформаційна війна є важливою складовою частиною російської геополітичної доктрини, яка забезпечила геополітичні інтереси й пріоритети РФ у сучасному світі, їх реалізацію та захист. Для її реалізації створено російські війська для «інформаційних операцій» як спеціальні підрозділи для ведення інформаційної боротьби в Інтернеті. Важливу роль у цій боротьбі відіграє й діяльність російської фабрики тролів у Санкт-Петербурзі, що існує як контора під назвою «Агентство інтернет-досліджень» і цілодобово працює в Петербурзі. Фахівці пропонують нейтралізувати інформаційні загрози з боку Росії на трьох рівнях: геополітичному, рівні ефективності та дієздатності системи управління, інформаційної інфраструктури, інформаційних ресурсів; а також на рівні громадськості, свідомості її громадян і цілісності кожної людини.

Перспективи подальших досліджень можуть бути пов‟язані з вивченням правових засад ведення інформаційної війни та особливостей її протікання в різних країнах Європи та світу.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. «Кремлеботи» як інструмент російського впливу в світі. URL: https://spa.ukma.edu.ua/kremleboty/?lang=en
2. 755 000 твітів, або Як російська «Фабрика тролів» намагалась впливати на порядок денний в Україні. Дослідження. URL: https://actual.today/755-000-tvitiv-abo-jak-rosijska-fabrika-troliv-namagalas-vplivati-na-porjadok-dennij-v-ukraini-doslidzhennja/
3. Бучин М., Курус Ю. Інформаційна війна Росії проти України: особливості та механізми протидії. *Гуманітарні візії.* Vol. 4. No. 1. 2018. С. 55–62.
4. Валюшко І. О. Інформаційна агресія Росії. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2016. С. 4–5.
5. Военная доктрина Российской Федерации. URL: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf
6. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. №. 1. С. 136–141.
7. Інформаційна війна коштує Росії 4$ мільярди. URL: www.ukrinform.ua/ukr.news/2030605
8. Магда Є. В. Виклики гібридної війни: інформаційний вимір. *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine.* 2014. №. 5. С. 138–142.
9. Малик Я. Інформаційна війна і Україна. URL: http://lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf
10. Новая доктрина информационной войны России. URL: https://www.ukrinform.ru/rubric-other_news/2140533-novaa-doktrina-informacionnoj-vojny-rossii.html

11. Об утверждении Доктрины информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460
12. Панченко В. М. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. *Інформація і право.* 2014. №. 3. С. 13–16.
13. Сасин Г. В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). *Грані.* 2015. № 3. С. 18–23.
14. У ЗС РФ створили пропагандистські війська. URL: https://replyua.net/news/56351-u-zs-rf-stvorili-propagandistsk-vyska.html
15. Черненко Т. В. Ідея сепаратизму як один з інструментів інформаційної війни проти України. *Стратегічні пріоритети.* 2016. № 2. С. 117–123.
16. Що таке інформаційна війна. URL: my.elvisti.com/sergandr/iv.html.
17. Lesyk Y. Rosyjsko-ukraiēska wojna informacyjna. *Вісник Львівського університету. Серія: Міжнародні відносини.* 2016. № 43. С. 106–112.
18. Russian New Generation Warfare Handbook. U.S. Army, Asymmetric Warfare Group. December 2016. URL: https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf
19. Zecurion Analytics: самая сильная армия в киберпространстве у США. URL: https://mresearcher.com/2017/01/11236.html

*Матеріал надійшов до редакції 03.01.2020 р.*

**RUSSIAN INFORMATION WAR: THEORETICAL AND PRACTICALLY APPLIED ASPECTS**

The article deals with the problem of the growth of the information war, which arose as a result of Russia's aggressive policy and created a danger for both the modern European and Ukrainian information space. The author, referring to the analysis of the results of scientific researches, through which some theoretical and practically applied aspects of this war were studied, speaks about the essence of the problem under study and the need for its study.
The purpose of this publication is: 1) to analyze the term «Russian information war» (interpreted as a set of measures taken by governmental and non-governmental organizations of Russia, first of all, in the information space of Ukraine and Russia, other countries of the world); 2) to identify the place of information warfare in Russian geopolitical doctrine, which is regarded as a system of officially accepted in the state views on the development of world processes, the international security system, the assertion of geopolitical interests and priorities of the Russian Federation in the modern world, their implementation and with; 3) characterize the features of Russian troops for «information operations», special units for conducting information fighting on the Internet; 4) the activity of the Russian troll factory in St. Petersburg, it is a branch called «Internet Research Agency», which works around the clock in Petersburg; 5) investigate the Kremlin's misinformation prevention problem.
**Key words:** information war, misinformation, Russian troops for «information operations», Russian geopolitical doctrine, Russian troll factory.

**REFERENCES**

1. «Kremleboty» yak instrument rosiiskoho vplyvu v sviti. URL: https://spa.ukma.edu.ua/kremleboty/?lang=en
2. 755 000 tvitiv, abo Yak rosiiska «Fabryka troliv» namahalas vplyvaty na poriadok dennyi v Ukraini. Doslidzhennia. URL: https://actual.today/755-000-tvitiv-abo-jak-rosijska-fabrika-troliv-namagalas-vplivati-na-porjadok-dennij-v-ukraini-doslidzhennja/
3. Buchyn, M., Kurus, Yu. (2018). Informatsiina viina Rosii proty Ukrainy: osoblyvosti ta mekhanizmy protydii. *Humanitarni vizii,* 4, 1, 55–62.
4. Valiushko, I. O. (2016). Informatsiina ahresiia Rosii. *Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo,* 4–5.
5. Voennaja doktrina Rossijskoj Federacii. URL: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf
6. Horban, Yu. O. (2015). Informatsiina viina proty Ukrainy ta zasoby yii vedennia. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy,* 1, 136–141.
7. Informatsiina viina koshtuie Rosii 4$ miliardy. URL: www.ukrinform.ua/ukr.news/2030605
8. Mahda, Ye. V. (2014). Vyklyky hibrydnoi viiny: informatsiinyi vymir. *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine,* 5, 138–142.
9. Malyk, Ya. Informatsiina viina i Ukraina. URL: http://lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf
10. Novaja doktrina informacionnoj vojny Rossii. URL: https://www.ukrinform.ru/rubric-other_news/2140533-novaa-doktrina-informacionnoj-vojny-rossii.html

11. Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii. URL: http://kremlin.ru/acts/bank/41460
12. Panchenko, V. M. (2014). Informatsiini operatsii v asymetrychnii viini Rosii proty Ukrainy: pidkhody do modeliuvannia. *Informatsiia i pravo,* 3, 13–16.
13. Sasyn, H. V. (2015). Informatsiina viina: sutnist, zasoby realizatsii, rezultaty ta mozhlyvosti protydii (na prykladi rosiiskoi ekspansii v ukrainskyi prostir). *Hrani,* 3, 18–23.
14. U ZS RF stvoryly propahandystski viiska. URL: https://replyua.net/news/56351-u-zs-rf-stvorili-propagandistsk-vyska.html
15. Chernenko, T. V. (2016). Ideia separatyzmu yak odyn z instrumentiv informatsiinoi viiny proty Ukrainy. *Stratehichni priorytety,* 2, 117–123.
16. Shcho take informatsiina viina. URL: my.elvisti.com/sergandr/iv.html.
17. Lesyk, Y. (2016). Rosyjsko-ukraiēska wojna informacyjna Yuliya Lesyk. *Вісник Львівського університету. Серія «Міжнародні відносини»*, 43, 106–112.
18. Russian New Generation Warfare Handbook. U.S. Army, Asymmetric Warfare Group. December 2016. URL: https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf
19. Zecurion Analytics: samaja sil'naja armija v kiberprostranstve u SShA. URL: https://mresearcher.com/2017/01/11236.html

УДК 327.88(470+571):[316.776.23:070+355.4(470:477)«2014/...»
**Шуляк Антоніна,**
доктор політичних наук, професор,
завідувач кафедри міжнародних комунікацій та політичного аналізу,
Східноєвропейський національний університет імені Лесі Українки,
43024, Україна, Волинська обл., м. Луцьк, вул. Винниченка, 28, каб. 8
Ant80@meta.ua, antonina.mytko@eenu.edu.ua
ORCID ID 0000-0002-5234-0758

# МЕДІА-ТЕХНОЛОГІЇ ПІД ЧАС МОДЕЛЮВАННЯ ОБРАЗУ «ІНШОГО» В ІДЕОЛОГІЇ «РУСКОГО МІРА»

*У статті розглянуто питання використання російськими мас-медіа комунікаційних та медійних технологій для створення й ефективного пропагування образу ворога, чужого, іншого під час українсько-російського конфлікту, який розпочався у 2014 р. Зазначено, що саме через пропаганду та маніпулювання просувається ідея «рускої міра» й формується образ противника цієї ідеї – «іншого», котрий не сприймає усього з позначкою «російське» як апріорі позитивне та краще й ставить під сумнів правильність такої позиції, а отже, бажає зла прихильникам «рускої міра». Проаналізовано інформаційні операції та найбільш поширені в російсько-українській інформаційній війні медіа-технології з моделювання образу «іншого» як загрози.*
***Ключові слова:*** *«рускій мір», Російська Федерація, Україна, пропаганда, інформаційні операції, «інший/чужий», маніпуляція.*

## 1. ВСТУП

**Постановка проблеми та її значення.** Ведення інформаційного протистояння між різними суб'єктами (державами, неурядовими, економічними та іншими структурами), що передбачає проведення комплексу з нанесення шкоди інформаційній сфері конкуруючої сторони й захисту власної інформаційної сфери, а також дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформаційним процесам, що ґрунтуються на інформації та інформаційних системах супротивника за одночасного захисту власної інформації, отримали в сучасній політичній науці назву «інформаційна війна».

Із моменту фактичного й формального розпаду СРСР і по сьогодні між Україною та Росією відбувається цивілізаційне протистояння «свій-чужий», пов'язане з історичним прагненням України до