УДК: 351.746.1:355.01–025.26(470+571)]:004.7
DOI: https://doi.org/10.31470/2518-7600-2020-9-150-179

INFORMATIONAL SECURITY OF UKRAINE IN THE CONDITIONS OF RUSSIAN AGGRESSION

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УКРАИНЫ В УСЛОВИЯХ РОССИЙСКОЙ АГРЕССИИ

Валерій Новородовський,
кандидат історичних наук,
молодший науковий
співробітник відділу
національних меншин
ORCID: 0000-0002-3701-775X
ResearcherID:
Інституту політичних і
етнонаціональних досліджень
ім. І.Ф. Кураса НАН України.
вул. Генерала Алмазова, 8, м.
Київ, 01011

Valerii Novorodovskyi,
Ph.D. in Historical Sciences,
Junior Research Scientist of the
Department of National
Minorities
ORCID: 0000-0002-3701-
775X
ResearcherID:
I. F. Kuras Institute of Political
and Ethno-National Research
of the National Academy of
Sciences of Ukraine.
Generala Almazova St., 8,
Kyiv, Ukraine, 01011

ABSTRACT

The main challenges and threats for national security with development of informational technology in Russian-Ukrainian war are considerate. Key trends of Russian information campaign are defined. The directions of Russian propaganda in Ukraine, in the occupied territories, in Russian and European territories were clarified. Threats to the democratic values and Ukrainian and

European security system were revealed. The scientific discourses of national and foreign scholars about the problem of information security and information war are highlighted. Based on a detailed analysis of existing scientific papers, most vulnerable places in the information space were identified. Role of network society in the informational war of Russia against Ukraine is marked. Features of informational weapons usage by Russian Federation during armed conflicts not only in Ukraine, but in Georgia, Nagorno-Karabakh, Transnistria are disclosed. Study of quantitative criteria of social media allowed to determinate level of information spread efficiency. Regulatory framework that regulates the questions of information security of European Union and Ukraine was analyzed. Weaknesses of the Ukrainian legislation concerning protection of information space are revealed, such as declarative nature of legislative acts and normative legal documents. Directions of improvements in information security measures were formed. The main measures of personal data, state institution, information space protection from hacker attacks, and dissemination of information that threatens national security or provokes hostility to ethnic, religious grounds are considered. The basic information on threats to Ukraine's information security in the conditions of Russian aggression is generalized and systematized. The study of the problem of Ukraine`s informational security, as a component of national security allows us to understand potential threats and ways to prevent them.

***Keywords**: information security, war, Ukraine, network society, social media.*

Постановка проблеми. У сучасних умовах розвитку мережевого суспільства вагоме значення для досягнення політичних цілей мають інформаційні технології. Аналізуючи історію воєн у різні періоди віддамо чільне місце інформаційній пропаганді, яка відігравала значну роль у формуванні негативного образу противника, а також застосовувалася для дезорієнтації та дестабілізації ворожих

сил. Нині інформаційна війна є складовою сучасної політики держав. Відтак, для збереження національної єдності та безпеки, держава має впроваджувати елементи захисту в інформаційному просторі, а також формувати комплекс заходів спрямованих на виявлення загроз для суспільства у цій сфері. В умовах російсько-української війни актуалізується вивчення проблеми інформаційної безпеки України.

Метою статті є комплексний аналіз медійного дискурсу для визначення впливу інформаційної війни Росії на етнополітичне становище України, а також пошук оптимальних шляхів захисту інформаційного простору держави.

Аналіз останніх досліджень. Проблема використання інформаційних технологій з метою внутрішньої дестабілізації суспільства для отримання певного політичного зиску окремими країнами розкривається у низці праць вітчизняних та іноземних науковців. Найбільш актуальним дослідженням в умовах сучасних реалій є праця Є. Магди «Гібридна війна», де чітко розписуються особливості російської агресії, зокрема в інформаційному просторі. Серед українських вчених цією проблемою займалися А. Войціховський (Войціховський, 2018), Ю. Горбулін (Горбулін), Є. Магда (Магда, 2015), М. Махній (Махній, 2018), Ю. Ніколаєць (Nikolaiets, 2018), М. Пілат (Пілат, 2013) та ін. У зарубіжному науковому дискурсі ця проблематика є досить актуальною. Нею займалися Е. Джуліано (Guliano), К. Джонес (Jones), Г. Мойніган (Moynihan), М. Яйтнер (Jaitner) та ін.

Виклад основного матеріалу. Новітні інформаційні технології сприяють з одного боку розвитку демократичних режимів у світі, з іншого стають засобом дестабілізації. Зважаючи на плюралізм думок, який поширений у глобалізованому суспільстві, використання проблемних питань іншими країнами дозволяє формувати невдоволеність серед населення і, як наслідок, створюються всі передумови для маніпуляції з метою задоволення певних політичних амбіцій. Відзначимо, що нині інформаційна війна спрямовується на

особистість, тобто на людину, що приймає рішення. На думку низки експертів, ці дії матимуть більшу ефективність у мирний час та на початкових етапах конфлікту (Гриняев, 2004: с. 22). Розвиток інформаційних технологій, зокрема поява соціальних мереж, зумовлює формування нової форми управління суспільством, яку шведські дослідники А. Бард і Я. Зодерквіст охарактеризували як нетократія. Дослідники переконували, що наявність відкритого інформаційного простору не гарантує розвиток демократичного суспільства. Попри відкритість мережевого суспільства, у ньому існує певна владна ієрархія (консумеріати та нетократи), що дозволяє формувати думку мас (Махній, 2018: с. 18). З появою соціальних мереж процеси інформаційної маніпуляції спростилися. В. Бойкіс розкрила особливості збору й обробки даних у facebook, відзначаючи при цьому, що використовуючи їх мережа формує стрічку новин згідно з політичними, культурними, спортивними та іншими уподобаннями користувача (Бойкіс). Відтак, ці дані та цей процес можуть використовувати не лише розробники facebook, але й спецслужби інших країн. У результаті це впливає на ефективність ведення інформаційної війни, яка на сучасному етапі розвитку інформаційних технологій здатна впливати практично на різні сфери державного і суспільного життя. Водночас, за висловом британського дослідника Е. Вілсона, поява нових медіа-технологій завершується пеклом пропаганди й брехні, а з ними приходять і війни (Вілсон). Зі зростанням кількості користувачів соціальних мереж (Digital 2020…; Social, Digital…) ефективність маніпуляцій над суспільством зростає.

Росія, прикриваючи власну агресивну політику, використовує інформаційні технології для дестабілізації ситуації у середині інших країни, шляхом створення проросійських груп. Це підтверджується дослідженням М. Косєнковські, В. Шрейбера, Дж. Хахн, де розкривалося роль інформаційних ресурсів та соціальних мереж у конфліктах в Грузії, Нагірному Карабасі, Придністров'ї. Фактично,

використовуючи facebook як основну інформаційну платформу, створювалася основа для конфлікту (Marcin Kosienkowski, William Schreiber & Joyce Hahn). Таким чином, створюються всі передумови для гібридної війни. На думку Я. Потапенка, елементи інформаційної війни з весни 2015 р. перетворилися на домінуючі у російсько-українському протистоянні (Потапенко, 2016). З цією тезою важко не погодитися, оскільки вплив на населення у мережевому суспільстві створює всі передумови до маніпуляцій з метою дестабілізації.

Упродовж 2014-2020 рр. в умовах російсько-української війни, розглянемо детально динаміку кількості користувачів інтернетом та соціальними мережами. За даними «We are Social» та «Hootsuite's» кількість українців, які використовують інтернет станом на січень 2020 р. становить 27,46 млн. осіб. Цей показник у порівняні з 2019 р. зріс на 5,7 % (1,5 млн) (Digital 2020: Ukraine). Згідно зі звітом «Digital 2017: Ukraine» їхня кількість становила лише 21,93 млн (Digital 2017: Ukraine). Відзначимо, що у 2014-2020 рр. зростає кількість користувачів соціальними мережами в Україні. У зв'язку з подіями Революції Гідності та початком російсько-української війни різко починає зростати кількість користувачів facebook, а також спостерігається їхнє зниження у «вконтакте». Лише за період 2017-2018 рр. кількість користувачів facebook зросла на 71 % (Лише 58 %), що пояснюється указом Президента України №133/2017 щодо обмеження українськими провайдерами доступу до російських соціальних мереж. Крім того, відзначимо високі темпи зростання кількості користувачів instagram: якщо у 2017-2018 рр. показник сягав 7,2 млн. (Лише 58 %), то у 2019-2020 – 11 млн. (Digital 2020: Ukraine). Зважаючи на той факт, що нині суспільство довіряє інформації із соціальних мереж, більше ніж традиційним ЗМІ, то, варто визнати, що вони стають не лише засобом комунікації, але й знаряддям для маніпуляцій масами. Низький рівень довіри до традиційних ЗМІ зумовлював пошук українським суспільством альтернативних джерел інформації, серед яких були й соціальні мережі (Протидія російській…).

На прикладі facebook доведено, що через соціальні мережі можна керувати емоціями людей (Kramer). Таким чином, використовуючи потенціал соцмереж, досить легко здійснювати маніпуляції суспільною свідомістю, а відтак можна впливати на внутрішню політику сусідніх країн, дискредитувати бізнес-конкурента чи політичного опонента тощо. К. Джонс у своїй праці «Online Disinformation and Political Discourse: Applying a Human Rights Framework» наводить приклад дослідження науковців Оксфордського університету в рамках проєкту Computational Propaganda Research Project (COMPROP), у якому відзначається, що лише за 2018 р. виявлені офіційні докази маніпулювань в соціальних мережах збоку політичних партій чи державних установ у 48 країнах світу, а на дослідження та реалізацію психологічних операцій з метою маніпуляцій громадською думкою витрачено 500 млн доларів. Обсяги маніпуляції свідомістю населення є значними, зважаючи на те, що 62 % користувачів не усвідомлюють вплив соцмереж на новини, які вони бачать, а близько 83 % компаній можуть збирати їхні поширені дані (Jones). Зважаючи на це, масштаби маніпуляцій та впливів на суспільну свідомість населення України збоку Росії можуть бути досить потужними, а соціальні мережі, як альтернатива ЗМІ стають одним із ключових знарядь пропаганди та інформаційних атак.

Росія, використовуючи соціальні мережі, зокрема «вконтакте» та «одноклассники», які були поширеними у пострадянському просторі, у тому числі й в Україні, формувала через певні спільноти меседжі, спрямовані на дезорганізацію та дезінтеграцію суспільства (Світова гібридна…, 2017). Юридичною основою для цього став документ «Стратегія національної безпеки Російської Федерації до 2020 року», де чітко зазначалося про необхідність поширення «правдивої» інформації для громадян Росії та росіян закордоном через ЗМІ та соціальні мережі (Стратегия национальной…). Таким чином, відбувалося поширення ідей «русского мира», що зумовлювало

маргіналізацію певних прошарків суспільства і створювало передумови для розгортання сепаратистських рухів на території іншої країни.

Свідченням того, що інформаційний простір є одним із ключових напрямів ведення зовнішньої політики є бюджет Російської Федерації. У 2015 р. на реалізацію федеральної програми «Інформаційне суспільство» виділено 44,7 млрд руб., а на «захист національних інтересів» – 23 млрд. Більше того, бюджет російського пропагандистського каналу «Russia Today» зріс на 41 % у порівнянні з 2014 р. (Інформаційні виклики…, 2016: 61-62). Цікавим є той факт, що розповсюдження російської пропаганди відбувається в усіх країнах світу, де завдяки викривленню і фальсифікуванню фактів, створюється хибна картинка подій на Донбасі та відбувається маніпуляція масовою свідомістю.

Упродовж останніх десятиліть кремлівська верхівка активно реалізовує політику «керованого хаосу» на пострадянському просторі, при цьому використовуючи інформаційні технології (Війна на Донбасі…). Москва застосовує «заборонені прийоми» психологічного та нейролінгвістичного характеру, зокрема «маніпуляції з прадавніми архетипами колективного безсвідомого, що їм протистояти шляхом раціональних аргументів практично неможливо (Потапенко, 2016: 144). Ю. Ніколаєць, досліджуючи медіа-дискурс російсько-українського протистояння, наголошував, що через засоби масової інформації відбувається програмування населення на певну поведінку, унаслідок якої відбувається агресивне неприйняття альтернативної інформації (Nikolaiets, 2018: 118).

Національне законодавство було побудоване на неефективних декларативних принципах, через які не вдалося сформувати ефективну систему інформаційної безпеки (Гібридні загрози…, 2018: 44). Водночас існують інші чинники, що зумовлюють вразливість України в інформаційній війні, зокрема: глобальні мережі, що знаходяться поза контролем

стрімко розвиваються; удосконалюються способи й засоби передачі пропагандистських матеріалів; зростання хакерських атак на державні інформаційні ресурси; зростання кількості систем супутникового зв'язку; розвиток науково-дослідних програм стосовно технічних засобів маніпуляції свідомістю; недостатньо ефективна підготовка фахівців ІТ-сфери; низький рівень розвитку комунікацій; використання неліцензійних програм (Бржевська, Довженко & Киричок & Гайдур & Аносов, 2019: 89-90). Відсутність ефективної системи захисту інформаційного простору спричинює ризики національної безпеки.

Хибною є думка про те, що війна Росії проти України розпочалася у 2014 р. Аналізуючи інформаційний простір за останні роки, відзначимо, що підґрунтя для воєнних дій готувалося набагато раніше. Якщо розглянути мовне питання, як наріжний камінь – то ще наприкінці існування СРСР окремі інтеррухи в інформаційному полі створювали уявлення серед жителів південно-східних регіонів про насильницьку українізацію в умовах незалежності України, а починаючи з середини першого десятиліття XXI ст., після офіційного введення до політичного обігу концепту «руський мир», цей процес набрав нових обертів. Метою його стало недопущення країн пострадянського простору до євроатлантичної інтеграції, а також формування важелів впливу для ведення власної політики на території Східної Європи. М. Яйтнер відзначала, що активні кібератаки Росії розгорнулися з 2010 р., оскільки у цей період офіційна влада зазнала впливу російських шкідливих шпигунських програм. У військовому плані це пов'язано з необхідністю отримати інформаційну перевагу на полі бою чи з поточними військовими операціями (Jaitner). Ймовірно, що такі кібератаки зумовлювалися з метою планування військової агресії. Ю. Сиротюк стверджує, що між Росією та Україною триває війна четвертого покоління, ключовими чинниками якої є економічні, інформаційні, релігійні (Між Україною і…). Г. Мойніган стверджувала, що

DDoS-атаки та злом сайту ЦВК відбулися зі сторони Росії у 2014 р. під час виборів Президента України, у результаті яких було змінено результати виборів, з метою формування уявлення про прихід право радикальних сил до влади (Moynihan). Відразу ж на російських каналах висвітлено інформацію про перемогу колишнього очільника «Правого Сектору» Д. Яроша. Очевидно, що таким чином, Кремль намагався створити вигідну картинку для росіян, а також показати зростання ворожнечі в Україні на національному, етнічному чи релігійному ґрунті через прихід націоналістів. Однак, значного ефекту вони не мали, оскільки: 1) відразу ж після злому сайту ЦВК пролунала заява щодо цих дій з української сторони; 2) в умовах розгортання війни відбувалася консолідація суспільства незалежно від етнічного походження. Таким чином, інформація такого змісту не мала впливу на маси в Україні та країнах Європи, але в Росії та окупованих територіях, де фактично блокуються ЗМІ з альтернативною точкою зору, на початкових етапах, очевидно, мала певний ефект, через використання емоційного чинника пропаганди. Відзначимо, що упродовж 2014-2017 рр. було здійснено 12 потужних кібератак спрямованих на урядові сайти чи критичну інфраструктуру (Найбільші кібератаки…). Аналітики «National Cyber Security Centre» відзначали, що це були сплановані операції російських спецслужб, спрямовані на дестабілізацію демократії та впливу на бізнес (Reckless campaign…). Уряд Великої Британії заявив, що постійні атаки на інформаційні ресурси України є «зневагою до суверенітету України» (Moynihan).

На сучасному етапі інформаційна війна Росії проти України вийшла на новий виток розвитку і несе глобальний характер через необхідність виправдати перед світовою спільнотою власні дії. В. Горбулін відзначав, що інформаційний фронт «гібридної війни» Кремля відбувається у 4 напрямках: 1) серед населення у зоні конфлікту; 2) серед населення країни, проти якої здійснено агресію, але територія якої не охоплена конфліктом; 3) серед громадян Росії; 4) на міжнародній арені

(Горбулін). Більше того, її головне завдання дезорієнтувати не лише українське суспільство, але і європейське, доводячи не легітимність дій української влади, зокрема у сфері захисту територіальної цілісності. Ю. Горбань, аналізуючи інформаційну війну Росії проти України розглядає 5 основних методів її ведення: 1) дезінформація та маніпуляція; 2) пропаганда; 3) диверсифікація громадської думки; 4) психологічний тиск; 5) поширення чуток (Горбань, 2015: с. 138). Відзначимо, що всі ці методи є частиною російської інформаційної політики в інших країнах, мета якої – формування важелів впливу на внутрішню політику. Особливо активною була їхня діяльність в умовах Революції Гідності через певні групи у соціальних мережах, особливо у «вконтакте» та «одноклассники».

Дослідниця М. Пілат розглядає такі типи шкідливої інформації для національної безпеки: 1) інформація, що провокує соціальну, расову, національну чи релігійну ненависть або ворожнечу; 2) заклики до війни; 3) пропаганда ненависті через зневагу чи перевагу; 4) посягання на честь окремих осіб; 5) недобросовісна, неетична чи неправдива реклама чи інформація; 6) інформація, що деструктивно впливає на свідомість та психіку людини (Пілат, 2013: 186-187). Детальніше зупинимося на інформації, яка зумовлює національну чи релігійну ворожнечу. Від початку Революції Гідності, а згодом російсько-української війни, в інформаційному полі російських ЗМІ зображувалася українська сторона як «фашисти», тобто отримувала негативний відтінок. Особливо це позначилося на жителях східних та південних регіонів країни, що сформувало у них ненависть до всього українського. Водночас, російські та проросійські ЗМІ в Україні, а також групи в соціальних мережах висвітлювали події намагаючись сформувати підґрунтя для ворожнечі на релігійній чи етнічній основі, при цьому використовуючи результати діяльності російської пропаганди у минулі роки. Особливо у цьому плані

відзначилися такі групи у «вконтакте» як: «АнтиМайдан», «Сводки от ополчения Новороссии», «Донецк ДНР Новости Новороссии» та ін. У них активно пропагується ненависть до українського, не лише шляхом інформаційних записів, але й відповідними коментарями учасників, які, очевидно працюють над формуванням суспільної думки відвідувачів групи (так звані «тролі», «боти» чи «ломи»). Більше того, російська пропаганда через ЗМІ та соціальні мережі поширювала тези щодо переслідування росіян та російськомовного населення в Україні, тим самим формуючи думку про дискримінацію за етнічною та мовною ознакою. Дослідження Київського міжнародного інституту соціології (КМІС), проведені у травні-червні 2015 р., засвідчили, що меседжі російської пропаганди щодо дискредитації Майдану, ЗСУ, добровольців не прижилися в українському суспільстві (Російський погляд…). Більше того, спроба нав'язати українському суспільству нетерпимість за національною ознакою була невдалою. Національні меншини України, зокрема кримські татари, вірмени, грузини, румуни, угорці частина ромів, білоруси, поляки підтримали територіальну цілісність України. Фактично, Революція Гідності, анексія Криму та бойові дії на території Донбасу сприяли згуртуванню громад етнічних груп через оновлене почуття української ідентичності (Вплив кризи…).

Ключові надії на упокорення України Кремль покладав на етнокультурний чинник. Це пояснюється не лише поліетнічністю України, але й наявністю значної частки росіян та русифікованого населення, яке стало об'єктом російської зовнішньої політики. Відтак, використовуючи інформаційні ресурси російські пропагандисти перекручували етнічну реальність, історію формування української території (Гай-Нижник, 2016). Маніпулюючи історичною пам'яттю та спекулюючи, мовним питанням російська пропаганда створила умови для конфлікту на етнічному ґрунті, при цьому використовуючи схему «свій – чужий». Іншим аспектом

російської інформаційної війни стало використання наративу геноциду російськомовного населення Донбасу. Застосовуючи засоби масової пропаганди, Кремль створював серед населення РФ окупованих нею територій враження підтримки світової спільноти дій Росії. (Золотухін, 2018). Щоправда, аналізуючи російські ЗМІ, Е. Джуліано стверджувала, що пропаганда мала ефект на вже проросійсько налаштоване населення. У дослідженні вона відмічала, що підтримали сепаратистів здебільшого представники з гібридною ідентичністю. Частка українців та росіян, які піддалися російському медіа-впливу була відносно невисока (Guliano).

Чільне місце у веденні інформаційної війни займає вміння використовувати емоції мережевого суспільства. Підкріплення відповідних емоцій відбувається через наявність певної картинки, фотографії, яке має відповідне смислове навантаження. Цей метод є ефективним для розпалювання ворожнечі на етнічному ґрунті, формування певних світоглядних цінностей в населення. Ілюстрування теми конфлікту відбувається шляхом використання українськими та російськими інформаційними ресурсами фотографій, інфографіків, малюнків, карикатур тощо (Глушко, 2017). Особливо таку методику використовує російська пропаганда з метою виправдати власні дії на території іншої країни та в негативному світлі показати українських військових. У праці Д. Золотухіна відзначається, що російська пропагандистська машина використовувала фотографії жертв з інших конфліктів, надаючи цим світлинам необхідного смислового значення, що зумовлювало б обурення суспільства і звинувачення в цих діях українських військових чи добровольців (Золотухін, 2018: 82-87). З однієї сторони поширення цих фотофейків мало на меті сформувати негативний імідж України на міжнародній арені, з іншої – створення певного образу військових ЗСУ, як «карателів». Водночас, подібні пости у соціальних мережах формували суспільне невдоволення та засудження, і, незважаючи на спростування експертами цієї дезінформації, вона все ж мала вплив на суспільну думку.

Зважаючи на інформаційний наступ та кібератаки збоку Росії, що зумовили дестабілізацію в українському суспільстві, існує необхідність створення механізму захисту від цих дій. У ЄС, розуміючи значний деструктивний вплив російської інформаційної політики, реалізували низку заходів, за для захисту свого інформаційного простору. Відзначимо, що Загальне положення про захист даних створене на основі законодавства ЄС про захист персональних даних, створило механізм захисту інформаційного простору Європи (Jones). Відповідно, будь-які документи, які приймаються Європарламентом чи Радою ЄС повністю узгоджуються з чинними міжнародними договорами. У липні 2016 р. Радою ЄС та Європейським парламентом було прийнято директиву «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу», враховуючи сучасні виклики, зокрема активності російської пропаганди на території ЄС, спроби заволодіти іншими країнами інформаційним полем, загрозу демократичним процесам через втручання у внутрішні справи Європейського Союзу. Основні положення документу не суперечать «Договору про функціонування Європейського Союзу» і мають на меті покращити безпеку інформаційного простору Європи. Документ передбачає не лише реалізацію загальноєвропейських заходів безпеки, але й створення національних стратегій, які ґрунтуються на положеннях директиви й мають на меті боротьбу зі злочинами у мережі (Директива Європейського…). Представники ЄС та НАТО неодноразово наголошували на необхідності вироблення тактики боротьби проти «гібридної війни», яку Росія розв'язала в України, Грузії, Молдові (Інформаційні виклики…, 2016: 79). Однак Україна, керуючись досвідом країн ЄС, а також враховуючи національні особливості в інформаційному просторі зобов'язана самостійно створити ефективний механізм захисту інформаційного простору від російської агресії.

В умовах розгортання російсько-української війни було прийнято низку нормативно-правових актів спрямованих на захист інформаційного простору та боротьбою з ворожою пропагандою, яка має деструктивні наслідки для України. Серед ключових документів, які врегульовують питання безпеки в інформаційному просторі слід відзначити Конституцію України, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Закон України «Про національну безпеку», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», «Стратегія національної безпеки України», «Стратегія кібербезпеки України», «Доктрина інформаційної безпеки» та ін. Особливе значення мав Указ Президента України № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», згідно з яким українські провайдери блокували російські соціальні мережі та сайти, зокрема «вконтакте», «однокласники», «mail.ru», «яндекс», «Лабораторія Касперского», «Dr. Web» та офіційного дистриб'ютора «1С» на території України строком на 3 роки (Указ Президента України № 133/2017…). Ці дії мали певні позитивні й негативні наслідки для українського мережевого суспільства. До позитивних слід віднести зниження рівня користування російськими інформаційними ресурсами, соціальними мережами, де розповсюджувалася негативна інформація щодо російсько-української війни, блокування цих ресурсів українськими провайдерами. Крім того, зниження чисельності користувачів російськими соціальними мережами зумовило спад активності рекламодавців, що мало, хоч і не значний, проте певний економічний вплив. Згідно з аналітичними даними Gemius аудиторія охоплення відеорекламою у «вконтакте» скоротилася на 92 % (Дмитренко). У дослідженні аналітиків InfoNapalm А. Лісовського і М. Макарчука зазначалося, що блокування «яндекс» є необхідною умовою для

національної безпеки, пояснюючи це не лише її підконтрольності Кремлю, але й масовості використання сервісу в Україні (Лісовський, Макарчук). Очевидно, що «яндекс» на території України та інших країн пострадянського простору виконував функцію «кремлівського рупора», а відтак санкції проти сервісу, в умовах російсько-української війни стало вже необхідністю. Водночас, блокування російських інформаційних ресурсів та соціальних мереж мало певні негативні наслідки, а саме: застосування користувачами VPN-сервісів, що також загрожує національній безпеці через доступ мережевого трафіку клієнта; використання державними установами програмного забезпечення «1С» і відсутність вітчизняних аналогів створила певні перешкоди; втрата часу на введення цих санкцій зі сторони держави; відсутність контролю за іншими мережами та інформаційними ресурсами, де поширюється російська пропаганда. Експерти відзначають, що використання програм для обходу блокування російських сайтів загрожують безпеці України. Тобто VPN-сервіси, надані іншими країнами створюють можливості для шпигунства, викрадення приватної інформації та маніпулювання інформаційною стрічкою (Использование украинцами…; Макарук). Крім того існує загроза створення бекдорів на персональних девайсах, корпоративних комп'ютерах, що формуватиме всі передумови для викрадення персональних даних, розробок тощо. Однак, це рішення мало вагоме значення в інформаційній війні проти Росії.

Забезпечення інформаційної безпеки суспільства покладено і в «Стратегію кібербезпеки України» та «Доктрину інформаційної безпеки». Обидва документи передбачають створення всіх можливих заходів для безпечного функціонування кіберпростору та протистояння інформаційній агресії Російської Федерації. «Стратегія кібербезпеки України» передбачає формування захисту кіберпростору, що є основою захисту прав людини. Серед пріоритетних напрямів передбачених документів є: 1) розвиток безпечного надійного

кіберпростору; 2) захист державних електронних інформаційних ресурсів та інформаційної інфраструктури; 3) захист критичної інфраструктури; 4) розвиток потенціалу сектору безпеки і оборони у сфері кібербезпеки; 5) боротьба з кіберзлочинністю (Указ Президента України, 27 січня 2016). «Доктрина інформаційної безпеки України» передбачає захищати життєво важливі інтереси суспільства і держави від агресії Російської Федерації в інформаційному просторі, зокрема спрямованої «на пропаганду війни, національної чи релігійної ворожнечі зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» (Указ Президента України, 29 грудня 2016). Водночас, відсутність критичного сприйняття суспільством інформації, засобів захисту інформаційного простору та інколи корупційна складова, яка дозволяє проросійським ЗМІ вести пропаганду, зумовлює невдачі України в інформаційній війні.

Захист інформаційного середовища передбачає пошук оптимальних механізмів протидії ворожій пропаганді. Використання контрпропаганди в українських реаліях може бути ефективним у боротьбі з російським інформаційним засиллям, але, водночас, може підривати основні демократичні цінності. Відтак важливо не лише боротися з пропагандою, але й об'єктивно висвітлювати факти. Тому євроатлантичний досвід для розв'язання цього питання пропонує стратегічні комунікації, тобто обмін ідеями, думками на підтримку національних цілей (Інформаційні виклики…, 2016). Зважаючи на це, держава повинна не лише заохочувати низку інформаційно-аналітичних центрів до цієї діяльності, але й брати активну участь у формуванні стратегічних цілей.

Боротьба проти російської пропаганди та фейків здійснюється недержавними організаціями чи приватними особами, які, таким чином, намагаються допомагати державі у протистоянні з РФ. Так, у 2014 р. створено Інформаційний спротив (ІС) – недержавний проєкт, який виконує завдання

протидії зовнішній ворожій інформаційній загрозі у різних сферах суспільного і державного життя. Фактично, від початку російської агресії ІС, шляхом перевірки різної інформації сповіщав про хід російсько-української війни, а також викривав факти неправдивої інформації зі сторони проросійських ЗМІ (Інформаційний спротив). Іншим проєктом, який боровся з російською інформаційною агресією став StopFake. Упродовж 2014–2020 рр. організація спростувала низку міфів, фейків, які поширювалися у вітчизняних чи іноземних ЗМІ, а також у соцмережах. Крім того, проєкт реалізує низку досліджень, спрямованих на визначення сприйняття суспільством інформації, а також формують рекомендації щодо розпізнання неправдивої інформації (StopFake), тим самим частково виконуючи функції держави у поширенні серед населення знань у цій сфері. Спростування неправдивої інформації здійснюють окремі проєкти у межах соціальних мереж. Перш за все це пояснюється охопленням аудиторії читачів, які досить часто, гортаючи стрічку новин, потрапляють під емоційний вплив певних постів. Одним із таких проєктів є «По той бік новин», де його ініціатори, шляхом аналізу низки інформаційних ресурсів спростовують неправдиву інформацію та висвітлюють власні дослідження. Контент-аналіз наявних матеріалів у цій спільноті дозволяє розкрити ключові особливості, а саме: 1) простий для сприйняття пересічною особистістю текст; 2) вдалий вибір ілюстративного матеріалу; 3) глибокий аналіз новин; 4) науковий підхід до обґрунтування і використання соціологічних досліджень провідних організацій (По той бік новин). У схожому руслі працює громадська організація «Без Брехні», яка викриває неправдиву інформацію ЗМІ, а також подає чіткий аналіз, мотивуючи при цьому читача задуматися (Без брехні). Зважаючи на те, що Україна на початкових етапах програвала інформаційну війну Росії, діяльність цих організацій фактично не допускала краху і засилля в інформаційному просторі країни. Вони здійснюють значну роботу у сфері інформаційної безпеки, однак держава

повинна сформувати власний потужний проєкт, яка зможе охопити всю аудиторію, при умові співпраці з іншими організаціями. Таким чином, суспільство бачитиме не лише спростування неправдивих новин, але й офіційну позицію держави.

Висновки. Отже, враховуючи використання Росією інформаційного тиску з метою посилити внутрішню кризу в Україні, постає необхідність враховувати сучасні світові тенденції інформаційної безпеки. Упродовж 2014–2020 рр. російські ЗМІ, групи у соціальних мережах створювали картинку з емоційним забарвленням для дискредитації України на міжнародній арені, для дестабілізації ситуації в Україні та для виправдання власних дій перед громадянами Росії й міжнародною спільнотою. ЄС та НАТО розуміючи потужність інформаційної зброї в умовах мережевого суспільства, розробили низку заходів для захисту себе від зовнішнього впливу і ймовірних кібератак. Використовуючи досвід провідних країн, Україна має застосовувати ці дії, але враховуючи внутрішні особливості. Для цього необхідно сформувати потужну нормативно-правову базу, яка б врегульовувала питання безпеки інформаційного простору і, на основі наукових інституцій чи аналітичних центрів, організувати систему контрпропаганди та боротьби з дезінформацією, при цьому не забуваючи про основні демократичні принципи. Водночас, держава зобов'язана стимулювати розвиток ІТ-сфери, зокрема у системі безпеки, зважаючи на новітні виклики та зовнішньополітичні загрози.

Подальші дослідження у цьому напрямку мають значні перспективи, оскільки з удосконаленням інформаційних технологій, зростають ризик для національної безпеки. Відтак, важливо більш детально вивчити особливості мережевого суспільства, формування світогляду і ціннісних орієнтирів через соціальні мережі. Вагоме значення для боротьби зі шкідливою інформацією є інформаційна гігієна, а отже експерти соціогуманітарного напрямку мають розробити

практичні рекомендації, а фахівці ІТ-сфери створити додаток чи аналітичну програму, яка стане помічником у пошуку достовірної інформації.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Digital 2017: Ukraine. URL: (Last access: 7.04.2020).
2. Digital 2020: 3,8 billion people use social media. URL: (Last access: 7.04.2020).
3. Digital 2020: Ukraine. URL: (Last access: 7.04.2020).
4. Guliano E. Who supported separatism in Donbas? Ethnicity and popular opinion at the start of the Ukraine crisis. URL: (Last access: 1.05.2020)
5. Jaitner M. Russian Information Warfare: Lessons from Ukraine. URL: (Last access: 15.05.2020).
6. Jones K. Online Disinformation and Political Discourse: Applying a Human Rights Framework. URL: https://cutt.ly/CaXez0h (Last access: 22.04.2020).
7. Kramer, A. Experimental evidence of massive-scale emotional contagion through social networks, Proceedings of the National Academy of Sciences of the United States of America 111 (24): pp. 8788–8790, doi: (Last access: 22.04.2020).
8. Marcin Kosienkowski, William Schreiber & Joyce Hahn. Social Media in the Service of Territorial Reintegration in the post-Soviet Area. URL: https://cutt.ly/uaXeE5T (Last access: 25.05.2020).
9. Moynihan H. The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention. URL: https://cutt.ly/faXePZ5 (Last access: 22.04.2020)
10. Nikolaiets Yu. The use of mass media content in the russian-ukrainian informational confrontation in 2014-2016. Humanitarium. Pereiaslav-Khmelnytskyi (Kyiv reg.); Nizhyn (Chernihiv reg.): Lysenko M. M. Vol. 40, Iss. 3: Philosophy. 2018. P. 177–183.
11. Reckless campaign of cyber attacks by Russian military intelligence service exposed. URL: https://cutt.ly/waXeJAv (Last access: 22.04.2020)

12. Social, Digital & Mobile Worldwide. URL: (Last access: 7.04.2020)

13. StopFake. Сайт. URL: (Last access: 27.04.2020).

14. Без брехні. Фактчек політичної риторики. Сайт. URL: (Last access: 27.04.2020).

15. Бойкіс В. Facebook сканує всі обличчя і створює «цифровий біометричний шаблон». ФБ слідкує за вами, навіть коли ви на інших сайтах. Зібрані дані продають. URL: https://cutt.ly/daXeMTk (Last access: 7.04.2020).

16. Бржевська З., Довженко Н., Киричок Р., Гайдур Г. Аносов А. Інформаційні війни: проблеми загрози протидія. Кібербезпека: освіта, наука, техніка. Київ, 2019. № 3 (3). С. 88-96.

17. Війна на Донбасі: реалії та перспективи врегулювання. URL: (Last access: 14.05.2020).

18. Вілсон Е. Сім смертних гріхів, або Сім причин, чому Європа неправильно розуміє російсько-українську кризу. URL: https://cutt.ly/saXrq16 (Last access: 22.04.2020).

19. Войціховський А. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26-37.

20. Вплив кризи в Україні на її західні області. Тематичний звіт СММ ОБСЄ. URL: (Last access: 7.04.2020).

21. Гай-Нижник П., Залізняк Л., Краснодемська І., Фігурний Ю., Чирков О., Чупрій Л. Агресія Росії проти України: історичні передумови та сучасні виклики. Київ: «МП Леся», 2016. 586 с.

22. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ. Київ, 2018. 105 с.

23. Глушко А. Візуальні засоби мови ворожнечі як інструмент інформаційної війни. Діалог. 2017. № 23. С. 132-154.

24. Горбань Ю. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України. 2015. Вип. 1. С. 136-141.

25. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. URL: https://cutt.ly/aaXrdtE (Last access: 27.04.2020).

26. Гриняев С. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. По материалам иностранной печати. Москва, 2004. 426 с.

27. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: (Last access: 24.04.2020).

28. Дмитренко О. Facebook обійшов ВКонтакте вже в перший тиждень після введення санкцій проти російських соцмереж. URL: https://cutt.ly/BaXrxrO (Last access: 21.04.2020).

29. Золотухін Д. #Біла книга спеціальних інформаційних операцій проти України 2014 – 2018.. Київ, 2018. 384 с.

30. Использование украинцами сомнительных программ для обхода блокировки санкционных российских сайтов угрожает кибербезопасности страны – эксперты (видео). УНІАН. URL: https://cutt.ly/daXrWL9 (Last access: 25.04.2020).

31. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с.

32. Інформаційний спротив. Сайт. URL: (Last access: 24.04.2020).

33. Лише 58 % українців користуються інтернетом – дослідження. URL: (Last access: 22.04.2020).

34. Лісовський А., Макарчук М. Гібридні війни: прихована загроза Яндекса (Інфографіка). URL: (Last access: 24.04.2020).

35. Магда Є. Гибридная война: выжить и победить. Харків, 2015. 320 с.

36. Макарук М. Санкції проти російських соцмереж і Яндексу: боротьба триває. URL: (Last access: 23.04.2020).

37. Махній М. Мережеве суспільство: кіберпсихологічний путівник. Київ: Academia.edu, 2018. 176 с.

38. Між Україною і Росією триває війна четвертого покоління – експерти. URL: (Last access: 21.04.2020).

39. Найбільші кібератаки проти України з 2014 року. Інфографіка. URL: https://cutt.ly/DaXrS2h (Last access: 21.04.2020).

40. Пілат М. Інформаційні впливи та інформаційні війни: сутність понять та їхній зв'язок в інформаційну епоху. Вісник Львівського університету. Серія міжнародні відносини. 2013. Вип. 32. С. 185-190.

41. По той бік новин. URL: The provided link is incorrect (Last access: 27.04.2020).

42. Потапенко Я.О. П'ята російсько-українська війна: від майдану до східного фронту (оцінки, підходи, інтерпретації). Переяслав-Хмельницький: «Видавництво К С В», 2016. 304 с.

43. Протидія російській пропаганді та медіаграмотність: результати всеукраїнського опитування громадської думки – Аналітичний звіт. URL: https://cutt.ly/zaXr8hg (Last access: 23.04.2020).

44. Російський погляд на Майдан та війну на Донбасі в Україні не прижився. Соцопитування. URL: (Last access: 27.04.2020).

45. Світова гібридна війна: Український фронт. Національний інститут стратегічних досліджень. Київ, 2017. 496 с.

46. Стратегия национальной безопасности Российской Федерации до 2020 года. URL: (Last access: 24.04.2020).

47. Указ Президента України № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». URL: (Last access: 14.05.2020).

48. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»». URL: (Last access: 14.05.2020).

49. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». URL: (Last access: 14.05.2020).

REFERENCE

1. *Digital 2017: Ukraine*. Retrieved from: .

2. *Digital 2020: 3,8 billion people use social media*. Retrieved from: .

3. *Digital 2020: Ukraine*. Retrieved from: .

4. Guliano E. *Who supported separatism in Donbas? Ethnicity and popular opinion at the start of the Ukraine crisis*. Retrieved from: .

5. Jaitner M. *Russian Information Warfare: Lessons from Ukraine*. Retrieved from: https://cutt.ly/UaXthBd.

6. Jones K. *Online Disinformation and Political Discourse: Applying a Human Rights Framework*. Retrieved from: https://cutt.ly/YaXtnnx.

7. Kramer, A. Experimental evidence of massive-scale emotional contagion through social networks, *Proceedings of the National Academy of Sciences of the United States of America* 111 (24): 8788–8790, doi: Retrieved from: .

8. Marcin Kosienkowski, William Schreiber & Joyce Hahn. *Social Media in the Service of Territorial Reintegration in the post-Soviet Area*. Retrieved from: https://cutt.ly/zaXtYol.

9. Moynihan, H. *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*. Retrieved from: https://cutt.ly/SaXumeu.

10. Nikolaiets, Yu. (2018). The use of mass media content in the russian-ukrainian informational confrontation in 2014-2016. *Humanitarium.* Pereiaslav-Khmelnytskyi (Kyiv reg.); Nizhyn (Chernihiv reg.): Lysenko M. M. 40, 3: Philosophy. 177-183.

11. Reckless campaign of cyber attacks by Russian military intelligence service exposed. Retrieved from: .

12. Social, Digital & Mobile Worldwide. Retrieved from: https://cutt.ly/TaXis.

13. StopFake. Sait. Retrieved from: .

14. Bez brekhni. [Without lies]. Faktchek politychnoi rytoryky. Sait. Retrieved from: https://www.bez-brehni.info/.

15. Boikis, V. *Facebook skanuie vsi oblychchia i stvoriuie «tsyfrovyi biometrychnyi shablon». FB slidkuie za vamy, navit koly vy na inshykh saitakh. Zibrani dani prodaiut.* [Facebook scans all faces and creates a «digital biometric template». FB follows you, even when you are on other sites. The collected data is sold]. Retrieved from: [in Ukrainian].

16. Brzhevska, Z. & Dovzhenko, N. & Kyrychok, R. & Haidur, H. & Anosov, A. (2019). Informatsiini viiny: problemy zahrozy protydiia. [Information war: problems, threats and antides]. *Kiberbezpeka: osvita, nauka, tekhnika*. Kyiv. 3 (3). 88-96 [in Ukrainian].

17. Viina na Donbasi: realii ta perspektyvy vrehuliuvannia. [The war in Donbas: realities and prospects for settlement]. Retrieved from: [in Ukrainian].

18. Vilson, E. *Sim smertnykh hrikhiv, abo Sim prychyn, chomu Yevropa nepravylno rozumiie rosiisko-ukrainsku kryzu*. [The Seven Deadly Sins, or the Seven Reasons Why Europe Misunderstands the Russian-Ukrainian Crisis]. Retrieved from: [in Ukrainian].

19. Voitsikhovskyi, A. (2018). Kiberbezpeka yak vazhlyva skladova systemy zakhystu natsionalnoi bezpeky yevropeiskykh krain. [Cyber Security as an Important Component for the Ensuring the National Security of European Countrie]. *Zhurnal skhidnoievropeiskoho prava*. 53. 26-37 [in Ukrainian].

20. Vplyv kryzy v Ukraini na yii zakhidni oblasti. [The impact of the crisis in Ukraine on its western regions]. *Tematychnyi zvit SMM OBSIe*. Retrieved from: [in Ukrainian].

21. Hai-Nyzhnyk, P. & Zalizniak, L. & Krasnodemska, I. & Fihurnyi, Yu. & Chyrkov, O. & Chuprii, L. (2016). *Ahresiia Rosii proty Ukrainy: istorychni peredumovy ta suchasni vyklyky.* [Aggression of the Russian Federation against Ukraine:

ethnonational dimension and civilizational confrontation.]. Kyiv, «MP Lesia». 586 [in Ukrainian].

22. Hibrydni zahrozy Ukraini i suspilna bezpeka. Dosvid YeS i Skhidnoho partnerstva (2018). [Hybrid threats to Ukraine and public safety. Experience of the EU and the Eastern Partnership]. *Analitychnyi dokument*. Kyiv. 105 [in Ukrainian].

23. Hlushko, A. (2017). Vizualni zasoby movy vorozhnechi yak instrument informatsiinoi viiny. [Visual means of hate speech as a tool of information warfare]. *Dialoh*. 23. 132-154 [in Ukrainian].

24. Horban, Yu. (2015). Informatsiina viina proty Ukrainy ta zasoby yii vedennia. [Informational war against Ukraine and means of its conduction]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy*. 1. 136-141 [in Ukrainian].

25. Horbulin, V. *«Hibrydna viina» yak kliuchovyi instrument rosiiskoi heostratehii revanshu.* [«Hybrid war» as a key tool of Russia's geostrategy of revenge]. Retrieved from: [in Ukrainian].

26. Grinyaev, S. (2004). *Pole bitvy – kiberprostranstvo. Teoriya, priemy, sredstva, metody i sistemy vedeniya informacionnoj vojny*. [The battlefield - cyberspace Theory, techniques, means, methods and systems of information warfare.]. *Po materialam inostrannoj pechati*. Moskva. 426 [in Russian].

27. Dyrektyva Yevropeiskoho Parlamentu i Rady (IeS) 2016/1148 vid 6 lypnia 2016 roku pro zakhody dlia vysokoho spilnoho rivnia bezpeky merezhevykh ta informatsiinykh system na terytorii Soiuzu. [Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union]. Retrieved from: [in Ukrainian].

28. Dmytrenko, O. *Facebook obiishov VKontakte vzhe v pershyi tyzhden pislia vvedennia sanktsii proty rosiiskykh sotsmerezh*. [Facebook bypassed VKontakte in the first week after the imposition of sanctions against Russian social networks] Retrieved from: [in Ukrainian].

29. Zolotukhin, D. (2018). *#Bila knyha spetsialnykh informatsiinykh operatsii proty Ukrainy 201-2018.* [#White Book

on Special Information Operations against Ukraine 2014-2018]. Kyiv. 384 [in Ukrainian].

30. Ispol'zovanie ukraincami somnitel'nyh programm dlya obhoda blokirovki sankcionnyh rossijskih sajtov ugrozhaet kiberbezopasnosti strany – eksperty (video). [Use by Ukrainians of dubious programs to circumvent the blocking of sanctioned Russian sites threatens the country's cybersecurity – experts (video)]. UNIAN. Retrieved from: [in Ukrainian].

31. Informatsiini vyklyky hibrydnoi viiny: kontent, kanaly, mekhanizmy protydii (2016).[Information challenges of hybrid warfare: content, channels, counteraction mechanisms]: analit. dop. / za zah. red. A. Barovskoi. Kyiv, NISD. 109 [in Ukrainian].

32. Informatsiinyi sprotyv. [Information resistance]. Sait. Retrieved from: [in Ukrainian].

33. Lyshe 58 % ukraintsiv korystuiutsia internetom – doslidzhennia. [Only 58% of Ukrainians use the Internet – research]. Retrieved from: [in Ukrainian].

34. Lisovskyi, A. & Makarchuk M. *Hibrydni viiny: prykhovana zahroza Yandeksa (Infohrafika).* [Hybrid wars: the hidden threat of Yandex]. Retrieved from: [in Ukrainian].

35. Mahda, Ye. (2015). *Gibridnaya vojna: vyzhit' i pobedit'* [Hybrid war: survive and win]. Kharkiv. 320 [in Ukrainian].

36. Makaruk, M. *Sanktsii proty rosiiskykh sotsmerezh i Yandeksu: borotba tryvaie.* [Sanctions against Russian social media and Yandex: the struggle continues]. Retrieved from: [in Ukrainian].

37. Makhnii, M. (2018). *Merezheve suspilstvo: kiberpsykholohichnyi putivnyk.* [Network society: a cyberpsychological guide]. Kyiv: Academia.edu. 176 [in Ukrainian].

38. Mizh Ukrainoiu i Rosiieiu tryvaie viina chetvertoho pokolinnia – eksperty. [The fourth generation war is going on between Ukraine and Russia - experts]. Retrieved from: [in Ukrainian].

39. Naibilshi kiberataky proty Ukrainy z 2014 roku. [The biggest cyber attacks against Ukraine since 2014]. *Infohrafika*. Retrieved from: [in Ukrainian].

40. Pilat, M. (2013). Informatsiini vplyvy ta informatsiini viiny: sutnist poniat ta yikhnii zviazok v informatsiinu epokhu. [Information influences and information wars: the essence of concepts and their connection in the information age]. *Visnyk Lvivskoho universytetu. Seriia mizhnarodni vidnosyny*. 32. 185-190 [in Ukrainian].

41. Po toi bik novyn. [On the other side of the news]. Retrieved from: [in Ukrainian].

42. Potapenko, Ya. (2016). *Piata rosiisko-ukrainska viina: vid maidanu do skhidnoho frontu (otsinky, pidkhody, interpretatsii).* [The Fifth Russian-Ukrainian War: from the Maidan to the Eastern Front (assessments, approaches, interpretations)]. Pereiaslav-Khmelnytskyi: «Vydavnytstvo K S V». 304 [in Ukrainian].

43. Protydiia rosiiskii propahandi ta mediahramotnist: rezultaty vseukrainskoho opytuvannia hromadskoi dumky – Analitychnyi zvit. [Countering Russian Propaganda and Media Literacy: Results of an All-Ukrainian Opinion Poll – Analytical Report]. Retrieved from: https://cutt.ly/gaXsAtP [in Ukrainian].

44. Rosiiskyi pohliad na Maidan ta viinu na Donbasi v Ukraini ne pryzhyvsia. [Russia's view of the Maidan and the war in the Donbass has not taken root]. *Sotsopytuvannia.* Retrieved from: [in Ukrainian].

45. Svitova hibrydna viina: Ukrainskyi front (2017). [The world hybrid war: Ukrainian front]. Natsionalnyi instytut stratehichnykh doslidzhen. Kyiv.496 [in Ukrainian].

46. Stratehyia natsyonalnoi bezopasnosty Rossyiskoi Federatsyy do 2020 hoda. [The strategy of national security Russian Federation until 2020]. Retrieved from: [in Ukrainian].

47. Ukaz Prezydenta Ukrainy № 133/2017 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2017 roku «Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii)». [Decree of the

President of Ukraine № 133/2017 «On the decision of the National Security and Defense Council of Ukraine of April 28, 2017» On the application of personal special economic and other restrictive measures (sanctions)»]. Retrieved from: [in Ukrainian].

48. Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy»». [Decree of the President of Ukraine «On the decision of the National Security and Defense Council of Ukraine of January 27, 2016» On the Cyber Security Strategy of Ukraine»»]. Retrieved from: https://zakon5.rada.gov.ua/laws [in Ukrainian].

49. Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»». [Decree of the President of Ukraine «On the decision of the National Security and Defense Council of Ukraine of December 29, 2016» On the Doctrine of Information Security of Ukraine»».]. Retrieved from: [in Ukrainian].

АНОТАЦІЯ

Розглядаються основні виклики і загрози для національної безпеки України з розвитком інформаційних технологій в умовах російсько-української війни. Визначено ключові тенденції російської інформаційної кампанії. З'ясовано напрямки російської пропаганди в Україні, на окупованих територіях, в Росії та Європі. Розкрито загрози демократичним цінностям і системі безпеки України та Європи. Висвітлено науковий дискурс вітчизняних та іноземних дослідників з проблеми інформаційної безпеки та інформаційної війни. На основі детального аналізу наявних наукових праць, встановлено найбільш вразливі місця в інформаційному просторі. Відзначено роль мережевого суспільства у ведені інформаційної війни Росії проти України. Розкрито особливості застосування інформаційної зброї Російською Федерацією під час збройних конфліктів не лише в

Україні, але й в Грузії, Нагірному Карабасі, Придністров'ї. Вивчення кількісних критеріїв соціальних мереж дозволив визначити рівень ефективності поширення інформації. Проаналізовано нормативно-правову базу, яка врегульовує питання інформаційної безпеки Європейського Союзу та України. Виявлено слабкі сторони українського законодавства стосовно захисту інформаційного простору, зокрема декларативний характер законодавчих актів та нормативно-правових документів. Сформовано напрями удосконалення заходів безпеки інформаційного простору. Розглянуто основні заходи захисту персональних даних, державних інституцій та інформаційного простору від хакерських атак, поширення інформації, що містить загрозу національній безпеці чи провокує ворожнечу етнічному, релігійному ґрунті. Узагальнено та систематизовано основні відомості щодо загроз інформаційній безпеці України в умовах російської агресії. Дослідження проблеми інформаційної безпеки України як складової національної безпеки дозволяє розуміти потенційні загрози та шляхи їхнього запобігання.

Ключові слова: *інформаційна безпека, війна, Україна, мережеве суспільство, соціальні мережі.*

АННОТАЦИЯ

Рассматриваются основные вызовы и угрозы национальной безопасности Украины с развитием информационных технологий в условиях российско-украинской войны. Определены ключевые тенденции российской информационной кампании. Выяснено направления российской пропаганды в Украине, на оккупированных территориях, в России и Европе. Раскрыто угрозы демократическим ценностям и системе безопасности Украины и Европы. Освещен научный дискурс отечественных и зарубежных исследователей по проблеме информационной безопасности и информационной войны. На основе детального анализа имеющихся научных трудов, установлены наиболее уязвимые

места в информационном пространстве. Отмечена роль сетевого общества в ведении информационной войны России против Украины. Раскрыты особенности применения информационного оружия Российской Федерацией во время вооруженных конфликтов не только в Украине, но и в Грузии, Нагорном Карабахе, Приднестровье. Изучение количественных критериев социальных сетей позволил определить уровень эффективности распространения информации. Проанализированы нормативно-правовую базу, которая регулирует вопросы информационной безопасности Европейского Союза и Украины. Выявлены слабые стороны украинского законодательства относительно защиты информационного пространства, в частности декларативный характер законодательных актов и нормативно-правовых документов. Сформированы направления совершенствования мер безопасности информационного пространства. Рассмотрены основные меры защиты персональных данных, государственных институтов и информационного пространства от хакерских атак, распространения информации, которая содержит угрозу национальной безопасности или провоцирует вражду этнической, религиозной почве. Обобщены и систематизированы основные сведения относительно угроз информационной безопасности Украины в условиях российской агрессии. Исследование проблемы информационной безопасности Украины как составляющей национальной безопасности позволяет понимать потенциальные угрозы и пути их предотвращения.

***Ключевые слова**: информационная безопасность, война, Украина, сетевое общество, социальные сети*