УДК 327.88:316.485.26](470:[477+4])
DOI https://doi.org/10.32782/2663-6170/2023.33.18

РОСІЙСЬКА ГІБРИДНА ВІЙНА: ЗАГРОЗИ І КІБЕРВИКЛИКИ ДЛЯ ЄВРОПЕЙСЬКОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

RUSSIAN HYBRID WAR: THREATS AND CYBER CHALLENGES TO EUROPEAN INFORMATION SECURITY

Білоусов М.В.,
аспірант кафедри соціології та політології
Чорноморського національного університету імені Петра Могили

Алєйник В.Г.,
аспірант кафедри соціології та політології
Чорноморського національного університету імені Петра Могили

У науковій статті досліджено прояви гібридної війни РФ в європейському інформаційному середовищі з 2014 року, тобто від початку війни на Сході України. Зроблено наголос на тому, що явище гібридної війни має комплексний характер, а у російській гібридній війні операції в інформаційному просторі, в якості складової гібридної війни, не менш важливі за військові дії. З'ясовано, що російські кібератаки з 2014 року мали місце не тільки в Україні, але й в європейських країнах, в тому числі і через підтримку ними України та накладання санкцій на РФ та представників її політикуму. На думку автора, гібридні загрози можна охарактеризувати як складний набір дій, що використовуються державними або недержавними акторами для маніпулювання системними вразливими місцями цільових держав або організацій.

Також автором статті виокремлено дві групи загроз європейській інформаційні безпеці під час війни Росії в Україні: 1) загрози пов'язані з дезорієнтацією та дезорганізацією європейського суспільства (стимулювання сепаратистських рухів шляхом здійснення кібератак на політичні партії та державні структури); 2) загрози пов'язані з активізацією дій ворожих збройних формувань, викликані російськими дезінформаційними атаками, пропагандою, маніпуляціями.

Проаналізовано основні виклики для країн ЄС породжені цим явищем з урахуванням використання інформаційної зброї, пропаганди та методів інформаційно-психологічного впливу на європейське суспільство. Для прикладу до них слід віднести перешкоджання демократичним процесам прийняття рішень шляхом масових кампаній дезінформації, використання соціальних медіа для контролю над політичним наративом або для радикалізації внутрішньополітичної ситуації.

Автором з'ясовано, що завдяки схожим підходам у боротьбі із загрозами і викликами в інформаційній сфері посилилася співпраця ЄС і НАТО проти майбутніх російських гібридних загроз. Зокрема, доведено, що ЄС надав Україні допомогу у протидії гібридним загрозам (кібератакам і дезінформації), а також виокремлено практичні рекомендації для держав-учасниць ЄС задля зміцнення європейської інформаційної безпеки на сучасному етапі.

Ключові слова: гібридна війна, інформаційна безпека, гібридні загрози, кібервиклики, Україна, Європейський Союз, Російська Федерація.

The scientific article examines the manifestations of the Russian Federation hybrid war in the European information environment since 2014, that is, since the beginning of the war in the Eastern Ukraine. Emphasis is placed on the fact that the phenomenon of a hybrid war is complex, and in the Russian hybrid war, operations in the information space, as a component of a hybrid war, are no less important than military operations. It was found that Russian cyber attacks since 2014 have taken place not only in Ukraine, but also in European countries, including due to support for Ukraine and the imposition of sanctions on the Russian Federation and representatives of its politicians. According to the author, hybrid threats can be described as a complex system of actions used by state or non-state actors in order to manipulate system vulnerabilities of target states or organizations.

Also, the author of the article identified two groups of threats to European information security during the Russian war in Ukraine: 1) threats associated with the disorientation and disorganization of European society (stimulating separatist movements by carrying out cyber attacks on political parties and state structures); 2) threats are caused by Russian disinformation attacks, propaganda, manipulations with the intensification of the actions of enemy armed formations.

The main challenges for the EU countries generated by this phenomenon are analyzed, taking into account the use of information weapons, propaganda and methods of information and psychological impact on European society. Examples include obstructing democratic decision-making processes through mass disinformation campaigns, using social media to control the political narrative, or radicalizing the domestic political situation.

The author finds out that thanks to similar approaches in combating threats and challenges in the information sphere, cooperation between the EU and NATO against future Russian hybrid threats has intensified. In particular, it is proved that the EU has provided Ukraine with assistance in countering hybrid threats (cyber attacks and disinformation), as well as practical recommendations for EU member states to strengthen European information security at the present stage.

Key words: hybrid war, information security, hybrid challenges, cyber challenges, Ukraine, the European Union, the Russian Federation.

Постановка проблеми. Слід зазначити, що європейська інформаційна сфера стала однією з важливих площин реалізації російської гібридної війни.

Анексія Криму та спалах військової напруженості на Донбасі у 2014 р. спровокували десятирічне інформаційне протистояння між Російською Федерацією (далі – РФ) – з одного боку, та Україною і Європейським Союзом (далі – ЄС) – з іншого. Варто зазначити, що російські гібридні загрози включають в себе інформаційний вплив та економічний тиск, які мають на меті послабити соціальну згуртованість, підірвати довіру до ЄС та його інституцій і, таким чином, дестабілізувати ситуацію в середині об'єднання. Першими результатами гібридних дій РФ щодо ЄС стали: втручання у виборчий процес та збільшення євроскептичних настроїв [9, с. 91].

Російське повномасштабне вторгнення в Україну в лютому 2022 р. породило побоювання в європейському суспільстві щодо нової хвилі великих інформаційних атак. Гібридна війна все ще залишається вигідною для Росії, оскільки несе за собою невеликі витрати. РФ постійно адаптує гібридну війну у відповідь на технологічні зміни. Російські операції у сфері гібридної війни змінилися, щоб створити більш потужні засоби впливу, які поєднують створення внутрішніх та міжнародних проблем.

Актуальність обраної проблематики підтверджує і той факт, що хоча РФ, виходячи з обмеженої позиції влади, намагається вплинути на найпотужніший у світі союз – ЄС, використовуючи відносно дешеві засоби, все ж не варто недооцінювати небезпеку кіберескалації в найближчому майбутньому. Різкі економічні санкції Заходу проти РФ можуть викликати загострення гібридної війни, з високим рівнем напруженості та численними загрозами після лютневого вторгнення в Україну у 2022 р.

Аналіз останніх досліджень і публікацій. Проблему впливу російської гібридної війни на європейську інформаційну безпеку досліджувала низка вітчизняних та зарубіжних науковців, експертів та аналітиків. Серед українських дослідників увагу цьому питанню приділяли: А. А. Головка [1], Є. М. Магда [2; 3], О. О. Мележик [4], Б. О. Парахонський [5], І. І. Проноза [6], С. С. Троян [7], А. О. Хмель [8; 9], С. Шваничик [10], Ю. Залізняк [25]. Серед зарубіжних науковців варто згадати напрацювання А. Барічелли [14], О. Джонсона [18], А. Кудорса [19], Н. Попеску [20], М. Вісере [24], Х. Каррейрас [15] та ін.. Згадані дослідники аналізували російську гібридну війну як комплексне явище і робили акцент саме на стані інформаційної безпеки України та держав-учасниць ЄС у зв'язку з постійним збільшенням гібридних загроз. Майже всі вони приходять до висновку, що суттєва співпраця європейських країн у сфері політики кіберзахисту все ще потребує подальшої роботи, задля розробки конкретних механізмів та процедур, які дадуть результати на практичному рівні.

Виділення невирішених раніше частин загальної проблеми. Важливо враховувати, що гібридна війна – це інструмент, за допомогою якого РФ змінює існуючий світовий порядок і ще раз нагадує всім про свої регіональні та глобальні амбіції, виявляючи тим самим значно більший політичний виклик на міжнародному рівні [3, с. 140]. Стратегія гібридної війни була створена півстоліття тому, і її рушійною силою стала саме ідеологія. А невід'ємною складовою ідеологічної війни виступила ідеологічна диверсія у процесі якої змінювалося сприйняття реальних речей в свідомості мільйонів людей. Фахівець радянської пропаганди, підривних дій та дезінформації, який з 1970 р. жив і працював у США під псевдонімом Томас Девід Шуман (справжнє ім'я – Юрій Безменов) у своїх роботах описував риси притаманні гібридній війні, а саму ідеологічну диверсію розділив на чотири стадії: 1) «деморалізація»; 2) «дестабілізація»; 3) «криза»; 4) «нормалізація» [22]. Ця методика досить широко використовувалась СРСР в роботі з країнами, які потрібно було ослабити та в майбутньому підкорити. Саме на стадії «деморалізації» відбувається підривна діяльність у сфері медіа (ЗМІ) за допомогою методів монополізації та маніпулювання задля створення «викривленої картини реальності» [22]. Стадії, які виокремлює Ю. Безменов реалізуються через інформаційні кампанії і давно притаманні РФ, ще з часів СРСР. З кожним роком механізм роботи російської пропагандистської машини набирав обертів і ставав все більш потужним. Російська гібридна війна в європейській інформаційній площині триває і досі, тому автор статті припускає, що обрана проблематика стане вагомим об'єктом наукового аналізу в майбутньому. Москва вирішила посилити свою шпигунську та дезінформаційну війну проти Європи, що почало давати певні результати. Тим не менш, ризик ескалації та розростання фази гарячої війни в Україні у надзвичайно руйнівну світову кібервійну є справжнім. Відтак проблема викликів і загроз для європейської інформаційної безпеки, породжених російською гібридною війною, вимагає більш детального політологічного дослідження.

Формулювання цілей статті (постановка завдання). Мета наукової статті полягає в здійсненні аналізу інформаційних загроз і кібервикликів для європейської інформаційної безпеки, породжених російською гібридною війною та відповідей ЄС на них з метою розробки актуальних та дієвих рекомендацій.

Виклад основного матеріалу дослідження. Інформаційна безпека ЄС є таким станом системи інформаційної безпеки, при якому вона, з одного боку, здатна протистояти дестабілізуючому впливу зовнішніх і внутрішніх інформаційних загроз, а з іншого – її функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища [7, с. 28-29].

Вважаємо, що гібридна війна – це широкомасштабна діяльність, однак російський спосіб її ведення виходить за межі західного загальнодержавного підходу та включає організовану злочинність і розвідувальні служби з глобальним охопленням і чіткою координацією [2, с. 9]. Під час ведення гібридної війни РФ залучає щонайменше шість управлінь адміністрації президента і низку президентських рад. Це демонструє різноспрямованість російської гібридної війни та її налагоджений механізм здійснення контролю, що становить неабиякий виклик для ЄС. Адже, з кожним роком ЄС все важче протидіяти суб'єкту, який використовує потужні засоби: від законних і незаконних фінансів до хакерів, ЗМІ та розвідувальних служб [18].

Гібридні загрози – це сукупність дій, що використовуються державними або недержавними акторами для маніпулювання системними вразливими місцями цільових держав або організацій. Гібридні загрози включають звичайні та нетрадиційні засоби, які важко оцінити кількісно [15].

Гібридні загрози не є новою темою в порядку денному безпеки. Але загроза від російської гібридної війни для європейської інформаційної безпеки залишається реальною. Загалом виклики для європейської інформаційної безпеки пов'язані з російською гібридною війною автор статті пропонує об'єднати в дві групи: 1) загрози пов'язані з *дезорієнтацією та дезорганізацією* європейського суспільства (стимулювання сепаратистських рухів шляхом здійснення кібератак на політичні партії та державні структури); 2) загрози *активізації дій ворожих збройних формувань,* викликані російськими дезінформаційними атаками, пропагандою, маніпуляціями з.

Прикладами вищевказаних гібридних загроз є перешкоджання демократичним процесам прийняття рішень шляхом масових кампаній дезінформації, використання соціальних медіа для контролю над політичним наративом або для радикалізації внутрішньополітичної ситуації.

Загрози пов'язані з дезорієнтацією та дезорганізацією європейського суспільства. ЄС залежить від політичної підтримки своїх держав-членів. У деяких країнах існує опозиція інституціям ЄС (що проявляється у наявності та діяльності партій-євроскептиків), яка може бути посилена та використана зі зловмисними намірами російською владою. Особливо вразливими є вибори та референдуми в європейських країнах, які, по суті, є процесами врегулювання політичних суперечок. У РФ є стимул впливати на результат цих процесів, щоб посіяти сумніви та створити нестабільність [5, с. 10-11]. Європейський парламент досить точно резюмує мету російських кібероперацій, спрямованих на ЄС: «Спотворення істини, провокація сумнівів, розділення держав-членів, створення стратегічного розколу між ЄС та його північноамериканськими партнерами та паралізування процесу прийняття рішень, дискредитація інституції ЄС і трансатлантичне партнерство … шляхом підриву та розмивання європейського наративу, заснованого на демократичних цінностях, правах людини та верховенстві права» [16].

Слід зазначити, що починаючи з 2014 р. ЄС вжив низку заходів для підвищення готовності до гібридних загроз породжених російською агресією на Сході України. Серед них – прийняття галузевих стратегій, створення експертних органів (Європейський центр з протидії гібридним загрозам; Центр передового досвіду з питань гібридних загроз), запровадження механізмів обміну інформацією, проведення навчань, партнерство з НАТО та збільшення інвестицій у кіберзахист. Зокрема, ЄС прийняв План дій проти дезінформації та створив ініціативу ЄС проти дезінформації у 2015 р. [11].

Європейська комісія координує та розробляє політичні ініціативи з кількох ключових питань у межах своєї компетенції: заходи кібербезпеки, боротьба з дезінформацією, забезпечення вільних і чесних виборів тощо. Проте варто зазначити, що у Європейській стратегії безпеки («Безпечна Європа в кращому світі») 2003 р. про гібридні загрози взагалі нічого не сказано, а у Стратегії прийнятій у 2016 р. зазначається те, що такі загрози існують і з ними потрібно боротися [8, с. 117-118].

Зокрема, «Сильніша Європа. Глобальна стратегія зовнішньої політики та політики безпеки ЄС» (2016 р.) визначила управління відносинами між ЄС і РФ ключовим стратегічним викликом для європейської безпеки, а гібридні загрози визначено одними з найбільш актуальних загроз для Європи. У рамках реалізації Стратегії ЄС намагався протистояти кібервійні Кремля та його кампаніям з дезінформації за допомогою низки корисних ініціатив у різних секторах політики. Реалізуючи ці ініціативи, ЄС загалом забезпечив узгодженість зовнішньої та внутрішньої політики та розширив співпрацю з НАТО [12]. Незважаючи на те, що у 2020 р. більшість положень Глобальної стратегії зовнішньої політики та політики безпеки ЄС щодо кібербезпеки та стратегічної комунікації було реалізовано, необхідні додаткові зусилля для ефективної протидії російській гібридній війні. З одного боку, підхід ЄС у цих питаннях все ще затьмарений інституційною та фінансовою фраг-

ментацією всередині ЄС, між Брюсселем і державами-членами ЄС. З іншого боку, ЄС все ще виділяє відносно обмежені ресурси для протидії російській дезінформації та кібератакам, особливо якщо порівнювати з інвестиціями Кремля [24].

Окрім вищезазначених документів слід згадати про те, що ЄС розробив чимало нормативно-правових актів, які поєднували в собі комплекс заходів для захисту інформаційної сфери ЄС, а саме його кібернетичного простору. Серед них «Спільна структура протидії гібридним загрозам – відповідь ЄС» (2016 р.); «Операційний протокол ЄС для протидії гібридним загрозам» (2016 р.); «Підвищення стійкості та посилення можливостей для подолання гібридних загроз» (2018 р.); «Звіт про впровадження Спільної програми протидії гібридним загрозам 2016 р. та Спільного повідомлення 2018 р. щодо підвищення стійкості та зміцнення можливостей для подолання гібридних загроз» (2020 р.) [9, с. 99].

Беручи до уваги групу викликів, які створюють перешкоди для демократичних систем, боротьба з гібридними загрозами була визначена пріоритетом у Стратегічному порядку денному ЄС на 2019-2024 рр. [13]. У липні 2020 р. ЄС також запровадив перші в історії санкції (заморожування активів і заборона на поїздки) у відповідь на російські кібератаки [17].

Загрози викликані російськими дезінформаційними атаками, пропагандою, маніпуляціями з активізацією дій ворожих збройних формувань. У боротьбі за громадську думку в самій РФ, Європі та за кордоном контрольовані державою російські ЗМІ використовують добре відомі або нові методи пропаганди [4, с. 5]. Російські агенти впливу працюють не лише на телеканалі RT у всьому світі, але й можуть змусити авторитетні ЗМІ у Великій Британії, Франції чи інших країнах публікувати повідомлення російських експертів. Інтернет став полем битви для російських тролів і хакерів [25, с. 30].

Через глобалізацію цифрових технологій національні кордони та географічні відстані є менш актуальними в кіберсфері. У лютому 2022 р. російські хакери здійснили численні кібератаки на Україну, які здебільшого полягали в атаках середнього та малого масштабу і включали шпигунство, інформаційно-психологічні операції та гібридну війну, яка поєднує цілеспрямовані кібератаки з кінетичними військовими ударами по землі. Хоча кібербезпека, безсумнівно, зіграла ключову роль у війні в Україні, події розгорталися всупереч очікуванням. Москва посилила кампанії кібершпигунства та дезінформації проти Заходу, намагаючись посіяти внутрішню розбіжність. Ризик непорозумінь посилювався залученням глобальної коаліції хакерів на чолі з «Anonymous», яка розпочала тривалу кампанію кібератак проти РФ [6, с. 82].

У перший же день повномасштабного вторгнення відбувся злом супутникової компанії "Viasat", що призвело до вимкнення модемів, підключених до супутника KA-SAT Viasat Inc. Незважаючи на те, що це призвело до порушення зв'язку в Україні, відбулося також поширення цієї проблеми по всій Європі, вплинувши на десятки тисяч людей, підприємств і державних установ у низці держав-членів ЄС від Польщі до Франції [14, с. 9-10].

Як і в Україні, кібератаки РФ проти країн ЄС тривають принаймні з 2014 р., якщо не раніше. Наприклад, у 2007 р. через дипломатичну суперечку з Москвою щодо радянського військового меморіалу Естонія постраждала від серії нищівних кібератак, у результаті яких через DDoS-атаки були виведені з ладу веб-сайти урядових, медіа та фінансових установ. На початку 2019 р. в Польщі було розкрито трирічну кампанію з дезінформації, яка діяла через соціальні медіа-платформи, такі як "Facebook"; потік фейкових новин на підтримку трьох проросійських польських політиків охопив аудиторію до 4,5 млн. осіб [10, с. 218].

Так само німецькі служби безпеки звинуватили підтримувані РФ групи у зламі файлів парламентського комітету, який розслідує шпигунську справу Агентства національної безпеки (далі – АНБ) у 2015 р. За цим прослідувала серія кібершпигунств і витоків даних у 2016 та 2017 рр. проти різних німецьких політичних організацій, а також з кампанією дезінформації на платформах соціальних мереж, з метою впливу на федеральні вибори в Німеччині, що проходили у 2017 р.. Крім того, у 2015 р. французька телерадіомовна служба "TV5Monde" постраждала від масштабної кібератаки, яка знищила комп'ютерні системи та припинила трансляцію всіх її дванадцяти каналів. Згодом французька влада виявила, що за зломом, ймовірно, стоїть підтримувана РФ група "Fancy Bear". Безпосередньо перед президентськими виборами у Франції в травні 2017 р. комп'ютерні системи політичної кампанії Еммануеля Макрона також були зламані: понад 20 тис. електронних листів викрадено, а потім скинуто на анонімний файлообмінний сайт, з метою дестабілізувати його кампанію. Наступне розслідування знову виявило зв'язки з хакерською групою "Fancy Bear" [10, с. 219].

Слід зазначити, що від російських гібридних загроз та кібервикликів страждають не тільки країни-члени ЄС, а й кандидати на вступ до цієї організації. Зокрема, держави Західних Балкан йдуть стабільним, але повільним шляхом до інтеграції з ЄС і НАТО. Західні Балкани знаходяться на лінії фронту між ЄС і НАТО з одного боку та РФ з іншого. У цьому регіоні можна спостерігати менш помічений, але не менш ефективний спосіб проштовхування російських наративів проти ЄС

і НАТО. До 2014 р. російське керівництво, здавалося, не надто дбало про це, але після того, як у 2014 р. РФ вторглася в Україну, її амбіції в регіоні зросли.

Чорногорія, зокрема, перебуває в процесі приєднання до ЄС. У травні 2016 р. країна завершила переговори про асоціацію з НАТО та приєдналася до Альянсу в червні 2017 р.. І за збігом обставин Чорногорія зазнала збільшення кількості кібератак як за складністю, так і за кількістю: з 22 у 2012 р. до понад 400 у 2017 р. [23].

Російське керівництво прагнуло зробити Чорногорію прикладом для країн, які розмірковують про членство в НАТО. Кібератаки були пов'язані з хакерською групою APT28, також відомою як "Fancy Bear", пов'язаною з російською військовою розвідкою ГРУ. Перед виборами була також спроба державного перевороту, яка мала на меті повалити уряд і вбити тодішнього прем'єр-міністра Мілo Джукановича. Зловмисниками були ідентифіковані офіцери ГРУ Едуард Широков і Володимир Попов. У 2017 р. їм висунули звинувачення разом із 12 іншими особами, які мали громадянство Росії, Сербії та Чорногорії. Кібератаки, розвідувальні операції та підривну діяльність у Чорногорії слід розглядати в поєднанні з більш масштабним інформаційним наступом РФ на Західні Балкани. Ключовим інструментом у цьому наступі був "Sputnik Serbia", який зосереджувався на проросійських, антиєвропейських і антинатовських наративах [20].

Важко оцінити сукупний вплив цієї дезінформації в міжнародному просторі, але деякі приклади можуть бути ілюстративними. Наприклад, 42% сербів бачили своїм найкращим партнером РФ, а 14% – ЄС.

Випадок із Чорногорією є яскравим прикладом поєднання офлайн- і онлайн-інструментів, які використовує Росія, і ширшого бажання російського керівництва підірвати членство в НАТО та ЄС. Самі по собі кібератаки чи інформаційні зусилля можуть здаватися незначними неприємностями, але поєднання цих різних інструментів робить їх потужними та дає синергію [5, с. 19].

Крім самої України, РФ зосередила багато своїх кібератак на такі країни Східної Європи, як Польща та Румунія, які слугували основними транзитними маршрутами для доставки зброї, обладнання та різних інших гуманітарних товарів для допомоги Україні. Наприклад, 25 лютого 2022 р. деструктивна кібератака була спрямована на пункт прикордонного контролю з метою перешкодити потоку біженців до Румунії, змусивши місцевих чиновників вручну обробляти документи людей, які перетинають кордон. Схоже, що ці кібератаки були помстою за заяву тодішнього президента сенату Румунії Флоріна Кіцу про те, що його країна збирається надати Україні військову техніку та виступати транзитером зброї НАТО.

Кібервтручання в режимі реального часу з боку європейських кіберагентств, а також допомога приватного сектора значно вплинули на хід гібридної війни. Через сподівання на «короткотривалу» війну Москва погано підготувала свій кібернаступ проти України. А руйнівні економічні санкції Заходу разом із відтоком мізків російських ІТ-експертів підсилили її програш в інформаційній площині.

Вищесказане змусило ЄС не залишатися байдужим до гібридних ризиків. Держави-члени ЄС несуть головну відповідальність за реагування на гібридні загрози шляхом підвищення їх стійкості, а також виявлення, запобігання та реагування на гібридні загрози. Ініціативи під керівництвом ЄС та НАТО були здійснені з метою нейтралізації кіберзагроз та захисту основної інфраструктури. У рамках цих ініціатив ЄС активізував свої Групи швидкого кібернетичного реагування для підтримки кіберзахисту України [21].

Кінцеві цілі ЄС у боротьбі із російськими гібридними загрозами полягають у запобіганні атакам на інституції та держави-члени ЄС шляхом підвищення їх стійкості до рівня, який коштує надто дорого для злочинців. Для ефективної боротьби з гібридними загрозами роль розвідувальних служб є життєво важливою. Інтелект збільшує знання та обізнаність про гібридну діяльність, що, у свою чергу, підтримує прийняття рішень на політичному рівні. Таким чином, навіть незважаючи на те, що ЄС рухається в правильному напрямку, розширення інструментів і потенціалу могло б і надалі сприяти зміцненню розвідувальних служб і створити міцнішу основу для розробки політики [15].

Висновки та перспективи подальших розвідок у цьому напрямі. Підсумовуючи, варто зазначити, що агресія РФ в Україні, яка у воєнному плані матеріалізувалася окупацією та анексією Криму в 2014 р. та початком війни на Сході України, змінила сприйняття загроз у всьому світі, особливо в ЄС. Автор статті розглянув інформаційну безпеку ЄС через медіа-територію фази гарячої війни в Україні, яка згодом може перерости у справжню світову кібервійну.

Починаючи з 2014 р. ЄС почав приділяти більше уваги проблемам у сфері кіберзахисту. У контексті європейської інформаційної безпеки реалізація гібридних загроз та кібервикликів мала не лише політичний вплив на колективні рішення країн ЄС, але також мала наслідки для інституційної архітектури, що призводить до суттєвих адаптацій у самому ЄС. Проаналізувавши гібридні загрози пов'язані з дезорієнтацією та дезорганізацією європейського суспільства та загрози викликані російськими дезінформаційними атаками, а саме пропагандою з активізацією дій ворожих збройних формувань, автор статті вважає за доцільне:

1. Країнам ЄС серйозно переглянути політику у сфері боротьби з уразливістю своїх ЗМІ. Уряди цих держав, як і раніше, мають уникати цензури, але в той же час, вони повинні обмежувати діяльність ЗМІ, яка є несумісною зі свободою преси та спотворенням фактів. Усі країни-члени ЄС повинні бути готові до боротьби з гібридними загрозами та кібервикликами, оскільки вразливі місця однієї країни представляють собою відповідальність для всього блоку.

2. ЄС також має докласти зусиль для боротьби з дезінформацією, посилюючи свою політику та законодавство щодо кібербезпеки, особливо з точки зору вирішення проблеми слабких сфер інформаційного середовища, що виникають через диференційовані норми в країнах-членах. Лише спільна політика кібербезпеки та оборони з метою виявлення та запобігання кібервикликів породжених російською гібридною війною зможе допомогти країнам-учасницям ЄС досягнути відповідного рівня кіберстійкості у майбутньому.

3. Ініціативи під керівництвом ЄС та НАТО були здійснені з метою нейтралізації кібернебезпек та захисту основної інфраструктури України. Не зважаючи на те, що був застосований режим кіберсанкцій ЄС проти осіб, організацій і органів, відповідальних або причетних до кібератак проти України, Європа не повинна зменшувати пильність і повинна прискорити кібердопомогу Україні за допомогою існуючих інструментів, таких як «Групи швидкого кіберреагування» задля зменшення російських гібридних загроз у майбутньому.

Враховуючи те, що наслідком багаторічної російської гібридної війни стала поява численних загроз і кібервикликів для країн ЄС, які ще більше посилилися після повномасштабного вторгнення РФ на територію України, перспективним напрямком для наших подальших наукових досліджень вбачається вивчення питання майбутнього посилення гібридних загроз для європейської інформаційної безпеки у зв'язку з можливою ескалацією збройних конфліктів на території Європи через останні події в Україні. Той факт, що ЄС активізував роботу над розробкою комплексного плану протидії гібридним загрозам та кібервикликам для європейської інформаційної безпеки у співпраці з НАТО, є значною подією, але ще багато потрібно зробити, щоб це втілилося в конкретні заходи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Головка А. А. Захист кіберпростору як складова інформаційної безпеки України в умовах гібридної війни. *Молодий вчений.* 2016. № 4. С. 333-336.

2. Магда Є. М. Гібридна війна: сутність та структура феномену. *Вісник Київського національного університету ім. Тараса Шевченка* «*Міжнародні відносини».* Серія «Політичні науки». 2014. № 4. С. 9-10. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2489/2220

3. Магда Є. М. Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України.* 2014. № 5. С. 138-142. URL: http://nbuv.gov.ua/UJRN/Nzizvru_2014_5_29.

4. Мележик О. О. Світова гібридна війна: український фронт. *Вісник НАН України.* 2017. № 2. С. 3-8.

5. Парахонський Б. О. Дестабілізація Європи: гібридна війна РФ. *Стратегічна панорама.* 2021. № 1-2. С. 5-29.

6. Проноза І. І. Гібридна російсько-українська війна як загроза європейській безпеці. *S.P.A.C.E. Society, Politics, Administration in Central Europe: електронний науково-практичний журнал.* Одеса: НУ «ОЮА». 2016. Вип. 1. С. 81-84.

7. Троян С. С. Інформаційно-безпекова політика Європейського Союзу. *Зовнішні справи : суспільно-політичний журнал.* 2019. № 2/3. С. 28-32.

8. Хмель А. О. Місце гібридних загроз у Стратегії безпеки ЄС 2020. *The European Union's Experience of Responding to Security Challenges.* Proceedings of the All-Ukrainian scientific-methodical seminar. Within the Erasmus+ Jean Monnet Modules project 621046-EPP1-2020-1-EN-EPPJMO-MODULE European political integration: historical retrospective and nowadays. Hlukhiv. 2021. P. 117-123.

9. Хмель А. О. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). *Acta de Historia & Politica: Saeculum XXI.* Вип. 4. 2022. С. 91-101.

10. Шваничик С. Чинники інформаційної війни Російської Федерації проти України. *Вісник Львівського університету.* Серія: Філософсько-політологічні студії. 2019. Вип. 24. С. 218-219.

11. A Europe that Protects: The EU steps up action against disinformation. *European Commission.* 2018. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6647

12. A Global Strategy for the European Union's Foreign and Security Policy. *The European Union Institute for Security Studies*. 2016. URL: https://www.iss.europa.eu/content/global-strategy-european-union%E2%80%99s-foreign-and-security-policy

13. A new strategic agenda for the EU (2019-2024). *European Council*. URL: https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/

14. Barichella A. Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe. *Jacques Delors Institute.* September 2022. P. 1-19. URL: https://institutdelors.eu/wp-content/uploads/dlm_uploads/2022/09/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf

15. Carreiras H. Hybrid Threats in the Context of European Security. *Instituto de Defesa Nacional*. 2021. URL: https://www.idn.gov.pt/pt/publicacoes/ebriefing/Documents/E-Briefing%20Papers/E-Briefing%20Papers%203.pdf

16. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. *European Parliament*. 2016. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html

17. Hybrid Threats. *European Commission*. 2023. URL: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

18. Jonsson O. The Evolution of Russian Hybrid Warfare: EU/NATO. *Center for European Policy Analysis.* 2021. 29 of January. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-eu-nato/

19. Kudors A. Hybrid War – A New Security Challenge for Europe. *IPEX.* 2015. URL: https://secure.ipex.eu

20. Popescu N., Secrieru S. Hacks, leaks and disruptions – Russian cyber strategies. *Jacques Delors Institute.* 2022. URL: https://institutdelors.eu/en/publications/la-dimension-cybersecurite-de-la-guerre-en-ukraine/

21. Russia's war on Ukraine: Timeline of cyber-attacks. *European Parliament*. 2022. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

22. Schuman T. D. Love letter to America. *Internet Archive.* 1984. URL: https://archive.org/details/BezmenovLoveLetterToAmerica

23. Tomovic D., Zivanovic M. Russia's Fancy Bear Hacks its Way into Montenegro. *Balkan Insight*. 2018. 5 of March. URL: https://balkaninsight.com/2018/03/05/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018/

24. Viceré M. The EUGS and Russian hybrid warfare: effective implementation but insufficient results. *Foundation for European Progressive Studies*. 2019. URL: https://feps-europe.eu/wp-content/uploads/2019/02/The-EUGS-and-Russian-hybrid-warfare-effective-implementation-but-insufficient-results.pdf

25. Zaliznyak Y. Information security and Russian aggression: Ukraine – EU –NATO hybrid response to hybrid war. *Yearbook of the Institute of East-Central Europe*. Vol. 14. No. 2. 2016. P. 23-42.