

**Є. О. Соломін**

кандидат наук із соціальних комунікацій, доцент  
завідувач кафедри журналістики  
e-mail: evgenlhu@gmail.com, ORCID: 0000-0001-6770-5505  
ДВНЗ «Ужгородський національний університет»  
пл. Народна, 3, м. Ужгород, 88000, Україна

## **ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВІЙНИ ТА ВТРУЧАНЬ У МЕДІАСЕРЕДОВИЩЕ**

**Мета дослідження** – виявлення системних загроз для інформаційної безпеки, способів поширення наративів російської пропаганди, втручання в медіасередовище й способів мінімізації на різних технологічних платформах руйнівного впливу.

**Методологія дослідження.** Для дослідження проблематики інформаційних втручання, систематичних пропагандистських кампаній було застосовано метод відбору та класифікації даних, їх обробка та аналіз, що дало змогу виявити задіявані технології маніпулювання.

**Результати.** Просування наративів «руського міра» в Україні відбувалось засобами гібридної війни, системного втручання в інформаційне поле та його розбалансування. Для російської пропаганди національний телерадіопростір з початку війни виявився закритим, натомість телеграм-канали, різні сайти та месенджери стали основними платформами для дезінформації, фейків, втручання та фактично ведення інформаційного тероризму. Міжнародний характер використання Росією цілого спектра засобів та інструментів дестабілізації й втручання визнав і Європарламент та обмежив чи заборонив їх основні технологічні ресурси. Натомість через втрату можливостей просування дезінформації на власних платформах пропагандисти використовують обхідні можливості.

**Новизна.** Універсалізовано інформаційні та пропагандистські виклики війни, що триває в медіасередовищі та кіберпросторі.

**Практичне значення.** Результати дослідження можуть бути використані під час вивчення журналістикознавчих, політологічних, історичних дисциплін. Методологічна база може стати в нагоді під час подальших наукових розвідок та досліджень у галузі стратегічних комунікацій, інформаційної безпеки.

**Ключові слова:** пропаганда, дезінформація, рашизм, телепростір, цифрові ресурси, інформаційний простір, гібридна війна.

### **I. Вступ**

Російсько-українська війна, яка стартувала у 2014 р. з анексії АР Крим та захоплення окремих районів Луганської та Донецької областей і в 2022 р. переросла у повномасштабне вторгнення, показала весь спектр застосування сучасних засобів ведення війни, де воєнним діям передували та супроводжували їх інформаційно-психологічні атаки, масована пропаганда, дезінформація, різні технології викривлення інформаційного поля, диверсійні, економічні, політичні акції, діяльність спецслужб на українській території тощо. Гібридна війна як «комбінація конвенційних, іррегулярних та асиметричних засобів, що включають постійну маніпуляцію політичним та ідеологічним конфліктом, а також залучення сил спеціальних операцій та конвенційних збройних сил, агентів розвідки, політичних провокаторів, представників медіа, економічний шантаж; кібератаки» [15] стала не лише частиною української реальності, а й викликом для Європи через постійне російське втручання у справи ЄС.

Методологічною основою осмислення проблематики є наукові праці, сформовані на основі досліджень учених, які аналізували різні аспекти масовокомунікаційної діяльності, гібридних викликів. Зокрема, причини та передумови російської агресії, її стратегічні цілі, а також особливості ведення гібридної війни в різних вимірах: воєнному, політичному, економічному, соціальному, гуманітарному, інформаційному – аналізували науковці Національного інституту стратегічних досліджень [4]. Вплив інформаційно-комунікаційних технологій та фактори стійкості інформаційного поля й протидії кібертероризму вивчав Ю. Бідзіля [9]. Важливими є дослідження ключових наративів російської пропаганди [3], з відповідними меседжами та підмеседжами й аналізом «перетлумачення» української історії з метою виправдання росіянами військової агресії. М. Бутиріна, О. Гудошник, О. Кирилова [2] аналізують різні аспекти вияву медіанаративів у практичній діяльності ЗМК. Є. Соломін розглядає етапи анексії частини національного

інформаційного простору [5], транскордонні виклики для системи інформаційної та національної безпеки [17]. Д. Гайслер, Д. Бер [10] аналізують російську пропаганду під час російсько-української війни, що триває, і визначають її системність, скоординованість зусиль з маніпулювання переконаннями та поведінкою в інтересах пропагандистів, виокремлюють загрози для суспільств, які виникають унаслідок цього. С. Парк, Д. Мендельсон [16] аналізують фейки, дезінформацію та виявляють інші стратегії російського зовнішнього маніпулювання та втручань.

Досвід російсько-української гібридної та повномасштабної війни є надзвичайно важливим, у тому числі з погляду вивчення технологій пропаганди, маніпуляцій, поширення фейків, просування наративів, дезінформації, втручання в кіберпростір до та безпосередньо під час ведення бойових дій. Технології, які в мирний час залишалися латентними, в умовах відкритого військового протистояння стали видимими, а, отже, такими, що можуть бути ідентифіковані, вивчені та знешкоджені. Подальші дослідження цього напрямку є вкрай актуальними, адже сприятимуть сталому розвитку та будуть дієвим механізмом нівелювання загроз для національної й міжнародної систем інформаційної безпеки.

## **II. Постановка завдання та методи дослідження**

Мета дослідження – виявлення системних загроз для інформаційної безпеки, способів поширення наративів російської пропаганди, з вкидами, дезінформацією, маніпуляціями, втручанням у справи третіх країн та медіасередовище й способів мінімізації руйнівного впливу рашизму в національному й міжнародному інформаційному просторі, цифрових ресурсах, у тому числі соціальних мережах і технологічних платформах.

Для дослідження проблематики втручань, дезінформації, систематичних пропагандистських кампаній, що становить виклик для національної та міжнародної системи інформаційної безпеки, було застосовано метод відбору та класифікацію даних, їх обробку та аналіз, що дало змогу виявити поточні й довготривалі цілі задіяваних технологій маніпулювання. Аналітичний метод дозволив розглянути агресивну інформаційну політику та втручання не лише як елемент реалізації локальних цілей окупантів в Україні, а і як засіб досягнення свого панування в геополітичному інформаційному просторі.

## **III. Результати**

Радянська пропаганда з її тоталітарною системою та боротьбою проти «загниваючого Заходу», неминучими «військовими загрозами НАТО» еволюціонувала в російський авторитаризм з удосконаленими загрозами та сформувала новий різновид тоталітарної ідеології – рашизм, який увібрав традиції радянського комуністичного режиму, фашистського націонал-соціалізму та російського шовінізму з просуванням імперського «руського міра», «комплексним застосуванням військових сил, політичних, економічних, інформаційних та інших засобів <...>, які реалізуються з широким застосуванням протестного потенціалу населення та сил спеціальних операцій» [18]. При цьому радянсько-російська пропаганда в національному просторі сукупно з глибокою інтеграцією медіа в політичний капітал, що легітимізувала таємні політичні рішення еліт, сприяла змиццю інтересів медіа, фінансово-економічних та політичних еліт і проросійської влади на місцях та цілих регіонах, як і цілеспрямовані атаки з використанням сучасних інформаційних технологій, систематичні інформаційні маніпуляції та дезінформація Кремля формуванню позитивно-схвального ставлення до путінсько-російської авторитарної системи.

Україна в умовах гібридної війни, «широкого застосування непрямих, та інших (у тому числі нетрадиційних) форм і засобів ведення бойових дій» [18] формувала каркас інформаційної безпеки, спрямований на створення «передумов для розвитку такого потенціалу інформаційної сфери в державі, який забезпечує її сталий розвиток та дозволяє уникати зовнішніх негативних впливів» [7]. Проте ані «Концепція інформаційної безпеки України» не дала прямих відповідей на багато питань, у тому числі щодо механізмів попередження та протидії пропаганді та різним втручанням, ані ухвалена у 2017 р. «Доктрина інформаційної безпеки України». Доктрина уточнювала засади формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни та декларувала захист українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора, але чіткої верифікації та механізмів нівелювання загрозам не містила.

Поняття інформаційної як складової національної системи безпеки окреслено в «Стратегії інформаційної безпеки» й визначено як «стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженням

доступом» [7]. Дефініція «інформаційна загроза» у цьому ж документі представлена як «потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні» [7].

Очікуваними результатами реалізації Стратегії визначено захищеність інформаційного простору країни, ефективне функціонування системи стратегічних комунікацій, ефективну протидію поширенню незаконного контенту, забезпечення сталого процесу інформаційної реінтеграції громадян України з окупованих територій, підвищення рівня медіакультури та медіаграмотності, формування української ідентичності тощо. Фактично Стратегія на етапі її ухвалення (28 грудня 2021 р. – фактично за два місяця до повномасштабної російсько-української війни) увібрала накопичений Україною 8-річний досвід ведення гібридної війни та існування в умовах окупації частини території (АР Крим, ОРДЛО) і суверенного інформаційного поля й визначила основні складові саме інформаційної безпеки (рис. 1), однак подальше нормативно-правове наповнення не відбулося через початок війни.



Рис. 1. Стратегічні цілі та напрями реалізації «Стратегії інформаційної безпеки»

Втручання Росії в інформаційне поле України та його розбалансування мало системний характер, натомість протидія дезінформації та викидам в інформаційний і кіберпростір у період з 2014 р. – перманентний та недостатньо ефективний. Заборона російських сервісів («Yandex», «Mail.Ru»), компаній («Group», «Лабораторія Касперського», DrWeb), соцмереж («ВКонтакте», «Однокласники»), найбільших російських телекомпаній («ТВ Центр», РБК, ВГТРК, «НТВ-Плюс», «Звезда», ТНТ, РЕН, ОТР та ін.) частково нівелювала пропагандистський тиск, проте клієнт-сервісні технології VPN дозволяли такі заборони обходити.

У період гібридної війни, що триває, помилковим для системи інформаційної безпеки було й рішення медіагруп «1+1 media», «Inter Media Group», «Медіа Групи Україна» та «StarLightMedia» закодувати власне супутникове мовлення за наявності в провайдерів програмних послуг альтернативи – безоплатного супутникового та ефірного мовлення російських каналів чи послуги російських OTT-платформ. Через це на значних територіях підконтрольній Україні частини Донецької та Луганської областей «продовжили домінувати пропагандистські російські федеральні та регіональні сепаратистські телеканали» [5, с. 21], а на непідконтрольній – все українське мовлення, крім супутникового, і так було недоступне з 2014 р. Деструктивний характер мала й ретрансляція російських каналів на українських ресурсах, поширення антиукраїнського контексту в ефірі національних телеканалів («112-Україна», «NewsOne», «ZIK», «Наш», «Перший незалежний»), в анексованому суверенному інформаційному полі та його частотному ресурсі, який використовували з пропагандистською метою, віртуальному й кіберпросторі, різними комунікаційними каналами, у тому числі за допомогою політичних сил, розгалуженій мережі

УПЦ МП, «проксі-сервери та сурогати, пара-військові, терористичні й кримінальні елементи» [13] тощо.

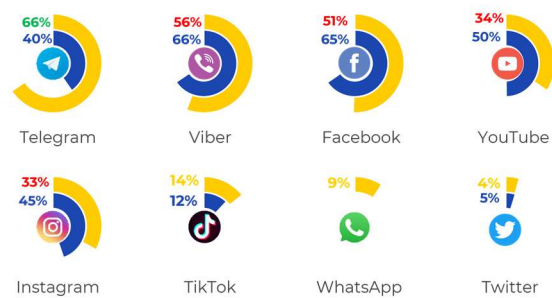
В умовах гібридної війни «поєднання військових і невійськових засобів досягнення стратегічних політичних цілей призвело до того, що кожний її елемент використовується як зброя, яка завдавала ураження різного рівня системам» [4, с. 19–20]. Так були сформовані ключові наративи російської пропаганди про «один народ»/«Крим, Донбас і південний схід України – це Росія», «Україну, як невдалу тінь Росії»/«штучний проєкт Заходу», «народ Донбасу, який годував всю країну»/«Донбас ніхто не чує», «Майдан розпочав війну в Україні»/«громадянський конфлікт»/«агресію Києва», «націоналістичну/фашистську/нацистську Україну», «кривавих неонацистів», «ЗСУ вбиває народ Донбасу», «8 років бомбили Донбас»/«де були 8 років, коли бомбили Донбас» та ін.

Повномасштабне вторгнення Російської Федерації в Україну призвело до втрати частини суверенного інформаційного поля в межах усієї території Луганської, значної частини Донецької та частково Херсонської, Миколаївської й Запорізької областей та поширення пропагандистського контенту на окуповані регіони. Через війну припинили мовлення 234 телерадіоорганізації та провайдери програмної послуги.

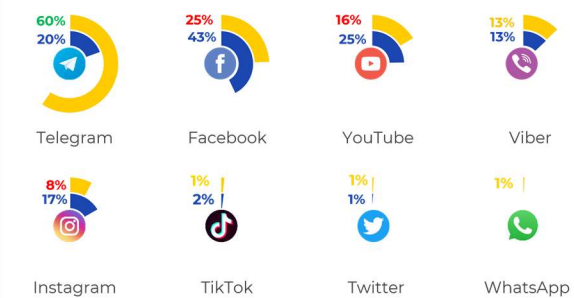
В умовах повномасштабної війни медіагрупи «1+1 media», «Inter Media Group», «Медіа Групи Україна» та «StarLightMedia», канали «Рада» й Суспільне (НСТУ) створили спільний проєкт – єдиний інформаційний марафон, який дістав назву «Єдині новини #UАразом», що в умовах воєнного стану дало змогу почати реалізовувати на цій платформі стратегічних комунікацій єдину інформаційну політику. Марафон «Єдині новини» в цілодобовому форматі мовлення транслюється на загальнонаціональних телеканалах «1+1», «Інтер», «Україна-24» (пізніше – «Ми – Україна»), ICTV, «Рада», Суспільне, а також в ефірах регіональних і місцевих мовників. Серед сталих переваг марафону «Єдині новини» для системи інформаційної безпеки – офіційна інформація від першоджерел, її верифікація, відсутність російських наративів, проросійських політиків, воєнної цензури.

І якщо для російської пропаганди та дезінформації національний телепростір з моменту початку вторгнення виявився закритим, то телеграм-канали, різні сайти та месенджери стали основними платформами для дезінформації, фейків, втручань і фактично ведення інформаційного тероризму. Суттєві обмеження для подібної діяльності запроваджені з боку фейсбуку, твіттера, ютубу, однак це не означає повної відсутності подібного контенту. При цьому не варто недооцінювати цей сегмент, адже опитування Internews [1] (рис. 2) свідчать, що 60% респондентів віддають перевагу саме телеграму як джерелу новин.

#### Користування соціальними мережами для спілкування, 2021-2022



#### Переважна мережа для отримання новин у соціальних мережах, 2021-2022



■ 2022 ■ 2021

**Запитання:**  
Якими соцмережами Ви користуєтесь для спілкування принаймні раз на місяць?  
Якій із соціальних мереж віддаєте перевагу для отримання новин?

**База:**  
Користувачі Інтернету, 2021 N=1413, 2022 N=1319  
Споживачі новин із соціальних мереж, 2021 N=1358, 2022 N=1079

x / x – значуще більше / менше на рівні 95% порівняно з попередньою хвилиною

Рис. 2. Користування соціальними мережами/Переважна мережа для отримання новин у соціальних мережах [1]  
(за даними дослідження InMind на замовлення Internews)

Дослідники з «Детектор медіа» [1] ідентифікували понад 300 телеграм-каналів, а «Центр відстеження дезінформації» [10] виокремив 372 онлайн-платформи, задіяні в пропаганді та дезінформації. Узагальнюючи основні меседжі російських наративів на цих ресурсах, можна виокремити такі: «Україна – маріонетка в руках союзників», «Україна програє економічно і військово у прямому конфлікті з росією», «українці радо зустрічають російську армію», «владу в Україні захопили нацисти і корупціонери», «сусідні країни невдовзі загарбають західні області України», «злочини росіян у Бучі (та інших раніше окупованих населених пунктах) – постановка», «Україна застосовує зброю проти цивільних росіян на прикордонних російських територіях», «українці крадуть і продають на чорному ринку зброю, яку дає Захід»; «Росія не

*краде зерно в Україні і не блокує поставки, як звинувачує Захід», «Нацизм процвітає в українській політиці та суспільстві, підтримується владою в Києві», «США мають мережу лабораторій з біозброї у Східній Європі», «російськомовні мешканці Донбасу піддалися геноциду» тощо.*

Емпіричні дослідження просування наративів у твіттері, проведені групою європейських дослідників [12], підтвердили скоординованість дезінформаційних кампаній. З маркованих як «проросійська підтримка» 349 455 повідомлень, розміщених у твіттері, 251 тис. отримали ретвіти, що дозволило охопити 14,4 млн користувачів з Індії, Південної Африки та США. Посилують поширення повідомлень боти чи «ймовірні боти» [12, с. 5], частка яких визначена на рівні 20,28% (їх акаунти переважно були створені на початку вторгнення). Інші висновки свідчать про «наявність широкомасштабної російської пропагандистської кампанії в соціальних мережах, що є свідченням нових загроз суспільству, які походять від неї» [12, с. 26], а виявлення та нівелювання ботів, фейкових акаунтів може бути ефективною стратегією пом'якшення таких кампаній.

Центр протидії дезінформації у співпраці з Національною радою України з питань телебачення і радіомовлення досліджують [8] російський та міжнародний інформаційний простір і фіксують пропаганду, вкиди, деструктивні інформаційні впливи та дезінформаційні кампанії РФ. Серед основних наративів – «російська федерація веде боротьбу за мир», «Захід – слабкий», «НАТО спровокувало росію до нападу на Україну», «надання Україні зброї сприяє ескалації», «росія воює з НАТО», «Україна – маріонетка НАТО» тощо. Сформована Центром протидії дезінформації та Нацрадою України з питань телебачення і радіомовлення база фейків Кремля доступна державним та недержавним структурам, а транскрибовані тексти пропагандистських передач «НТВ», «Вести недели с Дмитрием Киселевым», «Воскресный вечер с Владимиром Соловьевым» та інші передані правоохоронцям.

Міжнародний характер використання Росією цілого спектра засобів та інструментів поширення дезінформації, пропаганди, вкидів та втручань визнав і Європарламент [13]. Це, зокрема, аналітичні центри та фонди («Russkiy Mir»), спеціальні організації («Rossotrudnichestvo»), багатомовні телевізійні станції («RT»), псевдоінформаційні агентства та мультимедійні платформи («Sputnik»), транскордонні соціальні та релігійні організації (останні позиціонуються як «єдині захисники традиційних християнських цінностей»), соціальні медіа та інтернет-тролі. До різних пакетів європейських санкцій потрапили найбільші медіапропагандисти країни-агресорки: «Russia Today», «Sputnik», «Rossiya RTR»/«RTR Planeta», «Rossiya 24»/«Russia 24», «TV Centre International», «NTV»/«NTV Mir», «REN TV», «Russia-1», «Channel One Russia».

Французькі дослідники Д. Ліччіа та Ж.-Б. Дельомм [14], аналізуючи механізми просування російської пропаганди в інформаційному просторі, відзначають її видозміну внаслідок запроваджених європейських санкцій та способи їх обходу. «Незважаючи на деплатформенність (пропагандистських ресурсів – ЄС) багато груп і сторінок у фейсбуці сьогодні продовжують транслювати контент із цих ЗМІ, використовують візуальний контент, копіюють та переносять матеріали на інші сторінки та мережі, уникаючи посилань» [14]. У ході дослідження було виявлено та ідентифіковано 1,8 тис. каналів, які одномоментно ширять до 8 млн повідомлень, що є свідченням глобального характеру пропагандистської діяльності та значного впливу російської блогосфери на телеграм як канал поширення пропаганди (рис. 3).

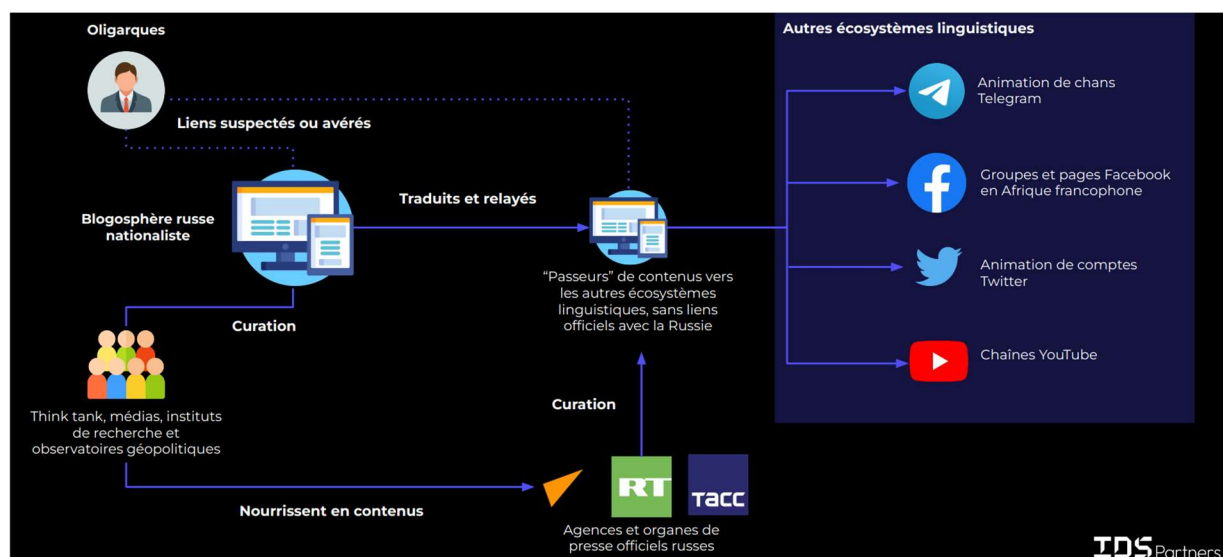


Рис. 3. Поширення проросійського контенту в контексті «деплатформізації» російських ЗМІ RT і Sputnik (за даними дослідження IDS Partners [14])



Пропагандисти через заборони втратили змогу доносити дезінформацію на власних платформах, тому використовують інші ресурси: VPN (у країнах з незаблокованим доступом до серверів), видозмінюють власні та створюють нові платформи (вебсайти, «дзеркальні» сайти), ресурси блогосфери. А після обмеження пропагандистських каналів у Франції, просування російської пропаганди потужностями «Sputnik France» відбувається на франкомовну Африку («Sputnik Afrique») та Латинську Америку із залученням фейкових фейсбук-сторінок та інших цифрових ресурсів, блогерів тощо.

#### IV. Висновки

Отже модель російської пропаганди, що функціонує, із системними загрозами для інформаційної безпеки, вкидами, дезінформацією, маніпуляціями, втручанням у справи третіх країн та медіасередовище, реалізацією ІПСО є частиною державної політики РФ. Медіа, цифрові ресурси, інформаційний простір зазнає безперервних атак, використовується для просування наративів «руського міра» та дестабілізації. В Україні все, це як і інші фактори, передувало окупації Криму та початку війни на сході у 2014 р. і засобами гібридних викликів супроводжувало російсько-українську війну на Донбасі (2014–2022 рр.) та повномасштабне вторгнення (з 24.02.2022). Накопичений Україною досвід мінімізації наслідків руйнівного впливу, втручань у медіасередовище є важливим, а транскордонний характер явища рашизму, протидія дезінформації, різним загрозам залишатимуться пріоритетними і для нашої держави, і для країн демократичного світу. Тож подальші спільні кроки з партнерами з Європейського Союзу та НАТО є взаємонеобхідними для захисту кіберпростору, визначення прозорості соціальних медіа, технологічних платформ, широкого залучення онлайн-інструментарію для аналізу даних, ефективної верифікації та швидкого нівелювання загроз для системи інформаційної безпеки.

#### Список використаної літератури

1. Кремлівська гідра: 300 телеграм-каналів, які отруюють український інфопростір. *Детектор медіа*. URL: <https://detector.media/monitorynh-internetu/article/205954/2022-12-14-kremlivska-gidra-300-telegram-kanaliv-yaki-otruyuyut-ukrainskyu-infoprostir/> (дата звернення: 29.04.2023).
2. Медіанаративи : колективна монографія. Дніпро : ЛІРА, 2022. 116 с.
3. Ревізія історії. Російська історична пропаганда та Україна. Київ : К.І.С., 2019. 99 с.
4. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.
5. Соломін Є. Телебачення Луганщини між війною інформаційною та повномасштабною: знищене відродження. *Образ*. 2023. Вип. 1 (41). С. 16–24.
6. Соломін Є. О. Інформаційна безпека України: від анексії до концепції через війну на сході. *Теле- та радіожурналістика*. 2016. Вип. 15. С. 68–72.
7. Стратегія інформаційної безпеки : Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n7> (дата звернення: 26.03.2023).
8. Центр протидії дезінформації. *Звіту*. URL: <https://cpd.gov.ua/category/reports/> (дата звернення: 29.04.2023).
9. Bidzilya Y. M., Solomin Y. O., Shapovalova H. V., Georgiievskaya V. V., Poplavskaya N. M. The stability of State information in the face of terrorist threats. *Cuestiones Políticas*. 2021. № 39 (70). P. 250–269.
10. Cadier A. Russia-Ukraine Disinformation Tracking Center. *News Guard*. URL: <https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/> (date of request: 29.04.2023).
11. Council of the European Union. *EU Imposes Sanctions on State-Owned Outlets RT/Russia Today and Sputnik's Broadcasting in the EU*. 2022. URL: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> (date of request: 13.03.2023).
12. Geissler D., Bär D., Pröllochs N., Feuerriegel S. Russian propaganda on social media during the 2022 invasion of Ukraine. URL: <https://arxiv.org/pdf/2211.04154> (date of request: 24.03.2023).
13. EU strategic communication to counteract propaganda against it by third parties. URL: [https://www.europarl.europa.eu/doceo/document/A-8-2016-0290\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html) (date of request: 13.03.2023).
14. IDS Partners. La propagande russe à l'épreuve de la déplateformisation (étude). URL: <https://www.ids-partners.com/post/la-propagande-russe-%C3%A0-l-%C3%A9preuve-de-la-d%C3%A9plateformisation-%C3%A9tude> (date of request: 30.04.2023).
15. Newton R. A. Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? *In Janine Davidson Blogspot: Defense in Depth*. 2014 (date of request: 12.03.2023).
16. Park C. Y., Mendelsohn J., Field A., Tsvetkov Y. Challenges and Opportunities in Information Manipulation Detection: An Examination of Wartime Russian Media. *Findings of the Association for Computational Linguistics: EMNLP*. 2022. P. 5209–5235.
17. Pidbereznykh I., Koval O., Solomin Y., Kryvoshein V., Plazova T. Ukrainian policy in the field of information security. *Amazonia Investiga*. 2022. № 11 (60). P. 206–213.
18. Russia's Military Doctrine. *Arms Control Today*. December 2014.

## References

1. Kremlivska hidra: 300 telehram-kanaliv, yaki otruiuiut ukrainskyi infoprostir» [Kremlin Hydra: 300 Telegram channels that poison the Ukrainian information space]. *Detector Media*. Retrived from <https://detector.media/monitorynh-internetu/article/205954/2022-12-14-kremlivska-gidra-300-telegram-kanaliv-yaki-otruiuyut-ukrainskyi-infoprostir/> [in Ukrainian].
2. *Medianaratyvy* [Media narratives: a collective monograph]. (2022). Dnipro: LIRA [in Ukrainian].
3. *Re-viziya istoriyi. Rosijska istorichna propaganda ta Ukrayina* [Revision of history. Russian historical propaganda and Ukraine]. (2019). Kyiv: K.I.S. [in Ukrainian].
4. *Svitova hibrydna viina: Ukrainskyi front* [World hybrid war: Ukrainian front]. (2017). Kyiv: NISD [in Ukrainian].
5. Solomin, Y. (2023). Telebachennia Luhanshchyny mizh viinoiu informatsiinoiu ta povnomasshtabnoiu: znyshchene vidrozhennia [Television of Luhansk region between the information and full-scale war: destroyed revival]. *Obraz*, 1 (41), 16–24. doi: <https://doi.org/10.21272/> [in Ukrainian].
6. Solomin, Ye. O. (2016). Informatsiina bezpeka Ukrainy: vid aneksii do Kontseptsii cherez viinu na skhodi [Information security of Ukraine: from Concept to annexation because of the east]. *Tele- ta radiozhurnalistyka*, 15, 68–72 [in Ukrainian].
7. Decree of the President of Ukraine Information security strategy from December 28 2021, № 685/2021. Retrieved from <https://zakon.rada.gov.ua/laws/show/685/2021#n7> [in Ukrainian].
8. Tsentr protydii dezinformatsii [Center for Countering Disinformation]. *Zvity*. Retrieved from <https://cpd.gov.ua/category/reports/> [in Ukrainian].
9. Bidzilya, Y. M., Solomin, Y. O., Shapovalova, H. V., Georgiievskaya, V. V., & Poplavskaya, N. M. (2021). The stability of State information in the face of terrorist threats. *Cuestiones Políticas*, 39 (70), 250–269 [in English].
10. Cadier, A. (2022). Russia-Ukraine Disinformation Tracking Center. *News Guard*. Retrieved from <https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/> [in English].
11. Council of the European Union. (2022). *EU Imposes Sanctions on State-Owned Outlets RT/Russia Today and Sputnik's Broadcasting in the EU*. Retrieved from <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> [in English].
12. Geissler, D., Bär, D., Pröllochs, N. & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. Retrieved from [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://arxiv.org/pdf/2211.04154.pdf](https://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://arxiv.org/pdf/2211.04154.pdf) [in English].
13. EU strategic communication to counteract propaganda against it by third parties. Retrieved from [https://www.europarl.europa.eu/doceo/document/A-8-2016-0290\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html) [in English].
14. IDS Partners. La propagande russe à l'épreuve de la déplateformisation (étude). Retrieved from <https://www.ids-partners.com/post/la-propagande-russe-%C3%A0-l-%C3%A9preuve-de-la-d%C3%A9plateformisation-%C3%A9tude> [in French].
15. Newson, R. A. (2014). *Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There?*» In Janine Davidson Blogspot: *Defense in Depth* [in English].
16. Park, C. Y., Mendelsohn, J., Field, A., & Tsvetkov, Y. (2022). Challenges and Opportunities in Information Manipulation Detection: An Examination of Wartime Russian Media. *Findings of the Association for Computational Linguistics: EMNLP*, 5209–5235 [in English].
17. Pidberezykh, I., Koval, O., Solomin, Y., Kryvoshein, V., & Plazova, T. (2022). Ukrainian policy in the field of information security. *Amazonia Investiga*, 11 (60), 206–213 [in English].
18. Russia's Military Doctrine. (2014). *Arms Control Today*. December [in English].

Стаття надійшла до редакції 03.05.2023.

Received 03.05.2023.

### Solomin Y. Information Security in the Conditions of War and Interventions in the Media Environment

**The purpose** of the research is to identify systemic threats to information security, ways of spreading Russian propaganda narratives, with inclusions, disinformation, manipulation, interference in the media environment, and ways to minimize the destructive impact on various technological platforms.

**Research methodology.** To study the problems of interventions, systematic propaganda campaigns, the method of selection and classification of data, their processing and analysis was applied, which made it possible to reveal the current and long-term goals of the manipulation technologies involved.

**The results.** The promotion of the narratives of the "Russian world" in Ukraine took place by means of hybrid war and loss of territories, systematic interference in the information field and its imbalance. For Russian propaganda, the national television and radio space has been closed since the beginning of the war, instead, Telegram channels, various sites and Messengers have become the main platforms for disinformation, fakes, interventions and actually conducting information terrorism. The international

nature of Russia's use of a whole range of means and instruments of destabilization and intervention was recognized by the European Parliament and limited or banned their main technological resources. Instead, due to the loss of opportunities to promote disinformation on their own platforms, propagandists use workarounds.

**Novelty.** The components of informational and propaganda challenges of hybrid aggression and ongoing war in the media environment and cyberspace are universalized.

**Practical meaning.** The results of the research can be used during the study of journalism, political science, and history disciplines. The methodological base can be useful for further scientific investigations and research in the field of strategic communications and information security.

**Key words:** propaganda, disinformation, racism, telespace, digital resources, information space, hybrid war.

**Solomin Ye. Bezpieczeństwo informacji w warunkach wojny i interwencji w środowisku mediów**

**Celem badania** jest identyfikacja systemowych zagrożeń bezpieczeństwa informacji, sposobów rozpowszechniania rosyjskich narracji propagandowych, z inkluzjami, dezinformacją, manipulacją, ingerencją w środowisko medialne oraz sposobów minimalizowania destrukcyjnego wpływu na różne platformy technologiczne.

**Metodologia badania.** Do badania problematyki interwencji, systematycznych kampanii propagandowych zastosowano metodę selekcji i klasyfikacji danych, ich przetwarzanie i analizę, co umożliwiło ujawnienie aktualnych i długofalowych celów zastosowanych technologii manipulacyjnych.

**Wyniki.** Promocja narracji «rosyjskiego świata» na Ukrainie odbywała się poprzez wojnę hybrydową i utratę terytoriów, systematyczną ingerencję w pole informacyjne i jego nierównowagę. Dla rosyjskiej propagandy krajowa przestrzeń telewizyjna i radiowa została zamknięta od początku wojny, zamiast tego kanały Telegram, różne strony i komunikatory stały się głównymi platformami dezinformacji, fałszerstw, interwencji i faktycznego prowadzenia terroryzmu informacyjnego. Międzynarodowy charakter wykorzystania przez Rosję całej gamy środków i instrumentów destabilizacji i interwencji został uznany przez Parlament Europejski i ograniczył lub zakazał ich głównych zasobów technologicznych. Zamiast tego, z powodu utraty możliwości promowania dezinformacji na własnych platformach, propagandyści stosują obejścia.

**Nowość.** Komponenty informacyjnych i propagandowych wyzwań agresji hybrydowej i toczącej się wojny w środowisku medialnym i cyberprzestrzeni ulegają uniwersalizacji.

**Praktyczne znaczenie.** Wyniki badań mogą być wykorzystane podczas studiów na kierunkach dziennikarstwo, politologia i historia. Baza metodologiczna może być przydatna do dalszych badań naukowych i badań w dziedzinie łączności strategicznej i bezpieczeństwa informacji.

**Słowa kluczowe:** propaganda, dezinformacja, rasizm, teleprzestrzeń, zasoby cyfrowe, przestrzeń informacyjna, wojna hybrydowa.