Цимбал Сергій Юрійович

Механізми та технології протидії інформаційній агресії у мережі інтернет

УДК 323.1:165.6 (477)
DOI https://doi.org/10.24195/2414-9616.2026-2.20

Цимбал Сергій Юрійович
здобувач третього (освітньо-наукового) рівня вищої освіти
спеціальності «Політологія»
ДЗ «Південноукраїнський національний педагогічний університет
імені К. Д. Ушинського»
вул. Старопортофранківська, 26, Одеса, Україна
ORCID: 0009-0007-3649-0338

Статтю присвячено комплексному аналізу інформаційної війни у сучасних інтернет-комунікаціях. Інформаційна агресія стала ознакою сучасного мережевого суспільства. Це потужна зброя, яку використовують авторитарні країни та лідери задля впливу на масову аудиторію. Однією із важливих складових російсько-української війни є російська інформаційна агресія у мережі інтернет. Визначено, що інтернет-комунікації перетворили світ на простір глобальної інформаційної боротьби. Метою статті є визначення ефективних механізмів та технологій протидії інформаційній агресії у мережі інтернет. У дослідженні інформаційної агресії та механізмів і технологій протидії їй в умовах російсько-української війни використовуються такі загальнонаукові методи як аналіз та синтез, індукція та дедукція, діалектичний метод, методи аналогії та узагальнення. Застосування системного методу дозволило визначити місце інформаційної агресії у інформаційній війні, а синергетичний метод спрямовується на окреслення ролі інформаційної агресії у руйнуванні політичного порядку та посилення хаосу. За допомогою історичного методу виокремлено етапи російської інформаційної агресії, а комунікативний метод окреслив вплив традиційних медіа та мережевих комунікацій на технології та механізми протидії інформаційній агресії. Інформаційна агресія у мережі інтернет є невід'ємною складовою інформаційної війни. Вона включає кібератаки, вплив на громадську думку за допомогою технологій пропаганди та маніпуляцій, розповсюдження фейків у соціальних мережах з використанням технологій таргетингу та мікротаргетингу. Задля протидії інформаційній агресії застосовуються наступні технології: 1) технологій моніторингу інформаційного простору; 2) застосування технологій блокування джерела інформаційної агресії; 3) моніторинг контенту з метою пошуку вірусів задля протидії кібератакам; 4) технології перевірки фото/відео/аудіо інформації з метою виявлення ознак маніпуляцій (Deepfakes); 5) сучасні технології перевірки даних (фактчекінг) задля оперативного реагування на фейки та їх спростування; 6) технології контрпропаганди та технології перенесення інформаційної війни на територію противника. До механізмів протидії інформаційній агресії у мережі інтернет слід віднести організаційні та правові механізми, соціокультурний механізм та комунікативний механізм. Усі вони передбачають взаємодію між інститутами публічної влади, громадянським суспільством та міжнародними партнерами.

Ключові слова: *інформаційна агресія, інформаційна війна, мережа інтернет, політика, політичні комунікації, механізми протидії інформаційній агресії, політичні технології, демократія.*

Вступ. Інформаційна агресія стала ознакою сучасного мережевого суспільства. Це потужна зброя, яку використовують авторитарні країни та лідери задля впливу на масову аудиторію. Однією із важливих складових російсько-української війни є російська інформаційна агресія. Вона спрямована як на українське суспільство, так і на глобальну міжнародну аудиторію, містить пропаганду та спеціальні інформаційні операції, маніпуляцію та дезінформацію. Варто погодитись із наступною думкою: «У 2014 році Україна зіштовхнулася з таким видом агресії з боку РФ, який науковці називають гібридною війною, яка передбачає поєднання традиційних і нетрадиційних методів агресії. Україна стала жертвою російської збройної агресії, що призвела до анексії Криму та військові дії на Донбасі та у подальшому до повномасштабного вторгнення у 2022 році. Інформація стала однією зі складових російської агресії проти України, що дозволяє говорити про наявність інформаційної війни між Україною та РФ. Йдеться про активне поширення негативної (часто неправдивої або викривленої) інформації про Україну з метою дискредитації нашої держави на світовій арені, кібератаки, пропаганда російських цінностей серед українського населення тощо» [4, с. 55].

Слід відзначити, що російська інформаційна агресія сучасної епохи «супроводжувала» відносини наших держав з моменту підготовки до референдуму щодо Незалежності України. Інформаційні операції, спрямовані як на українську так і на міжнародну аудиторію були ознакою протистояння навколо о. Тузла, «газових війн», виборів в Україні, навіть спортивних змагань та конкурсу «Євробачення» тощо. Зокрема, у 2003 році інформаційна війна навколо острова Тузла стала одним із перших проявів російської агресивної інформаційної політики, спрямованою на тестування реакції української влади та міжнародної спільноти. А виступ на «Євробаченні» у 2007 році В. Сердючки (А. Данилко) спричинив хвилю російської інформаційної агресії через фразу «лаша тумбай», яка було сприйнята російськими пропагандистами як «раша гудбай». З початком війни А. Данилко офіційно перейменував цю пісню на «Russia, goodbye» [1].

Якщо епоха традиційних медіа встановлювала технологічні обмеження для інформаційної експансії та агресії одних держав проти інших (пресу було складно перевозити через державні кордони, а для протидії телебаченню та радіомовленню вистачало системи радіоелектронних перешкод), то інтернет-комунікації перетворили світ у простір глобальної інформаційної боротьби.

Для інформаційної агресії використовуються не лише інтернет-комунікації (мережі, месенджери, платформи та мережеві медіа), а й технології мобільного зв'язку. До інформаційної агресії слід також віднести методи психологічного впливу, які використовуються задля зниження рівня довіри між інститутами публічної влади та суспільством, спрямовані на делегітимізацію влади в Україні та зниження обороноздатності. Погодимось із тим, що «Інформаційна агресія виступає ключовим інструментом у веденні війни з боку російської федерації, яка використовує пропаганду для маніпулювання громадською думкою не лише в Україні, але й у міжнародному масштабі» [3, с. 68]. Усе вищезазначене актуалізує дослідження механізмів та технологій протидії інформаційній агресії у мережі інтернет.

Мета та завдання. Метою статті є визначення ефективних механізмів та технологій протидії інформаційній агресії у мережі інтернет. Визначена мета обумовила необхідність постановки та вирішення наступних дослідницьких завдань: 1) визначити сутність інформаційної агресії у мережі інтернет; 2) обґрунтувати необхідність розробки не лише технологій реагування на інформаційну агресію, а й вироблення дієвих механізмів (правових, комунікативних, організаційних, мотиваційних, економічних тощо) задля ефективної та комплексної протидії інформаційній агресії у мережі інтернет; 3) розкрити конкретні механізми та технології протидії російській інформаційної агресії як складової російсько-української війни.

Методи дослідження. У дослідженні інформаційної агресії та механізмів і технологій протидії їй в умовах російсько-української війни використовуються такі загальнонаукові методи як аналіз та синтез, індукція та дедукція, діалектичний метод, методи аналогії та узагальнення. Застосування системного методу дозволило визначити місце інформаційної агресії у інформаційній війні, а синергетичний метод спрямовується на окреслення ролі інформаційної агресії у руйнуванні політичного порядку та посилення хаосу. Серед українських дослідників протидії інформаційній агресії у мережі інтернет слід відзначити А. Бадер, А. Бахметьєва, М. Бучина, С. Вовк, Ю. Данько, С. Демедюк, Н. Елящевську, Т. Короткого, О. Кирилову, С. Наумкіну, ін.

Інформаційна агресія є складником інформаційної війни. Погодимось із наступним визначенням: «У XXI столітті на зміну традиційним видам збройних конфліктів приходять нові форми протистояння між державами. Найчастіше щодо них в широкому значенні використовують дефініцію «війна». Виділяють дипломатичні, торгові, економічні, енергетичні, психологічні та інформаційні війни. І хоча класичне поняття «війна», як збройний конфлікт міжнародного / неміжнародного чи змішаного характеру, має своє спеціальне визначення і зміст, однак такі конфлікти на даний час не можливі без інформаційної складової, і найчастіше інформаційні війни мають основне значення для отримання переваги або деморалізації супротивника, легітимації агресії та обґрунтування перемоги у збройному конфлікті при відповідній дискредитації противника» [4, с. 55].

За допомогою історичного методу виокремлено етапи російської інформаційної агресії, а комунікативний метод окреслив вплив традиційних медіа та мережевих комунікацій на технології та механізми протидії інформаційній агресії.

Результати. Протидія інформаційній агресії у мережі інтернет є складним, багатовимірним процесом, який поєднує комплексне застосування політичних технологій та вироблення дієвих механізмів у публічній політиці та публічному управлінні. Адже, головне завдання полягає не у проективній реакції на чергову інформаційну провокацію, маніпуляцію чи пропаганду. Швидкість інформаційних потоків під час інформаційної агресії часто перевищує здатність надати адекватну відповідь.

Погодимось: «Російська інформаційна агресія спрямована на зниження довіри до українських владних структур, розпалювання міжетнічних конфліктів та загальну дестабілізацію ситуації в країні, що несе ризик зниження обороноздатності України… У зв'язку з цим, розвиток і впровадження ефективних практик протидії інформаційній агресії є важливим завданням для України. Ефективні стратегії протидії інформаційній агресії включають комплексні заходи на державному, інституційному та громадянському рівнях, які спрямовані на формування інформаційної культури українського суспільства» [3, с. 69].

До сучасних технологій інформаційної агресії у мережі інтернет відносять кібератаки, технології пропаганди та маніпуляції, інформаційну розвідку та дезінформацію, психологічні спецоперації тощо.

Варто безумовно погодитись із тим, що «Аналізуючи результати найвідоміших міжнародних військових, політичних та економічних конфліктів кінця XX – початку XXI ст., стає зрозумілим, що інформаційно-психологічну зброю сьогодні треба прирівняти до зброї масового знищення. Не вбиваючи фізично, психотехнології спричиняють групові, а також масові психічні розлади, вибухаючи згодом у соціальні конфлікти, жертвами яких стають конкретні індивіди. Використовуючи весь спектр інформаційно-психологічних операцій, соціальні мережі у інформаційному протистоянні можуть забезпечувати: − координацію протестних та терористичних

рухів; − поширення контенту, що належить до категорії інформаційної зброї; − отримання важливої для нападника інформації про персоналії або організації; − збирання розвідувальної інформації про офлайн-дії противника; − відстежування суспільних настроїв; − локалізацію джерел інформації, що становлять небезпеку» [4, с. 57].

Сутність протидії інформаційні агресії у мережі інтернет визначається як створення інформаційного простору взаємодії між інститутами публічної влади, громадянським суспільством, медіа та мережевими спільнотами задля зменшення руйнівної сили ворожого інформаційного повідомлення, а надзавданням виступає формування середовища, яке не є чутливим для інформаційної агресії. Взаємодія із громадянським суспільством полягає не лише у здійсненні постійного моніторингу інформаційного контенту та аналізу інформаційних повідомлень, а й проведенні освітніх заходів, тренінгів із медіаграмотності тощо.

Солідаризуємось із наступною думкою: «Формування інформаційної культури суспільства вимагає від української влади систематичної і комплексної стратегії на рівні держави у взаємодії з інститутами громадянського суспільства. Так, незалежність та професіоналізм ЗМІ відіграють визначальну роль у протидії інформаційній російській агресії в Україні. Сучасне інформаційне середовище засноване на постійному потоці новин та інформації, яка може бути використана як засіб маніпуляції та впливу на суспільство. У цьому контексті, ключовими факторами є ефективна комунікація, фактична перевірка інформації та здатність розрізняти дезінформацію від правдивої інформації. Професійна робота ЗМІ, спрямована на висвітлення подій та аналіз суспільно-політичної ситуації, є важливим чинником формування об'єктивної картини світу серед громадян. Незалежність редакцій від політичних або комерційних впливів дозволяє забезпечити об'єктивність та достовірність інформації, що подається громадськості» [3, с. 69].

У контексті російсько-української війни це означає пошук механізмів протидії інформаційній агресії, які мають бути адаптовані для протистояння гібридним загрозам та забезпеченню національної безпеки України.

До технологій протидії інформаційній агресії відносяться: 1) технологій моніторингу інформаційного простору (соціальних мереж, месенджерів, платформ, мережевих медіа, ін.) та аналізу інформаційних повідомлень з метою виявлення аномальної активності, використання «ботоферм» та блогерів задля поширення фейків. Щодо феномену блогерства, то саме блогери у мережі інтернет є «лідерами громадської думки». Солідаризуємось із наступною думкою: «…варто відзначити феномен появи «лідерів громадської думки», які можуть бути представлені як ще одна незалежна особистість, група або сторінка в соціальній мережі. Користувачі беззаперечно довіряють їм і навіть вважають їх найнадійнішим джерелом інформації з певних питань, іноді ігноруючи той факт, що вони можуть не бути експертами в цій галузі. За допомогою таких «лідерів громадської думки» країни та компанії можуть забезпечити прихильність користувачів або переконувати користувачів у своїх ідеях підтримки конкретних важливих подій, чи явищ у функціонуванні держави чи різних сферах суспільства» [4, с. 60]; 2) застосування усіх можливих технологій задля блокування джерела інформаційної агресії (від скарг у соціальних мережах до блокування доступу до ресурсів, які беруть участь у інформаційній агресії); 3) аналіз файлів та підозрілого контенту на предмет пошуку вірусів з метою уникнення кібератак, як складників інформаційної агресії; 4) технології перевірки фото/відео/аудіо інформації з метою виявлення ознак маніпуляцій (Deepfakes); 5) сучасні технології перевірки даних (фактчекінг) задля оперативного реагування на фейки та їх спростування; 6) технології контрпропаганди та технології перенесення інформаційної війни на територію противника.

Особливо слід наголосити на необхідності підвищення рівня медіаграмотності громадян, здатність розпізнавати інформаційну агресію, провокації та маніпуляції, а також адекватно реагувати на них.

Слід погодитись із тим, що «Здатність розпізнавати дезінформацію та фейкові новини стає ключовою для громадян у контексті постійного потоку інформації з різних джерел. Розвиток медіаграмотності серед населення, а також підвищення уваги до джерел та авторитетності інформації стають важливими завданнями для суспільства. Такий підхід сприяє побудові стійкого механізму протидії інформаційній агресії та підвищує рівень інформаційної безпеки в країні. Високий рівень свідомості громадян та готовності критично мислити стають надзвичайно важливими в умовах, коли дезінформація та фейкові новини активно використовуються для маніпулювання громадською думкою. Освіта ж громадян у сфері медіаграмотності є підґрунтям для їхньої здатності розпізнавати дезінформацію та критично аналізувати інформаційні потоки. Спільна діяльність громадськості, державних інституцій та громадських організацій стає ключовим елементом ефективної протидії інформаційній агресії» [2, с. 25].

Окремо слід відзначити напрямок стратегічних комунікацій, який є проміжною ланкою між технологіями та механізмами протидії інформаційній агресії. Стратегічні комунікації є інтегрованим та скоординованим між державними та недержавними агентами використанням комунікативних можливостей зв'язків із громадськістю, публічної дипломатії, мережевих спільнот та інформаційних операцій для досягнення визначених цілей.

Слід безумовно погодитись із наступним: «Розвиток системи стратегічних комунікацій спрямований на забезпечення національних інтересів України, які є важливою складовою національної безпеки держави. Зауважимо що стратегічні комунікації України перебувають на стадії становлення через активне залучення зарубіжного досвіду щодо практики здійснення ефективних державних комунікацій [6, с. 273]… Стратегічні комунікації активно використовують сферу сучасних технологій та мережу інтернет з метою отримання та передачі інформації, координації інформаційних потоків, а також для аналізу інформаційного простору для виявлення та оцінки потенційних загроз, так як кіберпростір може використовуватися для виведення з ладу системи комунікацій супротивника. Проте війна в Україні продемонструвала, що кіберпростір також може використовуватись для проведення інформаційних операцій, де основними цілями є не машини чи мережі, а індивідууми. Інтернет та соціальні медіа, через їх здатність швидко поширювати інформацію з невеликими витратами все частіше використовується для проведення пропаганди, інформаційної війни та психологічних операцій, що може суттєво змінити як сприйняття так і поведінку цільової аудиторії» [6, с. 275].

Серед механізмів протидії інформаційній агресії слід відзначити: 1) організаційні та правові механізми. До них відносяться як законодавче регулювання, зокрема, встановлення відповідальності за поширення дезінформації, закликів до повалення конституційного ладу та кібератаки так і співпраця із зарубіжними партнерами (державними і недержавними) для посилення інституційної спроможності інститутів публічної влади та громадянського суспільства в Україні; 2) соціокультурні механізми протидії інформаційні агресії. Йдеться про формування критичного мислення та медіаграмотності, а передусім – розвиток та підтримку проектів, спрямованих на посилення національної та політичної ідентичності. Погодимось: «В умовах глобалізації розвиток особистості виступає одним із головних чинників успішності суспільства та держави. Повною мірою це стосується українського суспільства, у якому, поряд із інституційними, політичними та економічними складовими демократичних реформ зростає вага культурних факторів самовизначення індивіда у процесі формування громадянського суспільства та правової демократичної держави. Соціокультурна ідентичність конструюється у процесі усвідомлення громадянином ціннісних основ та культурних орієнтирів власної діяльності… інтерпретації ідентичності доби модерну пройшли три історичні етапи, які глибоко пов'язані із еволюцією політичної та економічної системи. По-перше, ідентичність, яка є основою легітимізуючих стратегій є характерною для індустріального суспільства. По-друге, резистентна ідентичність, яка формується на основі презентації локальних спільнот та потреби їх визнання на національному та глобальному рівні. По-третє, проектна ідентичність, яка виступає основою формування особистості, як актора, дійової особи інформаціонального суспільства» [5, с. 42]; 3) комунікативний механізм протидії інформаційній агресії у мережі інтернет передбачає налагодження взаємодії (вертикальної та горизонтальної комунікації) між інститутами публічної влади, громадянським суспільством, міжнародними організаціями задля захисту інформаційного простору, нейтралізації ворожих наративів, спрямованих на делегітимацію влади в Україні. Водночас, комунікативний механізм передбачає не лише боротьбу із російськими міфами в інформаційному просторі, а й створення позитивного іміджу України у світі, формування порядку денного українського суспільства на основі національних інтересів.

Комплексне використання цих механізмів дозволить підвищити ефективність протидії інформаційній агресії, зменшити її вплив на громадську думку та забезпечити національну безпеку України.

Висновки. Відтак, визначаючи механізми та технології протидії інформаційній агресії у мережі інтернет слід зазначити наступне. По-перше, інформаційна агресія у мережі інтернет є невід'ємною складовою інформаційної війни. Вона включає кібератаки, вплив на громадську думку за допомогою технологій пропаганди та маніпуляцій, розповсюдження фейків у соціальних мережах з використанням технологій таргетингу та мікротаргетингу.

По-друге, задля протидії інформаційній агресії застосовуються наступні технології: 1) технологій моніторингу інформаційного простору; 2) застосування технологій блокування джерела інформаційної агресії; 3) моніторинг контенту з метою пошуку вірусів задля протидії кібератакам; 4) технології перевірки фото/відео/аудіо інформації з метою виявлення ознак маніпуляцій (Deepfakes); 5) сучасні технології перевірки даних (фактчекінг) задля оперативного реагування на фейки та їх спростування; 6) технології контрпропаганди та технології перенесення інформаційної війни на територію противника.

По-третє, до механізмів протидії інформаційній агресії у мережі інтернет слід віднести організаційні та правові механізми, соціокультурний механізм та комунікативний механізм. Усі вони передбачають взаємодію між інститутами публічної влади, громадянським суспільством та міжнародними партнерами.

ЛІТЕРАТУРА:

1. Андрій Данилко розповів, як насправді відбувся скандал з «Раша, Гудбай» після Євробачення. *Регіональні Новини*. 21 травня 2025 року. URL: https://regionews.ua/ukr/news/life/1747792537-andriy-danilko-rozpoviv-yak-naspravdi-vidbuvsya-skandal-z-rasha-gudbay-pislya-evrobachennya

2. Вовк С. Ефективність протидії інформаційній агресії Росії. *Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів* : матеріали VIII Всеукраїнської науково-практичної конференції, м. Одеса, 30 квітня 2024 року. Одеса : ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2024. С.24-27. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/19598/1/Vovk.pdf

3. Вовк С. Практики протидії інформаційній агресії Росії. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2024. Випуск 57. С. 68–74. DOI https://doi.org/10.30970/PPS.2024.57.9

4. Данько Ю.А. Соціальні мережі як інструмент інформаційної війни РФ проти України: особливості та механізми протидії. *Сучасне суспільство.* 2023. Том 2. № 27. С. 54-66. DOI: https://doi.org/10.34142/24130060.2023.27.2.05

5. Малінін В. В. Механізми формування соціокультурної ідентичності в умовах паритетної демократії. *Актуальні проблеми політики*. 2012. Вип. 47. С. 42-48. URL: https://app.nuoua.od.ua/archive/47_2012/8.pdf

6. Сидоренко І. Стратегічні комунікації України. *Evropský politický a právní diskurz.* 2018. Sv. 5, Vyd. 2. С. 273-279. URL: http://nbuv.gov.ua/UJRN/evrpol_2018_5_2_38.

REFERENCES:

1. Danylko, A. (2025). Andrii Danylko rozpoviv, yak naspravdi vidbuvsia skandal z “Rasha, Hudbai” pislia Yevrobachennia [Andrii Danylko рассказал how the “Russia, Goodbye” scandal actually happened after Eurovision]. Rehionalni novyny, May 21. Available at: https://regionews.ua/ukr/news/life/1747792537-andriy-danilko-rozpoviv-yak-naspravdi-vidbuvsya-skandal-z-rasha-gudbay-pislya-evrobachennya [in Ukrainian].

2. Vovk, S. (2024). Efektyvnist protydii informatsiinii ahresii Rosii [Effectiveness of counteracting Russia’s information aggression]. In: Suchasna ukrainska derzhava: vektory rozvytku ta shliakhy mobilizatsii resursiv: materialy VIII Vseukrainskoi naukovo-praktychnoi konferentsii, Odesa, April 30. Odesa: Pivdennoukrainskyi natsionalnyi pedahohichnyi universytet imeni K. D. Ushynskoho; Tsentr sotsialno-politychnykh doslidzhen “Politicus”, pp. 24–27. Available at: http://dspace.pdpu.edu.ua/bitstream/123456789/19598/1/Vovk.pdf [in Ukrainian].

3. Vovk, S. (2024). Praktyky protydii informatsiinii ahresii Rosii [Practices of counteracting Russia’s information aggression]. Visnyk Lvivskoho universytetu. Seriia filosofsko-politolohichni studii, iss. 57, pp. 68–74. DOI: https://doi.org/10.30970/PPS.2024.57.9 [in Ukrainian].

4. Danko, Yu.A. (2023). Sotsialni merezhi yak instrument informatsiinoi viiny RF proty Ukrainy: osoblyvosti ta mekhanizmy protydii [Social networks as a tool of Russia’s information war against Ukraine: features and counteraction mechanisms]. Suchasne suspilstvo, vol. 2, no. 27, pp. 54–66. DOI: https://doi.org/10.34142/24130060.2023.27.2.05 [in Ukrainian].

5. Malinin, V.V. (2012). Mekhanizmy formuvannia sotsiokulturnoi identychnosti v umovakh parytetnoi demokratii [Mechanisms of formation of sociocultural identity in conditions of parity democracy]. Aktualni problemy polityky, iss. 47, pp. 42–48. Available at: https://app.nuoua.od.ua/archive/47_2012/8.pdf [in Ukrainian].

6. Sydorenko, I. (2018). Stratehichni komunikatsii Ukrainy [Strategic communications of Ukraine]. Evropský politický a právní diskurz, vol. 5, iss. 2, pp. 273–279. Available at: http://nbuv.gov.ua/UJRN/evrpol_2018_5_2_38 [in Ukrainian].

Mechanisms and technologies to counter information aggression on the internet

Tsymbal Serhiy Yuriyovych

Student of the Third (Educational and Scientific) Level of Higher Education Specialty “Political Science”
State Higher Educational Institution “South Ukrainian National Pedagogical University named after K. D. Ushynsky”
Staroportofrankivska str., 26, Odesa, Ukraine
ORCID: 0009-0007-3649-0338

The article is devoted to a comprehensive analysis of information warfare in modern Internet communications. Information aggression has become a feature of the modern network society. It is a powerful weapon used by authoritarian countries and leaders to influence the mass audience. One of the important components of the Russian-Ukrainian war is Russian information aggression on the Internet. It is determined that Internet communications have turned the world into a space of global information struggle.

The purpose of the article is to determine effective mechanisms and technologies for countering information aggression on the Internet.

In the study of information aggression and mechanisms and technologies for countering it in the conditions of the Russian-Ukrainian war, such general scientific methods as analysis and synthesis, induction and deduction, dialectical method, methods of analogy and generalization are used. The application of the systemic method made it possible to determine the place of information aggression in the information war, and the synergistic method is aimed at outlining the role of information aggression in the destruction of political order and the intensification of chaos. The historical method identified the stages of Russian information aggression, and the communicative method outlined the influence of traditional media and network communications on technologies and mechanisms for countering information aggression.

Information aggression on the Internet is an integral part of information warfare. It includes cyberattacks, influencing public opinion through propaganda and manipulation technologies, and spreading fakes on social networks using targeting and microtargeting technologies. The following technologies are used to counter information aggression: 1) information space monitoring technologies; 2) the use of technologies to block the source of information aggression; 3) content monitoring to search for viruses to counter cyberattacks; 4) technologies for checking photo/video/audio information to detect signs of manipulation (Deepfakes); 5) modern data verification technologies (fact checking) to promptly respond to fakes and refute them; 6) counter-propaganda technologies and technologies for transferring information warfare to the enemy’s territory. Mechanisms for countering information aggression on the Internet include organizational and legal mechanisms, socio-cultural mechanisms, and communication mechanisms. All of them involve interaction between public authorities, civil society, and international partners.

Key words: *information aggression, information warfare, the Internet, politics, political communications, mechanisms for countering information aggression, political technologies, democracy.*

Дата першого надходження статті до видання: 12.03.2026
Дата прийняття статті до друку після рецензування: 15.04.2026
Дата публікації (оприлюднення) статті: 21.05.2026