



УДК 327:325

DOI <https://doi.org/10.32782/2305-9389/2024.31.21>

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У ПОЛІТИЧНІЙ ПРАКТИЦІ

Кобець Тарас,

аспірант кафедри політології

Прикарпатського національного університету імені Василя Стефаника

ORCID ID: 0009-0001-2179-321X

У сучасному світі стрімкого розвитку технологій інформація стає одним із найпотужніших складників політичної боротьби. Технології інформаційних операцій, що передбачають використання медіа, соціальних мереж та цифрових платформ для впливу на громадську думку й політичні процеси, відіграють дедалі важливішу роль. Інформаційні операції охоплюють широкий спектр – від поширення пропаганди та дезінформації до ведення психологічної війни, і їх використовують як державні, так і недержавні суб'єкти. Метою таких операцій є формування певного політичного порядку, вплив на рішення виборців та політичні результати, що й формує актуальність дослідження.

У статті розглянуто ключові аспекти використання технологій інформаційних операцій у політичній практиці, їх вплив на демократичні процеси та механізми поширення політичних наративів через цифрові канали. Особливу увагу приділено методам виявлення та протидії таким операціям, а також оцінці ефективності наявних регулятивних заходів для захисту інформаційного простору. Автори аналізують вплив соціальних мереж, алгоритмів штучного інтелекту та великих даних на поширення інформаційних операцій, які використовують для маніпуляції електоральними процесами, підризу політичної стабільності, а також формування та підтримки політичних наративів. У статті також акцентується увага на тому, як інформаційні операції впливають на демократичні процеси, викликаючи недовіру до традиційних медіа, інститутів влади й політичних процесів, що здатне призвести до політичної радикалізації та поляризації суспільства. Аналізується роль держав і міжнародних організацій у протидії таким загрозам, зокрема способи підвищення інформаційної безпеки та розробка стратегій щодо боротьби з дезінформацією. У висновках акцентовано на необхідності посилити регулювання та розробити етичні норми для використання інформаційних технологій у політичній сфері, а також на важливості розвинути медіаграмотність як засіб захисту громадян від маніпулятивного впливу.

Ключові слова: інформація, зброя, війна, стратегія, політична кампанія, дискредитація.

Kobets Taras. Use of information operations technologies in political practice

In today's world of rapid technological development, information is becoming one of the most powerful components of political struggle. Information operations technologies, which include the use of media, social networks and digital platforms to influence public opinion and political processes, are playing an increasingly important role. Information operations cover a wide range of activities, from spreading propaganda and disinformation to conducting psychological warfare, and are used by both state and non-state actors. The purpose of such operations is to shape a certain political order; influence voters' decisions and political outcomes, which is why this study is relevant.

This article examines the key aspects of the use of information operations technologies in political practice, their impact on democratic processes and mechanisms for disseminating political narratives through digital channels. Particular attention is paid to methods of detecting and counteracting such operations, as well as assessing the effectiveness of existing regulatory measures to protect the information space. The authors analyze the impact of social media, artificial intelligence algorithms, and big data on the spread of information operations used to manipulate electoral processes, undermine political stability, and shape and support political narratives. The article also focuses on how information operations affect democratic processes, causing distrust of traditional media, government institutions and political processes, which can lead to political radicalization and polarization of society. The article analyzes the role of states and international organizations in countering such threats, including ways to improve information security and develop strategies to combat disinformation. The conclusions emphasize the need to strengthen regulation and develop ethical standards for the use of information technology in the political sphere, as well as the importance of developing media literacy as a means of protecting citizens from manipulative influence.

Key words: information, weapons, war, strategy, political campaign, discreditation.

Актуальність теми. Інформаційна індустрія в сучасному світі залишається провідною галуззю діяльності, куди щорічно інвестують дедалі більшу кількість ресурсів. Брак інформації так чи так відображається на втратах у всіх аспектах життєдіяльності. Так, поширеними стають так звані інформаційні операції, що відображають як легальну сферу діяльності, так і певні тіньові операції, розуміння яких здатне вберегти суб'єкта від потенційних проблем чи негативних наслідків.



Концепт «інформаційні операції» сформувався на початку XXI ст. і як феномен, притаманний власне періоду активної глобалізації та інформатизації, дає змогу більш точно дослідити природу та вивчити зміст поняття інформаційних воєн. Як правило, під ними розуміють цілеспрямовані дії, орієнтовані на досягнення інформаційної переваги через завдання шкоди процесами, що відбуваються на стороні ворога, при цьому захищаючи власні інтереси та інформаційні системи від вторгнення. Інформаційні операції та мікрояви відповідних протиборств ми спостерігаємо щодня, починаючи від просування товарів і послуг у вигляді реклами й завершуючи передвиборчими кампаніями та спробами рейдерських атак.

Відповідно, у контексті аналізу інформаційних воєн конкретна операція розглядається як процес застосування зброї – поширення, обробки, передавання, одержання даних. Специфіка використання інформаційних операцій розкривається залежно від сегмента, про який ідеться. Особливо яскраво це простежується на прикладі політичної практики, як на цьому наголошено в дослідженнях О. Верголяс, у яких розкрито юридичний аспект проведення інформаційних операцій [2]; монографії В. П. Горбуліна, у якій зазначено на співвідношенні інформаційних операцій та безпеки суспільства [3]. Цінними стали міркування Ю. Мороз і Ю. Твердохліб [8], які розглядають інформаційно-психологічні операції як найпотужніший та найефективніший засіб досягнення політичних цілей в умовах гібридної війни.

Мета статті – виявити основні стратегії та інструменти інформаційних операцій у політичній сфері, оцінюючи їх ефективність у досягненні політичних цілей, а також визначити наслідки їх використання для демократичних процесів та політичної стабільності.

Виклад основного матеріалу. Останніми роками значно зросла кількість випадків використання інформаційно-комунікаційних технологій та глобального інформаційного середовища для поширення спеціально підготовленого контенту в неправомірних політичних та економічних цілях. Глобалізаційні процеси чітко транслують: інформація перетворилася на стратегічний ресурс, а її контроль і маніпулювання стали важливими інструментами впливу на політичні процеси.

Базовим полем для проведення політичних кампаній слугує інтернет, зокрема соціальні мережі, які дають змогу швидко поширювати інформацію, охоплюючи при цьому обширну аудиторію. Технології штучного інтелекту й великі дані допомагають створювати персоналізовані повідомлення, які враховують інтереси, уподобання та психологічні особливості кожного користувача. Зазначене дає змогу не тільки ефективніше донести потрібну інформацію, а й сприяти поширенню фейкових новин та маніпуляцій.

На сучасному етапі політичні інформаційні операції стали невід'ємною частиною виборчих кампаній і політичних дебатів. Вони можуть бути спрямовані на дискредитацію опонентів, посилення соціальної поляризації, створення ілюзії підтримки певних політичних рішень або впровадження конкретних наративів [7]. Наприклад, під час виборів технології таргетованої реклами часто використовують для того, щоб впливати на окремі групи населення, формуючи в них відповідні політичні вподобання. Політичні інформаційні операції також використовують для управління кризами, коли політики намагаються формувати або змінювати громадську думку [9]. У таких випадках медіаконтроль, швидке реагування та стратегічне використання соціальних мереж дають змогу значно змінювати наративи і впливати на громадські настрої.

В епоху інтернету багато понять стали більш мобільними, плинними, почали видозмінюватися, піддаватися дифузії та взаємодоповнюватися ідеями із суміжних галузей. Не став винятком феномен інформаційної війни. Так, два останні десятиліття нерідко трапляється, що віртуальний складник конфлікту значно перевершує реальний як за діями, так і за наслідками. Сьогодні накопичено значний обсяг даних у цій царині, що потребує ретельного наукового аналізу, класифікації й термінологічної однозначності. Сучасні інформаційні операції – це аж ніяк не класичні інформаційні кампанії, засновані на вибуховому піарі та спецефектах; це оперативні комбінації, у реалізації яких головну роль відіграють класичні методи агентурної, оперативної, оперативно-технічної та оперативно-розшукової роботи. За ними завжди стоять розвідки конкретної держави.

Основні об'єкти впливу під час інформаційних операцій:

- органи публічного управління держави та її збройних сил;
- інформаційно-керівні системи цивільної інфраструктури (телекомунікаційні, включно із засобами масової інформації, транспортні, енергетичного комплексу, фінансового та промислового секторів);
- інформаційно-керівні елементи військової інфраструктури (системи зв'язку, розвідки, бойового управління, тилового забезпечення, управління зброєю);
- лінії, канали зв'язку та передавання даних;
- інформація, що циркулює або зберігається в системах управління;



- суспільство загалом (як цивільне населення, так і особовий склад збройних сил), його державні, економічні та соціальні інститути;
- засоби масової інформації (насамперед електронні);
- керівний склад і персонал автоматизованих систем управління, який бере участь у процесі ухвалення рішень [11].

У період проведення миротворчих операцій об'єктами впливу можуть бути також воєнізовані, партизанські та політичні організації, релігійні й соціальні групи, окремі особи, які відкрито або таємно виступають проти присутності збройних сил або союзників і перешкоджають виконанню ними своєї місії. Оскільки інформаційні операції пов'язані з використанням інформації та інформаційних технологій для впливу на військові та цивільні системи з метою досягнення інформаційної переваги над супротивником, низка фахівців дають подібні визначення інформаційним операціям [5, с. 26]. Інформаційна операція – це комплекс взаємопов'язаних за метою, місцем і часом заходів та акцій, спрямованих на ініціалізацію та управління процесами маніпулювання інформацією, для досягнення й утримання інформаційної переваги шляхом впливу на інформаційні процеси в інформаційних системах противника [2; 8, с. 98]. Сучасні інформаційні операції плануються і проводяться за кодифікованою і формалізованою технологією, з прорахованими реакціями об'єктів впливу, що забезпечує високу ймовірність досягнення мети.

Інформаційна операція структурно налічує послідовність інформаційних атак, об'єднаних єдиним задумом, узгоджених за цілями, завданнями, об'єктами, формами й методами інформаційного впливу [4, с. 72]. Інформаційну атаку проводять у вигляді вкидання в інформаційне поле за політичних та економічних обставин, обраних для атаки. Вкидання – блок спеціально підготовленої інформації, що провокує об'єкт інформаційного впливу на вчинення негайних дій у відповідь (як реакцію на отриманий зовнішній стимул). Інакше кажучи, мета інформаційної операції – впровадження у свідомість і підсвідомість об'єктів програмних установок на дотримання певної моделі поведінки, вигідної організаторам операції.

Використання інформаційних операцій у політичній практиці має далекосяжні наслідки. По-перше, це підриває довіру до традиційних медіа й політичних інститутів, оскільки велика кількість фейкових новин і маніпуляцій ускладнює можливість отримати достовірну інформацію. По-друге, інформаційні операції часто призводять до зростання політичної поляризації, коли суспільство поділяється на ворожі табори через різні наративи та ідеологічні установки. Окреслене, безумовно, посилює соціальне напруження й ускладнює досягнення компромісів у політичних дискусіях.

Після кожної інформаційної атаки витримується період експозиції (тиші), протягом якого ведеться спостереження за реакцією об'єкта на вкидання. Складовим елементом інформаційної операції є психологічний вплив на об'єкт за розробленим планом. Попередньо складають портрет людини або людей, які є об'єктом операції, оцінюють мотивацію їхньої поведінки й прораховують реакції на інформаційний вплив. Далі проводиться контрольований вплив з оцінкою реакцій об'єкта й корекцією подальших дій.

Отже, поняття «інформаційна операція» і «психологічна операція» відображають різні аспекти одного процесу. Коли говорять «інформаційна операція», мається на увазі змістовний і технологічний аспект. Якщо застосовують концепт «психологічна операція», мається на увазі аспект впливу на об'єкт і спостереження за його реакціями. Інформаційні операції, по суті, є основою ведення інформаційної війни; самостійним видом оперативного забезпечення, який реалізує на полі бою концепцію інформаційної війни.

Інформаційна зброя впливає на інформацію, якою володіє ворог і його інформаційні функції. При цьому наші інформаційні функції захищаються, що дає змогу зменшити його волю або можливості вести боротьбу [6]. Тож інформаційна війна в нашому розумінні – це будь-яка дія з використання, руйнування, спотворення ворожої інформації та її функцій; захисту власної інформації проти таких дій і використання військових інформаційних функцій. Указаний термін є основою для таких тверджень-характеристик:

- інформаційна війна – комплексне спільне застосування сил і засобів інформаційної та збройної боротьби;
- інформаційна війна – комунікативна технологія щодо впливу на інформацію та інформаційні системи противника з метою досягнення інформаційної переваги в інтересах національної стратегії, за одночасного захисту власної інформації та своїх інформаційних систем;
- інформаційна війна – тільки засіб, а не кінцева мета, аналогічно до того, як здійснюється бомбардування. Інформаційну війну можна використовувати як засіб для проведення стратегічної атаки або протидії [3].



Першим термін використав «інформаційна війна» американський експерт Томас Рона у звіті «Системи зброї та інформаційна війна», підготовленому ним 1976 року для компанії Boeing. Т. Рона вказав, що інформаційна інфраструктура позиціонується ключовим компонентом американської економіки. Водночас вона стає і вразливою ціллю, як у воєнний, так і в мирний час. Саме цей документ можна вважати першою згадкою терміна «інформаційна війна» [1, с. 159]. Публікація звіту Т. Рона стала початком активної кампанії в засобах масової інформації. Сама постановка проблеми вельми зацікавила американських військових, яким властиво займатися «секретними матеріалами». Військово-повітряні сили США почали активно обговорювати такий концепт уже з 1980 року.

Наприкінці 1996 р. Роберт Банкер, експерт Пентагону, на одному із симпозіумів представив доповідь, присвячену новій військовій доктрині збройних сил США XXI ст. (концепції Force XXI). В її основу покладено поділ усього театру воєнних дій на два складники: традиційний простір і кіберпростір, причому останній має навіть більш вагоме значення. Р. Банкер запропонував доктрину кіберманевру, яка має стати природним доповненням традиційних військових концепцій, що мають мету нейтралізувати або придушити збройні сили противника [10, с. 135]. Так, до числа сфер ведення бойових дій, крім землі, моря, повітря й космосу, тепер входить й інфосфера. Як підкреслюють військові експерти, основними об'єктами ураження в нових війнах будуть інформаційна інфраструктура й психіка противника (з'явився навіть відповідний термін – human network).

Основними формами ведення технічної інформаційної війни є радіоелектронна боротьба, війна з використанням засобів електронної розвідки й завдання віддалених точкових ударів з повітря, психотропна війна, боротьба з хакерами, кібернетична війна. Їй притаманна одна важлива характеристика: ведення інформаційної війни ніколи не буває випадковим або відокремленим, а має на увазі узгоджену діяльність із використання інформації як зброї для ведення бойових дій чи то на реальному полі бою, чи в економічній, політичній, соціальній сферах. Який би сенс у поняття «інформаційна війна» не вкладався, воно народилося в середовищі військових і позначає насамперед жорстку, рішучу й небезпечну діяльність, яку можна порівняти з реальними бойовими діями.

Військові експерти, які сформулювали доктрину інформаційної війни, чітко уявляють собі окремі її грані: це штабна, електронна, психотропна, інформаційно-психологічна, кібернетична війна тощо. Вищенаведене дає змогу виокремити такі ключові особливості інформаційних операцій:

- порівняно низька вартість створення засобів інформаційного протистояння та інформаційної зброї, а відповідно – низькі фінансові та матеріальні витрати на проведення інформаційних операцій;
- ліквідація статусу традиційних державних кордонів при підготовці та проведенні інформаційних операцій;
- посилення ролі управління сприйняттям ситуації через маніпулювання інформацією за її описом і контекстом;
- зміна пріоритетів у діяльності стратегічної розвідки, які зміщуються у сферу завоювання й утримання інформаційної переваги;
- ускладнення завдання виявлення початку інформаційної операції;
- складність створення коаліції проти агресора, який проводить інформаційну операцію.

За цілями та рівнем управління, на яке здійснюється вплив, інформаційні операції класифікують на інформаційні операції на державному рівні та інформаційні операції на військовому рівні.

На державному рівні цілями інформаційної операції є ослаблення позицій держав-конкурентів, підірвання їхніх національно-державних підвалин, порушення системи державного управління завдяки інформаційному впливу на політичну, дипломатичну, економічну та соціальну сфери життя суспільства, проведення інформаційно-психологічних операцій, підривних та інших деморалізаційних пропагандистських акцій. Крім цього, інформаційні операції на державному рівні можуть захищати національні інтереси, запобігати міжнародним конфліктам, припинити провокаційні й терористичні акції, а також забезпечити безпеку національних інформаційних ресурсів.

На військовому рівні інформаційні операції є комплексом заходів, які проводять у масштабах країни, їхніх видів, об'єднаних командувань у зонах і є складовою частиною військових кампаній (операцій). Вони спрямовані на досягнення інформаційної переваги над противником (насамперед в управлінні військами) і захист своїх систем управління. Для цього можуть використовувати будь-які військові й технічні сили та засоби, наявні в розпорядженні, за формального дотримання правових, моральних, дипломатичних, політичних і військових норм [5, с. 24].

За рівнем військового управління, на яке здійснюється вплив, і масштабом впливу інформаційні операції на військовому рівні можуть бути класифіковані так:



– стратегічні інформаційні операції проводять за рішенням військово-політичного керівництва країни, є впливом на елементи державного устрою потенційних супротивників (політичні, військові, економічні та інформаційні) за одночасного захисту своїх державних структур і покликані забезпечити досягнення національних стратегічних цілей;

– оперативні інформаційні операції проводять для забезпечення успішного перебігу військової операції чи кампанії загалом або розв'язання її головних завдань, є впливом на лінії зв'язку, системи тилового забезпечення та бойового управління супротивника за одночасного захисту аналогічних власних систем як своїх збройних сил, так і союзників;

– тактичні інформаційні операції проводять з метою забезпечення розв'язання тактичних військових завдань і зосереджені на впливі на інформацію та інформаційні системи, як-от системи зв'язку, бойового управління, розвідки та інші, які безпосередньо забезпечують ведення бойових дій з'єднаннями й частинами супротивника за одночасного захисту своїх систем.

Водночас перед сторонами під час проведення інформаційних операцій уперше ставлять завдання вплинути на противника ще в загрозовий період (до початку активних бойових дій), щоб забезпечити вигідну для своєї сторони спрямованість процесів управління та ухвалення рішень стороною, яка протистоїть.

У політичній практиці є значна кількість успішних / безуспішних прикладів інформаційних операцій. Згадаємо про найбільш резонансні. Так, російська дезінформаційна кампанія під час виборів президента США 2016 року є одним із найбільш гучних і масштабних прикладів, що мала великий міжнародний резонанс. Росія, за даними численних розслідувань, прагнула вплинути на результат президентських виборів у США, щоб підтримати кандидата Дональда Трампа та послабити позиції його опонентки Гіллари Клінтон. Для цього вони використовували різні методи. Наприклад, основним інструментом було застосування фейкових акаунтів, контрольованих «Агентством інтернет-досліджень» (IRA) із Санкт-Петербурга. Вони поширювали поляризуювальні повідомлення щодо таких тем, як імміграція, расові питання, релігія та зброя, а цільовою аудиторією були громадяни США, яких намагалися розділити за політичними та соціальними ознаками. Не хтувала країна-агресор і хакерськими атаками. Російські спецслужби здійснили кібератаки на сервери демократичної партії та отримали доступ до електронної переписки штабу Гіллари Клінтон. Злиті дані були використані для дискредитації Клінтон та підриву її репутації. Через проросійські ЗМІ та спеціально створені сайти поширювали недостовірні повідомлення, які спотворювали факти, наприклад, щодо діяльності Клінтон на посаді державного секретаря. Як наслідок, інформаційна кампанія значно посилила політичну поляризацію в США. Незважаючи на те що прямий вплив на результат виборів важко оцінити, це призвело до масових дебатів щодо дезінформації, втручання у вибори та майбутнього регулювання соціальних мереж.

Згадаємо також референдум про вихід Великої Британії зі складу ЄС у 2016 році, що став одним із найбільш помітних прикладів маніпуляцій через інформаційні операції. Кампанія за Brexit мала на меті переконати більшість британців у необхідності вийти з ЄС, маніпулюючи страхами щодо імміграції, економічних втрат та втрати суверенітету. Одним із найвідоміших прикладів фейкової інформації було твердження про те, що Велика Британія щотижня виплачує 350 млн фунт. до бюджету ЄС. Така цифра була неправдивою, але стала головним лозунгом кампанії Leave. Через компанію Cambridge Analytica та інші ресурси прихильники Brexit використовували мікротаргетинг у соціальних мережах, щоб поширювати маніпулятивну рекламу, яка зачіпала найбільш гострі теми для різних категорій виборців (наприклад, імміграція, суверенітет, страх перед біженцями). Також є припущення про російське втручання через підтримку дезінформаційної кампанії та фінансову підтримку певних політичних груп, які виступали за Brexit. У результаті референдуму 51,9 % виборців проголосували за вихід Великої Британії з ЄС. Інформаційні операції значно вплинули на рішення виборців, оскільки вони поширювали недостовірну інформацію, маніпулювали страхами та емоціями, що сприяло поляризації суспільства й загостренню конфліктів між прихильниками та противниками Brexit.

Технології цілеспрямованої підготовки та розсилки контенту постійно вдосконалюються: таргетування інформації, використання інтернет-профілів користувачів, фейк-новини та застосування образу лідерів громадської думки для тиражування цих новин. Сьогодні також велике значення надається можливостям використання технологій штучного інтелекту (далі – ШІ) в цій галузі, причому як для захисту, так і для нападу. Видається, що технології ШІ можуть бути використані на кожному з етапів інформаційної операції, але найбільш істотними є можливості з аналізу великих даних, створення та аналізу текстів. Сьогодні видимі зусилля наукової спільноти зосереджені на проблемах використання ШІ для виявлення фейкових новин. Однак ці ж технології можуть бути використані й для зворотної мети – наприклад, створення генераторів правдоподібних текстів із заданим змістом. Що стосується великих



даних, тут можна відзначити значні успіхи у створенні програмних комплексів, які дають змогу проводити глибокий аналіз користувачьких даних у соціальних мережах і, з огляду на це, виявляти лідерів громадської думки та пов'язані з ними групи людей. Такі системи вже активно і з великим успіхом застосовують для превентивного запобігання протиправних інформаційних вкидань й інформаційних дій та атак екстремістської і терористичної спрямованості. В основі подібних заходів лежать постійний моніторинг інтернету і аналіз соціальних мереж.

Висновки. Інформаційний вплив у тому чи тому вигляді супроводжував людську цивілізацію на багатьох ключових етапах її розвитку – і людство адаптувалося до нових умов. Сьогодні ми вже є очевидцями того, як технології штучного інтелекту починають застосовувати для управління масовою поведінкою людей з використанням єдиних загальносвітових систем зв'язку – насамперед мережі інтернет. На державному рівні триває не тільки реалізація наступальних інформаційних операцій, а й активний пошук науково обґрунтованих рішень для проведення захисних та оборонних заходів; проблемам інформаційно-психологічного протиборства приділяється підвищена увага в науковому середовищі, насамперед у центрах, афілійованих із відповідними відомствами. Перспективи подальших наукових пошуків вбачаємо в аналізі основних моделей організації інформаційних воєн.

Література:

1. Баглікова М. Інформаційна війна і Україна. *Науковий вісник Ужгородського університету. Серія: Політологія, Соціологія, Філософія*. Вип. 14. 2010. С. 158–161
2. Верголяс О. О. Правове забезпечення спеціальних інформаційних операцій : дис. ... канд. ю. н. НДІП НАПрН України. Київ, 2020. 287 с.
3. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.
4. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ, 2017. 104 с.
5. Крайнов В. О. Перспективні напрямки удосконалення безпеки інформаційного середовища органів управління військами. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матер. наук.-практ. конф. (Київ, 18.03.2016): у 2 ч. Ч. 1. Київ : Нац. акад. СБУ, 2016. С. 24–27
6. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник. Київ : ВКНУ, 2016. 286 с.
7. Міненко Є. С. Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності : дис.. за спец. політологія. Український державний університет імені Михайла Драгоманова, Київ, 2024. 257 с.
8. Мороз Ю., Твердохліб Ю. Інформаційно-психологічні операції в умовах проведення гібридної війни. *Вісник Львівського університету. Серія міжнародні відносини*. 2016. Вип. 38. С. 97–105
9. Городок М. Д., Карташов А. В., Романенко Є. О., Стасюк В. Ю. Перемога на виборах: технології, кампанії, принципи : практичний посібник; за заг. ред. М. Д. Городка. Київ : 2016. 264 с.
10. Ткаченко В. В. Стандарти вищої освіти у сфері кібербезпеки – важливий інструмент модернізації освітнього процесу та запорука національної безпеки України. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів наук.-практ. конф. Київ : Нац. акад. СБУ, 2017. С. 135–137
11. Шугаєв А. В. Феномен інформаційної війни. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Соціальні комунікації*. 2019. № 4 (2). С. 151–156.