

ПрАТ «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Навчально-науковий інститут права та безпеки ім. Володимира Великого

ЗБІРНИК МАТЕРІАЛІВ

XI Міжнародної науково-практичної конференції

**«Розвиток української держави
в умовах активізації євроінтеграційних процесів»**

08 травня 2026 р.

м. Київ

Кукін І.В.

д.н.держ.упр.,

*доцент кафедри публічного управління та адміністрування
Державного університету інформаційно комунікаційних технологій*

Свірський А.П.

здобувач (першого) бакалаврського рівня вищої освіти

*Навчально-наукового інституту права та
безпеки ім. князя Володимира Великого ПрАТ ВНЗ МАУП*

Розвиток стратегічного планування у сфері протидії інформаційно-психологічним операціям

Перебіг українсько-російської війни показує, що результативність ведення бойових дій суттєво залежить від застосування сторонами збройного конфлікту інформаційно-психологічних операцій. У сучасних гібридних війнах об'єктом ураження є не лише військові сили про-

тивника, а й свідомість, воля, когнітивні здібності населення країни-жертви агресії та міжнародної спільноти.

Немаловажним фактором сучасних міждержавних конфліктів залишається інформаційний вплив країни-агресора на власне населення для забезпечення підтримки агресії з його боку. Ускладнює протидію інформаційно-психологічним операціям той факт, що для їх проведення можуть застосовуватися сучасні алгоритми штучного інтелекту.

Технології протидії сучасним інформаційним загрозам знаходяться на початковому етапі розвитку, що підвищує актуальність дослідження проблем забезпечення інформаційної безпеки людини, суспільства, держави та міжнародної спільноти під час проведення країною-агресором інформаційно-психологічних операцій.

Інформаційно-психологічні операції заздалегідь плануються та координуються. Вони включають комплекс взаємопов'язаних заходів, що посилюють один одного. В сучасних конфліктах суб'єктами інформаційно-психологічних операцій є не лише держави та їх збройні сили, але й спецслужби, терористичні організації, транснаціональні медіакорпорації, мережі анонімних акторів. Об'єктом впливу є свідомість, переконання та поведінка людини, а не фізичне знищення сил та засобів оборони держави. Інформаційно психологічні операції можна вважати інструментом досягнення стратегічних, оперативних або тактичних цілей країни-агресора [1].

Основними цілями інформаційно-психологічних операцій є: перенасичення інформаційного середовища суперечливими повідомленнями; унеможливлення адекватного сприйняття інформації цільовою аудиторією, що перешкоджає раціональному реагуванню нею на розвиток суспільно значущих подій; підміна дійсності штучно сконструйованими наративами [2].

Сучасні дослідники виокремлюють наступні функції інформаційно-психологічних операцій, зокрема: дестабілізуючу (руйнівний вплив на роботу механізмів публічного управління) [3, с. 201]; деструктивну (руйнування вольової цілісності суспільства) [4, с. 58]; конструктивну (формування та підтримка патріотичних настроїв, мотивація добровільної служби в підрозділах сил безпеки та оборони, підтримання довіри до власного командування та союзників, обґрунтування стратегії протиборства); легітимізуючу (обґрунтування законності дій); розвідувальну (отримання інформації про настрої, ймовірну поведінку цільової аудиторії у майбутньому) [2]; стратегічного відволікання (введення противника в оману щодо часу, сил, засобів та планів його дій) [5, с. 80].

З питань забезпечення інформаційної безпеки Законом України «Про національну безпеку України» передбачено обов'язковість розробки

«Стратегії національної безпеки України» та на її основі – «Стратегії кібербезпеки України». Необхідність опрацювання «Стратегії інформаційної безпеки» та «Стратегії протидії інформаційно-профілактичним операціям» зазначеною нормою права не передбачена [6].

На протязі багатьох років в Україні із залученням європейських експертів тривало опрацювання та обговорення проєкту «Концепції інформаційної безпеки України», яка так і не набула статусу нормативно-правового акту [7]. Разом з тим указом Президента України наприкінці 2021 року була введена в дію «Стратегія інформаційної безпеки». Порядок її опрацювання, реалізації, звітності та періодичного удосконалення досі залишається не узгодженим з технологією опрацювання документів стратегічного планування, що визначена Законом України «Про національну безпеку України» [8].

Тривала відсутність в Україні концепції та стратегії протидії інформаційно-психологічним операціям негативно впливає на доцільне визначення системи органів державної виконавчої влади, на які покладаються функції формування та реалізації державної політики, координації спільної діяльності суб'єктів у зазначеній сфері забезпечення національної безпеки України. Ускладнюються процеси опрацювання документів стратегічного планування, що визначені Законом України «Про національну безпеку України».

На нашу думку, впровадження документів стратегічного планування з питань протидії інформаційно-психологічним операціям потребує розробки та впровадження системи індикаторів та показників, їх критичних порогових значень, що дозволяють виявляти та оцінювати динаміку змін швидкості реагування органів державної влади та місцевого самоврядування, інституцій громадянського суспільства і громадян на фейки. Також, одними з важливих показників доцільно вважати: результати оцінки обізнаності громадян щодо забезпечення особистої інформаційної безпеки; розвитку їхньої інформаційної культури; та визначення рівня довіри населення до державних і муніципальних офіційних каналів комунікації.

Окремим напрямом щодо зміцнення стійкості українського суспільства до інформаційно-психологічних операцій вважаємо посилення відповідальності за розповсюдження небезпечної та шкідливої інформації. Удосконалення визначень об'єкта, об'єктивної та суб'єктивної сторони правопорушень у сфері забезпечення інформаційної безпеки.

Утворення стратегічного, координаційного та оперативного рівнів протидії інформаційно-психологічним операціям нагально потребує перерозподілу повноважень, прав та відповідальності суб'єктів публі-

чного управління у зазначеній сфері забезпечення національної безпеки України. В сучасних умовах успішність протидії небезпечним та шкідливим інформаційним впливам країни-агресора залежить від залучення до процесів забезпечення національної безпеки інститутів громадянського суспільства та дієвості громадянського контролю за діяльністю органів державної влади.

В умовах стрімкого розвитку технологій штучного інтелекту та соціальних мереж ефективність протидії інформаційно-психологічним операціям залежить від стану когнітивної стійкості громадян України та населення держав, які є стратегічними партнерами України. Заходи з блокування шкідливих та небезпечних ресурсів дедалі стають більш затратними та мало ефективними. Одними з основних шляхів зміцнення когнітивної стійкості громадян можна вважати цілеспрямований розвиток органами державної влади інформаційної культури населення, подолання цифрової нерівності громадян, популяризація знань щодо розподілу гілок державної влади, публічного управління, міського самоврядування, основ правознавства.

Генеральною Асамблеєю ООН № 3314 (XXIX) від 14.12.1974 визначено наступні ознаки агресії: вторгнення або напад; анексія території; бомбардування; блокада портів; напад на збройні сили; використання території іншої держави; надання державою території іншій державі для агресії; засилання озброєних банд або іррегулярних сил, найманців [9]. На час прийняття зазначеної резолюції неможливо було врахувати перспективи розвитку гібридних війн. На сьогодні зазначений перелік ознак агресії можна вважати недосконалим.

Для посилення захисту міжнародної спільноти від інформаційно-психологічних операцій країни-агресора потребується чітке визначення терміну «інформаційна агресія». Зважаючи на переважно гібридний характер сучасних війн зазначена ознака може бути додана до визначених Генеральною Асамблеєю ООН ознак агресії. Це дозволить прискорити реакцію міжнародної спільноти на початковому етапі розв'язання агресором гібридних війн.

Отже, на сучасному етапі розвитку України та ведення проти неї Російською Федерацією гібридної війни нагально необхідним є розробка концепції та стратегії забезпечення протидії інформаційно-психологічним операціям і плану реалізації її стратегічних цілей. Це дозволить чітко окреслити перелік загроз, відповідні механізми публічного управління, індикатори та показники реалізації стратегічний цілей.

Напрямом подальших досліджень може бути визначення шляхів оцінки ефективності практичної реалізації документів стратегічного планування у сфері забезпечення інформаційної безпеки.

Список використаних джерел

1. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). URL: <https://www.hybridcoe.fi> (дата звернення: 04.05.2026).
2. Joint Publication 3-13.2. Psychological Operations. 2010. URL : https://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_2%2810%29.pdf (дата звернення: 03.05.2026).
3. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203. DOI: <https://doi.org/10.32782/2524-0374/2020-2/52>.
4. Роговець В. Інформаційні війни у сучасному світі: причини, механізми, наслідки. *Персонал*. 2000. № 5. С. 56–69.
5. Куйбіда В. Державність, демократія та національна безпека. Київ : САК Лтд, 2019. 478 с.
6. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 03.05.2026).
7. Концепції інформаційної безпеки України (проект). URL: <https://cdn.osce.org/sites/default/files/f/documents/0/2/175056.pdf>.
8. Стратегія інформаційної безпеки : Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 03.05.2026).
9. Resolution № 3314-XXIX(1974), UN General Assembly. URL: <http://hrlibrary.umn.edu/instree/GAres3314.html> (дата звернення: 03.05.2026).