УДК 355.244.1

МЕХАНІЗМИ ПРОТИДІЇ НЕГАТИВНИМ ВПЛИВАМ ІНФОРМАЦІЙНОЇ ПРОПАГАНДИ

Я. М. Жмака
здобувач вищої освіти третього (освітньо-наукового) рівня Факультету журналістики
Науковий керівник – д.н.соц.ком., професор О. А. Мітчук

Київський столичний університет імені Бориса Грінченка
м. Київ, Україна

У статті досліджено механізми протидії негативним впливам інформаційної пропаганди. Визначено, що методи протидії інформаційній війні на рівні держави – це великий комплекс можливих методів і дій, які вже давно, як засвідчує наша робота, вироблені українськими дослідниками у вигляді практичних рекомендацій.
Ключові слова: механізми протидії, негативні пливи, інформаційна пропаганда, інформаційна війна, інформаційна безпека, протидія.

The article examines mechanisms to counter the negative effects of information propaganda. It has been determined that methods of countering information warfare at the state level are an extensive set of possible methods and actions that, as our work shows, have long been developed by Ukrainian researchers in the form of practical recommendations.
Keywords: countermeasures, negative influences, information propaganda, information war, information security, counteraction.

Протидія інформаційній пропаганді та інформаційним атакам постає актуальним завданням державної політики на сучасному історичному етапі. Механізми протидії, по суті, становлять зворотній бік інформаційної війни – інформаційну безпеку. Як справедливо зазначає Уляна Ільницька, інформаційна безпека є інтегрованим компонентом національної безпеки і її доцільно розглядати як «пріоритетну функцію держави.

Інформаційна безпека, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій» [1, С. 28].

Метою роботи є дослідження механізмів протидії негативним впливам інформаційної пропаганди. .

Теоретичною базою дослідження послугували праці таких вчених: О. Довгань, О. Доренського, А. Котенко, В. Лисенко, П. Полянського, Г. Сасин, А. Шумки.

Дослідники по-різному визначають коло завдань і методів, форм протидії, якими повинна послуговуватися держава задля уникнення інформаційного шкідливого впливу, збереження власного інформаційного суверенітету і захисту суспільної та індивідуальної свідомості громадян від маніпулятивних впливів. Валентин Лисенко зазначає у розвідці «Проблеми інформаційної незалежності держави»: «На часі створення спеціальних підрозділів з проблем інформаційно-психологічної війни, які повинні захищати державні інтереси, здійснювати психологічний захист національної еліти і населення країни» [5, С. 146].

На думку дослідника, їхнім ключовим завданням має бути «виявлення і кваліфікація інформаційно-психологічних впливів, визначення ступеня загроз, створення системи запобігання і протидії спеціальним інформаційним операціям проти держави, суспільства, певних соціальних груп чи особистостей, вироблення механізмів ліквідації наслідків та відновлення на випадок уражень під час інформаційно-психологічних атак. Структура інформаційної безпеки має відповідати таким сучасним викликам, як тероризм і політичний екстремізм, стояти на захисті індивідуума, суспільства, держави» [5, С. 146–147]. Створення такої структури, переконує вчений, допоможе активно захищати українські національні й державні внутрішньо- та зовнішньополітичні цінності в соціокомунікаційному середовищі.

Ольга Довгань вважає, що функціональні характеристики складових ефективності складових інформаційного середовища базується на всебічному узагальненому підході та містить кілька компонентів: правовий; організаційний, психологічний [2, С. 71–72].

Правовий аспект пов'язаний із розробкою відповідних законів і нормативно-правових актів, що супроводжують відповідальність в соціально-інформаційній сфері щодо реалізації та дотримання інформаційної безпеки. Організаційний елемент обумовлений покращенням організаційної структури державних і комерційних підприємств, а також включає сертифікацію і стандартизацію засобів захисту інформації та ліцензування будь-якої діяльності у сфері захисту інформації. Психологічний компонент формує моральні та етичні норми у працівників, які забезпечують діяльність інформаційно-комунікаційної системи, та супроводжують критичну, тобто винятково важливу для функціювання всієї держави і її сфер життя інфраструктуру.

Алла Котенко пише, що «зважаючи на сутність феномену гібридної війни, Україні для забезпечення системи національної безпеки необхідно зосередитись на розробці нетрадиційних методів як складників сучасних форм ведення бойових дій» [4].

Власне, як розуміємо, під поняттям «бойових дій» йдеться загалом про організовану форму протистояння, що передбачає переважно традиційні методи і форми здійснення воєнної кампанії. На думку дослідниці, «суттєвим внеском у систему протидії гібридній агресії є «коригування власної стратегії щодо роботи із суспільством для формування громадської думки через державні та орієнтовані на різноманітні політичні сили ЗМІ, а також доведення позиції країни на міжнародному рівні» [4].

Крім того, Алла Котенко пише про «потребу створення «належної системи координації та взаємодії на державному рівні всіх суб'єктів інформаційного простору з питань відпрацювання заходів протидії спробам іноземних держав нанесення шкоди національним інтересам України, а також створення єдиної державної системи інформаційно-психологічної протидії іноземним впливам, до діяльності якої, окрім підрозділів спеціальних служб, також повинні активно залучатися і цивільні державні установи, організації, аналітичні центри, а також PR-компанії та засоби масової інформації різних форм власності» [4]. Ці рекомендації виглядають доцільними і релевантними засобами і способами протидії інформаційним атакам на державному рівні.

Втілити кампанію державної протидії інформаційній агресії можливо за допомогою інформаційно-ударної операції. Основоположними завданнями і цілями інформаційно-ударної операції є, за словами дослідника, такі:

– забезпечення інформаційної переваги шляхом активного впливу на системи державного та військового управління противника та на джерела інформаційних загроз;

– обман суперника щодо здійснюваної операції;

– погіршення морально-психологічної стійкості й «бойового духу» особового складу військ ворога;

– протидія негативному інформаційному впливу суперника [3, С. 132–133].

Інформаційно-ударну операцію слід проводити:

– з використанням сучасних інформаційних і телекомунікаційних засобів, технологій, соціальних мереж тощо;

– із застосуванням військових засобів;

– з демонстрацією потенціалу й можливостей сучасної зброї й показовою передислокацією військових підрозділів;

– активно висвітлюючи в засобах масової комунікації об'єктів ураження, з детальною їх характеристикою;

– організовуючи хвилі біженців і провокації громадських зіткнень;

– здійснюючи цілеспрямований вплив на громадську думку з метою несприйняття противника, блокування кордонів, введення ембарґо на поставку військової та інших видів продукції противника.

Також можна застосовувати такі військові кроки, як:

– масове використання безпілотних літальних апаратів й високоточної зброї;

– висвітлення подій у світових інформаційно-телекомунікаційних мережах;

– знищення військово-стратегічних цілей [3, С. 132–133].

Дослідниця Галина Сасин пропонує власний перелік засобів і методів, дій для протидії російській інформаційній війні на Сході й інформаційній агресії в міжнародних відносинах загалом. Цю протидію авторка ототожнює з захистом інформаційного простору та національної безпеки України, надаючи їй першорядного значення. Відтак пані Сасин пропонує такі рішучі кроки для української влади в цьому напрямі:

✓ зміна інформаційної політики (як зовнішньої, так і внутрішньої) з доповненням законодавчої та нормативно-правової бази, яка відповідала б нормам міжнародного права;

✓ здійснення захисту національної інформаційної сфери; просування української інформації на територію агресора з використанням сучасних технологій;

✓ проведення люстрації серед власників українських медіа-ресурсів;

✓ зменшення впливу олігархів на ЗМІ;

✓ формування і захист сприятливого образу України за допомогою сучасних технологій;

✓ створення та підтримка національного бренду, розвиток конкурентоспроможності на міжнародній арені;

✓ здійснення політики для збереження єдиної української політичної нації, на зближення політичних поглядів населення Сходу та Заходу України;

✓ обмеження російської інформації, яка впливає на населення півдня і сходу України;

✓ контроль іноземних ЗМІ, які акредитовані та функціонують на території України;

✓ сприяння розвитку вітчизняних інтернет-ресурсів, які просувають іномовлення;

✓ збільшення якості та кількості українського продукту (цікаві телепрограми, друкована продукція тощо);

✓ здійснення діяльності в інформаційному та віртуальному просторі у національних інтересах нашої держави, поширення позитивної інформації про Україну;

✓ участь у світових інформаційних процесах;

✓ організація та проведення розвідувальної діяльності, пов'язаної з проникненням в органи влади інших країн з метою просування наших національних інтересів; контроль донесення правдивої інформації до споживача; заклики «вироблено в Росії», «не купуй російське» тощо, доцільніше було б замінити на «купуй українське», адже воно рідне, якісне та перевірене;

✓ блокування інтернет-ресурсів, які є загрозливими для інформаційної безпеки держави;

- ✓ стимулювання наукових досліджень щодо державної інформаційної політики та безпеки;
- ✓ вдосконалення рівня підготовки фахівців у галузі інформаційної безпеки [7, С. 20–21].

Дослідник А. Шумка в розвідці «Теоретичні аспекти інформаційних війн та національна безпека» зазначає, що діяльність, яка супроводжується із реалізацією інформаційної безпеки соціо-комунікаційного середовища, мають включати:

- спостереження, аналіз, оцінку і прогноз загроз та небезпек;
- відпрацювання стратегії і тактики, планування попередження нападу, зміцнення потенційних зв'язків, підсилення ресурсів забезпечення інформаційної безпеки;
- відбір сил і засобів протидії, нейтралізації, недопущення нападу, мінімізації шкоди від нападу;
- дії із забезпечення інформаційної безпеки; управління наслідками інциденту (кібератаки, інформаційні операції, інформаційні війни) [8, С. 10].

Організація ефективної системи забезпечення інформаційної безпеки, як наголошує автор, «передбачає централізоване управління із конкретними функціями, які забезпечують моніторинг і контроль за всіма компонентами національного інформаційного простору» [8, С. 10].

Історик Павло Полянський пропонує свій погляд на варіанти протидії українського боку російській інформаційній війні в сучасних умовах. На його думку, Україні необхідно створити єдину інформаційну політику, а також:

- ✓ сформувати систему захисту національної інформаційної сфери та систему створення сприятливого образу України за допомогою сучасних технологій;
- ✓ обмежити вплив російської інформації на населення Півдня та Сходу України;
- ✓ контролювати діяльність іноземних засобів масової інформації, які акредитовані та функціонують на території України;
- ✓ сприяти розвитку вітчизняних інтернет-ресурсів; підвищити якість та кількість українського продукту (цікаві телепрограми, друкована продукція тощо);
- ✓ поширювати позитивну інформацію про Україну і контролювати донесення правдивої інформації до споживача; блокувати інтернет ресурсів, які є загрозливими для інформаційної безпеки держави;
- ✓ стимулювати наукові дослідження в напрямі державної інформаційної політики та безпеки [6].

Отже, методи протидії інформаційній війні на рівні держави – це великий комплекс можливих методів і дій, які вже давно, як засвідчує наша робота, вироблені українськими дослідниками у вигляді практичних рекомендацій. Вважаємо, що нині Україна повинна активно звернутися і впроваджувати ці та інші запропоновані дії для того, щоб дати відповідну інформаційну відсіч Росії і подолати її експансію в інформаційному просторі.

1. Інформаційна боротьба в сучасних умовах : навч. посіб. / за ред. В. Б. Толубко та ін. К. : НАОУ, 2002. 193 с. **2.** Довгань О. Сучасна інформаційна інфраструктура Україні основні завдання щодо її захисту. *Юридична наука.* 2015. № 7. С. 64–73. **3.** Доренський О. Модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни. *Інформаційна безпека держави, суспільства та особистості* : Всеукр. наук.-практ. конф., 16 квіт. 2015 р., м. Кіровоград : зб. тез доп. Кіровоград : КНТУ, 2015. С. 131–133. **4.** Котенко А. Гібридна війна як форма сучасного міжнародного конфлікту. *Міжнародні відносини. Сер. Політичні науки.* 2017. № 13. **5.** Лисенко В. Проблеми інформаційної незалежності держави. *Політичний менеджмент.* 2006. № 4. С. 135–147. **6.** Полянський П. Освіта як об'єкт інформаційної війни Росії проти України і як ресурс протидії такій війні. URL: https://maidanua.org/2015/03 (дата звернення: 05.03.2024). **7.** Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). *Грані.* 2015. № 3. С. 18–23. **8.** Шумка А., Черник П. Теоретичні аспекти інформаційних війн та національна безпека. *Грані*. 2015. № 9. С. 10–16.