РОЗДІЛ 6
СТОРІНКА МОЛОДОГО НАУКОВЦЯ

6.1. ПУБЛІЧНЕ УПРАВЛІННЯ

УДК 316.77:159.923.2
DOI https://doi.org/10.51547/ppp.dp.ua/2021.2.19

Іванов Артемій Вікторович,
магістр державного управління,
військовослужбовець
ORCID ID: 0000-0001-7689-9807

БЕЗПЕКОВИЙ СТАН ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА УКРАЇНИ У СФЕРІ ПРОТИСТОЯННЯ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ ІНОЗЕМНИХ ДЕРЖАВ

SECURITY STATE OF THE INFORMATION ENVIRONMENT OF UKRAINE IN THE FIELD OF RESISTANCE TO SPECIAL INFORMATION OPERATIONS OF FOREIGN STATES

У статті доводиться, що найбільшою загрозою інформаційній безпеці держави під час ведення гібридної війни є інформаційна війна, яка реалізується шляхом проведення низки спеціальних інформаційних операцій. СІО можуть використовуватись як інструмент ведення війни, так і в ролі інструмента забезпечення інформаційної безпеки, що своєю чергою є складником національної безпеки. Метою статті виступає дослідження процесу адаптації системи державного управління України для протидії спеціальним інформаційним операціям з боку РФ та пропозиції щодо її удосконалення. Розглянуто етапи створення нових центрів і органів у системі державного управління, що залучаються до сфери забезпечення інформаційної безпеки. Також у статті проведений аналіз безпекового стану інформаційного середовища України. Розкрите поняття «спеціальна інформаційна операція» та запропоновані нові методики забезпечення інформаційної безпеки як складника національної безпеки.

Встановлено, що спеціальна інформаційна операція – це діяльність, яка складається із комплексу заходів гласного і негласного характеру, спрямована на організоване приховане керування процесами інформаційної публічної сфери, що здійснюється шляхом впливу на свідомість і поведінку цільової аудиторії для досягнення певної мети. Зазвичай СІО проводяться в напрямах системи прийняття та розроблення політичних рішень, формування суспільної свідомості та громадської думки.

Наголошено, що значним кроком до вирішення цієї проблеми та поліпшенням забезпечення інформаційної безпеки держави може стати закріплення на законодавчому рівні терміна «спеціальна інформаційна операція», опис методології відстежування та виявлення СІО, що створить належні умови для швидкого та ефективного протистояння зовнішнім та внутрішнім інформаційним загрозам національній безпеці.

Ключові слова: *державна безпека, спеціальна інформаційна операція, гібридна війна, інформаційна війна, державне управління, національна безпека, інформаційно-психологічний вплив.*

The article states that the biggest threat to the information security of the state during a hybrid war is the information warfare, which is realized through a series of special information operations. SIO can be used both as a tool of warfare and as a tool of ensure information security, which is part of national security system. The purpose of the article is to research the process of adaptation of the public administration system of Ukraine to counteract special information operations by the Russian Federation and proposals for its improvement. The stages of creation of new centers and bodies in the system of public administration, which are involved in the sphere of information security, are considered. Also, the article analyzes the security state of the information environment of Ukraine. The concept of the term "special information operation" is revealed and new methods of information security as a component of national security are proposed.

It is established that a special information operation is an activity consisting of a set of measures of public and private nature, aimed at organized covert management of public information processes, carried out by influencing the consciousness

and behavior of the target audience to achieve a certain goal. JIUs are usually conducted in the areas of political decision-making and development, the formation of public consciousness and public opinion.

It was emphasized that a significant step towards solving this problem and improving the information security of the state could be the consolidation at the legislative level of the term "Special Information Operation", a description of the methodology for tracking and detecting SIO, which will create appropriate conditions for rapid and effective response to external and internal information threats national security.

Key words: *state security, special information operation, hybrid war, information war, public administration, national security, information psychological influence.*

Постановка проблеми. XXI століття є віком інформації та інформаційних технологій, технологічний розвиток суспільства дає змогу отримати безперешкодний доступ до всієї актуальної інформації майже з будь-якої точки Земної кулі. Завдяки своїй доступності та швидкій поширюваності інформація є одним із елементів впливу на суспільство та громадську свідомість, через що дедалі частіше використовується як легальна зброя державами та різними міжнародними організаціями задля досягнення своїх цілей. Якщо такий вплив на інформаційний простір країни здійснюється під час збройних або локальних конфліктів, то термін такого ведення бойових дій наближується до ознак «гібридної війни» [1; 2; 11].

Найбільший інформаційний вплив проти України здійснюється зі сторони Російської Федерації в контексті збройної агресії на Сході нашої країни [3]. При цьому, окрім зовнішнього впливу, країна-агресор використовує також і внутрішній вплив, поширюючи через підконтрольні та лояльні засоби масової інформації відповідні тези, які створюють деструктивний вплив на свідомість населення.

Зазначені події змушують адаптуватися державний апарат, через що зазнає змін сектор державного управління та правоохоронної діяльності, саме у такий спосіб, щоб ефективно протистояти новітнім загрозам та посяганням на конституційний лад, суверенітет і територіальну цілісність.

Аналіз останніх досліджень і публікацій. Починаючи з 2014 року на інформаційних та бібліографічних ресурсах українського наукового середовища почала збільшуватись кількість статей та публікацій на тему гібридної війни та спеціальних інформаційних операцій, зокрема досліджено праці таких науковців, як Г. Пєвцов, А. Підлісний, С. Залкін, І. Юзова, С. Сідченко та ін. Разом з цим проаналізовано низку законодавчих та підзаконних актів профільних органів державної влади України. Важливий внесок у розширення поняття «інформаційний вплив на свідомість» був зроблений фактом розсекречування внутрішнього плану Міністерства Оборони США "Information Operations Roadmap" [6], який містить у собі доволі детальні вказівки щодо методики використання інформаційно-психологічного впливу під час ведення бойових дій за межами своєї держави.

Метою статті є дослідження процесу адаптації системи державного управління України для протидії спеціальним інформаційним операціям з боку РФ під час гібридної агресії на Сході країни та пропозиції щодо її удосконалення.

Виклад основного матеріалу. Першими зафіксованими спланованими заходами із впливу на людську свідомість через транскордонні та локальні засоби масової інформації у воєнних цілях є інформаційні кампанії під час військових конфліктів на Корейському півострові (1950–1953 рр.), в Афганістані (1979–1989 рр. (СРСР), Кувейті (1991–1992 рр.), Югославії (1999 р.), Іраку (2003–2011 рр.), Афганістані (2001–2014 рр. (США). Перелічені збройні конфлікти супроводжувалися постійним проведенням різних спеціальних інформаційних операцій (далі – СІО) на територіях країн, в яких проходили бойові дії.

Інформаційна перевага стала основною метою під час ведення сучасних воєнних дій. Важливість домінування в інформаційному спектрі пояснює ціль перетворення інформаційних операцій з другорядних на основну військову компетенцію нарівні з повітряними, наземними, морськими та спеціальними операціями [6, с. 4]. СІО почали широко застосовуватись наприкінці XX та на початку XXI століть та стали одним з основних маркерів, які свідчать про гібридність ведення воєнних дій.

Найбільш дослідженою з наукового боку є інформаційна кампанія США в Іраку (1991–2011 рр.) [7], яка методом здійснення інформаційно-психологічного впливу посередництвом ЗМІ підготувала високий рівень підтримки американських військ з боку населення Іраку та стала певним «трафаретом» проведення спеціальних інформаційних операцій для інших країн.

Після вдалого проведення інформаційної операції такого масштабу інші держави почали приділяти все більше уваги інформаційно-психологічному впливу під час здійснення воєнних операцій. Зокрема, вказані дії їдужешироковикористовуються

Російською Федерацією у веденні гібридної війни проти України.

З вищезазначеного можна зробити висновок, що СІО – це діяльність, яка складається із комплексу заходів гласного і негласного характеру, спрямована на організоване приховане керування процесами інформаційної публічної сфери, що здійснюється шляхом впливу на свідомість і поведінку цільової аудиторії для досягнення певної мети. Зазвичай СІО проводяться в напрямах системи прийняття та розроблення політичних рішень, формування суспільної свідомості та громадської думки.

Результатами СІО є дистанційне формування політичних (ідеологічних) переконань, поглядів, думок, ідей, які впливають на психологічний стан, шляхом виклику необхідних позитивних або негативних емоцій у масах, здійснюючи у такий спосіб прихований інформаційно-психологічний вплив на цільову аудиторію.

Завдання СІО різняться між цілями їх проведення в мирний (підготовчий) період та у воєнний період [21], що зазначено на рис. 1.

Аналіз проблеми. Під час проведення низки СІО проти України РФ здійснює тиск через інформаційні, політичні, економічні та військові інструменти впливу. Наприклад, до процедури анексії територій Автономної республіки Крим РФ готувалась багато років, проводячи довготривалу СІО у мирний час, у рамках якої поширювались чутки щодо нібито *«історичної помилковості належності Кримського півострову Україні»*. Вказані чутки проникали усюди – від звичайного населення до лав Збройних сил України та політичного керівництва півостровом.

Вказана СІО дала можливість військам РФ на початку 2014 року під час політичної кризи в Україні здійснити військову інтервенцію та встановити фактичний військовий контроль на території АР Крим. Після чого РФ спробувала застосувати зазна-

Рис. 1. Основні цілі спеціальних інформаційних операцій

чену тактику гібридної воєнної агресії на Сході нашої країни під гаслами «*Донбасс – це Россія*», але зазнала певної поразки, через що військовий локальний конфлікт затягнувся на 7 років поспіль.

Притому іноземні спеціалісти зазначають, що інформаційна агресія проти України не зупинилась, а навпаки, стала набирати нових обертів у медіапросторі. Зокрема, РФ почала посилено пропагувати низку різних міфів, які здебільшого пов'язані з подіями під час Другої світової війни та українським націоналізмом 1940 років, ототожнюючи їх із сучасною Україною та висвітлюючи під призмою неонацизму та насильства проти власного населення. Одночасно поширюючи при цьому образи «славетного» Радянського Союзу та його правонаступника Російську Федерацію як протагоніста боротьби із нацизмом та захисника всієї частини російськомовного населення від «корумпованої, незаконної, фашистської хунти», яка нібито захопила владу.

Водночас засоби масової інформації РФ позиціонують Збройні сили України та добровольчі підрозділи як "Einsatzgruppen" (розстрільні загони СС), вбивць мирного населення, терористів та слуг київської хунти. Така інформація поширюється як у внутрішніх, так і в транснаціональних російських ЗМІ [22].

Зазначена медіакампанія має всі ознаки проведення спеціальних інформаційних операцій, оскільки вона націлена на зневажання та зниження рівня довіри до органів державної влади та армії.

Наведені події змусили громадянське суспільство та систему державного управління України адаптуватися під нові формати ведення воєнних дій задля ефективнішого протистояння зовнішній агресії РФ за правилами гібридної війни.

Зокрема, свою трансформацію державний апарат почав із закріплення на рівні нормативно-правових документів корегування системи захисту національної безпеки, а саме з введення в правове поле поняття таких загроз, як «гібридна війна», протистояння не тільки стандартним військовим загрозам, а й інформаційним на одному рівні з ними. Зазначені поняття присутні як у попередній Стратегії національної безпеки 2015 [9], так і у сучасній Стратегії 2020 [10]. Також основою для протидії інформаційній експансії держави-агресора та контрольованих нею структур під час гібридної агресії стала Стратегія кібербезпеки України (2016 р.) [14], Доктрина інформаційної безпеки України (2016 р.) [12] та Закон України про основні засади забезпечення кібербезпеки України (2017 р.) [13].

Окрім зазначеної трансформації законодавства, почались зміни і у секторі державного управління. Для протидії спеціальним інформаційним операціям проти України було створено Ситуаційний центр забезпечення кібербезпеки при Департаменті кібербезпеки СБУ [15; 16] (2018 р.), Центр протидії дезінформації при РНБО (2021 р.) [17; 18] та Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики (2021 р.) [19].

Перелічені центри задумувались та створювались як хаби для зв'язку та поліпшення комунікації у сфері протистояння кіберзагрозам між державними органами та інститутами влади, тим самим створивши трикутник взаємодії між Службою безпеки України, Кабінетом Міністрів України та Офісом Президента України.

Водночас на початку 2021 року Україна почала активну фазу протистояння російській інформаційній агресії через введення обмежувальних заходів (санкцій) шляхом блокування ангажованих та контрольованих з РФ засобів масової інформації, які транслювали свій медіаконтент на території України [20].

Наведений спосіб боротьби з інформаційною агресією показує наявність та актуальність зазначеної проблеми, а разом із цим відкриває нові вразливі місця у законодавстві, що своєю чергою не дають ефективно та упорядковано протистояти інформаційному впливу, змушуючи керівництво держави шукати законодавчі «лазівки» та здійснювати адекватні реакції в протистоянні інформаційній загрозі, роблячи це шляхом введення непередбачених обмежувальних заходів (санкцій).

Значним кроком до вирішення цієї проблеми та поліпшенням забезпечення інформаційної безпеки держави може стати закріплення на законодавчому рівні терміна «спеціальна інформаційна операція», опис методології відстежування та виявлення СІО, що створить належні умови для швидкого та ефективного протистояння зовнішнім і внутрішнім інформаційним загрозам національній безпеці.

Наступним етапом боротьби з інформаційною загрозою стане механізм встановлення цілей та методів реалізації СІО іноземних держав проти України, розробка системи ефективного комплексу заходів протистояння таким загрозам.

Зокрема, таким кроком може стати віднесення СІО до категорії суспільно небезпечного діяння та в подальшому прирівняння СІО до кримінального правопорушення (злочину). Таке поняття дозволить внести відповідні зміни в розділі «Злочини проти основ національної безпеки»

Кримінального кодексу України, що своєю чергою дасть змогу Службі безпеки України як єдиному органу, відповідальному за протидію проведення проти України спеціальних інформаційних операцій [12], спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій, ефективно протистояти інформаційним загрозам зазначеного типу.

Висновки. Виходячи із наявних даних стану безпекового простору Української держави, можна зробити висновки щодо тривалості процесу сталої трансформації системи державного управління у сфері протидії інформаційним загрозам. Зазначений процес, своєю чергою, показує недостатню захищеність інформаційного простору країни та необхідність корегування законодавства та інших підзаконних актів у сфері кібербезпеки.

Як зазначено в основному матеріалі статті, інформаційний простір є однією із найважливіших стратегічних сфер національної безпеки, позаяк він зазвичай використовується державами-агресорами як плацдарм, який до початку повномасштабних воєнних дій дає змогу здійснювати інформаційну агресію та є знаковим маркером початку гібридної війни.

Важливим кроком у покращенні стану захищеності національної безпеки є її модернізація шляхом чіткого формулювання загроз інформаційному простору держави, визначенням поняття «спеціальна інформаційна операція» на законодавчому рівні.

Основними ознаками початку інформаційної агресії є проведення іноземною державою спеціальних інформаційних операцій як у локальному, так і у світовому інформаційному середовищі. Це здійснюється шляхом публікації та поширення у внутрішніх, зовнішніх та транскордонних ЗМІ, соціальних мережах та Інтернет-месенджерах провокативних статей та дописів деструктивного для іншої держави змісту. Насамперед такі статті публікуються на теми територіальної належності областей та регіонів інших держав (*або гострою надуманою критикою керівництва держави, негативним висвітленням ефективності рішень державної влади та органів місцевого самоврядування і т.д.*). У разі достатнього висвітлення та поширення таких статей у рамках інформаційної агресії СІО починає чинити значний психологічний вплив на свідомість населення, що надалі дає змогу країні-агресору приступати до наступних фаз гібридної війни, таких як масові заворушення та збройний конфлікт.

Зазначена схема впливу на свідомість у разі комплексного виконання та публікації інформації на різних джерелах дає змогу як проводити спеціальні інформаційні операції, так і виявляти їх, що повинно лягти в основу процесу методик відслідковування та протидії спеціальним інформаційним операціям іноземних держав.

Тематика публікацій, які використовуються для інформаційного впливу, може бути як локальною, такою, що висвітлює реальні проблеми суспільства, а може так само здійснюватися в рамках СІО спеціальними службами іноземних держав як здійснення прихованої інформаційної атаки, що у сукупності з іншими інформаційними акціями переслідує одну й ту саму мету. Тому задля протидії реальним загрозам необхідно розробити та закріпити на законодавчому рівні процес моніторингу і відстеження іноземних СІО на шкоду державному суверенітету, конституційному ладу та територіальній цілісності України. А надалі розробити законний процес щодо заборони здійснення подібної діяльності засобами масової інформації та механізми спростування вже висвітлених деструктивних публікацій, не перешкоджаючи при цьому засадам демократичного розвитку суспільства та вільного доступу до інформації.

Зазначена процедура закріплення поняття «спеціальна інформаційна операція» на законодавчому рівні та формування методик її відстежування є складною та такою, що потребує розробки та постійного корегування і доопрацювання, що в майбутньому дасть змогу ідентифікувати СІО проти України та відкрито й ефективно їм протистояти, не створюючи при цьому додаткових органів державної влади або центрів протидії будь-яким загрозам, тим самим підвищуючи ефективність системи державного управління, створюючи більшу прозорість системи судочинства та доопрацьованість чинного законодавства.

СПИСОК ЛІТЕРАТУРИ:

1. The hybrid mindset and operationalizing innovation: toward a theory of hybrid. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a611901.pdf.

2. Попович К.В. Гібридна війна як сучасний спосіб ведення війни: історичний та сучасний виміри. *Науковий вісник Ужгородського університету. Серія: Історія*. 2016. Вип. 2. С. 75–79. URL: http://nbuv.gov.ua/UJRN/Nvuuist_2016_2_13.

3. Юзова І.Ю. Аналіз організації та ведення інформаційно-психологічних операцій при веденні гібридної війни. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2020. № 2. С. 40–44. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2020_2_8.

4. Твердохліб Ю. Інформаційно-психологічні операції Російської Федерації проти України – основні етапи та цілі. *Вісник Львівського університету. Серія: Міжнародні відносини.* 2019. Вип. 46. С. 206–213. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_20.

5. Пєвцов Г.В. Пропозиції щодо удосконалення процесу управління інформаційно-психологічними впливами в ході проведення інформаційно-психологічних операцій / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський. *Наука і техніка Повітряних Сил Збройних сил України*. 2020. № 3. С. 43–49. URL: http://nbuv.gov.ua/UJRN/Nitps_2020_3_7.

6. Information operations roadmap. United States Department of Defense. 2003. URL: https://www.hsdl.org/?abstract&did=460304.

7. Підлісний А.Р. Воєнна кампанія США в Іраку як зразок інформаційно-психологічного забезпечення на державно-політичному та військовому рівнях. *Військово-науковий вісник*. 2012. Вип. 17. С. 178–189. URL: http://nbuv.gov.ua/UJRN/vnv_2012_17_18.

8. Пєвцов Г.В. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський. *Наука і оборона.* 2015. № 2. С. 28–32. URL: http://nbuv.gov.ua/UJRN/nauio_2015_2_7.

9. Указ Президента України № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». 2015. URL: https://www.president.gov.ua/documents/2872015-19070.

10. Указ Президента України № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» 2020. URL: https://www.president.gov.ua/documents/3922020-35037.

11. Загорулько А.П. Теоретико-правовий аналіз визначення поняття «гібридна війна». Національна академія державного управління при Президентові України. 2019. URL: http://visnyk.academy.gov.ua/pages/dop/84/files/3f4a88ef-eba1-45a0-8a2b-16ed09c603ba.pdf.

12. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». 2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#n12.

13. Закон України «Про основні засади забезпечення кібербезпеки України». / *Верховна Рада України*. 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

14. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». 2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

15. Ситуаційний центр забезпечення кібербезпеки. Структура СБУ. 2021. URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky.

16. В Україні з'явився Ситуаційний центр, що відбиватиме кібератаки. *Укрінформ.* 2017. URL: https://www.ukrinform.ua/rubric-technology/2389847-v-ukraini-zavivsa-situacijnij-centr-so-vidbivatime-kiberataki.html.

17. Указ Президента України № 187/2021 «Питання Центру протидії дезінформації». 2021. URL: https://www.president.gov.ua/documents/1872021-38841.

18. Центр протидії дезінформації розпочав роботу. *Укрінформ.* 2021. URL: https://www.ukrinform.ua/rubric-polytics/3222362-centr-protidii-dezinformacii-rozpocav-robotu.html.

19. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. *Урядовий портал.* 2021. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki.

20. Указ Президента України № 43/2021 «Про рішення Ради національної безпеки і оборони України від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» 2021. URL: https://www.president.gov.ua/documents/432021-36441.

21. Нарис теорії і практики інформаційно-психологічних операцій / М.Т. Дзюба, Я.М. Жарков, О.І. Ольховой, М.І. Онищук. Київ : ВІКНУ, 2006. 471 с. (Міністерство оборони України).

22. Müür K. Russian Information Warfare Against Ukraine I: Online News and Social Media Analysis / K. Müür, V. Sazonov. *ENDC OCCASIONAL PAPERS.* 2017. No. 7. С. 69–73.