УДК 355.01:316.776.23«2022/2024»
DOI https://doi.org/10.32782/2786-9385/2024-4-5

ВІТЧИЗНЯНА ТА ЗАРУБІЖНА ПРАКТИКА ПРОТИДІЇ ВОРОЖИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ 2022–2024 РР.

Стрелков Владислав Володимирович,
Ph. D., старший викладач кафедри національної безпеки
Волинського національного університету імені Лесі Українки
ORCID ID: 0000-0001-8436-3260

Дриганюк Діана Олександрівна,
здобувач кафедри національної безпеки
Волинського національного університету імені Лесі Українки
ORCID ID: 0009-0000-9760-9549

В рамках даного дослідження автори здійснили комплексний аналіз інформаційно-психологічних операцій, що проводилися російською федерацією проти України за період 2022–2024 рр., з метою виявлення методів, цілей та наслідків їх втілення. Дослідники розглянули конкретні стратегії та тактики, що використовувалися Росією для проведення інформаційно-психологічних операцій, включаючи дезінформацію, пропаганду, кібератаки та інші форми психологічного впливу. Значну увагу приділено аналізу впливу проведення інформаційно-психологічних операцій на українське суспільство, внутрішню політику, міжнародні відносини та економіку України. Також автори висвітлили заходи, вжиті нашою державою та міжнародною спільнотою для протидії проведенню інформаційно-психологічних операцій в інформаційному просторі України, надали оцінку їх ефективності та визначили кращі практики у сфері інформаційної безпеки на основі зарубіжного досвіду.

Автори дослідження акцентують увагу читачів на тому, що аналіз інформаційно-психологічних операцій, які здійснювала Росія протягом 2022–2024 рр., є критично важливим для розробки та впровадження ефективних контрзаходів. Вони повинні включати в собі як тактичні, так і стратегічні аспекти, спрямовані на забезпечення національної безпеки, захист національних інтересів в інформаційному просторі та збереження довіри суспільства до державних інституцій. Дослідники встановили, що інформаційно-психологічні операції РФ проти України проводилися комплексно, включали такі компоненти як дезінформація, пропаганда, кібератаки та інші форми психологічного впливу. Вони мали на меті дестабілізацію ситуації в Україні, дискредитацію українського керівництва, створення паніки серед населення та посилення внутрішніх конфліктів. Ці операції були добре сплановані та здійснювалися через різноманітні канали, що зробило їх надзвичайно ефективними у досягненні поставлених цілей.

Ключові слова: *інформаційно-психологічні операції, національна безпека, гібридна війна, пропаганда, дезінформація, міжнародні організації.*

Strelkov Vladyslav, Dryhaniuk Diana. Domestic and foreign practice of countering enemy information and psychological operation 2022–2024

Within the framework of this study, the authors carried out a comprehensive analysis of informational and psychological operations carried out by the Russian Federation against Ukraine in the period 2022–2024, with the aim of identifying the methods, goals and consequences of their implementation. The researchers examined specific strategies and tactics used by Russia to conduct information and psychological operations, including disinformation, propaganda, cyberattacks and other forms of psychological influence. Considerable attention is paid to the analysis of the impact of information and psychological operations on Ukrainian society, domestic politics, international relations and the economy of Ukraine. The authors also highlighted the measures taken by our state and the international community to counter the conduct of information and psychological operations in the information space of Ukraine, provided an assessment of their effectiveness and identified best practices in the field of information security based on foreign experience.

The authors of the study draw readers' attention to the fact that the analysis of information and psychological operations carried out by Russia during 2022-2024 is critically important for

the development and implementation of effective countermeasures. They should include both tactical and strategic aspects aimed at ensuring national security, protecting national interests in the information space, and maintaining public trust in state institutions. The researchers established that the informational and psychological operations of the Russian Federation against Ukraine were carried out in a complex manner, including such components as disinformation, propaganda, cyberattacks and other forms of psychological influence. They were aimed at destabilizing the situation in Ukraine, discrediting the Ukrainian leadership, creating panic among the population and intensifying internal conflicts. These operations were well planned and executed through various channels, which made them extremely effective in achieving their objectives.

Key words: *information and psychological operations, national security, hybrid warfare, propaganda, disinformation, international organizations.*

Вступ. Інформаційно-психологічні операції (далі в тексті – ІПсО) стали невід'ємною складовою сучасних гібридних воєн, де інформація використовується як зброя. Війна між Росією (далі в тексті – РФ) та Україною в цьому контексті є яскравим прикладом того, як дезінформація, пропаганда та інші форми ІПсО можуть впливати на хід конфліктів, політичні процеси і суспільні настрої.

Конфлікт між РФ та Україною набув нових масштабів з початком повномасштабного вторгнення в лютому 2022 року, разом з яким РФ активно використовує ІПсО для підриву морального духу українців, поширення фейкових новин, створення паніки та розколу в суспільстві. Ці дії спрямовані не лише на внутрішню аудиторію, але й на міжнародну, щоб дискредитувати Україну на світовій арені та впливати на підтримку з боку західних країн.

Актуальність теми обумовлена й тим, що в сучасному глобалізованому світі інформаційні атаки можуть мати далекосяжні наслідки. Вони здатні впливати на політичні рішення, економічну стабільність та міжнародну безпеку. Вивчення ІПсО РФ проти України допоможе зрозуміти механізми та методи, які використовуються для ведення інформаційних війн, що є важливим для розробки стратегій захисту та протидії.

Тому, вивчення актуальних ІПсО РФ проти України (за період 2022–2024 рр.) є надзвичайно важливим для розуміння сучасних викликів у галузі інформаційної безпеки, розробки ефективних методів захисту від інформаційних атак та забезпечення стабільності та безпеки як на національному, так і на міжнародному рівнях.

Матеріали та метод. У цьому дослідженні автори розглядають заходи, вжиті нашою державою та міжнародною спільнотою для протидії російським ІПсО, з метою оцінки їх ефективності та вивчення наявного досвіду задля визначення найкращих практик. Дослідження ґрунтується на публікаціях засобів масової інформації та звітах міжнародних організацій. Серед методів, що використовувалися авторами, слід відзначити такі: компаративного аналізу, контент-аналізу та "case-study".

Результати. ІПсО є складовою частиною сучасних військових та політичних стратегій, що використовуються для впливу на свідомість і поведінку великих груп людей. Основною метою ІПсО є зміна сприйняття реальності у цільової аудиторії через маніпуляцію інформацією, що може включати пропаганду, дезінформацію, поширення чуток, та інші засоби психологічного впливу [5].

ІПсО мають давню історію і використовувалися у військових конфліктах і політичних протиборствах різних епох. У сучасному контексті, з розвитком інформаційних технологій та глобальної комунікаційної мережі, ІПсО набули нових форм і масштабів. Інтернет, соціальні мережі, телебачення та інші медіа-платформи стали головними інструментами для проведення таких операцій. Використовуючи ці канали, агресори можуть швидко і ефективно поширювати необхідні їм наративи, впливаючи на широку аудиторію в різних країнах.

Одним з ключових елементів ІПсО є пропаганда, яка спрямована на створення і поширення певних ідей, що мають викликати емоційний відгук і формувати необхідні установки в суспільстві.

Пропаганда може бути як позитивною, так і негативною, але в контексті гібридних воєн вона часто використовується для дискредитації опонента, створення розколів у суспільстві та підриву довіри до уряду і державних інституцій [5].

Дезінформація є ще одним важливим компонентом ІПсО. Це цілеспрямоване поширення неправдивої або викривленої інформації з метою обману цільової аудиторії. Дезінформаційні кампанії можуть включати створення фейкових новин, маніпулювання фактами, використання підроблених документів та інших засобів для введення людей в оману. Основна мета дезінформації – створити хаос, викликати недовіру до офіційних джерел інформації та посіяти сумніви серед населення.

Психологічний вплив у рамках ІПсО може бути досягнутий через використання спеціально підібраних меседжів, спрямованих на емоційний стан людей. Це може включати залякування, поширення паніки, створення відчуття безнадії або, навпаки, надмірного оптимізму. Такі тактики використовуються для маніпулювання настроями і поведінкою людей, що може мати серйозні наслідки для суспільної стабільності [6].

Кіберпростір також став важливим полем для ІПсО. Кібератаки можуть бути спрямовані на викрадення конфіденційної інформації, поширення шкідливих програм, зламання інформаційних систем та дезорганізацію комунікаційних мереж. Це дозволяє агресорам не тільки отримувати важливі дані, але й сіяти недовіру та паніку серед населення.

В загальному, ІПсО є потужним інструментом впливу в руках держав та недержавних акторів, який використовується для досягнення стратегічних цілей без застосування відкритої військової сили. Вони дозволяють змінювати політичні та соціальні процеси, впливати на міжнародні відносини та здійснювати контроль над інформаційним простором. У сучасному світі, де інформація стала однією з найважливіших складових національної безпеки, розуміння та вміння протидіяти ІПсО є критично важливими для захисту державних інтересів та забезпечення стабільності [6].

У період 2022–2024 рр. РФ здійснила чимало ІПсО проти України, вони мали значний вплив на різні аспекти життєдіяльності українського суспільства. Одним із найпомітніших прикладів була кампанія з дезінформації щодо подій на фронті. Російські медіа систематично публікували фейкові новини про нібито великі втрати серед українських військових, вигадані перемоги російської армії та інсценовані випадки здачі українських підрозділів у полон. Такі повідомлення поширювалися через соціальні мережі, телебачення та інші канали, спрямовані на підрив морального духу українського населення та зниження довіри до Збройних сил України [4 с. 40].

Ще одним прикладом стала дезінформаційна кампанія, спрямована на дискредитацію українського керівництва. Російські пропагандисти регулярно поширювали фейкові новини про корупцію у вищих ешелонах влади, зв'язки українських політиків з неонацистськими угрупованнями та їхню участь у незаконних схемах. Зокрема, часто фігурували вигадані історії про Президента Володимира Зеленського та його найближче оточення. Метою цих дій було підрив довіри населення до влади та створення внутрішньої політичної нестабільності [1].

У соціальних мережах активно діяли російські боти та тролі, які поширювали панічні настрої та фейкові повідомлення про нібито катастрофічний стан економіки, відсутність товарів першої необхідності, перебої в постачанні електроенергії та води. Ці повідомлення часто супроводжувалися фотографіями та відео, взятими з інших контекстів або спеціально створеними для викликання паніки. Такі інформаційні атаки мали на меті дестабілізацію суспільства та підвищення рівня тривожності серед громадян.

Російські кібератаки стали ще одним потужним інструментом ІПсО. У 2022–2024 рр. хакери, пов'язані з РФ, здійснили численні атаки на українські державні установи, енергетичну інфраструктуру та медіа. Одним із найбільш

резонансних випадків була атака на енергетичну компанію «Укренерго», що спричинила перебої в постачанні електроенергії на значних територіях. Крім того, були зламані сайти урядових установ, що спричинило витік важливої інформації та дезорганізацію їх роботи. Ці кібератаки були спрямовані на підрив критичної інфраструктури та посилення хаосу в країні [4 с. 40–41].

Психологічний вплив здійснювався також через культурну війну. Російська пропаганда намагалася використати мовне питання для розколу українського суспільства, наголошуючи на утисках російськомовного населення. Поширювалися вигадані історії про заборону російської мови в школах та на роботі, а також про переслідування за використання російської мови у повсякденному житті. Ці дії мали на меті посилення внутрішніх конфліктів та створення напруженості між різними частинами населення.

Конкретним прикладом ІПсО стала також кампанія зі створення паніки під час воєнних дій. Російські джерела поширювали фейкові повідомлення про нібито заплановані великомасштабні атаки на цивільні об'єкти, що змушувало людей покидати свої домівки і створювало хаос. Одним із найбільш помітних випадків була фейкова інформація про заплановані удари по великих містах, таких як Київ, Львів та Харків, що викликало масову евакуацію і паніку серед населення [4 с. 42].

З огляду на викладене вище, можемо говорити про те, що ІПсО РФ проти України в 2022–2024 рр. були комплексними і включали дезінформацію, пропаганду, кібератаки та інші форми психологічного впливу. Вони мали на меті дестабілізацію ситуації в Україні, дискредитацію українського керівництва, створення паніки серед населення та посилення внутрішніх конфліктів. Ці операції були добре сплановані та здійснювалися через різноманітні канали, що робило їх надзвичайно ефективними у досягненні поставлених цілей.

Значну роль у протистоянні російським ІПсО відіграли міжнародні організації та країни-союзники, які своєчасно забезпечили різнопланову підтримку та протидію цим загрозам [1, с. 139].

Північноатлантичний альянс (далі – НАТО) та Європейський Союз (далі – ЄС) активізували свої зусилля у сфері кібербезпеки та інформаційної безпеки. НАТО, наприклад, надає технічну допомогу та консультації щодо захисту критичної інфраструктури від кібератак, організовував тренінги для українських фахівців з інформаційної безпеки та кіберзахисту. Співпраця в рамках кіберцентрів НАТО, таких як Cooperative Cyber Defence Centre of Excellence в Таллінні, забезпечила обмін передовими практиками та методами захисту [2].

ЄС також відіграв важливу роль у боротьбі з російськими ІПсО. ЄС запровадив санкції проти російських пропагандистів та медіа, які поширювали дезінформацію. Окрім того, Європейська служба зовнішніх справ активно працювала над викриттям фейкових новин та дезінформаційних кампаній через проєкт East StratCom Task Force та його платформу EUvsDisinfo. Ця платформа моніторила і аналізувала дезінформацію, публікувала спростування та навчала громадськість розпізнавати фейки [3].

Серед країн-союзників Сполучені Штати Америки (далі – США) були одними з найактивніших у наданні допомоги Україні в протидії ІПсО. США надавали Україні фінансову та технічну допомогу для зміцнення кібербезпеки, підтримували незалежні медіа та громадські організації, що протидіють поширенню дезінформації. Агентства, такі як Агентство США з міжнародного розвитку (USAID), фінансували програми з підвищення медіаграмотності та критичного мислення серед українців.

Велика Британія також активно підтримувала Україну в боротьбі з інформаційними загрозами. Британські урядові організації надавали консультації щодо комунікаційних стратегій, допомагали у викритті дезінформації та підтримували українські медіа в забезпеченні правдивої та перевіреної інформації. Крім того, британські експерти

проводили навчання для українських журналістів і державних службовців щодо ефективної комунікації в умовах кризи [3].

Міжнародні організації, такі як Організація з безпеки і співробітництва в Європі (ОБСЄ), також сприяли зусиллям з протидії ІПсО. ОБСЄ здійснювала моніторинг інформаційного простору, документувала випадки дезінформації та пропаганди, а також надавала платформи для діалогу і обміну інформацією між державами-членами.

Висновки. Проаналізувавши публікації в засобах масової інформації та дослідивши безпекову політику зарубіжних інституцій та міжнародних організацій, можемо зробити висновок, що ІПсО РФ проти України в досліджуваний період свідчать про масштабність і систематичність цих заходів, спрямованих на дестабілізацію українського суспільства, підрив національної єдності та дискредитацію державних інституцій. ІПсО РФ охопили широкий спектр тактик, включаючи дезінформацію, пропаганду, кібератаки та психологічний тиск, які були ретельно сплановані та спрямовані на досягнення стратегічної воєнної цілі щодо зламу опору та національної стійкості громадян України.

Кібератаки стали важливою складовою ІПсО, спрямованою на підрив критичної інфраструктури, зламування державних систем та розповсюдження шкідливого програмного забезпечення. Атаки на українську енергетичну систему, урядові сайти та медіа-ресурси викликали значні перебої в роботі та посіяли паніку серед населення, що було частиною стратегічного плану з дестабілізації країни.

Російські дезінформаційні кампанії активно послуговувалися засобами масової інформації, соціальними мережами та інші платформами для поширення неправдивих новин, фейкових наративів та маніпулятивних повідомлень. Ці операції мали на меті створення хаосу, викликання паніки та недовіри до офіційних джерел інформації. Часто дезінформація була спрямована на дискредитацію українського керівництва, зокрема через фальшиві звинувачення у корупції та некомпетентності.

Пропагандистські зусилля РФ намагалися легітимізувати агресію проти України, поширюючи наративи про «неонацистський» режим у Києві та необхідність «захисту» російськомовного населення. Ці повідомлення були спрямовані не лише на внутрішню російську аудиторію, але й на міжнародне співтовариство, з метою виправдання агресивних дій і зменшення міжнародної підтримки України.

ЛІТЕРАТУРА:

1. Агресія Росії проти України: історичні передумови та сучасні виклики / П. П. Гай-Нижник та ін. Київ : МП Леся, 2016. 586 с.

2. ІПСО: як жити та працювати в епоху інформаційних атак. URL: https://www.ukrinform.ua/rubric-presshall/3658359-ipso-ak-ziti-ta-pracuvati-v-epohu-informacijnih-atak.html (дата звернення 22.05.2024).

3. Довгань К. Обережно, ІПСО: як розпізнати та протистояти російським гібридним загрозам. 2022. URL: https://24tv.ua/shho-take-ipso-yak-rozpiznati-protistoyati-rosiyskim-gibridnim_n2156656 (дата звернення 24.05.2024).

4. Присяжнюк Д. М. Застосування маніпулятивних психотехнологій з боку Росії в ЗМІ України. *Вісник Київського національного університету ім. Т. Г. Шевченка*. 2019. № 23. С. 250.

5. Вишневська А. Що таке ІПСО та як його застосовує Росія. 2022. URL: https://24tv.ua/ipso-shho-tse-take-yak-yogo-zastosovuye-rosiya-24-kanal_n2188897 (дата звернення 25.05.2024).

6. Гранатова К. Що таке ІПСО та як росія використовує їх у війні проти України. 2023. URL: https://chas.news/current/scho-take-ipso-ta-yak-rosiya-vikoristovue-ih-u-viini-proti-ukraini (дата звернення 28.05.2024).

REFERENCES:

1. Hai-Nyzhnyk P. P. (2016). Ahresiia Rosii proty Ukrainy: istorychni peredumovy ta suchasni vyklyky [Russia's aggression against Ukraine: historical prerequisites and modern challenges]. Kyiv : MP Lesia. 586 s. [in Ukrainian].

2. Ukrinform (2024). IPSO: yak zhyty ta pratsiuvaty v epokhu informatsiinykh atak [IPSO: how to live and work in the age of information attacks]. Retrieved from: https://www.ukrinform.ua/rubric-presshall/3658359-ipso-ak-ziti-ta-pracuvati-v-epohu-informacijnih-atak.html [in Ukrainian].

3. Dovhan K. (2022). Oberezhno, IPSO: yak rozpiznaty ta protystoiaty rosiiskym hibrydnym zahrozam [Beware, IPSO: How to Recognize and Counter Russian Hybrid Threats]. Retrieved from: https://24tv.ua/shho-take-ipso-yak-rozpiznati-protistoyati-rosiyskim-gibridnim_n2156656 [in Ukrainian].

4. Prysiazhniuk D. M. (2019). Zastosuvannia manipuliatyvnykh psykhotekhnolohii z boku Rosii v ZMI Ukrainy [The use of manipulative psychotechnologies by Russia in the mass media of Ukraine]. *Visnyk Kyivskoho natsionalnoho universytetu im. T. H. Shevchenka.* № 23. S. 250 [in Ukrainian].

5. Vyshnevska A. (2022). Shcho take IPSO ta yak yoho zastosovuie Rosiia [What is IPSO and how is it applied by Russia]. Retrieved from: https://24tv.ua/ipso-shho-tse-take-yak-yogo-zastosovuye-rosiya-24-kanal_n2188897 [in Ukrainian].

6. Hranatova K. (2023). Shcho take IPSO ta yak rosiia vykorystovuie yikh u viini proty Ukrainy [What are IPSOs and how is Russia using them in the war against Ukraine]. Retrieved from: https://chas.news/current/scho-take-ipso-ta-yak-rosiya-vikoristovue-ih-u-viini-proti-ukraini [in Ukrainian].