

2. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення Ради Національної безпеки і оборони України від 29 груд. 2016 р. (введено в дію Указом Президента України від 13 лют. 2017 р. № 32/2017). *Верховна Рада України* : [сайт]. URL: <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text>.

3. Лисеюк А., Свінцицька Т. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. *Право та інноваційне суспільство*. 2024. № 2(23). С. 89–95.

Мартинюк Софія Володимирівна
студентка 109_СПД н.гр. ННІ права та психології НАВС

Науковий керівник:
Грищенко Олег Ігорович
старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

ЦІЛІ ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В КІБЕРПРОСТОРІ

Інформаційні та психологічні операції в кіберпросторі спрямовані на системну зміну поведінки, рішень і світоглядних орієнтирів цільових аудиторій через контроль інформаційного середовища та вплив на когнітивні процеси.

Інформаційні та психологічні операції в кіберпросторі в сучасних умовах трансформувалися в один із ключових інструментів геополітичного протистояння та гібридних конфліктів. Стрімка цифровізація суспільства, інтеграція інформаційно-комунікаційних технологій у всі сфери державного управління, економіки та соціальної взаємодії зумовили формування якісно нового середовища безпеки. Кіберпростір став не лише технічною інфраструктурою передачі даних, а й когнітивним середовищем, у межах якого відбувається формування суспільних установок, ціннісних орієнтирів і моделей поведінки. Саме тому вплив на інформаційне середовище дедалі частіше використовується як альтернатива або доповнення до традиційних військових засобів.

У доктринальному розумінні інформаційні операції (Information Operations) розглядаються як інтегрований комплекс заходів, спрямованих на вплив на інформаційні системи, процеси прийняття рішень та інформаційне середовище противника при одночасному захисті власного інформаційного простору [1].

Відповідні підходи системно закріплені в документах NATO та United States Department of Defense, де інформаційний компонент визначається як складова багатодомених операцій. Психологічні операції (PSYOPS) є функціональною частиною ширшої системи інформаційного впливу й орієнтовані на зміну установок, переконань, емоційного стану та поведінки конкретних цільових аудиторій – військовослужбовців, цивільного населення, політичного керівництва, міжнародної спільноти [2].

Стратегічні цілі інформаційних та психологічних операцій у кіберпросторі мають комплексний характер. Передусім йдеться про дестабілізацію політичної системи противника шляхом підризу довіри до державних інститутів, судової системи, виборчих процедур, правоохоронних органів та збройних сил. Через поширення маніпулятивних наративів і дезінформації формується сумнів у легітимності владних рішень, що сприяє зростанню соціальної напруги та поляризації. Іншою ціллю є вплив на процеси стратегічного та оперативного прийняття рішень шляхом створення інформаційного тиску, формування хибних уявлень про реальний стан справ або нав'язування вигідного порядку денного [3].

Окремим напрямом є деморалізація особового складу збройних сил і цивільного населення. Поширення панічних настроїв, перебільшення втрат, дискредитація командування або маніпуляція фактами можуть істотно впливати на морально-психологічний стан суспільства. У цьому контексті кіберпростір дозволяє здійснювати точковий вплив через соціальні мережі, месенджери, а також через таргетовану рекламу з персоналізованим контентом. За оцінками аналітичних досліджень RAND Corporation, сучасні інформаційні кампанії дедалі більше спираються на аналіз великих масивів даних для ідентифікації вразливих груп і конструювання повідомлень, що максимально відповідають їхнім когнітивним особливостям [4].

Кіберпростір має низку характеристик, що роблять його особливо ефективним для реалізації інформаційно-психологічного впливу. Анонімність та складність атрибуції створюють сприятливі умови для прихованих операцій, оскільки доведення причетності конкретного суб'єкта є складним з технічної та правової точки зору. Глобальність цифрового середовища забезпечує охоплення міжнародної аудиторії практично без географічних обмежень. Висока швидкість поширення інформації та алгоритмічні механізми соціальних платформ сприяють вірусному ефекту, особливо щодо емоційно насиченого контенту. Використання бот-мереж, фабрик тролів, технологій deepfake та синтетичних медіа дозволяє створювати ілюзію масової підтримки певної позиції або дискредитувати конкретних осіб [5].

Психологічна складова таких операцій базується на глибокому розумінні когнітивних механізмів сприйняття інформації. Використовуються ефект підтвердження власних переконань, феномен інформаційних «бульбашок», механізми соціального доказу та емоційної поляризації [6].

Створення інформаційного перевантаження знижує здатність до критичного аналізу, а постійне повторення певних меседжів формує стійкі установки. Маніпуляція історичною пам'яттю, національною ідентичністю та культурними символами дозволяє поглиблювати розколи всередині суспільства та підсилювати конфліктні лінії.

У міжнародно-правовому вимірі питання застосування інформаційних і кібероперацій аналізуються в межах норм міжнародного права, зокрема в експертному дослідженні Tallinn Manual щодо застосування міжнародного права до кібероперацій [2]. Питання формування довіри, прозорості та заходів зміцнення безпеки в інформаційному просторі розглядаються також у документах OSCE. Аналітичні звіти European Union Agency for Cybersecurity систематизують сучасні кіберзагрози, включаючи інформаційні кампанії як елемент гібридних атак [3].

Висновки. Інформаційні та психологічні операції в кіберпросторі мають стратегічну спрямованість і спрямовані на досягнення довгострокових політичних, військових та геоекономічних результатів. Їх кінцевою метою є контроль над інформаційним порядком денним, формування вигідної картини реальності та зміна поведінкових моделей цільових аудиторій без застосування військової сили. У сучасному безпековому середовищі ефективна протидія таким операціям потребує комплексного підходу: розвитку національних систем кіберзахисту, удосконалення стратегічних комунікацій, підвищення рівня медіаграмотності населення та активної міжнародної співпраці у сфері кібербезпеки.

Список використаних джерел:

1. NATO. *Allied Joint Doctrine for Information Operations (AJP-3.10)*. URL: <https://info.publicintelligence.net/NATO-IO.pdf>.
2. Tallinn Manual. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. URL: https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf.
3. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape Report*. URL: <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>.
4. RAND Corporation. *The Russian "Firehose of Falsehood" Propaganda Model*. URL: <https://www.rand.org/pubs/perspectives/PE198.html>.
5. Influence: The Psychology of Persuasion – Robert Cialdini. URL: <https://ia803201.us.archive.org/7/items/ThePsychologyOfPersuasion/The%20Psychology%20of%20Persuasion.pdf>.
6. Thinking, Fast and Slow – Daniel Kahneman. URL: <https://dn790002.ca.archive.org/0/items/DanielKahnemanThinkingFastAndSlow/Daniel%20Kahneman-Thinking%20Fast%20and%20Slow%20%20.pdf>.