Кам’янець-Подільський національний університет
імені Івана Огієнка

ЗБІРНИК МАТЕРІАЛІВ

МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»

ЕЛЕКТРОННЕ ВИДАННЯ

Кам’янець-Подільський
2023

УДК 32.019:004.056.5(063)
ББК 66.0Я431
З-41

Рекомендувала вчена рада Кам'янець-Подільського національного університету імені Івана Огієнка, протокол № 13 від 29 грудня 2022 р.

З-41 **Збірник матеріалів Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи»** [Електронний ресурс] / [за заг. ред. О. В. Віннічук]. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с.

Електронна версія збірника доступна за покликаннями:

URL: http://elar.kpnu.edu.ua:8081/xmlui/handle/123456789/7060

Збірник містить тексти доповідей і тези виступів учасників Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи», яку було проведено на базі Кам'янець-Подільського національного університету імені Івана Огієнка 3 листопада 2022 р. До збірника входять матеріали, в яких висвітлено проблеми інформаційної безпеки на міжнародному та українському просторі.

УДК 32.019:004.056.5(063)
ББК 66.0Я431

УДК 004.056.5

В. В. Зінченко, *доктор філософських наук, професор, старший науковий співробітник, головний науковий співробітник відділу дослідницької діяльності університетів Інституту вищої освіти НАПН України,*

Л. М. Червона, *кандидат філософських наук, старший науковий співробітник, завідувач відділу інтеграції вищої освіти і науки Інституту вищої освіти НАПН України*

ІНФОРМАЦІЙНА БЕЗПЕКА У КОНТЕКСТІ ТЕНДЕНЦІЙ РОЗВИТКУ СИСТЕМ AI (ARTIFICIAL INTELLIGENCE) І ПАРАДИГМ НАУКИ

Анотація. *Ми живемо в епоху Четвертої промислової революції (4IR), де кібернетика та обчислення ввійшли в життя людини. Роботи все більше стають схожими на людину, а людина вчиться взаємодіяти з ними, постійно вдосконалюючи їх не тільки зовні, але і внутрішньо. Огляд досліджень даної проблематики, котра виходить нині на «передній край» не лише у робототехніці та ШІ (штучному інтелекті), але й у – еволюційній генетиці, психології, філософії, педагогіці тощо, показує, що все більш вагомим стає підхід міжнаукової та мультидисциплінарної спільноти трансгуманістів. Згідно котрого – якщо машини (андроїди, кіборги, сигоми etc) стануть здатними до відчуття, почуття та емпатії – вони вже не будуть за суттю машинами. Тому зростає необхідність в усвідомленні можливих ризиків, пов'язаних, наприклад, з технологічною сингулярністю – гіпотетичним моментом в майбутньому, коли технологічний розвиток стане в принципі некерованим і незворотнім, що породить радикальні зміни (сингулярність) характеру людської цивілізації.*

Ключові слова: *інформаційна безпека, штучний інтелект, інтелектуальні системи.*

Розробки у сфері *штучного інтелекту* (ШІ), робототехніка та інтелектуальні системи стрімко розвиваються безпосередньо зараз, суто зараз приносять користь (і, водночас – вірогідні небезпеку та шкоду), безпосередньо зараз – істотно визначають наше буття – і незабаром визначатимуть ще істотніше.

Роботи все більше стають схожими на людину, а людина вчиться взаємодіяти з ними, постійно вдосконалюючи їх не тільки зовні, але і внутрішньо. В Японії робот що розмовляє, – андроїд Pepper – офіційно прийнятий до середньої школи в японському місті Васеда. Pepper вчиться разом з дітьми, яким надано можливість використовувати унікальний шанс спілкування з роботом. Вчені і педагоги вважають, що подібне спілкування стане в нагоді їм у майбутньому житті. Як стверджують розробники, робот оснащений великою кількістю камер і датчиків, які дозволяють йому розпізнавати і реагувати практично на весь спектр людських емоцій: радість, смуток, страх, хвилювання, роздратування. Він також має здатність до самонавчання [12].

Раніше в Японії вперше в історії кібернетичний андроїд на ім'я NAO зарахований до штату найбільшого в Японії банку The Bank of Tokyo-Mitsubishi UFJ. NAO – це людиноподібні роботи, розроблені корпорацією інформаційних технологій SoftBank. NAO легко пересуваються і жестикулюють маніпуляторами, за допомогою камер і звукових сенсорів вони реагують на відвідувачів, відповідають на питання і можуть підтримувати тематично різноманітні бесіди на багатьох мовах [9].

Сучасним соціальним проектантам варто приділити особливу увагу останнім технологічним тенденціям в інноваціях і вміти прогнозувати майбутнє. А для цього перш за все багато вчених рекомендують читати наукову фантастику, оскільки саме ця література стимулює мозкову діяльність, розвиває уяву і мислення.

Не випадково у Китаї в даний час велика увага приділяється науковій фантастиці. Ніл Гейман в інтерв'ю «The Guardian» заявив, що інтерес до наукової фантастики у китайців пов'язаний з тим, що у них блискуче виходило добре наслідувати, але було погано з новаторством, винаходами і були проблеми з уявою [5].

У результаті – китайці спрямували своїх представників до США – в Apple, в Microsoft, в Google – і просили людей, які винаходять майбутнє, розповісти про себе. У результаті з'ясувалося, що в дитинстві вони всі читали наукову фантастику. Фокусування на тверду наукову фантастику в Китаї дуже добре співвідноситься з перемогами китайських школярів в міжнародних тестах і конкурсах.

Виходить, що китайці активно почали формувати свій образ майбутнього. Бажаного позитивного майбутнього.

Однак і страх перед штучним інтелектом (ШІ) народився ще у 1960-х роках завдяки Ірвіну Гуду, британському математику і криптографу, який працював з Аланом Тьюрингом над зламом німецької шифрувальної машини «Енігма» під час Другої Світової війни.

Роздуми Гуда про ШІ привели його до думки про надрозумну машину, яка за рахунок самонавчання здатна перевершити інтелект людини, яким би розумним він не був. Коли ця машина почне будувати подібні собі машини, то відбудеться «інтелектуальний вибух» – це буде останній винахід, який потрібно буде зробити людині.

У 1965 році він створив концепцію, відому тепер як «інтелектуальний вибух» або «технологічна сингулярність», яка передбачає можливу появу надлюдського інтелекту [6].

Технологічна сингулярність (Technological singularity) – гіпотетичний момент в майбутньому, коли технологічний розвиток стає в принципі некерованим і незворотнім, що породжує радикальні зміни (сингулярність) характеру людської цивілізації. «Технологічна сингулярність» у футурології – це вибухоподібне зростання швидкості науково-технічного прогресу, яке ймовірно настане внаслідок створення штучного інтелекту і машин, здатних до самовідтворення. Гіпотетичний момент, після якого, на думку прихильників цієї концепції, технічний прогрес стане настільки швидким і складним, що виявиться недоступним для розуміння.

Але що якщо надрозумна машина одного разу втямить, що людина їй не потрібна, і стане вести себе на кшталт Термінатора – обмежувати права людей і, можливо, вбивати?

Тож не дивно, що в нинішній час ідеї Гуда знову стали актуальними. Хіба дивно й те, що їх підхопили провідні представники науки та ІТ-індустрії.

«Давайте визначимо надрозумну машину як машину, яка може набагато перевершити усю інтелектуальну діяльність будь-якої людини, якою б розумною вона не була б. Оскільки проектування машин є одним з цих видів інтелектуальної діяльності, надрозумна машина може створювати машини навіть краще; тоді, безсумнівно, стався б

«вибух інтелекту», і розум людини залишився б далеко позаду... Таким чином, перша надрозумна машина – це останній винахід, який коли-небудь знадобиться людині, за умови, що машина досить слухняна, щоб сказати нам, як тримати це під контролем. Цікаво, що за межами наукової фантастики про це так рідко говорять. Іноді варто серйозно поставитися до наукової фантастики» [8].

«Розробка повністю штучного інтелекту може наблизити занепад людської ери», – казав в 2014 році знаменитий фізик Стівен Хокінг [7].

«Спочатку не обтяжені інтелектом машини будуть виконувати більшу частину роботи за нас. І це добре, якщо ми навчимося правильно ними управляти. Але через кілька десятиліть ШІ розвинеться до тієї міри, щоб стати причиною для занепокоєння», – вторує йому засновник "Microsoft" Білл Гейтс [1].

Глава «Tesla» Ілон Маск пішов ще далі, він виділяє мільярди доларів щодо цих питань і, зокрема, пожертвував мільйони доларів на дослідження з безпеки ШІ «Future of Life Institute» [10] і порівняв розробників ШІ з озброєними святою водою екзорцистами, які намагаються приручити демона.

«Я думаю, що небезпека ШІ набагато більше, ніж навіть небезпека ядерних боєголовок, – сказав Маск. – Ніхто ж бо не запропонував би, щоб ми дозволили усьому світу просто вільно створювати ядерні боєголовки, якщо вони захочуть, – це було б божевіллям.

Згадаєте ще мої слова: ШІ – це набагато небезпечніше ядерної зброї» [4].

Глобальна пандемія спричинила безпрецедентні виклики кожному аспекту взаємодії з суспільством. В університетах перехід до віртуального викладання та навчання активізував дискусії щодо актуальності та майбутнього звичайних режимів контактних занять.

Незважаючи на пандемію, ми вже живемо в епоху ***Четвертої промислової революції (4IR)***, де кібернетика та обчислення ввійшли в життя людини.

В університетах виробництво знань стало «включати й машинний спосіб мислення», – як зазначила філософ Лучіана Паризі [11].

Ще за часів СРСР почала розвиватися така галузь психології, як «інженерна психологія та педагогіка», котра досліджує процеси і засоби інформаційної взаємодії між людиною і машиною, а також з/(між) технічними засобами автоматизації.

У Європейському Союзі – Європейською Комісією прийнято План дій з цифрової освіти [3].

Розроблено засадничий концептуальний та теоретико-прикладний і методично-інструментальний матеріал-книгу для використання у ЗВО та розвитку університеті «Біла книга: Штучний інтелект у вищій освіті», яка описує та визначає можливості та повноваження і проблеми штучного інтелекту у дослідженнях і навчанні, сприяє обговоренню про зміни в університетському викладанні, навчання культурі і можливостей викладання й розвитку освітнього, навчального контенту у взаємодії із застосуванням штучного інтелекту у контексті сучасних нейронаук.

Крім того, цей матеріал представляє бачення майбутнього університетської освіти і навчання з точки зору студентів та викладачів, щоб продемонструвати, як освіта і навчання можуть у зв'язку з ШІ змінитися в найближчі роки [13].

Коли університети стверджують, що слід приділити вагому та пильну увагу 4IR, це означає, що вони більше не можуть покладатися лише на традиційні форми людського мислення та уяви, але їм також потрібне мислення, яке залежить від алгоритмічних обчислень машин або форм технології. У цьому сенсі 4IR змінила не тільки те, що ми робимо і як це ми робимо, але й те, ким ми стали.

«Справа не в тому, що машини прийшли на заміну людині в найсуворішому розумінні, а в тому, що люди стали втіленими у машинах.

Таким чином, ми мусимо зупинитися і ретельно подумати над тим, що відбувається з освітньою зустріччю між викладачем та студентом за окремими просторами екранів.

Ми маємо звернутися до питань про людські зв'язки в епоху парадоксального посилення зв'язків між людьми» [2, с.56].

Огляд досліджень даної проблематики, котра виходить нині на «передній край» не лише у робототехніці та ШІ (штучному інтелекті), але й у – еволюційній генетиці,

психології, філософії, психіатрії, педагогіці, нейрології, біохімії та органічній хімії, мікробіології, антропології тощо показує, що все більш вагомим стає підхід міжнаукової та мультидисциплінарної спільноти трансгуманістів. Згідно котрого – якщо машини (андроїди, кіборги, сигоми etc) стануть здатними до відчуття, почуття та емпатії – вони вже не будуть за суттю машинами.

Список використаних джерел:

1. Bill Gates on dangers of artificial intelligence: «I don't understand why some people are not concerned». URL: https://www.washingtonpost.com/news/the-switch/wp/2015/-01/28/bill-gates-on-dangers-of-artificial-intelligence-dont-understand-why-some-people-are-not-concerned.
2. Davids N., Waghid Y. Teaching, Friendship and Humanity. Springer (Briefs in Citizenship Education for the 21st Century). 2020. 132 p.
3. Digital Education Action Plan (2021-2027). Commission Staff Working Document: Resetting education and training for the digital age. – Brussels, SWD (2020) 209 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 30.9.2020. 109 p. URL: https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-swd-sept2020_en.pdf.
4. Elon Musk said people who don't think AI could be smarter than them are «way dumber than they think they are». URL: https://www.businessinsider.com/elon-musk-smart-people-doubt-ai-dumber-than-they-think-2020-7?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+typepad%2Falleyinsider%2Fsilicon_alley_insider+%28Silicon+Alley+Insider%29.
5. Gaiman N. Why our future depends on libraries, reading and daydreaming. URL: https://www.theguardian.com/books/-2013/oct/15/neil-gaiman-future-libraries-reading-daydreaming.
6. Good I.J. Speculations Concerning the First Ultraintelligent Machine. 1965. URL: https://purl.stanford.edu/gz727rg3869.
7. Hawking S. Warns artificial intelligence could end mankind. URL: https://www.bbc.com/news/technology-30290540.
8. Koch C. When Computers Surpass Us. *Scientific American*. 2015. Vol. 26. Issue 5. P. 26-29. doi:10.1038/scientificamericanmind0915-26.
9. McCurry J. Japanese bank introduces robot workers to deal with customers in branches: Mitsubishi UFJ Financial Group is employing 'Nao', a multilingual 5.4-kg robot, who will begin work

in a branch in April. 4 Feb 2015. The Guardian. URL: https://www.theguardian.com/world/2015/feb/04/japanese-bank-introduces-robot-workers-to-deal-with-customers-in-branches.
10. Musk Donates $10 Million to Keep AI From Going Rogue. URL: https://www.technewsworld.com/story/82239.html.
11. Parisi L. Instrumentality, or the Time of Inhuman Thinking. – Technosphere Magazine. April 15, 2017. URL: https://technosphere-magazine.hkw.de/p/Instrumentality-or-the-Time-of-Inhuman-Thinking-5UvwaECXmmYev25GrmEBhX.
12. Pepper. *The Japan Times.* URL: https://www.japantimes.co.jp/tag/pepper/
13. De Witt C., Rampelt F., Pinkwart N. (Hrsg.). Das Whitepaper «Künstliche Intelligenz in der Hochschulbildung. Whitepaper. Berlin: KI-Campus, 2020. 59 s. DOI: 10.5281/zenodo.4063722.

INFORMATION SECURITY IN THE CONTEXT OF TRENDS IN THE DEVELOPMENT OF AI (ARTIFICIAL INTELLIGENCE) SYSTEMS AND PARADIGMS OF SCIENCE

Abstract. *We live in the era of the Fourth Industrial Revolution (4IR), where cybernetics and computing have entered human life. Robots are becoming more and more human-like, and humans are learning to interact with them, constantly improving them not only externally but also internally. A review of research on this issue, which is now coming to the forefront not only in robotics and AI (artificial intelligence), but also in evolutionary genetics, psychology, philosophy, pedagogy, etc. shows that the approach of the interdisciplinary and multidisciplinary community of transhumanists is becoming increasingly important. According to which – if machines (androids, cyborgs, sigmas, etc.) become capable of feeling, sentience and empathy – they will no longer be essentially machines. Therefore, there is a growing need to understand the possible risks associated, for example, with the technological singularity – a hypothetical moment in the future when technological development will become basically uncontrollable and irreversible, which will generate radical changes (singularity) in the nature of human civilization.*

Key words: *information security, artificial intelligence, intelligent systems.*

Отримано: 22.11.2022

УДК 101.37

С. О. Ганаба, доктор філософських наук, професор, кафедри психології, педагогіки та соціально-економічних дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького

МАНІПУЛЯЦІЯ ІНФОРМАЦІЄЮ В УМОВАХ ВЕДЕННЯ ВІЙНИ

Анотація. *Війна триває не лише у територіальному, а й інформаційному просторі країни. Створення й поширення інформаційного ресурсу є важливим засобом ведення боротьби, який вносить суттєві зміни у методи й тактику ведення війни. Засадничою умовою у застосуванні інформаційного ресурсу у протистоянні сторін є застосування інформації з метою нав'язування людям думки, вигідної лише для однієї сторони конфлікту з метою інформування людей. Єдиним шляхом збереження власної інформаційної стабільності є уважний аналіз повідомлень, усвідомлення політичних побажань, обов'язкова перевірка фактів у різних засобах інформації та критичне мислення.*

Ключові слова: *інформація, дезінформація, критичне мислення, фейки, інформаційна пропаганда.*

Військові дії між росією та Україною актуалізували проблему розповсюдження недостовірної інформації. Інформація відіграє головну роль у сучасному світі, саме тому американський дослідник М. Маклуен вивів таку тезу: «Істинно тотальна війна – це війна за допомогою інформації» [1]. Цей дослідник увів до наукового обігу поняття «інформаційна війна» й продемонстрував важливість інформаційного ресурсу в отриманні як нових суспільних благ, так й у привнесенні суспільних змін. Очевидно, що військові конфлікти різного масштабу та інтенсивності також залучають інформаційний ресурс, перетворюючи його у різновид зброї стратегічного значення.

Український інформаційний вплив зазнає сьогодні суттєвого впливу. Війна триває не лише у територіальному, а й інформаційному просторі країни. Створення й поширення інформаційного ресурсу є важливим засобом ведення боротьби, який вносить суттєві зміни у методи й

тактику ведення війни. Засадничою умовою у застосуванні інформаційного ресурсу у протистоянні сторін є застосування інформації з метою нав'язування людям думки, вигідної лише для однієї сторони конфлікту з метою інформування людей. Небезпека провокаційних повідомлень передусім у тому, що вони швидко поширюються. Згодом недостовірну інформацію спростують, але не завжди спростування прочитає той, хто читав перше, неправдиве повідомлення. Та й саме спростування може бути запізнілим, бо збурення мізків уже відбулося, й добре, якщо не перейшло у соціальне. Недостовірність може ховатися не лише у тексті, але в ілюстраціях.

Завданням тих, хто поширює дезінформацію, є саме підхоплення цих матеріалів найбільш популярними, головними мас-медіа, навіть, якщо це згадування відбувається у формі дійсності та сприйняття подій. Посилення й поширення наративу є одними з основних цілей пропагандистів. Процес розповсюдження фейків має властивості інформаційних операцій.

Однією із маніпуляцій них технологій – є фейкові новини, тобто інформація про резонансні події, яка не відповідає дійсності. Фейки бувають двох видів. Це або спеціально створена інформація про події, яких ніколи не було або ж неповна інформація, яка не повідомляє про всі відомості, які стосуються події. Обидва варіанти спотворюють об'єктивне відображання події. Варто зазначити, що фейки можуть створюватися ненавмисно. Основною причиною є непрофесійність журналістів чи блогерів, які не перевіряють достовірність інформації. Відповідно, що поняття фейків й дезінформації необхідно розмежовувати. Якщо фейки є результатом індивідуального виробництва, а дезінформація – інституційного. В одному випадку це людина, яка може і помилитися, оскільки в голові у неї немає наміру обдурити кого-то. Уразі дезінформації вихідним джерелом може бути структура, яка приховує свій справжній характер. Її дії спрямовані на те, щоб увести в оману. Однак і ті, й інші належать до інструментів маніпуляції.

Фейк – це новини без справжніх подій. Парадоксальним чином фейк є «правдивим» повідомленням, тому що йому вірять багато людей. Фейки приходять одночасно і паралельно з популізмом, що вразив багато країн. Борють-

ба з фейками ускладнюється тим, що це реагування не на розум, а на психіку людей. Навчання розпізнаванню фейків вибудовується як раз на раціональній основі, а вона тут працює слабо. Сила фейків аж ніяк не в них самих, вона у психології людей. Технології просто полегшили доставку конкретного «тригера» того чи іншого психологічного типажу людини, зробивши це в один момент масово. З цієї причини фейки прийшли всерйоз і надовго, адже цей старий трюк отримав абсолютно нову силу через механізми інтернету. Саме через анонімність і масовий характер, ховаючись за ширмою інтернету, можна безстрашно завдавати удару найбільшій аудиторії.

Фейк для хорошого поширення повинен мати низку характеристик. Наприклад, він повинен нести негативну інформацію, тому що негатив поширюється в кілька разів сильніше. Він повинен бути з тих же причин, адже тоді це може зачепити людину за живе. Є навіть застереження: якщо є занадто багато емоцій, хтось намагається маніпулювати вами. Фейк сам по собі не є страшним, небезпечно, коли він є частиною кампанії.

Отож, лише критичне сприйняття будь-якого виду інформації, її ретельна перевірка в альтернативних джерелах допоможуть визначити правдивість повідомлень. Достовірною уважають інформацію, якщо є джерело повідомлення, є вказівка на компетентність джерела, за потреби – наявність кількох джерел інформації. Особливе значення має точність інформації під час висвітлення конфліктів. Перекручування, неадекватність подання цитованої мови; виривання фраз із контексту, що дає хибне уявлення про сенс сказаного; додавання до прямої мови слів, які не відповідають переконанням респондентів, усе це грубі порушення стандарту точності.

Єдиним шляхом збереження власної інформаційної стабільності є уважний аналіз повідомлень, усвідомлення політичних побажань, обов'язкова перевірка фактів у різних засобах інформації та критичне мислення.

Список використаних джерел:

1. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. Київ: НІСД, 2011. 30 с.

2. Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. Інформаційне суспільство: технології та безпека. *Інформація та відкритість влади як засоби демократизації суспільства*: збірник матеріалів «круглого столу». Київ: Альтпрес, 2003. С. 119-124.

MANIPULATION OF INFORMATION IN THE CONDITIONS OF WARFARE

Abstract. *The war continues not only in the territorial, but also in the information space of the country. The creation and dissemination of an information resource is an important means of fighting, which makes significant changes in the methods and tactics of warfare. A basic condition in the use of information resources in the conflict between the parties is the use of information with the aim of imposing on people an opinion that is beneficial to only one side of the conflict for the purpose of informing people. The only way to maintain one's own informational stability is careful analysis of messages, awareness of political wishes, mandatory fact-checking in various media and critical thinking.*

Key words: *information, disinformation, critical thinking, fakes, information propaganda.*

Отримано: 25.11.2022

УДК 327:001.5

В. В. Кривошеїн, *доктор політичних наук,*
в.о. декана факультету суспільних наук
і міжнародних відносин Дніпровського національного
університету імені Олеся Гончара

АНАЛІТИЧНИЙ ПОТЕНЦІАЛ ТЕОРІЇ РЕГІОНАЛЬНИХ КОМПЛЕКСІВ БЕЗПЕКИ БАРРІ БУЗАНА

Російсько-українська війна, розпочата 24 лютого 2022 року, надзвичайно актуалізувала інтерес науковців до проблеми регіональної безпеки. Продуктивним у цьому ключі може бути теорія регіональних комплексів безпеки Баррі Бузана (нар. 1946 р.), який головним критерієм виокремлення конкретних міжнародних регіонів називає високий рівень взаємозалежності у сфері безпеки, що усвідомлюється сусідніми між собою державами.

Під комплексом безпеки Б. Бузан розуміє транснаціональний регіон, що містить держави та їхні складові частини, яких об'єднують сталі уявлення про безпеку та відносини у сфері безпеки. При цьому інтереси цих держав у сфері безпеки настільки близькі, що жодна з них не може розглядати свою національну безпеку у відриві від національної безпеки своїх сусідів.

За Б. Бузаном, основними параметрами регіональних комплексів безпеки є:

- кордони, які відокремлюють один регіон від іншого;
- анархічна структура, тобто регіон має складатися з двох або більше автономних одиниць (держав);
- полярність, яка характеризує поширення сили між основними учасниками регіону;
- соціальна складова, яка визначає сприйняття державами сусідів усередині регіону за шкалою «друг-ворог» (див.: [1]).

По суті, концепція безпекових комплексів фокусує свою увагу на існуванні в регіоні більше, ніж двох суб'єктів, полярності між ними та діалогу у форматі «друг-ворог». Полярність між регіональними державами варіюється від однополярності (уніполярності) до багатополярності (мультиполярності) та від дружби до ворожнечі. Такі

варіації проходять певну еволюцію від конфліктогенності через режим безпеки до безпекової спільноти.

На основі цієї закономірності Б. Бузан виділяє типологію регіональних безпекових комплексів:

1. Стандартний, за яким полярність визначається регіональними державами (силами). Наприклад, Середній Схід, Південна Америка, Південно-Східна Азія, Південна Африка).
2. Центральний, який представлений декількома головними формами. Тут Б. Бузан виділяє дві форми, які характеризуються однополярністю, але різниця між ними полягає у домінуванні в регіоні або наддержави, або світової держави. Ці держави є лідерами не лише на регіональному, а й на глобальному рівні, тому інші суб'єкти регіонального угрупування не мають змоги створити полюс силової противаги попереднім двом (за Б. Бузаном, такими потенційними полюсами можуть бути Україна, Канада і Мексика; потенційно до цього типу може належати й Південна Азія, де Індія, як гравець з якостями лідера, не сприймає Пакистан за інший полюс сили). Ще однією формою є інституціональна, яка характеризує першість у регіоні не як один силовий центр, а через інтеграційне об'єднання, яке досягло високої безпекової взаємодії. Прикладом цього є Європейський Союз, який виступає актором як регіональної (європейської), так і світової арен. Б. Бузан також припускає наявність перехідної форми від однополярності до інституціональної форми (хоча прикладів цієї форми він не знаходить).
3. Світова держава, обумовлена існуванням біполярного або мультиполярного центру сил у регіоні. Прикладом цього може слугувати Східна Азія, де силове ядро представлено двома конкуруючими державами – Китаєм та Японією. Світова держава в цьому контексті пояснюється через залучення цих акторів до діяльності на міжнародному рівні. Тобто гібридне утворення із глобального і регіонального рівнів взаємодії в одному безпековому комплексі.
4. Суперкомплекси, у яких формується сильний міжрегіональний рівень безпеки, який динамічно зростає та на

якому слабкі держави можуть заручитися допомогою наддержави або світової держави проти держави-ядра регіону. Прикладом цього слугує Південно-Східна Азія, де спостерігається співпраця по лінії Пакистан – Китай на противагу Індії (див.: [2]).

Кожний регіон можна розглядати за класичними для всіх держав рівнями взаємодії в межах системи регіональної безпеки: рівень внутрішньої ситуації у тій чи іншій державі регіону, зокрема, наявність дестабілізуючих факторів усередині країни, які впливають на центральну владу та створюють сприятливе середовище для виникнення у неї страху перед загрозами безпеці; відносини у форматі «держава-держава» у регіоні, тобто двосторонні контакти; співпраця конкретного регіону із сусідніми регіональними структурами, у результаті якої відбувається процес безпекової залежності; роль світових держав у регіоні, яка визначається взаємодією між регіональним та глобальним рівнями безпеки. Тобто регіональна безпека може існувати окремо в деяких аспектах, але на неї впливає стан як національної, так і глобальної, які є основними складовими міжнародної безпеки.

Отже, за теорією Б. Бузана, проблема безпеки в регіоні розглядається на чотирьох рівнях:

1) внутрішньодержавний рівень або внутрішня ситуація у тій чи іншій державі регіону;
2) регіональний рівень або відносини у форматі «держава-держава;
3) міжрегіональний рівень або співпраця конкретного регіону із сусідніми регіональними структурами;
4) глобальний рівень або роль світових держав у регіоні.

Список використаних джерел:

1. Buzan B. New Patterns of Global Security in the Twenty-First Century. *International Affairs*. 1991. Vol. 67 (3). P. 431-451.
2. Buzan B., Waever O. Regions, and Powers. The Structure of International Security. New York: Cambridge University Press, 2003. 570 p.

Отримано: 23.11.2022

УДК 32.019.5

А. А. Шуліка, *доктор політичних наук, доцент, професор кафедри політології Дніпровського національного університету імені Олеся Гончара*

ЗАСОБИ ПОЛІТИЧНОЇ ПРОПАГАНДИ РФ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Анотація. *У статті розглядаються особливості формування політичної пропаганди в сучасному інформаційному комунікативному просторі. Стверджується, що сучасна пропаганда Російської федерації використовує значний обсяг засобів впливу. Це застосовується для маскування власних агресивних дій та замовчування військових злочинів.*

Ключові слова: *пропаганда, політична пропаганда, інформаційний простір, засоби пропаганди, російська пропаганда.*

Пропаганда у світі існує у багатьох формах завдяки розвитку форм комунікації та різноманітності технічних форм передачі інформації. Але при цьому пропаганда завжди має характерні ознаки, які можна чітко виділити, наприклад, пропаганда завжди реалізує функцію переконання, чітко орієнтовану цільову аудиторію, емоційні заклики та ін.

Пропаганда передається за допомогою низки прийомів, їх виявлення дозволяє провести аналіз інформаційного потоку та сформувати чіткий алгоритм боротьби з пропагандою, що є особливо актуальним у контексті війни України з Росією. Набір пропагандистських прийомів та методів різняться у більшості дослідників. Нижче ми опишемо прийоми пропаганди та форми їхнього прояву в сучасній російській пропаганді. За основу ми візьмемо список прийомів пропаганди, запропонований колективом авторів, дослідників пропаганди в сучасному світі [1].

1. Використання специфічних мовних маркерів. Наприклад, сюди відноситься використання слів/фраз, які уособлюють сильні емоційні тригери для впливу аудиторію. Так, у разі російської пропаганди для опису українського народу, політиків, армії вже багато років використовують терміни «нацизм», «фашизм» та інші маркери, пов'язані з цими термінами.

2. Навішування ярликів. Позначення об'єкта пропагандистської кампанії як чогось, чого цільова аудиторія боїться, ненавидить, що визиває негативні асоціації. Такі ярлики російська пропаганда постійно намагається навісити на представників ЗСУ, в основному називаючи їх «бандерівцями», «націоналістичними батальйонами». Також на тлі успіхів ЗСУ російська пропаганда почала використовувати ярлики, пов'язані з маркерами «іноземні найманці», «війська НАТО», що мало підкреслити «боротьбу армії РФ з усіма військами НАТО». Також в ЗМІ РФ по відношенню до української влади використовуються постійні образи, на кшталт, «наркомани».

3. Повторення одного і того ж повідомлення, щоб глядачі зрештою прийняли його. Цей метод застосовується для того, щоб сформувати стійке поняття, термін або твердження, яке навіть у тому випадку, якщо воно повністю вигадане, фейкове за допомогою постійного повторення входить до соціально-політичного порядку денного. Як приклад можна навести постійні твердження російської пропаганди про існування «біологічних лабораторій» в Україні та підготовку «біологічної зброї проти росіян». Сюди ж можна віднести постійні повторення про те, що «Україна готувала напад на РФ і Білорусь».

4. Перебільшення чи применшення. Або уявлення чогось у надмірній мірі: збільшення, поліпшення, погіршення та ін. Якщо аналізувати російську пропаганду під час наступу та звільнення територій України, то ми можемо побачити коливання російської пропаганди від применшення можливостей ЗСУ («вони гинуть тисячами, але не можуть перемогти») до паніки та перебільшення чисельності армії України («тисячі іноземних найманців», «війська НАТО», «число переважаючих сил України»).

5. Сумнів у достовірності. Так під час наступу ЗСУ у Харківській та Херсонській області офіційні російські ЗМІ та Міністерство оборони РФ визнавали відступ військ із запізненням у 1-2 дні від реального часу, при цьому називаючи сумнівними не лише офіційні українські новини, а й повідомлення, які публікували військові кореспонденти РФ.

6. Взивання до страху/упередження. Прагнення побудувати підтримку ідеї, вселяючи тривогу та/або паніку серед населення. До цього можна віднести великий інфо-

рмаційний потік повідомлень, що після звільнення Харківської області «війська ЗСУ нападуть на Бєлгород та інші території РФ». Сюди можна віднести постійну спробу пропаганди РФ просунути «подвиги» «загонів Кадирова».

7. «Розмахування прапором» [1]. Пропаганда намагається впливати на групову ідентичність (національність, расу, стать, політичні уподобання) для виправдання чи просування дії або ідеї. Багато в чому цим пунктом прийомів пропаганди пояснюється постійний наголос російської пропаганди на концептах «російського народу», «російськомовного населення», також можна віднести сюди концентрацію РФ на гендерних питаннях і сексуальної орієнтації. Тут пропаганда концентрується на протиставленні «свій-чужий».

8. Спрощення. Пропаганда передбачає одну (найчастіше конкретну та максимально зрозумілу) причину, коли є цілий ланцюжок різноманітних причин, що стоять за існуючою ситуацією. Так у сучасному РФ постійно намагаються знайти конкретних винних у економічних, політичних та військових поразках РФ, не згадуючи прізвище президента Росії і не згадуючи загальний рівень соціального та економічного розвитку.

9. Гасла, які виступають як емоційні заклики. Тут можна згадати спроби пропаганди РФ нав'язати мирному населенню України на тимчасово окупованих територіях гасла «Росія прийшла назавжди» та ін.

10. Звернення до авторитету. Стверджуючи, що претензію виправдано просто тому, що обраною пропагандою авторитет/експерт підтримує це без будь-яких інших підтвердних доказів. Для цього в російському інформаційному просторі існує цілий набір експертів з будь-яких питань, які постійно підтримують позицію офіційних ЗМІ РФ. Наприклад, досить важливим елементом російської пропаганди є залучення «іноземних експертів та аналітиків». Вони постійно залучаються до політичних пропагандистських програм РФ і навіть під час фейкового «референдуму» в областях України пропаганда окремо наголошувала на участі іноземних спостерігачів, хоча жодна сертифікована міжнародна організація не оголошувала про участь у цьому псевдо-волевиявленні.

11. «Чорно-біле протиставлення» [1]. Подання двох альтернативних варіантів як єдиних можливостей. У контексті російської пропаганди тут можна назвати тезу, що часто згадується, про те, що «Росія або виграє, або перестане існувати».

12. Кліше. Слова чи фрази, що перешкоджають критичному осмисленню та осмисленому обговоренню заданої теми. Це зазвичай короткі, загальні пропозиції, які пропонують, здавалося б, прості відповіді на складні питання або які відволікають увагу від інших ліній роздумів. Наприклад, кліше «Донбас бомбили 8 років» відразу став основою російської пропаганди, який просувався через «фабрики тролів».

13. «Що з приводу» [1]. Пропаганда дискредитує позицію опонента, звинувачуючи його в лицемірстві, не спростовуючи його аргументи. До цього пункту можна віднести постійні згадки пропаганди РФ про «небажання української сторони вести мирні переговори», при цьому ніяк не акцентується на реальних позиціях «переговорників» Росії.

14. «Червоний оселедець» [1]. Введення матеріалу, що не відноситься до обговорюваного питання, щоб відвернути увагу всіх від суті події. Цей прийом пропаганди є відволікаючим аргументом, який відводить від проблеми, яка була в центрі обговорення. Цей прийом дуже популярний у російської пропаганди. Він активно використовувався ще у 2014 році у випадку збиття Boeing 777, коли РФ вкидала величезну кількість версій: «ракетний удар», «збила Україна» та ін. У 2022 році це можна було побачити в контексті опублікування результатів військових злочинів РФ в Бучі, коли у відповідь з'явилася велика кількість фейкових новин про «манекени», «акторів», «тіла, що рухаються», «заморожені трупи», «постановочні кадри для ЗМІ», що мало розосередити інформаційний порядок денний.

15. Заплутаність, навмисна неясність. Використання свідомо незрозумілих термінів, слів, щоб аудиторія сформувалась певна інтерпретація подій. До цього можна віднести відомі терміни російської пропаганди «відхід більш вигідні позиції», «добра воля РФ», «негативне зростання» та ін.

Таким чином, сучасна російська пропаганда використовує величезну кількість різноманітних прийомів та ме-

тодів під час війни в Україні. Дослідження сутності російської пропаганди забезпечує найкраще розуміння світовим та українським суспільством політичної реальності. Також це впливає на більш якісне формування механізмів боротьби з російською пропагандою.

Список використаних джерел:

1. Da San Martino G., Yu S., Barron-Cede A., Petrov R., Nakov P. Fine-Grained Analysis of Propaganda in News Articles. *Conference on Empirical Methods in Natural Language Processing.* Hong Kong. China. November 3-7, 2019. P. 5636-5646.

MEANS OF POLITICAL PROPAGANDA OF THE RUSSIAN FEDERATION IN THE MODERN INFORMATION SPACE

Abstract. *The article examines the peculiarities of the formation of political propaganda in the modern information and communication space. It is claimed that modern propaganda of the Russian Federation uses a significant amount of means of influence. It is used to mask one's own aggressive actions and silence war crimes.*

Key words: *propaganda, political propaganda, information space, means of propaganda, Russian propaganda.*

Отримано: 21.11.2022

УДК 323.2:327

С. Г. Вонсович, *доктор політичних наук, професор кафедри політології та філософії Кам'янець-Подільського національного університету імені Івана Огієнка*

ІНФОРМАЦІЙНА ВІЙНА ЯК ПРОТИДІЯ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Анотація. *Розкрито ознаки інформаційної війни в нових історичних і політичних умовах. Зазначено, що метою інформаційної війни є, вплив на свідомість і поведінку людей, щоб змусити їх мислити і діяти в своїх інтересах за допомогою маніпулювання інформацією. Визначено особливості ведення інформаційної війни в умовах повномасштабної війни Росії проти України.*

Ключові слова: *інформаційна війна, загрози інформаційній безпеці, війна сенсів, інформаційна зброя.*

Однією з головних рис сучасності є широкомасштабне використання інформаційно-комунікаційних технологій, які стали уособленням нової стадії науково-технічного та соціально-економічного прогресу людства. Проте вони ж породили безліч проблем і загроз, про які раніше ніхто не здогадувався. Однією з них є інформаційна війна, яка стає все більш важливою темою у наукових дослідженнях. Для забезпечення інформаційної безпеки доречно виокремити низку ознак та, власне, й мету інформаційної війни: монополізація газет, журналів, радіо і телебачення, а також засобів зв'язку спеціалізованими корпораціями; пряме підпорядкування засобів інформації та зв'язку олігархічному капіталу; відкрите втручання державних органів у сферу ЗМІ, заборона або позазаконне обмеження свободи слова; панування порівняно невеликої кількості засобів масової інформації й інформаційних агентств на світовому ринку новин; монополізація інформаційного простору країни або регіону; поглиблення диспропорцій у забезпеченості засобами інформації та зв'язку між розвиненими державами і країнами, що розвиваються; використання друкованою пресою, радіо, телебаченням та інформаційними агентствами розвинених країн інформаційного забезпечення власної внутрішньої та зовнішньої політики на теренах інших країн; публікацію низки мате-

ріалів, спрямованих на дискредитування певної політичної сили, заходу, політика; створення негативного іміджу політичної сили, руху, державного діяча, значного заходу в країну об'єктів інформаційної експансії. Мета – за допомогою маніпулювання інформацією, впливати на свідомість і поведінку людей, щоб змусити їх мислити і діяти в інтересах агресора. Інформаційна війна пронизує нині всі форми боротьби, починаючи від дипломатичної й економічної та закінчуючи збройною боротьбою, розвиваючись разом з тим, як самостійна сфера діяльності. Не випадково багато авторитетних дослідників уважають, що забезпечення військової безпеки в XXI ст. все більше залежатиме від інформаційних чинників. Так, відомий американський футуролог О. Тоффлер у книзі «Війна та антивійна» [1, p.45] зазначав, що інформація стає найважливішим військово-стратегічним ресурсом щонайменше або навіть важливішим, аніж традиційні види озброєнь і військової техніки. А це означає, що держава, яка дбає про свій оборонний потенціал, має приділяти величезну увагу розвитку методів інформаційної протидії та інформаційного впливу.

Про масштабність інформаційної війни Росії проти України свідчить ряд фактів: інформаційний фронт розгортається одразу на кількох напрямах. По-перше, серед населення в зоні конфлікту; По-друге, серед населення країни, проти якої здійснюється агресія, однак територія якої не охоплена конфліктом; По-третє, серед громадян країни агресора; По-четверте, серед міжнародного співтовариства. Хоча інформаційний складник справді став наскрізною темою війни, проте він виконує не самостійну, а допоміжну роль, більшою мірою супроводжуючи військову фазу операції. Однак В українському випадку маємо справу не просто з ворожою пропагандою, а з тим, що фахівці слушно характеризують як «війну смислів/сенсів» [2; 3]. Для ретрансляції цих смислів задіяно множину каналів донесення інформації. Основним структурним елементом у цій війні стають симулякри – образи того, чого в реальності не існує. Стратегічна мета експлуатації цих симулякрів – замінити об'єктивні уявлення цільових груп про характер конфлікту тими «інформаційними фантомами», які потрібні агресору.

Саме тому сукупність умов і факторів, які створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері виступають загрозою інформаційній безпеці. Це: загрози впливу неякісної інформації (недостовірної, дезінформації, шейків, квазіфейків) на особистість, суспільство, державу; загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання); загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.). Доречно виділити джерела загроз, які торкаються інтересів особистості, суспільства і держави. Найнебезпечнішим джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за рахунок формування навколо неї індивідуального «віртуального інформаційного простору», а також можливість використання технологій впливу на її психічну діяльність. Важливою особливістю способу життя людини в інформаційному суспільстві є суттєве скорочення «інформаційних» відстаней: часу доступу до необхідної інформації. Людство впритул підходить до межі, за якої інформаційна інфраструктура стає основним джерелом інформації для людини, здійснює безпосередній вплив на її психічну діяльність, на формування її соціальної поведінки. Іншим джерелом загроз інтересам особистості є використання на шкоду її інтересам персональних даних, які нагромаджуються різноманітними структурами, в тому числі органами державної влади, а також розширення можливості латентного збору приватної інформації. Це зумовлено, у першу чергу, труднощами реалізації механізмів охорони цих відомостей, подальшими досягненнями у мікромініатюризації засобів прихованого збирання і передачі інформації. Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливих інфраструктур забезпечення життя суспільства. Такі загрози можуть прояв-

лятися у вигляді спроб здійснення шахрайських операцій з використанням глобальних або локальних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою. Проте найбільш небезпечним є неконтрольоване розповсюдження інформаційної зброї. Небезпека полягає у створенні атмосфери бездуховності та аморальності, негативного ставлення до культурної спадщини противника; маніпулюванні суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та керованого хаосу; дестабілізації політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокуванні репресій проти опозиції, провокації взаємного знищення; зниженні інформаційного забезпечення влади та управління, інспірації помилкових управлінських рішень, та інше.

Сучасне інформаційне середовище характеризується технологіями та політичною поляризацією. Автор концепції суверенності, професор права Стренфорда, Персілі, побачив новизну кампанії Трампа якраз у руйнуванні традиційних політичних та інформаційних інститутів. Персілі пише: «Переважання фальшивих історій в онлайні формує бар'єри для поінформованого прийняття політичних рішень і робить менш ймовірним те, що виборці вибиратимуть на підставі справжньої інформації, а не брехні» [4].

Отже, в сучасних умовах констатуємо Виокремимо ряд факторів, які змінили інформаційне середовище і сприяють появі нових форм інформаційної війни, які загрожують інформаційній безпеці. Це: демократизація створення та розповсюдження інформації, за чого будь-який індивід або група може впливати в онлайні на велику кількість людей; інформаційна соціалізація, що призводить до отримання інформації звідусіль, а не з інституційних джерел, які відповідають стандартам журналістики; атомізація як розходження індивідуальних новин від брендів та джерел; анонімність створення та розповсюдження інформації: для читача сьогодні важливіше те, хто надіслав інформацію, ніж її

джерело; персоналізація інформаційного середовища, що відрізняє його від друку, радіо та телебачення, дозволяючи користуватися мікротаргетингом.

Список використаних джерел:

1. Toffler A. War and Anti-War. N.Y.: Little, Brown and Company, 1993. 302 p.
2. Почепцов Г. Інформаційна війна як інтелектуальна війна. URL: http://osvita.mediasapiens.ua/material/133032 (дата звернення: 20.09.2022).
3. Горбулін В. Геополітичний реванш: від ідеї до стратегії. URL: https://dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html (дата звернення: 19.07.2022).
4. Persily N. Can Democracy Survive the Internet? *Journal of Democracy*. 2017. Vol. 28. №2. P. 63-76.

INFORMATION WARFARE AS COUNTERACTION TO INFORMATION SECURITY

Abstract. *The signs of information warfare in new historical and political conditions are revealed. It is noted that the purpose of the information war is to influence people's consciousness and behavior in order to make them think and act in their own interests by manipulating information. The specifics of conducting an information war in the conditions of a full-scale war between Russia and Ukraine have been determined.*

Key words: *Information war, threats to information security, war of meanings, information weapons.*

Отримано: 16.11.2022

УДК 327:001.5

І. М. Ковальська-Павелко, *кандидат історичних наук,*
доцент кафедри історії України Дніпровського
національного університету Імені Олеся Гончара

АХІСТОРИЦИЗМ СТРУКТУРНОГО РЕАЛІЗМУ КЕННЕТА ВОЛТЦА

Творець структурного реалізму Кеннет Волтц (1924-2013) у 1979 р. запустив механізм трансформації класичного політичного реалізму в неореалізм. Зберігаючи основні категорії класичного політичного реалізму – сила, національний інтерес, боротьба за владу, – неореалізм прагне до збагачення його досягненнями системної теорії [1, p. 37].

Головна заслуга К. Волтца у розвитку теорії реалізму полягає в тому, що він привернув увагу до проблем аналізу міжнародних відносин. На його думку, природа людини може призвести до війни, але навряд чи її можна використовувати як аналітичний інструмент, щоб пояснити, чому іноді розв'язується війна, а іноді встановлюється мир. К. Волтц стверджував, що в будь-якому випадку це був один із факторів першого образу або рівня аналізу міжнародних відносин, і оскільки людську природу неможливо змінити, то увага зміщується на аналіз політичних інститутів [1, p. 150]. Ця сфера державних режимів, що складаються порізному, і багато факторів, що діють в них – їх демократична чи автократична структура, їхня домінуюча політична ідеологія, їхній економічний стан, їх соціальна структура, вплив груп, громадської думки тощо – втілювали другий рівень аналізу. Але були очевидні межі визначального впливу внутрішньої природи держав, тому пропонується третій рівень аналізу, який містить саму міжнародну систему, і розуміння її істотної анархії і обмеження, які вона могла б накладати на державних акторів.

Саме пропагування представниками неореалізму третього рівня аналізу призвело до звуження теорії до питань структури міждержавної системи та викликало подальше відчуження багатьох істориків від цієї галузі. К. Волтц намагався пояснити довгострокову безперервність у міжнародних відносинах («вражаючу однаковість якості міжнародного життя протягом тисячоліть»), яка зберігалася «на-

віть коли діючі особи змінюються», побудувавши теорію міжнародної політики, яка б усунула недоліки сучасних теорій. Вчений активно використовував метод висунення гіпотез, які можна було б довести або спростувати шляхом спостереження за взаємодією держав протягом всієї історії. Він прагнув створити теорію, позбавлену несуттєвих змінних, які могли б встановити значні обмеження на поведінку держави, які були породжені панівною анархічною структурою, в рамках якої повинні були діяти унітарні суверенні держави. Такий підхід створив більш м'яку теорію, але вона була за своєю суттю неісторичною (хоча історичні дані вибірково використовувалися для підтвердження гіпотез, що висувалися). Ця відмова від історизму (ахісторицизм) була закріплена в припущеннях К. Волтца щодо системних обмежень для акторів здійснювати раціональні розрахунки (не пом'якшених культурними та соціальними факторами) та міждержавного режиму, який залишився незмінним у своїх основних характеристиках з часу виникнення суверенної держави у XVII ст. Для К. Волтца історія була корисною лише тому, що вона могла встановити довгострокову фіксовану безперервність структури (або парадигми), в рамках якої продовжували функціонувати сучасні міжнародні відносини.

За К. Волтцем, мета неореалізму полягає в тому, щоб показати, як глобальна система створює параметри для міжнародних відносин, маючи на увазі, що теорія може передбачити ймовірні результати краще, ніж історія, яка зайнята унікальністю події, або історична соціологія, в якій домінують концепція прогресивного розвитку. У той же час американський представник неореалізму підкреслював, що його теорія не стосується прогнозування конкретних результатів, реакції окремих станів у будь-який момент часу на обмеження системи. Він запропонував науковий метод, який не потребував «історичної випадковості»: «Нації змінюються за формою та метою; відбувається науковий прогрес; озброєння радикально трансформується; союзи створюються і розриваються. Це зміни всередині системи» [1, p. 87]. Його теорія позбулася як необхідності аргументації, заснованої на людській природі, так і пошуку безлічі факторів другого образу (рівня) аналізу.

Отже, відповіддю неореалістів на критику щодо неврахування історичних змін продовжили полягати в тому, що тією мірою, якою історія може бути використана, вона не впливає на ядро теорії. Історичне питання про те, як склалася сучасна державна система з її структурною анархією, не має особливого значення для теоретичних цілей. Структура не враховує все, а також теорія не пояснює і не передбачає всього. Збагачення теорії історією, як пропонують критики, лише незначно підвищить її точність опису, водночас зменшуючи її теоретичну чіткість і силу передбачення. Таким чином, неореалізм виглядає стійким до спростування через звинувачення в його неісторичності, принаймні на теоретичному рівні. У той же час критики та прихильники конкуруючих теорій чи підходів не заперечують історичних узагальнень, які робить К. Волтц, принаймні у зв'язку з основною епохою, до якої вони стосуються, а саме системою держав, що існує з 1648 року.

Список використаних джерел:

1. Waltz K. Theory of International Politics. New York: McGraw-Hill, 1979. 256 p.

Отримано: 16.11.2022

УДК 316.774+32.19.51

О. С. Зубченко, *кандидат соціологічних наук,*
доцент кафедри політології та соціології
Маріупольського державного університету

ІНФОРМАЦІЙНА БЕЗПЕКА У СПОЖИВАННІ ЕЛЕКТОРАЛЬНИХ ДАНИХ

Анотація. *Доповідь присвячено проблемі об'єктивного представлення результатів електоральних досліджень у засобах масової інформації. У період виборчих кампаній ці дані стають інструментом впливу на громадську думку та політичних маніпуляцій. За таких умов завдання соціолога – чітко розрізняти професійні та громадсько-політичні ролі, дотримуватись законодавчих та етичних стандартів, сприяти підвищенню рівня соціологічної культури представників ЗМІ.*

Ключові слова: *електоральні дослідження, псевдосоціологи, ефект луна-камери, соціологічна просвіта.*

В епоху інформаційного суспільства електоральна соціологія все більше набуває просвітницької функції. Професійна діяльність соціологів виходить далеко за академічні межі та охоплює широке коло соціально-політичних та медійних практик. Все частіше вони керують виборчими кампаніями, стають частими гостями телевізійних ток-шоу та головними героями випусків новин.

У період виборчих кампаній рейтинги, що оприлюднюються у мас-медіа, стають важливим інструментом впливу на громадську думку. Як зазначає О. Стегній, електоральні дослідження поєднують теоретичні та емпіричні складові соціологічного знання, його професійний та публічний виміри [4, с. 15]. Це відкриває перед фахівцями можливість отримати статус авторитетних експертів, здобути довіру у професійному середовищі та громадськості або навпаки – дискредитувати свою репутацію, поставити під сумнів власну спроможність бути об'єктивним і незалежним модератором у відносинах влади і суспільства.

Під час висвітлення у ЗМІ виборчих перегонів соціологи виступають у двох основних ролях – як аналітика та як полстера. Іпостась аналітика – це насамперед характеристика сфери наукових інтересів дослідника, його фор-

мального визнання державними установами (наукові ступені та вчені звання), авторитету серед колег, підтвердженого низкою наукових публікацій у цій сфері. Натомість полстер – це насамперед людина, яка вміє на високому методичному та організаційному рівні провести збір, обробку та аналіз емпіричних даних на задану замовником тему. Ця відмінність суттєво впливає на стиль і формат подання та інтерпретацію результатів опитувань, але, на жаль, лишається майже непомітною для більшості журналістів та пересічних громадян.

Але часто дослідник може виступати ще у одній, не притаманній для себе якості, – безпосереднього учасника виборчого процесу. В цьому немає нічого поганого, адже професійні соціологи, як і решта громадян України, можуть мати власні політичні погляди та переконання. У такому випадку у медіа-просторі соціолог має проводити чітку межу – де він виступає як громадсько-політичний діяч, а де – як представник професійного співтовариства.

Також під час виборів на медійні вогники злітається чимало самозванців – людей, які щось, десь, колись чули про соціологію, знають кілька професійних термінів, але жодного дня не працювали за фахом та не мають відповідних наукових здобутків. Н. Паніна влучно зауважувала, що завдяки розвиненому відчуттю політичної та медійної кон'юнктури, лексиці та логіці, що наближена до широкого загалу, та чіткій прагматичній мотивації вони отримують низку переваг над справжніми вченими [3, с. 48]. Псевдофахівці не обтяжують себе науковими обґрунтуваннями і викладають свої думки різко та безапеляційно.

Загалом, проблема оприлюднення соціологічних даних у ЗМІ має два аспекти – юридичний та професійно-етичний. Стаття 50 Виборчого кодексу України визначає, що організатори досліджень мають обов'язково зазначати час проведення електорального дослідження, територію, яку воно охоплювало, розмір та спосіб формування вибіркової сукупності, метод збору інформації, точні формулювання запитань, можливу статистичну похибку та замовника опитування [1]. Такі самі вимоги поширюються і на всі без виключення ЗМІ, в тому числі інтернет-сайти. Оприлюднення результатів електоральних досліджень забороняється за два дні до виборів. Проте у соцмережах та

телеграм-каналах проконтролювати дотримання цих принципів практично неможливо. Окрім цього, закон регламентує проведення інтерактивних опитувань під час телепередач, які пов'язані із виборами або проходять за участі кандидатів на різні посади. Демонструючи ці дані, журналісти мають наголошувати, що вони відображають думку не всього населення, а лише аудиторії певної програми.

Проте навіть при формальному дотриманні вимог законодавства у виборчому процесі соціологічні дані все рівно часто перетворюються на знаряддя політичної боротьби. Останніми роками для цього активно застосовуються соціальні мережі. Вони сприяють виникненню «фільтраційного сита», коли ми бачимо у власній стрічці Фейсбук або Інстаграм новини тільки від наших друзів. Внаслідок користувачі соцмереж опиняються в інформаційній бульбашці або «луна-камері». Людина починає сприймати лиш те, що відповідає її попереднім переконанням, є комфортним та зрозумілим для неї. Саме так народжуються спільноти «порохоботів», «зелеботів», антивакцинаторів, прихильників теорії змов, «всепропальщиків» тощо. За часів війни це стає вкрай небезпечним явищем, адже «луна-камера» є поживним середовищем для продукування та поширення російської дезінформації, відверто фейкових «рейтингів» та «опитувань».

Саме тому все більш актуальним питанням стає виявлення псевдосоціологів. Можна виділити такі критерії «заробітчан від соціології»: відсутність публічної інформації стосовно роботи у міжвиборчий період, раптова поява перед виборами та миттєве зникнення після завершення кампанії; приховані зв'язки керівників та спікерів організації із різними електоральними акторами; надмірні розбіжності між оприлюдненими опитуваннями, прогнозами та реальними результатами голосування; масова поява у багатьох ЗМІ близьких за формою, змістом та заголовками повідомлень, які істотно відрізняються від даних інших дослідницьких структур; відкритий або прихований піар певних партій чи кандидатів.

Загалом, в Україні працює не більше десятка загальнонаціональних соціологічних служб, які можуть організувати якісне та достовірне опитування громадської думки. Проте правдиві результати не завжди влаштовують полі-

тиків – комусь здається низьким власний рейтинг, а іншим не подобається висока підтримка конкурентів. Саме у такій ситуації і приходять на допомогу «псевдосоціологи», адже багато учасників виборів і досі щиро вважають, що люди можуть повірити фальшивим рейтингам та ухвалити рішення на користь їхньої політичної сили. У різні часи такими соціологічними махінаціями займалися практично всі українські партії та провідні політики. Автори порталу texty.org.ua створили базу «псевдосоціологів», до якої увійшли понад 70 установ та організацій.

За таких обставин актуальним стає питання соціологічної просвіти журналістів. Велику роботу у цьому напрямі веде фонд «Демократичні ініціативи» імені Ілька Кучеріва, який протягом останніх років видає тематичну літературу із детальним та популярним описанням методики і техніки підготовки, проведення та подання результатів соціологічних досліджень [2]. У 2019-2020 роках було проведено десять семінарів-тренінгів для журналістів у Харкові, Краматорську, Сєвєродонецьку, Одесі, Дніпрі, Львові, Вінниці, Чернігові, Івано-Франківську та Києві.

Таким чином, під час виборчих кампаній соціологічне знання втрачає свою самодостатню наукову цінність та перетворюється на засіб політичної маніпуляції. Фейкові рейтинги стають невід'ємною частиною політичної реклами. Все це значно підриває довіру до соціології як науки та дискредитує ідею вільної політичної конкуренції та відкритості медіа для всіх суб'єктів виборів. Попри все це, прагнення до високих стандартів соціології у медіа – це робота на майбутнє, яка сприятиме становленню громадянського суспільства та чесної журналістики та дасть свої результати вже на перших після нашої перемоги виборах.

Список використаних джерел:

1. Виборчий кодекс України. URL: https://zakon.rada.gov.ua/laws/show/396-20#Text (дата звернення 17.10.2022).
2. Опитування громадської думки: посібник для журналістів. Київ: Фонд «Демократичні ініціативи ім. Ілька Кучеріва», 2020. 110 с.
3. Паніна Н.В. Технологія соціологічних досліджень: Курс лекцій. 2-е видання, доповнене. Київ: Ін-т соціології НАН України, 2007. 320 с.

4. Стегній О.Г. Публічний простір достовірності соціологічного знання: case «електоральні дослідження». *Соціологія: теорія, методи, маркетинг.* 2020. №3. С. 13-32.

INFORMATION SECURITY IN CONSUMPTION ELECTORAL DATA

Abstract. *The report is devoted to the problem of objective presentation of the results of electoral research in the media. During election campaigns, these data become an instrument of influence on public opinion and political manipulation. Under such conditions, the task of the sociologist is to clearly distinguish between professional and socio-political roles, to adhere to legal and ethical standards, to promote the level of sociological culture of media representatives.*

Key words: *electoral research, pseudo-sociologists, echo chamber effect, sociological education.*

Отримано: 23.11.2022

УДК 316.61:32

Т. І. Мазур, *магістр з менеджменту організацій, викладач громадянської освіти Кам`янець-Подільського медичного фахового коледжу*

ВПЛИВ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА НА ПОЛІТИЧНУ СОЦІАЛІЗАЦІЮ ОСОБИСТОСТІ

Анотація. *В доповіді здійснено аналіз засад та проблемних аспектів політичної соціалізації та вплив інформаційного середовища на формування політичної та громадянської ідентичності особистості. Наведено основні наукові підходи до особливостей та специфіки процесу політичної соціалізації молоді в сучасних умовах розвитку українського інформаційного суспільства. Визначено теоретичне підґрунтя для характеристики основних передумов та принципів політичної соціалізації молоді в Україні. Приділено значну увагу критичному аналізу різних наукових поглядів щодо засобів та інструментів політичної соціалізації молоді, зокрема розглянуто роль Інтернету як сучасного засобу комунікацій для активного та прискореного включення молоді у політичне життя. Зроблено висновки про вплив інформаційного середовища на встановлення політичної соціалізації студентської молоді.*

Ключові слова: *соціалізація, сучасний інформаційний простір, медіа-соціалізація, медіа-середовище, інформаційна соціалізація, соціальні мережі, бібліотечна установа, інформаційна функція, інформаційне суспільство.*

Розкриття актуальних питань впливу Інтернет-середовища, ЗМІ на особистість, а саме на особистість в процесі політичної соціалізації.

Особливості процесу соціалізації в умовах інформаційного суспільства досліджували Г. Лактіонова, П. Плотніков, А. Рижанова, С. Савченко, Н. Гавриш, Н. Лавриченко, Р. Вайнола, Н. Заверіко, І. Звєрєва, Л. Міщик, В. Оржеховська, А. Капська та ін. Питаннями впливу нових медіа на соціалізацію людини займалися В. Абраменкова, М. Бутиріна, Я. Гошовський, Є. Кудашкіна, В. Мудрик, В. Плешаков, П. Винтерхофф-Шпурк, Р. Пацлаф та ін.

Метою доповіді є аналіз впливу інформаційного середовища на політичну соціалізацію особистості. З`ясування місця мережі Інтернет у процесі розвитку сучасного

суспільства, вивчення характеристик процесу політичної соціалізації у молоді.

Виклад основного матеріалу. Соціологи визначають соціалізацію як процес розвитку соціальної природи індивіда, що відбувається як у результаті стихійного впливу оточення, так і керованого впливу суспільства.

Соціалізація (від латин. socialis – суспільний) – це складний і тривалий процес включення індивіда до системи соціальних зв'язків і відносин, його активної взаємодії з оточенням, унаслідок якої він засвоює зразки поведінки, соціальні норми та цінності, необхідні для його успішної життєдіяльності у цьому суспільстві [1].

Стадії політичної соціалізації.

1. Стадія первинної соціалізації.
2. Стадія індивідуалізації.
3. Стадія інтеграції.

Політична соціалізація функціонує на таких рівнях:

1) соціальному – суспільний рівень у цілому, коли людина долучається до політики під дією проблем, з якими стикається все суспільство;
2) соціально-психологічному – характерна для малих груп через міжособистісне спілкування;
3) внутрішньо-особистісному – проходить через інтереси та потреби особистості, мотиви й ціннісні орієнтації.

Політичні цінності, традиції, зразки поведінки та інші елементи політичної культури засвоюються людиною безперервно, і цей процес може бути обмежений тільки тривалістю її життя.

Вікові етапи політичної соціалізації людини (за В. Муляром):

1-й етап (5-13 років) – потреба ідентифікації з кимось, формування перших політичних поглядів, зв'язок першого політичного досвіду з морально-політичною атмосферою в сім'ї;

2-й етап (13-18 років) – формування власного політичного «я», зростання ролі власного досвіду у формуванні політичної культури, сім'я не є єдиним фактором політичної соціалізації;

3-й етап (від 18 років) – одержання рівних політичних прав поряд з іншими, зростаюча роль власного досвіду у

формуванні політичної культури, набуття юридичних політичних прав.

Молодь – одна з великих соціально-демографічних груп суспільства, вона залишається однією з незахищених соціальних груп, на яку впливає чимало чинників. Вони водночас і визначають подальше позиціювання молоді до процесів і явищ суспільного розвитку.

Провідними сучасними засобами, завдяки яким відбувається соціалізація, є засоби масової комунікації. У сучасному світі вони володіють значною символічною владою, адже вони репрезентують циркулюючі в соціумі знання, норми, цінності, ідеали, образи тощо, які незалежно від того, адекватно вони відображають реальність чи нееквівалентні їй, завжди відтворюють домінанти та атрибути суспільного устрою, соціального порядку, культури, надаючи легітимності цивільним категоріям колективної та індивідуальної свідомості.

Як зазначають деякі науковці [8, с. 89], головним фактором Інтернету як агенту політичної соціалізації є принцип свободи: не тільки слова але і дії. Фактично, в Інтернеті у кожної молодої людини є свій власний профіль, а для деяких осіб і, власне, друге віртуальне життя, у якому в неї може бути власний сайт, блог, група тощо. «Четвертий вимір» XXI століття створюють соціальні мережі. Під даним поняттям розуміють певну структуру, яка базується на людських зв'язках чи взаємних інтересах. У якості інтернет-сервісу соціальна мережа може розглядатися як платформа, за допомогою якої люди можуть здійснювати зв'язок між собою та об'єднуватись за своїми специфічними інтересами. Завдання такого сайту полягає у тому, щоб забезпечити користувачів всіма можливими шляхами для взаємодії один з одним (відео-чати, зображення, музика, блоги). Особливо важливими для політичної соціалізації тематичні соціальні мережі, які можуть за допомогою спілкування передавати певний соціальний досвід чи норми і цінності певної спільноти [8, с. 110-111].

Також існують два види політичної соціалізації у молоді на які впливають Інтернет- середовище та засоби масової інформації (ЗМІ): індивідуальний рівень – формування політичного «Я», яке сприяє політичному самовираженню особистості.

Вплив ЗМІ не можуть забезпечити систематичне і глибоке засвоєння політичних знань. Це завдання спеціальних освітніх установ. Та все-таки мас-медіа, супроводжуючи людину протягом усього життя, у тому числі й після завершення навчання, значною мірою впливають на сприйняття нею політичної та соціальної інформації. При цьому під виглядом політичної освіти в людей можуть формуватися й псевдораціональні структури свідомості, що спотворюють реальність під час її сприйняття.

Освітня роль ЗМІ тісно пов'язана з їхньою функцією соціалізації й, по суті, переростає в неї. Проте якщо політична освіта передбачає систематичне набуття знань і розширює пізнавальні й оцінювальні можливості особи, то політична соціалізація означає інтерналізацію, засвоєння людиною політичних норм, цінностей і зразків поведінки.

У демократичному суспільстві найважливіше політико-соціалізаційне завдання ЗМІ полягає в масовому впровадженні заснованих на пошані закону і прав людини цінностей, навчанні громадян мирно розв'язувати конфлікти, не ставлячи під сумнів суспільний консенсус із засадничих питань державного устрою. Проте важливо в цьому контексті враховувати і вплив основних тенденцій розвитку самих ЗМІ. Тому в процесі політичної соціалізації завдяки ЗМІ, заангажованим власниками, молоді люди часто підпадають під їхні маніпуляційні можливості, що не є безпечним для свідомого та об'єктивного сприйняття інформації.

У постіндустріальному суспільстві ЗМІ набувають визначальної ролі в управлінні суспільством – саме мас-медіа є безпосередніми носіями та розповсюджувачами знання і політично значимої інформації. Масові комунікації стали невід'ємною складовою сучасної політичної системи суспільства, яка використовує спеціальні засоби інформаційного обміну для встановлення та підтримки постійних зв'язків як на рівні індивідів, так і суспільства в цілому.

Соціологічні підходи до вивчення масової комунікації дозволяють сформулювати таке її визначення: це інституціоналізований, соціально обумовлений макропроцес виробництва, розповсюдження інформації та обміну нею, який реалізується за допомогою особливих технологій і засобів (технічно обладнаних мас-медіа). У той час, коли термін "масова комунікація" вказує на процес чи стан со-

ціальної взаємодії, засоби масової комунікації є соціальним інститутом, який регулює цей процес. Преса, радіо, телебачення, а також Інтернет сприймаються як найадекватніший спосіб існування масової комунікації.

У зв'язку з цим розширюється коло впливу та перелік функцій, виконуваних ЗМІ. Взаємодіючи на основі прямих і зворотних зв'язків з аудиторією, соціальними інститутами, ЗМІ вирішують ряд завдань, що сприяють діяльності цих інститутів, включенню в суспільні процеси аудиторії. Це визначає суспільне призначення, функції ЗМІ в суспільстві.

Медіакультура особистості як комплекс настановлень щодо характеру інформаційного продукту, отримуваного від мас-медіа, як систему інформаційних потреб, орієнтацій, знань, умінь, навичок користування засобами мас-медіа та інших соціальних характеристик особистості, сформованих і розвинених у процесі політичної соціалізації.

Використання ЗМІ агресивних технологій і поширення негативної інформації зменшує рівень довіри до них і призводить до зниження виборчої активності. Поширення Інтернету та його українського сегмента, де відносно високий рівень свободи слова і обмежений адміністративний контроль з боку влади, а також життєва необхідність для студентства оволодіння комп'ютерними технологіями стимулюватимуть роль інформаційних систем щодо можливості впливу на електоральну поведінку студентської молоді.

Поява багатопартійності в перехідний період становлення незалежної України зумовила, з одного боку, певний прогрес у розвитку ЗМІ, бо нові партії створювали власні друковані видання та прагнули отримати доступ до ефірного часу на телебаченні. Протягом останнього десятиріччя в українських ЗМІ відбувалася дедалі більша диференціація на офіціозні й неофіціозні.

Проте, незважаючи на ці проблеми, гадаємо, що загальні процеси розвитку глобального інформаційного простору й медіакультури, зокрема тенденція до справжньої демократизації та створення громадянського суспільства з властивою йому альтернативною формою політичної комунікації, дедалі більше впливатимуть на процес політичної соціалізації молодого покоління, особливо з огляду на входження України до європейської та світової спіль-

нот. Тож інформаційний сектор стає потужним засобом забезпечення реальної демократії та запобігання загрозам чи небезпеці типу диктаторських, монополістичних чи олігархічних аномалій. Цей чинник передбачає певний ступінь виключення загроз і небезпеки для громадян у процесі їх інформування.

Із сказаного можна зробити висновки, що ЗМІ:

- у процесі політичної соціалізації молоді сприяють забезпеченню стабільного соціального консенсусу;
- здійснюють інформаційний зв'язок між політичною системою та навколишнім середовищем і є важливим чинником у процесі політичної соціалізації молоді та її електоральної поведінки;
- виступають як один із інструментів управління суспільством в інтересах економічних, а також політичних відносинах соціальних прошарків і груп. Оптимізують медіа-вплив і каталізують формування певної моделі суспільної думки;
- виконують роль контролюючої противаги.

Отже, політична соціалізація постає як сукупність процесів становлення політичної культури, свідомості та поведінки особистості, прояву політичної активності, залучення індивіда до цінностей, знань, рольових зразків, які дозволяють адаптуватися до політичного життя суспільства. Зміст політичної соціалізації складають процеси інтеріоризації (внутрішнього прийняття) вимог соціально-політичної системи суспільства у внутрішню структуру особистості (політичні потреби, установки, цінності, норми), та екстеріоризації (зворотний процес) – перетворення політичного досвіду особистості в політичну дію, поведінку, реалізації його в статусно-рольових моделях поведінки в даному політичному просторі.

Список використаних джерел:

1. Загальна соціологія: навч. посіб. Київ: Професіонал, 2004. 592 с.
2. Ліфарєва Н.В. Психологія особистості: навч. посіб. для студ. вищ. навч. закл. Київ, 2003. 237 с.
3. Юрій Н.М. Політична соціалізація молоді в умовах трансформації суспільства: порівняльний аналіз міжнародного і українського досвіду: автореф. дис.... канд. політ. наук: 23.00.04. Одеса, 2002. 16 с.

4. Бебик В.М., Головатий М.Ф., Ребкало В.А. Політична культура сучасної молоді. Київ, 1996. С. 41-65.
5. Волинський А. Стадії політичного процесу. *Політичний менеджмент.* 2004. №1 (4). С. 41-52.
6. Загородній Ю.І., Куріло В.С., Савченко С.В. Політична соціалізація студентської молоді в Україні: досвід, тенденції, проблеми. Київ: Генеза, 2004. С. 21-27.
7. Пащенко В. Моделі нормативного обґрунтування «громадянськості». *Політичний менеджмент.* 2004. №3. С. 58-70.
8. Данько Ю.А. Соціальні мережі як форма сучасної комунікації: плюси і мінуси. *Сучасне суспільство: політичні науки, соціальні науки, культурологічні науки.* 2012. С. 179-184.

THE INFLUENCE OF THE INFORMATION ENVIRONMENT ON THE POLITICAL SOCIALIZATION OF THE INDIVIDUAL

Abstract. *The report analyzes the principles and problematic aspects of political socialization and the influence of the information environment on the formation of political and civic identity of the individual. The main scientific approaches to the peculiarities and specifics of the process of political socialization of youth in the modern conditions of development of the Ukrainian information society are presented. The theoretical basis for characterizing the basic prerequisites and principles of political socialization of youth in Ukraine is determined. Considerable attention is paid to the critical analysis of various scientific views on the means and tools of political socialization of youth, in particular, the role of the Internet as a modern means of communication for the active and accelerated inclusion of young people in political life. Conclusions about the influence of the information environment on the establishment of political socialization of student youth are made.*

Key words: *socialization, modern information space, media socialization, media environment, information socialization, social networks, library institution, information function, information society.*

Отримано: 17.11.2022

УДК 342.951

Т. В. Грубі, *кандидат соціологічних наук,*
доцент кафедри психології, педагогіки
та соціально-економічних дисциплін
Національної академії Державної прикордонної
служби України імені Богдана Хмельницького

СВІТОВІ ТА ВІТЧИЗНЯНІ ПРАКТИКИ В СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ СУЧАСНОСТІ

Анотація. *У дослідженні презентовано досвід європейських держав, США та України в системі заходів забезпечення інформаційної безпеки загалом і кібербезпеки, зокрема як потужного засобу посилення національної безпеки і надійності інформаційних систем. Розкрито ключові засади національних стратегій кібербезпеки, виявлено проблеми, що потребують подальшого вирішення.*

Ключові слова: *інформація, інформаційна безпека, кібербезпека, кібератаки.*

Національна безпека у сучасному світі значною мірою залежить від забезпечення інформаційної безпеки і як показує практика, з розвитком технічного прогресу ця залежність лише зростатиме. Найчастіше інформаційну безпеку визначають як наявність захисту інформації та потрібної для її підтримки інфраструктури від випадкових чи цілеспрямованих впливів природного або штучного походження, які можуть заподіяти неприйнятну шкоду суб'єктам інформаційних відносин, серед іншого власникам і користувачам інформації та згаданій вище її підтримуючій інфраструктурі [1, с. 67]. Сучасна геополітична ситуація та військова агресія Росії щодо України активізували питання належного забезпечення інформаційної безпеки. Адже сьогодні наша держава потерпає від систематичних атак на критичну інфраструктуру шляхом вимкнення електростанцій, руйнування нафтопроводів, навіть припинення постачання води та опалення комунальних підприємств, тощо. Усі ми розуміємо, що саме ці обставини в значній мірі можуть підірвати основи національної безпеки України. Саме тому, сьогодні кіберпростір розглядається як надзвичайно важливий безпековий імператив, оскільки від його реалізації залежать соціальна, економічна, військова та інші сфери безпеки держави.

Останніми десятиліттями інформаційний аспект розвитку суспільства був об'єктом досліджень як зарубіжних, так і вітчизняних науковців. Зокрема, основні аспекти інформаційного суспільства висвітлено в класичних працях західних дослідників Д. Белла, Н. Вінера, М. Кастельса і Д. Тапскота та ін., Г. Хакена та інші. Глобальні проблеми інформаційного розвитку розглядались у роботах вітчизняних дослідників, таких як О. Панарін, Г. Почепцов, С. Луценко, С. Чукут та ін. Особливостям забезпечення національної безпеки присвятили свої праці О. Валевська, О. Власюк, В. Голобуцький, В. Горбулін, А. Гуз, О. Данільян, С. Луценко, Є. Макаренко, О. Сенченко, В. Степанов та ін.

Однією з важливих характеристик інформаційної безпеки суспільства і держави є ступінь їх захищеності, тобто фактично стійкість усіх головних сфер життєдіяльності (як-то економіка, наука, технології, державне управління тощо) до всіх небезпечних, зокрема дестабілізуючих і деструктивних інформаційних впливів, що зачіпають інтереси країни, незалежно від того, здійснюються вони у вигляді впровадження (підкидання) чи навпаки, вилучення інформації. На нашу думку, інформаційна безпека в цьому випадку визначальним чином зумовлюється спроможністю убезпечити державу і суспільство від цих впливів, зокрема нейтралізувати їх. Усвідомлюючи останнє, більшість держав світу почали здійснювати внутрішньодержавні комплексні заходи з безпеки в кіберпросторі. Вони пов'язані з розробкою і вдосконаленням національного законодавства в даній галузі і створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі. Адже державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави. Стратегії з кібербезпеки були прийняті такими державами як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Список країн наочно показує, що дана проблема визнається актуальною в усьому світі. Не залишилась осторонь цих процесів і Україна, яка 6 березня 2016 р. схвалила Стратегію кібербезпеки України. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

Базисним напрямком такої політики є розробка заходів, спрямованих на впровадження культури кібербезпеки. Остання повинна посилювати розвиток безпеки інформаційних систем та мереж, а також формувати нові способи мислення та поведінки під час використання інформаційних систем, а також під час спілкування або транзакцій через мережі. Ряд країн уже адаптували власне законодавство до означених вимог. Так, в межах Стратегії кібербезпеки Німеччини передбачено оперативне співробітництва між усіма державними установами й поліпшення координації заходів із захисту інформації, протидії кібератакам, Національний центр кіберзахисту. Така Єдина система дозволяє здійснювати моніторинг та блокувати спроби реалізації кібератак, розслідувати комп'ютерні злочини, здійснювати міжнародну взаємодію з питань протидії кіберзагрозам [2, с. 29-30]. Аналогічною є Національна Стратегії кібербезпеки у Великій Британії, що була розроблена ще у 2011 році. Загалом практично у всіх європейських державах існують подібні документи. Має місце і уніфікація законодавства в межах Євросоюзу. Так, у 2001 р. Комісією ЄС було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід». У наступні роки органами ЄС було прийнято велику кількість нормативно-правових документів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах-членів ЄС. Серед них: рамкове рішення Ради ЄС 2005/222/JHA щодо нападу на інформаційні системи від 24 лютого 2005 р.; повідомлення Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» 2007 р., в якому даються визначення терміну «кіберзлочинність» та основні напрями політики ЄС щодо інформаційної безпеки; Стратегія кібербезпеки ЄС «Відкритий, надійний та безпечний кіберпростір» 2013 р., яка рекомендує державам-членам ЄС розвивати міждержавне співробітництво у протидії кіберзагрозам; Директива Європейського парламенту і Ради ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі 2016 р. та інші [3, с. 286-287].

Країною-лідером забезпечення інформаційної безпеки залишаються США. Остання редакція американської націо-

нальної інформаційної стратегії відбулася у березні 2018 р. У ній відповідальність за забезпечення критичної інфраструктури нації та управління ризиками кібербезпеки розподіляється між приватним сектором та Федеральним Урядом. У документі, визначено пріоритетність діяльності по зменшенню ризиків у семи ключових сферах: національна безпека (інформаційна безпека у т.ч.) енергетика та потужності, банківська справа і фінанси, охорона здоров'я і безпека, зв'язок, інформаційні технології та транспорт.

Україна не залишається осторонь цих процесів і також активно формує державну політику захисту інформаційної безпеки загалом і кібербезпеки, зокрема. Так, 6 грудня 2017 р. КМ України була схвалена Концепція створення державної системи захисту критичної інфраструктури [4, с. 41]. У документі визначаються основні напрямки, механізми і строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління в цій сфер. Завдання практичної реалізації даної політики визначено Законом України «Про національну безпеку України» 2018 р.

З метою посилення стійкості критичної національної інфраструктури з кібербезпеки Україна регулярно бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів реагування на них. Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС та НАТО посилюють спроможності нашої держави у сфері кібербезпеки і відповідають національним інтересам. У рамках взаємодії з міжнародними організаціями з питань реагування на кіберінциденти було організовано участь України у Форумі команд реагування на інциденти інформаційної безпеки FIRST (Forum for Incident Response and Security Teams), що об'єднує різні групи CERT (Computer Emergency Response Team – Команда реагування на надзвичайні ситуації) у країнах Європи [5, с. 155].

Серед викликів, що сьогодні існують перед світовою спільнотою в контексті посилення інформаційної безпеки, вважаємо необхідним посилення кібербезпеки виборчих

систем та критичної інфраструктури, сприяти реалізації Стратегій кібербезпеки, розробка більш ефективних заходів реагування на кіберінциденти. Доцільно також докладати більше зусиль для встановлення державно-приватного партнерства, розробки та запровадження механізмів обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі. Задля своєчасного реагування на кіберінциденти і здійснення практичних заходів зі зміцнення володіння ситуацією у кіберпросторі важливо організовувати проведення тренінгів з підготовки висококваліфікованих фахівців у галузі кібербезпеки та цифрової криміналістики із залученням міжнародних фахівців. Критично важливі інфраструктурні компанії мають дотримуватись принципу «безпека понад усе». Оскільки понад 90% усіх несанкціонованих доступів, уражень і атак відбувається через людський фактор, то на підприємствах потрібно ввести прості регламентні норми, щоб максимально мінімізувати можливі витоки загроз і уражень [5, с. 155].

Підкреслимо, що проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства.

Список використаних джерел:

1. Торічний В.О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект: монографія. Харків: НУЦЗУ, 2020. 274 с.
2. Чічановский А.А., Старіш О.Г. Інформаційні процеси в структурі світових комунікаційних систем: підручник. Київ: Грамота, 2010. 568 с.
3. Войціховський А. Інформаційна безпека як складова системи національної безпеки(міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна.* Серія «ПРАВО». Вип. 29. С. 281-288.
4. Бєлай С.В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика. Харків: Національна акад. НГУ, 2015. 349 с.
5. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації.* 2019. Т. 21. №3. С. 150-157.

WORLD AND NATIONAL PRACTICES IN THE FIELD OF CYBERSECURITY: CHALLENGES OF OUR TIME

Abstract. *The study presents the experience of European countries, the USA and Ukraine in the system of measures to ensure information security in general and cybersecurity, in particular, as a powerful means of strengthening national security and reliability of information systems. The key principles of national cybersecurity strategies are revealed, problems that need further solution are identified.*

Key words: *information, information security, cybersecurity, cyberattacks.*

Отримано: 24.11.2022

УДК 316.3

М. П. Плахтій, *кандидат філософських наук, доцент кафедри політології та філософії Кам'янець-Подільського національного університету імені Івана Огієнка,*

Т. В. Сулятицька, *кандидат філософських наук, доцент кафедри політології та філософії Кам'янець-Подільського національного університету імені Івана Огієнка*

ІНФОРМАЦІОНАЛЬНО-КОМУНІКАТИВНИЙ СПОСІБ РОЗВИТКУ СУЧАСНОГО СУСПІЛЬСТВА

Анотація. *У статті здійснено аналіз існуючих підходів до визначення сучасного суспільства, яке прийнято називати «інформаційним». Наголошено на соціокультурному змісті інформатизації та комунікації, які трансформують фундаментальні виміри людського життя, інформація та знання стають системоутворюючим фактом розвитку суспільства нового типу.*

Ключові слова: *інформатизація, інформація, знання, комунікація, розвиток.*

Одним із викликів сучасної цивілізації є інформатизація. Перехід від використання традиційних методів зберігання, пошуку та поширення інформації (бібліотек, ручних методів пошуку й аналізу, пошти, телеграфу) до нових безпаперових (автоматизованих робочих місць, баз даних, комп'ютерних мереж, інформаційно-пошукових систем, супутниковому зв'язку, систем обробки текстів,) приведе до кращої орієнтації в міжнародних подіях, явищах, економічних процесах, торговельних операціях, нових технічних рішеннях, при можливості бути одночасно у декількох місцях, спілкуватися он-лайн з представниками різних континентів, бути студентом кількох вузів (закордонних), постійно перебувати у величезному коловороті інформації й безпосередньо, виступати творцем інформації. Усі ці процеси активно впливають на людину, на розвиток її як особистості, на взаємовідносини між людьми, країнами. Суспільство, яке набуває вище перерахованих ознак, прийнято називати «інформаційне».

Інформатизація суспільства є однією із закономірностей сучасного суспільного процесу. Однак, не слід отото-

жнювати її із схожим поняттям «комп'ютеризація суспільства». Хоча вони виникають приблизно в один час, внаслідок розвитку науково-технічних інновацій, пов'язаних з появою та розвитком комп'ютерних мереж, все ж таки між ними мають місце певні відмінності.

Під час комп'ютеризації суспільства основна увага приділяється розвитку і впровадженню технічної бази комп'ютерів, що забезпечують оперативне отримання результатів переробки інформації та її накопичення.

В процесі інформатизації основна увага суспільства приділяється комплексу заходів, направлених на забезпечення повного використання достовірного, вичерпного і своєчасного знання усіх видів людської діяльності.

В сучасному суспільстві вище згадуваний процес комп'ютеризації надає людям доступ до надійних джерел інформації, позбавляє їх від рутинної роботи, забезпечує високий рівень автоматизації обробки інформації у виробничій та соціальній сферах.

Рушійною силою інформаційного суспільства стало виробництво інформаційного, а не матеріального продукту. Матеріальний продукт став більш інформаційномістким, що означає збільшення частки інновацій, дизайну й маркетингу в його вартості.

Зміст інформатизації полягає в забезпеченні економічних, соціальних, правових, культурних і технологічних умов накопичення, збереження й активізації нових ідей, створення можливостей кожній людині зафіксувати свої ідеї, зробивши їх доступними широким масам, а також створення умов для їхнього використання.

Але поряд з позитивними моментами процесу інформатизації створюється й реальна загроза використання досягнень в інформаційній сфері, з метою несумісних із завданнями підтримки світової стабільності й безпеки, дотриманням принципів суверенної рівності держав, мирного врегулювання конфліктів, незастосування сили, невтручання у внутрішні справи, поваги прав і свобод людини. З огляду на швидкість розвитку даної області, варто визнати, що в правовому, організаційному й технологічному відношенні інформаційна сфера є найменш захищеним елементом державного механізму. Недостатня увага до проблем інформатизації може поставити країни з

менш розвиненим рівнем інформаційних технологій (Індія, Єгипет, Нігерія) у свідомо залежне положення від країн, які мають переваги в інформаційній сфері (Японія, США, Франція, Англія, Росія, Україна).

Вивчення тенденцій глобальних змін у суспільстві, зумовлених інформатизацією з залученням інформації і фактичного матеріалу про періодизацію технологічних укладів має багаті традиції у рамках концепцій постіндустріалізму. Загалом наукова концептуалізація процесів інформатизації почала відбуватись відносно недавно – з початку 80-х рр. XX ст., що обумовлено виникненням мереж кіберкомунікації, формування на їх основі глобального простору економічної та культурної взаємодії [1, с. 12]. Серед авторів, що займаються цими питаннями слід назвати Д. Белла, З. Бжезинського, П. Дракера, Д. Рісмена, Г. Кана, Р. Катца, М. Кастельса, М. Маклюена, Й. Масуда, М. Пората, Е. Тоффлера та інших. Дослідження проблеми формування інформаційного суспільства на теренах України та СНД репрезентовані роботами Р. Авдєєва, Н. Васильєвої, В. Вітковського, Б. Головко, С. Дятлова, Л. Земляновой, В. Іноземцева, О. Назарчука та багатьох інших науковців.

Розглянути дослідження всіх перерахованих вище авторів представляється практично неможливим у межах даної роботи, зупинимося лише на деяких з них, необхідних для того, щоб показати особливості міжкомунікаційної взаємодії в такому суспільстві.

За Д. Беллом [2], постіндустріальне суспільство визначається як суспільство, в економіці якого пріоритет перейшов від переважного виробництва товарів до виробництва послуг, проведення досліджень, організації системи освіти й підвищення якості життя. Знання та інформацію, американський вчений вважає не тільки ефективним каталізатором інформації постіндустріального суспільства, але і його стратегічним ресурсом.

Заслуговує на увагу філософська концепція інформаційного суспільства, яка належить японському вченому Й. Масуда. Основні принципи побудови такого суспільства представлені в його книзі «Інформаційне суспільство як постіндустріальне суспільство» [3]. На думку автора, фундаментом нового суспільства стане комп'ютерна технологія, головна функція якої бачиться ним у заміщенні або в

значному посиленні розумової праці людини. Сучасна епоха, як зазначає П. Дракер, являє собою час радикальної перебудови, коли з розвитком нових інформаційно-телекомунікаційних технологій людство отримало реальний шанс перетворити капіталістичне суспільство в суспільство, засноване на знаннях.

На особливо увагу заслуговує монографічне дослідження М. Кастельса, що виокремлюється різноманітністю і переконливістю доказів, за допомогою яких автор наполегливо, але не нав'язливо, збалансовано та гнучко намагається зацікавити читачів актуальністю виявлених ним найновіших тенденцій в суспільному житті світу, їх складністю, суперечністю і в перспективі неоднозначними результатами для долі людської цивілізації [4, с. 58].

На думку М. Кастельса, в сучасних умовах інформація стає системоутворюючим фактором розвитку суспільства нового типу – «інформаціонального», «мережевого», суспільства, в якому комунікативні процеси відбуваються безупинно, вони слугують основою, простором, в якому живе і яким живе людина, котра будь-якої миті творить. Комунікаційна взаємодія стає сутністю цього суспільства.

Теорія мережевого суспільства (theory of network society) Мануеля Кастельса, що виникла у 90-х рр. минулого століття фіксує новий тип суспільства, яке створюється потоками інформації. Нове суспільство – це мережа взаємин, нічим не обмежена, відкрита та рухлива. Мережеве суспільство – це безшовна мережа взаємин, що розширюється або звужується завдяки інформації та комунікації. Ключовою характеристикою інформаціонального суспільства є мережева логіка організації соціальної структури. Автор фундаментальної «теорії мереж» – Кастельс називає соціальну структуру інформаційної епохи мережевим суспільством, оскільки воно створене мережами виробництва, влади і досвіду, які утворюють культуру віртуальності в глобальних потоках, що пересікають час та простір [5, с. 505]. Сутність такого суспільства полягає у функціонуванні соціальної структури на основі мережі інформаційних технологій, які зв'язують багатоманітних акторів певних сегментів суспільної діяльності, насамперед економічної. Домінуючими стають процеси та функції, які організовуються за принципом мережі. Внаслідок розвитку ко-

мунікаційних мереж суспільство стає схожим на павутиння інформаційних зв'язків та взаємодій, його функціонування подібне до процесів, які відбуваються у мережі.

В інформаційних виданнях набув поширення такий термін, як «кіберпростір», який використовується для позначення всіх аспектів роботи людини з комп'ютером та Інтернетом. Цей термін досить часто відображає можливість сприйняття комп'ютерів та їхніх мереж як особливого психологічного "простору". Людям, які активно працюють із комп'ютерами, пишуть електронні листи, грають в ігри, спілкуються одночасно з людьми на різних континентах, важко не уявляти все це як особливий "простір", в який вони потрапляють за допомогою свого комп'ютера та мережі. Творці інтерактивних сервісів вносять свою частку у створенні цього образу, називаючи окремі частини власної продукції «світами», «кімнатами» і «територіями».

П. Тейяр де Шарден у свій час помітив, що «… ноосфера прагне стати однією замкнутою системою, де кожний елемент окремо бачить, почуває, бажає, страждає так само, як усі інші, й одночасно з ними» [6, с. 192]. А це означає, що, перебуваючи у мережі, навіть сидячи в себе дома, ми постійно включені в простір де перебуває ще хтось, і цей хтось теж зі своїми ідеями, проблемами є цікавим іншому, третьому, четвертому та ін., тобто всі учасники створюють середовище, в якому незнайомі люди можуть радитись, співчувати за власним вольовим бажанням без нав'язування.

Створюючи нові умови життєдіяльності соціуму, нова реальність впливає не тільки на його організаційні, комунікаційні особливості, але й на характер суспільних відносин, які стають більш стрімкими, медіа насиченими, розмаїтими та інтенсивними, породжуючи нові соціально-психологічні феномени: інформаційні фобії, інформаційні навантаження, агресію та інформаційні злочини. У XXI ст. інформація зайняла провідне місце у суспільному житті: науці, політиці, освіті, буденних справах. У буденному розуміння інформація та знання завжди супроводжували людську діяльність, але тільки з появою глобальної інфраструктури і набуттям ознак предметності в системі соціальних комунікацій спеціальний інтерес до них різко зростає. Зростання потреб суспільства, накопичення документально-фіксо-

ваної інформації, формування мета текстового простору інформаційних систем, необхідність переробки інформації та включення її до системи соціальних комунікацій, все це зумовило розвиток інтелектуального компонента суспільної діяльності. Адже інформаційно-аналітична діяльність невід'ємно пов'язана з процесом інтелектуалізації суспільного життя і займає вищий щабель у ієрархії інформаційно-комунікаційних відносин у суспільстві.

Однією з ознак інформаціонального суспільства стане забезпечення вільного своєчасного доступу населення до регіонального, державного і світовому інформаційному фонду, формування потреби і свідомості необхідності його використання в процесі своєї діяльності у кожного члена суспільства.

Однак, поряд з позитивними моментами необхідно звернути увагу і на деякі ризики та небезпечні тенденції. По-перше, збільшиться вплив на суспільство засобів масової інформації, воно стане залежним від них, що створюватиме умови для маніпуляції свідомістю людей. По-друге, з'явиться проблема відбору якісної і достовірної інформації, що визначатиметься, передусім рівнем ціннісних преференцій індивіда. По-третє, інформаційні технології можуть зруйнувати приватне життя людей. Багатьом людям буде важко адаптуватися до середовища інформаціонального суспільства. Існує небезпека розриву між «інформаційною елітою» (людьми, що займаються розробкою інформаційних технологій) і споживачами.

Схарактеризуємо інформаціональне суспільство, з точки зору комунікативної взаємодії, які переваги і можливості воно створює.

По-перше, кожен член суспільства має можливість вчасно й оперативно одержувати за допомогою глобальних інформаційних мереж повну й достовірну інформацію будь-якого виду й призначення з будь-якої держави, перебуваючи при цьому практично в будь-якій частині географічного простору. Інформація стає головною цінністю, яка активно впливає як на функціонування суспільства, так і на процес соціалізації особистості, яка повинна мати необхідні знання про інформаційну сферу, розуміти закони її функціонування та розвитку, бути мобільною у світі сучасної інформації. Змінюється не лише життя людини, посту-

пових змін зазнає і вона сама, оскільки на планеті поступово зникають просторові та часові розмежування, стираються міждержавні кордони, пропагуються певні цінності, моделі поведінки та світоглядні стереотипи.

Інформація завдяки своїм особливостям висувається на пріоритетне місце як ресурс стійкого розвитку, а інформатизація формує новий образ майбутнього, де головним засобом рішення глобальних проблем стане інтелект людини і всього людства. З одного боку інформація формує матеріальне середовище життя людини, виступаючи в ролі інноваційних технологій, комп'ютерних програм, телекомунікаційних протоколів і таке інше, а з іншого, служить основним засобом міжособистісних взаємин, постійно виникаючи, видозмінюючись і трансформуючись в процесі переходу від однієї людини до іншої. У такий спосіб інформація означає і соціокультурне життя людини і його матеріальне буття [7, с. 72].

По-друге, реалізується можливість оперативної, практично миттєвої комунікації кожного члена суспільства з державними та суспільними структурами поза залежністю від місця проживання на земній кулі. Тобто, комунікація сьогодні пронизує всі сфери людського життя. Ми живемо в світі комунікації. 70% свого часу людина витрачає саме на комунікацію. Без ефективного ведення зв'язку зупинилося б чимало виробничих процесів. Саме комунікація забезпечує існування соціальної пам'яті, зберігання й передачу інформації – в межах одного покоління, а також від однієї генерації до іншої.

По-третє, трансформується діяльність засобів масової інформації (ЗМІ) по формах створення та поширення інформації, розвивається й інтегрується з інформаційними мережами цифрове телебачення. Формується нове середовище – мультимедія, у якій поширюється також інформація із традиційних ЗМІ. Нова епоха створює нову глобальну медіасферу, яка є гарантом успішного впровадження у всі сфери сучасного життя та стимулюючим фактором від економіки до культури, політики та науки швидкісних електронно-технічних засобів зв'язку та інформації, які суттєво перетворюють звичні форми життєдіяльності, скеровуючи їх від споживчого індустріального суспільства до інформаціонального суспільства знань.

По-четверте, зникають географічні й геополітичні кордони держав у рамках інформаційних мереж; світ з кожним роком стає дедалі тіснішим та взаємозалежнішим. Поступово стираються кордони між державами. Люди стали більш мобільними, менш чутливими до національних стереотипів, толерантнішими. Вони не бажають обмежувати себе жодними рамками: ані територіальними, ані мовними чи релігійними. В умовах глобалізації значна частина населення планети виявилась включеною в нову інформаційну реальність, яка характеризується суттєвим розширенням доступу до різноманітних джерел інформації. Ми отримали можливість звертатись до подій у режимі реального часу, ставати їх співучасниками.

По-п'яте, у суспільстві виробляється, функціонує й доступна будь-якому індивідові, групі або організації сучасна інформаційна технологія. Сучасні інформаційні технології дозволяють контрольовано встановлювати інформаційні відносини та впливати на інформаційним простір. Інтернет суттєво змінив методи доступу до інформації та її поширення. Ця мережа, порівняно з іншими ЗМІ передбачає значно ширші можливості щодо реалізації права особи на вільне збирання, зберігання, використання й поширення інформації. Будь-який процес розвитку і діяльності в сучасному суспільстві пов'язаний з передачею, використанням і опрацюванням інформації. Інформаційно-комунікативні технології, поступово активно інтегруються в усі сфери діяльності людини, суспільства, стають могутнім каталізатором і визначальним джерелом їх активного розвитку. Свобода комунікацій в мережі Інтернет, породжує ілюзію здійснення на новій технологічній основі ідеалів свободи, рівності і братерства.

По-шосте, відбувається процес прискореної автоматизації й роботизації всіх сфер і галузей виробництва й керування. Автоматизовані інформаційні системи і нові технології дають можливість у десятки і сотні раз збільшити швидкість і якість оброблення управлінської інформації при мінімальних затратах людських ресурсів. Серед вже втілених прикладів можна назвати заміну громіздкого паперового документообігу на багатофункціональний і оперативний електронний документообіг.

Отже, сучасне людство постало на порозі епохальних трансформацій, основними напрямками яких є інтенсивний розвиток інформаційно-технологічного сектору та інформатизація всієї системи суспільних відносин. Соціокультурний зміст інформатизації полягає у тому, що нові інформаційно-телекомунікаційні технології докорінно змінюють систему соціокультурного співіснування, через формування мережевих суспільних комунікацій, налагодження зворотних зв'язків між інститутами суспільства і державами та встановлення системи вільного доступу до суспільно-важливої та особисто корисної інформації. Саме завдяки сучасним технологіям уможливлюється і набуває обертів міжкультурний обмін, який веде до міжкультурної взаємодії, що в подальшому при спілкуванні з іншими культурами, потраплянні в їх простір, веде до збагачення власної культури.

Формування інформаціонального суспільства, як бачимо, породжує цілий комплекс проблем, від вирішення яких залежить вибір і реалізація шляху розвитку людства. І зауважимо, що якщо на початковому етапі інформатизації основну роль відіграють науково-технічні і технологічні проблеми, то на подальших етапах головну роль починають грати соціальні проблеми вирішення яких і визначить результат інформатизації.

Таким чином, формування такого суспільства повинно бути спрямовано на підвищення ефективності використання потенціалу країни, на реалізацію механізмів розвитку цивілізації в цілому, і бути орієнтовано на задоволення інформаційних потреб всіх членів суспільства.

Список використаних джерел:

1. Юнг К.Г. Различие между восточным и западным мышлением. Сознание и бессознательное. Санкт-Петербург. Москва, 1997. 544 с.
2. Белл Д. Прихід постіндустріального суспільства Сучасна зарубіжна соціальна філософія. Київ: Либідь, 1996. 251 с.
3. Masuda Y. The Information Society as Post-Industrial Society, Washington, D.C., USA: World Future Society, 1981, P. 6.
4. Землянова Л.М. Сетевое общество, информационализм и виртуальная культура. *Вестник Московского университета*, Серия 10, «Журналистика» №2, 1999. С. 58-69.

5. Кастельс М. Информационная эпоха: экономика, общество, культура / пер. с англ. под научн. ред. О.И. Шкаратона. Масква: Гос. ун-т. Высш. шк. экономики, 2000. 606 с.
6. Тейяр де Шарден П. Феномен человека. Преджизнь, жизнь, мысль, сверхжизнь. Москва: Наука, 1987. 240 с.
7. Зощенко О.В. Інформаційне суспільство: ознаки й динаміка. *Інтелект. Особливість. Цивілізація.* Тематичний збірник наукових праць із соціально-філософських проблем. Донецьк: ДонДУЕТ, 2004. №3. С. 72.

INFORMATIONAL AND COMMUNICATIVE METHOD OF DEVELOPMENT OF MODERN SOCIETY

Abstract. *The article analyzes the existing approaches to the definition of modern society, which is commonly called «information society». Emphasis is placed on the socio-cultural content of informatization and communication, which transform the fundamental dimensions of human life, information and knowledge become a system-forming fact of the development of a new type of society.*

Key words: *informatization, information, knowledge, communication, development.*

Отримано: 17.11.2022

УДК 342.4:351.86]:004.056.5

А. В. Найчук, *кандидат філософських наук, доцент кафедри політології та філософії Кам'янець-Подільського національного університету імені Івана Огієнка*

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВ

Анотація. *У статті проаналізовано підходи до понять «інформація», «інформаційна безпека», «національна безпека». Висвітлено співзв'язок інформаційної безпеки і національної безпеки.*

Ключові слова: *інформація, інформаційна безпека, національна безпека, держава, війна.*

Швидкий розвиток технологій у другій половині XX ст. призвів до переходу суспільства в нову інформаційну епоху, яка характеризується визнанням інформації одним з найважливіших суспільних ресурсів. Інформатизація та комп'ютеризація докорінно змінюють сутнісну основу суспільства.

Поширення використання нових технічних засобів, через призму яких здійснюється інформатизація у всьому світі, робить «відкритими» державні кордони і формує нові геополітичні парадигми у розумінні глобальних соціотехнічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угрупованнями. Електронно-комунікаційна інфраструктура, як й інші інформаційні ресурси, стає об'єктом міждержавної боротьби за світове лідерство або об'єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносин [1]. За таких умов забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки.

Метою дослідження виступають теоретико-методологічні засади інформаційної безпеки як складової національної безпеки держави.

Слід зазначити, що незважаючи на широке поширення поняття «інформація» (*від латинської informātiō «роз'яс-*

нення, уявлення, поняття про що-небудь») воно залишається одним із найбільш дискусійних у науці, а сам термін у різних галузях людської діяльності може мати різне змістове наповнення.

Так Ростислав Калюжний зазначає, що інформація є властивістю лише високоорганізованої, тобто живої матерії. Інформація й інформаційні процеси, на його думку, властиві тільки біологічній і соціальній формам руху матерії. Він вважав, що живі організми розвивають необхідну їм інформацію завдяки постійній взаємодії із природою, обміну з навколишнім середовищем. При цьому інформації належить особлива інтегруюча роль, завдяки якій у живих істот й насамперед у людини, розвилися адаптаційні здібності. У такий спосіб інформація лежить в основі процесів саморегулювання у живій природі

Відповідно, Володимир. Богуш, на основі функціонального підходу до розуміння сутності інформації, розглядає інформацію як властивість лише систем, що самоорганізуються, не тільки у живій природі, але й у техніці. До них, наприклад, відносять і живі істоти й кібернетичні системи, для яких характерні процеси саморегулювання завдяки передаванню, зберіганню й переробленню інформації [2].

Відтак, можна констатувати, що інформація – це об'єкт багатофункціональний. Вона створюється й застосовується в усіх сферах діяльності та забезпечує виконання багатоманітних функцій і завдань, що постають перед найрізноманітнішими суб'єктами – органами державної влади, місцевого самоврядування, перед фізичними і юридичними особами, іншими соціальними утвореннями. Саме тому Закон України «Про інформацію» від 02.10.1992 р. трактує інформацію як «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі» [3].

Віктор Шульга пропонує вибудовувати зміст поняття «інформація» на двох рівнях:

Перший, макрорівень, коли інформація впевнено займає позиції головного фактора могутності держави, адже здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно

управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї політичної та економічної міцності.

Другий, мікрорівень, обсяг, достовірність, цілісність, якість обробки інформації визначає ефективність дій менеджменту підприємства, а, отже, актуалізує використання інформаційних технологій в управлінні грошово-кредитними, фінансовими, соціально-економічними процесами даного підприємства [2].

У нашому досліджені, відповідно до мети, будемо виходити із розуміння поняття «інформація» через призму макрорівневого підходу.

Національна безпека держави – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам [4, с. 3].

Поняття «інформаційна безпека», як складова національної безпеки характеризується як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [5].

У сучасних умовах інформаційна складова національної безпеки держави відіграє надзвичайно важливу роль через наявні в ній ризики та загрози, до яких доцільно відносити кібертероризм, кіберзлочинність, агресивну пропаганду, поширення антиконституційних та антидержавних гасел, обмеження доступу населення до публічної інформації тощо.

На вирішення зазначених складових, направлені Закон України «Про національну безпеку України», Указ Президента України від 14.09.2020 № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» та інші законодавчі.

Так, в Законі України «Про національну безпеку України» від 21 червня 2018 року зазначається: «Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо» [6]. Сформульовано найбільш важли-

ві потенційні та реальні ризики стабільності в суспільстві та національній безпеці України в інформаційній сфері:

1) розголошення конфіденційної інформації, що є власністю держави та спрямована на забезпечення національних інтересів та потреб держави та суспільства;
2) прояви обмеження доступу громадян до інформації та свободи слова;
3) поширення через засоби масової інформації культу та ідеології насильства, жорстокості тощо;
4) комп'ютерна злочинність та комп'ютерний тероризм;
5) розголошення інформації, що становить як державну, так і іншу таємницю, що передбачена Законом;
6) намагання маніпулювання суспільною свідомістю, зокрема, шляхом поширення упередженої, неповної чи недостовірної інформації [6].

Разом з тим, для забезпечення інформаційної безпеки та виконання зазначених вище завдань, з урахуванням російської агресії проти України в 2014 році, був прийнятий Указ Президента України від 14.09.2020 №392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України», Указ Президента України від №56/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»

В яких інформаційна безпека трактується – як стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам

та національній безпеці України. Інформаційна безпека є складовою національної безпеки України[6]. Формуються завдання для забезпечення інформаційної безпеки України, які передбачають:

- забезпечення постійного об'єктивного моніторингу інформаційного простору (внутрішнього та зовнішнього), систематичний аналіз результатів моніторингу;
- чітке визначення єдиного загальнодержавного стратегічного наративу та особливостей його трактування різними державними інституціями України;
- створення механізмів унеможливлення відхилення від наративу при здійсненні інформаційної діяльності різними державними інституціями;
- скоординована діяльність в інформаційному просторі всіх державних інституцій України;
- реалізація принципів та методології стратегічних комунікацій всіма державними інституціями, які здійснюють інформаційну діяльність;
- виявлення, оцінювання та прогнозування наслідків загроз національним інтересам та національній безпеці України в інформаційній сфері;
- протидія зовнішнім інформаційним впливам на населення України, зокрема на воєнно-політичне керівництво, особовий склад всіх складових Сектору безпеки і оборони України; захист об'єктів критичної інформаційної інфраструктури України (зокрема від кібератак);
- підвищення медіаграмотності населення [1].

Широкомасштабне вторгнення росії в Україну 24 лютого 2022 року, поширення інформаційної пропаганди акту агресії, вимагає продукування ефективної політики інформаційної безпеки, тому що інформаційне забезпечення національної безпеки являє собою процес задоволення інформаційних потреб суб'єктів національної безпеки.

Список використаних джерел:

1. Актуальні проблеми управління інформаційною безпекою держави XII Всеукраїнська науково-практична конференція Збірник тез наукових доповідей (Київ, 26 березня 2021 року). Електронне видання. URL: https://academy.ssu.gov.ua/-uploads/p_57_53218641.pdf.

2. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*. 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514.
3. ЗАКОН УКРАЇНИ «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, N48, ст.650). Верховна Рада України. 1992. URL: https://xn-80aagahqwyibe8an.com/ukrajiny-zakony/zakon-ukrajini-pro-informatsiyu-vidomosti1992.html.
4. Дзьобань О.П. Національна безпека в умовах соціальних трансформацій (методологія дослідження та забезпечення): монографія Харків: Константа, 2006. 440 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/5234/1/Dzeban_2006.pdf.
5. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України.* 2019. Вип. 3. URL: https://www.rdc.org.ua/-download/stati/Informational-warehouse.pdf.
6. Закон України «Про національну безпеку України» (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241). URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.
7. Указ Президента України від 14.09.2020 № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.
8. Указ Президента України від № 56/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». URL: https://www.president.gov.ua/documents/562022-41377.

INFORMATION SECURITY AS A COMPONENT OF NATIONAL SECURITY OF STATES

Abstract. *The article analyzes approaches to the concepts of «information», «information security», «national security». The relationship between information security and national security is highlighted.*

Key words: *information, information security, national security, state, war.*

Отримано: 19.11.2022

УДК 32.019.5:004.056.5]:[070:004.49]]:355.48(470:477)2014/...

О. В. Віннічук, *кандидат політичних наук, доцент кафедри політології та філософії Кам'янець-Подільського національного університету імені Івана Огієнка*

МЕДІА-ВІРУСИ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Анотація. *Відзначено, що в умовах інформаційної війни медіа-віруси виступають важливим інструментом впливу на інформаційне поле супротивника. Розкрито сутність медіа-вірусів та їх різновиди. Проаналізовано найбільш популярні меми в українському інформаційному просторі від початку повномасштабної російсько-української війни. Зроблено висновки, що ефективна робота «інформаційних військ» у мережевому просторі як однієї з важливих гілок протистояння кремлівській військовій агресії, наближає українське суспільство до перемоги.*

Ключові слова: *медіа-вірус, інформаційна безпека, меми, російсько-українська війна.*

В умовах сьогодення інформація для будь-якої держави виступає стратегічно важливим ресурсом, від раціонального використання якого залежить безпека країни та перспективи формування демократичного суспільства, де реалізуються всі конституційні права та свободи громадян.

Адже застосування найновіших інформаційних технологій впливу на свідомість громадян, які спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, порушення суверенітету і територіальної цілісності України в умовах сьогодення вимагають відповідальності українського суспільства у споживанні інформаційних масивів.

В умовах інформаційної війни важливим інструментом для проникнення на вороже інформаційне поле є медіа-віруси.

Медіавіруси – це меми та мемокомплекси, які поширюються в інформаційних мережах та привертають увагу широкого кола громадськості до локальних та глобальних подій. До медіа вірусу відносять контент, який має здатність ширитися миттєво, зацікавлювати широкі верстви населення та немає корисного змісту. Це можуть бути по-

дії, сенсації, скандали, чутки тощо, які укріплюються у масовій свідомості у якості гасел, міфів, мемів [4, с. 270].

Американський дослідник Д. Рашкофф виділяє декілька типів медіа-вірусів, серед яких:

1. Цілеспрямовані віруси (як реклама, передвиборчі гасла, «інформаційні бомби»);
2. Віруси-тягачі – спонтанно виникають та миттєво підхоплюються, а також наповнюються певним змістом та зазвичай спрямовані на вирішення конкретних завдань;
3. Спонтанні віруси – народжуються та поширюються без конкретної цілі, в разі успішності можуть бути використані для вирішення певних завдань [3, с. 268].

Варто розуміти, що медіа-вірусом може стати будь-яке актуальне повідомлення, якому фахівці нададуть привабливого змісту.

Існує чимало практик поширення вірусного повідомлення в Мережі. Зокрема, особливу роль відіграють соціальні зв'язки, публічні дії, емоційні стани, мотивація. Як показує практика, саме зазначені підходи найчастіше використовуються для поширені мемів у період російсько-української війни.

Приклади медіа-вірусів в українському суспільстві [6]:

– «Герої не вмирають» – гасло, яке виховує у нашій свідомості почуття поваги, вдячності до загиблих воїнів. Розуміння того факту, що за яких би обставин не загинув воїн, він завжди для патріотів своєї держави залишиться Героєм.

Проте варто розуміти, що гасло в першу чергу використовується з метою придушення емоційного протистояння рідних загиблих військових/добровольців, кола друзів та знайомих чи просто обурених суспільних мас бездіяльність провладних еліт.

– «Доброго вечора, ми з України!» – насправді фраза з треку популярного українського гурту *«Даха Браха»*. Трек отримав популярність ще у жовтні 2021 році в Tik Tok, проте вже з 24 лютого 2022 року це не просто слова з треку, а неофіційне військове привітання в Україні, що стало популярним після російського вторгнення. В умовах війни слова треку лунають у багатьох бомбосховищах України, підіймаючи дух українців до заповітної перемоги.

Меми.

Мем як поняття є одиницею імітації та комунікації. Може вміщувати в себе широке коло інформації, яке надходить різними каналами (звуковими, тактильними, зоровими тощо).

Існує чимало визначень мемів. Зокрема [8, с. 210-219]:

- як культурної одиниці;
- як концепт чи ідея, що відображається в вербальному, візуальному чи звуковому рівнях;
- як моделі різновиду інформації;
- як частина інформації, що відзначається стислістю та швидким розповсюдженням.

Часто меми вважаються вірусними культурними одиницями. Термін «вірусний» (та пов'язаний з ним інтернет-«мем») у популярному використанні – це дивакуватий жарт або навичка, що дуже поширено імітуються [8, с. 213].

Застосовуючи до класифікації мемів текстовий критерій структурної організації, можна виділити:

- меми-слова (« Паляниця»);
- меми-словосполучення («Привид Києва»);
- фразові (коли мем становить цілу фразу, речення («Доброго вечора, ми з України»).

Таким чином, мемами можуть бути мелодії, ідеї, модні слова, вирази, які набувають популярності та вкорінюються у суспільстві.

Центром уваги в умовах військового протистояння російським інформаційній машині є Інтернет-меми. Зазвичай Інтернет-меми є вірусними жартами, які поширюються з мегашвидкістю та представляються широкому загалу у вигляді картинки, фото чи відео сюжету.

Інтернет-меми є засобом впливу на свідомість людей та виступають запорукою успішної пропаганда ідей чи поглядів. Соціальні мережі допомагають миттєвому розповсюдженню Інтернет-мемів, виконуючи при цьому роль психологічних вірусів.

Варто відзначити особливість Інтернет-мемів – це їхня емоційна насиченість, яка сприяє підвищенню зацікавленості контентом та швидкості його поширення.

Найбільш популярні меми в українському інформаційному просторі лютому – червня 2022 р.

«Паляниця» [7].

Володіючи на високому рівні навиками комунікації рідної мови та не вивчаючи іноземної, чимало людей не розуміють, як важко може даватися вимова окремих звуків, а іноді й взагалі не вдається. Представникам рф не під силу належно вимовляти слово «паляниця». Таким чином, українці стали застосовувати цей мем для перевірки «своїх» та «чужих».

«Привид Києва» [5].

Насправді мова йде про прізвисько невідомого пілота МіГ-29, який успішно виконував завдання, збиваючи чимало винищувачів на Києвом у перші дні війни. І хоча чимало сумнівалися у існуванні «Героя», проте Він став легендою війни та улюбленцем українок.

«Байрактар» [9].

Bayraktar TB2 – це ударний оперативно-тактичний безпілотний літальний апарат (БПЛА), який розробляється на території Туреччини. Здатний розганятися до 200 км за годину та підніматися на висоту понад 8 км. «Байрактар» скидає авіабомби та керовані протитанкові ракети. При цьому дрон може протягом доби перебувати в польоті. Свою назву безпілотник отримав на честь засновника компанії Baykar.

В умовах російсько-української війни «байрактарам» присвячують треки та навіть називають дітей.

«Цигани з трактором» [1].

Цей мем заполонив соціальні мережі та був спрямований на підняття емоційного стану українців. 27 лютого 2022 року в с. Любимівка місцеві роми помітили на дорозі російську військову техніку і вирішили допомогти окупантам знайти шлях до себе додому.

Винахідливі українці транспортували танк у невідомому напрямку за допомогою трактора. Один з російських військових намагався наздогнати «диво техніки», проте так і не зміг.

«Чорнобаївка» [2].

Населений пункт Чорнобаївка, що знаходиться неподалік м.Херсон стало легендою. Саме тут розташований аеродром, в межах якого постійно зазнає втрат російська

армія. Критично осмислюючи ситуацію, українці намагаються зрозуміти, які магічні сили притягують росіян до до цієї місцини.

Користувачі соцмереж створили безліч чудових мемів і жартів, пов'язаних зі знищенням ворога в с. Чорнобаївка.

Вперше на аеродромі с. Чорнобаївка техніку росіян було знищено 27 лютого 2022 р. «Ефект Чорнобаївки» продовжувався протягом березня-травня 2022 р., загалом більше 28 раз. Таким чином, с. Чорнобаївка стало відомим у світі. Навколо подій в Чорнобаївці було створено чимало популярних жартівливих мемів.

В умовах сьогодення регулювати медіапростір достатньо складно. Для того, щоб відвернути увагу від однієї вірусної новини, необхідно продукувати інший вірусний контент, що вплине на емоції споживача. Адже вдалий вірусний контент може ширитися соціальними мережами неконтрольованими темпами.

Отже, медіавіруси відносяться до інформаційної зброї XXI століття. На прикладі ведення російсько-української війни можна припустити, що без коректної роботи «інформаційного війська» (до складу яких входять хакери, знавці ІТ-сфери, пересічні громадяни України та всі противники «путінської диктатури») стало б неможливим протистояння на інформаційному фронті з боку Української держави. Окрім того, якісні меми доволі часто несуть позитивні емоції, підбадьорюючи українців та налаштовуючи їх на безумовну ПЕРЕМОГУ.

Правове регулювання інформаційного простору наразі виступає основною умовою подальшого розвитку онлайнових мереж.

Список використаних джерел:

1. Орлова В. Під Каховкою українські роми вкрали у російських окупантів танк. УНІАН. 27.02.2022. URL: https://www.unian.ua/-war/pid-kahovkoyu-ukrajinski-romi-vkrali-u-rosiyskih-okupantiv-tank-novini-vtorgnennya-rosiji-v-ukrajinu-11720335.html
2. Коновалюк Е. «Добрий ранок» під дулом автомата: як росіяни кошмарять легендарну Чорнобаївку. URL: https://life.pravda.com.ua/society/2022/06/21/249184/
3. Курбан О. В. Медіавіруси та їх використання як інформаційної зброї. *Наукові записки.* 2016. Вип. 1 (52). С. 268.

4. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник. Київ: ВІКНУ, 2016. 286 с.
5. Лоуренс Пітер. Привид Києва. Як народилась легенда, яка підняла дух українців. 2022 (1 травня). URL: https://www.bbc.com/ukrainian/features-61291455.
6. Маркітантов В.Ю., Віннічук О.В. Рибщун О.В. Російська гібридна війна: від доктрини до тактики: навчальний посібник. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2022.
7. Мазуренко А. Не вимовив «паляниця»: на Рівненщині затримали росіянина з вибухівкою. 2022 (12 квітня). URL: https://www.pravda.com.ua/news/2022/04/12/7339167/
8. Неклесова В. Меми як частина онімного простору. *Записки з ономастики.* 2017. Вип. 20. С. 210-222
9. Що таке «Байрактар» – які його головні характеристики? URL: https://api.visicom.ua/uk/posts/bayraktar100322

MEDIA VIRUSES AS A THREAT TO INFORMATION SECURITY IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR

Abstract. *It is noted that in the conditions of information warfare, media viruses are an important tool for influencing the enemy's information field. The essence of media viruses and their varieties is revealed. The most popular memes in the Ukrainian information space since the beginning of the full-scale Russian-Ukrainian war are analyzed. The conclusions are drawn that the effective work of «information troops» in the network space as one of the important branches of confrontation with the Kremlin's military aggression brings Ukrainian society closer to victory.*

Key words: *media virus, information security, memes, Russian-Ukrainian war.*

Отримано: 15.11.2022

УДК 004:327

Л. А. Руда, *кандидат політичних наук,*
асистент кафедри політології та філософії
Кам'янець-Подільського національного
університете імені Івана Огієнка

МІЖНАРОДНІ СТАНДАРТИ З ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Інформаційні технології в даний час набули глобального характеру і стали невід'ємною частиною всіх сфер діяльності особи, суспільства та держави. Розширення областей та сфер застосування інформаційних технологій значно розширює перспективи розвитку нових інформаційних погроз та змінює міжнародні стандарти з забезпечення інформаційної безпеки.*

Ключові слова: *інформаційна безпека, стандарт інформаційної безпеки, інформаційні технології, кібернебезпека.*

В сучасному світі існує велика кількість підходів до забезпечення та управління інформаційною безпекою. Найбільш ефективні з них викладені в міжнародних стандартах в сфері інформаційної безпеки та управління інформаційними технологіями, які є орієнтиром при формуванні інформаційної безпеки, а також допомагають у проблемах пов'язаних з інформаційною безпекою всіх рівнів (стратегічних, тактичних та операційних).

Міжнародні стандарти інформаційної безпеки розвиваються роками, і за цей час удосконалюються і вбирають в себе кращий досвід фахівців-практиків. Однією з переваг вивчення стандартів є можливість ефективної взаємодії спеціалістів з інформаційної безпеки, адже аналіз загальноприйнятих стандартів міжнародного рівня дозволяє спеціалістам обмінюватися інформацією без використанням специфічних термінів і визначень, що сприяє покращенню комунікації з уникненням мовних бар'єрів.

Існує безліч поглядів і різних способів групування міжнародних стандартів. Міжнародні стандарти інформаційної безпеки умовно можна поділити на 4 групи:

1) стандарти для огляду і введення в термінологію;

2) стандарти, які визначають обов'язкові вимоги до система управління інформаційною безпекою;
3) стандарти, що визначають вимоги і рекомендації для аудиту системи управління інформаційною безпекою;
4) стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення системи управління інформаційною безпекою [4].

Стандарти розвитку та вдосконалення системи управління інформаційною безпекою також можна поділити на:

1) технічні або контрольні, що регламентують різні аспекти реалізації засобів захисту. Технічні стандарти допомагають забезпечити технічний захист інформації – вибрати необхідний комплекс захисних заходів і провести їх грамотне налаштування.
2) процесно-орієнтовані, що описують процедуру від розробки процесів до формування інформаційної безпеки в цілому.

У сучасному світі існує значна нормативна база стандартів та найкращих практик з інформаційної безпеки. Аналіз нормативних документів слід розпочати з серії стандартів ISO 27x [2], Міжнародної Організації зі Стандартизації (International Organization for Standardization) [7] та Міжнародної Електротехнічної Комісії (International Electrotechnical Commission) [3]. Серія стандартів містить найкращі практики та рекомендації щодо створення, розвитку та підтримки системи менеджменту інформаційної безпеки.

Існуючі міжнародні стандарти описують методологію оцінки ризиків, як складової частини під час моделювання загроз інформаційної безпеки. При цьому необхідно враховувати, що збитки від реалізації загроз інформаційної безпеки можуть бути прямими чи непрямими. Прямі збитки – це безпосередні та прогнозовані втрати від реалізації загроз інформаційної безпеки, наприклад втрата прав інтелектуальної власності, судові витрати та виплата штрафів та компенсацій.

Міжнародний підхід до управління інформаційними технологіями, розроблений Асоціацією контролю та аудиту систем (Information Systems Audit and Control Association) та Інститутом керівництва IT (IT Governance Institute) та називається «Контрольні цілі для інформаційних та сумі-

жних технологій» (Control Objectives for Information and related Technology (COBIT)) [1]. На сьогодні актуальною є 5 редакція даного документа, де розміщено близько 40 документів про міжнародні та національні стандарти і керівництва в сфері управління інформаційними технологіями та забезпечення інформаційної безпеки. Аналіз даних документів свідчить, що мінімум 2 мають безпосереднє відношення до інформаційної безпеки (APO13 Manage Security та DSS05 Manage Security Services), а близько 11 можливо використовувати при впровадженні процесів комплексної системи інформаційної безпеки.

Одним із найважливіших документів є Загальний регламент про захист даних (The General Data Protection Regulation), затверджений Європейським Парламентом і Радою Європейського Союзу 27 квітня 2016 р. Регламент передбачає захист фізичних осіб у відносинах обробки персональних даних. У відповідності з Регламентом, право на захист особистих даних забезпечується для всіх у рівній мірі, оскільки всі, незважаючи на стать, національність чи місце проживання, наділені рівним правом на захист персональних даних. Регламент, застосовується при обробці персональних даних установами, органами, організаціями та агентствами Євросоюзу, покликаний забезпечити свободу, безпеку та справедливість в розвитку Євросоюзу, зміцненню та соціальному прогресу, зміцненню та зближенню економіки на внутрішньому ринку. Персональні дані, відповідно до Регламенту, поділяються на категорії: «генетичні дані», «біометричні дані», «дані про здоров'я» [5].

Розголошення персональних даних, що пов’язані з расовим чи етнічним походженням, політичними поглядами, релігійними чи філософськими переконаннями, дані про перебування в громадських об’єднаннях чи професійних союзах, а також обробка генетичних даних, біометричних даних для фізичної ідентифікації особи, даних, що мають відношення до здоров’я, статевого життя чи сексуальної орієнтації, заборонене.

Окрім теоретичного забезпечення міжнародної стандартизації інформаційної безпеки поширена розробка та практичне використання рекомендації для практичної реалізації забезпечення інформаційної безпеки. Наприклад, за підтримки австралійського Центру забезпечення

безпеки в кіберпросторі, що пережив низку кібератак в 2000 році, було розроблено Посібник з інформаційної безпеки уряду Австралії, що поєднує як технічні рекомендації для забезпечення інформаційної безпеки, так і стратегічні обґрунтування, які спеціалісти даної галузі можуть практично використовувати. Окрім цього, існує багато організацій і проектів, метою яких є практичне забезпечення безпеки та поширення інформації, що допомагає спеціалістам з інформаційної безпеки перевіряти об'єкти захисту від потенційних загроз.

Для якісної побудови системи інформаційної безпеки потрібно узагальнювати знання і підходи, отримані з різних джерел, так як кожна система поглядів містить плюси і мінуси і вимагає адаптації до умов конкретної компанії. Фахівцям з інформаційної безпеки необхідно постійно вдосконалюватися, розширювати набір компетенцій і професійних знань, а прийняті закордонні стандарти істотно сприяють даному процесу та є джерелом для формування національних стандартів з інформаційної безпеки.

Список використаних джерел:

1. COBIT. URL: https://web.archive.org/web/20191025104017/-index.php/homepage/download/category/2-standards?download=1:cobit-4-1-ukr (дата звернення 22.10.2022).
2. CRAMM (CCTA Risk Analysis and Management Method). URL: http://rm-inv.enisa.europa.eu/methods/m_cramm.html (дата звернення 22.10.2022).
3. Reference material International Electrotechnical Commission. URL: https://www.iec.ch/news-resources/reference-material (дата звернення 22.10.2022).
4. Дикий О. В., Флюнт М. О. Стандарти інформаційної безпеки: компаративне дослідження. Право та державне управління. 2019 р., № 2 (35) том 1. С. 80-87.
5. Загальний регламент про захист даних. URL: http://data.europa.eu/eli/reg/2016/679/oj (дата звернення 22.10.2022).
6. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. URL: https://naurok.com.ua/keruvannyamehanizmami-zahistu-mizhnarodnistandarti-informaciyno-bezpeki-1047 26.html. (дата звернення 22.10.2022).
7. Стандарты ИСО согласованы экспертами на международном уровне. URL: https://www.iso.org/ru/standards.html (дата звернення 22.10.2022).

INTERNATIONAL STANDARDS FOR INFORMATION SECURITY

Abstract. *Information technologies have now acquired a global character and have become an integral part of all spheres of activity of a person, society and the state. The expansion of areas and areas of application of information technologies significantly expands the prospects for the development of new information threats and changes international standards for ensuring information security.*

Key words: *information security, IT security standards, Information technology, cybersecurity.*

Отримано: 29.11.2022

УДК 316.776.2

А. Е. Бородай, *студентка 1 курсу*
ОС «Магістр» спеціальності «Соціологія»
Маріупольського Державного Університету

КІБЕРЗЛОЧИННІСТЬ ЯК ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *У статті розглянута кіберзлочинність як проблема інформаційної безпеки в Україні, що становить серйозну загрозу для персональних даних суспільства та держави в мережі Інтернет, також більшою мірою актуалізовані значущість розвитку інформаційного захисту на державного рівні та захисту себе від кіберзлочинців у повсякденному житті.*

Ключові слова: *кіберзлочинність, Інтернет, кібершахраї, інформаційна безпека.*

Зараз ми проживаємо у тотальній діджиталізації та розвитку інформаційних технологій, де все більш важливого значення набуває інформація. В наш час, коли життя без зв'язку здається неможливим, коли весь світ перетворився на одну глобальну мережу та коли Інтернет дає нескінченність можливостей, важливо пам'ятати про безпеку та дбати про свій захист у мережі, щоб не виникало проблем. Тому що саме через Всесвітню мережу черпаємо інформацію для навчання, шукаємо розваги, купуємо різноманітні товари, оплачуємо безліч послуг та ділимося майже всіма аспектами свого життя.

За законом України «Про основні засади забезпечення кібербезпеки України», кіберзлочин – це суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. У Кримінальному кодексі України ці злочини закріплено в розд. 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [1]. У сфері інформаційних технологій можна визначити, що ситуація з кіберзлочинністю набуває все більшої загрози для суспільства.

Питання кіберзлочинності є надзвичайно важливим на державному рівні. Найчастіше під ударами кібератак опиняються об'єкти критичної інфраструктури: енергетичні об'єкти, транспорт та банківський сектор. У 2017 році в Україні відбулася масштабна атака вірусом Petya: були уражені енергетичні компанії, українські банки, аеропорт «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен тощо. Такого безпрецедентного масштабного вторгнення в сервери вітчизняних компаній наша країна ще не зазнавала. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya становили майже 850 млн доларів. Водночас заяви постраждалих компаній до кіберполіції про втрату даних часто залишались без відповіді, адже знайти та притягти до відповідальності зловмисника в цьому разі виявилось неможливо [2].

Організована злочинність дедалі частіше використовує Інтернет з метою приховання своєї діяльності. Зараз нікого не здивуєш існуванням мережі Darknet, за допомогою якої злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених товарів тощо. Завдяки технологіям, які забезпечують мережеву анонімність, ця частина Інтернету залишається абсолютно безконтрольною, а тому безпечною для діяльності різноманітних злочинних угруповань.

Основними види таких злочинів перш за все є: незаконний доступ, незаконне перехоплення, втручання у дані, зловживання пристроями, шахрайство, пов'язане із комп'ютерами, правопорушення, пов'язані з дитячою порнографією тощо. Кібершахраї використовують старі схеми обману довірливих громадян, яким повідомляють, що їхні знайомі потрапили до халепи иґ терміново необхідні гроші, щоб їм допомогти. Теж досить часто кіберзлочинці протиправно отримують доступ до особистої переписки, фото або відео, а потім за доступ чи видалення вимагають гроші. Нерідко кіберзлочином є також цифрове піратство, тобто встановлення та користування неліцензійного програмного забезпечення, завантаження та перегляд фільмів і серіалів із піратських сайтів. Традиційно популярним методом кібершахрайських дій є створення фальшивих сайтів відомих інтернет-магазинів, брендів, фінансових

установ, де користувачі через заповнення певних форм повідомляють свої персональні дані та паролі від банківських карток. Наприклад, тепер на тлі інтересу довкола криптовалютного ринку мають попит фальшиві сайти купівлі-продажу й обміну криптовалют.

У зв'язку з вищесказаним, не варто забувати про власну інформаційну безпеку. Перше і головне правило – відповідально ставитися до публікації і передачі будь-яких персональних даних: ім'я та прізвище, дата та місце народження, сімейний стан, паспортні дані, професія тощо. Разом із тим, паролі та аккаунти не являються персональними даними, адже не несуть ніякої конкретної інформації про особу. Але можуть бути використані у скоєнні віртуальних злочинів. Також експерти радять видаляти геолокації з ваших особистих постів задля забезпечення власного захисту. Прикріпляти до свого персонального, а тим паче до бізнес-аккаунту, мобільний номер телефону – звичайна практика, досить зручна та розповсюджена. Проте, і тут є певні небезпеки, адже номер телефону може посприяти злому персональної сторінки для використання облікового запису. Не варто ділитися фотографіями своїх посадкових талонів в аеропорту, світлинами паспорту чи водійських прав. Нікому не передавайте ваші паролі від облікових записів. Безкоштовні мережі в кафе чи кінотеатрах є чудовою можливістю для зловмисників. Програми, які дозволяють слідкувати за вами, є у вільному доступі. Тож важливі операції краще проводити лише за перевіреного з'єднання з Інтернетом. Не варто скачувати додатки із неперевірених джерел, якщо скачувати програми із сумнівних джерел – ми самі наражаємось на небезпеку. Завжди перевіряйте правильність адреси веб-сайтів, на яких ви виконуєте якісь фінансові операції або вводите конфіденційну інформацію. Дотримання даних правил допоможе уникнути або мінімізувати можливість бути об'єктом уваги кіберзлочинності [3].

Можна зробити висновок, що кіберзлочинність на сьогодні становить безпеку не тільки для держави, а й для суспільства. Вирішення цієї проблеми потребує більше фахівців зі спеціальних знань та сучасних методів виявлення комп'ютерних злочинів.

Список використаних джерел:

1. Кримінальний кодекс України від 05.04.2001 р. URL: http://zakon3.rada.gov.ua/laws/show/2341-14.
2. Гуцалюк М. Інтернет: протидія кримінальним проявам та боротьба зі злочинністю. URL: http://www.lawyer.org.ua/-?w=r&i=10&d=500.
3. Кавуненко Т. Безпека в Інтернеті: як захистити себе і не стати жертвою зловмисників? URL: https://agentyzmin.org.ua/-news/bezpeka-v-interneti-iak-zakhystyty-sebe-i-ne-staty-zhert-voiu-zlovmysnykiv.

CYBERCRIME AS A PROBLEM OF INFORMATION SECURITY OF UKRAINE

Abstract. *The article examines cybercrime as a problem of information security in Ukraine, which poses a serious threat to the personal data of society and the state on the Internet, as well as the importance of developing information protection at the state level and protecting oneself from cybercriminals in everyday life.*

Key words: *cybercrime, Internet, cyber fraudsters, information security.*

Отримано: 25.11.2022

УДК 32(477):004.738.5

В. М. Сорокін, *здобувач 1 курсу третього освітнього ступеня «доктор філософії» спеціальності 052 «Політологія»*

ОСОБЛИВОСТІ ЕЛЕКТРОННОГО УРЯДУВАННЯ: ДОСВІД ВЕЛИКОЇ БРИТАНІЇ ТА УКРАЇНИ

Анотація. *Розкрито сутність та переваги е-урядування у державі та суспільстві. Проаналізовано особливості його розвитку на державному та місцевому рівнях в Україні та Великій Британії. На основі порівняльного аналізу визначено спільні та відмінні риси е-урядування зазначених країн. Виокремлено основні вимоги, яких необхідно дотримуватися в умовах розвитку е-урядування в Україні, з урахуванням досвіду Великобританії.*

Ключові слова: *електронне урядування, інформаційні технології, електронна демократія, держані програми.*

Невід'ємною складовою розвитку сучасного суспільства є глобалізація та інформатизація, що сприяє оперативності та доступності інформації, яка є підґрунтям ефективної комунікації між суспільством та органами влади. Відкритий та доступний діалог між громадянином та державною владою є важливою складовою сучасності. Інструментом його реалізації виступає електронне урядування, що дозволяє забезпечити демократичність та ефективність урядової діяльності.

У праці «Електронне урядування, як форма організації державного управління» автор Архіпова Є.О. визначає поняття електронне урядування як систему взаємодії органів державної влади з населенням, що будується на широкому застосуванні інформаційних технологій з метою підвищення доступності та якості державних послуг, зменшення строків їх надання, а також зниження адміністративного навантаження на громадян та організації щодо їх отримання [1].

Використання е-урядування забезпечує переваги для держави та суспільства, зокрема:

- спрощення надання послуг громадянам;
- усуває непотрібні рівні для прийняття рішень у системі держорганів;

- відкриває доступ для громадян, бізнесу та інших структур до інформації та потрібних служб;
- сприяє розвитку виконавчих процесів в інститутах влади;
- покращує підзвітність та прозорість діяльності влади;
- знижується рівень витрат за рахунок інтеграції та видалення дублюючих систем;
- підвищує ефективність державних дій, які направлені на задоволення потреб громадян [6, с. 7].

У праці «Електронна демократія» українські дослідники Н.В. Грицяк, С.Г. Соловйов виокремлюють наступні етапи розвитку е-демократії та е-урядування в Україні:

І етап (2000-2001 рр.) мав підготовчий характер: визначалися найбільш загальні моменти використання сучасних інформаційних технологій, формувалося необхідне підґрунтя для подальших дій держави в цьому напрямі.

ІІ етап (2002-2003 рр.) – характеризувався формуванням механізмів електронного уряду в Україні, що мало на меті підвищення ефективності та прозорості діяльності органів державної влади та органів місцевого самоврядування, поліпшення поінформованості громадян щодо діяльності цих органів та активізації зворотного зв'язку між владою та суспільством за допомогою мережі Інтернет.

ІІІ етап розпочався у 2003 р. прийняттям постанови КМУ «Про заходи щодо створення електронної інформаційної системи «е-уряд».

Початком IV етапу можна вважати 25.12.2013 р., коли розпорядженням Кабінету Міністрів України затверджено зміни до плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні [2, с. 12].

Саме Концепція розвитку електронного урядування в Україні [4] в період 2010-2015 рр. була одним з найважливіших нормативно-правових документів з розбудови е-урядування. Її метою було визначення засад та створення умов для досягнення європейських стандартів якості послуг, відкритості та прозорості діяльності органів влади.

Основний етап розвитку е-урядування в Україні розпочався з 2015 року після прийняття Коаліційної угоди парламентських фракцій Верховної Ради України (2014 рік) та Стратегії сталого розвитку «Україна – 2020», схваленої Указом Президента України від 12.01.2015 року.

Серед урядових програм, що сприяли розвитку е-урядування в Україні, найбільш популярним для громадян став онлайн-сервіс державних послуг Дія (взаємодія «Держава і я»). Метою сервісу «Дія» є перетворення України на справжню цифрову державу шляхом створення єдиного порталу, де можна отримати всі послуги онлайн швидко, зручно та людяно, та мобільного додатка в якому усі потрібні документи в одному місці.

Відповідно до Закону України «Про публічні закупівлі», у сфері взаємодії держави та бізнесу, усі держзакупівлі повинні проводитися у електронній системі Prozoro через торгові майданчики, що забезпечує прозорість та законність використання бюджетних коштів [5].

Спостерігається позитивна тенденція розвитку е-урядування в Україна на місцевому протягом останніх років, навіть в умовах складної економічної та політичної ситуації. Воно в основному розвивається за рахунок ініціативи місцевих рад, громадян та бізнесу, що в свою чергу, займаються пошуками способів та джерел коштів для фінансування їх проектів. Проте потребує ще вдосконалення нормативно-правова база для ефективності його впровадження.

Дослідження розвитку е-урядування на місцевому рівні в Україні займається Коаліція неурядових організацій, за підтримки Програми розвитку ООН в Україна та фінансується Європейським Союзом.

У процесі удосконалення е-урядування в України, необхідно враховувати зарубіжну практику його впровадження на державному та місцевому рівнях. Зокрема, однією з країн, де можна запозичити досвід е-урядування є Велика Британія, яка займає передові позиції у питаннях стандартизації підходів та рішень формування е-урядування. Передумовами, що сприяли цьому, стали англійські багатовікові традиції побудови політичної системи та демократії у державі.

У Великій Британії є єдина платформа gov.uk, що являє собою простір, де будь-який орган влади може публікувати необхідну йому інформацію у зручний йому спосіб. Процесу створення послуг, що надаються на даній платформі приділяється значна увага. Кожен орган влади має можливість завантажити спеціальний e-Services Tool Kit,

що являє собою локальний сервіс для моделювання власної послуги. У ньому можна самостійно вибрати та сформувати послугу від її зовнішнього оформлення і завершуючи особливостями обробки. Наступним етапом є проведення фокус-групи, тобто випробування своєї послуги на цільовій аудиторії, за підсумками яких, буде оцінено зрозумілість та доступність інтерфейсу користувачу і виявити можливі проблеми у користуванні е-послугою.

У Великій Британії відсутня чинна цілісна законодавча база регулювання питань е-урядування, існують лише окремі напрацювання.

Законодавство щодо електронної комерції (e-Commerce Legislation) = орієнтовані на допомогу у здійсненні електронної комунікації та створенні легальної бази для електронної комерції, використання електронного підпису, обидва як у приватному, так і в публічному секторі.

Законодавство електронних комунікацій (eCommunications Legislation) – забезпечує прозорість нової європейські регуляції для комунікативних підрозділів електронного уряду.

Законодавство щодо електронного підпису (eSignatures Legislation) орієнтоване на допомогу у формуванні нової системи електронного підпису у приватній та публічній сфері.

Електронне урядування у Великій Британії на державному рівні здійснюється за досить складною схемою, де задіяні різні департаменти, кожен з яких виконує свою функцію. Очолює систему електронного врядування Cabinet Office, співпрацює з членами CIO Council, який насамперед регламентує діяльність електронного уряду.

Впровадженням новітньої системи надання послуг громадянам щодо догляду за містами, планування та місцевим контролем у Великій Британії займається Department for Communities and Local Government.

Разом ці установи являють сукупність органів, що відповідальні за електронне урядування на місцевому рівні [3, с. 7-21].

Проаналізувавши особливості розвитку е-урядування вищезазначених країн, можна виділити спільні ознаки у даній сфері, зокрема:

- наявність до 2013 р у кожного органу влади власного сайту;

- взаємодія великої команди спеціалістів, як внутрішніх, так і зовнішніх фахівців, у процесі створення е-послуг;
- використання в органах влади та в бізнесі електронного цифрового підпису, як базового інформаційної технології електронного урядування;
- функціонування е-урядування на двох рівнях: державний та місцевий.

У розвитку е-урядування України та Великої Британії відмінності проявляються у наступних аспектах:

- оформленні, дизайні та поданні інформації на сайтах влади;
- мисленні та підходах до надання послуг держави;
- рівні довіри населення до органів державної влади та місцевого самоврядування;
- різній політичній та економічній ситуації у країнах, що впливає на його швидкість та якість.

Отже, можна виділити основні вимоги, яких необхідно дотримуватися розвитку системи е-урядування в Україні, на основі досвіду Великобританії:

- врахування особливостей розвитку України;
- врахування бажань потенційних користувачів;
- забезпечення максимально можливого рівня безпечності та приватності персональних даних користувачів;
- сформувати різновекторну команду фахівців;
- застосовувати єдину платформу та відкриті стандарти е-урядування;
- гнучкість підходів, що використовуються.

Дотримання даних вимог допоможе переформатувати зручний державний сервіс для громадян та мінімізує труднощі у їх взаємодії з державою.

Список використаних джерел:

1. Архипова Є.О. Електронне урядування як форма організації державного управління. Державне управління: удосконалення та розвиток: електронне наукове фахове видання. 2015. N4. URL: http://www.dy.nayka.com.ua/?op=1&z=855.
2. Грицяк Н.В. Електронна демократія. Київ: НАДУ, 2015. 66 с.
3. Камінська Т., Камінський А., Пасічник М. Зарубіжний досвід упровадження електронного урядування / за заг. ред. д-ра наук з держ. упр., проф. С.А. Чукут. Київ, 2008. 200 с.

4. Про затвердження Порядку подання документів в електронному вигляді до органу ліцензування та видачі ним документів в електронному вигляді за допомогою телекомунікаційних засобів зв'язку: Постанова Кабінету Міністрів України від 23.08.2016 р. №561. URL: http://www.kmu.gov.ua/control/-ru/cardnpd?docid=249265385.
5. Про публічні закупівлі. Закон України від 25.12.2015 № 922-VIII. URL: https://zakon.rada.gov.ua/laws/show/922-19#Text.
6. Семенченка А.І., Дрешпака В.М. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. Частина 7: Розвиток електронного урядування на місцевому та регіональному рівнях. Київ: ФОП Москаленко О.М., 2017. С. 7-31.

PECULIARITIES OF ELECTRONIC GOVERNANCE: THE EXPERIENCE OF GREAT BRITAIN AND UKRAINE

Abstract. *The essence and advantages of e-governance in the state and society are revealed. The peculiarities of its development at the state and local levels in Ukraine and Great Britain are analyzed. On the basis of a comparative analysis, the common and distinctive features of e-government of the specified countries are determined. The main requirements, which must be followed in terms of the development of e-government in Ukraine, are highlighted, taking into account the experience of Great Britain.*

Key words: *electronic governance, information technologies, electronic democracy, state programs.*

Отримано: 18.11.2022

УДК 327.7:355.48(470:477)«2014/...»

А. Ситнік, *здобувачка1 курсу третього освітнього ступеня «доктор філософії» спеціальності 052 «Політологія»*

ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ЩОДО РОСІЙСЬКОЇ ЗБРОЙНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ: ВІД «СТУРБОВАНОСТІ» ДО САНКЦІЙ

Анотація. *У статті проаналізовано ефективність інформаційної політики міжнародних організацій та місце міжнародної спільноти у ході російсько-української війни. Висвітлено якісні зміни у діяльності міжнародних організацій, що простежуються через їхню інформаційну політику, яка пройшла шлях від консультативної участі та політики «умиротворення агресора» до санкційного тиску на агресора та його свиту. Результати дослідження доводять, що початок широкомасштабної війни на східних теренах Європи змінив риторику «занепокоєння ситуацією» з боку міжнародних організацій, на практичну участь останніх у протистоянні рашизму. У статті підкреслюється важливість посилення санкцій з боку міжнародної спільноти та надання різного спектру допомоги Україні.*

Ключові слова: *інформаційна політика, міжнародні організації, російсько-українська війна, політика умиротворення агресора, санкції.*

Сьогодні на території Європи точиться наймасштабніший військовий конфлікт з часів Другої світової війни, де разом зі звичним військовим озброєнням має місце і новий її різновид – інформаційно-пропагандистський. При цьому, застосування росією інформаційно-пропагандистських інструментів у реалізації власних імперсько-шовіністичних цілей – давній випробуваний підхід. Зокрема, століттями ці інструменти були спрямовані проти України та українства, вирізняючись лише інтенсивністю та формами застосування в окремі історичні періоди.

З проголошенням незалежності України, росією вкотре була запущена тривала інформаційно-пропагандистська операція, у якій було задіяно колосальні ресурси і яка заклала «гуманістичні» і культурологічні основи для обґрунтування

нинішнього масштабного військового вторгнення до України. При цьому впродовж трьох десятиліть концепція такого «впливу» еволюціонувала від ідеологем «старшого брата» та меншовартості українства до маніакального заперечення існування України на історичній мапі світу [18]. Сьогодні, аналізуючи вектор російської пропаганди у ЗМІ, стає все більш очевидним, що політика росії за цей час трансформувалась від антиукраїнської пропаганди до пропаганди війни.

Як виявилось, застосування такої стратегії мало певні ефекти, одним із яких стало притуплення пильності світової спільноти щодо ймовірності відродження у цивілізованій спільноті неототалітаризму та неофашизму на рівні державної політики. Так, хоча на момент анексії в 2014 році українського Криму ряд країн не визнали псевдореферендум, а ключові міжнародні організації виступили з офіційними осуджувальними заявами, ефективність реакції світового співтовариства була зведена лише до корекції нормативно-правової бази, висловлення стурбованостей та засуджень російської вседозволеності [1]. Деякі більш рішучі акти урядів окремих країн також явно не відповідали дійсному характеру загрози. Зокрема, США та ЄС пригрозили російській федерації санкціями та закликали росію вийти з Кримського півострову, згодом ввели їх у дію. Натомість росія, звинувативши Сполучені Штати Америки та країни ЄС у фінансуванні та організації «державного перевороту» в Україні, показово ввела санкції у відповідь, продовжуючи при цьому ескалацію щодо України. Водночас, попри падіння російської валюти та російську фінансову кризу 2014-2016 років, зумовлені санкційним механізмом, санкції спричинили й контрнаслідки, коли низка країн-членів ЄС також зазнали певних економічних збитків [14].

До того ж США, Канада, ЄС та інші європейські країни (включаючи Україну) запровадили економічні санкції, спрямовані проти Криму. Завдяки цьому певні товари та технології стали недоступними для кримчан. Постраждали також туристичні й інфраструктурні сфери [7]. Круїзним суднам було заборонено заходити у визначені санкційними обмеженнями порти, а для жителів Криму були встановлені обмеження на поїздки та заморожені активи.

Водночас, далеко не весь світ, зокрема й європейські країни діяли узгоджено, що стимулювало російську владу до подальшого виношування імперських планів. Так, у складі ЄС до санкцій критично поставилися Італія, Угорщина, Греція, Франція, Кіпр і Словаччина. Показовими стали події червня 2017 року, коли Німеччина й Австрія розкритикували Сенат США за нові санкції проти росії, які стосувалися газопроводу «Північний потік-2» [12].

Ще більш непевною виявилась позиція міжнародних інституцій. Чи не найбільш практичним тут став мандат Спеціальної моніторингової місії ОБСЄ в Україні, створеної 21 березня 2014 року на запит уряду України до ОБСЄ та на підставі консенсусного рішення 57 країн-учасниць ОБСЄ. Місія, створена у складі 100 осіб строком на 6 місяців та збільшена до 500 осіб влітку 2014 року, після загострення конфлікту, врешті діяла до початку 2022 року (мандат місії продовжувався кожного року, останній річний період – з 1 квітня 2021 року по 31 березня 2022 року [13]. Проте вже після повномасштабного вторгнення навіть цей механізм виявився заблокованим.

Разом з тим, аналізуючи мету та власне діяльність місії, бачимо, наскільки кволими та обмеженими виявились спроможності міждержавних асоціацій та міжнародних інституцій перед посталими викликами. Декларуючи і реалізуючи мету роботи СММ – збір інформації, спостереження, встановлення фактів і звітування про ситуацію з безпекою по всій Україні, до повноважень СММ не увійшли висновки або будь-які розслідування. Як наслідок, попри те, що за час своєї роботи місія багаторазово фіксувала на Донбасі зразки військової техніки, що перебувала на озброєнні армії росії, у тому числі зразки сучасної військової техніки, яка не мала аналогів у світі, реальних практичних сценаріїв протидії подібній військовій присутності на території іншої суверенної держави представниками місії вироблено не було [19].

У вересні 2014 року європейська спільнота ініціювала стіл переговорів між Україною та росією. Врешті такі перемовини щодо врегулювання ситуації на Донбасі відбулися в Нормандському форматі (Україна-Німеччина-Франція-Росія), однак росія одразу ж усіма можливими способами розпочала процес долучення до переговорів ватажків

ОРДЛО аби легалізувати їх на політичній арені. І вкотре міжнародна спільнота на дії росії продовжувала «дивитися крізь пальці», розцінюючи її потужним гравцем на світовій політичній арені, акцентуючи на її ядерному арсеналі, про що сама росія неодноразово наголошувала. Наслідками такої політики стали мінські протоколи першої версії, укладачами яких, окрім учасників Тристоронньої контактної групи, стали представники квазіреспублік [9]. І практично одразу ж розпочинається примушування України до виконання катастрофічних, з огляду на її національну безпеку, рішень. Так, вже у 2015 році був підписаний «комплекс заходів щодо виконання Мінських угод», узгодження якого відбулось на саміті в Мінську 11-12 лютого 2015 року за участі лідерів Німеччини, Франції, України, Росії та самопроголошених «народних республік» у форматі «нормандської четвірки» (документ, який підписали, ще називають «Мінськ-2»). Резолюцією Ради безпеки ООН 2202 (2015) від 17 лютого 2015 відбулося його схвалення. Водночас було ухвалено «Декларацію Президента РФ, Президента України, Президента Франції та Канцлера Німеччини на підтримку Комплексу заходів щодо виконання Мінських угод, прийнятого 12 лютого 2015 року» [4].

Разом з тим, повноцінно узгодити прийняті рішення із системою міжнародного права не вдалося. З правової точки зору «Мінських угод» як міждержавної угоди не існує, натомість є лише Протокол (який містить низку домовленостей) і Комплекс заходів щодо їх виконання. При цьому мінські домовленості є, насамперед, політичними, а не юридично зобов'язуючими документами. Врешті вони не були ратифіковані українським парламентом як міжнародно-правові договори, що дозволило Україні переконати Захід, що Мінськ треба розділити на «безпекову» та «політичну» складові, при цьому не може бути прогресу в політичній до виконання безпекової (припинення обстрілів, відведення військ тощо) [2]. Україна роками наполягала на виконанні безпекової частини угод, російська сторона наполягала на політичній – фактичного визнання та легалізації квазіутворень на тілі Української держави. При цьому від світової спільноти путінський уряд домагався визнання росії у статусі геополітичного актора, апелюючи при цьому до власного ядерного потенціалу, гарантуючи у такому разі при-

пинення подальших провокацій та ескалацій. Паралельно з тим росія прагнула поширити свій вплив на Європу не лише страхітливим образом ядерної держави, а й інкорпоруючись у її енергетичний сектор [10].

Результатом політики «умиротворення агресора», яку сповідувало світове співтовариство і, зокрема, Європа, став тривалий конфлікт на сході України, що роками залишався жевріти. Однак світова спільнота не взяла до уваги, що така ж політика «умиротворення агресора» вже мала місце в історії ХХ ст. Саме оманливе умиротворення гітлерівської Німеччини призвело в результаті до мільйонних жертв. Можливо, боячись повторення цього сценарію Європа обрала максимально пацифістський шлях у вирішенні російсько-українського питання. Дещо послабила увагу світової спільноти до українського питання ситуація з пандемією ковіду. І лише на кінець 2021 року у світових таблоїдах та риториці світових лідерів почали звучати попередження щодо широкомасштабної війни, до якої готується росія. При цьому, на фоні збільшення військ на українському кордоні, міжнародна спільнота нарощувала рівень стурбованості, продовжуючи політику умиротворення ядерного агресора.

21 лютого 2022 року в. путін підписав укази про визнання російською федерацією «незалежності» «ДНР» та «ЛНР», що фактично підтвердило її свідомий односторонній вихід з Мінських домовленостей [17].

24 лютого розпочався новий етап російсько-української війни, що фактично поставив хрест на подальшій політиці загравання з агресором з боку світового співтовариства. Оголосивши «спеціальну воєнну операцію» з метою «демілітаризації та денацифікації України», російське військово-політичне керівництво дало відмашку армії, яка вже за кілька хвилин завдала ракетних ударів по всій території України, у тому числі по району столиці [6]. Російські бронетанкові та механізовані колони увійшли до України поблизу Харкова, Херсона, Чернігова, Сум з напрямків росії, Білорусі й тимчасово окупованого Криму. При цьому російський уряд фактично втягнув у війну Білорусь. Із прикордонних районів останньої неодноразово завдавалися ракетні удари, здійснювалися вильоти бойової авіації, відбувалася передислокація військ та їх забез-

печення. Проте, вже в перші дні агресії, російське військо зазнало надмірних втрат у живій силі та техніці. У своїй новітній історії, за оцінками українських та міжнародних експертів, Росія в жодній війні ще не зазнавала навіть приблизно таких великих втрат за такий короткий час. За визнанням західної розвідки, росія зустріла сильніший, ніж очікувала, опір, що зумовило матеріально-технічні проблеми для її військ, нестачу пального, боєприпасів і продовольства, підрив бойового духу нападників.

Водночас акт безпричинної агресії та стійкість української армії, готовність до опору українського суспільства і вищого політичного керівництва України «пробудили» світову спільноту. Відбулося доволі швидке об'єднання значної кількості країн світу навколо ідеї допомоги Україні, а запровадження потужних санкцій проти росії стало несподіваним ударом для країни-агресора [16].

Повертаючись власне до інформаційної складової російської військово-політичної агресії проти України, зазначимо, що активну інформаційну війну та шовіністичну пропаганду російська влада з моменту вторгнення лише посилювала. При цьому, окрім звичного дискурсу їй доводиться виконувати додаткове завдання – замилювати у інформаційному шумі резонуючі свідчення про масові випадки порушень правил ведення війни та воєнні злочини, які скоюють рашистські військові злочинці. Проте цього разу потужностей пропагандистської машини виявилось недостатньо. Саме такі численні свідчення злочинного, а то й відверто терористичного характеру, якими наразі заповнене інформаційне поле, врешті примусили світову спільноту піти далі політики «стурбованості діями з боку російської федерації». Міжнародні організації, засуджуючи дії агресора врешті розпочали, вслід за національними урядами, впроваджувати пакети санкцій проти широкого кола фізичних та юридичних осіб, причетних до війни та геноциду українського народу.

Євросоюз, як колективне міждержавне утворення ввів санкції, що стосуються фінансового, енергетичного, транспортного, технологічного сектору, а також візової політики. 27 лютого Євросоюз повністю закрив свій повітряний простір для будь-яких літаків, що належать, зареєстровані або контрольовані з росії, у тому числі для приватних літаків «олігархів».

Спільний пакет санкцій узгодили США, ЄС, Канада та Велика Британія. Зокрема, було заморожено резерви Центрального банку рф, що перебувають у банках країн G7 (йдеться про половину резервів ЦБ), скасовано програму «золотих паспортів» для інвесторів із росії, відключено частину російських банків від системи SWIFT. В подальшому цей пакет неодноразово доповнювався та розширювався [15]. Португалія призупинила видачу «золотих» віз громадянам росії. МЗС Британії повідомило, що підготувало чорний список російських багатіїв, яких Лондон вважає пов'язаними з владою росії.

27 лютого ЄС оголосив про заборону мовлення Russia Today, Sputnik та їхніх дочірніх організацій на своїй території, закриття неба ЄС для літаків, пов'язаних з росією, заморожування активів високопосадовців, представників російської еліти, а також членів їхніх сімей та посібників, і обмеження видачі їм «золотих паспортів».

Паралельно з санкціями міжнародні організації розпочинають активну військово-гуманітарну кампанію із надання всебічної допомоги для постраждалого цивільного населення України [3]. Від національних урядів провідних країн світу надходить суттєва допомога озброєнням та військовою технікою, водночас військовослужбовців ЗСУ розпочинають готувати на західних полігонах. При цьому характер такої допомоги постійно еволюціонує – від обмежених постачань до широкої номенклатури сучасного високотехнологічного озброєння. Для підвищення інтенсифікації цього процесу західними країнами-донорами вироблено узгоджувальну міжурядову платформу – Рамштайнський формат, яка дуже швидко постала, за влучним виразом українського міністра оборони О. Резнікова «справжньою коаліцією вільного світу на підтримку України» [11].

Ще однією потужною ініціативою від західної коаліції стає ініційований адміністрацією США закон про ленд-ліз для України. Так, з-під ініціативи президентської адміністрації, після впевненості у спроможності українського війська протистояти російській агресії, американський Сенат 7 квітня 2022 року ухвалив цей закон, що дозволило президенту Дж. Байдену використовувати ленд-ліз для прискорення надання військової техніки та інших поставок до України під час повномасштабного вторгнення російських

військ. Важливо також відмітити, що одним із головних аргументів, що вплинули на американський політикум при прийнятті рішення стала ефективна контрпропагандистська політика від України, коли відбулося широке оприлюднення злочинів російських військових у Бучі [5].

Новий етап санкційного тиску на російську федерацію розпочинається восени 2022 року. Зокрема, у листопаді, вслід за рішеннями кількох національних парламентів, Європарламент визнав росію державою-спонсором тероризму. Відповідна резолюція, ухвалена 23 листопада, закликала ЄС та його держави-члени розробити правову базу для визначення держав як спонсорів тероризму та механізми обмежувальних заходів проти цих країн. Відтак Європарламент закликав Раду ЄС згодом розглянути питання про внесення російської федерації до такого списку держав-спонсорів тероризму ЄС, а партнерів ЄС – вжити аналогічних заходів. Окрім того, євродепутати закликали ЄС та його держави-члени вжити заходів для ініціювання всеосяжної міжнародної ізоляції російської федерації, в тому числі щодо членства росії в міжнародних організаціях та органах, таких як Рада Безпеки ООН, та утриматися від проведення будь-яких офіційних заходів на території російської федерації [8].

Аналогічний законопроєкт також внесений на розгляд Конгресом США. Його ухвалення вкотре посилить тиск США та росію, дозволивши зокрема включити росію до чорного списку Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF). Водночас буде суттєво обмежено допомогу від Сполучених Штатів та від організацій, членом яких є США країнам, що зберігатимуть двосторонні партнерські відносини із росією; під тотальну заборону потрапить увесь російський оборонний експорт; ще більше посилиться контроль над експортом, реекспортом і передачею товарів подвійного використання; будуть запроваджені додаткові фінансові обмеження. Окрім цього, присвоєння такого статусу для росії розкриває безпосередньо для США право накладати вторинні санкції взагалі на усіх третіх осіб, які здійснюють будь-які операції з російською державою та суб'єктами приватного сектору. Така загроза вторинних санкцій очевидно збільшить імовірність дотримання вже наявних санкцій, таким чином посилив-

ши їхню ефективність [7]. Водночас, визнання росії державою-спонсором тероризму, як вказано у роз'ясненнях до внесеного законопроекту, приверне більше глобальної уваги до характеру дій російського режиму та звірств і терору, які він вчинив проти невинних українських громадян. Це дасть змогу ще більше посилити санкційний тиск, обсяг та ефективність заходів впливу на путінський режим.

Отже, якщо аналізувати риторику міжнародних організацій та світових лідерів впродовж останнього десятиліття, то стає все більш очевидним, що війна росії проти України кардинально змінила бачення та сприйняття реалій міжнародною спільнотою. Ставши жертвою російської інформаційно-пропагандистської кампанії, економічної та енергетичної політики, Європа вдруге за століття помиляється із обраною стратегією «умиротворення агресора». Європейська спільнота, тривалий час потураючи апетитам ядерного агресора та не бажаючи мати ескалацію на своїх східних кордонах, врешті постала перед загрозою континентальної війни небаченого розмаху. Відсутність твердості позицій від європейських лідерів та енергетичний гак, яким путінський режим утримував ряд країн, врешті породив тоталітарного монстра із безумним комплексом імперства та ідеологією реваншизму. Історія вкотре зробила виток, на якому гітлеризм замінено путінізмом, а в горнило війни окрім російського та українського народів ризикують втрапити й інші нації та народності світу. І лише усвідомлення цього, на фоні масштабних військових злочинів рашистів врешті примусило світову спільноту опам'ятатися і перейти від політики «глибокої стурбованості» до більш конкретних форм протидії божевіллю диктатора.

Список використаних джерел:

1. Russian official accuses US of fueling Ukraine. URL: http://www.presstv.com/detail/2014/02/06/349524/us-accused-of-funding-crisis.
2. Бабін Б. Мінські домовленості: «безальтернативні», але не обов'язкові. URL: https://lexinform.com.ua/dumka-eksperta/-minski-domovlenosti-bezalternatyvni-ale-ne-obov-yazkovi.
3. Базар О. ЄС забороняє мовлення Russia Today і Sputnik. *LB.UA.* URL: https://lb.ua/world/2022/02/27/507211_ies_zaboronyaie_movlennya_russia_today_i.html.

4. Баркар Д. Мінські угоди: хто не виконує домовленості? *Радіо Свобода.* URL: https://www.radiosvoboda.org/a/30432975.html.
5. Богданьок О. Закон США про ленд-ліз для України набув чинності – Стефанчук. *Суспільне. Новини.* URL: https://suspilne.media/287539-zakon-ssa-pro-lend-liz-dla-ukraini-nabuv-cinnosti-stefancuk.
6. Від «денацифікації» та «демілітаризації» – до «покласти край домінуванню США». Як змінювалася риторика Росії в ході війни проти України. URL: https://texty.org.ua/fragments/-106329/vid-denacyfikaciyi-ta-demilitaryzaciyi-do-poklasty-kraj-dominuvannyu-ssha-yak-zminyuvalasya-rytoryka-rosiyi-v-hodi-vijny-proty-ukrayiny.
7. Головна база даних санкцій накладених після нападу росії на Україну. URL : https://sanctions.nazk.gov.ua.
8. Європарламент визнав Росію державою-спонсором тероризму. *BBC NEWS Україна.* URL: https://www.bbc.com/ukrainian/news-63730807.
9. Коваль І., Губа Р. Переговори в «нормандському форматі» не принесли прориву. *DW.* URL: https://www.dw.com/uk/bahatohodynni-perehovory-v-normandskomu-formati-ne-prynesly-proryvu/a-60739632.
10. Остін: «Росія модернізує і нарощує ядерний арсенал». *Голос Америки.* URL: https://ukrainian.voanews.com/a/6870691.html.
11. Павлюк О. У Білому домі розповіли подробиці військової допомоги Україні після зустрічі на «Раммштайні». URL: https://suspilne.media/233001-u-bilomu-domi-rozpovili-podrobici-vijskovoi-dopomogi-ukraini-pisla-zustrici-na-rammstajni.
12. Солонина Є. «Північний потік-2»: затримка запуску, санкції та шанси для України. *Радіо Свобода.* URL: https://www.radiosvoboda.org/a/gas-ukrayina-rosiya-tranzyt-nordstream-2-ssha-sanktsiyi/31589375.html.
13. Спеціальна моніторингова місія ОБСЄ в Україні (закрито). URL: https://www.osce.org/special-monitoring-mission-to-ukraine-closed.
14. США і ЄС пригрозили Росії новими санкціями. URL: https://lb.ua/news/2014/06/21/270577_ssha_es_prigrozili_rossii_novimi.html
15. Ткачук Б. Євросоюз повністю закриває свій повітряний простір для Росії. Санкції накладуть і на російські ЗМІ. *Hromadske.* URL: https://hromadske.ua/posts/yevrosoyuz-povnistyu-zakrivaye-svij-povitryanij-prostir-dlya-rosiyi.
16. Цюпин Б. На саміті ЄС хочуть домовитися про допомогу Україні і санкції проти Росії. URL: https://ukrainian.voanews.com/-a/6877481.html.
17. Чайковська В. Путін підписав указ про визнання РФ незалежності «ЛДНР». *DW.* URL: https://www.dw.com/uk/putin-pidpysav-ukaz-pro-vyznannia-rf-nezalezhnosti-dnr-i-lnr/a-60865101.

18. ЯК змінюється антиукраїнська риторика рф. URL: https://cpd.gov.ua/main/yak-zminyuyetsya-antyukrayinska-rytoryka-rf/ukraine-rioters/
19. Яневський О. Опубліковано докази : зброя на Сході України походить з Росії. URL: https://ukrainian.voanews.com/a/-2559931.html

TRANSFORMATION OF INFORMATION POLICY OF INTERNATIONAL ORGANIZATIONS REGARDING RUSSIAN ARMED AGGRESSION AGAINST UKRAINE: FROM «CONCERN» TO SANCTIONS

Abstract. *The article analyzes the effectiveness of information policies of international organizations and the place of the international community in the process of russian-ukrainian war. Qualitative changes in activity are highlighted in international organizations activity, traced through their information a policy that has moved away from consultative participation and politics "appeasement of the aggressor" to sanction pressure on the aggressor and his retinue. The results of the study prove that the beginning of a large-scale war on in the eastern regions of Europe changed the rhetoric of "concern about the situation" from the side international organizations, for the practical participation of the latter in the confrontation with racism. The article also emphasizes the importance of strengthening sanctions from the side of the international community and providing a variety of assistance to Ukraine.*

Key words: *information policy, international organizations, russian-ukrainian war, policy of appeasement to the aggressor, sanctions.*

Отримано: 27.11.2022

УДК 342:[004.056.5:316.774]:355.48(470:477)«2014/…»

Я. Пінкас, *магістр політології*

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ (2014-2022 рр.)

Анотація. *У статті проаналізовано нормативно-правові акти 2014-2022 рр., що регулюють сферу інформаційної та кібербезпеки України. Інформаційну безпеку розглянуто, як частину національної безпеки, що особливо актуально під час російсько-української війни. Зосереджено увагу на загрозах інформаційній безпеці України, які виділенні в законах, що регулюють дану сферу.*

Ключові слова: *інформаційна безпека України, національна безпека, державна інформаційна політика, військовий стан, кібербезпека.*

Увага до проблеми гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, що пропагують ідеї сепаратизму, насильства та національної ворожнечі, є спробами руйнування національної ідентичності України, знищення національної злагоди, посягання на конституційний лад України та територіальну цілісність держави [3].

Нормативно-правове регулювання інформаційної безпеки, зокрема і кіберпростору здійснюється Конституцією України, законами України, указами Президента та постановами КМУ і ВРУ. Нова законодавча база почала формуватися із 2014 року із врахуванням нових загроз.

Відповідно до статті 17 Конституції України [4], забезпечення інформаційної безпеки є одною із найважливіших функцій держави, поряд із захистом суверенітету та територіальної цілісності. Її законодавче визначення зафіксовано в Указі Президента «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Відповідно до нього, інформаційна безпека України є складовою частиною національної безпеки України, станом захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства та держави. Тут також підкресле-

но, що інформаційною безпекою є забезпечення конституційних прав і свобод на користування інформацією, доступ до неї та її захист. Під захистом мається на увазі, протидія пропаганді, дезінформації та ворожим інформаційним операціям, а також безпека носіїв інформації [14].

26 квітня 2014 року у зв'язку із початком російської агресії на сході України та анексією півострова Крим, в.о. Президента було видано розпорядження «Про деякі заходи щодо забезпечення безпеки в інформаційній сфері» відповідно до якого Службі безпеки України було доручено забезпечення безпеки представників преси, а міністерству внутрішніх справ забезпечення безперебійної трансляції національного аудіовізуального продукту в південно-східних регіонах України та забезпечення охорони об'єктів наземної радіотелевізійної передавальної мережі в південно-східних регіонах України [8].

У зв'язку із посиленням російською федерацією поширення недостовірної та упередженої інформації з метою маніпулювання свідомістю українців, було введено в дію Рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [19]. В результаті було внесено зміни до деяких законів щодо протидії інформаційній агресії та визначено механізм протидії негативному інформаційно-психологічному впливу. Даний нормативно-правовий документ передбачав також й формування стратегії кібернетичної безпеки та розвитку інформаційного простору України.

Зміни було внесено в наступні закони: «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України». Вони мали відповідати міжнародним стандартам з питань інформаційної та кібернетичної безпеки та вдосконалити державну політику у сфері інформаційної безпеки.

Радою національної безпеки і оборони у 2016 році було розроблено Доктрину інформаційної безпеки України [20], правовою основою, якої стала Стратегія національної безпеки України, затверджена Указом Президента

від 26 травня 2015 року [21]. Метою Доктрини було уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії інформаційному впливу російської федерації в умовах розв'язаної нею гібридної війни.

Загрозами національним інтересам та безпеці України в доктрині було визначено дії російської федерації, зокрема здійснення спеціальних інформаційних операцій, спрямованих на деморалізацію особового складу ЗСУ, підрив обороноздатності, пророкування екстремістських проявів, панічних настроїв, дестабілізацію внутрішньополітичної ситуації та створення негативного іміджу України у світі. До того ж, у якості загроз зазначались: інформаційне домінування держави-агресора на тимчасово окупованих територіях, недостатня розвиненість національної інформаційної інфраструктури, неефективність державної інформаційної політики, недосконалість законодавства, пропаганда, поширення ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Національними інтересами державної інформаційної політики в Доктрині визначено:

- створення системи оцінки та реагування на інформаційні загрози;
- удосконалення повноважень державних регуляторних органів та захищеність від інформаційно-психологічних впливів;
- захист українського суспільства від інформаційного впливу та деструктивної пропаганди Російської Федерації [20].

Одним із пріоритетів системи національної безпеки України та важливою складовою захищеного інформаційного простору є забезпечення кібербезпеки.

У 2016 року Указом Президента було затверджено Стратегію кібербезпеки України [18], що стало важливим кроком у запровадженні довгострокового планування в цій сфері. За роки реалізації Стратегії було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття в 2017 році Закону України «Про основні засади забезпечення кібербезпеки України» в якому охаракте-

ризовано її суб'єкти, об'єкти, принципи та національну систему [11]. Законом визначалися правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [2, с. 102-103].

Окрім доктрини було прийнято й інші нормативно-правові акти. Зокрема, для активізації протидії російській інформаційній агресії та пропаганді було введено в дію Указ Президента України «Про рішення Ради національної безпеки і оборони України від 26 січня 2018 року «Про додаткові заходи щодо протидії інформаційній агресії Російської Федерації». Вміст документа доступний лише для службового користування [17]. Метою і завданням цього указу, як помітно із його назви, є додаткові заходи, що мають на меті протидію російській агресії в інформаційній сфері. Це ж підтверджується в одному із досліджень проведеним аналітичним центром Українського Католицького Університету, що стосувалось законодавчої бази щодо окупованої території України [1, с. 139].

У 2021 році було розроблено нову стратегію інформаційної безпеки. Однією з актуальних загроз і надалі визначалася *інформаційна політика російської федерації, а основними викликами залишилися*:

- інформаційний вплив російської федерації як держави-агресора на населення України;
- інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України;
- обмежені можливості реагувати на дезінформаційні кампанії [14].

Основною загрозою для України, відповідно до Стратегії кібербезпеки України, затвердженої указом Президента від 14 травня 2021 року, була гібридна агресія російської федерації проти України у кіберпросторі.

Відповідно, пріоритетами забезпечення кібербезпеки України було визначено:

- убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- європейська і євроатлантична інтеграція у сфері кібербезпеки [13].

Задля нормативного врегулювання процесу побудови та процедури акредитації з безпеки інформаційно-комунікаційних систем, призначених для оброблення і передачі інформації НАТО, з обмеженим доступом застосовуються різні нормативні документи НАТО та військові стандарти України, які перелічені в наказі Державної служби спеціального зв'язку та захисту інформації України [9].

З початком повномасштабного вторгнення 24 лютого 2022 року було прийнято ряд нормативно-правових актів, внесено зміни до деяких законів та затверджено нові укази Президента і постанови Верховної Ради України. Зокрема було прийнято Закон України «Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора» [5]. Відповідно до нього, заборонено прославлення російської агресії та російських силових структур, представлення збройного конфлікту, як громадянської війни. Додатково було внесено зміни до кримінального кодексу України.

Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» було об'єднано частину загальнонаціональних телеканалів у цілодобовому інформаційному марафоні «Єдині новини #UAразом», де в інформаційних та/або інформаційно-аналітичних передачах повідомляється та роз'яснюється об'єктивна інформація органів державної влади про становище та процес російсько-української війни [16].

Постановою Верховної Ради України «Про прийняття за основу проекту Закону України про внесення змін до Закону України «Про Державну службу спеціального

зв'язку та захисту інформації України», було підкреслено важливість забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі. Тому, одним із завдань даної служби стала протидія в кіберпросторі [7].

При державній службі спеціального зв'язку та захисту інформації діяв урядовий фельд'єгерський зв'язок. До його завдань входило приймання, обробка та доставка кореспонденції, що містить інформацію, що становить державну таємницю або призначена лише для службового користування. Оскільки документи передавались кур'єром, що є досить небезпечно і не актуально у сучасному світі, до законодавства було внесено зміни. У вищевказаному Законі України було виключено пункт 4, що забезпечував і регулював міжурядовий фельд'єгерський зв'язок [6].

Отож, Російська федерація і надалі залишається однією з основних загроз національній та зокрема інформаційній безпеці. Держава-агресор активно здійснює ворожі атаки в інформаційному просторі. Її дії базуються на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операціях, що доповнюють збройну агресію, впливаючи на морально-психологічний стан населення та роботу інформаційно-комунікаційних мереж. Різноманітні механізми для реалізації вищевказаних планів, активно застосовуються у російсько-українській війні проти України.

Російсько-українська війна стала вагомим поштовхом до суттєвих змін у вітчизняному законодавстві. Об'єктами ворожих атак є інформаційно-комунікаційна система та свідомість і мислення громадян України. Нова реальність повністю змінила державну політику в сфері інформаційної безпеки. З 2014 року чітко окреслено основні загрози та виклики, що спрямовані до України від російської федерації. Розроблено стратегію інформаційної безпеки, реалізація якої розпланована до 2025 року, та є частиною національної безпеки. Створено стратегію кібербезпеки та ведеться серйозна робота у напрямку виявлення та протидії загрозам у кіберпросторі. Вдосконалено та внесено зміни до низки законів України, що регулюють інформаційну безпеку у різних сферах життєдіяльності суспільст-

ва. Та все ж, важливим й надалі залишається реалізація всієї вітчизняної нормативно-правової бази задля суттєвого зміцнення позицій України.

Список використаних джерел:

1. Алієв А., Кривдик О., Кулаковська О., Федорчук С. Окуповані території та закон: аудит законодавства щодо АР Крим та ОРДЛО у 2014-2020 рр.: дослідження Аналітичного центр УКУ, 2021. 212 с. URL: https://ac.ucu.edu.ua/wp-content/uploads/2021/11/Final_Report_DLK_2014-2020-1.pdf.
2. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. №9. С. 100-108.
3. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision.* 2016. Vol. 2. Num. 1. С. 27-32. URL: https://science.lpnu.ua/sites/-default/files/journal-paper/2017/jun/4352/ilnicka0.pdf.
4. Конституція України від 01.01.2020 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр?find=1&-text=інформаційна+безпека#w1_.
5. Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора: Закон України від 03.03.2022 № 2109-IX. URL: https://zakon.rada.gov.ua/-laws/show/2109-20#Text.
6. Про внесення зміни до статті 10 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» у зв'язку з виходом України з Угоди про Міжурядовий фельд'єгерський зв'язок та Протоколу про внесення поправок до Угоди про «Міжурядовий фельд'єгерський зв'язок»: Закон України від 06.09.2022 № 2562-IX. URL: https://zakon.rada.gov.ua/-laws/show/2562-20#n2.
7. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 30.10.2022 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
8. Про деякі заходи щодо забезпечення безпеки в інформаційній сфері : Розпорядження в. о. Президента України від 26.04.2014 № 762/2014. URL: https://zakon.rada.gov.ua/-laws/show/762/2014-%D1%80%D0%BF#Text.
9. Про застосування окремих нормативних документів НАТО та військових стандартів України для побудови та акредитації з безпеки інформаційно-комунікаційних систем, призначених для оброблення (передачі) інформації НАТО з обмеженим доступом: Наказ державної служби спеціального зв'язку та захи-

сту інформації України від 19.08.2021 № z1181-21. URL: https://zakon.rada.gov.ua/laws/show/z1181-21#Text.
10. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення Ради національної безпеки і оборони від 01.05.2014 № n0004525-14. URL: https://zakon.rada.gov.ua/laws/-show/n0004525-14#n2.
11. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#Text.
12. Про прийняття за основу проекту Закону України про внесення змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі» : Постанова Верховної Ради України від 18.07.2022 № 2416-IX. URL: https://zakon.rada.gov.ua/laws/show/2416-20#Text.
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 № 447/2021. URL: https://www.president.gov.ua/documents/-4472021-40013.
14. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року №685/2021. URL: https://www.president.gov.ua/documents/-6852021-41069.
15. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року №685/2021. URL: https://www.president.gov.ua/documents/-6852021-41069.
16. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ президента України від 19.03.2022 №151/2022. URL: https://zakon.rada.gov.ua/laws/show/151/2022#Text.
17. Про рішення Ради національної безпеки і оборони України від 26 січня 2018 року «Про додаткові заходи щодо протидії інформаційній агресії Російської Федерації»: Указ Президента України від 09.02.2018 № 25/2018. URL: https://zakon.rada.gov.ua/laws/show/25/2018#Text.
18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України №96/2016. URL: https://www.president.gov.ua/documents/962016-19836.

19. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»: Указ в. о. Президента України від 01.05.2014 №449/2014. URL: https://zakon.rada.gov.ua/laws/show/449/2014#Text.
20. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25. 02. 2017 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.
21. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року №287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

REGULATORY AND LEGAL PROVISION OF INFORMATION SECURITY IN UKRAINE UNDER THE CONDITIONS OF THE RUSSIAN-UKRAINIAN WAR (2014-2022)

Abstract. *In this article has been analyzed the regulatory and legal acts since 2014 during 2022 years which regulate the sphere of information and cybersecurity of Ukraine. Informational security is reported as part of national security, which is especially relevant during the Russian-Ukrainian war. Attention is focused on the threats to informational security of Ukraine, which are issued in the laws regulating this sphere.*

Key words: *information al insurance of Ukraine, national security, state informational policy, military state, cyber security.*

Отримано: 19.11.2022

УДК 323.266+316.776.23]:355.48

В. Ю. Маркітантов, *кандидат політичних наук,*
доцент кафедри політології та філософії
Кам'янець-Подільського національного
університету імені Івана Огієнка

ФЕЙКИ ТА МАНІПУЛЯЦІЇ У СУЧАСНІЙ ІНФОРМАЦІЙНІЙ ВІЙНІ

Анотація. *Статтю присвячено інформаційній війні та зміні ролі інформації у забезпеченні запланованих результатів. Визначено напрямки інформаційного фронту. Зазначено, що однією з цілей інформаційної війни є маніпулювання громадською думкою та масовою свідомістю. Розглянуто фейки як один із головних інструментів інформаційної війни.*

Ключові слова: *інформаційна війна, маніпуляція, фейк, «фабрика тролей».*

Усі масштабні збройні конфлікти кінця XX – початку XXI століття супроводжувалися масованими інформаційними атаками. Чим сучасніше суспільство, тим більше воно залежить від інформації та засобів її надання, а, отже, й уразливіше в інформаційній війні. Сьогодні у багатьох арміях світу діють спеціалізовані підрозділи відповідного профілю.

Інформаційна війна безпосередньо не спричиняє кровопролиття та руйнування, а її хід не призводить до жертв, що часто породжує надто безпечне ставлення до неї. Натомість, шкода, яку може завдати інформаційна війна суспільству за масштабом та значенням не поступається, а іноді навіть й перевищує наслідки конвенційної війни. В цих умовах роль інформації поступово змінювалась, еволюціонуючи від допоміжної сили в умовах війни до основної, що безпосередньо впливає на її результат [9]. Сьогодні інформація перетворилась на один із найнебезпечніших видів зброї. Використання компроматів, поширення бруду та неправдивої інформації, прагнення за допомогою інформації ввести в оману стали звичним способом життя. Вона має значний вплив на маси, вдале маніпулювання свідомістю яких дозволяє досягти практично будь-якої мети: «знищити» опонентів, прибрати з дороги конкурентів або ж розпалити війну [1].

За визначенням поданим у Енциклопеції сучасної України, інформаційна війна трактується як «вплив на населення іншої країни у мирний або військовий час через розповсюдження певної інформації та захист громадян власної країни від такого впливу» [8]. У той же час І. Жаровська та Н. Ортинська, зазначають, що інформаційну війну в сучасній науці трактують як «вплив на цивільне населення і / або військовослужбовців іншої держави шляхом поширення певної інформації» [2, с. 59].

Основними об'єктами протистояння під час інформаційної війни є інформаційний простір, інформаційні ресурси та інформаційно-технічні системи управління, зв'язку, навігації, комп'ютерні мережі, радіоелектронні засоби тощо. Основні її завдання полягають у підриві морально-психологічного стану, зміні поведінкового та емоційного настрою, дезорієнтації та дезінформації, послабленні певних традицій та переконань, забезпеченні ринків збуту, залякуванні власного народу образом ворога, а ворога – своєю могутністю [8].

На думку американських фахівців, до елементів інформаційної війни варто відносити: збір розвідувальної інформації, дезінформацію, психологічні операції, фізичне руйнування інформаційних ресурсів противника (включно з застосуванням електромагнітного впливу), атаки (фізичні та електронні) його інформаційних структур, ураження комп'ютерними вірусами обчислювальних мереж і систем противника, проникнення в його інформаційні мережі тощо, а також відповідні заходи захисту власних інформаційних ресурсів [див.: 2, с. 58].

В. Горбулін, характеризуючи інформаційну складову «гібридної війни», зазначав, що її інформаційний фронт розгортається одночасно за кількома напрямками:

- серед населення в зоні конфлікту;
- серед населення країни, проти якої вчинено агресію, але територія якої не охоплена конфліктом;
- серед громадян країни-агресора;
- серед міжнародної спільноти [див.: 3].

Так, наприклад, російська інформаційна війна спрямована на вплив на свідомість мас як всередині власної країни, так і за її межами, на підштовхування їх до циві-

лізаційної боротьби між євразійською культурою та Заходом. До того ж вона зорієнтована на широку російськомовну діаспору, що була розділена у пострадянський час по різних країнах. Інформаційна війна також є основним інструментом посилення дипломатичного впливу держави та досягнення своїх зовнішньополітичних цілей. Вона безпосередньо обслуговує геополітичні інтереси росії, яка претендує на статус цивілізації. Шляхом скоординованої маніпуляції через усі інформаційні канали (включно з газетами, телебаченням, інтернет-сайтами, блогами та іншими ресурсами), російські фахівці із зони конфлікту створюють віртуальну реальність, яка або впливає на сприйняття або ж (серед частини російськомовної аудиторії) замінює фактичну правду на проросійську фантастику [4, с. 67-68].

Особливість інформаційної війни полягає не лише у впливі найсучаснішими засобами, але й у переважній непідконтрольності ресурсів, що слабко підлягають правовому регулюванню, а отже активному використанні неправдивої та спотвореної інформації з метою маніпулювання свідомістю [2, с. 60]. Отже, однією з цілей інформаційної війни є маніпулювання громадською думкою та масовою свідомістю. Воно полягає у програмуванні думок і бажань мас, їх настроїв та психічного стану задля забезпечення бажаної для маніпулятора поведінки. Маніпуляція визначається первинною формою взаємодії, за якої одна сторона змушує іншу сторону діяти в її інтересах і відповідно до її програми таким чином, що інша сторона не розпізнає та не опирається цьому. Маніпулятивного впливу важко уникнути, оскільки маніпулятор апелює до базових потреб та мотивів, що не може не привернути увагу та не викликати емоції у тих, на кого він здійснюється [5, с. 81].

В основу такої маніпуляції покладено: підміну основної думки (тези) підтвердження; підміну спростування тези спростуванням аргументу; розширення або скорочення тези; втрату тези; видавання фальшивих суджень за істинні; псевдопричинний зв'язок; нав'язані наслідки; порочне коло у доведенні; некоректну дихотомію; створення видимості доведеності; передбачення підстави; базовий прогноз; ухиляння від доказів тощо [7, с. 75].

Одним із головних інструментів інформаційної війни є фейки – неправдива інформація, навмисно поширювана особами, що переслідують певні, зазвичай політичні, цілі, або прагнуть заробити на онлайн-трафіку [10]. На думку І. Мудрої таке трактування не відображає суті фейку, оскільки під ним варто розуміти підробку, фальшивку, поширювану спеціально для дезінформації аудиторії [6, с. 184]. Фейки поширюються переважно через ЗМІ та соціальні мережі. Мета фейкової інформації полягає у введенні людей в оману. Популярність фейкових повідомлень у ЗМІ та у соціальних медіа гарантує суспільству щоденну дозу дезінформації, чуток та відвертої брехні. Вести безперервну боротьбу з таким інструментом інформаційної війни складно, оскільки не завжди вдається відрізнити правду від обману.

Для поширення фейків у соціальних мережах часто створюють «фабрики інтернет-тролей», до яких входять молоді люди, які видають себе за справжніх учасників мережі, що централізовано й масово поширюють провокаційну та скандальну інформацію. Метою такої діяльності є психологічна обробка громадян не лише протиборчої сторони, але й інших країн, у тому числі власних інтернет-користувачів. «Фабрики тролей» працюють за принципом: «брехня, яку повторюють багато разів, стає правдою». Їх працівники отримують завдання від «кураторів» створити враження масового протесту або існування альтернативної думки [3].

Основна мета фейків як засобів ведення інформаційної війни – посіяти сумніви та переконати громадськість в правдивості інформації, що поширюється. До їх завдань входять: дезінформація громадськості; популяризація власного бачення, політики чи позиції; розпалювання агресії; розхитування позиції людини та змушення її сумніватися; сіяння паніки; зміна усталеної громадської думки; спонукання до певних дій; активізація уваги та суспільного інтересу; переконування сфабрикованими фактами; залякування громадськості тощо. Враховуючи вищезазначене, І. Мудра пропонує наступне визначення фейку – «це спеціально створена новина, подія чи журналістський матеріал, який містить неправдиву або перекручену інформацію, що дискримінує певну людину чи групу осіб в очах аудиторії» [6, с. 185].

Не треба боротися з фейками, їх потрібно розвінчувати та висміювати, але ні в якому разі не можна поширювати. На думку О. Покальчука як власне фейкові новини, так і їх обговорення й боротьба з ними створюють «інформаційний шум», який відволікає від значно важливіших проблем та інформації. Для цього вони й створюються та поширюються. Разом із тим, вони спрямовані на формування в людей відчуття невпевненості та страху, їх деморалізацію, що мало би позбавити мотивації працювати та захищати свою країну, довіряти власним джерелам інформації [див.: с. 186].

Отже, в сучасному світі, коли інформація стає все більш доступною, фейки та маніпуляції перетворюються на невід'ємну частину суспільного життя, поширюючись завдяки розвитку технологій та росту соціальних мереж. Інтернет і соціальні мережі дають необмежені можливості для розповсюдження інформації, але вони також стають й місцем, де легко можуть поширюватися фейки та маніпуляції. Відповідно, роль фейків і маніпуляцій у інформаційній війні є неминучою.

Список використаних джерел:

1. Бабенко Ю. Інформаційна війна – зброя масового знищення! Українська правда. 20.04.2006. URL: https://www.pravda.com.ua/-rus/articles/2006/04/20/4399050/
2. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка».* Серія: «Юридичні науки». 2020. Т. 7. № 2. С. 56-61. URL: https://science.lpnu.ua/sites/default/-files/journal-paper/2020/sep/22118/10.pdf.
3. Зозуля О. Фейк як інструмент інформаційної війни. *Юридична газета online*. 2019. № 19. URL: https://yur-gazeta.com/-publications/practice/inshe/feyk-yak-instrument-informaciy-noyi-viyni.html.
4. Маркітантов В.Ю., Рибщун О.В., Столяр Ю.В. Російська гібридна війна: від доктрини до тактики: навчальний посібник. Кам'янець-Подільський: ТОВ «Друкарня «Рута», 2018. 234 с.
5. Младьонова О. Маніпулювання суспільної свідомістю як технологія ведення інформаційної війни. *Вісник Харківського національного університету імені В.Н. Каразіна.* Серія «Питання політології». Харків, 2017. Вип. 32. С. 79-82.
6. Мудра І. Поняття «фейк» та його види у ЗМІ. *Теле- та радіожурналістика.* 2016. Вип. 15. С. 184-188. URL:

http://publications.lnu.edu.ua/collections/index.php/teleradio/-article/viewFile/694/699publications.lnu.edu.ua/collections/index.php/teleradio/article/viewFile/694/699.
7. Невельська-Гордєєва О., Нечитайло В. Маніпуляції як засіб інформаційно-психологічного впливу в інформаційній війні. *Вісник Національного юридичного університету імені Ярослава Мудрого.* 2021. № 3 (50). С. 71-83. URL: http://fil.nlu.edu.ua/article/view/235389.
8. Пилипчук Р. Інформаційна війна. *Енциклопеція сучасної України* : енциклопедія / ред.: І.М. Дзюба, А.І. Жуковський, М.Г. Железняк та ін.; НАН України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, 2011. Т. 11. URL: https://esu.com.ua/article-12460.
9. Яковчук В., Малець Б. Борзов Ю. Інформаційні війни в сучасному світі. *Інформаційна безпека та інформаційні технології*: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів. 2020. С. 75-78. URL: https://sci.ldubgd.edu.ua/-bitstream/123456789/7424/1/Інформаційні%20війни%20в%20сучасному%20світі.pdf.
10. Fake News: Develop Your Fact-Checking Skills: Some News Literacy Vocabulary. *Benedictine University Library.* URL: https://researchguides.ben.edu/c.php?g=608230&p=4220191.

FAKES AND MANIPULATIONS IN THE MODERN INFORMATION WAR

Abstract. *The article is devoted to the information war and the changing role of information in ensuring planned results. The directions of the information front have been determined. It is noted that one of the goals of the information war is the manipulation of public opinion and mass consciousness. Fakes are considered as one of the main tools of the information war.*

Key words: *information war, manipulation, fake, «troll factory».*

Отримано: 18.11.2022

ЗМІСТ

Міністерство освіти і науки України
Кам'янець-Подільський національний університет
імені Івана Огієнка

НАУКОВЕ ВИДАННЯ

ЗБІРНИК МАТЕРІАЛІВ

МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»

ЕЛЕКТРОННЕ ВИДАННЯ

Підписано 09.02.2023. Формат 60x84/16. Гарнітура «Книжник».
Об'єм даних 1 Мб. Обл.-вид. арк. 5,8. Зам. № 1019.

Кам'янець-Подільський національний університет
імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.

Виготовлено в Кам'янець-Подільському національному
університеті імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.