ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351:354.1:327.8
DOI https://doi.org/10.32782/TNU-2663-6468/2023.5/16

Бондар В.Т.
ПЗВО «Київський міжнародний університет»

ФАКТОР ПЕРСПЕКТИВИ США ТА ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ: УДОСКОНАЛЕННЯ СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Статтю присвячено дослідженню практики вироблення владою США державних підходів з протидії дезінформації через призму концепції фактора перспективи країни у гібридній війні, яка стала об'єктом інформаційно-психологічного впливу з боку країни-агресорки та пов'язаних з нею зовнішніх акторів. Предмет вивчення полягає у розгляді законодавчих ініціатив, експертних рекомендацій стосовно вдосконалення системи національної безпеки у напрямі посилення функціональної спроможності компонентів системи державного управління, впровадження інноваційних організаційно-адміністративних рішень, розширення інституційних механізмів формування державно-приватного партнерства з протидії дезінформації.

Метою є дослідження підходів влади по вдосконаленню механізмів державного управління системою національної безпеки США у контексті фактора перспективи цієї країни як об'єкта інформаційної складової гібридної війни. У праці виокремлено особливості модернізації системи державного управління Сполучених Штатів Америки заснуванням при одному із ключових федеральних стейкхолдерів – Національній розвідці − незалежних центрів з розподілом їх функціональних повноважень.

Зроблено висновки щодо підходів американських законодавчих органів у формуванні інституційного середовища по залученню незалежних і приватних суб'єктів та інститутів громадянського суспільства до опосередкованої партнерської взаємодії з державними ключовими стейкхолдерами сектора безпеки через безпосередню співпрацю з центрами консультативно-дорадчого спрямування при федеральному відомстві. Відображено перспективи подальших наукових розвідок з предмета дослідження. В якому смислі позитивний досвід США може становити інтерес для вітчизняних стейкхолдерів сектора безпеки, регулювання інформаційного і медійного простору: розвитку двосторонніх американо-українських зв'язків; гарантуванні стабільності системи національної безпеки України, у тому числі з урахуванням фактора перспективи обох країн як об'єкта інформаційної складової гібридної війни.

Ключові слова: *державне управління, фактор перспективи, інформаційно-психологічний вплив, протидія дезінформації, система національної безпеки.*

Постановка проблеми. На засіданні Національного прес-клубу в м. Вашингтон (вересень 2023 р.), Нобелевська лауреатка Марія Ресса зазначила, що до кінця 2024 року стане зрозумілим майбутнє демократії: «чи виживе вона, чи помре», а в центрі цього – «боротьба за правду». «Не матимемо цілісності фактів, не матимемо цілісності виборів [1]». Причиною, на думку філіппінської журналістки-розслідувачки, є використання зовнішніми акторами в цифровому і медіа просторі досягнень у галузі інформаційних технологій, штучного інтелекту з деструктивною метою. Звідси – розгортання світової тенденції інтенсифікації інформаційного й психологічного тиску на публічний простір, державне регулювання медіа та інформаційного середовища, медіаграмотність населення.

Правозахисною організацією Фрідом Хаус у документі під назвою «Свобода у світі – 2023. Відзначаючи 50 років у боротьбі за демократію» (2023 р.) наголошується, «що «рівень свободи у глобальному вимірі знижується упродовж 17 років поспіль [2]». Це віддзеркалює наслідки транзиту країн до шостого технологічного укладу,

виникнення перед людством викликів, пов'язаних з протидією дезінформації. Використанням значною мірою авторитарними режимами соціальних комунікацій та інформаційних засобів для маніпулювання громадською думкою і підриву довіри до державних інституцій, застосуванням маніпулятивних PR-технологій, втручанням у виборчі кампанії.

У 2020 році чисельність країн, проти яких застосовувалися інформаційні засоби зі шкідливим контентом зросла до 81-ї у порівнянні з 70-ю у попередньому періоді, за переважаючої ролі рф, КНР, Ірану [3]. Важливості загрозам напередодні виборчої кампанії-2024 в США додають висновки експертів Міністерства національної безпеки, позиціонуючи цілеспрямованість акторів походженням із цих трьох країн як джерело інформаційно-психологічного впливу, створенням порівняно дешевого синтетичного текстового, візуального й аудіо контенту високої якості [4].

Аналіз останніх досліджень і публікацій. Дослідження протидії дезінформації набуло першості у працях вітчизняних науковців О. Бодрука, М. Вавринчука, С. Горбатюка, В. Горбуліна, Р. Марутян, М. Орел, Г. Ситника та інших. Серед іноземних – відзначаємо Д. Бочковського, С. Бредшоу, А. Глапяк, Ф. Говарда, Дж. Онга, П. Стоктона, С. Франк й ін. Разом з аналітичними оглядами дослідницьких зарубіжних інституцій, це сформувало наукове підґрунтя для аналізу вдосконалення механізмів державного управління щодо гарантування стійкості системи національної безпеки США в умовах сучасних зовнішніх інформаційних загроз.

У звіті корпорації Майкрософт «Загрози в цифровій сфері походженням зі Східної Азії зростають за масштабністю та ефективністю» (2023 р.) зокрема йдеться, що співробітники китайських спеціальних служб усе частіше застосовують генеративний штучний інтелект у заходах впливу. До прикладу, з березня 2023 року експертами зафіксовано використання прокитайськими акторами, що асоціюються зі спеціальними службами КНР, генерованого візуального контенту в американських соціальних медіа для надання повідомленням більшої достовірності. За сутністю, інформаційно-психологічні акції упродовж місяця фокусувалися на темах першочергового значення для американського суспільства: збройне насильство, приниження місцевих політичних діячів і державної символіки США [5].

Узагальнення аналізу прокремлівської кампанії дезінформації під час виборів президента США 2016 року в останніх дослідженнях, серед основних висновків знаходимо. На переконання С. Франк, на той період часу американська влада, *по-перше*, була неготовою протидіяти дезінформації; *по-друге*, спроможність російських акторів здійснювати інформаційно-психологічний вплив на американське громадянське суспільство із застосуванням інформаційних засобів – достатньо висока [6]. Відзначаємо припущення П. Стоктона стосовно використання в 2024 році росією та КНР тактики, апробованої владою рф 2014 року в тимчасово окупованому Криму. За якої державні інституції України було від'єднано від каналів комунікації з населенням півострова, а етер заповнено російськими контрольованими телевізійними станціями для розповсюдження у регіоні дезінформації про природу і масштаби військового нападу. Аналогічно, на думку експерта, висока імовірність загрози дестабілізації системи комунікацій президента США з суспільством й одночасним розгортання через онлайн платформи акторами, підконтрольними росії або Китаю, шкідливого континенту для насичення інформаційного та медійного вакууму, що утворюватиметься [7]. Виходячи з цього, на нашу думку, якщо до 2016 року фактор перспективи США відображав їх статус як спостерігача − з початком військової агресії рф проти України у 2014 році, то за перетворенням політичного устрою і публічного простору заокеанської країни на ціль деструктивного інформаційного впливу країни-агресорки, послідувала трансформація Сполучених Штатів Америки на об'єкт інформаційної складової гібридної війни.

Враховуючи роль США як стратегічного партнера і союзника України, для вітчизняної сфери державного управління потреба в ознайомленні з процесами вдосконалення американською владою системи державного управління, зміцнення спроможності ключових стейкхолдерів сектора безпеки з протидії зовнішнім загрозам.

Мета статті – дослідити підходи влади по вдосконаленню механізмів державного управління системою національної безпеки США у контексті фактора перспективи цієї країни як об'єкта інформаційної складової гібридної війни.

Виклад основного матеріалу. За концептуального підходу, автори монографії «Світова гібридна війна: український фронт» (2017 р.) підкреслюють значення фактора перспективи для влади країни, інституційні основи якої стали предметом інформаційного тиску агресора – чинника, що перетво-

рює її зі спостерігача конфлікту на його повноцінного учасника як об'єкта гібридного нападу [8].

Отже, з точки зору об'єктності США, фактор перспективи спонукає владу до модернізації механізму системи державного управління. Як зауважує М. Матишак, першість за інноваційними підходами федерального уряду в оборонному плануванні, проведенні інформаційних операцій доповненням чи підсиленням Конгресом й Виконавчим офісом Президента США повноважень тих стейкхолдерів, які вже функціонують і спеціалізуються на протидії втручанню у вибори, деструктивним інформаційним засобам відносно системи демократичного управління. Насамперед, на думку фахівця, із найбільш придатних спеціалізованих структур, це оперативна група з протидії іноземному впливу у складі Міністерства національної безпеки разом з подібною за профілем − оперативною групою іноземного впливу у підпорядкуванні ФБР. До інших перспективних механізмів при плануванні, ним віднесено: координаційний міжвідомчий Центр глобального залучення при Державному департаменті США; програми Федерального агентства з надзвичайних ситуацій та Міністерства національної безпеки щодо протидії дезінформації під час надзвичайних подій [9]. Вважаємо, що розширення повноважень діючих спеціалізованих підрозділів у посиленні їх функціональної спроможності, модернізація механізмів державного управління активізацією федеральних програм, має інноваційну перспективу вдосконалення системи національної безпеки з урахуванням особливостей поведінки компонентів зовнішнього середовища.

Інші підходи вдосконалення системи національної безпеки, які, на наш погляд, слід виокремити в обговоренні, це розширення інституційної бази створенням вузькоспеціалізованих відомств. Відзначаємо заснування при Офісі Директора Національної розвідки США у 2021 році Центру протидії деструктивному іноземному впливу, який був перейменований 2022 року на Центр іноземного деструктивного впливу (Foreign Malign Influence Center) [10]. За задумом, Центр повинен стати *пріоритетною* установою в ієрархічній структурі сектора безпеки США по *оцінюванню розвідувальної інформації* на предмет виявлення ознак деструктивного впливу акторів іноземних держав з метою аналізу та інформування ключових профільних стейкхолдерів про таку активність, а також членів Конгресу і представників політичних кіл. Його діяльність під мотто: «Викриття обману на захист свободи».

Також нашої уваги заслуговують законодавчі ініціативи. До прикладу, у § 3369 «Спільні дії щодо виявлення та протидії іноземним операціям впливу» Розділі 50 «Війна та національна безпека» Кодексу США, Конгресом визнано проведення росією через її головне розвідувальне управління спільно з асоційованими організаціями, передусім «російським агентством інтернет-досліджень», інформаційної війни проти США й їх союзників і партнерів задля реалізації стратегічних інтересів рф. Враховуючи, що прокремлівські актори приховано використовують американські приватні онлайн платформи соціальних комунікацій, відповідно до Кодексу, як першочергове реагування державою визнається невідкладне застосування вимог відносно провайдерів − самостійно виявляти та сприяти видаленню супротивної сторони шляхом співпраці на постійній основі між собою, з незалежними організаціями, індивідуальними дослідниками. З метою нагляду, директору Національної розвідки США у координації з міністром оборони було доручено створити в червні 2021 року Центр з аналізу загроз і даних соціальних медіа (Social Media Data and Threat Analysis Center) [11] зі статусом незалежної, неприбуткової організації, фінансуванням за кошт грантів чи на контрактній основі. Передбачено механізм звітування про проведену роботу перед Конгресом, як одна із форм громадського контролю – періодична публікація звітів.

Наступний крок законодавця, це закріплення повноважень і сфери компетенції зазначеного вище Центру в окремому Законі Палати представників [12]. Виходячи з його положень, систематизуючи одинадцять головних завдань, до основних напрямів спеціалізації можна віднести, *по-перше*, ключову роль Центру по *координації взаємодії* між компаніями з надання послуг у соціальних мережах та третьою стороною з числа незалежних експертів, НУО, журналістів, федеральних дослідницьких й впроваджувальних центрів, академічних кіл, медіа, зарубіжних партнерів з метою проведення спільного аналізу даних соціальних медіа, іноземних акцій впливу, хакерських атак, витоку інформації, інших протизаконних дій, джерел фінансування.

По-друге, повноваження з розробки та оприлюднення: порядку обміну інформацією між державними інституціями, представниками приватного і громадського сектору; критеріїв й стандартів кваліфікації приватних суб'єктів, індивідуальних дослідників для визначення можливості

залучення до взаємодії з Центром тих суб'єктів, які відповідають встановленим вимогам; етичних стандартів для розслідування діяльності іноземних акторів що становлять загрозу, з подальшим використанням результатів за гарантування нерозголошення особистих даних користувачів соціальних мереж та інформаційних масивів онлайн і медіа операторів; порядку проведення технічного й операційного контролю, аналізу договірної бази задля уникнення зловживання при поводженні з даними включаючи аудиторські перевірки, огляд апаратних чи програмних засобів або обладнання; критеріїв та умов, відповідно до яких Центр може передавати інформацію стейкхолдерам сектора безпеки з даними на предмет загроз відносно системи національної безпеки чи порушень чинного законодавства внаслідок діяльності зовнішніх акторів з використанням соціальних мереж; стандартів даних з метою гармонізації на федеральному рівні технічних умов поводження з інформацією.

По-третє, проведення ідентифікації спільно з компаніями-провайдерами даних і метаданих, які містять ознаки загроз походженням від мережі іноземних акторів, що використовують дану платформу для надання доступу державним інституціям по дослідженню їх активності та аналізу.

По-четверте, право на формування архіву зведених даних про іноземний вплив і кампанії дезінформації для вироблення спільних підходів щодо сутності загроз, сприяння експертизі за дотримання вимог конфіденційності.

Таким чином, перебіг президентських кампаній 2016 та 2020 років, спроби захоплення Конгресу й пов'язані з цим загрози стабільності системи національної безпеки, змушують владу США, поряд з необхідністю розширення компетенції діючих державних інституцій, також активізувати рівною мірою і суб'єкт-суб'єктну взаємодію у площині «державні інституції – громадянське суспільство». Імплементувати підходи з передбачення додаткових інституційних механізмів, інноваційних організаційно-адміністративних рішень. Впроваджувати на законодавчому й виконавчому рівні узгоджену політику раціонального залучення інститутів громадянського суспільства, приватних та незалежних суб'єктів інформаційного і медіа середовища до партнерства з державою.

Висновки. Виходячи із обговореного, можна узагальнити результати дослідження.

Відзначаємо цілеспрямовану політику американської влади зі створення незалежного експертно-аналітичного середовища поєднанням компонентів системи державного управління з елементами громадянського суспільства для вироблення спільних підходів регулювання інформаційного і медіа простору з метою спільної та узгодженої протидії деструктивному інформаційно-психологічному впливу зовнішніх акторів.

Серед інноваційних підходів – передбачення організаційно-адміністративних рішень задля посилення функціональної спроможності суб'єктів системи державного управління при плануванні і реалізації політики з протидії дезінформації, активізації державних програм, стимулювання діяльності профільних оперативних груп різних федеральних відомств.

У зміцненні системи державного управління виокремлюємо створення при Національній розвідці двох незалежних центрів консультативно-дорадчого спрямування, наділених функціональними повноваженнями різнопланової дії з: оцінювання розвідувальної інформації на предмет ознак деструктивного впливу від кампаній дезінформації; координації між ключовими стейкхолдерами сектора безпеки та інститутами громадянського суспільства.

Послідовним можна охарактеризувати реагування американського законодавця по вдосконаленню інституційного середовища, визнанню одним із головних об'єктів інформаційно-психологічних загроз в інформаційному і медіа просторі цілеспрямованої дії зовнішніх акторів, пов'язаних з рф, КНР, Іраном.

Перспективні подальші теоретичні дослідження й ознайомлення з реагуванням США на зовнішні інформаційні загрози як країни-об'єкта російської агресії. Можливий практичний досвід Сполучених Штатів Америки з вдосконалення інституційного середовища, впровадження інноваційних організаційно-адміністративних рішень для вітчизняних стейкхолдерів сектора безпеки у напрямі вдосконалення системи національної безпеки України.

Не виключаємо контекст двосторонніх відносин − адже США та Україна як країни-об'єкти інформаційної складової гібридної війни – в смислі модернізації двосторонніх механізмів взаємодії на основі застосування симетричних заходів, синхронізації впровадження інноваційних організаційно-адміністративних рішень. Формування рамок євроатлантичної інтеграції між профільними відомствами зазначених країн, а також інших союзників.

Список літератури:

1. World Faces «Tech-Enabled Armageddon», Maria Ressa Says. September 05, 2023. URL : https://www.voanews.com/a/world-faces-tech-enabled-armageddon-maria-ressa-says-7256196.html?utm_source=substack&utm_ medium=email.
2. Freedom in the World. Marking 50 Years in the Struggle for Democracy. *Freedom House.* March 2023. URL : https://freedomhouse.org/ sites/ default/ files/2023-03/FIW_World_2023_ DigtalPDF.pdf.
3. Bradshaw S., Bailey H., Howard, P. (February 22, 2021). Industrialized Disinformation. Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute, University of Oxford. URL : https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/ CyberTroop-Report-2020-v.2.pdf.
4. Homeland Threat Assessment 2024. *Office of Intelligence and Analysis. Homeland Security.* 23-333-IA. URL : https://cyberscoop.com/wp-content/ uploads/sites/3/2023/09/2024HTA.pdf.
5. Digital threats from East Asia increase in breadth and effectiveness. *Microsoft Threat Intelligence.* September 2023. URL : https://query.prod. cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW.
6. François C. Actors, Behaviors, Content: A Disinformation ABC. Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses. *Transatlantic Working Group*. Philadelphia, USA; Amsterdam, the Kingdom of the Netherlands. 2019. 12 pp.
7. Stockton Paul. Defeating coercive information operations in future crises. National Security perspective. *John Hopkins Applied Physics Laboratory* (NSAD-R-21-002), 2021. URL : https://www.jhuapl.edu/sites/ default/ files/ 2022-12/DefeatingCoerciveIOs.pdf.
8. Світова гібридна війна: український фронт : моногр. / за заг. ред. В.П. Горбуліна. К. : НІСД, 2017. 496 с.
9. Matishak Martin. Intelligence Community Creating Hub to Gird against Foreign Influence. *Politico*, April 26, 2021. URL : https://www. politico.com/ news/ 2021/04/26/intelligence-community-hub-foreig n-influence-484604.
10. The Intelligence Community's Foreign Malign Influence Center (FMIC). *Congressional Research Service in Focus (IFI 2470)*, August 09, 2023. URL : https://sgp.fas.org/crs/intel/IF12470.pdf .
11. 50 U.S. Code § 3369 – Cooperative actions to detect and counter foreign influence operations. *Legal Information Institute. Cornell Law School.* URL : https://www.govinfo.gov/content/pkg/USCODE-2021-title50/pdf/USCODE-2021-title50-chap44-sec3001.pdf.
12. A Bill. To make certain modifications relating to the Social Media Data and Threat Analysis Center. *H.R. 8409. In the House of Representatives.* July 18, 2022. URL : https://www.govinfo.gov/content/pkg/BILLS-117hr8409ih/ pdf/BILLS-117hr8409ih.pdf.

Bondar V.T. U.S.A. PERSPECTIVE FACTOR AND COUNTERING DISINFORMATION: IMPROVEMENT OF THE NATIONAL SECURITY SYSTEM

The article is devoted to the study of the practice of development by the U.S.A. government of State approaches to counter disinformation through the prism of the concept of the factor of the country's perspective in hybrid war, which has become the object of informational and psychological influence on the part of the aggressor country and external actors associated with it. The subject of the study is the consideration of legislative initiatives, expert recommendations regarding the improvement of the national security system towards strengthening the functional capacity of the components of the public administration system, the implementation of innovative organizational and administrative solutions, the expansion of institutional mechanisms for the formation of public-private partnerships to counter disinformation.

The goal is to study the government's approaches to improving the public management mechanisms of the U.S.A. national security system in the context of the perspective factor of this country as an object of the informational component of the hybrid war. The work highlights the peculiarities of the modernization of the public administration system of the United States of America by the establishment of independent centers with the sharing of their functional power under one of the key federal stakeholders - the National Intelligence Service.

Conclusions are made regarding the approaches of the American legislative bodies in forming an institutional environment for the involvement of independent and private subjects and institutions of civil society in indirect partnership interaction with the State key stakeholders of the security sector through direct cooperation with the centers of consultative and advisory direction under the federal agency. The prospects of further scientific research on the subject are reflected. In what sense can the positive experience of the U.S.A. be of interest to domestic stakeholders of the security sector, regulation of the information and media arena: the development of bilateral American-Ukrainian relations; guaranteeing the stability of the national security system of Ukraine, taking into account the perspective factor of both countries as the object of the informational component of the hybrid war.

Key words: *public administration, perspective factor, informational and psychological impact, countering disinformation, national security system.*