АКТУАЛЬНІ ПРОБЛЕМИ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

УДК 37.036.5:351.863
DOI https://doi.org/10.32782/TNU-2663-6468/2022.6/27

Чуб С.В.
Міжрегіональна Академія управління персоналом,
https://orcid.org/0009-0001-3703-9414

Ніколаєв К.Д.
Міжрегіональна Академія управління персоналом,
https://orcid.org/0000-0003-0404-6113

ПОПЕРЕДЖЕННЯ ДЕЗІНФОРМАЦІЙНИХ ВПЛИВІВ ТА ОСНОВНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Наукова стаття присвячена дослідженню актуальної тематики стосовно попередженню дезінформаційних впливів та основні напрями забезпечення інтелектуальної безпеки держави. Метою статті визначено окреслення сучасних методів протидії дезінформації та напрямків забезпечення інтелектуальної безпеки держави. Виділено види дезінформації без злого умислу такі як клікбейт, що відзначається використанням зазвичай перебільшених або сумнівних заголовків, зображень і описів у соціальних мережах або на інтернет-платформах; його метою є привернути увагу інтернет-користувачів і змусити їх клікнути на контент. Та сатира, що використовується для створення фейкових матеріалів з метою розваги та гумору; вона може виглядати як реальна інформація, але має гумористичний або сатиричний підтекст, і її не слід сприймати серйозно. А також відзначено види дезінформації, які ставлять на меті умисний вплив на свідомість населення, зокрема це: пропаганда, фейки, упереджені новини, джинса. Зазначено, що вагомим засобом захисту від руйнівного впливу дезінформації та фейкових новин, які поширюються через цифрові медіа, є медіаосвіта та медіаграмотність. Проаналізовано фактчекінг, оскільки це процес перевірки фактів, даних та інформації, щоб визначити їх достовірність та правдивість. Відзначено, що цей напрям стає дуже важливим в інформаційному суспільстві, де навіть невеликі помилки або спотворення фактів можуть призвести до серйозних наслідків.

Ключові слова: *фейки, дезінформація, клікбейт, пропаганда, фактчекінг, інтелектуальна безпека, публічне управління, національна безпека.*

Постановка проблеми. Фейки та дезінформація стали нормою для сучасного світу. З одного боку, недостовірну інформацію свідомо подають з метою підвищення популярності власного ресурсу, надаючи максимально помітну назву новині. Проте є й інший бік, коли дезінформація використовується ворожою державою, задля впливу на маси та послаблення єдності в державі, яка атакується. Подібне використання дезінформації є проявом гібридних загроз та активно використовується російським агресором у ході розпочатої ним війни проти України, що стало досить дієвим за рахунок вільного доступу до різних масивів інформації через різні медіа канали. Гібридні загрози, що включають в себе дезінформаційні кампанії, стали складовою сучасної геополітичної реальності. Держави та недержавні актори використовують дезінформацію для досягнення своїх стратегічних цілей, що може викликати суспільний розлад, втручання у внутрішні справи і навіть загрозити національній безпеці. Дезінформаційні кампанії можуть впливати на виборчий процес та політичну стабільність країн, зловживання інформацією може порушити довіру до демократичних інститутів та викликати соціальні конфлікти. За таких умов перед Україною постає проблема попередження та боротьби з дезінформаційними впливами, які полягають у розробці стратегій, які сприятимуть побудові інтелектуальної безпеки держави.

Мета статті – окреслити сучасні методи протидії дезінформації та напрями забезпечення інтелектуальної безпеки держави.

Ступінь дослідження. Подана у статті тематика є не новою для українського наукового дискурсу. Зокрема, у роботах О. Марченко, Г. Лозової, А. Сухорукова [7; 6; 9] досліджувалась інтелектуальна безпека держави, але виключно крізь призму економічного фактору. В контексті дезінформаційних впливів подана тема науковцями не підіймалася.

Власне дезінформація, відповідно до українських тлумачних словників – це введення в оману через поширення неправдивої інформації [5]. Дезінформація може бути як свідомою, коли автор умисно наводить неправдиву інформацію, а може бути несвідомою, коли автор джерела бере за основу чутки або відомості з іншого ресурсу та поширює їх без проведення попередньої верифікації. В питаннях, які відносяться до державного життя, сфери державного управління у будь-якому випадку дезінформація є небезпекою для національної безпеки держави.

Дезінформація може розповсюджуватися зі злим умислом, так і без нього. Зокрема, без злого умислу можемо віднести такі види дезінформації, як клікбейт (відзначається використанням зазвичай перебільшених або сумнівних заголовків, зображень і описів у соціальних мережах або на інтернет-платформах; його метою є привернути увагу інтернет-користувачів і змусити їх клікнути на контент. Це може бути використано для збільшення кількості переглядів або прибутку від реклами) та сатира (використовується для створення фейкових матеріалів з метою розваги та гумору; вона може виглядати як реальна інформація, але має гумористичний або сатиричний підтекст, і її не слід сприймати серйозно) [1, с. 99]. Але навіть у такому вигляді відбувається вплив на маси, можливе її розповсюдження створить неправильну картинку серед громадян. Особливо актуальне це для клікбейтів, адже багат людей, особливо більш літнього віку, читають лише заголовки новин, і вже не їх основі будують власну думку.

Інші види дезінформації вже ставлять на меті умисний вплив на свідомість населення. Розберемо деякі з них:

Пропаганда – включає в себе розповсюдження неправдивої інформації та чуток з політичною метою. Головна мета – впливати на громадську думку або засуджувати окремі особи чи групи людей. Це може призвести до поділу суспільства та погіршення міжнародних відносин.

Фейки – це вигадані історії або імітація новинних статей. Їх створюють для того, щоб обманювати аудиторію та передавати неправдиву інформацію. Фейки можуть мати серйозні наслідки, особливо коли вони стосуються важливих подій або глобальних проблем.

Упереджені новини – представляють собою контент, який підтверджує або посилює певні думки або переконання читача. Цей тип інформації може бути використаний для підтримки певної агенди або для маніпуляції громадською думкою, надаючи спотворений або вибірковий погляд на події.

Джинса – включає в себе поширення неправдивої інформації урядом з метою маніпуляції громадянами. Цей термін зазвичай застосовується до ситуацій, коли уряд намагається приховати або спотворити інформацію, щоб зберегти свою владу чи вплив.

Останній вид притаманний тоталітарним та автократичним режимам, до яких можемо віднести російського агресора.

Свідома дезінформація, яка поширюється зі злим умислом, також може називатися дезінформаційними впливами (або дезінформування), тобто – спосіб психологічного впливу, який полягає в намірі надання об'єктові такої інформації, яка вводить його в оману стосовно справжнього стану справ, та створює викривлену реальність [4].

Говорячи про джерела дезінформації в умовах сучасної війни, то діджиталізація хоча й надала вільний доступ до інформаційного масиву, але не створила системи перевірки інформації та головне – розумного вибору споживачем каналів, з яких вони черпають інформацію. В умовах війни досить поширеними каналами інформації стали так звані «нові медіа», які дозволяють миттєво поширювати новину, досить часто, не здійснюючи її верифікації. Такими медіа виступають телеграм та ютуб канали, інші соціальні мережі. Дезінформації сприяють й невдалі висловлювання політиків у ході їх виступів, які стають мемами.

Відповідно до офіційної позиції НАТО, дезінформацію треба не зупиняти, а уповільнювати, що витікає з того, що повністю в епоху діджиталізації її не спинити [4].

На наш погляд, одним з найбільш вагомих методів попередження дезінформації є створення команд реагування. Сьогоденні реалії роблять майже не можливим не допустити вкиду фейків та інших видів дезінформаційних впливів у загальний доступ. Тому першочергове завдання держави – це попередження їх масового поширення та розвінчення недостовірної інформації. Тому, наявність відповідних команд, які б займалися пошуком інформації, її блокуванням та розвінченням є вельми необхідна складова сучасної

національної безпеки. Навіть перевірені ресурси можуть бути зламані зловмисниками та розмістити хибну інформацію.

Другий напрям – фактчекінг. Фактчекінг – це процес перевірки фактів, даних та інформації, щоб визначити їх достовірність та правдивість. Цей напрям стає дуже важливим в інформаційному суспільстві, де навіть невеликі помилки або спотворення фактів можуть призвести до серйозних наслідків.

Основні аспекти фактчекінгу включають:

1) Перевірка джерел інформації. Фактчекери аналізують джерела інформації, їх репутацію та об'єктивність. Вони визначають, чи є конфлікти інтересів або політичні спрямування, які можуть впливати на об'єктивність поданої інформації.

2) Перевірка фактів. Фактчекери аналізують конкретні факти, числа, події та статистику, щоб переконатися в їхній точності. Вони шукають підтверджуючі докази та незалежні джерела інформації для підтвердження чи спростування поданих фактів.

3) Перевірка контексту. Фактчекери звертають увагу на контекст інформації. Іноді правдива інформація може бути спотворена через відсутність контексту або виведена з контексту, що може створювати неправдиве враження.

4) Виявлення маніпуляцій. Фактчекери аналізують можливі маніпуляції, такі як обрізання фотографій, монтаж відео чи використання заголовків з перебільшеннями. Вони визначають, чи спрямована інформація на створення обману чи психологічного впливу.

5) Публікація результатів. Фактчекери публікують свої результати та висновки, щоб інформувати громадськість про точність або недостовірність конкретних тверджень чи інформації [2; 3].

Головний критерій – наявність перевіреного фактчекінг-ресурсу, адже для маніпуляції свідомістю можуть бути утворені фейкові ресурси, які підтверджуватимуть хибну інформацію та спростовуватимуть реальну. Наразі в Україні функціонують декілька європейських мереж фактчекінгу. Вважаємо, що фактчекінг має бути нормативно прописаний в українському законодавстві, адже в такому разі буде офіційний канал, який займатиметься боротьбою з дезінформацією.

Вагомим засобом захисту від руйнівного впливу дезінформації та фейкових новин, які поширюються через цифрові медіа, є медіаосвіта та медіаграмотність. На поданому напряму наголошує власне НАТО. Зокрема, визначаючи наступні цілі:

1. Підвищення знань, обізнаності та розуміння серед громадян способів протидії дезінформації, пропаганді та іншій ворожій інформаційній діяльності;

2. Розроблення інноваційних та нетрадиційних способи підвищення стійкості суспільства у вищезазначених сферах;

3. Створення контенту тривалої цінності, який можна широко поширювати в межах і за межами мереж НАТО та громадянського суспільства [4].

Критичне мислення та освіта відіграють ключову роль у цьому процесі, оскільки саме завдяки цим навичкам стає можливим ефективне використання соціальних мереж. Одним із суттєвих викликів полягає в тому, що пересічний користувач часто не має достатньої медіаграмотності для розрізнення фейкових новин або дезінформації. Тому важливо виховувати громадян в дусі медіаосвіти, демонструючи, хто може здійснювати деструктивний вплив в соціальних мережах і як фейки можуть набрати вигляд звичайних повідомлень, що вступають у взаємодію з нами.

Медіаграмотність глядачів і слухачів є найбільш надійним засобом протистояння тому, щоб громадяни не потрапляли в пастку дезінформації та не ставали жертвами фейкових новин. Добре підготовлені люди здатні розрізнити правдиву інформацію від маніпуляцій, що може запобігти їх дезінформації та налаштування на штучні конфлікти, неправильні атаки і вигадані особистості. Все це може відволікти громадян від реальних проблем і занурити їх в соціальну апатію і безпорадність [1, с. 189–193].

Окремо варто згадати і щодо захисту об'єктів інтелектуальної власності. В умовах воєнного стану – це в першу чергу різнопланові військові розробки, які мають сприяти деокупації територій. Так, захист подібних розробок, їх наявності, можливих способів використання є важливим завданням для держави, адже в перспективі сприяє не тільки успіхам на фронті, але й збереженню життів військових.

Загрози інтелектуальній безпеці України виникають з різних джерел та походжень, мають різні способи виявлення та складаються з різноманітних проявів, утворюючи багаторівневу структуру. Це в першу чергу відсутінсть законодавчної регламентації галузі. Другу сферу складають загрози інституційного характеру, тобто такі як Відсутність державної інституції або мережі інститутів, які б спеціалізувалися на аналізі та впровадженні Стратегії інтелектуального просування України; обмежений розвиток національної інноваційної

системи через відсутність ефективної взаємодії між секторами освіти, науки та бізнесу; прояви корупції. Вагомою загрозою у сфері прийняття організаційно-управлінських рішень є низький інтелектуальний рівень ухвалення державних рішень; недостатній рівень кваліфікації осіб, які приймають рішення у сфері державних повноважень; високий ступінь впливу лобістських угрупувань на прийняття державних рішень [9, с. 165–168].

Варто відмітити ще загрозі глобалізаційного характеру, головною сутністю яких є технологічна залежність України від передових країн світу та відтік наукових кадрів закордон. Зокрема, Україна в період незалежності, тривалий період не вела активної підтримки української науки, покладаючись на закордонних партнерів у багатьох питаннях (одним з яких майже два десятиліття був нинішній агресор). Подібна залежність є головною на наш погляд проблемою інтелектуальної безпеки, адже знаходячись у постійній потребі від закордонних партнерів, практично відбувається визнання залежності на державному рівні. Тому, підготовка кадрів, які б працювали на користь держави та державне стимулювання різних галузей (а в реаліях сьогодення це військова та критична інфраструктура) є вагомим показником сформованості інтелектуальної безпеки.

Враховуючи вищеозначений матеріал, держава має сприяти забезпеченню інтелектуальної безпеки держави. В першу чергу, варто окреслити саму сутність та державну стратегію через ухвалення нормативно-правових актів, враховуючи як український, так і світовий досвід. Адже, відсутність законодавчого регулювання сфери робить будь-які атаки на об'єкти інтелектуальної безпеки небезпечними в тому плані, що викликатимуть активні дискусії з їх рішення у зв'язку з відсутністю наявності планових стратегій.

Важливим аспектом такого законодавства є впровадження правових механізмів, спрямованих на запобігання порушенням інтелектуальних прав та патентів. Це включає в себе процедури визначення порушень, відшкодування завданих збитків, а також можливість застосування судових заходів для захисту правовласників. Правові механізми повинні бути чіткими і ефективними, щоб стимулювати інновації та захищати інтелектуальні активи як національного, так і міжнародного значення.

Держава має створити активну мережу захисту інформації, найдоцільніше це робити в контексті міжнародних баз (для прикладу, доєднання наукових журналів до міжнародних наукометричних баз), що нівелює питання першості у відкриті. Проте, слід врахувати ймовірність кібератак на бази. Тому виникає потреба створення ефективних систем аутентифікації, шифрування та моніторингу мережевого трафіку для виявлення та реагування на потенційні загрози. Технологічний аспект такого захисту є важливим, оскільки кіберзлочинці постійно вдосконалюють свої методи атак.

Освіта і підвищення обізнаності громадян і підприємств стосовно інтелектуальної безпеки є фундаментальними компонентами захисту інтелектуальних активів та знань. Проведення навчальних заходів і кампаній в цій сфері має на меті надати інформацію та навички, необхідні для ефективного реагування на загрози та збереження конфіденційності.

Однією з основних цілей цих навчальних ініціатив є підвищення інформованості щодо ризиків порушення прав інтелектуальної власності. Вона включає в себе розуміння того, що таке інтелектуальна власність, які види прав захищені законом, і які загрози можуть існувати щодо їх порушення.

Українська науковці також визначають, що інтелектуальна безпека відповідає не лише за підготовку в Україні високоякісних фахівців у будь-якій галузі. В такому разі, підготовка кваліфікованих фахівців у кожній галузі, які б розуміли вагомість своєї праці, в першу чергу для користі держави.

Таким чином, дезінформаційні впливи наразі є головним методом ведення гібридної війни у світі. Не маючи трактування у нормативно-правових актах, як порушення міжнародного права, агресор використовує дезінформацію задля впливу на маси: отримання їх підтримки або засобу залякування (що є притаманним для РФ у їх агресивних діях щодо України). Перед державою стоїть проблема попередження дезінформаційних впливів, які в першу чергу мають базуватися на зменшенні розповсюдження неправдивої інформації та її розвінчання серед мас, адже повноцінне попередження в епоху медіамереж є неможливим з технічної точки зору. Окрім того існує потреба у розвитку медіаграмотності самих громадян та створенні державної мережі фактчекінгу, закріпленої законодавчо. Забезпечення інтелектуальної безпеки держави вимагає спільних зусиль уряду, громадськості та освітніх установ. Тільки таким чином можна забезпечити стійкий захист від дезінформації та зберегти надійність інформаційного середовища.

Список літератури:

1. Bennet L., Livingston S. The disinformation age. Cambridge University Press. Cambridge : Cambridge University Press, 2021. 324 p.
2. European Democracy Action Plan. European Commission. 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250
3. Halbert, D. Intellectual property theft and national security: Agendas and assumptions. Information Society. 2016. № 32 (4). P. 256–268.
4. Increasing societal resilience: innovative ways to counter disinformation and hostile information activities. NATO public diplomacy programmes. 2022. URL: https://www.nato.int/structur/pdd/2022/220411-ResilienceContentGuidelines.pdf
5. Дезінформація. Словник UA. URL: https://slovnyk.ua/index.php?swrd=%D0%B4%D0%B5%D0%B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F
6. Лозова Г. М., Шорубалко Б. В. Інтелектуальна безпека держави в системі конкурентоспроможності національної економіки. Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. 2018. Вип. 20 (2). С. 102–106.
7. Марченко О.С. Інтелектуальна безпека у вимірі економіки знань. Вісник НУ «Юридична академія України імені Ярослава Мудрого». 2012. № 1 (8). С. 278–279.
8. Протидія дезінформації в інтернеті : куди рухатися Україні? Аналітичний звіт. Київ : ABA ROLI, 2021. 30 с.
9. Система економічної безпеки держави / заг. ред. А. І. Сухорукова ; Національний інститут проблем міжнародної безпеки при РНБО України. – К. : ВД «Стилос», 2009. – 685 с.
10. Що таке дезінформація і як вона впливає на людину. URL: https://inshe.tv/suspilstvo/2023-08-08/785476/
11. Semenets-Orlova, I., Mykhailych, O., Klochko, A., Nestulya, S., & Omelyanenko, V. (2019). Readiness of the education manager to provide the organizational development of institutions (based on the sociological research). *Problems and Perspectives in Management*, *17*(3), 132–142.
12. Семенець-Орлова, І. А. (2015). Державне управління освітніми змінами: наукові категорії, методологія та актуальна проблематика досліджень на основі досвіду України та США. *Університетські наукові записки*, (1), 302–311.
13. Семенець-Орлова, І. А. (2015). Результативне лідерство в процесі управління освітніми змінами. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління*, (4), 107–112.
14. Семенець-Орлова, І. А. (2017). Нормативно-правове забезпечення освітніх змін в Україні. *Теорія та практика державного управління*, (3), 91–100.
15. Radchenko, O., Kovach, V., Radchenko, O., Kriukov, O., Sydorchuk, L., Sharov, P., & Semenets-Orlova, I. (2021). Principles of natural capital preservation in the context of strategy of state environmental safety. In *E3S Web of Conferences* (Vol. 280, p. 09024). EDP Sciences.

Chub S.V., Nikolaiev K.D. PREVENTION OF DISINFORMATION INFLUENCES AND MAIN DIRECTIONS OF ENSURING THE PUBLIC INTELLECTUAL SECURITY

The scientific article is devoted to the study of topical topics related to the prevention of disinformation influences and the main directions of ensuring the intellectual security of the state. The purpose of the article is to outline modern methods of countering disinformation and directions for ensuring the intellectual security of the state. Types of disinformation without malicious intent are highlighted, such as clickbait, which is characterized by the use of usually exaggerated or questionable titles, images and descriptions in social networks or on Internet platforms; its purpose is to attract the attention of Internet users and make them click on the content. That satire used to create fake material for the purpose of entertainment and humor; it may look like factual information but has a humorous or satirical connotation and should not be taken seriously. The types of disinformation aimed at deliberately influencing the public's consciousness were also noted, in particular: propaganda, fakes, biased news, jeans. It is noted that media education and media literacy are a powerful means of protection against the destructive impact of misinformation and fake news that spreads through digital media. Fact-checking is analyzed because it is the process of checking facts, data, and information to determine their reliability and truthfulness. It was noted that this direction is becoming very important in the information society, where even small mistakes or distortions of facts can lead to serious consequences.

Key words: *fakes, disinformation, clickbait, propaganda, fact-checking, intellectual security, public management, national security.*