



Наказом МОН України від 10.10.2022 р. №894 видання включено до **категорії «Б»** за спеціальностями:
051 – економіка; 072 – фінанси, банківська справа, страхування та фондовий ринок; 073 – менеджмент;
076 – підприємництво, торгівля та біржова діяльність; 292 – міжнародні економічні відносини

DOI 10.56197/2786-5827/2024-3-3-5

УДК 323.284

Паламарчук Дмитро Миколайович,
кандидат економічних наук, доцент,
доцент кафедри міжнародної економіки та бізнесу,
Черкаський державний технологічний університет,
бульв. Шевченка, 460, м. Черкаси, 18006, Україна,
email: dmytropalamarchuk@gmail.com,
ORCID ID: <https://orcid.org/0000-0002-6023-9780>
Researcher ID: AAI-5198-2021
Scopus ID: 56529650700

Palamarchuk Dmytro,
PhD in Economics, Associate Professor,
Associate Professor at Department of International Economy and Business,
Cherkasy State Technological University,
Bld. Shevchenko, 460, 18006, Cherkasy, Ukraine,
email: dmytropalamarchuk@gmail.com,
ORCID ID: <https://orcid.org/0000-0002-6023-9780>
Researcher ID: AAI-5198-2021
Scopus ID: 56529650700

ПРОТИСТОЯННЯ ВОРОЖІЙ ІНФОРМАЦІЙНІЙ ДІЯЛЬНОСТІ З ВИКОРИСТАННЯМ СОЦІАЛЬНИХ ПЛАТФОРМ

COUNTERING HOSTILE INFORMATION ACTIVITIES USING SOCIAL PLATFORMS

Вступ. Стаття присвячена аналізу ворожої інформаційної діяльності з використанням соціальних платформ та пошуку методів протистояння їй. Відзначено особливу вразливість сучасного суспільства до дезінформації через зміни в інформаційному середовищі та розвиток технологій. Основна мета дослідження – аналіз інструментів, які використовують країни та міжнародні організації для протидії дезінформації, а також визначення напрямків подальшого розвитку інформаційної політики для посилення спроможності протистояння ворожій інформаційній діяльності.

Матеріали та методи. Основними джерелами для аналізу є офіційні звіти міжнародних організацій, урядів держав, дослідження неурядових організацій та аналітиків. Для аналізу і узагальнення результатів досліджень та наукових публікацій щодо ворожої інформаційної діяльності та її впливу на суспільство використаний метод синтезу наукових даних.

Результати і обговорення. В дослідженні детально представлено інструменти ворожої інформаційної діяльності, такі як дезінформація, пропаганда, зовнішня маніпуляція інформацією тощо. Автором визначені та описані наслідки використання цих інструментів, включаючи зниження довіри до традиційних медіа, поляризацію суспільства та підрив довіри до державних інституцій. Проаналізовано етапи російського ворожого інформаційного впливу на Україну, здійснено аналіз та виділено основні групи ворожих наративів та дезінформації, що поширюються росією в період повномасштабного вторгнення. Визначено заходи, що Україна здійснила для захисту свого інформаційного простору та протидії російській інформаційній агресії.

Наведено приклади інформаційної агресії з боку росії та Китаю щодо інших країн, з використанням соціальних платформ. Описані цілі та методи, які використовуються цими країнами, включаючи поширення дезінформації та маніпуляцію громадською думкою.

Визначено рекомендації, що підвищують здатність протидії ворожій інформаційній діяльності та стійкість суспільства до зовнішніх загроз.

Висновки. У висновках підкреслюється критична важливість розуміння та контролю інформаційних процесів для забезпечення національної безпеки в умовах гібридної війни. Ворожі дії, особливо через соціальні мережі, спрямовані на розповсюдження дезінформації та маніпуляцію громадською думкою з метою дестабілізації, створення соціальних розривів і підвищення політичної поляризації загрожують не лише національній безпеці, а й демократичним процесам. У відповідь на це, країни мають здійснювати різноманітні та масштабні заходи протидії, включаючи збільшення медіа-грамотності, моніторинг дезінформації та співпрацю з іншими країнами для зменшення впливу інформаційних загроз.

Ключові слова: ворожа інформаційна діяльність, дезінформація, ворожі наративи, соціальні платформи, протидія ворожій інформаційній діяльності.

Introduction. The article is devoted to analyzing hostile information activities utilizing social platforms and seeking methods to counter them. It acknowledges the particular vulnerability of contemporary society to disinformation due to changes in the information environment and technological advancements. The primary aim of the research is to analyze the tools employed by countries and international organizations to combat disinformation and to identify directions for further development of information policy to enhance resilience against hostile information activities.

Materials and methods. Official reports from international organizations, government entities, research from non-governmental organizations, and analysts constitute the main sources for analysis. The method of synthesizing scientific data is utilized to analyze and consolidate research findings and scholarly publications concerning hostile information activities and their societal impact.

Results and discussion. The study extensively presents instruments of hostile information activities such as disinformation, propaganda, external information manipulation, among others. The author identifies and describes the consequences of employing these instruments, including diminished trust in traditional media, societal polarization, and erosion of trust in governmental institutions. An analysis of stages of Russian hostile information influence on Ukraine is conducted, highlighting major categories of hostile narratives and disinformation propagated by Russia during periods of full-scale intrusion. Measures undertaken by Ukraine to safeguard its information space and resist Russian information aggression are delineated.

Instances of information aggression from Russia and China toward other nations via social platforms are provided. The objectives and methods employed by these countries, including the dissemination of disinformation and manipulation of public opinion, are described.

Conclusions. Recommendations aimed at enhancing the capacity to counter hostile information activities and society's resilience to external threats are identified. The conclusions underscore the critical importance of understanding and controlling information processes to ensure national security amid hybrid warfare. Hostile actions, particularly through social networks, aimed at spreading disinformation and manipulating public opinion to destabilize societies and heighten political polarization, pose threats not only to national security but also to democratic processes. In response, countries must implement diverse and extensive measures to counteract these threats,

including increasing media literacy, monitoring disinformation, and collaborating with other nations to mitigate the impact of informational threats.

Keywords: hostile information activities, disinformation, disinformation, social platforms, countering hostile information activities.

JEL Classification: D83, L86, F52

Вступ. Останніми роками дезінформація стала серйозною проблемою, з якою зіткнулися в усьому світі. Завдяки інтернет-платформам інформація може швидко поширюватись, не зважаючи на її достовірність. Люди стають мішенями для дезінформації, навіть не усвідомлюючи цього, і часто стають поширювачами неправдивих тверджень через соціальні мережі.

Україна, подібно багатьом іншим країнам, стикається з викликами інформаційної агресії, що стала серйозним випробуванням для національної безпеки та стабільності. Інформаційна агресія проявляється через розповсюдження дезінформації, маніпуляції громадською думкою та інші засоби впливу.

Дослідження інструментарію протидії ворожій інформаційній діяльності має велике значення для розуміння сучасних викликів та пошуку ефективних методів протистояння їй.

Основна мета дослідження полягає у аналізі інструментів, що використовуються країнами та міжнародними організаціями для протидії дезінформації, а також у визначенні напрямків подальшого розвитку інформаційної політики з метою зміцнення здатності протистояти ворожій інформаційній діяльності.

Матеріали та методи. Основними джерелами для аналізу є офіційні звіти міжнародних організацій, урядів держав, дослідження неурядових організацій та аналітиків, наукові публікації. Серед українських науковців, зокрема, дослідженнями інформаційної агресії та маніпуляцій займаються Горбань Ю. (Горбань, 2015) та Драбюк С. (Драбюк, 2022), вивчення пропаганди та способів протидії їй здійснюють Горун О. (Горун, 2023), Денисюк Ж. (Денисюк, 2021), Шевців М. та Гончарук К. (Шевців, 2019), аналізом впливу дезінформації займаються Дубов Д., Баровська А., Каздобіна Ю. (Дубов, 2020), Лісневська, А. (Лісневська, 2019), Павленко Т. (Павленко, 2022), Шульська Н., Зінчук Р., Кевлюк І. (Шульська, 2023), історичний контекст пропаганди та дезінформації є об'єктом досліджень Іваницької Б., Даниліва О. (Іваницька, 2020), Золотухіна Д. (Золотухін, 2018). Важливий доробок в дослідження ворожого інформаційного впливу забезпечує Центр протидії дезінформації¹. До іноземних публікацій, що стали важливим джерелом інформації для цього дослідження належать публікації НАТО², звіти по дослідженнях, що проводились RAND Corporation для Командування спеціальних операцій ВПС США (Treyger, 2022), звіт “Countering Disinformation in the United States: CSC White Paper #6”, підготовлений Коміцією з кіберпростору США³, розроблений згідно рекомендацій Європейської Комісії “The Strengthened Code of Practice on Disinformation 2022”⁴ а також дослідження ОЕСР “Disinformation and Russia’s war of aggression against Ukraine” (Disinformation and russia’s, 2022) та ін.

Для узагальнення та систематизації отриманих результатів використаний метод синтезу наукових даних, що передбачає об'єднання різноманітних джерел інформації для отримання комплексного уявлення про проблему. Цей підхід дозволяє систематизувати та аналізувати різні аспекти ворожої інформаційної діяльності та її впливу на суспільство. Аналізується не лише сам факт поширення дезінформації, а й її потенційні наслідки для національної безпеки, стабільності та демократичних процесів. Такий підхід дозволяє отримати глибше розуміння проблеми та визначити можливі шляхи протидії цьому явищу.

Результати і обговорення. НАТО визначає ворожу інформаційну діяльність як широкий спектр узгоджених заходів, що має на меті поширення недовіри та маніпулювання

¹ URL: <https://cpd.gov.ua/> (дата звернення 20.05.2024)

² URL: <https://www.nato.int/cps/en/natohq/topics.htm> (дата звернення 20.05.2024)

³ URL: <https://www.solarium.gov/> (дата звернення 20.05.2024)

⁴ URL: <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation> (дата звернення 20.05.2024)

думками, зазвичай із застосуванням одного або сукупності зазначених вище методів і прийомів, включаючи оманливі меми, теорії змови, діпфейкові зображення або відео, цитати поза контекстом або просто відверту брехню, яку люди поширюють з метою маніпулювання іншими. Наслідком ворожої інформаційної діяльності може бути підрив репутації країни, суспільний розкол та недовіра до державних установ, спотворення реальності та створення хаосу у суспільстві шляхом дезінформації та поширення ворожих наративів.

Тоталітарні режими таких країн як росія, Китай, Іран, активно поширюють неправдиву та маніпулятивну інформацію для впливу на громадську думку як в своїх країнах, так і за кордоном.

Згідно підходів НАТО у галузі боротьби з дезінформацією, можна виділити наступні інструменти ворожої інформаційної діяльності:

- Дезінформація – поширення неправдивої або неточної інформації, з метою введення в оману та маніпулювання цільовою аудиторією;
- Мізінформація – ненавмисне поширення неправдивої та/або неточної інформації не з лихого умислу;
- Ворожий наратив – спрямована на дискредитацію або паплюження певного суб'єкта спеціально створена історія;
- Пропаганда – інформаційний вплив, націлений на маніпулювання цільовою аудиторією з метою формування певної поведінки або переконань, що здійснюється державним суб'єктом протягом тривалого часу для досягнення політичних цілей;
- Зовнішнє маніпулювання інформацією та втручання – формування моделей поведінки, що загрожує або може негативно позначитися на цінностях, процедурах і політичних процесах в цільовій країні. Така діяльність здебільшого не порушує закон, але має маніпулятивний характер, ведеться цілеспрямовано та узгоджено державними або недержавними суб'єктами як на своїй території, так і поза її межами⁵.

В багатьох випадках розрізнити описані інструменти досить складно, дезінформація, ворожий наратив, пропаганда, зовнішнє маніпулювання інформацією та втручання часто перетинаються та використовуються взаємозамінно в повсякденному мовленні. Попри це, зазначений інструментарій має суттєві відмінності в очікуваних наслідках застосування (табл. 1).

Таблиця 1

Інструменти ворожої інформаційної діяльності та очікувані наслідки застосування

Інструмент	Очікувані наслідки застосування
Дезінформація	Зниження рівня довіри до традиційних джерел новин і владних структур, сприяння розколу та конфліктам між людьми та соціальними групами.
Мізінформація	
Ворожий наратив	Посилення трайбалізму, поляризація, створення та поглиблення розколів у суспільстві, створення спотвореного сприйняття реальності шляхом підриву довіри до ЗМІ та державних інститутів.
Пропаганда	Формування мислення і поведінки цільової аудиторії з метою досягнення конкретних цілей, часто з використанням дезінформації.
Зовнішнє маніпулювання інформацією і втручання	Підрив довіри до демократичних інститутів, зміцнення поляризації в суспільстві та порушення здатності здійснювати свою політику як всередині країни, так і за кордоном, посилення насильства в конфліктогенних регіонах, формування процесів прийняття рішень на користь іноземних держав.

Складено автором за джерелом⁵

⁵ URL: https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en (дата звернення 20.05.2024)

Ворожа інформаційна діяльність може бути елементом гібридної війни, масштабнішого набору інструментів та засобів, який передбачає одночасне застосування військових та не військових засобів відкрито чи приховано з метою дестабілізації та ослаблення супротивника, примусу до зміни політики, створення та/або посилення суспільного розколу, підриву демократичних процесів, ініціювання громадських заворушень, сепаратистських рухів, розриву союзів.

Ворожа інформаційна діяльність здійснюється через різні канали – телебачення, радіо, друковані ЗМІ, публічні заходи та Інтернет, зокрема, соціальні платформи. Технічний прогрес та поширення Інтернету значно вплинули на можливості розповсюдження дезінформації. Сьогодні соціальні платформи, використовується як важіль для дестабілізації цільових країн за допомогою ворожої інформаційної діяльності. В широкому розумінні соціальні платформи це онлайн-сервіси, що дозволяють користувачам спілкуватися, обмінюватися інформацією та взаємодіяти один з одним через Інтернет. Соціальні мережі, форуми, блоги, відеохостинги та інші сервіси, наприклад, Facebook, Twitter, Instagram, YouTube, Reddit, Telegram – це все приклади соціальних платформ, що дають можливість спілкування користувачів з усього світу.

Соціальні платформи працюють за алгоритмами, що аналізують поведінку користувачів, їх взаємодію та інтереси і на основі цього пропонують персоналізований контент. Загалом, в основі бізнес-моделей соціальних платформ лежить просування контенту, який привертає увагу користувачів, та продаж цієї уваги рекламодавцям.

В результаті, алгоритми соціальних платформ створюють ехокамери, де користувачі отримують контент, який відповідає їхнім інтересам і посилює впевненість стосовно поширеності / “правильності” / безальтернативності власних переконань⁶. І хоча соціальні платформи дають можливість спілкування користувачів з усього світу, вони також здатні фрагментувати суспільство та сприяють трайбалізму – явищу, коли користувачі формуються в певні групи зі схожими переконаннями, інтересами, цінностями, а це, відповідно, робить важчим сприйняття інших поглядів та посилює політичну і соціальну поляризацію⁷.

В свою чергу ехокамери та трайбалізм створюють сприятливі умови для ведення ворожої інформаційної діяльності. Ізольовані групи користувачів більше схильні довіряти “однодумцям” та розповсюджувати інформацію, що підтверджує їхні уявлення та переконання, навіть якщо ця інформація є неправдивою (тобто, здійснювати мізінформацію). Це сприяє швидкому поширенню неправдивої інформації, посилюючи розколи та поляризацію суспільства (серед різних спільнот може поширюватися різна інформація, в тому числі і така, що суперечить одна одній).

Згідно дослідження Массачусетського технологічного інституту, неправдиві новини поширюються значно швидше, ніж правдиві, і поширюють їх, здебільшого, звичайні користувачі а не боти⁸. На великих соціальних платформах повідомлення, яке подвоюється кожні 15 хвилин, гіпотетично може отримати мільйон переглядів за п’ять годин і 16 мільйонів переглядів за шість годин⁹. За рахунок цього неправдиві новини можуть поширюватися серед користувачів подібно епідемії, і в інформаційному середовищі, перенасиченому контентом, швидко стати вірусними.

Ворожа інформаційна діяльність росії проти України є однією з наймасштабніших в історії та ведеться з використанням всього набору інструментів, від систематичної дезінформації до маніпуляції громадською думкою, через традиційні ЗМІ та соціальні платформи, з залученням платних “тролів”, інфлюенсерів та використанням офіційних каналів.

⁶ URL: <https://www.nature.com/articles/d43978-021-00019-4> (дата звернення 20.05.2024)

⁷ URL: <https://www.psychologytoday.com/intl/blog/beyond-school-walls/202304/tribalism-in-the-age-of-social-media> (дата звернення 20.05.2024)

⁸ URL: <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308> (дата звернення 20.05.2024)

⁹ URL: <https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html> (дата звернення 20.05.2024)

Наявність російськомовного населення, історичні та релігійні зв'язки між країнами надають російській дезінформації додаткової ефективності. Україна була пріоритетною ціллю для російської ворожої інформаційної діяльності задовго до анексії Криму та початку війни в 2014 році. Через традиційні ЗМІ, публічні виступи та соціальні платформи, в тому числі російські соціальні мережі ВКонтакте та Однокласники, здійснювалася популяризація концепції “русского мира”, за якою Україна є частиною російського світу (російської зони впливу), пропагувалася ностальгія за Радянським Союзом, відбувалася “демонізація” США і НАТО.

На початку війни, в 2014-2015 рр., акцент російської інформаційної діяльності в Україні змістився в сторону дискредитації уряду та просування ідей його нелегітимності, виправдання військової агресії та створення паніки серед населення. росія намагалася розколоти українське суспільство, підірвати міжнародну підтримку та знизити бойовий дух українських військ (Disinformation and russia's, 2022).

Перед повномасштабним вторгненням в 2022 році та вже після росія продовжила зосереджувати свою інформаційну діяльність на створенні та посиленні суспільного розколу, погіршенні ставлення до України з боку інших держав та покращення ставлення до росії. Ворожі наративи та дезінформацію, що поширювалися росією в цей час можна виділити в кілька основних груп (табл. 2).

Таблиця 2

Групи основних наративів та дезінформації, що поширюються росією в період повномасштабного вторгнення

Група	Суть	Мета
Агресивні дії та провокації з боку України	Україна – агресор, який планує або здійснює провокаційні атаки проти росії або проросійських сил на Донбасі.	Виправдання дій росії та підтримки міжнародної підтримки України.
Заперечення фактів	Заперечення фактів реальної війни та військових злочинів росії, представлення їх як інсценування або неправдивих повідомлень	Зменшення репутаційних втрат росії на міжнародній арені.
Зовнішня загроза та змова	Сіяння страху перед зовнішніми загрозами, зокрема з боку США та НАТО. Зображення військових дій як необхідного захисту.	Мобілізація внутрішньої підтримки в росії та виправдання її дій.
Легітимність дій росії	Обґрунтування дій, посиляючись на історичні та юридичні аргументи. Пропагування ідеї, законних підстав росії для війни проти України.	Виправдання дій росії.
Негативний образ України	Дискредитація українського суспільства, як негуманного та екстремістського	Зменшення міжнародної підтримки України та негативне ставлення до неї.
Недостатня підтримка України Заходом	Зображення допомоги Заходу Україні як недостатньої або неефективної	Створити сумніви щодо якості та результативності західної підтримки

Складено автором за джерелами (Disinformation and russia's, 2022) та Cadier et al. (2022)¹⁰.

¹⁰ URL: <https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/> (дата звернення 20.05.2024)

З 2014 року Україна здійснила ряд реформ у сфері захисту інформаційного простору. В 2015 році прийнята Воєнна доктрина України, яка чітко визначила російську федерацію як агресора та реальну загрозу, створила концептуальну основу для розробки і реалізації стратегій, спрямованих на протидію російській інформаційній агресії. Доктрина інформаційної безпеки України, затверджена у 2017 році, визначила національні інтереси в інформаційній сфері, загрози їх реалізації, а також напрями і пріоритети державної політики, що посилює спроможність держави ідентифікувати та реагувати на інформаційні загрози. Стратегія інформаційної безпеки до 2025 року, введена в дію 2021 року, надала додаткові ресурси та інструменти для посилення інформаційного захисту та адаптивності до нових викликів у сфері інформаційної безпеки. Стратегія забезпечення державної безпеки України, введена в дію 2022 року, інтегрувала заходи інформаційної безпеки в ширший контекст державної безпеки, забезпечуючи комплексний підхід до протидії інформаційним атакам та дезінформації. Це посилює спроможність України протистояти російській інформаційній агресії через чітке визначення загроз, встановлення пріоритетів державної політики, надання необхідних ресурсів та інтеграцію інформаційної безпеки в загальну стратегію державної безпеки.

Протидія України російській інформаційній агресії включає створення центру протидії дезінформації, контроль над приватними медіаорганізаціями для забезпечення єдиного цілодобового телевізійного висвітлення подій, обмеження доступу до російських ЗМІ, сприяння розвитку медіа-грамотності та фактчекінгових ініціатив, заборону російських соціальних платформ, заборону російської відео- та аудіо продукції та ін.

росія та Китай здійснюють інформаційну агресію, в тому числі, на Захід, намагаючись роз'єднати НАТО та ЄС, а також відокремити США від їхніх союзників. ЗМІ, які контролюються росією використовують неправдиві новини і проблемні історії для зміцнення своїх наративів і підтримки антиамериканізму та антиглобалізму, посилення хаосу та зменшення довіри до ЗМІ держави-жертви (Flore, 2020).

росія використовує соціальні платформи для досягнення чотирьох загальних цілей:

- Сприяння військовим діям. росія використовує соціальні мережі для створення дезінформації, зокрема під час конфліктів в Україні та Сирії. Це включає розповсюдження фейкових новин, маніпуляцію громадською думкою та психологічний тиск на супротивників.
- Підтримка російських наративів. Протидія критиці та захист росії від звинувачень у протиправних діях, поширення дезінформації, спрямованій на послаблення НАТО та ін.
- Досягнення конкретних результатів в інших країнах. Просування кандидатів, дружніх російській владі, та делегітимізація демократичних процесів. За допомогою соціальних мереж, російські актори намагалися вплинути на вибори в США, Франції, Сполученому Королівстві та Каталонії шляхом поширення неправдивої інформації.
- Загострення внутрішніх розбіжностей в західних країнах. Посилення розбіжностей та соціальної нестабільності в західних суспільствах. Це включає деструктивну діяльність, спрямовану на збільшення впливу росії та ослаблення західних інституцій. Ілюстраціями цього є спрямовані на загострення конфліктів в Сполучених Штатах та Європі дії російського “Агентства інтернет-досліджень” (Treuger, 2022).

Китайський уряд також впливає на іноземну аудиторію через соціальні платформи. Основні підходи включають розповсюдження китайського та іншомовного контенту на китайських і іноземних платформах, контроль державних ЗМІ на іноземних платформах та використання їх для просування китайської позиції. Найбільш активно ворожу інформаційну діяльність Китай проводить по відношенню до Тайваню. Можна виділити три основні типи кампаній, які Китай проводить на Тайвані:

- Спроби дестабілізації стану. Кампанії спрямовані на поглиблення соціальних розбіжностей, зниження морального духу та довіри до демократії.
- Підтримка дискретних або обмежених у часі цілей. Ці кампанії спрямовані на досягнення конкретних цілей, таких як ускладнення військових навчань або вплив на результати виборів.

- Опортуністичні атаки. Посилення уваги до правдивих “поганих” новин з метою створення образу некомпетентності та зменшення суспільної підтримки владних інститутів.

Китай намагається розділити та деморалізувати тайванське суспільство, створити негативний образ уряду Тайваню, покращити свій імідж та посилити підтримку ідеї приєднання Тайваню до Китаю (Harold, 2021).

Європейський Союз вважає зовнішнє маніпулювання інформацією та втручання зростаючим політичним викликом та викликом безпеці. Іноземні актори, такі як росія та Китай, проводять скоординовані спроби маніпулювати фактами, вводити в оману та сіяти розкол, страх і ненависть, з метою виправдання своїх дій, досягнення політичних та економічних цілей, підриваючи довіру до демократичних інституцій та сприяючи поляризації.

Згідно звіту “2nd EEAS Report on Foreign Information Manipulation and Interference Threats”¹¹ з 1 грудня 2022 року по 30 листопада 2023 року Європейська служба зовнішніх справ виявила та розслідувала 750 випадків зовнішнього маніпулювання інформацією та втручання. У більшості випадків країною-мішенню була Україна (160), за якою слідували Сполучені Штати Америки (58), Польща (33), Німеччина (31), Франція (25) та Сербія (23). Загалом, зовнішнє маніпулювання інформацією та втручання здійснювалося по відношенню до 53 країн, включно з Австралією та країнами Латинської Америки, що свідчить про його глобальний характер.

Зважаючи на стрімке зростання в останні роки серйозності та масштабу загрози, США, ЄС, інші країни та організації активізували зусилля спрямовані на протидію ворожій інформаційній діяльності з використанням соціальних платформ.

Звітом “Countering Disinformation in the United States: CSC White Paper #6”¹², підготовленим Комісією з кіберпростору США для підвищення стійкості суспільства до ворожої інформаційної діяльності запропоновано посилення федеральних установ для боротьби з дезінформацією, співпрацю уряду з громадянським суспільством, моніторинг іноземної дезінформації та ін.

Звіти по дослідженнях, що проводились RAND Corporation для Командування спеціальних операцій ВПІС Chinese Disinformation Efforts on Social Media та Russian Disinformation Efforts on Social Media (Treyger, 2022; Harold, 2021) серед іншого містять рекомендації для посилення протидії ворожій інформаційній діяльності Китаю та росії з використанням соціальних платформ, що включають навчання персоналу, виявлення та відстеження пропагандистських кампаній, розвиток авторитетних джерел інформації та залучення партнерів для спільної протидії ворожій інформаційній діяльності.

Розроблений згідно рекомендацій Європейської Комісії та підписаний 2022 року представниками онлайн-платформ, рекламного бізнесу, фактчекінгових організацій та громадянського суспільства ЄС “The Strengthened Code of Practice on Disinformation 2022”¹³ містить зобов'язання спрямовані на зменшення розповсюдження дезінформації в Інтернеті в межах ЄС. Серед підписантів зі сторони онлайн-платформ такі компанії як Google, Meta, Microsoft, TikTok, Twitch, Vimeo, Clubhouse та ін..

Аналіз рекомендацій для підвищення спроможності протидії ворожій інформаційній діяльності викладених в вищезазначених документах дозволяє систематизувати їх та виділити в кілька груп (табл. 3).

Реалізація зазначених рекомендацій зменшить вплив дезінформації та ризики витоку інформації та значно покращить спроможність країни протидіяти ворожій інформаційній діяльності, зміцнить інформаційну безпеку та стійкість суспільства до зовнішніх загроз, підвищить довіру до медіа, якість модерації контенту на соціальних платформах і оперативність реагування на загрози.

¹¹ URL: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (дата звернення 20.05.2024)

¹² URL: <https://www.solarium.gov/home#h.jlr70j8saqnt> (дата звернення 20.05.2024)

¹³ URL: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (дата звернення 20.05.2024)

Рекомендації для підвищення спроможності протидії ворожій інформаційній діяльності

Рекомендації	Зміст рекомендацій
Підвищення медіаграмотності	Підвищення громадської обізнаності про ворожу інформаційну діяльність, навчання вищих посадових осіб основам кібербезпеки та зменшення ризиків витоку інформації.
Інформування громадськості	Розробка та підтримка достовірних інформаційних ресурсів та платформ в Інтернеті, забезпечення прозорості власності ЗМІ. Поширення контрнарративів і розвінчання дезінформації шляхом створення авторитетних джерел інформації, регулярна публікація чітких та послідовних повідомлень для уникнення поширення дезінформації.
Моніторинг та аналіз дезінформації	Відслідковування дезінформаційних кампаній, створення бази даних з інформацією про кампанії дезінформації в соціальних мережах.
Залучення спільноти та громадських організацій	Залучення місцевих спільнот та громадських організацій до роботи з протидії дезінформації та розповсюдження інформації. Фінансування досліджень дезінформаційних кампаній.
Моніторинг на соціальних платформах та прозорість	Розробка ефективніших алгоритмів виявлення неправдивої інформації та ворожих наративів, розробка технологічних інструментів для перевірки автентичності контенту. Протидія маніпулятивним поведінкам і практикам, обмін інформацією між платформами для виявлення та запобігання маніпуляціям, встановлення прозорих правил модерації контенту.
Військова підготовка та тренування	Забезпечення військовослужбовців навичками розпізнавання та протистояння дезінформації. Розроблення політики використання військовослужбовцями соціальних платформ та мобільних пристроїв для захисту.
Співпраця з громадянами іноземного походження	Залучення громадян іноземного походження до роботи з протидії ворожим інформаційним кампаніям ініційованих країнами їх походження (для кращого розуміння контексту).
Міжнародна співпраця та обмін досвідом	Залучення союзників і партнерів до вивчення досвіду та спільної протидії дезінформації.

Складено автором за джерелами: ^{14,15} Treyger, 2022; Harold, 2021.

Висновки. У сучасних умовах, забезпечення національної безпеки стає критично важливим завданням, яке неможливо виконати без ефективного розуміння та контролю інформаційних процесів. Однією з найбільш небезпечних загроз є ворожі дії, спрямовані на розповсюдження дезінформації та маніпуляцію громадською думкою, зокрема через соціальні платформи. Ці дії мають за мету дестабілізацію суспільства, створення соціальних розривів та підвищення політичної поляризації, що загрожує не лише національній безпеці, але й демократичним процесам в цілому.

¹⁴ URL: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (дата звернення 20.05.2024)

¹⁵ URL: <https://www.solarium.gov/home#h.jlr70j8saqnt> (дата звернення 20.05.2024)

Проведений аналіз ворожої інформаційної діяльності в період повномасштабного вторгнення росії дозволив виділити основні групи ворожих наративів та дезінформації. На основі дослідження, присвяченого ролі соціальних платформ у поширенні неправдивої інформації та ворожих наративів, сформульовано рекомендації, спрямовані на підвищення опору ворожій інформаційній діяльності та стійкості суспільства до зовнішніх загроз. Серед яких розвиток медіа-грамотності серед населення, що допоможе громадянам критично оцінювати інформацію та розпізнавати дезінформацію, систематичний моніторинг дезінформаційних кампаній та співпраця з іншими країнами з метою обміну інформацією та координації зусиль у протидії інформаційним загрозам.

Подальші дослідження у цьому напрямку можуть включати вивчення способів виявлення та протидії маніпуляціям у соціальних мережах, розумінні психологічних механізмів сприйняття дезінформації та її вплив на суспільну стабільність.

Список використаних джерел.

1. Горбань Ю. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. 136-141. URL: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21
2. Драбюк С. Пропаганда та її види. Шляхи протидії пропаганді. *Аналітично-порівняльне правознавство*. 2022. №5. 153-157. URL: <https://doi.org/10.24144/2788-6018.2022.01.28>
3. Горун О. Засади формування ворожої пропаганди та заходи протидії їй в умовах воєнного стану в Україні. *Інформація і право*. 2023. № 2(45). 163-171. URL: [https://doi.org/10.37750/2616-6798.2023.2\(45\).282340](https://doi.org/10.37750/2616-6798.2023.2(45).282340)
4. Денисюк Ж. 3. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В.І. Вернадського. Серія: державне управління*. 2021. Том 32 (71) № 2. 46-51. URL: <https://doi.org/10.32838/TNU-2663-6468/2021.2/08>
5. Шевців М., Гончарук К. Пропаганда як соціально-правове явище: проблеми розуміння. *Актуальні проблеми історико-правової та міжнародно-правової науки. Південноукраїнський часопис*. 2019. Випуск 1. 119–122. URL: <https://doi.org/10.32850/sulj.2019.1-29>
6. Дубов Д., Баровська А., Каздобіна Ю. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод.мат. К.: УФСБ, 2020. 60 с. URL: https://ufss.com.ua/wp-content/uploads/2020/03/UFSS_MediaLiteracy.pdf
7. Лісневська А. Дезінформація в новинному відеоконтенті: маркери та методи розпізнавання. *Вісник Львівського університету. Серія Журналістика*. 2019. 45. 60-66. URL: <http://dx.doi.org/10.30970/vjo.2019.45.9985>
8. Павленко Т. Дезінформація: поняття, ознаки та перспективи протидії. *Юридичний науковий електронний журнал*. 2022. 7. 337-339. URL: <https://doi.org/10.32782/2524-0374/2022-7/80>
9. Шульська Н., Зінчук Р., Кевлюк І. Наративи формування зневіри як вияв ворожої інформаційно-психологічної операції: на матеріалі мови ЗМІ. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Журналістика*. 2023. Т. 34 (73). № 2. Ч. 2. 152–157. URL: <https://doi.org/10.32782/2710-4656/2023.2.2/25>
10. Іваницька Б., Данилів О. Вплив та значення фейків у світовій історії. *Вісник Національного університету “Львівська політехніка”*. Серія: Журналістські науки. 2020. 4. 143-147. URL: <https://doi.org/10.23939/sjs2020.01.143>
11. Золотухін Д. Біла книга спеціальних інформаційних операцій проти України 2014-2018. Київ: 2018. 384 с.
12. Treyger E., Cheravitch J., Raphael S. Cohen, Russian Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation. 2022, URL: <https://doi.org/10.7249/RR4373.2>
13. Disinformation and russia’s war of aggression against Ukraine. OECD Policy Responses on the Impacts of the War in Ukraine. 2022. URL: <https://doi.org/10.1787/dc825602-en>

14. Flore M. Understanding Citizensâ Vulnerabilities (II): From Disinformation to Hostile Narratives. EUR 30029 EN. Publications Office of the European Union, Luxembourg, 2020 URL: : <https://doi.org/10.2760/276141>, JRC118914.

15. Harold S., Beauchamp-Mustafaga N., Hornung J. Chinese Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation. 2021. URL: <https://doi.org/10.7249/RR4373.3>

References.

1. Horban, Yu. (2015), "Information war against Ukraine and means of its conduct", *Bulletin of the National Academy of State Administration under the President of Ukraine*, Vol., 1, 136-141, URL: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21

2. Drabyuk, S. (2022), "Propaganda and its types, Ways of countering propaganda". *Analytical and comparative jurisprudence*, Vol. 5, 153–157. URL: <https://doi.org/10.24144/2788-6018.2022.01.28>

3. Horun, O. (2023), "Principles of formation of enemy propaganda and countermeasures against it in the conditions of martial law in Ukraine", *Information and Law*, Vol. 2(45), 163-171. URL: [https://doi.org/10.37750/2616-6798.2023.2\(45\).282340](https://doi.org/10.37750/2616-6798.2023.2(45).282340)

4. Denisyuk, Zh. Z. (2021), "Propaganda and counter-propaganda in the context of state information policy strategies", *Academic notes of TNU named after V.I. Vernadskyi. Series: Public Administration*, Vol. 32 (71) No. 2, 46-51. URL: <https://doi.org/10.32838/TNU-2663-6468/2021.2/08>

5. Shevtsiv, M. and Honcharuk, K. (2019), "Propaganda as a socio-legal phenomenon: problems of understanding". *Actual problems of historical-legal and international legal science. South Ukrainian magazine*, Issue 1, 119–122. URL: <https://doi.org/10.32850/sulj.2019.1-29>

6. Dubov, D., Barovska, A. and Kazdobina, Yu. (2020), Destructive influences and negative narratives: detection and countermeasures tools: method. mat. K.: UFBS, 60 p., URL: https://ufss.com.ua/wp-content/uploads/2020/03/UFSS_MediaLiteracy.pdf

7. Lisnevskaya, A. (2019), "Misinformation in news video content: markers and methods of recognition", *Bulletin of Lviv University. Series of Journalism*, 45, 60-66. URL: <http://dx.doi.org/10.30970/vjo.2019.45.9985>

8. Pavlenko, T. (2022), "Disinformation: concepts, signs and countermeasures prospects", *Legal Scientific Electronic Journal*, 7, 337-339. URL: <https://doi.org/10.32782/2524-0374/2022-7/80>

9. Shulska, N., Zinchuk, R. and Kevlyuk, I. (2023), "Narratives of the formation of despair as a manifestation of a hostile informational and psychological operation: on the material of the language of mass media", *Scholarly notes of V. I. Vernadsky Tavri National University. Series: Philology. Journalism*, T. 34 (73), No. 2. Part 2, 152–157. URL: <https://doi.org/10.32782/2710-4656/2023.2.2/25>

10. Ivanytska, B. and Danilov, O. (2020). The influence and importance of fakes in world history. *Bulletin of the Lviv Polytechnic National University. Series: Journalistic Sciences*, 4, 143-147. URL: <https://doi.org/10.23939/sjs2020.01.143>

11. Zolotukhin, D. (2018). White book of special information operations against Ukraine 2014–2018. Kyiv: 384 p.

12. Treyger, E., Cheravitch, J. and Raphael, S. (2022). Cohen, Russian Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation. URL: <https://doi.org/10.7249/RR4373.2>

13. Disinformation and Russia's war of aggression against Ukraine. (2022), OECD Policy Responses on the Impacts of the War in Ukraine, URL: <https://doi.org/10.1787/dc825602-en>

14. Flore, M. (2020). Understanding Citizensâ Vulnerabilities (II): From Disinformation to Hostile Narratives, EUR 30029 EN, Publications Office of the European Union, Luxembourg, URL: <https://doi.org/10.2760/276141>, JRC118914.

15. Harold, S., Beauchamp-Mustafaga, N. and Hornung J. (2021). Chinese Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation. URL: <https://doi.org/10.7249/RR4373.3>

Стаття надійшла до редакції 20.05.2024 р.

Рецензовано 16.08.2024 р.

Опубліковано 30.08.2024 р.