УДК 343.2/.7:004.056(477)
DOI: 10.15587/2523-4153.2024.309074

ЄВРОПЕЙСЬКИЙ ДОСВІД ПРОТИДІЇ ДЕЗІНФОРМАЦІЙНИМ ВПЛИВАМ

А. Ю. Ковальчук, Б. В. Чернявська

Information-psychological influences, attacks, and operations do not have a physical manifestation but generate destabilizing internal and external processes within a state. These processes cause aggression, anxiety, and dissatisfaction among the population, potentially leading to open physical conflict. The use of the Internet enables extremist organizations to access mass media, spreading propaganda, informing about their goals, tasks, measures, and forms of support. The authors emphasize the significant impact of modern information and communication technologies on increasing threats to political stability and the security of any state. The aim of this paper is to highlight foreign experiences regarding organizational and legal measures that prevent the spread of disinformation, aimed at inciting hostility and hatred within a state. The study draws on experiences from large-scale protest actions, organized and coordinated through social networks on the Internet. The authors note that blogs, social networks, electronic maps, and video hosting sites are currently used without restrictions for political destabilization. Social networks enable immediate support from like-minded individuals and the publication of extremist materials, which contribute to the escalation of socio-political, ethnic, and interfaith conflicts. The main research methods are comparative analysis, statistical method, historical method, structural-functional method of cognition. Having studied the periods of formation of the system for countering the spread of disinformation in the EU, the authors concluded that the work on countering the spread of disinformation is conducted comprehensively and systematically and is constantly being improved in accordance with the challenges. In the EU countries, not only the practice of combating disinformation has been developed, but also an array of normative legal acts has been adopted to prevent the spread of disinformation. The European experience demonstrates the importance of a balance between freedom of speech and security measures in the information space. Such a comprehensive and conceptual approach should be the basis for creating a system for countering the spread of disinformation in Ukraine

Keywords: *security, threats, disinformation, national/state security, information security, information and communication technologies, information-psychological influences, information warfare*

How to cite:
Kovalchuk, A., Cherniavska, B. (2024). European experience in counteracting disinformation influences. ScienceRise: Juridical Science, 2 (28), 50–54. http://doi.org/10.15587/2523-4153.2024.309074

1. Вступ

Інтенсивне впровадження інформаційних технологій у всі сфери суспільного життя є ключовим глобальним фактором, який визначає подальший розвиток людства у духовному, інтелектуальному та соціально-економічному плані. Разом з такою інтенсивністю глобальних змін відбувається наповнення новим змістом інформаційне буття людини, відбуваються зміни у технологіях донесення інформації. Разом з тим, одним з негативних наслідків глобальної інформатизації стало поширення різних форм міждержавних протиборств, які розпалюються шляхом здійснення інформаційно-психологічних впливів, як частини операцій наступального значення. Одним з найпоширеніших видів інформаційно-психологічних впливів є дезінформація. Європейське співдружність ще у 2014 році, на світовому економічному форумі означила поширення дезінформації в Інтернеті як одну з десяти тенденцій розвитку сучасного світу [1]. Невдовзі, дезінформація була визнана головним викликом сьогодення для об'єднаної Європи, європейської демократії та європейських цінностей [2]. Таке гостре питання не оминає й науковців, які з різних сторін досліджують проблему запобігання поширенню дезінформації та інших деструктивних інформаційно-психологічних впливів.

Поширення дезінформації становить значну загрозу для національної безпеки будь-якої країни. Разом з тим, слід уточнити, що операції з поширення дезінформації, є комплексними і включає у себе певний процес, що складається з елементів та стадій розгортання, а саме: обрання методів інформаційно-психологічних впливів, підготовки інфраструктури в країнах-мішенях, що включають: розгортання місцевих ЗМІ, некомерційних організацій, громадських об'єднань та кластерів впливу з лідерів громадської думки, створення регіональних представництв подібних глобальних структур на користь замовника інформаційної операції, для просування альтернативної порядку денного, підриву авторитету чинної влади країни-мішені з завданням їхнього подальшого зміщення та заміни на підконтрольних фігур [3]. Тобто, дезінформація, яка розповсюджується є

фактично завершальною стадією досягнення поставленої цілі країною-замовником, або країною агресором. З 2015 – 2024 рік зовнішньополітична служба Євросоюзу зафіксувала 17 тисяч інцидентів прокремлівської дезінформації, пов'язаних із прокремлівськими діячами. З цих інцидентів понад 1500 – у 2024 році [4]. Це значна кількість, але достеменно невідомо реальні наслідки таких дезинформаційних впливів. Тому, нині особливого значення пошуку шляхів упередження поширення дезінформації на ранішніх стадіях їх розповсюдження, з метою упередження настання негативних наслідків, а саме посилення агресивних настроїв у суспільстві.

На перший погляд, невидимі інструменти інформаційно-психологічних впливів, як елементи будь-якої інформаційної або кібероперації (які проводяться із залученням методів соціальної інженерії), стали сьогодні самостійним інструментом як внутрішньої, так і зовнішньої політики противборств. Якісний стрибок у розвитку інформаційно-комунікаційних технологій, насамперед мережі Інтернет, а також розвиток штучного інтелекту і Інтернету речей надають безпрецедентні можливості щодо формування громадської думки, впливу на прийняття політичних, економічних та військових рішень, впливу на інформаційні ресурси та дезінформацію опонентів [5]. Це сприяє розширенню можливостей задля дестабілізації будь-яких процесів у державі: від політичних, економічних до соціальних. Новітні технології, у поєднанні з науковими дослідженнями у сфері психології, PR, менеджменту, соціології тощо, впливають на розширення можливостей впливати на об’єкти впливу (людську свідомість та підсвідомість) і дають можливість залучити більшу кількість прихильників тієї чи іншої ідеї, поглядів тощо. Послідовна реалізація інформаційно-психологічних впливів у результаті проявляється як відкриті протистояння і збройні конфлікти. Тому надзвичайно важливою є розробка правового визначення стандартів психотехнологічного захисту з метою убезпечення людини, суспільства та держави в цілому від наслідків деструктивних впливів.

2. Літературний огляд

Аналіз останніх досліджень та публікацій у відкритих джерелах вказує на проблему швидкого поширення дезінформації та політичних наслідків, які стали можливі у результаті непродуманих дій, якими країни намагалися нейтралізувати загрозу поширення дезінформації [2, 5]. У деяких випадках заходи були занадто надмірні, відповідно, порушували європейські цінності у контексті забезпечення свободи слова (de Hingh, A. E., & Lodder, A. R. (2017) [6]. У інших, такі дії взагалі ігнорувалися відповідно негативні наслідки не забарилися. На жаль, разом з розвитком технологій невідмінно зростають й виклики для системи забезпечення безпеки: розширяється інструментарій технологій комунікативної політики держав, поширюється проблема інформаційного тероризму (інформаційного насильства), поширюється застосування невербальних технологій інформаційних впливів тощо (Van der Linden, T. (2024) [5]. А відтак, проблема протидії дезінформації й вироблення загальноєвропейської політики забезпеченні інформаційної безпеки ще не набула належної концептуалізації [5, 6].

В основу дослідження були покладені матеріали розслідувань, судових рішень щодо джерел розповсюдження дезінформації у Європі. Лідером по поширенню неправдивої інформації залишається Doppelganger (DoppelGänger). DoppelGänger – це кампанія, що організовує і здійснює інформаційні компанії впливу, які спрямовані як на поширення дезінформації у Франції, Німеччині, Україні та США. Крім того, їх цілеспрямовані зусилля спрямовані на аудиторію у Великобританії, Литві, Швейцарії, Словаччині та Італії, але в меншому масштабі [7]. Мережа Doppelganger використовує комбінацію «контент-ботів», які розміщують посилання, і «ботів-промоутерів», які потім поширюють ці заздалегідь підготовлені твіти. Doppelganger добре відома тим, що використовує мережу для поширення посилань на фейкові версії справжніх новинних сайтів.

З метою вироблення нових підходів у протидії поширенню дезінформації вивчалися погляди науковців з різних галузей. Щодо огляду суто теоретичних джерел слід зазначити, що інформаційні впливи, як елемент інформаційно-психологічних операцій, є предметом дослідження представників різних галузей науки. Як зазначає Карл фон Клаузевіц: «Війна завжди була пов’язана з розумом: визначав війну як «акт насильства, спрямований на те, щоб змусити супротивника виконати нашу волю» [8]. У світлі військової історії та стратегічної думки твердження Джеймса Джордано про те, що «людський мозок став полем бою 21 століття» актуально і сьогодні. Tom Dobber, Sanne Kruikemeier and Ellen Goodman окремо досліджують політичну рекламу як інструмент маніпулювання думкою громадян [9].

Репрезентативним, на наш погляд, є дослідження, що проведено Дж. Аркіллою у якому сформовано поняття «інформаційна революція» і зазначається, що новітні досягнення в області інформаційних технологій істотно посилили процеси об’єднання людей навколо певної ідеї, відповідно впливати на їх спосіб мислення стає легше й ефективніше. Дж. Аркілла стверджує: «звичні ієрархічні структури держав виявилися малоефективними в протистоянні з мережами, таким чином «щоб протистояти мережі, потрібна мережа» [10].

3. Мета та завдання дослідження

Проаналізувати сучасні правові та організаційні важелі, які застосовуються у різних країнах світу задля перешкоджання масовому розповсюдженню дезінформації та виділити серед них позитивні практики, а також визначити шляхи впровадження їх у сучасну систему протидії дезінформації в Україні.

Для досягнення мети, нами були визначені такі дослідницькі завдання:

1) визначити зміст заходів, у тому числі організаційно-правових, протидії дезінформації в ЄС;

2) дослідити процедуру вироблення контрзаходів з метою протидії дезінформації;

3) охарактеризувати інструменти та види поширення дезінформації;

4) означити нерозв'язані проблеми політики протидії дезінформації.

4. Матеріали і методи

Матеріалами, що були покладені в основу дослідження становлять як практичні посібники з виявлення дезінформації, так і практика реалізації 27-х компаній з дезінформації, які були проведені різними представництвами Doppelganger, які обслуговують російську пропаганду і були проведені на території різних країн Європи та інших країнах світу у період з 2022–2027 років.

Для пошуку джерел інформації дослідження були використані різноманітні ресурси: електронна бібліотека Ради Європи, наукові бази даних Google Scholar, Clarivate, Web of Science, Scopus та інші, що надають доступ до великої кількості академічних статей і досліджень.

Методологічною основою дослідження складає сукупність загальновизнаних методів наукового пізнання. Для отримання наукових результатів застосовувалися загальнонаукові принципи та підходи. Використання історичного, соціологічного та інших методів зумовлено необхідністю дослідження різних підходів до визначення дезінформації. Історико-правовий, історико-порівняльний, нормативний, діалектичний, системно-структурний та інші методи були задіяні з метою виявлення закономірностей формування заходів протидії дезінформації. Основним методом дослідження є метод компаративістики й комплексного підходу до вирішення проблеми протидії дезінформації.

5. Результати дослідження та їх обговорення

У ЄС вироблялися різні стратегії протидії дезінформації. Спочатку були виділені найбільш вразливі сфери. Ще у 2014 році зазначалося, що поширення дезінформації викривлює думку громадян, які є суб'єктами вироблення політики на національному та європейському рівнях, призводить до можливостей маніпулювання змістом політики, переважно в сферах національної безпеки, міграційних процесів, охорони здоров'я, наукової та освітньої політики. Близько 80 % європейців кілька разів на місяць і більше стикалися з інформацією, яку вони вважають неправдивою або такою, що вводить в оману, і 85 % сприймають це як проблему для своєї країни. Зважаючи на те, що дезінформація руйнує довіру до політичних інститутів демократії, перешкоджає громадянам у використанні створених нею можливостей впливати на політику відповідно до власних, а не нав'язаних переконань, та спрямована на підтримку радикальних та екстремістських ідеї та моделей політичної діяльності, починаючи з 2014 р., Європейський Союз систематизував процес вироблення спільної політики протидії зовнішнім інформаційним впливам, метою яких є сфера політичних відносин. Така систематизація відбулася за суб'єктами донесення інформації. Цікавим є досвід Німеччини, законодавство якої поклало на власників соцмереж обов'язок один раз на пів року звітувати про отримані скарги на розповсюдження на їхніх платформах протиправного контенту. Окрім того, вони повинні запровадити на платформах ефективну та прозору систему розгляду скарг на контент і видаляти його протягом 24 годин (для очевидно протиправного контенту) або 7 днів (для «простого» протиправного контенту) після отримання скарги. Штрафи за порушення цих вимог можуть досягати 5 мільйонів євро.

Знову ж таки, такими заходами фіксувалися явні впливи, або застосування слів «мови ненависті». Саме ж поняття дезінформації дещо ширше. Дезінформація, як один з видів інформаційно-психологічних впливів (від фран. «спотворення інформації») – це продукт діяльності людини, спроба створити хибне враження і, відповідно, підштовхнути об'єкт впливу до бажаних дій чи бездіяльності. До головних понять, що є основою будь-яких маніпуляцій, можна віднести такі поняття, як «брехня» та «омана». Окрім цих понять, з метою омани застосовуються наступні дії: «блеф», «хитрість», «демагогія», «махінація», «інтрига» тощо. Цей перелік не вичерпний, відповідно такі дії не визначені у правовому полі. Дезінформація, це маніпуляції не лише з самою інформацією, а й її сприйняттям. Тобто, розробляючи дезінформаційні впливи, передбачається як саме вони будуть трактовані об'єктом сприйняття. Відповідно будуючи систему протидії дезінформації не слід забувати про особливості сприйняття інформації, й уразливості психіки людини.

Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг і внесення змін до Директиви 2000/31/ЕС (Закон про цифрові послуги) став правовою основою діяльності, яка спрямована на виявлення, ідентифікацію та протидію незаконному контенту, або поширенню дезінформації.

Також у ЄС в червні 2022 року було підписано Кодекс практик протидії дезінформації (The Code of Practice on Disinformation). Це був перший прецедент, коли власники медійних каналів тощо погодилися на саморегулювальні стандарти задля боротьби з дезінформацією. Кодекс охоплював 44 зобов'язання та 128 конкретних заходів у таких сферах:

1. контроль за розміщенням реклами (в тому числі зменшення фінансових стимулів для розповсюджувачів дезінформації);

2. забезпечення прозорості політичної реклами;

3. доброчесність послуг;

4. розширення прав і можливостей користувачів;

5. надання ширшого доступу до даних дослідникам; 6. посилення співпраці зі спільнотами фактчекінгу.

Втім, на практиці платформи не запровадили ці заходи задля ефективної протидії дезінформації, як виявилося невдовзі [11].

Європейський центр SAGE Publishing на платформі SAGE Knowledge [12] розробив довідник з пропаганди та дезінформації, де роз'яснюється їх шкода для психіки людини. У довіднику зроблено огляд того, як інформація, що подається за допомогою цілком законних методів, вторгається в людську психіку і які деструктивні наслідки відбуваються. Будучи спокусливим інструментом політичного переконання під час війни, миру та невизначеності, дезінформація спонукає людей до свідомих чи несвідомих дій, часто насильницьких. Цей інформаційно-психологічний вплив особливо поширений у світовій політиці та міжнародних відносинах [9]. Слід звернути особливу увагу поширенню дезінформації в Інтернеті. У довіднику також приділено увагу застосуванню таргетованої онлайн-реклами, під час якої застосовується інформаційна асиметрія між рекламодавцем і одержувачем. Вважається, що інформаційна асиметрія є проблематичною для громадян, оскільки асиметрія обмежує здатність громадян оцінювати інформацію, що негативно впливає на здатність громадян приймати обґрунтовані та самостійні рішення. Ця асиметрія знайшла відображення у справі Cambridge Analytica, коли дані мільйонів мимовільних користувачів Facebook були зібрані та використані для класифікації їхніх особистісних рис. Тоді Cambridge Analytica стверджувала, що використовувала цю інформацію, щоб розсилати людям політичну рекламу, адаптовану до їх особистості (застосовуючи таргетовану рекламу і dark patterns). Ці приховані спроби переконати людей були названі маніпулятивними, і його можна розглядати як поворотний момент, який активізував діяльність урядових структур до розробки правових механізмів захисту суспільних цінностей та приватних даних споживачів, а також щодо продуктів і діяльності великих технологічних компаній, таких як Facebook [9, 10].

Наступним етапом становлення політики протидії дезінформації стало поширення інформаційного просвітництва та організація поширення знань про кібергігієну. Але, інформаційна гігієна й кібергігієна дещо різні знання. Разом з тим, слід зазначити, що заходи з протидії поширення дезінформації у ЄС постійно удосконалюються. Такий всеосяжний та концептуальний підхід повинен бути покладений в основу створення системи протидії поширенню дезінформації та іншим інформаційно-психологічним впливам в Україні.

Перспективою подальших досліджень вбачається розробка спільних проєктів представників різних галузей науки. Ми ще раз підкреслюємо вірність погляду Дж. Аркіллою [10] про те, що лише спільним зусиллями та системною діяльністю можна ефективно протидіяти поширенню дезінформації.

6. Висновки

Вивчивши періоди становлення системи протидії поширенню дезінформації у ЄС, можна зробити висновки про те, що робота ведеться комплексно й системно. В країнах ЄС напрацьована не лише практика, а й прийнятий масив нормативно-правових актів щодо упередження розповсюдження дезінформації. Європейський досвід демонструє важливість балансу між свободою слова та безпекою в інформаційному просторі.

Підводячи підсумки, пропонується:

1. З метою приведення чинного законодавства України до стандартів ЄС, повернутися до розробки проекту закону «Про протидію дезінформації» в Україні, з метою визначення системи державних і недержавних суб'єктів, що будуть наділені повноваженнями у сфері протидії поширенню дезінформації.

2. Слід у законі передбачити концептуальний підхід до системи протидії дезінформації та утвердження демократії. Принцип свободи слова та свободи вираження власних переконань повинен бути врахований при обранні заходів з протидії дезінформації.

3. Запровадити обов'язкову звітність для власників соціальних мереж та платформ щодо отриманих скарг на розповсюдження дезінформації та протиправного контенту, як це реалізовано у Німеччині. Наприклад, платформи повинні звітувати про кількість скарг та їх результати, що сприятиме прозорості та підзвітності (CFR, 2024).

4. Сприяти розвитку інформаційної та кібергігієни серед громадян шляхом інформаційного просвітництва та кампаній, спрямованих на підвищення медіаграмотності. Це включає освітні програми та інформування громадян про небезпеку дезінформації (SAGE Publishing, 2024).

5. Зміцнити співпрацю з міжнародними організаціями та залучити досвід інших країн у розробці і впровадженні ефективних методів протидії дезінформації. Наприклад, використання досвіду ЄС щодо впровадження Digital Services Act (DSA) може бути корисним для України у створенні національних стандартів забезпечення інформаційної безпеки.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

У рукописі є дані, включені як додатковий електронний матеріал https://stratcomcoe.org/pdfjs/?file=/publications/download/The-Doppelganger-Case-DIGITAL.pdf?zoom=page-fit

Використання засобів штучного інтелекту

Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Література

1. Top 10 trends of 2014: 10. The Rapid Spread of Misinformation Online (2014). World Economic Forum.
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling Online Disinformation: a European Approach. COM/2018/236 final (2018). Eur-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236
3. McCuen, J. J. (2008). Hybrid Wars. Military Review. Fort Leavenworth: Combined Arms Center. March-April, 107–113. Available at: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Military Review_20080430 _art017.pdf
4. Польска, К. (2024). Дослідження: Росія – головний дезінформатор у ЄС. Available at: https://www.dw.com/ru/issledovanie-rossia-glavnyj-rasprostranitel-dezinformacii-v-es/a-69089063
5. Van der Linden, T. (2024). AI: We Need Another Hero. ALTI Amsterdam. Available at: https://alti.amsterdam/ai-we-need-another-hero/
6. de Hingh, A. E., Lodder, A. R. (2017). Informatieveiligheid: de digitale veerkracht van Nederlandse overheden. Bestuurskunde, 26 (1), 27–34. https://doi.org/10.5553/bk/092733872017026001005
7. The Doppelganger case assessment of Platform Regulation on the EU Disinformation Environment (2024). Riga. Available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/The-Doppelganger-Case-DIGITAL.pdf?zoom=page-fit
8. фон Клаузевіц, К. (2023). Найважливіші принципи ведення війни. Арій, 384.
9. Dobber, T., Kruikemeier, S., Helberger, N., Goodman, E. (2023). Shielding citizens? Understanding the impact of political advertisement transparency information. New Media & Society. https://doi.org/10.1177/14614448231157640
10. Arquilla, J. (2007). Information strategy and warfare: a guide to theory and practice. Available at: https://ocul-yor.primo.exlibrisgroup.com/discovery/fulldisplay?docid=alma991000892449705164&context=U&vid=01OCUL_YOR&lang=enT
11. The Strengthened Code of Practice on Disinformation (2022). Available at:https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf
12. Baines, P., O'Shaughnessy, N., Snow, N. (2020). The SAGE Handbook of Propaganda. SAGE Publications Ltd. https://doi.org/10.4135/9781526477170

Received date 07.05.2024
Accepted date 25.06.2024
Published date 30.06.2024

Ковальчук Алла Юріївна, доктор юридичних наук, професор, кафедра міжнародного права та інших галузевих правових дисциплін, Київський університет права Національної академії наук України, вул. Доброхотова, 7а, м. Київ, Україна, 01001

Чернявська Богдана Вадимівна, PhD, доцент, кафедри теорії та історії держави і права, Національна академія управління, вул. Ушинського, 15, м. Київ, Україна, 03151, Guest Researcher at the Faculty of Law, Department of Criminology, Vrije Universiteit Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands

***Corresponding author:** Alla Kovalchuk, e-mail: Kovalchukay@i.ua*