Протидія дезінформації в соціальних мережах

Єфіменко І. В.[1]

Опубліковано	Секція	УДК
30.06.2025	Право	004.62:004.77

DOI: https://doi.org/10.5281/zenodo.15826202

Анотація. У статті розглянуто поняття дезінформації, як постійно мінливої загрози, яка впливає на демократії світу та всі частини суспільства. Актуалізовано проблематику протидії дезінформації в соціальних мережах та її висвітлення в міжнародних та національних нормативно-правових актах та дослідженнях. Сьогодні потенціал соціальних медіа у поширенні дезінформації викликає серйозне занепокоєння як держави, так і громадянського суспільства. Здійснено аналіз основних аспектів та викликів, пов'язаних із розповсюдженням дезінформації рф в умовах воєнного стану. Вказано на комплексність проблеми впливу розповсюдження дезінформації та фейків на економічну, оборонну та політичну ситуацію в країні та світі. Окремо виділені питання змін у засобах та методах діяльності в медіа спецслужб рф під час повномасштабного вторгнення. Зроблені висновки щодо шляхів удосконалення протидії України шкідливому впливу дезінформації в соціальних платформах та впровадження досвіду провідних країн світу в цій сфері.

Ключові слова: штучний інтелект; інфлюєнсери; національна безпека; гібридна війна; протидія впливу спецслужб рф.

Countering disinformation on social media

Abstract. The article examines the concept of disinformation as a constantly changing threat that affects the democracies of the world and all parts of society. The issue of countering disinformation in social networks and its coverage in international and national regulatory acts and research is updated. Today, the potential of social media in spreading disinformation is of serious concern to both the state and civil society. Countering disinformation in successful democracies around the world is based on the principles of public trust in key state institutions, cooperation between the state and civil society, and a common understanding of approaches to mass media, including social platforms. According to the European Union guidelines, major online platforms need regulation to stop the flow of fake news, along with the introduction of a Code of Conduct against Disinformation, as well as the need for greater transparency of algorithms and the removal of harmful content. An analysis of the main aspects and challenges associated with the spread of disinformation in the Russian Federation under martial law is carried out. The complexity of the problem of the impact of the spread of disinformation and fakes on the economic, defense and political situation in the country and the world is proven. The issues of changes in the means and methods of activity in the media of the Russian special services during a full-scale invasion are separately highlighted. Conclusions are drawn on ways to improve Ukraine's counteraction to the harmful impact of disinformation on social platforms

[1] науковий співробітник наукової лабораторії ННІ ІБ СК, Національна академія СБ України, https://orcid.org/0009-0007-7917-1767

and the implementation of the experience of leading countries in this area. The need for decisive measures to counter disinformation, which can undermine trust, increase disagreements and hinder political participation, is emphasized. Cooperation between the states of the democratic world is of crucial importance, including information exchange and early warning systems.

Key words: artificial intelligence; influencers; national security; hybrid warfare; countering the influence of the russian special services

Вступ

За визначенням Офісу Таємної Ради Уряду Канади (Privy Council Office - центральне агентство уряду Канади, яке діє як секретаріат Кабінету Міністрів Канади та надає неупереджені консультації та підтримку канадському уряду, а також здійснює керівництво, координацію та підтримку департаментів та агентств уряду), дезінформація – це неправдива інформація, навмисно спрямована на введення в оману. Після того, як дезінформаційний наратив впроваджується в інформаційну екосистему, метою є його вірусне та несвідоме поширення іншими [1]. Дезінформація – це постійно мінлива загроза, яка впливає на демократії світу та всі частини суспільства. Протидія дезінформації – це глобальна проблема, яка вимагає реагування з боку всіх сфер суспільства – урядів, бізнесу, громадянського суспільства та окремих громадян.

В протидії дезінформації успішних демократій світу закладені принципи довіри суспільства до ключових інституцій держави, співпраці між державою та громадянським суспільством та спільне розуміння підходів до мас-медіа, в тому числі соціальних платформ. При цьому варто пам’ятати, що дезінформація може завдати шкоди як окремому громадянину, так і суспільству в цілому, атакуючи, поляризуючи та дезінформуючи людей. У найгіршому випадку дезінформація може призвести до ненависті, насильства та політичних переслідувань.

З початком повномасштабної збройної агресії рф, поєднаної з гібридною війною, в тому числі кібер-атаками на Україну, в лексиконі фахівців з інформаційної безпеки з’явився новий термін – інформаційна гігієна. За даними українських дослідників лише від 3 до 11% наших співгромадян можуть відрізнити правду від брехні в інформаційному просторі. Саме з розуміння та визнання проблеми необізнаності українців в інформаційному просторі, зокрема в найпопулярніших соціальних мережах, і починається формування інформаційної гігієни [2]. К.І. Бєляков та І.М. Шопіна, впроваджуючи новий напрямку наукового дослідження, – «інформаційна гігієна», пропонують розглядати її як «проблемний напрямок інформаційної безпеки та культури людини в межах доктрини інформаційно-правових досліджень» [3].

Для дезінформації населення України та країн демократичного світу, рф використовує різні інструменти як то іноземні (псевдо-незалежні) медіа, «хороші рускі», блогери-інсайдери та «поінформовані» телеграм-канали, ІПСО тощо. Соціальні мережі завдяки своєму проникненню у різні верстви українців та вагомий вплив на сучасну думку відіграють значну роль у веденні «інформаційної війни», застосуванні «спеціальних психологічних операцій» та пропаганді. Українські користувачі соціальних мереж несвідомо використовуються для цих шкідливих процесів та стають допоміжним інструментом для ворога.

Стратегія інформаційної безпеки України визначає її забезпечення однією з найважливіших функцій держави. Стратегія ставить завдання посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації

інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [4].

Головним викликом в процесі протидії впливу дезінформації є необхідність забезпечення гласності, права на приватність (захист конфіденційної інформації про особу, невтручання в особисте життя), яке є одним з основних прав людини, що закріплено в Загальній декларації прав людини, Конвенції про захист прав людини і основоположних свобод, інших міжнародних документах, а також українському законодавстві та конституціях більшості держав світу.

Держава повинна забезпечити баланс між цифровою трансформацією суспільства, протидією дезінформації та захистом прав людини.

Частково проблематика, пов'язана з протидією дезінформації в соціальних мережах, знайшла своє відображення у працях таких вітчизняних дослідників серед яких Мороз О., Донченко О., Кушнір І., Адамчук С. та інші. Проте, предметно особливості та виклики деструктивного впливу та протидії дезінформації в інформаційному просторі соціальних медіа, зокрема, в умовах воєнного стану, майже не досліджені.

Метою цієї статті є аналіз способів та заходів протидії дезінформації в соціальних мережах, особливо пов'язаних із протидією агресії рф.

Результати

Соціальні мережі дедалі стають одним із основних суб'єктів впливу в інформаційному просторі. Розвиток інформаційного простору в умовах глобалізації зумовили посилення ролі соціальних мереж у національному та світовому інформаційному просторі, їх вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини. Сьогодні провідні соціальні мережі зазвичай доступні кількома мовами та дозволяють користувачам спілкуватися з через географічні, політичні чи економічні кордони. За оцінками, у 2025 році кількість користувачів соціальних мереж сягне 5,42 мільярда, і очікується, що ці цифри продовжуватимуть зростати, оскільки використання мобільних пристроїв та мобільних соціальних мереж дедалі більше набирає обертів на всіх ринках.

Дослідження іноземних джерел інформації щодо протидії дезінформації в соціальних мережах дозволяє стверджувати, що правове регулювання соціальних платформ провідних країн світу іноді виглядає фрагментарним. При цьому, не існує «спеціального» законодавства для регулювання соціальних мереж, що обумовлює його різноманітність. Тому сучасна протидія дезінформації в соціальних мережах вимагає багатогранного підходу, що включає перевірку фактів (факт-чекінг), навчання медіаграмотності та регулювання платформ. Вкрай важливо розуміти контекст, потенційне охоплення аудиторії та вплив дезінформації, а також психологію того, як інформація поширюється та як у неї вірять. Сприяючи критичному мисленню, заохочуючи скептицизм користувачів та використовуючи довірені джерела, держави та спеціальні організації можуть активно боротися з поширенням неправдивої інформації [5].

Ключові рекомендації урядів Північної Америки, ЄС та європейських дослідників щодо протидії дезінформації включають наступні стратегії:

- перевірка фактів, викладених в соціальних медіа: залучення незалежних організації для перевірки контенту та викриттю дезінформації;
- освітні програми з медіаграмотності: навчання оцінюванню джерел інформації, виявленню фейків та розпізнанню маніпуляцій суспільною думкою;

- саморегулювання соціальних платформ: платформи соціальних мереж повинні впроваджувати ефективну політику для видалення шкідливого контенту, сприянню прозорості та запобігання поширенню дезінформації.
- скептицизм користувачів: заохочення користувачів критично ставитися до онлайн-інформації та перевіряти контент перед його поширенням [6];
- використання довірених джерел: користування перевіреними джерелами, такими як державні установи, наукові організації та авторитетні ЗМІ;
- психологічні підходи: застосування психологічних знань;
- стійкість до дезінформації на рівні громади: важливо розвивати стійкість громади до дезінформації через освіту, інформаційні кампанії та ініціативи, що проводяться громадою за підтримки урядів [7].

Зарубіжні дослідники вбачають такі інструменти ефективної протидії дезінформації в соціальних мережах:

- співпраця із соціальними мережами у протидії поширенню фейкового контенту на рівні встановлення чітких алгоритмів запобігання дезінформації;
- розробка інструментів на основі штучного інтелекту, що можуть бути використані для виявлення та позначення потенційно неправдивої інформації, враховуючи необхідність забезпечення прозорості та керованості таких інструментів;
- міждисциплінарні та міжгалузеві дослідження для розробки ефективних рішень на рівні співпраці між такими галузями, як інформатика, соціальні науки та психологія;
- сприяння відкритому діалогу: заохочення відкритого та шанобливого діалогу щодо суперечливих тем може допомогти зміцнити довіру та протидіяти поширенню дезінформації [8].
- Українські стратегії та інструменти протидії дезінформації в соціальних мережах, зокрема з боку рф, напрацьовуються останні десятиліття як на рівні державних органів, так і громадянського суспільства та провідних медіа. Українські дослідники визначають дезінформацію як відомості, які не відповідають дійсності, котрі адресуються як широкому загалу, так і окремому адресату, спрямовані на зміну світогляду, виклик бажаної реакції та мають (відомості) негативний контекст. Констатовано, що невід'ємним супутником поширення дезінформації є мета, якої хоче досягти суб'єкт її поширення, як правило, може мати декілька завдань, найперше це введення в оману тих, кому вона транслюється (конкретній особі чи безособово), а далі зазвичай наступний результат, якого хотів досягти зловмисник – отримання персональних даних, зміна суспільної думки (очікувана реакція) в суспільстві під час проведення виборів, інформаційної війни, отримання доступу до фінансів тощо [9].

Всі дослідники наголошують на тому, що дезінформація формується та поширюється умисно. Але з цим твердженням можна сперечатись. Йдеться про випадки дезінформації з боку блогерів, зокрема, «мільйонників», які висловлюючи власну думку можуть помилятися, дезінформуючи таким чином своїх численних підписників. В даному випадку дуже важко визначити межу між навмисною дезінформацією та ненавмисною помилкою, яка знаходить свій вираз у, так би мовити, авторській позиції.

Зважаючи на серйозний вплив дезінформації на суспільну свідомість у 2021 році було утворено Центр протидії дезінформації (ЦПД) як робочий орган Ради національної безпеки і оборони України. Метою утворення зазначеного органу було досягнення цілей та завдань Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392, у напряму протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, ефективної протидії пропаганді, деструктивним дезінформаційним впливам та кампаніям, недопущення маніпулювання

громадською думкою тощо [10]. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

ЦПД постійно наголошує на значний вплив медіа на свідомість людей. Зокрема, відзначається важливість соцмереж, які сьогодні стали не тільки ефективним засобом комунікації із суспільством, а й відкривають широкі можливості для маніпуляцій громадською думкою, зокрема, у випадку коли йдеться про блогерів у яких аудиторія 100, 200, 500 тисяч підписників або мільйон.

Керівник Центру протидії дезінформації Андрій Коваленко зазначає використання росією соцмереж для проведення інформаційних операцій на Заході, в країнах Глобального Півдня і в Україні, намагання ворога використовувати технологію створення «опозиційних медіа» для просування потрібних наративів аудиторії, що виступає проти режиму путіна.

Очільник ЦПД також наголошує на важливості об'єднання держави, вільних медіа та інфлюєнсерів у питаннях боротьби з російськими агентами, протидії інформаційним операціям та проведенню власних заходів проти російського впливу [11]. Тому час від часу ми спостерігаємо як на деякі відверті «вкиди» в соцмережах офіційні представники органів влади реагують спростуванням, також бачимо роботу СБУ по затримці тих, хто розповсюджує протиукраїнську інформацію в соцмережах тощо.

Українські спеціалісти у сфері протидії дезінформації та дослідники цієї проблематики, пропонують декілька стратегій, які можна застосувати для подолання та пом'якшення впливу дезінформації. По-перше, необхідно сприяти підвищенню медіаграмотності. Тобто, навчати людей як критично оцінювати інформацію, виявляти дезінформацію та перевіряти джерела. По-друге, це співпраця з фактчекерами. По-третє, підвищення цифрової грамотності у школах та закладах вищої освіти. Наступне – дотримання прозорості з боку соціальних мереж [12]. Також, окремою стратегією слід визначити роботу з лідерами суспільної думки щодо виваженої ретрансляції власних думок та відтворення певної інформації з чітким усвідомленням власної відповідальності за її вплив на свідомість своїх підписників. Адже недотримання зазначеної стратегії призводить до створення неприємних ситуацій, накшталт булінгу та травлі лідерів думок одним одного в соцмережах. А це, у свою чергу, призводить до схожого відношення між підписниками блогерів і створює додаткове напруження і підґрунтя для внутрішніх конфліктів всередині суспільства.

З-поміж іншого фахівці також вказують на велике значення використання алгоритмічних утручань для такого налаштування соціальних мереж, щоб вони надавали перевагу точній і достовірній інформації, а не сенсаційному чи оманливому контенту. Соціальні платформи повинні використовувати штучний інтелект і машинне навчання для виявлення та мінімізації поширення дезінформації. В епоху «роботизованої журналістики» відповідь фейкам та оманливій інформації повинна бути максимально технологічною.

Коли ми говоримо про дезінформацію у XXI столітті, маємо справу не просто з перекрученими фактами. Ми стикаємося з абсолютно новим явищем: контент, якого ніколи не існувало, але який виглядає справжнім. Це – генеративні системи штучного інтелекту. Простіше кажучи, машини, які можуть не просто обробляти інформацію, а створювати її: вигадувати зображення, писати новини, імітувати голоси та навіть генерувати обличчя, яких ніколи не було. І саме ці інструменти лежать в основі нового покоління дезінформаційних кампаній [13].

Інструменти штучного інтелекту (далі – ШІ), задіяні в поширенні дезінформації це:

- штучний інтелект, який творить ілюзію: генеративні змагальні мережі (GANs), які стоять за так званими deepfakes (англ. deepfake; поєднання слів deep learning («глибоке навчання») та fake («підробка»));
- боти, фабрики фейків і автоматизована пропаганда**:** автоматизоване створення дезінформації та її масове поширення – скрипти, армія ботів, фейкові акаунти, що поширюють фейкову інформацію тисячами репостів за лічені хвилини [14].

Найбільш суворим засобом протидії поширенню дезінформації є посилення цифрової криміналістики (Digital forensics) - комп'ютерна криміналістика або кібер-криміналістика – процес дослідження та аналізу цифрових доказів для реконструкції подій, розкриття злочинів або відновлення даних. Він включає збір, збереження, вивчення та представлення цифрових даних таким чином, щоб зберегти їх цілісність та допустимість у суді. Ця галузь має вирішальне значення як для кримінальних, так і для цивільних розслідувань, оскільки допомагає виявляти інформацію з цифрових пристроїв та систем. заохочування ініціативи громадянської журналістики, які сприяють точному висвітленню подій та сприяють створенню більш різноманітної та надійної інформаційної екосистеми [15].

В українській науці цифрова криміналістична експертиза, зокрема, відноситься до процесу збору, отримання, зберігання, аналізу та подання електронних доказів (також відомих як цифрові докази) з метою отримання слідчої інформації та розслідування та переслідування різних видів злочинів, у тому числі кіберзлочинів. Цифрова криміналістична експертиза включає процеси ідентифікації, отримання, зберігання, аналізу та представлення цифрових доказів. Криміналістичні артефакти та криміналістичні методи (наприклад, збір статичних даних або даних у реальному часі) залежать від пристрою, його операційної системи та функцій безпеки [16].

Водночас, не останню роль у протидії дезінформації в соціальних мережах відіграє наявність в них суттєвої частки відкритої, чесної, правдивої інформації – практично робота з населенням по роз’ясненню ситуацій, фейків тощо. Тому виявляється найнеобхіднішим в особливих умовах протидії збройній агресіїю працювати над тим, щоб обсяг наявної в соцмережах (наприклад, ТікТок, Інстаграм, Трендс) правдивої інформації від офіційних джерел був достатньо суттєвим відносно дезінформації.

Висновки

Соціальні мережі докорінно змінили спосіб взаємодії людей один з одним, їх спілкування та доступу до інформації. Сьогодні потенціал соціальних медіа у поширенні дезінформації викликає серйозне занепокоєння як держави, так і громадянського суспільства. Як свідчить сьогодення політична дезінформація поширена на таких найпопулярніших платформах, як Facebook, X/Twitter та Reddit, де формується думка великої кількості населення, що є особливо небезпечним під час війни.

Сучасна держава формує відповідні механізми та спеціальні органи протидії та блокування дезінформації. Однак в цій ситуації, незважаючи на воєнний стан, необхідно знайти «делікатний баланс» між боротьбою з неправдивою інформацією та захистом свободи слова, адже саме вона є основою демократії. Тому не можна заборонити висловлювати свою думку, адже лише відкритий діалог з населенням, освіта в частині інформаційної безпеки, достатня присутність якісного, актуального і цікавого контенту справді може змінити ситуацію щодо дезінформації в соцмережах та не обмежити свободу слова.

Згідно із настановами Євросоюзу, основні онлайн-платформи потребують регулювання, щоб зупинити потік фейкових новин, разом із запровадженням Кодексу поведінки проти дезінформації, а також необхідністю більшої прозорості алгоритмів та видалення шкідливого контенту. Ключову роль у боротьбі з дезінформацією відіграють ЗМІ. ЄС повинен захищати плюралізм та незалежність ЗМІ, надаючи фінансування та

підтримку незалежним ЗМІ, сприяючи журналістським розслідуванням та притягуючи ЗМІ до відповідальності за поширення дезінформації. ЄС також має заохочувати заходи саморегулювання, підтримувати ініціативи щодо перевірки фактів та вирішувати питання концентрації власності ЗМІ для забезпечення прозорості та підзвітності.

Для захисту демократичних виборчих процесів необхідні рішучі заходи для протидії дезінформації, яка може підривати довіру, посилювати розбіжності та перешкоджати політичній участі. Співпраця між державами демократичного світу, включаючи обмін інформацією та системи раннього попередження, має вирішальне значення.

Список використаних джерел

1. Офіційний сайт Уряду Канади. URL : https://www.canada.ca/en/privy-council.html.
2. Мороз О. Інформаційна гігієна під час війни: 7 базових правил. Освіторія. URL : https://osvitoria.media/experience/informatsijna-gigiyena-pid-chas-vijny-7-bazovyh-pravyl/.
3. Харітонов Є.О., Харітонова О.І., Бєляков К.І. Права приватної особи в умовах пандемії COVID-19. Київ: Гельветика. 2020. С. 404.
4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text.
5. Fighting the Invisible Enemy: Countering Disinformation & Misinformation. European Movement International. URL : https://europeanmovement.eu/policy/fighting-the-invisible-enemy-countering-disinformation-misinformation/#:~:text=Key%20Recommendations,media%20accountable%20for%20spreading%20disinformation.
6. Detecting and reporting disinformation : Privy Council Office, Government of Canada. URL : https://www.canada.ca/en/privy-council/news/2025/03/detecting-and-reporting-disinformation.html.
7. 8 recommendations for countering misinformation : American Psychological Association. URL : https://www.apa.org/topics/journalism-facts/misinformation-recommendations.
8. Combating Misinformation on Social Media. ScincesPo Magazine. 26.02.2025. URL : https://www.sciencespo.fr/en/news/combating-misinformation-on-social-media/#:~:text=The%20first%20process%20leads%20users,Each%20process%20impacts%20this%20cost.
9. Кушнір І.П., Адамчук С.В. Протидія дезінформації: організаційно-правовий аспект. Аналітично-порівняльне правознавство. 2025. Вип. 01. URL : https://app-journal.in.ua/wp-content/uploads/2025/02/80.pdf.
10. Про створення Центру протидії дезінформації : Рішення Ради Національної безпеки і оборони України від 11 бер. 2021 р. № 0015525-21. URL : https://zakon.rada.gov.ua/laws/show/n0015525-21#Text.
11. Як рф використовує соцмережі для інформаційних операцій на Заході та Глобальному Півдні : Офіційний сайт ЦПД. URL : https://cpd.gov.ua/events/yak-rf-vykorystovuye-soczmerezhi-dlya-informaczijnyh-operaczij-na-zahodi-ta-globalnomu-pivdni/.
12. Бондаренко С. Ю. Негативні наслідки та шляхи протидії дезінформації в соціальних мережах як масовому негативному явищу. Протидія дезінформації в умовах російської агресіїпроти України: виклики і перспективи. Харків, 2023. С. 200-204.
13. Роль штучного інтелекту, дипфейків та алгоритмів соцмереж у поширенні дезінформації. Vilni Media Production. 8 чер. 2025. URL : https://vilni-media.com/2025/06/08/rol-shtuchnoho-intelektu-dypfejkiv-ta-alhorytmiv-sotsmerezh-u-poshyrenni-dezinformatsii/.

14. Komendantova N., Erokhin D. Artificial Intelligence Tools in Misinformation Management during Natural Disasters. Public Organiz Rev 25, 81–105 (2025). https://doi.org/10.1007/s11115-025-00815-2.
15. Digital forensics : Офіційний сайт Інтерполу. URL: https://www.interpol.int/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20law%20enforcement%20investigations.
16. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. Київський часопис права. 2022. № 1. С. 176-180.