УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2025.6.20

ШКЛЯР Д.М.

ПОНЯТТЯ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ШКІДЛИВОМУ КОНТЕНТУ В МЕДІА

THE CONCEPT OF PREVENTING AND COUNTERING DISINFORMATION AND HARMFUL CONTENT IN THE MEDIA

Актуальність статті полягає в тому, що система забезпечення національної безпеки носить складний характер, що обумовлено її широким елементним складом. Водночас, аналіз наукових позицій дає підстави стверджувати, що зазначені дослідники, попри комплексний характер запропонованих ними підходів, не виокремлювали запобігання та протидію дезінформації, а також поширенню шкідливого контенту в медіа як самостійні елементи системи національної безпеки, що свідчить про наявність певної прогалини у теоретичному осмисленні сучасних інформаційних загроз. Мета статті полягає у необхідності визначити поняття запобігання та протидії дезінформації та шкідливому контенту в медіа. У статті, спираючись на аналіз наукових поглядів вчених, аргументовано, що дезінформація відрізняється від шкідливого контенту, насамперед, за своєю природою та функціональним призначенням, оскільки перша полягає у цілеспрямованому поширенні неправдивої або спотвореної інформації з метою введення аудиторії в оману, тоді як шкідливий контент може містити як правдиві, так і неправдиві відомості, але завдає шкоди через свій зміст, форму або контекст поширення, наприклад, шляхом пропаганди насильства, мови ворожнечі, маніпуляції емоціями чи підриву моральних і правових засад суспільства. Зроблено висновок, що запобігання та протидія дезінформації та шкідливому контенту в медіа представляє собою врегульовану нормами чинного законодавства цілеспрямовану, системну діяльність держави, медіасередовища й суспільства, яка спрямована на своєчасне виявлення, обмеження поширення та нейтралізацію навмисно або структурно викривленої, маніпулятивної чи деструктивної інформації, що здатна завдати шкоди суспільним інтересам, демократичним процесам, правам і свободам людини, інформаційному суверенітету та національній безпеці Україна, а також на створення умов для формування стійкого, відповідального й достовірного медіапростору через правові, інституційні, технологічні та освітні механізми.

Ключові слова: *запобігання, протидія, дезінформація, шкідливий контент, медіа.*

The relevance of the article lies in the fact that the system of ensuring national security is complex, which is due to its wide elemental composition. At the same time, the analysis of scientific positions gives grounds to assert that the mentioned researchers, despite the complex nature of the approaches they proposed, did not single out the prevention and counteraction to disinformation, as well as the spread of harmful content in the media as independent elements of the national security system, which indicates the presence of a certain gap in the theoretical understanding of modern information threats. The purpose of the article is the need to define the concept of prevention and counteraction to disinformation and harmful content in the media. The article, based on the analysis of the scientific views of scientists, argues that disinformation differs from harmful content,

© ШКЛЯР Д.М. – здобувач (Науково-дослідний інститут публічного права) https://orcid.org/0009-0005-2231-5403

primarily in its nature and functional purpose, since the former consists in the purposeful dissemination of false or distorted information with the aim of misleading the audience, while harmful content can contain both true and false information, but causes harm due to its content, form or context of dissemination, for example, by promoting violence, hate speech, manipulating emotions or undermining the moral and legal foundations of society. It was concluded that preventing and countering disinformation and harmful content in the media is a targeted, systematic activity of the state, media environment and society, regulated by the norms of current legislation, which is aimed at timely detection, restriction of the distribution and neutralization of intentionally or structurally distorted, manipulative or destructive information that can harm public interests, democratic processes, human rights and freedoms, information sovereignty and national security of Ukraine, as well as at creating conditions for the formation of a sustainable, responsible and credible media space through legal, institutional, technological and educational mechanisms.

Key words: *prevention, counteraction, disinformation, harmful content, media.*

Актуальність теми. Система забезпечення національної безпеки носить складний характер, що обумовлено її широким елементним складом. Зокрема, О.В. Глазов акцентує увагу на тому, що на сучасному етапі розвитку науки безпекознавства виділяють основні елементи структури національної безпеки: 1) державну безпеку – поняття, що характеризує рівень захищеності держави від зовнішніх і внутрішніх загроз; 2) громадську безпеку – поняття, виражене у рівні захищеності особистості і суспільства, переважно, від внутрішніх загроз; 3) техногенну безпеку – рівень захищеності від загроз техногенного характеру; 4) екологічну безпеку і захист від загроз стихійних лих; 5) економічну безпеку; 6) енергетичну безпеку; 7) інформаційну безпеку; 8) безпеку особистості [1]. Схожий підхід пропонують Д.Г. Павленко, Ю.В. Семенюк та Ю.М. Лисецький. Автори пишуть, що на сучасному етапі розвитку науки безпекознавства виділяють такі основні складники національної безпеки: безпеку особистості; державну безпеку – поняття, що характеризує рівень захищеності держави від зовнішніх і внутрішніх загроз; громадську безпеку – поняття, виражене рівнем захищеності особистості й суспільства переважно від внутрішніх загроз; техногенну безпеку – рівень захищеності від загроз техногенного характеру; екологічну безпеку й захист від загроз стихійних лих; економічну безпеку; енергетичну безпеку (як складник економічної безпеки); інформаційну безпеку; кібербезпеку [2]. Водночас, аналіз наведених наукових позицій дає підстави стверджувати, що зазначені дослідники, попри комплексний характер запропонованих ними підходів, не виокремлювали запобігання та протидію дезінформації, а також поширенню шкідливого контенту в медіа як самостійні елементи системи національної безпеки, що свідчить про наявність певної прогалини у теоретичному осмисленні сучасних інформаційних загроз.

Стан дослідження. Окремі проблемні питання, присвячені запобіганню та протидії дезінформації та шкідливому контенту в медіа, у своїх наукових працях розглядали: К.А. Дубняк, І.П. Кушнір, Л.А. Найдьонова, С.В. Руцький, М.М. Шевченко, Р.М. Шевчук, В.С. Шестак та багато інших. Втім, незважаючи на значний теоретичний доробок, в науковій літературі фактично неопрацьованим є поняття запобігання та протидії дезінформації та шкідливому контенту в медіа.

Саме тому метою статті є: визначити поняття запобігання та протидії дезінформації та шкідливому контенту в медіа.

Виклад основного матеріалу. І.П. Кушнір та С.В. Адамчук вказують, що розглядати дезінформацію, як інформацію (дані) чи повідомлення, яке повністю чи частково є неправдивим, перекрученим, взятим із контексту з негативною метою (може бути будь-що: психологічний вплив, зміна поведінки та думок суб'єкта впливу, отримання даних про банківські картки, коди доступу/паролі, отримання грошей, дестабілізації у суспільстві, дискредитація органів влади, тощо). Протидія дезінформації залежить від багатьох чинників, у тому числі від: нормативно-правових, інституційних, організаційних, освітніх, принципової позиції населення України щодо бажання оволодіти навичками її розпізнання та недопущення впливу, психологічної стійкості, інформаційної гігієни тощо [3, с.474]. К.С. Кузьменкова слушно зазначає, що у сучасних умовах військових конфліктів і геополітичних змін дослідження феномену дезінформації набуває ключового значення, оскільки становить серйозну загрозу національним інтересам держави. Під час збройної агресії проти України дезінформація виступає основним інструментом реалізації стратегій інформаційної війни, що актуалізує питання розробки ефективних методів

протидії проникненню фейків та їх негативному впливу на суспільну свідомість. Завдання боротьби з поширенням дезінформації вимагає вдосконалення існуючих механізмів формування державної політики та пошуку нових підходів до організації публічного управління у цій сфері [4]. Фейкові новини, зазвичай, стосуються новин або заголовків, навмисно сфабрикованих для введення в оману або маніпулювання читачами. Ці історії часто виглядають як справжні новини, але є повністю вигаданими або перекрученими версіями реальних подій, створених з метою обману. Фейкові новини – це вид дезінформації: неправдива інформація, створена з метою введення в оману. Дезінформація включає не лише фейкові новини, а й інші типи тверджень, такі як ті, що поширюються як урядова пропаганда, або ж обліковими записами чи брендами соціальних мереж з метою продажу продукту чи послуги. З іншого боку, дезінформація — це будь-який вид неправдивої або неточної інформації, незалежно від того, чи поширюється вона навмисно, чи ні. Люди часто поширюють дезінформацію, бо щиро вірять у її правдивість і не усвідомлюють, що поширюють щось неправдиве [5]. З огляду на зазначене вище, цілком справедливим буде говорити про те, що дезінформація в медіа являє собою навмисне створення, спотворення або поширення неправдивої інформації з метою введення аудиторії в оману, формування викривленого уявлення про події, явища або осіб, а також впливу на суспільні настрої, політичні процеси чи поведінку людей. На відміну від помилкової інформації, яка може виникати ненавмисно, дезінформація має цілеспрямований характер і зазвичай використовується як інструмент маніпуляції у політичній, інформаційній, економічній або безпековій сферах. Її шкідливість полягає в тому, що вона підриває довіру до медіа та суспільних інститутів, ускладнює формування об'єктивної громадської думки, провокує соціальну напруженість і поляризацію, а також може створювати загрози для національної безпеки, зокрема, шляхом дестабілізації суспільства, дискредитації органів влади чи деморалізації населення.

У Стратегії інформаційної безпеки в якості окремої цілі визнається протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини [6]. У вказаному стратегічному документі вказується, що досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань: створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; ужиття заходів щодо запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України; розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі; підготовка та проведення складовими сил оборони інформаційно-психологічних операцій та інших заходів, спрямованих на запобігання, стримування та відсіч збройної агресії Російської Федерації проти України; посилення відповідальності за поширення недостовірної інформації (дезінформації); запровадження дієвих механізмів виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом; ефективна взаємодія державних органів, органів місцевого самоврядування та інститутів громадянського суспільства при формуванні та реалізації державної політики в інформаційній сфері; тощо [6].

Дезінформація відрізняється від шкідливого контенту, насамперед, за своєю природою та функціональним призначенням, оскільки перша полягає у цілеспрямованому поширенні неправдивої або спотвореної інформації з метою введення аудиторії в оману, тоді як шкідливий контент може містити як правдиві, так і неправдиві відомості, але завдає шкоди через свій зміст, форму або контекст поширення, наприклад, шляхом пропаганди насильства, мови ворожнечі, маніпуляції емоціями чи підриву моральних і правових засад суспільства. Шкідливий контент – це такий контент в інтернеті, що приносить людині страждання чи шкоду або може спонукати до небезпечних дій. До розповсюдженого шкідливого контенту в онлайн відносяться матеріали, що зображують: удушення – ігри з задухою, утопленням або підвішуванням, поїдання неїстівних предметів; використання зброї; вживання небезпечних предметів і речовин, які не є харчовими продуктами та можуть викликати отруєння або іншим способом завдати шкоди здоров'ю; дії, які в результаті можуть призвести до обморожень, опіків чи ударів струмом; нанесення собі травм або каліцтв; нанесення травм або каліцтв іншим, наприклад, раптовий удар; небезпеку без

заподіяння фактичної фізичної шкоди – погрози зброєю або вибухівкою, інсценування дзвінка в поліцію або пограбування, інсценування викрадення; розіграші, що викликають серйозні емоційні потрясіння, – інсценування смерті або самогубства, насильства, наміри батьків (опікуна) кинути дитину, психологічне насильство (образи, приниження) стосовно дитини; інструкцію, як створити вибуховий пристрій; насильство – зображення справжніх бійок або інших епізодів насильства; рекламу, вживання, виготовлення наркотичних речовин; позитивне ставлення до харчових розладів; порнографічні матеріали [7]. Отже, шкідливий контент, зокрема маніпулятивні наративи, мова ворожнечі та пропаганда, використовується для нав'язування викривленої картини реальності, легітимації агресивних дій проти держави та деморалізації населення, що безпосередньо впливає на обороноздатність і стратегічну стійкість країни. В умовах гібридних загроз, обумовлених сучасним веденням війни, інформаційні атаки можуть бути скоординовані з політичним, економічним і воєнним тиском, посилюючи їхній ефект та ускладнюючи ухвалення зважених управлінських рішень. Саме тому системна протидія дезінформації, розвиток медіа грамотності, забезпечення відповідальності суб'єктів медіа сфери і захист інформаційного суверенітету є необхідними складовими комплексного підходу до національної безпеки, спрямованого на збереження конституційного ладу, демократичних цінностей і довгострокової стійкості держави.

У 2023 році найпопулярнішим джерелом інформації в Україні є Інтернет. Згідно з опитуванням, 62% учасників отримують інформацію з соціальних мереж і 48% з новинних сайтів. Дезінформація може легко поширюватися в соціальних мережах через відсутність редакційного контролю, свободу публікацій для будь-якого користувача та можливість швидко створювати та поширювати інформацію безкоштовно. Користувачі Інтернету можуть легко поширювати вірусний вміст, що призводить до широкого поширення на багатьох сайтах. Отже, сьогодні соціальні мережі набрали величезної популярності, адже там кожен може створювати контент. В інтернеті, переповненому інформацією, стає вкрай важливо розрізняти джерела, що заслуговують на довіру, і ті, що вводять в оману [8]. Повномасштабне вторгнення російських військових в Україну у лютому 2022 року продовжує підривати свободу інтернету в країні. Атаки російських військових завдали серйозної шкоди інтернет-інфраструктурі, що призвело до перебоїв у роботі мережі. Український уряд блокує широкий спектр російських та підтримуваних Кремлем веб-сайтів, включаючи блоги та новинні видання, сайти соціальних мереж та сайти, що надають інші послуги. Крім того, суди винесли вироки особам, звинуваченим у створенні прокремлівської пропаганди, співпраці з російським урядом у створенні онлайн-контенту або розміщенні в Інтернеті інформації про ухилення від призову. Кібератаки російських суб'єктів на державні установи, критичну інфраструктуру та ЗМІ є звичним явищем [9].

Український уряд блокує численні російські та проросійські вебсайти. Вебплатформи, що належать Росії, зокрема «Вконтакте», «Одноклассники» та Mail.ru; широкий спектр вебсайтів, які вважаються такими, що містять російську пропаганду; а також пов'язані з Росією компанії, такі як Dr. Web, Kaspersky та Yandex, були заблоковані за допомогою «санкцій», які неодноразово поновлювалися з 2017 року. У травні 2021 року санкції були запроваджені проти російських та проросійських кримських ЗМІ, платіжних систем та компаній інформаційних технологій. У різні періоди накази про блокування також стосувалися онлайн-ресурсів самопроголошених органів влади підконтрольної Кремлю Луганської Народної Республіки, а також «Ростелекому», RT, «Національної медіагрупи», Всеросійської державної телерадіокомпанії, «Первого каналу», інформаційного агентства ITAP-TACC та інших. Фактичне впровадження блокування вебсайтів було непослідовним, оскаржено в суді та ніколи належним чином не контролювалися. Після запровадження воєнного стану у відповідь на вторгнення у лютому 2022 року, NCEC попросила інтернет-провайдерів заблокувати величезну кількість російських вебсайтів, які нібито поширювали дезінформацію, або сприяли кібератакам. До березня 2022 року NCEC наказала заблокувати понад 48 мільйонів російських IP-адрес. Покаранням за невиконання вимог є виключення з реєстру операторів та провайдерів зв'язку, а регулятор має право застосовувати більш суворі заходи. Наразі зареєстровано щонайменше один такий випадок [9].

Віталій Дячук, аналітик Інституту Центральноєвропейської стратегії переконаний: навіть там, де журналістські стандарти формально дотримуються, політики все одно обходять традиційні ЗМІ. Про це свідчать і останні вибори в Україні та інших країнах світу, де політичні кампанії свідомо ігнорували професійні медіа. «Традиційні ЗМІ, які працюють за стандартами, просто залишилися поза інформаційною грою. Політики масово перейшли у Telegram-канали, до альтернативних ЗМІ та блогерів, тобто в нові медіа, які не регулюються законами чи журналістськими

нормами, а часто навіть елементарними етичними принципами, – каже Віталій Дячук. – Схожа ситуація спостерігається у Словаччині. Після зміни влади комунікація з незалежними медіа практично припинилася: журналістів не допускають на пресконференції, а інформаційний простір заповнили маніпулятивні та дезінформаційні ресурси. Ті самі медіа, з якими колишня влада боролася, тепер стали офіційними рупорами уряду. В Угорщині інформаційне поле фактично монополізоване. Провідні незалежні видання втратили доступ до джерел інформації та ігноруються» [10].

Висновки. Таким чином, запобігання та протидія дезінформації та шкідливому контенту в медіа представляє собою врегульовану нормами чинного законодавства цілеспрямовану, системну діяльність держави, медіасередовища й суспільства, яка спрямована на своєчасне виявлення, обмеження поширення та нейтралізацію навмисно або структурно викривленої, маніпулятивної чи деструктивної інформації, що здатна завдати шкоди суспільним інтересам, демократичним процесам, правам і свободам людини, інформаційному суверенітету та національній безпеці Україна, а також на створення умов для формування стійкого, відповідального й достовірного медіапростору через правові, інституційні, технологічні та освітні механізми.

Список використаних джерел:

1. Глазов О. В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Наукові праці Чорноморського державного університету імені Петра Могили.* Сер. : Політологія. 2011. Т. 155, Вип. 143.С. 42-46. URL: http://nbuv.gov.ua/UJRN/Npchdupol_2011_155_143_10

2. Павленко Д.Г., Семенюк Ю.В., Лисецький Ю.М. Національна безпека: поняття, складники, чинники впливу. *Вчені записки ТНУ імені В.І. Вернадського.* Серія : Державне управління. 2021. Том. 32(71). № 3. С. 102-107

3. 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.

4. Кузьменкова К.С. Феномен «дезінформація» як об'єкт наукових досліджень вітчизняних та зарубіжних вчених. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: Публічне управління та адміністрування. 2025. Том 36 (75) № 1. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2025/1_2025/18.pdf

5. A quick guide to spotting misinformation. Tips for fact-checking, staying informed and talking it out. URL: https://www.unicef.org/eca/stories/quick-guide-spotting-misinformation

6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України; Стратегія від 28.12.2021 № 685/2021 URL: https://zakon.rada.gov.ua/laws/show/685/2021/conv#Text

7. Шкідливий контент - поліція нагадує що варто знати батькам для захисту дітей під час користування інтернет-мережі. URL: https://mk.npu.gov.ua/news/shkidlyvyi-kontent-politsiia-nahaduie-shcho-varto-znaty-batkam-dlia-zakhystu-ditei-pid-chas-korystuvannia-internet-merezhi

8. Дезінформація: як розпізнати та боротися. URL: https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/

9. Freedom House. Key Developments, June 1, 2023 – May 31, 2024 URL: https://freedomhouse.org/country/ukraine/freedom-net/2024

10. Інформаційна безпека Закарпаття: хто повинен боротися з дезінформацією. URL: https://zaholovok.com.ua/informatsiyna-bezpeka-zakarpattya-khto-povynen-borotysya-z-dezinformatsiyeyu

Дата першого надходження статті до видання: 09.10.2025
Дата прийняття статті до друку після рецензування: 10.11.2025
Дата публікації (оприлюднення) статті: 24.11.2025