

*Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019).
Спеціальність – 281.
Державне управління: удосконалення та розвиток. 2023. № 8.*

DOI: <http://doi.org/10.32702/2307-2156.2023.8.5>

УДК 351/354.1 (477)

*Л. А. Гаєвська,
д. держ. упр., професор, професор кафедри національної економіки та
публічного управління, Київський національний економічний університет
імені Вадима Гетьмана
ORCID ID: <https://orcid.org/0000-0003-1463-9481>*

*Н. О. Васюк,
к. держ. упр., доцент, докторант кафедри національної економіки та
публічного управління, Київський національний економічний університет
імені Вадима Гетьмана
ORCID ID: <https://orcid.org/0000-0002-8493-6644>*

МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ОРГАНАМИ ДЕРЖАВНОЇ ВЛАДИ ЗАСОБАМИ МЕРЕЖЕВОГО УПРАВЛІННЯ

*L. Gaievska,
Doctor of Sciences in Public Administration, Professor, Professor of the
Department of National Economy and Public Administration, Kyiv National
Economic University named after Vadym Hetman
N. Vasiuk,
PhD in Public Administration, Associate Professor, Doctoral student of the
Department of National Economy and Public Administration, Kyiv National
Economic University named after Vadym Hetman*

MECHANISMS OF COUNTERING DISINFORMATION BY STATE AUTHORITIES BY MEANS OF NETWORK MANAGEMENT

У статті досліджено проблеми поширення дезінформації та визначено шляхи вдосконалення механізмів протидії дезінформації органами державної влади засобами мережевого управління в Україні, використавши зарубіжний досвід.

Встановлено, що за допомогою сучасних засобів мережевого управління можна здійснювати вплив на боротьбу з дезінформацією (мережевою інформаційною війною), зокрема забезпечити участь громадянського суспільства шляхом забезпечення обміном достовірної інформації (користуватись перевіреними фактами, джерелами, сайтами та ін.); забезпечення вільного доступу до інформації (не здійснювати обмеження щодо поширення інформації незалежними ЗМІ при встановленні відповідальності за поширення дезінформації); забезпечення нагляду і громадського контролю за діяльністю в он-лайн просторі; забезпечення участі у формуванні мережевої інформаційної інфраструктури.

Доведено, що на сьогодні в більшій мірі, ніж в «епоху доцифровізації», виникає необхідність у такому методі протидії дезінформації як перевірка фактів. В зв'язку з цим, необхідно розробити механізми мережевого управління інформаційними потоками в соціальних мережах та інтернет-ЗМІ таким чином, щоб сформувати в аудиторії можливість вироблення критичного мислення при отриманні будь-якої інформації.

Визначено, що на сьогодні більшість інформації швидко поширюється в онлайн просторі, окрім традиційних ЗМІ, існує ризик отримання недостовірної інформації, дезінформації та інших «шкідливих» повідомлень, тому необхідно встановити відповідальність за поширення неправдивого контенту, особливо користувачів соціальних мереж, які це публікують.

Запропоновано розробити Доктрину протидії дезінформації саме в мережевому просторі, яка б враховувала механізми мережевого управління в інформаційному протиборстві з поширенням дезінформації.

Встановлено, що у боротьбі з дезінформацією одного лише

законодавчого регулювання, зокрема встановлення відповідальності за її поширення, недостатньо. І в цьому контексті ефективним засобом протидії дезінформації є мережеве управління, зокрема залучення в цей процес громадянського суспільства та вироблення конкретних пропозицій щодо його участі.

The article research the problems of spreading disinformation and identifies ways to improve the mechanisms of counteracting disinformation by state authorities by means of network management in Ukraine, using foreign experience.

It has been established that with the help of modern means network management tools it is possible to influence the fight against disinformation (network information war), in particular, to ensure the participation of civil society by ensuring the exchange of reliable information (use verified facts, sources, sites, etc.); ensuring free access to information (not to impose restrictions on the dissemination of information by independent media when establishing liability for the dissemination of disinformation); ensuring supervision and civil control over activities in the online space; ensuring participation in the formation of a network information infrastructure.

It has been proven that today, to a greater extent than in the “era of pre-digitalization”, there is a need for such a method of counteracting disinformation as fact checking. In this regard, it is necessary to develop mechanisms for network management of information flows in social networks and online media in such a way as to form in the audience the possibility of developing critical thinking when receiving any information.

It has been determined that today most information is rapidly spreading in the online space, in addition to traditional media, there is a hazard of receiving false information, disinformation and other "harmful" messages, therefore it is necessary to establish responsibility for the dissemination of false content, especially users of social networks publishing this.

It is proposed to develop the Doctrine of counteracting disinformation in the

network space, which would take into account the mechanisms of network management in the information confrontation with the spread of disinformation.

It has been established that in the fight against disinformation, legislative regulation alone, in particular, establishing responsibility for its dissemination, is not enough. And in this context, network management is an effective means of counteracting disinformation, in particular, involving civil society in this process and developing specific proposals for its participation.

Ключові слова: *дезінформація, фейкова інформація, інформаційна безпека, кібербезпека, поширення надійної та достовірної інформації, протидія дезінформації, протидія дезінформації в мережевому просторі, мережеве управління, засоби мережевого управління, участь громадянського суспільства в протидії дезінформації.*

Keywords: *disinformation, fake information, information security, cyber security, dissemination of reliable and authentic information, countering disinformation, countering disinformation in the network space, network management, means of network management, participation of civil society in countering disinformation.*

Постановка проблеми. На сьогодні Україна перебуває під впливом значних викликів та випробувань, в першу чергу – це російська військова агресія, що спричинила збільшення значної кількості поширеної дезінформації в суспільстві.

Проблеми, пов'язанні з заподіянням шкоди від поширення дезінформації, актуалізуються в сучасному цифровому світі та призвели до різкого збільшення активності держав та міжнародних організацій щодо протидії дезінформації [1].

Викликати сумніви й переконати користувачів у достовірності розповсюдженої інформації – це і є мета фейкових новин (повідомлень), які розглядаються як інструментарій інформаційної війни та загрози

інформаційній безпеці. Дослідження довели, що навіть поширена позитивна фейкова інформація в результаті дає негативний вплив та наносить шкоду і є загрозливим явищем [2].

Стратегія зовнішньополітичної діяльності України визначає, що поширення дезінформації та ворожої пропаганди становлять інформаційну загрозу для України [3].

Важливу роль у суспільстві відіграють мережеві та інформаційні системи і послуги, надійність та безпека яких є суттєвою для економічної та соціальної діяльності [4].

Аналіз останніх досліджень і публікацій. Актуальним питанням нормативно-правового регулювання інформаційної безпеки та протидії дезінформації, розповсюдженням фейковим новин присвячено праці Р. Басенко, М. Гребенюк, Ю. Довгаль, О. Звоздецька, А. Кравченко, Б. Леонов, А. Марущак, О. Тронько, Р. Шаравара Р. Черниш, Д. Чумаш, та ін.

Заслуговує на увагу Посібник із «фейкових новин» та інших інформаційних розладів (автори L. Bounegru, J. Gray, T. Venturini, M. Mauri), в якому досліджено використання цифрових методів для вивчення неправдивих вірусних новин, політичних мемів, практики тролінгу та їхнього соціального життя в Інтернеті. Посібник дає відповідь на сучасні виклики та зростаючий попит на розуміння взаємодії між цифровими платформами, оманливою інформацією, пропагандою та практиками вірусного контенту, а також їхнього впливу на політику та суспільне життя в демократичних суспільствах [5].

У статті J. Gray, L. Bounegru, T. Venturini досліджено як «фейкові новини» впливають на соціальні хвилювання. Автори припускають, що загроза проблемних і «вірусних сміттєвих новин» може викликати екзистенційні питання щодо поширення, залучення та монетизації контенту через Інтернет і соціальні медіа. Також авторами запропоновано методологічні підходи до подолання цих наслідків [6].

Разом з тим, питання протидії дезінформації засобами мережевого

управління залишаються недостатньо дослідженими.

Мета статті. Дослідити проблеми поширення дезінформації та визначити шляхи вдосконалення механізмів протидії дезінформації органами державної влади засобами мережевого управління в Україні, використавши зарубіжний досвід.

Виклад основного матеріалу дослідження. Окремі автори дезінформацію розглядають за такими характеристиками (ознаками): усвідомлена інформація; інформація, що може бути підтверджена; недостовірність інформації, що поширюється; поширення інформації з метою економічної вигоди або навмисного обману аудиторії; умисел та заподіяння шкоди публічному інтересу при її поширенні [1].

Протидія дезінформаційним атакам із зовнішніх джерел, що здійснюються на шкоду національним інтересам та іміджу України за кордоном є однією із цілей зовнішньополітичної діяльності України [3].

Стійкість та взаємодія є основними напрямками забезпечення інформаційної безпеки України. З метою їх досягнення необхідно виконати стратегічні цілі та завдання, зокрема стратегічної цілі «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» шляхом виконання таких основних завдань [7]:

- 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;

– посилення відповідальності за поширення недостовірної інформації (дезінформації).

Сучасні Інтернет-технології надають можливості для неправдивого інформування населення та поширення дезінформації [8].

Соціальні мережі та інтернет-платформи, сприяючи поширенню негативної інформації, стали чи не найнебезпечнішим середовищем для поширення дезінформації. Через такі механізми поширення дезінформації як публікація дописів, пересилання гіперпосилань та повідомлень у великих групах та ін. розповсюдження недостовірної інформації збільшується та розширюється [1; 2].

Протидія дезінформації та її контролю, охорона інформаційного суверенітету, протидія негативним інформаційним впливам, а також захист державного інформаційного простору від маніпулятивних дій та інформаційних війн – це і є основними функціями забезпечення інформаційної безпеки держави [9].

В Україні Кодексом про адміністративні правопорушення встановлено адміністративну відповідальність за поширення неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку [10].

У Європі у процес протидії дезінформації втрутилися уряди, а у 2018 році Німеччина та Франція прийняли законодавство, яке забороняє фейкові новини та встановлює механізми видалення незаконних (недостовірних) публікацій і розпалювання ненависті (ворожнечі) в соціальних мережах Facebook і Twitter [11].

На сьогодні в Україні немає спеціального нормативно-правового регулювання протидії дезінформації. Тому для протидії дезінформації органам державної влади необхідно використовувати інші засоби, зокрема можливості мережевого управління.

Поняття «мережеве управління» С. Ситник визначає як «сучасний підхід до розуміння публічного управління як системи, побудованої на переході від ієрархічного управління до управління за допомогою переговорів, узгодженні інтересів, кооперації державних, суспільних, приватних, змішаних структур, покликаних задовольняти суспільні інтереси та вирішувати суспільні завдання» [12]. Особливо важливою у цьому контексті є, на наш погляд, роль (участь) громадянського суспільства у боротьбі з дезінформацією.

На думку авторів, існує активна взаємодія між державними інституціями та приватними партнерами, а також громадянським суспільством, і в той же час відчувається недостатність спільного прийняття управлінських (політичних) рішень. В зв'язку з цим, виокремлюють структуру мережі (network structure) та мережеву взаємодію (networking) [13].

У протидії з поширенням дезінформації необхідно чітко виокремити саме поняття та типи «феномену фейкових новин», зокрема журналістські помилки, політичну пропаганду, вигадані (неправдиві) новини, сатиру [2].

Погоджуємося, що універсальних механізмів протидії дезінформації ще не створено. У зв'язку з тим, що дезінформація поширюється в соціальних мережах, то і протидія дезінформації має концентруватися в мережевому просторі [1], що можна досягти засобами мережевого управління.

Країни-члени ЄС інтегрують захист основних принципів (права людини, прозорість та довіра громадськості) до своїх національних стратегій кібербезпеки. Це дуже важливо, особливо якщо йдеться про дезінформацію, яка поширюється за допомогою традиційних засобів масової інформації або платформ соціальних мереж. На європейському рівні Європейська Комісія окреслила План дій проти дезінформації [14] для активізації зусиль з протидії дезінформації в Європі, який спрямований на 4 основні сфери (виявлення, співпраця, взаємодія з онлайнплатформами та обізнаність) і слугує для розбудови спроможностей ЄС та зміцнення співпраці між країнами-членами [15].

Стратегія інформаційної безпеки визначає, що суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації шляхом підвищення рівня медіакультури та медіаграмотності суспільства (Стратегічна ціль 3) [7].

Перебування України в епіцентрі дезінформаційних новин та кібератак робить партнерство з ЄС у цій сфері взаємовигідним. В зв'язку з цим, необхідним є удосконалення взаємодії України з ЄС у сфері стратегічних комунікацій (на основі міжнародного законодавства), в тому числі з протидії дезінформації та розвитку співробітництва у сфері кібербезпеки [3].

Планом дій з реалізації Стратегії зовнішньополітичної діяльності України передбачено здійснення моніторингу українського і міжнародного медіапростору для виявлення антиукраїнських дезінформаційних кампаній, спеціальних інформаційних операцій та інших потенційно небезпечних наративів. При цьому засобами мережевого управління можуть бути спростування та запобігання поширенню дезінформації, зокрема у тісній співпраці з громадянським суспільством (громадські центри з протидії гібридним загрозам та ін. організаціями) [16].

На основі дослідження «Базовий документ з питань національної та кібербезпеки, інтернет-свободи та міжнародного права», виданого в червні 2020 року Американською асоціацією юристів – Ініціатива з верховенства права (ABA ROLI) в Україні, надано рекомендації органам державної влади України, зокрема [17]:

- здійснення постійного моніторингу виконання Стратегій у сфері національної безпеки та її інформаційних та кібер складових, а також забезпечення їх ефективної реалізації;

- здійснення регулярного аналізу та оцінки виконання (дотримання) законодавства у цій сфері, а також вільного вираження поглядів і поширення достовірної інформації;

- прискорення гармонізації українського законодавства із законодавством Європейського Союзу, стандартами Ради Європи у сфері

інформаційної та кібербезпеки, вільного вираження думок та поглядів;

- внесення змін до чинного законодавства, які мають бути спрямовані на встановлення порядку обмеження доступу до розповсюдження інформації в мережевому просторі, яка є або може бути шкідливою;

- проведення ефективних консультацій з громадянським суспільством та з заінтересованими особами;

- посилення контролю за обробкою, зберіганням персональних даних та доступом до іншої інформації з обмеженим доступом під час надання адміністративних послуг, запобігаючи незаконному витоку персональних даних (при цьому особлива увага має бути приділена такій інформації як відомості про стан здоров'я).

Для вдосконалення механізмів протидії дезінформації може бути ефективним використання засобів мережевого управління, зокрема забезпечення участі громадськості в цьому процесі шляхом висловлення відповідної критики, втручання та відповідальності за поширення недостовірної інформації (здійснення громадського контролю), а також вибір альтернатив щодо дослідження фактів.

Висновки. Встановлено, що за допомогою сучасних засобів мережевого управління можна здійснювати вплив на боротьбу з дезінформацією (мережевою інформаційною війною), зокрема забезпечити участь громадянського суспільства шляхом забезпечення обміном достовірної інформації (користуватись перевіреними фактами, джерелами, сайтами та ін.); забезпечення вільного доступу до інформації (не здійснювати обмеження щодо поширення інформації незалежними ЗМІ при встановленні відповідальності за поширення дезінформації); забезпечення нагляду і громадського контролю за діяльністю в он-лайн просторі; забезпечення участі у формуванні мережевої інформаційної інфраструктури.

На сьогодні в більшій мірі, ніж в «епоху доцифровізації», виникає необхідність у такому методі протидії дезінформації як перевірка фактів. В зв'язку з цим, необхідно розробити механізми мережевого управління

інформаційними потоками в соціальних мережах та інтернет-ЗМІ таким чином, щоб сформувати в аудиторії можливість вироблення критичного мислення при отриманні будь-якої інформації.

У зв'язку з тим, що на сьогодні більшість інформації швидко поширюється в онлайн просторі, окрім традиційних ЗМІ, та існує ризик отримання недостовірної інформації, дезінформації та інших «шкідливих» повідомлень, необхідно встановити відповідальність за поширення неправдивого контенту, особливо користувачів соціальних мереж, які це публікують.

Необхідно розробити Доктрину протидії дезінформації саме в мережевому просторі, яка б враховувала механізми мережевого управління в інформаційному протиборстві з поширенням дезінформації.

Вважаємо, що у боротьбі з дезінформацією одного лише законодавчого регулювання, зокрема встановлення відповідальності за її поширення, є недостатньо. І в цьому контексті ефективним засобом протидії дезінформації є мережеве управління, зокрема залучення в цей процес громадянського суспільства та вироблення конкретних пропозицій щодо його участі.

Література

1. Дворовий М., Людвиг А. Протидія дезінформації в інтернеті: куди рухатися Україні? Аналітичний звіт. 2021. URL: https://dslua.org/wp-content/uploads/2022/01/DSLUA_Disinformation_Ukraine_Report.pdf (Дата звернення: 26.07.2023).
2. Маляренко В. І. Кращі практики зарубіжного досвіду боротьби з фейками та дезінформацією. *Інформація і право*. 2021. № 3(38). С. 21-27.
3. Про рішення Ради національної безпеки і оборони України від 30 липня 2021 року "Про Стратегію зовнішньополітичної діяльності України". Указ Президента України від 26 серпня 2021 року № 448/2021. URL: <https://zakon.rada.gov.ua/laws/show/448/2021#n11> (Дата звернення: 26.07.2023).
4. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6

липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. Офіційний вісник Європейського Союзу від 19.07.2016. L 194/1. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (Дата звернення: 26.07.2023).

5. Bounegru, L., Gray, J., Venturini, T., & Mauri, M. (Eds.). A Field Guide to “Fake News” and Other Information Disorders. Amsterdam: Public Data Lab. 2018. URL: <https://zenodo.org/record/1136272> (Accessed: 26.07.2023).

6. Gray, J., Bounegru, L., & Venturini, T. (2020). ‘Fake news’ as infrastructural uncanny. *New Media & Society*, 22(2), 317–341.

7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069> (Дата звернення: 26.07.2023).

8. Чукут С. А., Клименко І. В., Линьов К. О. Електронний Уряд. Науково-практичний довідник. 2016. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Elektronnij-uryad_nauk_prak-dovidnik_CNukut_Linov_Klimenko.pdf (Дата звернення: 26.07.2023).

9. Черниш Р. Ф., Ігнатюк М. В., Заріцький О. Ю. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал*. 2022. № 1. С. 213-216.

10. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (Дата звернення: 28.07.2023).

11. Jan Melissen. Part II: fake news, and what (not) to do about it. *USC Center on Public Diplomacy*. 2018. URL: <https://uscpublicdiplomacy.org/blog/part-ii-fake-news-and-what-not-do-about-it> (Дата звернення: 28.07.2023).

12. Куйбіда В. С., Білинська М. М., Петроє О. М. Публічне управління:

термінологічний словник. Навчальний посібник. Київ: НАДУ, 2018. 224 с.

13. Делія О. В. Governance як концептуальний підхід до розуміння публічного управління. *Державне управління: удосконалення та розвиток*. 2015. № 7. URL: <http://www.dy.nayka.com.ua/?op=1&z=869> (Дата звернення: 28.07.2023).

14. Керівництво з оцінки національних спроможностей. Європейське агентство з питань мережевої та інформаційної безпеки (ENISA). 2020. URL: <https://www.cip.gov.ua/services/cm/api/attachment/download?id=40770> (Дата звернення: 28.07.2023).

15. Action Plan against Disinformation. European Commission. 2018. JOIN(2018) 36 final. URL: <https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation> (Дата звернення: 28.07.2023).

16. Про затвердження плану дій з реалізації Стратегії зовнішньополітичної діяльності України: Розпорядження Кабінету Міністрів України від 18 квітня 2023 р. № 327-р. URL: <https://zakon.rada.gov.ua/laws/show/327-2023-%D1%80#Text> (Дата звернення: 28.07.2023).

17. Рекомендації щодо покращення ситуації зі свободою вираження поглядів онлайн в контексті інтересів національної безпеки. 2021. URL: <https://www.pppl.org.ua/bibliotech-2> (Дата звернення: 28.07.2023).

References

1. Dvorovyj, M. and Liudva, A. (2021), "Combating disinformation on the Internet: where should Ukraine go?", available at: https://dslua.org/wp-content/uploads/2022/01/DSLU_Disinformation_Ukraine_Report.pdf (Accessed 26.07.2023).

2. Maliarenko, V.I. (2021), "Best practices of foreign experience in combating fakes and disinformation", *Informatsiia i pravo*, vol. 3 (38), pp. 21-27.

3. President of Ukraine (2021), Decree "On the decision of the National Security and Defense Council of Ukraine dated July 30, 2021 "On the Strategy of

Foreign Policy of Ukraine””, available at: <https://zakon.rada.gov.ua/laws/show/448/2021#n11> (Accessed 26.07.2023).

4. EU (2016), “Directive of the European Parliament and of the Council (EU) 2016/1148 of July 6, 2016 on measures for a high common level of security of network and information systems in the territory of the Union”, available at: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (Accessed 26.07.2023).

5. Bounegru, L. Gray, J. Venturini, T. and Mauri, M.A. (2018), “Field Guide to “Fake News” and Other Information Disorders”, Public Data Lab, available at: <https://zenodo.org/record/1136272> (Accessed: 26.07.2023).

6. Gray, J. Bounegru, L. and Venturini, T. (2020). ‘Fake news’ as infrastructural uncanny. *New Media & Society*, vol. 22 (2), pp. 317-341.

7. President of Ukraine (2021), Decree “On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy””, available at: <https://zakon.rada.gov.ua/laws/show/685/2021#n5> (Accessed 26.07.2023).

8. Chukut, S.A. Klymenko, I.V. and Lyn'ov, K.O. (2016), “Electronic Government”, available at: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Elektronnij-uryad_nauk_prak-dovidnik_CHukut_Linov_Klimenko.pdf (Accessed 26.07.2023).

9. Chernysh, R.F. Ihnatiuk, M.V. and Zarits'kyj, O.Yu. (2022), “Counteracting destructive information influence in Ukraine: legal and organizational aspects”, *Yurydychnyj naukovyj elektronnyj zhurnal*, vol. 1, pp. 213-216.

10. Verkhovna Rada of Ukraine (1984), “Code of Ukraine on administrative offenses”, available at: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (Accessed 28.07.2023).

11. Melissen, J. (2018), “Part II: fake news, and what (not) to do about it”, USC Center on Public Diplomacy, available at: <https://uscpublicdiplomacy.org/blog/part-ii-fake-news-and-what-not-do-about-it> (Accessed 28.07.2023).

12. Kujbida, V.S. Bilyns'ka, M.M. and Petroie, O.M. (2018), Publichne upravlinnia: terminolohichnyj slovnyk [Public administration: terminological dictionary], NADU, Kyiv, Ukraine.

13. Delia, O.V. (2015), "Governance as a concept approach to understanding public administration", Derzhavne upravlinnia: udoskonalennia ta rozvytok, vol. 7, available at: <http://www.dy.nayka.com.ua/?op=1&z=869> (Accessed 28.07.2023).

14. ENISA (2020), "Guidelines for assessing national capabilities", available at: <https://www.cip.gov.ua/services/cm/api/attachment/download?id=40770> (Accessed 28.07.2023).

15. European Commission (2018), "Action Plan against Disinformation", available at: <https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation> (Accessed 28.07.2023).

16. Cabinet of Ministers of Ukraine (2023), Resolution "On the approval of the action plan for the implementation of the Strategy of Foreign Policy of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/327-2023-%D1%80#Text> (Accessed 28.07.2023).

17. Human Rights Platform (2021), "Recommendations for improving the situation with freedom of expression online in the context of national security interests", available at: <https://www.ppl.org.ua/bibliotech-2> (Accessed 28.07.2023).

Стаття надійшла до редакції 03.08.2023 р.