Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”

№ 3 (39), 2023

УДК 34.096

Ірина Крикавська
Національний університет “Львівська політехніка”,
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права,
психології та інноваційної освіти,
кандидат юридичних наук, доцент
iryna.v.krykavska@lpnu.ua
ORCID iD: https://orcid.org/0000-0002-6108-2447

Мар’яна Повалена
Національний університет “Львівська політехніка”,
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права,
психології та інноваційної освіти,
кандидат юридичних наук, доцент
mariana.v.povalena@lpnu.ua
ORCID iD: https://orcid.org/0000-0001-5638-200X

Остап-Зеновій Музика
Національний університет “Львівська політехніка”,
студент другого курсу магістратури
Навчально-наукового інституту права,
психології та інноваційної освіти
ostap-zenovii.muzyka.mpvpr.2022@lpnu.ua

ІНФОРМАЦІЙНІ ЗАГРОЗИ В МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ВІЙНИ В УКРАЇНІ: ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ

http://doi.org/10.23939/law2023.39.082

У статті досліджуються питання інформаційної безпеки як стану захищеності життєво важливих інтересів людини, суспільства і держави, за якого слід запобігати заподіянню шкоди через: неповноту, невчасність та невірогідність інформації, що використовується.

Мережа Інтернет впливає на інформаційну безпеку як позитивно, так і негативно, з одного боку, повний доступ до всієї інформації з можливістю подальшої фільтрації, перевірки і визначення для себе, яким джерелам можна довіряти, а яким не варто, з другого боку, легкість просування ворожих наративів через недостатність контролю, а також легкість через незнання потрапити не на ті посилання, наприклад, у тих людей, які користуються Інтернетом російською мовою, будуть в стрічці переважно промосковські новини і без знання обох мов дуже легко потрапити під вплив пропаганди.

Досліджуються шляхи негативного впливу, що застосовуються ворогом в інформаційному середовищі Інтернет.

На сучасному етапі розвитку законодавчого регулювання боротьби з дезінформацією в мережі Інтернет немає чітких механізмів притягнення до відповідальності осіб, що створюють пабліки чи так звані канали з поширення дезінформації, а тим паче, за коментарі в таких пабліках.

Враховуючи сутність і складність цифрового середовища та основ його функціонування, притягнення до відповідальності за поширення інформації, що не є обмеженою законами України, зокрема законом "Про інформацію", потребує додаткового вивчення та вирішення шляхів врегулювання.

Окреслено необхідні пріоритетні напрями для протидії масштабним інформаційним загрозам в мережі Інтернет, операціям інформаційної війни ворога.

Важливим є висновок щодо необхідності підвищення рівня інформаційної грамотності населення України для подолання інформаційних загроз в мережі Інтернет, прийняття на законодавчому рівні урядових програм та освітніх заходів органів місцевого самоврядування для підвищення цифрової грамотності населення, особливо з тих питань, що стосуються інформаційної безпеки в мережі Інтернет.

Ключові слова: інформаційна безпека; інформаційні загрози; Інтернет.

Постановка проблеми. Сучасна ситуація в Україні, зокрема війна з Росією, поглиблює розуміння надважливості необхідності розбудови ефективної системи забезпечення захисту українського інформаційного простору, зокрема в мережі Інтернет. Для забезпечення інформаційної безпеки було прийнято нормативні акти, що врегульовують основні питання, зокрема рішення Ради національної безпеки й оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", а також Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану".

Однак інформаційні загрози в мережі Інтернет є дуже динамічним явищем, що потребує постійного реагування і вдосконалення правового регулювання для їх подолання.

Мережа Інтернет впливає на інформаційну безпеку як позитивно, так і негативно. З одного боку – повний доступ до всієї інформації з можливістю подальшої фільтрації, перевірки, і визначення для себе, яким джерелам можна довіряти, а яким не варто, з другого – легкість просування ворожих наративів через недостатність, а подекуди й неможливість контролю.

Аналіз дослідження проблеми. У вітчизняній науковій літературі проблеми інформаційної безпеки досліджували Д. Смотрич, Л. Браілко, І. Боднар, С. Кавун та інші.

Метою статті є розгляд проблемних питань інформаційної безпеки в умовах війни на просторах Інтернету та шляхи протистояння таким загрозам.

Виклад основного матеріалу. Інформаційне середовище завжди впливало на емоційний стан людей, ставлення до певних подій та явищ, цінності. В умовах війни вплив через інформаційне середовище використовується ворогом для маніпуляцій свідомістю та діями не лише окремих індивідів, але й цілих груп осіб, що є загрозою національній безпеці. Слід звернути увагу на те, що вважається загрозою на законодавчому рівні, відповідно до Закону України "Про національну безпеку України" загрози національній безпеці України – це явища, тенденції та фактори, які унеможливлюють або утруднюють, чи можуть унеможливити або утруднити реалізацію національних інтересів і збереження національної цінності України [1]. Такий негативний вплив здійснюється за допомогою засобів масової інформації, а найактивніше за допомогою соціальних мереж у мережі Інтернет.

В інформаційному середовищі Інтернет для пропаганди ворогом найактивніше використовуються соціальні мережі, месенджери, зокрема пабліки у них, що зумовлено реаліями сьогодення. Оскільки в умовах війни для кожного українця стало щоденною звичкою відстеження новин у реальному часі за допомогою отримання інформації у групах у месенджерах та соціальних мережах, логічним є активація пропагандистської діяльності ворога саме на цих платформах. Найбільшої популярності набули такі соціальні мережі, як Телеграм і Фейсбук, хоч і довіра до місцевих медіа і зросла, але чистота споживання їх контенту навпаки знизилась. Натомість, спостерігається значне зростання груп і каналів у месенджерах (від 11 до 41 %), а також ютуб (від 21 до 29 %) [2].

Однак негативний вплив ворог здійснює не лише шляхом маніпуляцій, створюючи власні пабліки, але й, наприклад, поширюючи "фейки" у коментарях у групах пабліків, що мають проукраїнську орієнтацію чи створюючи дуже правдоподібні "інформаційні вкиди", які поширюють ці пабліки.

Слово "фейк" походить від англ. fake – підробка, інформаційна містифікація чи відверта дезінформація з метою введення в оману, шахрайство [3]. Незважаючи на існування такого явища, такого терміна немає у законодавстві України, що ускладнює його регулювання та подолання.

Слушно зазначає І. Мудра: "… на фейки взагалі можна було б не звертати увагу, сприймати їх як байки чи гуморески, якби такі повідомлення не були б інформаційною зброєю масового ураження проти українського народу, яку активно застосовує у війні Росія. Основна мета фейкових повідомлень як інструменту інформаційної війни – це посіяти сумніви і переконати аудиторію у правдивості поданої інформації. А завдання: дезінформувати аудиторію; пропагувати власне бачення, політику чи позицію; викликати агресію; похитнути позицію індивідума і заставити його засумніватися; посіяти паніку; змінити уставлену думку в аудиторії; спонукати по певної дії; активувати увагу і зацікавити аудиторію; переконати аудиторію за допомогою вигаданих фактів; залякування аудиторії тощо. Тому пропонуємо таке визначення фейку: Фейк – це спеціально створена новина, подія чи журналістський матеріал, який містить неправдиву або перекручену інформацію, що дискримінує певну людину чи групу осіб в очах аудиторії" [4].

На сучасному етапі розвитку законодавчого регулювання боротьби з дезінформацією в мережі Інтернет немає чіткого механізму притягнення до відповідальності осіб, що створюють пабліки чи так звані канали, за поширення фейкової інформації, а тим паче, за коментарі в таких пабліках.

Враховуючи сутність і складність цифрового середовища й основ його функціонування, притягнення до відповідальності за поширення інформації, що не є обмеженою законами України, зокрема законом "Про інформацію", потребує додаткового вивчення та вирішення шляхів врегулювання.

Важливим є також рівень інформаційної грамотності населення України для подолання інформаційних загроз у мережі Інтернет. Оскільки ми звикли сприймати Інтернет як безпечне середовище, з якого отримуємо корисну інформацію, розваги, спілкування, перебудова сприйняття такого середовища як такого, що може нести значні загрози, є досить складним процесом, що потребує усвідомленості і конкретних знань, зокрема щодо методів маніпуляцій свідомістю людей за допомогою інформаційної пропаганди в мережі Інтернет. Отже, необхідним є прийняття на законодавчому рівні урядових програм та освітніх заходів органів місцевого самоврядування для підвищення цифрової грамотності населення, особливо з тих питань, що стосуються інформаційної безпеки в мережі Інтернет.

Слушною є думка, що для протидії масштабним інформаційним загрозам у мережі Інтернет, операціям інформаційної війни ворога, пріоритетними напрямами мають бути: 1) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 2) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; 3) вдосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове

регулювання інформаційних процесів; 4) розвиток національної інформаційної інфраструктури; 5) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 6) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління; 7) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері [5].

Висновки. Як свідчать реалії сьогодення, інформаційна війна Росії не має кордонів – вона направлена як на Україну, так і на країни Європи. А види інформаційних операцій в мережі Інтернет обмежені тільки уявою ворога, і щоб запобігти та протидіяти інформаційним загрозам, потрібно не лише прийняти нормативно правові-акти, які б відповідали реаліям сьогодення, а й створити ефективну систему інформаційної безпеки, розробити дієві стратегії та тактики протидії тим чи іншим загрозам, розробити новий план заходів щодо реалізації Стратегії інформаційної безпеки.

Не варто недооцінювати те, що в умовах інформаційної війни на нас діє цілий комплекс інформації, який був розрахований на маніпуляцію громадською думкою за допомогою різних методів.

Сьогодні відповідні міністерства і відомства працюють над посиленням комунікацій, підтримують різного роду ініціативи, але без конкретного плану заходів ця робота не може бути ефективною. Отже, виникає необхідність не лише вчасних відповідей на такі інформаційні загрози, але і здатність попереджувати загрози.

В умовах сьогодення інформаційний простір України в мережі Інтернет є недостатньо захищений від ворожих атак, що і допомагає державі агресору раз за разом знаходити способи здійснювати негативний вплив. Оскільки цифрове середовище складно піддається демократичному централізованому регулюваню, вбачається доцільним розглянути інші шляхи вирішення, зокрема інформаційна освіта населення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31.

2. Комплексне дослідження: як війна змінила мене та країну. Підсумок року. https://ratinggroup.ua/research/ukraine/kompleksne_dosl_dzhennya_yak_v_yna_zm_nila_mene_ta_kra_nu_p_dsumki_roku.

3. Слово фейк. Словотвір. https://slovotvir.org.ua/words/feik

4. Мудра І. (2016). Поняття фейк та його види у ЗМІ. *Теле- та радіожурналістика*, *вип. 15,* 184–188. http://publications.lnu.edu.ua/collections/index.php/teleradio/article/viewFile/694/699

5. Ільницька У. (2016). Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам, *Humanitarian vision, Vol. 2, Num. 1,* 27–32. http://nbuv.gov.ua/UJRN/hv_2016_2_1_7

REFERENCES

1. ***Pro natsional'nu bezpeku Ukrayiny : Zakon Ukrayiny vid 21.06.2018 r. No. 2469-VIII*** [On the national security of Ukraine: Law of Ukraine dated June 21, 2018 No. 2469-VIII].Vidomosti Verkhovnoyi Rady Ukrayiny. 2018. No. 31 [in Ukrainian].

2. ***Kompleksne doslidzhennya: yak viyna zminyla mene ta krayinu*** [Comprehensive Study: How the War Changed Me and the Country]. Pidsumok roku. Retrieved from: https://ratinggroup.ua/research/ukraine/kompleksne_dosl_dzhennya_yak_v_yna_zm_nila_mene_ta_kra_nu_p_dsumki_roku (accessed 29.09.2023). [in Ukrainian].

3. ***Slovo feyk. Slovotvir.*** [The word fake. Word work]. Retrieved from: https://slovotvir.org.ua/words/feik (accessed 29.09.2023).

4. Mudra I. (2016). ***Ponyattya feyk ta yoho vydy u ZMI*** [The concept of fake and its types in mass media]. Tele- ta radiozhurnalistyka, Vyp. 15, 184–188. Retrieved from: http://publications.lnu.edu.ua/collections/index.php/teleradio/article/viewFile/694/ 699(accessed 29.09.2023). [in Ukrainian].

5. Il′nyts'ka U. (2016). ***Informatsiyna bezpeka Ukrayiny: suchasni vyklyky, zahrozy ta mekhanizmy protydiyi nehatyvnym informatsiyno-psykholohichnym vplyvam*** [Information security of Ukraine: modern challenges, threats and countermeasures against negative informational and psychological influences], Humanitarian vision, Vol. 2, No. 1, 27–32. Retrieved from: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7 (accessed 29.09.2023). [in Ukrainian].

Дата надходження: 12.08.2023 р.

Iryna Krykavska
Lviv Polytechnic National University,
Assistant professor of the Department of administrative and informational law of
Educational and Scientific Institute of Jurisprudence,
Psychology and Innovative Education
Candidate of Laws Sciences
iryna.v.krykavska@lpnu.ua
ORCID iD: https://orcid.org /0000-0002-6108-2447

Mariana Povalena
Lviv Polytechnic National University,
Assistant professor of the Department of administrative and informational law of
Educational and Scientific Institute of Jurisprudence,
Psychology and Innovative Education
Candidate of Laws Sciences
mariana.v.povalena@lpnu.ua
ORCID iD: https://orcid.org /0000-0001-5638-200X

Ostap-Zenovii Muzyka
Lviv Polytechnic National University,
Master's degree student of
Educational and Scientific Institute of Jurisprudence,
Psychology and Innovative Education
ostap-zenovii.muzyka.mpvpr.2022@lpnu.ua

INFORMATION THREATS ON THE INTERNET IN THE CONDITIONS OF WAR IN UKRAINE: PROBLEMATIC ISSUES OF LEGAL REGULATION

The article examines the issue of information security as a state of protection of the vital interests of a person, society and the state, in which damage should be prevented due to: incompleteness, untimeliness and implausibility of the information used.

The current situation in Ukraine, in particular the war with Russia, deepens the understanding of the urgency of the need to build an effective system to ensure the protection of the Ukrainian information space, in particular the Internet. In order to ensure information security, normative acts regulating the main issues were adopted, in particular the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On the Information Security Doctrine of Ukraine", as well as the decision of the National Security and Defense Council of Ukraine dated March 18, 2022 "Regarding the implementation of a unified information policy in the conditions of martial law." However, informational threats on the Internet are a very dynamic phenomenon that requires constant response and improvement of the legal regulation of their submission.

The Internet affects information security both positively and negatively. On the one hand – full access to all information, with the possibility of further filtering, checking, and determining for yourself

which sources can be trusted and which should not, on the other hand – the ease of promoting hostile narratives, due to the insufficiency, and in some cases, the impossibility of control.

The Internet network affects information security both positively and negatively, on the one hand, full access to all information, with the possibility of further filtering, checking, and determining for yourself which sources can be trusted and which should not, on the other hand, the ease of promoting hostile narratives, through the lack of control, as well as the ease due to ignorance to fall into the wrong tags, for example, those people who use the Internet in Russian will have mainly pro-Moscow news in their feed, and without knowledge of both languages it is very easy to fall under the influence of propaganda.

The ways of negative influence used by the enemy in the information environment of the Internet have been studied.

The essential priority directions necessary to counteract large-scale information threats on the Internet, the enemy's information warfare operations, are outlined.

An important conclusion is the need to increase the level of information literacy of the population of Ukraine in order to overcome information threats on the Internet.

Keywords: information security; information threats; Internet.