УДК 343.9
DOI 10.33244/2617-4154.2(11).2023.125-131

В. В. Топчій,
д-р юрид. наук, професор,
заслужений юрист України
e-mail: tv1959@ukr.net
ORCID ID 0000-0003-4596-6469;
Г. В. Дідківська,
д-р юрид. наук, професор,
Державний податковий університет
e-mail: galynadid@gmail.com
ORCID ID 0000-0002-3545-0429

НЕОБХІДНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ОКУПАЦІЇ: ІРПІНЬ, БУЧА, ГОСТОМЕЛЬ

У статті зазначено, що окупація територій Ірпеня, Бучі, Гостомеля та інших територій, що і досі в окупації, показала, що інформаційна маніпуляція є небезпечним чинником в умовах війни, яка, безперечно, ведеться повною мірою також і у кіберпросторі. Акцентується увага і на тому, що терміни «інформаційна війна», «інформаційна зброя» та «інформаційний тероризм» давно набули поширення, але в умовах воєнного часу вони набувають зовсім іншого значення з огляду на загрози, які існують. Тому пріоритетним завданням держави є сприяння формуванню інформаційної культури суспільства. Одним з елементів такої культури є здатність аналізувати інформацію та фільтрувати джерела її поширення.

Вказується, що на сьогодні основними можливостями розповсюдження інформаційних викривлень та отримання недостовірної інформації, особливо в умовах військових конфліктів та війни, можуть бути джерела надання інформації через інтернет-мережу різних соціальних груп або зчитування інформації з підроблених соціальних сторінок відомих політиків, акторів, підроблених сторінок відомих блогерів, отримання інформації через перегляд новин на теле- та радіомовних каналах країни-агресора.

У статті також зазначається, що інформаційна безпека має велике значення, а саме в періоди ведення війни та воєнних конфліктів. Адже неправильно, неправдиво подана інформація може призвести до хаосу у суспільстві, мати негативний вплив на перебіг подій, недовіру до керівництва держави, підривати авторитет ЗСУ, що може негативно впливати на ведення бойових дій, а також завдати невиправних тяжких наслідків перебігу військових дій. Ось чому запобігання розповсюдженню недостовірної інформації, особливо під час війни, має надважливе значення для стабілізації ситуації у нашій державі та остаточної перемоги над ворогом.

***Ключові слова**: інформаційна безпека, війна, військова агресія, тяжкі наслідки, воєнний конфлікт, кібератака, протидія розповсюдженню недостовірної інформації.*

Враховуючи, що Україна зазнала військової агресії та щодо неї здійснено повномасштабне вторгнення з території рф і Білорусі від 24 лютого 2022 року, у нашій державі запроваджено воєнний стан. Водночас російські військові здійснюють агресію проти України і через соціальні мережі, інші засоби зв'язку. Кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури зросла втричі. Більшість нападів здійснюють військові хакери з ворожого боку, діяльність яких фінансується владою-терористом. Це відчутно особливо на територіях, які були окуповані: Буча, Ірпінь, Гостомель, інші тимчасово окуповані території, також які досі під окупацією і на територіях яких відчувається сильний інформаційний тиск ворога.

Тому основними механізмами протидії неправдивої, викривленої, неперевіреної інформації в умовах військових конфліктів і бойових дій вважають такі: необхідність формування медіаграмотності населення; медіаграмотність виступає як комплексний феномен, що дозволяє населенню захищатися, зокрема, від маніпулятивних впливів та брати участь у реалізації інформаційної безпеки; медіа грамотність має чотири важливі складові: критичне мислення, медіаорієнтування, медіаспоживання та медіадизайн. Медіаманіпуляція суспільною свідомістю чи думкою досягається за рахунок впливів на наше сприйняття через зір (це медіадизайн); через можливість орієнтуватися в інформаційних потоках, часто у рядового споживача їх досить багато, а часу мало на фактичне орієнтування; через великі обсяги контенту, які сипляться на кожну людини, також через неможливість критично сприймати інформацію через довіру, наприклад, конкретним ЗМІ [1].

Оскільки на початок військової агресії населення нашої держави не було інформаційно підготовленим, країна агресор всебічно цим скористалась.

Одним з основних завдань рф постало намагання завдати якомога більше шкоди звичайним людям шляхом як ракетних та інших обстрілів, так і кібератак, у зокрема і в інформаційному просторі.

Через воєнні дії багато установ перенесли свої дані – хтось в інші, більш спокійні регіони країни, хтось – у хмару на території України, хтось – у хмару за кордон. Проте, як і раніше, всі інформаційні системи, вимагають захисту. Захисту, який закріплений у законодавстві України. Інформаційні системи мають бути захищені за чинними стандартами. Зокрема, КСЗІ, а в деяких випадках допустиме використання європейських стандартів ISO/IEC 27 серії. Саме системи захисту інформації є першим кордоном, що стримує ворога від знищення нашої країни в кіберпросторі [2].

Варто акцентувати увагу, що поняття інформаційної безпеки, залежно від його використання, розглядається у декількох аспектах.

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини: створення і розповсюдження

вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації. Також дві забезпечувальні предметні частини: створення та застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення; створення та застосування засобів і механізмів інформаційної безпеки.

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Варто зазначити, що задоволення будь-якою мірою потреб в інформації приводить до оволодіння відомостями про навколишній світ та процеси, що протікають у ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності та, як наслідок, обґрунтованість рішень і дій, що приймаються.

Залежно від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати так: забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформація та інформаційні ресурси від неправомірного впливу сторонніх осіб; інформаційні права і свободи людини та громадянина.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави й акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [3].

Дещо відмінними є визначення, наведені та закріплені на законодавчому рівні.

Так, інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій;

інформаційна сфера – сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб'єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин;

інформаційна інфраструктура – сукупність організаційних структур і систем, які забезпечують функціонування та розвиток інформаційного простору, засобів інформаційної взаємодії та доступу користувачів до інформаційних ресурсів;

забезпечення інформаційної безпеки – діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України;

загрози інформаційній безпеці – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави в інформаційній сфері [4].

Метою інформаційної безпеки вважають насамперед забезпечення безперервності бізнесу і захисту інформаційних даних, інфраструктури від випадкового чи навмисного втручання, що може стати причиною втрати даних або їх несанкціонованої зміни [5].

Етичні норми передбачають, що користувачі комп'ютерів не використовують комп'ютерну техніку та програмне забезпечення для завдання шкоди іншим людям, не порушують авторських прав.

Правові основи захисту даних базуються на правових актах, що утверджують права і свободи людини та якими встановлено відповідальність за злочини в галузі інформаційної безпеки. В Україні ухвалено ряд законів та постанов щодо забезпечення інформаційної безпеки: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних», «Про авторське право та суміжні права» тощо. Незаконне втручання в роботу комп'ютерів, комп'ютерних мереж та розповсюдження вірусів зумовлює кримінальну відповідальність (ст. 361 Кримінального кодексу України) [6].

Як показала окупація територій Ірпеня, Бучі, Гостомеля та інших територій, що і досі в окупації, інформаційна маніпуляція є небезпечним чинником в умовах війни, яка, безперечно, ведеться повною мірою також й у кіберпросторі. Терміни «інформаційна війна», «інформаційна зброя» та «інформаційний тероризм» давно набули поширення, але в умовах воєнного часу вони набувають зовсім іншого значення з огляду на загрози, які існують. Тому пріоритетним завданням держави є сприяння формуванню інформаційної культури суспільства. Одним з елементів такої культури є здатність аналізувати інформацію та фільтрувати джерела її поширення [7].

Отже, цілком слушною є думка, що інформаційна безпека передбачає: належний рівень інформаційної культури, тобто теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку й задоволення потреб особи в інформації незалежно від наявності інформаційних загроз; гарантування, розвиток і використання інформаційного середовища в інтересах особистості; захищеність від різних інформаційних загроз [8]. У цьому контексті важливо зазначити важливість освітньої складової, яка полягає в систематичному навчанні інформаційній безпеці й інформаційній культурі у закладах середньої та вищої освіти, підвищенні кваліфікації для працівників органів державної влади та місцевого самоврядування, які працюють з інформацією. Згідно із Законом України «Про національну безпеку України» загрозами національній безпеці України є явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [9].

Отже, варто мати на увазі, що гарною запорукою є підготовка кращої допомоги близьким і тим, хто особливо її потребує. Необхідно чітко розуміти послідовність впровадження заходів, які допоможуть більш ефективно впоратися з кризою окупації чи військової агресії та зменшити негативні наслідки для суспільства загалом. Коли безпека суспільства під загрозою, готовність до взаємної допомогти стає вирішальним чинником.

В умовах військової агресії Україна вимушена протидіяти ворожій пропаганді та дезінформації. Агресивні дії з боку росії мають на меті дестабілізувати наше суспільство та дискредитувати керівництво країни, змусити нас сумніватися у своїх силах і готовності захищатися. Питання інформаційної безпеки набуває особливого значення в умовах кризи, адже ворожі інформаційні атаки стають більш інтенсивними саме тоді, коли здатність суспільства чинити опір послаблено. Найкраще підґрунтя для ворожих операцій впливу – страх, паніка, дезорієнтація. Тому важливо дотримуватися базових правил інформаційної гігієни і бути особливо пильними до інформації, яка надходить і яку поширюєте ви самі [10].

Як бачимо, стрімке зростання соціальної значущості інформаційних технологій полягає в тому, що, як вважають дослідники, «соціальні мережі, месенджери, інтернет-магазини, онлайн-банкінг – усі ці засоби зв'язку та комунікації потенційно вразливі» [11].

На сьогодні основними можливостями розповсюдження інформаційних викривлень та отримання недостовірної інформації, особливо в умовах військових конфліктів і війни, можуть бути джерела надання інформації через інтернет-мережу різних соціальних груп або зчитування інформації з підроблених соціальних сторінок відомих політиків, акторів, підроблених сторінок відомих блогерів, отримання інформації через перегляд новин на теле- та радіомовних каналах країни-агресора.

Висновки. Як бачимо, інформаційна безпека має велике значення, а саме в періоди ведення війни та воєнних конфліктів. Адже неправильно, неправдиво подана інформація може призвести до хаосу у суспільстві, мати негативний вплив на перебіг подій, недовіру до керівництва держави, підривати авторитет ЗСУ, що може негативно впливати на ведення бойових дій, а також може завдати невиправних тяжких наслідків перебігу військових дій. Ось чому запобігання розповсюдженню недостовірної інформації, особливо під час війни, має надважливе значення для стабілізації ситуації у нашій державі та остаточної перемоги над ворогом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bykov I. A., Balakhonskaya L. V., Gladchenko I. A., Balakhonsky V. V. Verbal aggression as a communication strategy in digital society. Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop. Saint-Petersburg, 2018. P. 12–14.

2. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. URL : https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku (дата звернення: 31.01.2023).

3. Поняття інформаційної безпеки. URL : https://sites.google.com/site/infobezosob/home/informacijna-dialnist (дата звернення: 31.01.2023).

4. Про засади інформаційної безпеки України : проєкт Закону України. URL : https://ips.ligazakon.net/document/JG3TH00A?an=8 (дата звернення: 31.01.2023).

5. Хто стоїть на варті кібербезпеки. URL : https://wiseit.com.ua/services/rishennya-ta-servisy/informaczijna-bezpeka/ (дата звернення: 31.01.2023).

6. Основні поняття інформаційної безпеки. URL : https://miyklas.com.ua/p/informatica/9-klas/programne-zabezpechennia-ta-informatciina-bezpeka-327110/informatciina-bezpeka-327251/re-813d7f93-b124-47bb-92c6-261cf0cd2162 (дата звернення: 31.01.2023).

7. Француз-Яковець Т. А. Інформаційна безпека в умовах війни. URL : http://dspace.onua.edu.ua/bitstream/handle/11300/19251/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7-%D0%AF%D0%BA%D0%BE%D0%B2%D0%B5%D1%86%D1%8C%20%D0%A2%D0%B5%D1%82%D1%8F%D0%BD%D0%B0%20%D0%90%D0%BD%D0%B0%D1%82%D0%BE%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y (дата звернення: 31.01.2023).

8. Інформаційна безпека (соціально-правові аспекти) : підручник / В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін. К. : КНТ, 2010. 776 с.

9. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради (ВВР)*. 2018. № 31.

10. Грошева Е. К., Невмержицкий П. И. Информационная безопасность: современные реалии. *Бизнес-образование в экономике знаний.* 2017. № 3. С. 35–38.

11. Пархоменко-Куцевіл О. І. Проблеми забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління у сфері державної безпеки та охорони громадського порядку.* 2022. Випуск 28. С. 177–181.

REFERENCES

1. Bykov I. A., Balakhonskaya L. V., Gladchenko I. A., Balakhonsky V. V. Verbal aggression as a communication strategy in digital society. Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop. Saint-Petersburg, 2018. P. 12–14.

2. Vymohy do zakhystu informatsii v informatsiinykh systemakh u voiennyi chas: roz'iasnennia Derzhspetszviazku. URL : https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku (data zvernennia: 31.01.2023).

3. Poniattia informatsiinoi bezpeky. URL : https://sites.google.com/site/infobezosob/home/informacijna-dialnist (data zvernennia: 31.01.2023).

4. Pro zasady informatsiinoi bezpeky Ukrainy : proekt Zakonu Ukrainy. URL : https://ips.ligazakon.net/document/JG3TH00A?an=8 (data zvernennia: 31.01.2023).

5. Khto stoit na varti kiberbezpeky. URL : https://wiseit.com.ua/services/rishennya-ta-servisy/informaczijna-bezpeka/ (data zvernennia: 31.01.2023).

6. Osnovni poniattia informatsiinoi bezpeky. URL : https://miyklas.com.ua/p/informatica/9-klas/programne-zabezpechennia-ta-informatciina-bezpeka-327110/informatciina-bezpeka-327251/re-813d7f93-b124-47bb-92c6-261cf0cd2162 (data zvernennia: 31.01.2023).

7. Frantsuz-Yakovets T. A. Informatsiina bezpeka v umovakh viiny. URL : http://dspace.onua.edu.ua/bitstream/handle/11300/19251/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7-%D0%AF%D0%BA%D0%BE%D0%B2%D0%B5%D1%86%D1%8C%20%D0%A2%D0%B5%D1%82%D1%8F%D0%BD%D0%B0%20%D0

%90%D0%BD%D0%B0%D1%82%D0%BE%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y (data zvernennia: 31.01.2023).

8. Informatsiina bezpeka (sotsialno-pravovi aspekty) : pidruchnyk / V. V. Ostroukhov, V. M. Petryk, M. M. Prysiazhniuk ta in. K. : KNT, 2010. 776 s.

9. Pro natsionalnu bezpeku Ukrainy : Zakon Ukrainy vid 21 chervnia 2018 roku № 2469-VIII. *Vidomosti Verkhovnoi Rady (VVR)*. 2018. № 31.

10. Hrosheva E. K., Nevmerzhytskyi P. Y. Ynformatsyonnaia bezopasnost: sovremennыe realyy. Byznes-obrazovanye v ekonomyke znanyi. 2017. № 3. S. 35–38.

11. Parkhomenko-Kutsevil O. I. Problemy zabezpechennia informatsiinoi bezpeky pid chas zdiisnennia viiskovykh operatsii ta boiovykh dii. *Publichne upravlinnia u sferi derzhavnoi bezpeky ta okhorony hromadskoho poriadku*. 2022. Vypusk 28. S. 177–181.

V. Topchii, G. Didkivska. The need for information security during the occupation: Irpin, Bucha, Gostomel

This article states that the occupation of the territories of Irpin, Buchi, Gostomel and other territories, which are still under occupation, showed that information manipulation is a dangerous factor in the conditions of war, which is undoubtedly being waged in full in cyberspace as well. Attention is also focused on the fact that the terms "information war", "information weapon" and "information terrorism" have long been widespread, but in wartime conditions they acquire a completely different meaning in view of the threats that exist. Therefore, the priority task of the state is to promote the formation of society's information culture. One of the elements of such a culture is the ability to analyze information and filter the sources of its distribution.

It is indicated that today, the main possibilities of spreading information distortions and obtaining unreliable information, especially in the conditions of military conflicts and war, can be the sources of providing information through the Internet network of various social groups, or reading information from fake social pages of famous politicians, actors, fake pages of famous bloggers Obtaining information through watching news on TV and radio channels of the aggressor country.

The article also notes that information security is of great importance, namely during periods of war and military conflicts. After all, incorrectly, falsely presented information can lead to chaos in society, have a negative impact on the course of events, distrust of the state leadership, undermine the authority of the Armed Forces, which can negatively affect the conduct of hostilities, and can also cause irreparable and serious consequences of the course of hostilities. That is why preventing the spread of false information, especially during wartime, is of paramount importance for the stabilization of the situation in our country and the final victory over the enemy.

Keywords*: information security, war, military aggression, grave consequences, military conflict, cyber attack, countering the spread of false information.*

Стаття надійшла до редколегії 28 лютого 2023 року