DOI https://doi.org/10.36059/978-966-397-287-9-83

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ

Шевчук Олександр Михайлович
доктор юридичних наук, професор,
професор кафедри адміністративного права
та адміністративної діяльності
Національного юридичного університету імені Ярослава Мудрого
м. Харків, Україна

Загрози в інформаційній сфері впливають на інтереси людини, суспільства та держави. У Конституції України (ст. 17) закріплюється пріоритетність інформаційної безпеки, як основної функції держави. Форми та прояви інформаційного тероризму є однією із загроз національній безпеці України [1, с. 173], та набувають особливо важливого значення під час воєнного стану. 24 лютого 2022 року в Україні введено воєнний стан, причиною чому стала військова агресія російської федерації проти України [2]. Продовження повномасштабного вторгнення російської федерації загрожує національній безпеці України та інших держав Балтійського і Чорноморського регіонів, та може спровокувати міжнародний збройний конфлікт у Європі [3, с. 326]. Це указує на актуальність теми дослідження щодо з'ясування проблемних питання становлення та розвитку законодавства з питань протидії інформаційному тероризму як загрозі національній безпеці України умовах воєнного стану в Україні.

Окремим питанням щодо досліджуваної тематики в юридичній літературі приділяли певну увагу дослідники, зокрема, в напрямках наукового пошуку щодо інформаційного тероризму як одного із способів інформаційної війни [4], з питань інформаційної безпеки за міжнародними стандартами [-], ознаки загроз «інформаційного тероризму» [5] та ін. Проте до сих пір не вироблено у науковців єдиного підходу щодо сутності та ознак інформаційного тероризму в умовах воєнного стану, що підкреслює новизну цієї публікації.

Однак, ще із кінця 90-х років минулого століття в рамках міжнародних організацій питання протидії інформаційному тероризму набуло актуальності. Зокрема, Генеральна Асамблея ООН у грудні 1998 року прийняла Резолюцію по кіберзлочинності, щодо кібертероризму та кібервійни [6]. В липні 2000 року у прийнятій Хартії Глобального інформаційного суспільства, визначено, що використання глобального інформаційного простору є основним фактором, що формує суспільство

21-го сторіччя, та є потреба повної реалізації його переваг і розробки напрямків зміцнення політики його використання та впровадження нормативно-правової бази по боротьбі зі зловживаннями інформаційних мереж [7]. У 2006 р. в Декларації саміту G8 щодо боротьби з тероризмом вперше «терористичну загрозу» було визнано «зловживання кіберпростором у терористичних цілях, включаючи підбурювання до здійснення терактів, зв'язок та планування терористичних актів, а також вербування на навчання терористів» [8]. У 2007 р. учасники засідання Міністрів юстиції та внутрішніх справ G8 підтримали позицію щодо кримінального переслідування терористичних груп за неправомірне використання Інтернету.

Законом України «Про національну безпеку» визначається, що загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України (ст. 1) [9]. Також наведемо термін «загрози державній безпеці» – як явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити захищеність державного суверенітету, територіальної цілісності та демократичного конституційного ладу й інших життєво важливих національних інтересів [10]. У цій Стратегії забезпечення державної безпеки передбачено термін «інформаційна безпека» та проголошено, що інформаційна безпека є складовою національної безпеки України. Інформаційна безпека – стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України [10].

Вкажімо, що термін «інформаційний тероризм» у положеннях Закону України "Про боротьбу з тероризмом" не визначено, однак потрібно навести категорію «технологічного тероризму», яка передбачена на законодавчому рівні. Цей термін законодавець указує як кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей

речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; (ст.1) [11]. Т.П. Яцик вважає, що сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму [4, с. 57]. В.О. Коршунов вказує, що інформаційний тероризм – це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [12, с. 6]. Із цим твердженням варто погодитись.

Інформаційний тероризм окремі експерти поділяють на: (1) інформаційно-психологічний тероризм (контроль над ЗМІ для поширення дезінформації, чуток, демонстрації могутності терористичних організацій); (2) інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу загалом: руйнування елементної бази, створення перешкод на лініях зв'язку, штучне перенавантаження вузлів комунікації та інше). В наукових джерелах до загроз віднесено: (1) поширення недостовірної, неповної або упередженої інформації; (2) прояви обмеження свободи слова та доступу громадян до інформації; (3) поширення засобами масової інформації культу насильства, жорстокості, порнографії; (4) комп'ютерна злочинність та комп'ютерний тероризм; (5) розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави [6]. Вищенаведені загрози можуть бути і в умовах воєнного стану. До основних ознак інформаційного тероризму в умовах воєнного стану слід віднести: (1) є однією із форм організованого насильства, як особливий різновид психологічного терору; (2) поширюється через засоби масової інформації; (3) мета інформаційного тероризму – привернути увагу до проблеми, залякати та деморалізувати населення; (5) публічний характер дій тощо. Отже, інформаційний тероризм в умовах воєнного стану – це насамперед, форма негативного впливу на особистість, суспільство і державу усіма видами інформації.

Література:

1. Леонов Б., Лихова С. Інформаційний тероризм як загроза національній безпеці України. Scientific works of National Aviation University. Series: Law Journal «Air and Space Law». 2021. Т. 2, № 59. С. 170–176.
2. Про правовий режим воєнного стану: Закон України від 12.05.2015 р. № 389-VIII. Відомості Верховної Ради. 2015. № 28. ст. 250.
3. Шевчук О.М. Розвиток громадянського суспільства та воєнна безпека в контексті Європейської інтеграції України. С. 326–329. Львів-Торунь : Liha-Pres, 2022. 344 с. DOI. https://doi.org/10.36059/978-966-397-271. URL. PDF view of the file omptestuser, 88.pdf (liha-pres.eu)
4. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Наук. вісн. Нац. ун-ту держ. податк. служби України (економіка, право).* 2014. № 2. С. 55–60.
5. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами. *Альманах економічної безпеки*. 1999. № 2. С. 15–17.
6. Герасименко К. С. Сучасні ознаки загроз “інформаційного тероризму” // *Форум права.* 2009. № 3. С. 162-166. URL: file:///C:/Users/User/Downloads/FP_index.htm_ 2009_3_26%20(12).pdf
7. Окінавская Хартія Глобального інформаційного суспільства. *Дипломатичний вісник.* 2000. № 8. С. 51-56
8. The Global Terrorism Index 2016. URL. http://visionofhumanity.org/app/uploads/2017/02/Global-Terrorism-Index-2016.pdf
9. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Відомості Верховної Ради. 2018. № 31. Ст. 241.
10. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». Указ Президента України від 16 лютого 2022 р. № 56/2022. https://zakon.rada.gov.ua/laws/show/56/2022#Text
11. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. Відомості Верховної Ради України. 2003. № 25. Ст.180.
12. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. …канд. політ. наук. Дніпропетровськ, 2008. 18 с.