Список використаних джерел:

1. Сидоренко Н.О. “Діджиталізація: електронні адміністративні послуги” https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/93/84
2. Закон України від 15 липня 2021 року № 1689-IX «Про особливості надання публічних (електронних публічних) послуг». https://zakon.rada.gov.ua/laws/show/1689-20#Text
3. Тищенко І. О. Електронні послуги у діяльності публічної адміністрації України.
4. Положення про Єдиний державний веб-портал електронних послуг від 4 грудня 2019 р. № 1137.
5. Закон України від "Про адміністративні послуги" №5203-VI https://zakon.rada.gov.ua/laws/show/5203-17#Text
6. Закон України "Про електронну ідентифікацію та електронні довірчі послуги" №2155-VIII https://zakon.rada.gov.ua/laws/show/2155-19#Text
7. Постанова Кабінету Міністрів України від 5 серпня 2022 р. №868 https://zakon.rada.gov.ua/laws/show/868-2022-%D0%BF#Text

Степаненко Наталія
Університет економіки та права “КРОК”,
доцентка кафедри теорії та історії держави і права,
докторка філософії в галузі права, доцентка

Забезпечення прав людини в умовах цифрових технологій під час воєнного конфлікту

Інтенсивне використання цифрових технологій у ході збройної агресії проти України та в умовах воєнного стану кардинально змінює парадигму захисту прав людини, генеруючи як безпрецедентні загрози, так і нові інструменти для правозахисної діяльності та документування воєнних злочинів. Ця реальність вимагає не лише глибокого аналізу викликів у межах національної правової системи, але й активного розвитку міжнародно-правових стандартів та механізмів їх імплементації з урахуванням українського досвіду. Цифровізація конфлікту ставить перед українською державою та суспільством складні завдання щодо забезпечення фундаментальних прав і свобод громадян в умовах, коли інформаційний простір став повноцінним театром воєнних дій [1].

Ключовими викликами для прав людини в Україні стали масові кібератаки на державні інформаційні ресурси та об’єкти критичної інфраструктури, що здійснюються державою-агресором та пов’язаними з нею хакерськими угрупованнями. Такі дії становлять пряму загрозу національній безпеці, стабільному функціонуванню суспільства та реалізації широкого спектру прав громадян, від права на життя та здоров’я до права на доступ до державних послуг. Окрему небезпеку становить використання цифрових інструментів для ведення агресивної інформаційно-психологічної війни, включаючи поширення масштабної дезінформації, пропаганди та фейкових новин з метою дестабілізації суспільства, підриву довіри до державних інституцій та маніпулювання громадською думкою, що прямо впливає на право громадян на отримання достовірної інформації [2, с. 125].

Правове регулювання протидії цим загрозам в Україні активно розвивається, однак застосування норм міжнародного гуманітарного права до кібероперацій залишається складним питанням, зокрема в частині кваліфікації атак, встановлення відповідальності (атрибуції) та застосування принципів розрізнення і пропорційності у цифровому просторі. Важливим завданням є гармонізація національного законодавства у сфері кібербезпеки та захисту інформації з міжнародними стандартами, а також вироблення ефективних механізмів реагування на порушення цифрових прав людини в умовах воєнного стану, включаючи право

на приватність та захист персональних даних під час ідентифікації осіб, моніторингу комунікацій чи використання систем відеоспостереження [4, с. 90].

Водночас, в умовах збройного конфлікту поглиблюється проблема «цифрової нерівності», коли частина населення, особливо внутрішньо переміщені особи, люди похилого віку та мешканці тимчасово окупованих або деокупованих територій, мають обмежений доступ до цифрових комунікацій, інтернету та державних електронних сервісів. Це створює додаткові перешкоди для реалізації їхніх соціальних, економічних та інформаційних прав. Також існує потенційний ризик дискримінації при використанні автоматизованих систем аналізу даних чи штучного інтелекту, якщо такі системи будуть впроваджуватися без належної перевірки на упередженість та без забезпечення прозорості їх роботи.

Поряд із загрозами, цифрові технології стали незамінним інструментом для України у фіксації та документуванні воєнних злочинів та злочинів проти людяності, скоєних агресором. Методи розвідки на основі відкритих джерел (OSINT), аналіз супутникових знімків, фото- та відеоматеріалів, зібраних громадянами та журналістами, використовуються правоохоронними органами та міжнародними слідчими групами як доказова база. Створюються державні та громадські платформи для збору свідчень. Цифрові канали забезпечують оперативну комунікацію, координацію гуманітарної допомоги та інформування громадян про небезпеку, що є критично важливим для збереження життів [6, с. 145].

Отже, ефективний захист прав людини в Україні в умовах цифрової війни вимагає комплексних зусиль: подальшого вдосконалення національного законодавства у сфері кібербезпеки, протидії дезінформації та захисту персональних даних відповідно до міжнародних стандартів та з урахуванням специфіки воєнного стану; зміцнення інституційної спроможності державних органів; розвитку механізмів міжнародного співробітництва для розслідування кіберзлочинів та притягнення винних до відповідальності; підтримки незалежних медіа та ініціатив з підвищення медіаграмотності населення; а також забезпечення максимальної доступності цифрових послуг для всіх громадян, особливо вразливих категорій. Український досвід протидії цифровим загрозам та використання технологій для захисту прав людини має стати предметом ретельного вивчення та врахування при формуванні глобальних підходів до регулювання цифрового простору в умовах конфліктів.

Список використаних джерел:

1. Правовий режим воєнного стану: український досвід та міжнародна практика : монографія / за заг. ред. Н. М. Оніщенко, Н. М. Пархоменко. Київ: Юридична думка, 2023. 416 с.
2. Цифрові технології на війні: загрози та засоби протидії : монографія / за заг. ред. В. Л. Шевченка. Київ : НДІ інформатики і права НАПрН України, 2023. 210 с.
3. Скрипнюк О. В. Протидія дезінформації в умовах воєнного стану: конституційно-правовий вимір. *Вісник Національної академії правових наук України*. 2022. Т. 29, № 2. С. 23–38. URL: http://visnyk.kh.ua/web/uploads/pdf/Visnik_2_2022%20(1).pdf#page=23
4. Фурашев В. М., Шемякін О. В. Застосування міжнародного гуманітарного права до кібероперацій під час збройних конфліктів. *Інформація і право.* 2022. № 3 (42). С. 81–93. DOI: 10.37750/2616-6798.2022.3(42).270201.
5. Арістова І. В. Захист персональних даних в умовах воєнного стану: правові виклики та шляхи їх подолання. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2023. Вип. 76. С. 215–220. DOI: 10.24144/2307-3322.2023.76.34.
6. Пилипенко В. П., Коваленко А. В. Використання даних з відкритих джерел (OSINT) при документуванні та розслідуванні воєнних злочинів в Україні. *Юридичний науковий електронний журнал.* 2023. № 4. С. 144–152. URL: http://www.lsej.org.ua/4_2023/34.pdf