№ 2956-IX. URL: https://zakon.rada.gov.ua/laws/show/2956-20#Text (дата звернення: 05.02.2024).

УДК 343.4(043.2)

Похиленко І.С., к.ю.н., доцент,
Київський національний університет будівництва і архітектури,
м. Київ, Україна

ПРАВОВІ ЦІННОСТІ В ЦИФРОВІЙ ПЛОЩИНІ ЯК СКЛАДОВА РОЗВИТКУ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ НА ШЛЯХУ ДО ЄС

Цифрові технології є невід'ємною частиною сучасного суспільства. Вони змінюють способи нашого життя, роботи та спілкування. Водночас цифрові технології створюють нові виклики та загрози для прав людини та демократичних цінностей.

Україна, як і інші країни Європейського Союзу, прагне до розвитку цифрової держави. Це передбачає створення ефективної та прозорої системи державного управління, яка використовує цифрові технології для підвищення якості життя громадян.

Успішний розвиток цифрової держави в Україні можливий лише за умови дотримання правових цінностей. Ці цінності є основою для справедливого та рівного доступу громадян до цифрових технологій, захисту їхніх прав та свобод у цифровій площині.

Серед правових цінностей, які є основою для розвитку цифрової держави, можна виділити такі:

Права людини: права людини є основою будь-якого демократичного суспільства. У цифровій площині вони включають право на приватність, свободу вираження поглядів, рівний доступ до інформації та освітніх ресурсів.

Демократичне управління: цифрові технології можуть бути використані для підвищення ефективності та прозорості державного управління. Водночас важливо, щоб ці технології використовувалися у спосіб, який відповідає демократичним цінностям.

Справедливість: цифрові технології можуть посилити соціальну несправедливість, якщо вони не будуть доступними для всіх громадян. Важливо забезпечити справедливий доступ до цифрових технологій для всіх, незалежно від їхнього соціального статусу, місця проживання чи інших характеристик.

Умови воєнного стану в Україні створюють додаткові виклики для забезпечення правових цінностей у цифровій площині. Російська агресія

призвела до порушення прав людини, зокрема, і в діджиталсфері (порушення приватності, поширення дезінформації та кібератаки).

Загалом кількість DDoS-атак у 1 кв. 2022 р., порівняно з 1 кв. 2021 р., збільшилася на 450%, а тривалість таких атак зросла майже на 8 000% [1]. Хоча найбільше збоїв відбувалось у лютому-березні 2022 р., DDoS-атаки продовжують вражати Україну. За даними Держспецзв'язку, з початку широкомасштабної війни росії проти України, остання зазнала 2 194 кібератаки. Рекорд склав 275 DDoS-атак на добу [2]. З початку війни СБУ нейтралізувала майже 3 500 кібератак на органи влади та об'єкти інфраструктури [3]. З них 1 650 кіберзагроз виявлено в режимі реального часу. Більшість російських атак мали на меті або знищити цифрові сервіси, або дестабілізувати роботу стратегічно важливих підприємств енергетичної та транспортної галузей. Також слід згадати масштабний збій у роботі оператора мобільного зв'язку "Київстар", який стався 12 грудня 2023 року. Офіційно мережу атакували хакери. Через збій по всій країні був відсутній мобільний зв'язок та інтернет від "Київстару" у 24 млн клієнтів. Не працював сайт оператора та мобільний додаток. При цьому компанія «Київстар» заявила, що персональні дані абонентів не скомпрометовані [4]. До ліквідації наслідків атаки були залучені компанії Microsoft, Cisco, Ericsson [5]. За словами начальника служби зв'язків з громадськістю командування Сухопутних військ ЗСУ підполковник Володимира Фітьо [6] збій у роботі «Київстар» не вплинув на дії українських військовослужбовців на лінії фронту. В свою чергу заступник глави Нацбанку України Олексій Шабан заявив, що українські банки мають створити резервні канали зв'язку для своєї інфраструктури через збої частини POS-терміналів після хакерської атаки на «Київстар». Він також зазначив, що Нацбанк «протягом 2022-2023 років постійно фіксував кібератаки різного рівня складності на об'єкти інформаційної інфраструктури банків та небанківських фінустанов» та закликав фінансові установи до посилення їхньої кібербезпеки [7].

Підсумовуючи викладене, слід відмітити, що в умовах воєнного стану важливо посилити правове регулювання цифрової сфери в Україні. Це дозволить забезпечити захист прав людини та демократичних цінностей у цифровій площині, а також сприятиме ефективному використанню цифрових технологій для забезпечення безпеки та розвитку України.

Для забезпечення правових цінностей у цифровій площині в Україні необхідно вжити таких заходів:

1) прийняти законопроєкт про захист персональних даних № 8153 від 25.10.2022 р., який пришвидшить інтеграцію України до Єдиного цифрового ринку Європейського Союзу, а також максимально наблизить положення національного законодавства до європейських вимог у сферізахисту персональних даних;

2) посилити систему захисту від кібератак на законотворчому та технічному рівнях;

3) продовжити впровадження освітніх програм з цифрової грамотності.

Процеси цифровізації українського суспільства надалі розгортаються, а інтеграція країни до Єдиного цифрового ринку визнається як логічний крок у напрямку реформ, які Україна активно впроваджує в рамках Угоди про асоціацію. За останні роки, завдяки посиленню співпраці з Європейським Союзом, Україні вдалося розширити свій доступ до онлайн-ринків та електронних послуг країн Європи, подолавши адміністративні бар'єри і розвинувши електронне врядування. Одночасно важливим завданням є забезпечення технічної спроможності та сумісності цифрових систем, поліпшення доступу громадян до високошвидкісного Інтернету, надання якісних онлайн-послуг та підвищення рівня цифрової грамотності.

Література

1. Doyle P. Major DDoS attacks increasing after invasion of Ukraine, TechTarget, 6 June 2022. URL: https://www.techtarget.com/searchsecurity/news/252521150/Major-DDoS-attacks-increasing-after-invasion-of-Ukraine (дата звернення: 22.01.2024).

2. Mingas M. Data published on Ukraine DDoS attacks, 28 March 2022, Capacity. URL: https://www.capacitymedia.com/article/29w6ghrh06rwvjbwsg35s/news/scale-of-ddos-attacks-on-ukraine-confirmed (дата звернення: 22.01.2024).

3. Майже половину кібератак СБУ виявляє у режимі «реального часу». — Укрінформ, 3 жовтня 2022 р. URL: https://www.ukrinform.ua/rubric-technology/3584942-majze-polovinu-kiberatak-sbu-viavlae-u-rezimi-realnogo-casu.html (дата звернення: 22.01.2024).

4. Атака на «Київстар» була дуже потужною. Частина віртуальної IT-інфраструктури зруйнована – гендиректор. Громадське телебачення. 12 грудня 2023. URL: https://hromadske.ua/posts/polsha-peredaye-novij-oboronnij-paket-dlya-ukrayini-zelenskij (дата звернення: 22.01.2024).

5. Microsoft, Cisco, Ericsson. У Київстарі назвали IT-гігантів, які допомагають відновити зв'язок. NV (New Voice). 13 грудня 2023. URL: https://biz.nv.ua/ukr/tech/zbiy-u-roboti-kijivstar-operator-nazvav-inozemni-kompaniji-yaki-dopomagayut-vidnoviti-zv-yazok-50376020.html (дата звернення: 22.01.2024).

6. Романенко В. Збій у "Київстарі" не вплинув на дії українських військових – Фітьо. 12 грудня 2023 р. URL: https://www.pravda.com.ua/news/2023/12/12/7432750/ (дата звернення: 22.01.2024).

7. НБУ рекомендує банкам створити резервні канали зв'язку після кібератаки на "Київстар". РБК-Україна. 14 грудня 2023 р. URL: https://www.rbc.ua/rus/news/nbu-rekomendue-bankam-stvoriti-rezervni-kanali-1702538362.html (дата звернення: 22.01.2024).