806. С. 34-39.

2. Русецький А.А., Марков В.В. Аналіз стану загроз критичній інфраструктурі в Харківській області. *Актуальні проблеми вітчизняної юриспруденції*. № 1. Том 2. 2017. С. 18-20.

3. Шевченко М. М. Методика системно-комплексного дослідження державного управління забезпеченням національної безпеки / М. М. Шевченко // *Вісник Національної академії оборони України*. 2010. № 4. С. 235–240.

УДК 321.011:341.211:342.3
DOI: 10.31733/15-03-2024/2/328-329

Олександр ТАЛДИКІН
доцент кафедри
загальноправових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

КІБЕРВІЙНА В КОНТЕКСТІ ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СУВЕРЕНІТЕТУ ДЕРЖАВИ

Питання визначення віртуального суверенітету неможливо без урахування проблем утворення принципово нової влади – влади мережі, або *нетократії,* адже віртуальна складова інформаційного суверенітету безпосередньо пов'язана з *кіберпростором*, його специфічним розташуванням поза фізичним виміром і часом. В попередніх роботах автор наголошував про актуальність дослідження особливостей інформаційної складової суверенітету держави, або інформаційного суверенітету в сучасних умовах інформаційного суспільства, коли суттєво змінюється роль держави, формується новий правовий простір наддержавного характеру, який доповнюється простором мережі, віртуальним, інформаційним, що у свою чергу обумовлює необхідність захисту від негативних зовнішніх впливів, потребу в існуванні механізму правової регуляції за допомогою норм як національного законодавства, так і норм міжнародного права [1], [2], [3].

Реальна спроможність віртуального світу бути сферою застосування *кіберсили*, яка спроможна нести загрозу державному суверенітету будь-якої держави [4; с. 6-7]. Разом з тим, проблема контролю у сфері віртуальної реальності, не означає нездатності утворювати власні ресурсні його складові та захищати свої суверенні права. Протистояння колишніх в інформаційних війнах людства, коли відбувався вплив інформації на свідомість за допомогою методів пропаганди, дезінформації та маніпулювання з метою формування необхідних для супротивника політичних поглядів сьогодні доповнилося *кібервійною*, як сучасною складовою війни інформаційної.

У 2017 році в Україні було прийнято Закон Про основні засади забезпечення *кібербезпеки* України, відповідно до якого визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі [5].

Ще у 2011 році резолюцією Ради Безпеки ООН № 1113 від 05.03.2011. кібервійна була інтерпретована, як використання комп'ютерів або цифрових засобів із боку уряду або з явним знанням чи схваленням цим урядом проти іншої держави або приватної власності в іншій державі, включаючи навмисний доступ, перехоплення даних або пошкодження цифрової та керованої цифровим методом управління інфраструктури. А також виробництво та поширення пристроїв, які можуть бути використані для підриву внутрішньої активності [6]. Безумовно, що в спрощеному розумінні кібервійна буде фактом протистояння у кіберпросторі в мережі Інтернет.

На сьогодні існує певна варіативність стосовно визначення самого поняття «кібервійна», так: більш розширену інтерпретацію кібервійни пропонують Нік Даєра-Візефорда та Світлана Матвієнко. Вони розглядають її через призму геополітичної динаміки та класових конфліктів, що спричиняють протиборство в цифрових мережах [7].

Суттєвою рисою кібервійни є *квазітериторія* її ведення. Кіберпростір відзначається тим, що для нього не існує державних кордонів. Він об'єднує географічні

доменні зони, Інтернет простору, які знаходяться у одному інформаційному середовищі [8; с. 32].

Також ознакою кібервійни є те, що вона може бути оголошена, в контексті загальної складової військового конфлікту, а також вестися формально без оголошення, тобто вона може відбуватись як: у *де-факто* мирний час, так і під час кризи збройного протистояння [9; с. 14,16].

Отже, особливості, методи, масштаби і стратегія, нападу кіберсуб'єктів, керованих РФ, на цифрову інфраструктуру України, її державні органи, стратегічні об'єкти встановлено, що ці дії є частиною масштабної «гібридної» війни проти України [10; с. 14,16].

На думку І. Воєводіна сьогодні існує певний правовий вакуум стосовно правил ведення війни у кіберпросторі, де також повинні застосуватись принципи та норми міжнародного гуманітарного права, розмежування між військовими цілями та цивільними об'єктами [11; с.47].

Разом із тим, можна відмітити специфічну особливість війни у кіберпросторі відносно складу сторін її ведення, коли вона реалізується переважно державними органами та спеціально уповноваженими особами, але не виключає участь осіб цивільних та приватних, що, у свою чергу, потребує додаткового корегування з позицій міжнародного гуманітарного права. На можливості латентного характеру кібервійни акцентує свою увагу Ю. Размєтаєва [12].

Отже, попри існування розбіжностей в інтерпретації поняття «кібервійна», сутнісний аспект самого факту цього явища дає підстави стверджувати про неабиякі ризики для віртуальної складової інформаційного суверенітету будь якої сучасної держави.

---

1. Талдикін О.В. Суверенітет держави в умовах мережевого суспільства: деякі аспекти. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 бер. 2022 р.). Дніпро 2022. Дніпроп. держ. ун-т внутр. справ С.111-112.

2. Талдикін О.В. Інформаційна складова суверенітету держави в умовах мережевого суспільства. *Права людини: методологічний, гносеологічний та онтологічний аспекти», присвячена 74-ій річниці проголошення Загальної декларації прав людини.* Матеріали Всеукраїнської науково-практичної конференції (Дніпро, 08 грудня 2022 р.); укладачі канд. юрид. наук, доцент І.А. Сердюк, викладач І.О. Смірнова. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. С.156-158.

3. Талдикін О.В. Інформаційний суверенітет та його зміст. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2023. № 2. С. 132-138

4. Камінський І.І. Концепція державного суверенітету в контексті застосування кіберсили. *Альманах міжнародного права*. Вип.16. С.3-10.

5. Про основні засади забезпечення кібербезпеки України: Закон України від 2017 р. Відомості Верховної Ради (ВВР). 2017. №45.

6. UN Security Council, Resolution 1113 (2011), 5 March 2011.

7. Нік Даєр-Візефорд, Світлана Матвієнко. Кібервійна і революція. Пер. з англ. А. Бондар. Київ. Критика. 2021. 328 с..

8. Дмитрук Я.В., Гришанович Т.О., Глинчук Л.Я., Жигаревич О. К. Кібервійна як різновид інформаційних війн. Захист кіберпростору України. *Кібербезпека: освіта, наука, техніка*. № 4 (16), 2022. С.28-34.

9. Камчатний М. В. Основні ознаки поняття «Кібервійна» в сучасному міжнародному праві. *Альманах міжнародного права*. Одеса. 2017. Вип. 15. С.12-22.

10. Бондар Г.Л. Кібервійна в Україні иа великі виклики національній безпеці: кібернапади на цифрову інфраструктуру(державні установи, об'єкти критичної інфраструктури та організації третього сектору) . *Public Administration and Regional Development*. 2022.15.02. pp. 30-67. URL : https://pard.mk.ua/index.php/journal (дата звернення: 05.03.2024).

11. Воєводін І.С. Кібервійна як сучасний метод ведення збройних конфліктив. Збірник матеріалів Міжнародної науково-практичної конференції. *Протидія кіберзагрозам та торгівлі людьми.* (29 листопада 2019 р., м. Харків) МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків. ХНУВС. 2019. С.46-48.

12. Размєтаєва Ю. С. Кібервійна: загальнотеоретичні аспекти. *Вісник Академії митної служби України*. Серія : Право. 2015. № 1. С. 12-22.