УДК 321.01
DOI https://doi.org/10.32782/app.v71.2023.11

Ю. В. Завгородня
orcid.org/0000-0003-3500-8638
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

РІЗНОВИДИ ПОЛІТИЧНИХ КОНФЛІКТІВ У КІБЕРПРОСТОРІ

Політика джерело нових інноваційних рішень, щодо узаконення процесів, котрі виникають у суспільстві. Кіберпростір поєднує у собі ряд методів комунікації, впливу та взаємодії між суб'єктами політики та активними громадянами. Разом з тим, кіберсередовище – це поєднання механізмів за допомогою яких можливо вести таку взаємодію та комунікацію, адже рівень модернізації телефонів, планшетів, комп'ютерів та ноутбуків безперервний.

Тому, виникає потреба в узагальненні існуючих даних щодо можливих видів кіберконфліктів, котрі шкодять політичним процесам, впливають на розвиток політичних процесів, зміну правлячих еліт, концентрацію влади в глобальному розумінні та регіональному аспекті. Окрім того, розуміння типології політичних конфліктів у кіберпросторі формує розуміння щодо можливих методів впливу на кіберконфлікт. Сучасна політична дійсність залежна від політичних рішень та дій, а використаний тип протидії у кіберпросторі показує методи політичного гравця, які він використовує для впливу на опонента чи громадську свідомість.

У сучасній управлінській системі світу формується цифровізація валютного обігу, яка обмежить використання готівкових валют, тому загрози кіберпростору наростатимуть, а політичні рішення не встигатимуть до сучасних подій у світі, тому формування системних знань, про кіберплощину, небезпеки та заходи попередження небезпек є активним сучасним процесом, який потребує уваги науковців різних напрямків спрямування їх сфери інтересів. Проте, саме політична сфера сприяє узаконенню цифровізованих процесів, відшуканню механізмів подолання кібернебезпек, які виникають при активній публічній діяльності. Разом з тим, теоретичне обґрунтування окремих видів політичних дій сприятиме розвитку знань, вмінь та навичок щодо протистояння небезпекам та загрозам, які набувають глобальних масштабів.

Наукові дослідження щодо розвитку кіберконфліктів, їх систематизації та типологізації досить активно розпочинають розвиватись, як в Україні так і за її межами. Так, дослідниками кіберконфліктів у вітчизняній науці варто відзначити Ю. Завгородня, Д. Дубов, В. Жадько, та інші, а питанням щодо різновидів політичних конфліктів в кіберпросторі висвітлювали І. Сопілко, В. Череватюк, М. Каветлі.

Звичайно, наявні наукові дослідження авторами в Україні та світі свідчать про актуальність та затребуваність досліджень про кіберконфлікти, як невід'ємний елемент розвитку політичних процесів та демократичних держав, тому аналіз існуючих видів загроз, які виникають від опонентів у кіберпросторі є джерелом систематизації знань та удосконаленню навичок у протидії та оцінці політичної кіберситуації.

Тому, метою даної статті є здійснення систематизованого аналізу типології кіберконфліктів у політиці, розуміння їх сутності, відмінності та небезпеки для суб'єктів політики та суспільства з глобалізаційними наслідками. Для досягнення мети поставлені такі завдання: розглянути існуючі різновиди кібернебезпек, як способів політичної протидії; систематизувати типи кіберконфліктів сучасності; провести аналіз небезпек від кожного існуючого виду; визначити позитивні та негативні кіберконфлікти; скоординувати подальший можливий розвиток дослідження типології кіберконфліктів. У зв'язку з цим, використано системний метод, аналіз та синтез, історичний метод та прогностичний метод, кібернетичний метод.

Типологізація політичних процесів у своїй специфіці демонструє розгалуженість можливих елементів взаємовідносин, їх специфіку, потребу на загострення та актуалізацію в суспільстві, або навпаки потребу не привертати увагу, як наслідок окремих подій без небезпеки

ескалації. Проте, якщо розглянути кіберконфлікти, та їх існуючі форми прояву, то переважно увага зосереджена саме на актуалізації небезпеки при чому глобального масштабу, що декламує глобалізаційну небезпеку, постійний аналіз зі сторони громадян їх втрат інформаційного та економічного характеру, дестабілізація управлінських процесів.

Проблема виникнення та розвитку, саме небезпечних видів конфліктної активності в кіберпросторі це низький рівень захищеності інформації та критичної інфраструктури, яка залежна від цифровізації та мережі Інтернет.

Тому, для держави, як важливої складової політичної системи, ключем діяльності є гарантування безпеки у кіберпросторі, усім користувачам починаючи від органів державної влади, критичної інфраструктури, суб'єктів політики, політичних партій, громадських організацій та окремих індивідів. Існуючими кіберзагрозами для держави, варто виокремити: «стан електронних інформаційних ресурсів та на можливість доступу до інформації; функціонування об'єктів критичної інфраструктури; складові частини інформаційно-комунікаційної інфраструктури; морально-психологічний стан суб'єктів кіберпростору» (Жадько, 2018, с. 247).

Тому, кіберзагрози охоплюють впливи агресора, котрим може бути держава, група та особи, на різні галузі життя держави: сферу державного управління, економічну, інфраструктуру електронних комунікацій, науково-технічну, оборонно-промисловий і транспортний комплекси, сектор безпеки та оборони України. Уявлення про негативні процеси впливу в кіберпросторі не обмежуються збиранням, зберігання, шантажуванням, публічним використанням, пошкодженням, поширенням персональних даних особи, фінансовими операціями незаконного спрямування, крадіжками і шахрайствами в інтернетпросторі, а стає глобальною проблемою та «здатна завдати значної шкоди інтересам особи, суспільства і держави» (Указ Президента, 2017).

Для загального аналізу типів протиборства суб'єктів політики у кіберпросторі варто відзначити, що усі вони реалізуються через кібератаки, тільки різниця в тому, яку форму кібератак вибрав опонент, це і буде видом політичного кіберконфлікту. Під кібератакою варто розуміти «сукупність дій противника або ворожої групи, яка намагається досягти певної негативної для об'єкта атаки цілі чи ефекту з використанням комп'ютерної техніки зокрема чи можливостей кіберпростору в цілому, найчастіше – з використанням спеціально розроблених для таких завдань засобів» (Дубов, 2016, с. 75).

Варто розуміти, що кібератаки, як процес політичний, не реалізується напряму політиком чи політичною партією. Як правило, таку діяльність здійснюють хакери, інсайдери, якщо питання застосування серйозних технічних процесів щодо впливу на комп'ютерну систему чи критичну інфраструктуру окремих країн. Разом з тим, у сучасних політиків є прес-центри, які займаються їх офіційними сторінками в інформаційному просторі, оприлюдненням візитів та зустрічей, тобто інформаційним забезпеченням політичного життя особи та навіть спростуванням кібератак у формі фейків, або навпаки розповсюдженням фейків з власних сторінок в інформаційному просторі (Завгородня, 2022, с. 67).

В сучасних кіберпроцесах присутня в політичних гравців так звана «ботоферма», за допомогою котрої відбуваються атаки на особу, яка поширює інформацію, що суперечить політиці окремої політичної сили, чи знецінює її здобутки на політичній арені. Усі ці дії направлені на політичну свідомість громадян з метою виявлення великої підтримки до політичної групи чи окремого політика. Такі, процеси розхитування політичних процесів можливі лише у демократичних країнах та свободі слова. Оскільки, до прикладу Китай, застосовує ряд санкцій, щоб обмежити будь які інформаційні протести суспільства, що політичної правлячої еліти (Zavhorodnia, 2021, с. 37).

Тому, аналізуючи специфіку розвитку політичних кіберконфліктів, варто відзначити, що М. Каветлі пропонує таку типологію кіберконфліктів «кібервандалізм (включає зміни чи знищення змісту, наприклад, веб-сайту, вимкнення чи перевантаження сервера, є найпоширенішою формою кіберконфлікту, що має значний суспільний резонанс, однак наслідки таких інцидентів обмежені в часі та відносно незначні); інтернет-злочини (діяльність переважно з метою отримання прямого фінансового зиску, може включати як злочини з комп'ютерної техніки, так і суто комп'ютерні злочини); кібершпигунство (головною жертвою найчастіше

стає корпоративний сектор. За окремими підрахунками, втрати компаній від такої діяльності становлять до 1 трлн доларів США на рік. Урядові мережі, в яких міститься конфіденційна інформація, стають жертвами атак доволі рідко, хоча останнім часом такі атаки частішають); кібертероризм (потенційно масштаби збитків від кібертеракту оцінюються надзвичайно високо, однак дотепер не було жодного реального випадку кібертероризму); кібервійна» (Жадько, 2018, с. 252-253).

В свою чергу Європейський інформаційно-дослідницький центр вважає, що основними видами загроз у кіберпросторі є: «кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави; використання Інтернету у терористичних цілях. Терористичні угрупування використовують Інтернет з метою пропаганди, збору коштів і вербування прихильників; кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом; захист персональних даних; захист електронної комерції та безпеки електронних транзакцій та платіжних інструментів; захист дітей; захист важливих об'єктів інфраструктури та інформаційних систем» (Європейський дослідницький центр, 2018).

На думку авторського колективу І. Сопілки та В. Череватюка «щодо типів кіберконфліктів, то варто звернути увагу на найпоширеніші з них, зокрема: кібервандалізм; кібершпигунство або комп'ютерне шпигунство; Інтернет – злочини; кібертероризм» (Sopilko, Cherevatiuk, 2021).

Звичайно, обрані класифікації авторами є найбільш актуальними та найбільш поширеними в мережі інформаційного впливу, проте варто звернути увагу, що політична площина охоплює більший спектр форм протистояння та впливу на суспільство, критичну інфраструктуру, суб'єктів політики.

Тому кіберконфлікти в політиці можливо класифікувати за об'єктом спрямування кібератак, а саме:

– об'єктом кібервпливу може бути громадянське суспільство, а кібератаки відбуваються у формі фейків, котрі розповсюджуються інформаційними ресурсами, соціальними мережами;

– об'єктом кібервпливу може бути критична інфраструктура, а кібератаки можуть бути у формі «знищення критичної інформаційної інфраструктури, шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони), а також інформаційно-психологічні операції та дезінформаційні вкиди з метою підриву довіри до спроможностей органів державної влади, сил безпеки та оборони, поширення панічних настроїв серед населення» (Державна служба спец. зв'язку, 2023). Ще одним важливим видом кібератаки в даному напрямку є хакерські дії в Україні, у формі розсилання шкідливого програмного забезпечення, що здійснює крадіжки облікових даних або знищує інформаційні системи.

– об'єктом кібервпливу є суб'єкт політики чи політична партія або група, а кібератаки можуть відбуватись у формі штучного банну сторінки, бот коментарів, котрі працюють на сторону опонента та виконують замовлення, в такому випадку розвивається суспільний резонанс та підрив політичної позиції політика чи політичної партії.

Окрім того, політичні кіберконфлікти можуть бути регіональні, загально-державні та глобальні. Проте, їх специфіка в тому, що навіть регіональний конфлікт може набути форм державного чи навіть глобального в силу відсутності просторових видимих меж. Така класифікація стосується відкритих країн, з демократичними формами розвитку, без обмеження глобально відомих мережевих форм комунікації.

Тому, суспільству та політичним елітам варто розуміти, що якщо в кіберпросторі буде відсутня координація дій, кіберкультура, кіберповага, то усі кіберконфлікти будуть тотально руйнівним явищем, для будь яких форм демократії. Через певний цикл розвитку людства може виникнути питання щодо повернення до системи управління жорсткого типу, без будь-яких проявів громадянських прав.

В свою чергу різновиди політичних кіберконфліктів демонструють сучасні форми протистояння, які мають шкідливі наслідки та недосконалу систему захисту, а вміння та таланти кіберфахівців координуються на протидію та економічну вигоду опонента.

Література

Жадько В.О. Гібридна війна і журналістика. *Проблеми інформаційної безпеки : навчальний посібник.* Київ. Вид-во НПУ імені М.П. Драгоманова, 2018. 356 с.

«Доктрина національної безпеки України» Указ Президента України № 47/2017 від 25 лютого 2017 року. URL: http://www. president.gov.ua/documents/472017-21374

Дубов Д. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України. *Нац. ін-т стратегічних досліджень.* Київ, 2016. 434 с.

Завгородня Ю.В. Фейки як сучасна форма політичного протиборства у кіберпросторі. *Регіональні студії.* № 28. 2022. Видавничий дім «Гельветика». С. 67-71

Yuliia Zavhorodnia, Features of protection of China's national interests within cybernetic space. *European Political and Law Discourse*, 2021, Volume 8, Issue 6. p.37-42

Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Європейський інформаційно-дослідний центр. 2023. URL: file:///C:/Users/38096/Desktop/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf

Iryna Sopilko, Viktoriya Cherevatiuk Types of cyber conflicts and the role of the state in their prevention and solution. *Journal of Law and Social Sciences «Legal, Economic Science and Praxis»*. 2021. URL: https://lesp.hu/wp-content/uploads/2022/01/2021-No2-p20-26.pdf

Готовність України до нових викликів. Кібербезпека і зв'язок. *Державна служба спеціального зв'язку та захисту інформації України.* 2023. URL: https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbezpeka-i-zv-yazok

References

Zhadko V.O. (2018) Hibrydna viina i zhurnalistyka. [Hybrid war and journalism] Problemy informatsiinoi bezpeky : navchalnyi posibnyk. Kyiv : Vyd-vo NPU imeni M.P. Drahomanova, 356 s. [in Ukrainian]

Doktryna natsionalnoi bezpeky Ukrainy. [The doctrine of national security of Ukraine] (2017) Ukaz Prezydenta Ukrainy № 47/2017 vid 25 liutoho 2017 roku URL: http://www. president.gov.ua/documents/472017-21374. [in Ukrainian]

Dubov D. (2016) Heopolitychne supernytstvo u kiberprostori yak chynnyk vplyvu na natsionalnu bezpeku Ukrainy [Geopolitical rivalry in cyberspace as a factor influencing the national security of Ukraine. Kyiv. 434 s. [in Ukrainian]

Zavhorodnia Yu.V. (2022) Feiky yak suchasna forma politychnoho protyborstva u kiberprostori. [Fakes as a modern form of political struggle in cyberspace] Rehionalni studii. № 28. Vydavnychyi dim «Helvetyka». S. 67-71. [in Ukrainian]

Yuliia Zavhorodnia, (2021) Features of protection of China's national interests within cybernetic space. European Political and Law Discourse, Volume 8, Issue 6. r. 37-42 [in English]

Zakonodavstvo ta stratehii u sferi kiberbezpeky krain Yevropeiskoho Soiuzu, SShA, Kanady ta inshykh. [Legislation and strategies in the field of cyber security of the countries of the European Union, USA, Canada and others.] (2023) Yevropeiskyi informatsiino-doslidnyi tsentr. URL: file:///C:/Users/38096/Desktop/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf. [in Ukrainian]

Iryna Sopilko, Viktoriya Cherevatiuk (2021) Types of cyber conflicts and the role of the state in their prevention and solution. Journal of Law and Social Sciences «Legal, Economic Science and Praxis». URL: https://lesp.hu/wp-content/uploads/2022/01/2021-No2-p20-26.pdf [in English]

Hotovnist Ukrainy do novykh vyklykiv. [Readiness of Ukraine for new challenges.] (2023) Kiberbezpeka i zviazok. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. URL: https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbezpeka-i-zv-yazok. [in Ukrainian]

Анотація

***Завгородня Ю. В.* Різновиди політичних конфліктів в кіберпросторі. –** Стаття.

Кіберпростір є глобальним середовищем, що акумулює у собі різні процеси, події, що впливають на окремі суспільства чи загалом увесь світ. Політичні конфлікти в кіберпросторі переважно виконують негативну функцію, оскільки завуальованість суб'єкта подання інформації чи впливу на кіберсистеми допомагає уникати осуду та відповідальності в правових рамках. Кібербезпека є сучасним важливим елементом для розвитку та стабільної діяльності політичної системи, оскільки допомагає створювати кіберзахист систем управління та критичної інфраструктури.

Дестабілізація ресурсів органів управління, які прив'язанні до кібермереж, є шляхом до деструктивного впливу на політичних суб'єктів, їх авторитет у суспільстві та в світі загалом. Тому, деталізація уваги окремим формам впливу, котрі можливі у кіберпросторі, досить актуальна, оскільки демонструє сучасні різновиди кіберзагроз під час конфліктного протистояння політичних лідерів.

В науковому обігу присутні характеристики окремих видів кіберзагроз, які уже отримали свою популярність за період цифровізації людства, характеристика таких загроз містить свою специфіку, котра залежить від політичного режиму, від рівня цифровізації суспільства, а відповідно і рівня можливих кібератак.

Типологія кіберконфліктів, які присутні у політичних процесах, сприяє розвитку наукових досліджень трансформаційних процесів щодо цифровізації управлінської діяльності, їх сучасному удосконаленню та спрямованості. У роботі розглянуто різноманітні узагальнення сучасних небезпек у кіберпросторі та запропоновано власну класифікацію для кіберконфліктів у кіберпросторі, які виникають з метою впливу на політичні процеси.

В залежності від того, який напрямок протиборства між сторонами політичного протистояння, то вид конфлікту буде різнитися, але усі типи протистояння у кіберпросторі відбуваються у формі кібератак, лише мета таких атак, об'єкт атак та наслідки будуть різними.

Ключові слова: кібертероризм, кібервандалізм, кібершпигунство, кіберконфлікти, інтернет-злочини, кібервійна.

Summary

Zavhorodnya Yu. V. **Types of political conflicts in cyberspace. –** Article.

Cyberspace is a global environment that accumulates various processes and events affecting individual societies or the whole world in general. Political conflicts in cyberspace mostly perform a negative function, since the veiling of the subject of information submission or influence on cyber systems helps to avoid condemnation and responsibility in the legal framework. Cyber security is a modern important element for the development and stable operation of the political system, as it helps to create cyber protection of management systems and critical infrastructure.

Destabilization of the resources of governing bodies, which are tied to cyber networks, is a path to destructive influence on political subjects, their authority in society and the world in general. Therefore, detailing attention to individual forms of influence that are possible in cyberspace is quite relevant, as it demonstrates modern types of cyber threats during the conflict between political leaders.

In scientific circulation there are characteristics of certain types of cyberthreats that have already gained popularity during the period of digitalization of humanity, the characteristics of such threats contain their own specificity, which depends on the political regime, on the level of digitalization of society, and, accordingly, on the level of possible cyberattacks.

The typology of cyber-conflicts, which are present in political processes, contributes to the development of scientific studies of transformational processes regarding the digitalization of management activities, their modern improvement and orientation. The work examines various generalizations of modern dangers in cyberspace and proposes its own classification for cyberconflicts in cyberspace that arise with the aim of influencing political processes.

Depending on the direction of the confrontation between the parties of the political confrontation, the type of conflict will differ, but all types of confrontation in cyberspace take place in the form of cyber attacks, only the purpose of such attacks, the object of the attacks and the consequences will be different.

Key words: cyber terrorism, cyber vandalism, cyber espionage, cyber conflicts, internet crimes, cyber war.