

УДК 32.019.5

DOI <https://doi.org/10.32837/apfs.v0i35.1100>**Ю. В. Завгородня**ORCID ID: <https://orcid.org/0000-0003-3500-8638>

кандидат політичних наук, доцент,

доцент кафедри політичних теорій

Національного університету «Одеська юридична академія»

## КІБЕРКОНФЛІКТИ ЯК СУЧАСНА ЗАГРОЗА ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА: ПОЛІТИЧНИЙ АСПЕКТ

Сучасний світ проходить процес трансформації управлінського порядку, однією з особливостей такого процесу є глобалізаційні процеси цифровізації суспільства. Оскільки, процес дуже швидко розвивається, то система унормування даних форм взаємодії не є ефективною, або взагалі не працює. Окремі політико-правові системи намагаються локально створювати умови захисту та безпеки інформаційного простору, однак усі вони не можуть стримати процеси кіберпротистояння.

Усі процеси політичної боротьби в кіберпросторі є невід'ємними елементами сучасних форм взаємодії політичних лідерів. Можливості, які створюють сучасні умови для взаємодії за допомогою гаджетів, телефонів, ноутбуків стирають просторові межі, зменшують час на обробку інформації, збільшують можливості швидкого публічного реагування на інформаційні атаки, фейки, провокації політичними лідерами.

Звичайно, для політичних рішень і політичної взаємодії у різних напрямках управління державними процесами важливий «ефект зустрічі», який сприяє до лібералізації взаємодії сторін. Однак, в умовах корона вірусного захворювання та небезпеки військових атак, які створюють загрозу для життя та здоров'я політичних лідерів, більшість політичних процесів внутрішньої взаємодії та зовнішньої взаємодії щодо політичних рішень, які стосуються української держави, можливо вирішувати в умовах онлайн спілкування. Проте, публічні зустрічі на безпечній території це знак поваги та сильної підтримки серед політичних гравців глобального чи регіонального рівня.

В рамках сучасних загальних форм взаємодії у кіберпросторі політичні процеси можна розділити на окремі групи. Так, перша група інформаційного протистояння це потужні держави світового рівня, такі як: США, КНР. Наступна група це так звані регіональні лідери: ЄС у Європі, росія в Євразії (до повномасштабного вторгнення), Бразилія в Латинській Америці, Індія в Азії, ПАР в Африці. Третя група характеризується реалізацією власних інтересів на локальному рівні без застосування широких підривних форм дії. Сюди входять країни, які знаходяться на етапі становлення

політичного та правового розвитку. Та, остання група це терористичні та екстремістські організації, які користуються кібернетичним простором для проведення підривної діяльності проти інших країн та міжнародних організацій, в т. ч. провідних держав світу.

Враховуючи особливості розвитку політичних процесів, публічних тверджень окремих політичних лідерів, публічних засуджень політичних лідерів, які не засуджують війну, усі вони є інцидентами, які виникають в інформаційній площині та швидко розповсюджуються за допомогою цифровізації суспільства та публічних політичних процесів.

Питання щодо цифровізації та кіберконфліктів у політичних процесах розглядалися в різних напрямках наукового дослідження, бо більшість авторів приділяли увагу цифровізації в загальному сприйнятті (Соснін О., Стігліц Д., Ван Арка Б., Вишневський О., Гудзь О., Ліклайдер Дж., Ляшенко В.), а інші оглядали політичні процеси у сучасному трансформованому кіберсередовищі, як сфері розвитку політичних конфліктів (Завгородня Ю., Кройтор А., Яковлев Д., Алексенцева-Тімченко К.). Однак, сучасна система взаємозв'язків у суспільстві демонструє взаємозалежність процесів, які створюють нові форми та шляхи до співпраці у політичній площині.

Тому, основною метою дослідження є аналіз кіберконфліктів, які досить активно розвиваються, мають армію публічних спостерігачів та створюють публічні процеси доступними для суспільного освідомлення при умові цифровізації населення. З метою досягнення поставленої мети виконано такі завдання, як: характеристика термінологічних понять «цифровізації» та «кіберконфліктів», які формують основу дослідження; виявлення проблемних аспектів цифровізації у сучасних політико-правових процесах та розвиток конфліктної активності; узагальнення подальших напрямків наукового аналізу, щодо ролі КНР та США; узагальнення впливу кіберконфліктів у політичному процесі сучасності.

Для ефективного виконання завдань використано методи аналізу і синтезу, порівняльний метод, метод наукового дослідження з викорис-

танням феноменів, які уже проаналізовано, проведено їх систематизацію, коригування нових та отриманих знань раніше та ін.

Так, на думку О. Сосніна «світ цифрових технологій, в який ми входимо, – це не тільки новий логічний етап розвитку технологічної сфери людства, а й усієї соціально-політичної реальності. Поки щодо неї не існує загальноприйнятих і гармонізованих визначень та правових дефініцій, однак цифрові технології вже стрімко захоплюють плацдарми для наступу» [1].

В свою чергу під цифровізацією О. Соснін розуміє «сучасний тренд розвитку і послідовного покращення всіх бізнес-процесів економіки та пов'язаних з нею соціальних сфер, заснований на збільшенні швидкості взаємного обміну, доступності й захищеності інформації» [1].

Таким чином, за допомогою цифровізації відбувається удосконалення саме політичних процесів, прийняття політичних рішень, здійснення політичної взаємодії та спрощення процесів комунікації серед політиків. Усі ці процеси по своєму сутнісному наповненні можуть супроводжуватись кіберконфліктами, які створюють деструктивні умови для модернізації політичної системи в середині країни та у світі загалом.

Цифровізація у політичній площині активно розпочалась з приходом до влади політичної партії «Слуга народу» та її лідера Володимира Зеленського, які в силу своєї недосвідченості у старих політичних процесах розпочали будувати сучасну цифровізовану політичну систему за допомогою гасла «країна в смартфоні» та застосування «Дія», який в умовах військового часу став корисною розробкою для громадян, які хотіли перетнути кордон, але не мали при собі паперових документів. Недосвідченість це не ознака поганої якості в політичному процесі країни, яка розвивається, це шлях до нових можливостей, якщо команда має на меті пріоритети держави та суспільства, а не власну вигоду. Саме такі зручні опції запровадженого застосування є зразком політики держави щодо створення умов спрощених процедур для реалізації прав громадян у найскладніші часи.

Сучасна політика держави зосереджена на спрощення бюрократичної системи, економію часу для будь-яких реєстраційних процесів, ефективного користування соціальними гарантіями. Однак, окрім позитивних аспектів існує ряд загроз щодо кібератак для оприлюднення персональних даних, можливості їх використання та видалення з баз даних. Саме такі загрози стоять перед сучасним сектором інформаційної політики з метою захисту та збереження персональної інформації.

Яскравим прикладом незручностей у сучасній Україні є зникнення у застосування «Дія» водійських прав та свідоцтва про реєстрацію транспортного засобу майже на два тижні після того, як розпочалось

повномасштабне вторгнення на територію України військ РФ. Тому, з метою захисту наших даних інформація про такі види документів були відсутні, а отже збережені від кібератак. Бо сучасна форма війни це не лише військо з сучасною військовою технікою, але і кібервійсько, яке намагається стерти будь-які данні щодо державного статусу та суверенітету в інформаційній площині.

Кіберконфлікти у політичній площині – це ряд заходів, які націлені впливати на інформаційні ресурси, офіційні сайти, банки та інші важливі для держави інформаційні портали, які ідентифікують її, як незалежну правову систему з окремою територією, населенням та органами управління [2; с. 145].

В сучасному світі роль кіберконфліктів зростає, бо інформація стає зброєю, яка може стати причиною політичної смерті для окремих політичних лідерів чи політичних сил. В Україні від моменту становлення незалежності в такому стані без можливостей відновлення, реанімації та перерформатування знаходяться дві політичні сили такі, як: комуністична партія, опозиційна платформа за життя. «За таких умов під суттєвою загрозою опиняються об'єкти критично важливих інфраструктур держави (енергетика, транспорт тощо), оскільки інформація, якою вони вільно користуються в повсякденному житті, у цифровому вигляді несе в собі всі ознаки зброї – як із точки зору психологічного, мовного, так і технічного або технологічного впливу» [1].

Розвиток кіберконфліктів відбувається у зв'язку виявленням політичного інциденту, який не має механізму правового продовження в інформаційній площині. Дуже важко забезпечувати достовірність інформації, в умовах відсутності санкційної форми захисту швидкого реагування в праві. В свою чергу виникає необхідність у цифровій трансформації, як діяльності направленої на пошук ефективних механізмів захисту інформаційного середовища загалом та окремих видів інформації частково.

На думку Девіда Террара «цифрова трансформація – це процес переходу до нових способів роботи і мислення з використанням цифрових, соціальних, мобільних і нових технологій та включає зміну мислення керівництва, заохочення інновацій і нових бізнес-моделей, оцифровку активів і ширше використання технологій для поліпшення досвіду співробітників, клієнтів, постачальників, партнерів і зацікавлених сторони» [3].

У зв'язку зі змінами в цифровізації суспільства можемо говорити про цифрову трансформацію політики, бо власне використання цифрових технологій демонструє удосконалення політичних процесів відповідно до умов сучасного світу, а це швидке реагування політичної системи на виклики і загрози, які виникають уже у сучасному політичному просторі.

Одними із найбільш прогресивних учасників глобального рівня цифровізації можна вважати США та КНР, які демонструють могутність власних країн у формуванні цифрового суверенітету на глобальному рівні.

У своїх методах щодо цифровізації суспільства та регулювання відносин в межах інформаційного простору вищезазначені країни діють по різному, однак обидві мають успіх у світовому впливі на інформаційні процеси. «Саме шляхом жорсткого контролю медійних ресурсів та інтернет ресурсів слідує Китайська Народна Республіка. Ця країна має свої індивідуальні особливості політичної системи та взаємодії з громадянами держави. Однак, це не заважає державі разом з її громадянами прогресувати та збільшувати економічний ріст країни. За формою правління Китай є республікою, в ній функціонує однопартійна система, єдиною партією цієї країни є Комуністична партія, по формі державного устрою Китай є унітарною державою, що показує ієрархію органів управління з чіткою системою розподілу повноважень» [5, с. 38].

«В силу ряду негативних аспектів захист національних інтересів Китаю у кіберпросторі продовжує удосконалюватись та індивідуалізуватись під власні інтереси та пріоритети. Роль системи органів управління у впливі на кіберпростір висока та чітко орієнтована. Сформовано державні органи, які відповідають за дану сферу. А найголовніше, це суспільне мовчазне визнання санкційної системи кібернетичного управління в державі, що не потребує міжнародної критики та осуду, адже міжнародна спільнота акцентує власний пріоритет це інтереси, права та свободи людини, якщо громадяни Китаю в більшій мірі позитивно сприймають систему управління, вирішення проблем та кіберконфліктів, тому можна стверджувати, що інтереси та права людини у Китаї повністю влаштовують її громадян» [5, с. 40].

У свою чергу в США «у 2015 році затверджено «Стратегічний план 2015–2018 рр.», у якому визначаються цілі щодо забезпечення громадських інтересів, зокрема прав споживачів, безпека та доступ до широкопasmового зв'язку. Також, у державному управлінні телекомунікаційним сектором у США велике значення надається стимулюванню конкуренції в телекомунікаційному середовищі. У 2009 році запроваджено правила нейтральності мережі, відповідно до яких тарифи зв'язку регулюються ринком, а питання щодо встановлення та моніторингу стандартів якості послуг регулюються державою» [6, с. 263].

Значимість цифровізації обґрунтовується щорічним збільшенням ВВП країн приблизно на 20%, однак у країнах з високим рівнем розвитку такий показник становить біля 7%. Так, до прикладу у 2019 році частка цифрової економіки у ВВП США становила від 6,9 до 21,6%, в свою

чергу у ВВП Китаю – від 6 до 30%. В порівнянні з прогресією розвитку від 2010 року до 2017 року лідером у збільшенні частки доданої вартості в цьому напрямку залишалася Тайвань (провінція Китаю) – 2,0%. Також, швидкі темпи додають країни Європи – Кіпр, Сербія, Ісландія, Польща, Ірландія, Німеччина [6, с. 262].

Отже, можемо прослідкувати різні методи цифровізації у суспільствах США та КНР, різні політичні режими, однак приблизно однаковий діапазон розвитку цифровізації, як сучасного процесу розвитку політико-правової площини людства.

Звертаючи увагу на ефективні зміни щодо цифровізації прогресивних країн світу, варто звернути увагу на запобігання кіберконфліктів, які є однією з ключових загроз щодо трансформації в політичній площі для окремих політичних систем. Для вирішення даних питань варто комплексно формувати систему попереджувальних та санкційних заходів на рівні державного управління.

Вдалою є думка авторського колективу Кройтора А., Яковлева Д., Алексенцева-Тімченко К. щодо необхідності враховувати розповсюдженість інформаційних технологій та активне використання їх серед юних громадян із мережі інтернет [7]. Адже, під час характеристики цифровізації варто враховувати і те, що приймати участь в окремих видах політичних процесів в інтернет просторі можуть люди, які ще не досягли повноліття та не можуть бути повноцінними учасниками політичного процесу.

Разом з тим, потребує уваги позитивний аспект кіберконфліктів, як джерела до виокремлення публічних швидких реакцій суспільства, підвищення рівня критичної свідомості щодо політичних процесів, вміння аналізувати та формувати індивідуальне бачення щодо політичної ситуації. Саме кіберпростір є джерелом політичної поінформованості та зниження рівня байдужих до політики людей.

Також, у стресових конфліктних процесах свідомість суспільства активізується з метою згуртованої співпраці та формування ключової мети, яка в процесі реалізації спонукає до ефективного розвитку політичної системи. Конфлікт є джерелом змін, наскільки влада та суспільство вдало використовують ці зміни, настільки завершення конфлікту буде позитивними чи негативними в процесі державно-політичного розвитку.

Небезпека кіберконфліктів у сучасному політичному процесі уповільнює розвиток цифровізації громадян, межі територіальної прив'язки конфлікту стираються. Тому, людство потребує конкретизації форм впливу на взаємовідносини в мережі вільного інформаційного доступу. Разом з тим, потрібно створення спільних звичаїв, які моделюють поведінку користувачів кіберпростору. Політичний простір набуває глобальних масштабів та потребує координації розвитку людей у взаємодії щодо використання інформаційних ресурсів.

## Література

1. Соснін О. Цифровізація як етап становлення цифрового суспільства знань. 2021. URL: <https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-etap-stanovlennya-tsyfrovogo-suspilstva-znan/>
2. Завгородня Ю. В. Кіберконфлікти, як елемент політичних технологій в інформаційному просторі. *Актуальні проблеми філософії та соціології*. 2021. № 32. С. 144–148.
3. What is Digital Transformation? *Theagileelephant.com*. website. URL: <http://www.theagileelephant.com/what-is-digital-transformation> (the date of application: 27.03.2022)
4. Розпорядження КМУ «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації» від 03.03.2021р. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#top> (дата звернення: 26.04.2022)
5. Yuliia Zavorodnia, Features of protection of China's National interests within cybernetic space. *European Political and Law Discourse*. 2021. Volume 8. Issue 6. P. 37–42.
6. Пустоваров А. І. Закордонний досвід цифрової трансформації управління розвитком національної економіки. *Причорноморські економічні студії*. 2020. Вип. 51. С. 261–267.
7. Кройтор А. В., Яковлев Д. В., Алексенцева-Тімченко К. С. «Апостоли» індоктринації: ідеологічні особливості репрезентації релігійного вибору у системі середньої освіти (на основі аналізу інтерв'ю експертів). *Ідеологія і політика*. 2019. № 2(13). URL: [https://www.ideopol.org/wp-content/uploads/2019/12/\\_\\_\\_\\_UKR.%201.7.%20Kroit%20et%20al.%20%20FIN.pdf](https://www.ideopol.org/wp-content/uploads/2019/12/____UKR.%201.7.%20Kroit%20et%20al.%20%20FIN.pdf) (дата звернення: 28.04.2022).

## Анотація

**Завгородня Ю. В. Кіберконфлікти як сучасна загроза цифровізації суспільства: політичний аспект.** – Стаття.

У світі відбуваються геополітичні зміни, які здійснюють безпосередній вплив на кіберпростір, оскільки в сучасному сприйнятті, – це виокремлене середовище протидіє між різними суб'єктами політики на міжнародному та регіональному рівнях. Русійним джерелом змін є конфлікти, а в розвитку цифровізації джерелом змін є кіберконфлікти, як площадка активних бойових інформаційних дій. Яскравим тому прикладом є зміни, які кожен день відбуваються через війну росії з Україною, однак сучасні позиції активності сторін змінюються практично кожного дня і важливо роль в цьому протидіє відіграють саме інформаційні мережі з яких сторони отримують велику кількість інформації про стан політико-військової ситуації.

Тому, питання щодо розвитку цифровізації суспільства, його значимості в умовах військової агресії, формування механізмів стримування та протидіє в інформаційній площині є важливими питаннями, які потребують деталізації та аналізу в сучасній російсько-українській війні та й загалом у світовому політико-правовому порядку, який на сьогоднішній день порушено.

Оскільки, умови розвитку кіберконфліктів інші, ніж звичайних політичних конфліктів, оскільки сто-

ронами протидіє можуть виступати усі учасники міжнародної взаємодії, які мають можливість відстоювати інтереси груп, які вони представляють, а відповідно мають технологічні можливості для кібернетичного впливу, які допоможуть реалізувати кібернетичну атаку по методам кібернетичного протидіє (війни).

Уже в сучасному науковому обігу в багатополарній системі устрою світу можливо виділити декілька груп, які активно проводять такого роду атаки та контратаки. Основна мета, таких глобальних форм впливу, це усвідомлення могутності інформаційного впливу у світі в умовах цифровізації людства.

Тому, питання цифровізації суспільства в умовах загострення кіберконфліктів досить актуальний напрям наукового дослідження в сучасних політико-правових процесах. Бо усі процеси протидіє виходять за адміністративні межі окремих країн чи регіонів, важко ідентифікуються з конкретними суб'єктами, які вчинили акт інформаційної боротьби.

**Ключові слова:** кіберпростір, кіберконфлікти, цифровізація суспільства, кібератака, громадянське суспільство, політичні суб'єкти.

## Summary

**Zavorodnya Yu. V. Cyberconflicts as a modern threat to the digitalization of society: political aspect.** – Article.

The world is experiencing geopolitical changes that have a direct impact on cyberspace, because in modern perception, it is a separate environment of confrontation between different policy actors at the international and regional levels. The driving force of change is conflict, and in the development of digitalization, the source of change is cyberconflict as a platform for active combat information operations. A striking example of this is the changes that occur every day due to Russia's war with Ukraine, but the current positions of the parties change almost every day and important role in this confrontation is played by information networks from which the parties receive a lot of information about the political and military situation.

Therefore, the issues of digitalization of society, its importance in the face of military aggression, the formation of mechanisms of deterrence and counterbalance in the information sphere are important issues that need to be detailed and analyzed in the current Russian-Ukrainian war and in general in the world political and legal order. today is broken.

Because the conditions for the development of cyberconflicts are different from ordinary political conflicts, as the parties to the conflict can be all participants in international cooperation who have the opportunity to defend the interests of groups they represent, and therefore have technological capabilities for cyber influence to help implement cyber attacks confrontation (war).

Already in modern scientific circulation in the multipolar system of world order it is possible to identify several groups that are actively conducting such attacks and counterattacks. The main goal of such global forms of influence is to realize the power of information influence in the world in the context of digitalization of mankind.

Therefore, the issue of digitalization of society in the context of exacerbation of cyber conflicts is a very important area of research in modern political and legal processes. Because all the processes of confrontation go beyond the administrative boundaries of individual

countries or regions, it is difficult to identify with specific actors who have committed an act of information struggle.

*Key words:* cyberspace, cyber-conflicts, digitalization of society, cyber-attacks, civil society, political actors.