УДК 32.341.1.342.1
DOI https://doi.org/10.32782/apfs.v048.2024.29

***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»*

## МОЖЛИВОСТІ ПОЛІТИКИ КІБЕРЗАХИСТУ В ЗОВНІШНІХ ТА ВНУТРІШНІХ ПРОЦЕСАХ

Державна політика щодо кіберзахисту стає важливою складовою системи державної безпеки та міжнародного порядку. Проведення міжнародних конференцій, формування наукового підґрунтя щодо проблеми безпеки в кіберпросторі набуває масштабного значення, адже кіберпротиріччя все частіше загострюються та не врегульовуються. Використання кіберпротиріч слугує за часту маніпулятивним чинником у політичних процесах, методом впливу на сторону взаємовідносин. Окрім того, кіберзахист є необхідною умовою під час демократичних процесів у суспільстві (виборах, референдумах, мирних зібраннях тощо).

Тому, виникає необхідність у формуванні цілісної систематизованої діяльності політичних діячів у формуванні зовнішнього та внутрішнього кіберзахисту, як взаємопов'язаних процесів. Оскільки, кіберпростір не має територіальних меж у розповсюджені інформації, тому формування якісного захисту мереж в кіберпросторі потребує зовнішнього політичного регулювання.

Актуальність обраного напрямку дослідження потребує вирішення важливих практичних та наукових завдань, а саме: теоретичне розуміння поняття «політика кіберзахисту», відмінність від «політики кібербезпеки»; визначення актуальних проблем у кіберпросторі для громадян; аналіз політики кіберззахисту в Україні; оцінка ролі інституційної консолідації суб'єктів кіберзахисту та кібербезпеки; перспективи політики кіберзахисту України та її вплив на внутрішні та зовнішні процеси.

Дослідження питань визначення вектору діяльності суб'єктів політики у реалізації безпеки кіберпростору створить можливості використання кібернетичних мереж усіх бажаючих в рівних можливостях. Так, як усі процеси у спілкуванні повинні містити межі допустимих можливостей, так і в кібернетичних діях усіх бажаючих мають бути такі допустимі межі.

Питання політики кібербезпеки активно займаються українські науковці, а саме: Горун О. [2], Бакалінська О. [3], Бакалинський О. [3], Веселова Л. [4], що активно охарактеризивують правові та політичні аспекти ролі кібербезпеки в період з 2014 року по 2021 рік, окрім цього питаннями кіберконфліктів у політичних процесах займається Кормич Л. [1], Завгородня Ю. [1], потребує продовження аналізу питання в аспекті врегулювання таких форм протиріччя, або попередження за допомогою політики кіберзахисту у сучасних геополітичних процесах.

Враховуючи проблематику та актуальність обраного напрямку дослідження, визначені завдання та існуючі наукові дослідження в напрямку кіберпросторових процесів, виникає необхідність формування *мети дослідження*, яка постає у систематизації уявлень про політику кіберзахисту, перспективи розвитку інституціоналізації в зовнішніх та внутрішніх політико-кібернетичних процесах.

*Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.*

Важливою складовою для розуміння політики кіберзахисту та її ролі у сучасних геополітичних процесах є формування теоретичної основи щодо сутності політики кіберзахисту та взаємозалежності з кібербезпеки.

Оскільки «у сучасних формах політичної взаємодії відбувається модифікація у нову політичну площину, а саме у кіберпростір. Специфікація даної «території» взаємодії у тому, що вона не містить будь-яких просторових меж, а учасники політичного процесу у своїй формі активності можуть виходити за межі регіонального чи державного впливу на суспільство» [1].

Відповідно до трактування у Словнику військових термінів та скорочень «кібербезпека» – це «захищеність життєво-важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [6, с. 14].

Тобто, аналізуючи дане тлумачення поняття «кібербезпека» це констатація певного стану справ щодо безпечності кіберсередовища, потенційне виявлення загроз, які можливі у цифровій комунікації, їх нейтралізація та створення уза-

гальнених уявлень про систему захисту кіберпростору, потреби в модернізації захисту.

Проте, щоб оцінювати безпеку в кіберпросторі потрібно розуміти, які заходи щодо захисту вживаються державою, міжнародною спільнотою, підприємствами, персональними користувачами по захисту персональних гаджетів.

В свою чергу, Словник військових термінів та скорочень дає роз'яснення «кіберзахисту», як: «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [6, с. 14].

Тобто «кіберзахист» це процесуальна складова до реалізації сталої «кібербезпеки». Тому, дані терміни взаємопов'язані, взаємозалежні та спрямовані на реалізацію стабільних шляхів комунікації в кіберпросторі. Оскільки, під час аналізу кіберконфліктів, як негативної складової в політичних процесах, прослідковується, що вони підривають кібербезпеку політичної системи та потребують модернізації кіберзахисту.

В Законі України «Про основні засади забезпечення кібербезпеки України» [7], відзначено, що «цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки».

Тому, аналізуючи політику щодо процесів в кіберпросторі доцільно оцінювати не лише політику кібербезпеки, як роблять у переважній більшості автори, а саме акцентувати увагу на захисті, як комплексі заходів, які або якісно сприяють кібербезпеці, або містять прогалини в кібербезпеці. Формування комплексу заходів захисту у кіберпросторі, а не лише проголошення принципів та засад кіберентичної комунікації, скоординують до сучасних форм кіберзахисту, пошуки протидії з кіберзагрозами та стабілізації заходів щодо стабільності в кіберпросторі.

На думку, Л. Яковлевої «комунікативна складова частина легітимності публічної влади має три виміри: 1) діяльність влади в комунікативному просторі (інформаційна політика, активність прес-служб посадових осіб та інформаційних департаментів органів влади); 2) олігархічна модель мас-медіа, яка сформувалась у вітчизняному комунікативному просторі; 3) рівень впровадження електронних послуг у взаємодії між владою та громадянами (від створення органами влади та місцевого самоврядування сайтів та сторінок у соціальних мережах до повноцінної комунікації в межах електронного уряду та електронної демократії із залученням громадян до вироблення та прийняття рішень)» [11, с. 104].

В свою чергу, О. Бакалінська та О. Бакалинський зосередивши свою увагу у дослідженні на нормативно-правовій складовій кібернетичної комунікації відзначили, що «сьогодні законодавче регулювання кіберзахисту в Україні перебуває на початку свого формування, проте найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту – пройдено» [3, с. 107].

В сучасних реаліях військового протистояння можемо відзначити, що за період повномасштабного вторгнення українськими фахівцями напрацьовано ряд форм для кіберзахисту, виявлено прогалин в кіберзахисті відшукання модернізованих форм захисту та стабілізації кіберпросторових відносин. Що створює можливості для формування сучасної зовнішньої та внутрішньої політики забезпечення кіберзахисту.

Щодо зовнішньої політики, то варто підтримати думку З. Свердлик, яка відзначає, що «важливим є питання подальшого поглиблення міжнародного співробітництва у питаннях кіберзахисту та кібербезпеки, створення спільних міждержавних платформ для обміну інформацією. Варто, на нашу думку, залучати до державних програм із розробки стратегій, рекомендацій кібернетичної безпеки також і спеціалістів із приватних організацій або фірм, адже такий крок консолідує суспільство та сприятиме виробленню максимально ефективного продукту» [5].

Використання можливостей, щодо реалізації наявного досвіду в українському суспільстві з погляду на різні аспекти прояву кіберінцедентів презентують Україну, як практичного фахівця у формах стабілізаційних заходів від кіберзагроз, які пройшли існуючі форми захисту. Проблеми, які виникають постійно в кіберпросторі можуть мати миттєвий прояв без можливості до реакції, а наслідки масштабні.

На конференції «IT Meets Tech: Кібербезпека», організованій Львівським IT Кластером за підтримки Державної служби спеціального зв'язку та захисту інформації України та Проєкту USAID «Кібербезпека критично важливої інфраструктури України» [8] визначено основні виклики колегіально для держави, підприємств, ЗМІ та громадян в питаннях зіберзагроз та кіберзахисту. В умовах невпинного розвитку кіберпросторових можливостей систему захисту кіберпростору постійно потрібно удосконалівати з появою новітніх форм кібератак та кіберінцедентів. Тому, мож-

ливо виділити основні виклики, які відносяться до усіх існуючих інститутів політичної системи держави.

До основних викликів інститутів політичної системи, за результатами конференції можна віднести:

– підвищена потреба у загальній кіберстійкості у державі – це те, що має об'єднувати всіх;

– реагування бізнесу на потенційні проблеми окремих представників бізнесу, державну комунікацію бізнесу та реакція на загрози через окремі випадки;

– загрози становить не лише власна недосконала система захисту інформаційних систем, а й недоліки у захищеності партнерів (наприклад успішна атака на енергорозподільчу систему, систему водопостачання чи великий банк);

– підготовка достатньої кількості висококваліфікованих фахівців (для усіх політичних інститутів держави);

– постійне здійснення удосконалення систем захисту кіберпростору;

– системне навчання співробітників та службовців (кібергігієна, ефективна реакція на кіберситуацію) [8].

Враховуючи досвід викликів, які уже сформували певні запити у суспільстві та органах управління щодо політики кіберзахисту, виникає потреба в консолідації суб'єктів кіберзахисту та кібербезпеки в державі та світі. Координація спільних зусиль сприятиме підвищенню рівня безпеки в кіберпросторі, а відповідно зниження напруженості щодо ескалації кіберконфліктів. Стабілізації комунікації в кіберпросторі сприятимуть глобальні процеси політичної ефективної діяльності щодо бажання реалізувати захист інформації, добросовісну конкуренцію, захист персональних даних, банківських рахунків, приватних переписок та інших процесів пов'язаних з цифровізованою активністю людей.

Разом з тим, суб'єкти політики у різних статусах своєї діяльності мають нести одну культуру кіберпросторової взаємодії, моделі та механізми публічного спілкування в кіберпросторі, виважену позицію щодо захищеності систем інформаційного потоку та врегулюванні меж державного впливу на кібервідносини та дієву можливість реалізації відповідальності в рамках норм права. Так, на думку В. Зуй стан регулювання кібербезпеки «має недостатній рівень санкцій за інформаційні правопорушення» [9].

На думку Бакалінської О. та Бакалінського О. «найбільш перспективними напрямами розвитку національної системи кіберзахисту, є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі; впровадження систем інформаційного комплаєнсу; створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль» [3; с. 104]

Проте, в умовах повномасштабного вторгнення практика кіберінцедентів продемонструвала, що пріоритети проголошенні державою повинні мати не лише нормативну основу, але й базу реалізації. Усі проголошенні напрямки кіберзахисту захишаються бути актуальними, але потребують наддержавного регулювання та добровільного міжнародного погодження, як прояв сучасного міжнародного партнерства, як прояв створення безпечного міжнародного кіберсередовища. Звичайно, виникає багато викликів щодо дотримання таких принципів, оскільки різні політичні режими, системи, економіки, політичні світові форми впливу. Проте, стабільність та безпека в світі повинні бути першопричиною усіх форм міжнародної взаємодії.

Варто розуміти, що існуючі форми міжнародних форм боротьби з кіберзлочинністю формуються в рамках організацій, які мають регіональний вплив, або не ефективні зі своїм глобальним статусом. До прикладу, Організація Об'єднаних Націй, та її спеціалізовані установи. «Особливі функції щодо боротьби з високотехнологічними злочинами покладені на Управління ООН з наркотиків та злочинності (United Nations Office on Drugsand Crime – UNODC), у рамках якого здійснюється Глобальна програма з кіберзлочинності (Global Program on Cybercrime – GPC), а також функціонує Міжурядова експертна група відкритого складу з кіберзлочинності (Open-ended Intergovernmental Expert Group on Cybercrime). UNODC сприяє довгостроковому і стійкому нарощуванню потенціалу в боротьбі з кіберзлочинністю шляхом підтримки національних структур і дій» [10].

Якісною перспективою політики кіберзахисту є створення міжнародної глобальної організації зі стратегією міжнародної кібербезпеки, формування кіберкультури, вивченням досвіду протидії кібератакам, формування договірних відносин між окремими державами з метою формування єдиної політики кібезрахисту та кібербезпеки в світі. Оскільки, процес цифровізації лише масштабується, то питання безупинного удосконалення процесуальних та нормативних дій безупинний.

Україна в такій якісній потребі кіберзахисту в світі може зіграти фундаторську роль на ряду з прогресивними країнами світу та виконати

внутрішні запити в політиці кіберзахисту та зовнішні, які зменшать ризики кібератак тим самим якісно сформують діяльність політичної стабільності в умовах тотального інформаційного суспільного впливу.

*Висновки з дослідження і перспективи подальших пошуків у даному науковому напрямку.* Враховуючи усе вищезазначене можемо узагальнити, що сучасні виклики, які переживає людство виникли тому, що органи управління не працюють на випередження проблеми, а навпаки оцінюють масштаби негативного впливу, який відбувся та оцінюють можливі шляхи реагування. Важливим аспектом політичного впливу залишається інформаційне маніпулювання політичного думкою суспільства, ґрунтоване на нав'язуванні політичного вектору з поступальним зниженням рівня суспільного розвитку, що сприймається як єдиний правильний шлях для стабілізації суспільно-політичної ситуації.

Тому, основною метою якісної сучасної політичної діяльності є кібернетичний захист, який формується через нормативно регламентовані дії у внутрішній політиці держави та зовнішніх політичних процесах. Така швидка система змін по суспільно-політичному просторі потребує реагування на виклики на глобальному рівні.

Оскільки, політика на рівні регіону чи окремої держави може мати жорсткі форми обмежень для суспільства в кіберпросторі. Тому ідея створення міжнародної організації по кіберзахисту, ратифікації її державами учасницями, впровадження міжнародної доктрини кіберзахисту, відповідальності за кіберзлочити за національним та міжнародним правом, популяризація культури кіберпростору формує сучасні тренди для глобальної системи управління.

### *Література*

1. Kormych L. Zavhorodnia Yu. The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*, Volume 9, Issue 1, 2023. https://academic.oup.com/cybersecurity/article/9/1/tyad017/7240366

2. Горун О. Ю. Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. Інформація і право. № 2(37). 2021. С. 93–102.

3. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100–108.

4. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету.* 2019. № 2. С. 23–28.

5. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*, 2022. (10), 175–188.

6. Словник військових термінів та скорочень (абревіатур). *Воєнно-наукове управління Генерального штабу Збройних сил України*, 2020. 52 с.

7. Закон України «Про основні засади забезпечення кібербезпеки України» *Відомості Верховної Ради*, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

8. Досвід війни: які виклики стоять перед державою та бізнесом у кіберпросторі. *Державна служба спеціального зв'язку та захисту інформації України.* 2023. URL: https://cip.gov.ua/ua/news/dosvid-viini-yaki-vikliki-stoyat-pered-derzhavoyu-ta-biznesom-u-kiberprostori

9. Зуй В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. *Правове забезпечення адміністративної реформи.* 2022. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_1/35.pdf

10. Яцишин Ю. Роль міжнародних організацій у протидії кіберзлочинності. *Міжнародне публічне право.* 2019. URL: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

11. Яковлева Л. І. Комунікативний вимір процесу легітимації публічної влади. Політикус : наук. журнал. 2020. № 3. С. 103–109.

### Анотація

***Завгородня Ю. В.*** **Можливості політики кіберзахисту в зовнішніх та внутрішніх процесах.** – Стаття.

У статті розглядаються перспективи щодо діяльності держави в реалізації політики кіберзахисту у кібернетичній боротьбі суб'єктів політики. Можливості політики проявляються по різному у зовнішніх та внутрішніх процесах. Адже, політичні рішення та політична воля проявляють на різних рівнях політичної діяльності унікально, інколи не прогнозовано. Нормативна діяльність політичних еліт реалізується відповідно до різних суспільно-політичних підстав, а саме: суспільні запити на захист кіберсистем, кібератаки на державні та підприємницькі сервери, глобальний аналіз витрат від кіберзлочинів, кібербезпека цифровізованих систем політичного управління, процеси дистабілізації в окремих країнах, регіонах та ін.

Загалом, розвиток стабільного функціонування взаємодії у кіберпросторі не можливий без протиріч та конфронтації, тому питання захисту та безпеки формують ключову роль у концепції безпекових засад політики державного та глобального рівня. Кіберпростір є новітньою платформою для швидкого спілкування та узгодження політичних питань, що спрощує усі форми дипломатичного спілкування, їх точність та швидкість в реалізації.

Окрім того, органи управління локально переходять на цифровізовану систему документообігу, що потребує надійної системи захисту серверів, які зберігають інформацію окремих органів, проте така діяльність має мітити статегічні цілі державного спрямування, або навіть глобального.

Стаття спрямована на визначення можливостей української держави щодо формування системи захисту кіберпростору на рівні внутрішньої політики та прояву власних можливостей щодо зовнішніх та глобальних процесів політики захисту кіберпростору. Світова спільнота зацікавлена в досвіді, який отримала

Україна у боротьбі з агресором на різних рівнях, а тому має якісну практичну основу для визначення проблемних аспектів боротьби в кіберпросторі.

*Ключові слова:* кібербезпека, кіберзахист, зовнішня політика, внутрішня політика, кіберконфлікт, міжнародні організації, інформаційний захист, політичні маніпуляції.

**Summary**

***Zavhorodnya Yu. V.*** **Possibilities of cyber protection policy in external and internal processes.** – Article.

The article considers the prospects for the state's activities in the implementation of the cyber protection policy in the cyber struggle of political actors. Policy opportunities are manifested in different ways in external and internal processes. After all, political decisions and political will manifest themselves at different levels of political activity in a unique, sometimes unforeseeable way. The normative activity of political elites is implemented according to various socio-political grounds, namely: public requests for the protection of cyber systems, cyber attacks on state and enterprise servers, global analysis of costs from cyber crimes, cyber security of digitalized political management systems, destabilization processes in individual countries, regions, etc.

In general, the development of stable functioning of interaction in cyberspace is not possible without contradictions and confrontation, therefore the issues of protection and security form a key role in the concept of security principles of state and global policy. Cyberspace is the latest platform for rapid communication and coordination of political issues, which simplifies all forms of diplomatic communication, their accuracy and speed of implementation.

In addition, local management bodies are switching to a digitized system of document management, which requires a reliable system of protecting servers that store information of individual bodies, but such activity should mark the strategic goals of state direction, or even global.

The article is aimed at determining the capabilities of the Ukrainian state regarding the formation of a system of cyberspace protection at the level of internal policy and the manifestation of its own capabilities in relation to external and global processes of cyberspace protection policy. The world community is interested in the experience gained by Ukraine in the fight against the aggressor at various levels, and therefore has a qualitative practical basis for determining the problematic aspects of the fight in cyberspace.

*Key words:* cyber security, cyber defense, foreign policy, domestic policy, cyber conflict, international organizations, information protection, political manipulation.