УДК 32.019.51
DOI https://doi.org/10.20535/2308-5053.2021.4(52).248130

КІБЕРБЕЗПЕКА ЯК ІННОВАЦІЙНИЙ ЗАХИСТ У ПОЛІТИЧНОМУ ПРОСТОРІ УКРАЇНИ

Завгородня Ю. В.,
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»
ORCID ID: 0000-0003-3500-8638
julija020890@gmail.com

У статті акцентовано увагу на цінності у сучасному інформаційному суспільстві ролі кібербезпеки. Для розвитку ефективної системи взаємодії в інформаційному просторі виникає необхідність у формуванні меж захисту для користувачів. Система захисту, яка існує в суспільстві, спрямована на врегулювання протиріч, які виникають на рівні фактичного протиборства та суттєвого впливу на політичні процеси з чітко визначеними суб'єктами політичної активності.

Для сучасного світу суб'єкти глобального управління звертають серйозну увагу на рівень захищеності системи управління в окремих країнах та регіонах, що свідчить про ефективність або дисбаланс у системі управління, а також роль такого суб'єкта на наддержавному рівні системи управління.

Тому обрана тема є досить актуальною для світового процесу взаємодії та врахування поглядів окремих регіонів. Окрім того, ефективний захист кіберпростору допоможе зменшити рівень маніпуляції з боку суб'єктів політики, а це допоможе підвищити рівень політичної культури серед політичних діячів та рівень політичної свідомості серед пересічних громадян.

У статті проаналізовано сучасні наукові підходи до розуміння поняття кіберзахисту та кібербезпеки, надано узагальнену характеристику цих понять, виокремлено сучасні форми безпеки в кіберпросторі, проаналізовано стан кібербезпеки в українському інформаційному просторі та визначено її статус як суб'єкта глобальної взаємодії в інформаційному просторі.

У політичному процесі невід'ємним елементом взаємодії є інформаційний простір, оскільки сучасна платформа для публічних взаємовідносин між суб'єктами політики переформатована під новітні способи, а тому і механізми впливу на громадян набувають інноваційного характеру та демонструють невизначену реакцію від суспільства та можливі шляхи розвитку політичних подій. У зв'язку із цим виникає потреба у формуванні ряду механізмів для захисту усіх користувачів кіберпростору, які беруть участь у публічному спілкуванні щодо важливих політичних питань.

Ключові слова: кібербезпека, політичний вплив, інформаційний простір, політична активність, протиборство в політиці.

Постановка проблеми. Світова політична спільнота зосереджує свою увагу на формуванні безпеки для усіх жителів планети Земля. Такі принципи та ідеї обговорюються практично на усіх серйозних світових форумах, конференціях, міждержавних перемовинах, оскільки безпечне та мирне існування людей є запорукою стабільного існування для усіх держав та регіонів. А тому питання безпеки виходить за будь-які територіальні межі та потребує глобального уявлення про систему захищеності, бо регіональні катаклізми можуть містити глобальну небезпеку.

Звичайно, у сучасному технологічному процесі питання безпеки переходять у нову стратегічно важливу площину, а саме у кіберпростір. Тому кібербезпека є сучасним новим напрямом, який потребує наукового обргунтування, нормативного врегулювання та практичного втілення у ситуаціях, які

створюють перешкоди для об'єктивізації політичного процесу. У зв'язку із цим тема є досить актуальною та потребує детального аналізу.

Виклад основного матеріалу. В українському суспільстві під час останніх місцевих виборів, які відбулися у 2020 році, починається активне використання в мережі ТікТок, Фейсбук, Інстаграм, Ютуб. Місцеві суб'єкти політичного процесу активно використовують соціальні мережі, створюють різні групи, вислуховують проблемні питання району, регіону в якому бажають здійснювати активну політичну діяльність.

Окрім того, питання кібербезпеки актуальне не лише в рамках політичних процесів. Адже сучасні форми виробництва переформатовуються під онлайн-мережу у співпраці та взаємодії. Для банківських установ ключова роль у використанні положень до дії полягає в даних на офіційних інформаційних платформах. Усі офіційні урядові напрямки мають власні офіційні Інтернет-сторінки. А тому будь-які спроби кібератак та кіберагресії в окремій галузі можуть створити проблеми для усієї суспільно-політичної системи загалом.

Такий прогресивний розвиток інформаційної мережі потребує формування фахівців у напрямку кібербезпеки, що формують систему ефективного захисту в різних суспільно-важливих сферах. Тому на прикладі українського суспільства спеціальності, пов'язані з кібербезпекою та ІТ-індустрією, активно розвиваються та очолюють рейтинги популярних сучасних прогресивних професій із високим рівнем оцінювання праці та дефіцитом якісних спеціалістів.

Звичайно, політика проникає в усі галузі суспільного існування, оскільки усі вони потребують політичної волі та нормативно врегульованих рішень, кіберпростір у сучасному суспільстві є важливим напрямком для удосконалення механізмів взаємодії між різними користувачами, для позначення меж допустимих, толерантних та коректних висловлювань, меж політичних та інших видів маніпуляцій, особливостей впливу усіх цих аспектів на громадські дії та поведінку.

Під час аналізу кібербезпеки та її ролі під час взаємодії в інформаційному просторі для суб'єктів політики, які також використовують цей простір як платформу для протиборств та спілкування з громадянами, варто враховувати нормативну складову частину, так звану легальну, та сприйняття політичних рішень у суспільстві (легітимність), серед звичайних громадян та самих політиків, які також користуються інформаційними платформами та у специфічний для політиків спосіб задовольняють власні політичні інтереси та отримують суспільну реакцію як відповідь на політичні дії.

Саме така потреба існує в політичній площині, тобто врахування і легальності, і легітимності в застосуванні механізмів кібербезпеки як інноваційної форми захисту, яка формується в політичній площині. Суб'єкти політики стають одночасно і об'єктами, на яких також розповсюджуються прийняті політичні рішення під час політичної активності, що додає такому процесу значимості та публічності. Адже саме політики стають дзеркалом для суспільства в питаннях меж допустимого в інформаційному просторі та меж ефективності чинної нормативно-правової бази, яка є запорукою для формування правового, демократичного, публічного суспільства з гідною політичною елітою та політичними лідерами, які стануть зразком для молодого покоління.

Ураховуючи аналіз наукового напряму та потенціал до розвитку інформаційного впливу, у суспільстві виникає потреба у формуванні завдань наукового дослідження, а саме: надати наукову та нормативну характеристику поняттям кібербезпеки та кіберзахисту; визначити та проаналізувати стан легальності та легітимності механізмів кібербезпеки в українському інформаційному просторі; визначити роль наявних механізмів у формуванні державного статусу держави як надійного та значимого суб'єкта глобальної взаємодії в інформаційному просторі.

Дослідженням даного напрямку займаються як вітчизняні, так і зарубіжні науковці, праці яких стали основою під час написання статті, а саме: Ю.П. Лісовська, А.Р. Крусян, Ю.В. Завгородня, Д.В. Дубов, Г.О. Дзяна, Н.Р. Дзяний, М.Ю. Крутов, В.Л. Бурячок, В.О. Ємельянов, Г.В. Бондар та ін. Окрім того, під час дослідження було проведено аналіз нормативної бази як невід'ємного елемента політико-правової системи безпеки.

Ураховуючи стрімкі умови модернізації і трансформації інформаційного простору, метою наукового дослідження стало формування узагальненого уявлення про роль кібербезпеки як важливого чинника ефективної діяльності політико-правової системи суспільства в умовах значного впливу інформаційних потоків на політичні процеси та політичну свідомість. Для досягнення цієї мети використано історичний, порівняльний, системний та інші методи наукового дослідження, які сформували обґрунтовану роль необхідності захисту інформаційного простору в умовах політичних та правових трансформацій у суспільстві.

Під час взаємодії в політичних процесах виникає розуміння проблемних галузей та потрібних механізмів їх вирішення. У сучасному світі існує велика кількість загроз, які формуються в інформаційному просторі, а тому виникає потреба у використанні механізмів для ефективного їх вирішення. Уразлива українська система продемонструвала неготовність вирішувати проблеми з кібератаками,

які стали частиною військової агресії на Сході України. Оскільки сучасні форми гібридних війн демонструють залучення інформаційних атак на серйозні вірусні програми на сервери державного та транскорпораційного рівня, які серйозно підривають політичну та економічну стабільність у країні та регіоні загалом.

На думку Г.О. Дзян, Н.Р. Дзян, до моменту розгляду кібербезпеки варто розтлумачити поняття «інформаційної безпеки», під якою автори розуміють «такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони» (Дзян, 2016). Тобто ключем інформаційної безпеки в межах однієї держави є можливість доступу до бажаних ресурсів та відсутність заборон та перешкод у використанні національних інформаційних ресурсів.

Під час ефективної інформаційної політики формується ефективна інформаційна безпека, яка є важливим елементом політичної діяльності. На думку Г.О. Дзян, Н.Р. Дзян, під поняттям «кібербезпека» розуміють «стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам» (Дзян, 2016).

Тобто авторським колективом ключем необхідності кібербезпеки визначено ризики можливого кібервпливу, оскільки під ризиком ми власне розуміємо можливість виникнення такого впливу в різні моменти, які дуже важко передбачити, а за допомогою механізмів впливу держави та наявності санкційних норм створюють можливість попередити вплив ризику. Загалом, «значна частина визначень поняття «ризик» пов'язана із двома твердженнями: ризик зумовлений випадковими подіями або процесами; наслідки цих подій або процесів є небажаними» (Пехник, Завгородня, 2019).

У кіберпросторі такими небажаними наслідками можна назвати класичні усім відомі комп'ютерні віруси, з якими стикався кожен громадянин, окрім того, ще виділяють так звані «мережні черв'яки, а також «троянські коні». Усі ці різновиди так званих атак у мережі, які мають свою специфіку та створюють негативний вплив на фактичну можливість, є формою небезпеки, у якій важко визначити суб'єкта впливу та застосувати до нього санкції як механізми захисту системи. У сучасній Україні не існує прикладу виявлення та покарання в межах норм національного права суб'єктів впливу.

Окрім публічних припущень та глобального засудження конкретних вчинків зі сторони органів управління та міжнародних організацій, метою діяльності яких є збереження миру та безпеки у світі, ніяких заходів вжито не було, бо процедуру доведення злочину дуже важко здійснити в інформаційному просторі.

У загальній системі уявлень про кібербезпеку варто охарактеризувати поняття «безпека». На думку Ю.П. Лісовської, під цим поняттям варто розуміти «стан, властивість від прикметника «безпечний» та одночасно дію від дієслова «убезпечити», безпечний означає відсутність небезпеки, загрози; збереженість і надійність» (Лісовська, 2019).

Отже, проблематика виникає саме у суті створення умов для надійності та сталого функціонування кіберпростору. У науковій спільноті відсутнє єдине бачення щодо сутності кібербезпеки, яка є важливою складовою частиною для реалізації надійності у ціннісному розумінні.

А тому варто проаналізувати деякі наукові погляди на дане поняття. На думку Б.А. Кормич, «кібербезпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави». Окрім того, сучасні українські науковці, такі як В.І. Андрєєв, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест, формують спільне уявлення про кібербезпеку як захищеність інфраструктури та інформації від можливих впливів, які можуть бути навмисними, випадковими або штучними та впливають негативно на власників та користувачів інформації та інфраструктури, яка допомагає» (Лісовська, 2019).

Окрім того, існує ще ряд наукових поглядів (О.А. Баранова, Р.А. Калюжного, В.С. Цимбалюк, О.М. Степко), основна ідея яких ґрунтується на визначенні кібербезпеки в умовах інформаційних правовідносин, регламентованих нормативно-правовими актами як захист умов життєдіяльності в процесі створення, зберігання, розповсюдження та використання інформації. Автори акцентують увагу на тому, що інформація повинна бути достовірною та не містити негативного впливу на користувачів, обмежувати так звані технології, які можуть містити негативний характер, а найголовніше, щоб інформація була публічною, а суб'єкти, які розповсюджують її в мережі, повинні це робити в законному порядку, який регламентується правовою системою» (Лісовська, 2019).

Отже, враховуючи уявлення про безпекову складову частину як невід'ємний елемент політико-правової стабільності у суспільстві, варто відзначити, що кібернетичний напрям є вагомою складовою частиною безпекової системи, а механізми конкретних дій для стабільного існування

інформаційної системи потребують подальшого вдосконалення. Окрім того, під час характеристики кібербезпеки дуже часто використовують поняття кіберзахисту. Під час характеристики цих понять варто відзначити, що кіберзахист є складовою частиною кібербезпеки. Варто відзначити, що це не тотожні поняття, адже кібербезпека – це узагальнена термінологія, а кіберзахист – конкретна форма впливу в конкретному напрямку для реалізації кібербезпеки.

Оскільки політичні процеси розвиваються в кіберпросторі, то важливим завданням для усіх суб'єктів політики та пересічних користувачів мережі Інтернет є дотримання нормативно урегульованих них правил для безпеки спільного співіснування. Тому змінюється платформа для взаємодії політичних суб'єктів, однак обов'язок прояву толерантності, політичної культури залишається незмінним.

Сучасна нормативна база українського суспільства чітко розмежовує поняття «кібербезпека» та «кіберзахист», а тим самим розвивається та деталізується. Так, Законом України «Про основні засади забезпечення кібербезпеки України» статтею 1 зазначено, що «кібербезпека – 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», «кіберзахист – 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» (Закон № 2163-VIII).

Висновки. У сучасному світі розвинуті країни демонструють занепокоєність у захисті саме інформаційного простору. Так, проаналізований досвід прогресивних країн світу, які намагаються стати глобальними управлінцями, демонструє трансформаційну форму військової складової частини органів управління. Так, до прикладу, «за даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі у 2010 р., уже більше 20 країн планували здійснювати або реально здійснювали різноманітні інформаційні операції у 2009–2010 рр. Формуються спецпідрозділи, які мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника. Згідно з офіційними заявами, такі підрозділи створено в США (U.S. Cyber Command), Великобританії (Cyber Security Operations Centre при уряді Великобританії), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence)» [11].

Отже, враховуючи міжнародний досвід, наукові розробки та нормативну регламентованість кібербезпеки в українському суспільстві, варто відзначити, що усім свідомим політичним діячам та громадянам в інформаційному просторі здійснюється виклик на власну систему позитивних якостей, які зможуть сформувати якісно нову форму взаємовідносин у кіберпросторі.

Кібербезпека стає актуальним сучасним невід'ємним елементом політичної діяльності в інформаційному просторі, яка зменшить небезпеку кібератак, попередить негативний вплив та поступово удосконалить механізми взаємодії. Політика держави повинна бути спрямована на подальший шлях удосконалення механізмів захисту.

Zavgorodnya Yu. Cyber security as an innovative protection in the political space of Ukraine

The article focuses on the values of the role of cybersecurity in the modern information society. To develop an effective system of interaction in the information space, there is a need to form boundaries of protection for users. The system of protection that exists in society is aimed at resolving the contradictions that arise at the level of actual confrontation and significant influence on political processes with clearly defined subjects of political activity.

For the modern world, the subjects of global governance pay serious attention to the level of security of the management system in individual countries and regions, which indicates the effectiveness or imbalance in the management system. Also, the role of such an entity at the supranational level of the management system.

Therefore, the chosen topic is quite relevant for the global process of interaction and taking into account the views of individual regions. In addition, effective protection of cyberspace will help reduce the level of manipulation by political actors, which will help increase the level of political culture among politicians and the level of political awareness among ordinary citizens.

The article analyzes modern scientific approaches to understanding the concept of cybersecurity and cybersecurity, provides a generalized description of these concepts, identifies modern forms of security in cyberspace, analyzes the state of cybersecurity in the Ukrainian information space and defines its status as a subject of global interaction in the information space.

In the political process, an integral element of interaction is the information space, as the modern platform for public relations between policy actors has been reformatted in the latest ways, and therefore the mechanisms of influencing citizens become innovative and demonstrate uncertain response from society and possible ways of political development. events. As a result, a number of mechanisms need to be put in place to protect all cyberspace users who engage in public communication on important policy issues.

Key words: cybersecurity, political influence, information space, political activity, confrontation in politics.

Література:

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII / Верховна Рада України. URL : https://zakon rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.10.2021).
3. AR Krusian, II Zadoia, YI Maslova, YV Zavhorodnia. The Institutional and Legal Justification of the Restriction of Freedom of Movement in Conditions of Counteraction the Spread of the Covid-19 Pandemic. *San Gregorio de Portoviejo University.* URL : http://dspace.onua.edu.ua/bitstream/handle/11300/14526/The%20Institutional%20and%20Legal%20Justification%20of%20the%20Restriction%20of%20Freedom...pdf?sequence=1&isAllowed> (2020, September, 17).
4. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. *НІСД.* 2014. 192 с.
5. Дзяна Г, Дзяний Н. Реалізація національної політики у сфері кібербезпеки. *Ефективність державного управління*. 2016. № 3(48). Ч. 1. С. 123–130.
6. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. *ДУТ*, 2015. 231с.
7. Завгородня Ю.В. Кіберпростір як сучасна платформа для вирішення конфліктів. *HISTORY, POLITICAL SCIENCE, PHILOSOPHY AND SOCIOLOGY: EUROPEAN DEVELOPMENT DIRECTION*. Riga, Latvia :Baltija Publishing. 2021. С. 53–56.
8. Ємельянов В., Бондар Г. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Державне управління та регіональний розвиток.* 2019. URL : https://www.researchgate.net/publication/337725857.
9. Пехник А.В. Теорія ризику: історія та сучасні підходи. *Актуальні проблеми політики.* Фенікс, 2019. Вип. 63. С. 33–47.
10. Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on Internet Freedom / Ma Zhaoxu, Ministry of Foreign Affairs, the People's Republic of China. URL : http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t653351.htm.
11. Сучасні тренди кібербезпекової політики: висновки для України. *Аналітична записка.* URL : http://old2.niss.gov.ua/articles/294/.

References:

1. Lisovska Yu.P. (2019) Kiberbezpeka: ryzyky ta zakhody: navch. posibnyk. [Cybersecurity: risks and measures: textbook. manual] *K.: Vydavnychyi dim «Kondor»* 272 s. [in Ukrainian]
2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy [On the basic principles of cybersecurity in Ukraine: the Law of Ukraine] vid 05 zhovtnia 2017 roku № 2163-VIII / Verkhovna Rada Ukrainy. URL: https://zakon rada.gov.ua/laws/show/2163-19#Text (data zvernennia 25.10.2021) [in Ukrainian]
3. AR Krusian, II Zadoia, YI Maslova, YV Zavhorodnia. (2020) The Institutional and Legal Justification of the Restriction of Freedom of Movement in Conditions of Counteraction the Spread of the Covid-19 Pandemic. San Gregorio de Portoviejo University. <http://dspace.onua.edu.ua/bitstream/handle/11300/14526/The%20Institutional%20and%20Legal%20Justification%20of%20the%20Restriction%20of%20Freedom...pdf?sequence=1&isAllowed> [in English]
4. Dubov D.V. (2014) Kiberprostir yak novyi vymir heopolitychnoho supernytstva[Cyberspace as a new dimension of geopolitical rivalry]. *NISD,* 192s. [in Ukrainian]
5. H. Dziana, N. (2016) Dzianyi Realizatsiia natsionalnoi polityky u sferi kiberbezpeky[Implementation of national cybersecurity policy.]. *Efektyvnist derzhavnoho upravlinnia*. № 3(48) ch.1. s. 123-130 [in Ukrainian]

6. Buriachok V. L. (2015) Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk[Information and cybersecurity: socio-technical aspect: textbook]. *DUT*, 2015. 231s. [in Ukrainian]
7. Zavhorodnia Yu.V. (2021) Kiberprostir yak suchasna platforma dlia vyrishennia konfliktiv[Cyberspace as a modern platform for conflict resolution.]. *HISTORY, POLITICAL SCIENCE, PHILOSOPHY AND SOCIOLOGY: EUROPEAN DEVELOPMENT DIRECTION*. Riga, Latvia:"Baltija Publishing". S. 53-56. [in Ukrainian]
8. V. Yemelianov, H. Bondar (2019) Kiberbezpeka yak skladova natsionalnoi bezpeky ta kiberzakhyst krytychnoi infrastruktury Ukrainy[Cybersecurity as a component of national security and cyber protection of critical infrastructure of Ukraine]. *Derzhavne upravlinnia ta rehionalnyi rozvytok.* Elektronnyi resurs. – Rezhym dostupu: https://www.researchgate.net/publication/337725857 [in Ukrainian]
9. Pekhnyk A. V. (2019) Teoriia ryzyku: istoriia ta suchasni pidkhody[Risk theory: history and modern approaches.]. *Aktualni problemy polityky*. Feniks, Vyp. 63. S. 33-47. [in Ukrainian]
10. Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on "Internet Freedom" [Electronic resource] Ma Zhaoxu, Ministry of Foreign Affairs, the People's Republic of China. – Access mode: http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t653351.htm[in English]
11. Suchasni trendy kiberbezpekovoi polityky: vysnovky dlia Ukrainy. [Current trends in cybersecurity policy: conclusions for Ukraine.] *Analitychna zapyska.* Elektronnyi resurs. [Rezhym dostupu]: http://old2.niss.gov.ua/articles/294/ [in Ukrainian]

Стаття надійшла до редакції 15.11.2021
Стаття рекомендована до друку 26.11.2021