УДК 004.056:32
DOI https://doi.org/10.32782/app.v75.2025.20

А. В. Козьміних
orcid.org/0000-0003-2534-7652
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

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

КІБЕРНЕТИЧНІ ЗАГРОЗИ ДЛЯ ПОЛІТИЧНИХ ІНСТИТУТІВ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

У сучасному глобалізованому світі, де цифрові технології проникають у всі сфери суспільного життя, питання кібернетичних загроз для політичних інститутів набуває особливої значущості. Політичні інститути, такі як уряди, парламенти, політичні партії та громадські організації, дедалі більше залежать від інформаційно-комунікаційних технологій для забезпечення ефективного функціонування, взаємодії з громадянами та реалізації державної політики. Водночас саме ця залежність робить їх вразливими до кібератак, спрямованих на порушення функціонування систем управління, крадіжку конфіденційної інформації, маніпулювання суспільною думкою та підрив легітимності влади. Подібні загрози здатні дестабілізувати політичні процеси, створюючи ризики для національної безпеки та демократичних цінностей.

Актуальність теми посилюється стрімким зростанням кількості та складності кібератак, що здійснюються як недержавними злочинними угрупованнями, так і державними структурами. Використання кіберзброї та методів гібридної війни для досягнення політичних цілей стає поширеним інструментом міжнародних відносин. Це особливо стосується країн, що перебувають у стані політичної або військової напруги. У цьому контексті особливої важливості набувають дослідження ефективних механізмів захисту політичних інститутів, попередження та протидії кіберзагрозам, розробка нормативно-правових актів, що регулюють питання кібербезпеки, а також розвиток міжнародного співробітництва у сфері кіберзахисту.

Вивчення проблематики кібернетичних загроз для політичних інститутів є надзвичайно актуальним у контексті забезпечення стабільності державного управління та функціонування політичної системи. Виявлення уразливостей, оцінка ризиків та пошук шляхів нейтралізації кіберзагроз сприятиме формуванню ефективної національної системи кібербезпеки, захисту демократичних процесів та збереженню політичної стабільності. Усе це вимагає інтеграції зусиль державних органів, наукових установ, громадських організацій та приватного сектора в умовах стрімких технологічних змін та розвитку глобальної кіберпростору.

Основною ціллю дослідження є вивчення небезпек та викликів у кіберпросторі для політичних інститутів, а також характеристика позитивних перспектив для розвитку окремих політичних інститутів України в кіберпросторі. Для реалізації поставлених цілей необхідно проаналізувати існуючі кібернетичні загрози для політичних процесів, дослідити політичні інститути, які вразливі до кіберзагроз, оцінити перспективи позитивного використання кіберпростору для політичних інститутів та виклики, їх цифровізації.

Питаннями наукового аналізу займалися такі вітчизняні та зарубіжні науковці, а саме: Ф. Барановський, Л. Кормич, Ю. Завгородня, А. Козьміних, І. Діордіца, І. Проноза та ін.

Теоретичне обгрунтування політичних процесів в інформаціному просторі, варто починати з розуміння поняття «кіберзагрози». Так, на думку І. Діордіца «кібернетичні загрози (кіберзагрози) – це реальні або потенційні явища та фактори, що створюють загрозу життєво

важливим інтересам особи, суспільства та держави, і виникають через залежність від стабільного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем» (Діордіца І., 2017).

Згідно з Доктриною інформаційної безпеки України (що втратила чинність), у сфері інформаційної безпеки України визначено такі життєво важливі інтереси: інтереси особи (гарантування конституційних прав і свобод громадян щодо збору, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання в процеси обробки, передачі та використання персональних даних; захист від негативного інформаційно-психологічного впливу); інтереси суспільства (збереження та розвиток духовних, культурних та моральних цінностей українського народу; забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; підтримка та розвиток демократичних інститутів громадянського суспільства); інтереси держави (запобігання інформаційній залежності, блокаді та експансії з боку інших держав та міжнародних структур; забезпечення ефективної взаємодії органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; розвиток інформаційного суспільства, забезпечення економічного та науково-технологічного зростання України; формування позитивного іміджу держави та її інтеграція у світовий інформаційний простір) (Діордіца І., 2017).

Таким чином, кібернетичні загрози потребують ефективної системи захисту, яка враховуватиме інтереси кожного рівня – особистого, суспільного та державного, а також сприятиме забезпеченню інформаційної безпеки України в умовах глобалізації та розвитку цифрових технологій.

Сьогодні до основних загроз кібербезпеці та безпеці інформаційних ресурсів відносять такі виклики: вразливість об'єктів критичної інфраструктури та державних інформаційних ресурсів до кібератак; фізичне та моральне застаріння системи захисту державної таємниці та інших видів інформації з обмеженим доступом.

Кібернетичні загрози для політичних партій та громадських організацій у кіберпросторі становлять серйозну небезпеку, здатну впливати на стабільність політичних процесів, функціонування демократичних інститутів та розвиток громадянського суспільства. Ці загрози охоплюють широкий спектр викликів, які можуть підривати довіру громадян, обмежувати можливості для вільного волевиявлення та створювати передумови для маніпуляцій суспільною думкою (Барановський Ф., 2024, с. 20).

Однією з ключових загроз є кібератаки на інформаційні системи політичних партій та громадських організацій. Такі атаки можуть призводити до несанкціонованого доступу до конфіденційної інформації, викрадення персональних даних членів організацій, фальсифікації внутрішніх документів, знищення або модифікації важливої інформації. Це здатне дискредитувати партії та організації, викликати недовіру до їхньої діяльності та підривати політичну стабільність.

Інша серйозна загроза – використання дезінформації та маніпуляції у кіберпросторі. Зловмисники можуть поширювати неправдиву інформацію, створювати фейкові новини, маніпулювати громадською думкою через соціальні мережі та інформаційні платформи. Це ускладнює політичні кампанії, підриває репутацію політичних партій та громадських організацій, а також може спричиняти політичні кризи.

Крім того, значні виклики створюють кібершпигунство та втручання у внутрішні процеси політичних структур. Зловмисники можуть стежити за політичною діяльністю, збирати дані про стратегії, позиції та слабкі сторони партій та організацій. Це дає можливість впливати на прийняття рішень, прогнозувати політичні кроки та використовувати цю інформацію для підриву конкурентів або просування власних інтересів.

Таким чином, кібернетичні загрози для політичних партій та громадських організацій вимагають особливої уваги та розробки ефективних механізмів захисту. Це передбачає посилення кібербезпеки, впровадження сучасних засобів захисту інформації, підвищення обізнаності про кіберзагрози серед членів організацій, а також активну співпрацю з державними та міжнародними структурами для спільної протидії кіберзлочинності.

Кібернетичні загрози для інституту Президента та парламенту України є складною та багатоаспектною проблемою, яка ставить під загрозу функціонування державних органів влади, забезпечення національної безпеки та стабільність політичної системи. В умовах сучасного цифрового середовища такі загрози можуть бути спрямовані як на інформаційну інфраструктуру держави, так і на репутацію та легітимність державних інститутів.

Інститут Президента та парламент України є стратегічними цілями для кібератак, оскільки їх інформаційні ресурси містять важливу державну та конфіденційну інформацію. Кібератаки можуть включати: неавторизований доступ до урядових систем, що загрожує витоком державних таємниць та службової інформації; викрадення персональних даних високопосадовців та депутатів, що може використовуватися для шантажу або дискредитації; знищення або модифікацію офіційних документів, що дестабілізує роботу державних органів; DDoS-атаки на урядові веб-ресурси, що паралізує їхню роботу та унеможливлює доступ громадян до офіційної інформації.

Кіберзагрози можуть впливати на процес прийняття державних рішень, блокуючи роботу урядових органів або створюючи кризові ситуації. Це ускладнює функціонування інституту Президента та парламенту, послаблюючи державу зсередини.

Таким чином, ефективна протидія кіберзагрозам для інституту Президента та парламенту України вимагає впровадження сучасних технологій кіберзахисту, розробки національних стратегій кібербезпеки, активної співпраці з міжнародними партнерами та підвищення рівня інформаційної обізнаності серед державних службовців.

В умовах збройного конфлікту та гібридної війни кіберзагрози стають важливим елементом протистояння, що спрямоване не лише на знищення матеріальних ресурсів, а й на підрив державної влади, деморалізацію населення та дестабілізацію суспільства. Військові дії супроводжуються масованими кібератаками, які стають частиною загальної стратегії ведення війни.

В умовах повномасштабної війни на території України можна виділити певні специфічні особливості кіберзагроз, а саме: знищення або порушення роботи систем енергопостачання, водопостачання, транспорту, зв'язку та банківської сфери має на меті дестабілізувати економіку та життєзабезпечення країни.

Окрім цього, відбувається активне використання соціальних мереж та медіа для поширення дезінформації, фейкових новин, пропаганди та підриву морального духу громадян. В умовах війни це спрямовано на деморалізацію населення та військових. Також, злом електронної пошти, акаунтів у соціальних мережах, поширення компрометуючих матеріалів для дискредитації політичного та військового керівництва. Злом урядових систем управління та військових мереж з метою отримання секретної інформації або дезорганізації командування. Отримання інформації про стратегічні плани, військові операції та особисті дані посадовців та військових.

Під час війни політика держави у сфері кібербезпеки реагує на виклики зростання кіберзагроз (Проноза І., 2024). Так, держава розробляє та впроваджує комплексну політику кібербезпеки, що включає такі напрями: створення національної системи кіберзахисту (впровадження єдиної системи моніторингу та реагування на кібератаки, координація дій між державними та приватними структурами, що забезпечують безпеку критичної інфраструктури); розробка нормативно-правової бази (удосконалення законодавства у сфері кібербезпеки, визначення відповідальності за кібератаки та створення умов для взаємодії державних органів та бізнесу); співпраця з міжнародними партнерами (обмін досвідом та технологіями з міжнародними організаціями та союзниками, участь у спільних кібероперація та тренуваннях).

Важливою складовою для держави є розробка інформаційних кампаній для протидії дезінформації, підтримка позитивного іміджу держави та зміцнення довіри громадян до влади. Застосування активних заходів кібероборони, включаючи проведення контратак на джерела кіберзагроз (Завгородня Ю., 2022).

У сучасних умовах війни кіберзагрози стали невід'ємною частиною гібридної війни, що вимагає від держави оперативного реагування та побудови надійної системи кібербезпеки. Комплексний підхід, міжнародна співпраця та постійне вдосконалення механізмів кібероборони дозволяють зменшити вплив кіберзагроз та забезпечити захист політичних інститутів, критичної інфраструктури та громадян.

Кіберпростір став важливим полем ведення гібридної війни та впливу на політичні інститути. Кібератаки на органи державної влади, політичні партії, громадські організації, інститут президента та парламент є складовою частиною сучасних конфліктів, що вимагає комплексного підходу до забезпечення кібербезпеки.

Кіберзагрози можуть підірвати довіру до політичних інститутів, вплинути на виборчі процеси, дестабілізувати внутрішню ситуацію в країні та створити умови для зовнішнього втручання. В умовах війни та гібридної агресії це стає реальною загрозою суверенітету та національній безпеці.

Для ефективного протистояння кіберзагрозам державі необхідно забезпечити постійний моніторинг, прогнозування та оперативне реагування на інциденти в кіберпросторі. Важливо створити єдину систему кіберзахисту, яка об'єднуватиме державні та приватні структури.

Кіберзагрози є глобальною проблемою, тому координація зусиль із міжнародними партнерами, обмін інформацією та досвідом, участь у спільних кібероперацій є критично важливими для забезпечення національної безпеки та захисту політичних інститутів.

Необхідно вдосконалити нормативно-правову базу у сфері кібербезпеки, визначити чіткі механізми притягнення до відповідальності за кібератаки та забезпечити надійний захист інформації з обмеженим доступом.

Підготовка фахівців у сфері кібербезпеки, підвищення кіберграмотності населення та інформаційні кампанії сприятимуть зміцненню стійкості до кіберзагроз та формуванню культури безпеки в кіберпросторі. Комплексна стратегія, яка враховує сучасні загрози та виклики, спрямована на захист політичних інститутів, забезпечення стабільності та розвитку держави, є важливим елементом державної політики в умовах війни та кіберконфліктів.

Таким чином, кібернетичні загрози для політичних інститутів вимагають скоординованої відповіді держави, міжнародної співпраці та всебічної підготовки фахівців. Виконання цих завдань сприятиме підвищенню рівня захищеності державних структур та політичних інститутів в умовах сучасних викликів і загроз.

Література

Барановський Ф. Гібридні загрози для демократичних політичних систем. Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів матеріали VII Всеукраїнської науково-практичної конференції (м. Одеса, 30 квіт. 2024 р.). Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2024. С. 19-21.

Завгородня Ю.В. Особливості поведінки учасників політичного процесу під час конфронтації в інформаційному просторі. *Політикус.* Випуск 4. 2022. Видавничий дім «Гельветика» – С. 29-34

Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право.* № 4, 2017. URL: http://pgp-journal.kiev.ua/archive/2017/4/22.pdf

Проноза І.І. Політичний консалтинг в умовах гібридних загроз та інформаційної війни: виклики для демократичних процесів. *Політикус.* Випуск 4. 2024. URL: http://politicus.od.ua/4_2024/15.pdf

Машталір В., Гук О., Мурасов Р., Фараон С., Лоза В. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*. № 49(1), 2024. С. 93–104.

Maltseva, I., Chernish, Y., Shtonda, R. Аналіз деяких кіберзагроз в умовах війни. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2022, 4(16), 37–44.

Пархоменко-Куцевіл О., Проблеми забезпечення національної безпеки в умовах воєнного часу. Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування», Вип. 3, 2023, С. 143-150.

Часник Д.В. Забезпечення прав людини у сфері національної безпеки в умовах протистояння військовій агресії російської федерації. Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична. 2022. Вип. 34. URL: https://nzlubp.org.ua/index.php/journal/article/download/600/551.

References

Baranovskyi, F. (2024). Hibridni zahrozy dlia demokratychnykh politychnykh system [Hybrid threats to democratic political systems]. In Suchasna ukrainska derzhava: vektory rozvytku ta shliakhy mobilizatsii resursiv. Materialy VII Vseukrainskoi naukovo-praktychnoi konferentsii (pp. 19–21). Odesa: DZ «Pivdennoukrainskyi natsionalnyi pedahohichnyi universytet imeni K. D. Ushynskoho», Tsentr sotsialno-politychnykh doslidzhen «Politicus». (in Ukrainian)

Zavgorodnia, Y. V. (2022). Osoblyvosti povedinky uchasnykiv politychnoho protsesu pid chas konfrontatsii v informatsiinomu prostori [Behavioral features of political actors during confrontation in the information space]. Politykus, (4), 29–34. (in Ukrainian)

Dioridtsa, I. (2017). Poniattia i zmist kiberzahroz na suchasnomu etapi [Concept and essence of cyber threats at the current stage]. Pidpryiemnytstvo, hospodarstvo i pravo, (4). http://pgp-journal.kiev.ua/archive/2017/4/22.pdf (in Ukrainian)

Pronoza, I. I. (2024). Politychnyi konsaltynh v umovakh hibridnykh zahroz ta informatsiinoi viiny: vyklyky dlia demokratychnykh protsesiv [Political consulting under hybrid threats and information warfare: challenges to democratic processes]. Politykus, (4). http://politicus.od.ua/4_2024/15.pdf (in Ukrainian)

Mashtalir, V., Huk, O., Murasov, R., Faraon, S., & Loza, V. (2024). Kiberborotba v umovakh zbroinoho protystoiannia: analiz, stratehii ta vyklyky [Cyber warfare under military confrontation: analysis, strategies, and challenges]. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 49(1), 93–104. (in Ukrainian)

Maltseva, I., Chernish, Y., & Shtonda, R. (2022). Analiz deiakykh kiberzahroz v umovakh viiny [Analysis of some cyber threats during war]. Kiberbezpeka: osvita, nauka, tekhnika, 4(16), 37–44. (in Ukrainian)

Parkhomenko-Kutsevil, O. (2023). Problemy zabezpechennia natsionalnoi bezpeky v umovakh voiennoho chasu [Problems of national security provision during wartime]. Naukovyi visnyk Vinnytskoi akademii bezperervnoi osvity. Seriia: Ekolohiia. Publichne upravlinnia ta administruvannia, (3), 143–150. (in Ukrainian)

Chasnyk, D. V. (2022). Zabezpechennia prav liudyny u sferi natsionalnoi bezpeky v umovakh protystoiannia viiskovii ahresii rosiiskoi federatsii [Ensuring human rights in the field of national security during military aggression of the Russian Federation]. Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia: ekonomichna, yurydychna, (34). https://nzlubp.org.ua/index.php/journal/article/download/600/551 (in Ukrainian)

Анотація

Козьміних А. В., Завгородня Ю. В. **Кібернетичні загрози для політичних інститутів: виклики та перспективи. –** Стаття.

У колективному дослідженні розглядаються кібернетичні загрози, що постають перед політичними інститутами в умовах глобальної цифровізації та розвитку інформаційних технологій. Особлива увага приділяється аналізу впливу кіберзагроз на політичний процес, функціонування політичних партій, громадських організацій, інституту президента та парламентаризму. Авторським колективом досліджено основні виклики, що виникають у сфері забезпечення політичної стабільності та демократичних процесів в умовах кіберпростору. Увага акцентується на проблемах захисту від кібернападів, що можуть впливати на виборчі процеси, дезінформацію та маніпулювання громадською думкою, а також на підриві легітимності державних інституцій.

Також, у науковому дослідженні розглядаються можливі шляхи подолання загроз за допомогою впровадження сучасних технологічних рішень, правових механізмів та міжнародного співробітництва. Визначено перспективи розвитку ефективних стратегій кібербезпеки для захисту політичних інститутів у контексті глобалізованого світу.

Окрім того, важливе значенні у формуванні кіберзахисту та стабільності у поілтичному процесі приділяється ролі міжнародних організацій та об'єднань у боротьбі з кіберзлочинністю, зокрема у сфері політики та державного управління. Проаналізовано значення колективних зусиль для формування загальних стандартів безпеки та створення ефективних механізмів протидії кіберзагрозам.

У статті також розглядаються можливості підвищення рівня кібербезпеки в Україні через реалізацію державних програм, посилення контролю за інформаційним простором та розвиток партнерства з міжнародними організаціями. Акцентується увага на важливості підготовки фахівців з кібербезпеки та активного впровадження цифрових технологій у політичні процеси.

Таким чином, стаття містить комплексний підхід до вирішення проблем кібербезпеки у політичній сфері, підкреслюючи важливість міждисциплінарної співпраці для формування ефективної стратегії протидії кіберзагрозам.

Ключові слова: політичний процес, кіберпростір, політичні інститути, політичні партії, громадські організації, інститут президента, парламентаризм.

Summary

Kozminykh A. V., Zavgorodnya Yu. V. **Cyber threats to political institutions: challenges and prospects. –** Article.

The collective study examines cyber threats facing political institutions in the context of global digitalization and the development of information technologies. Particular attention is paid to analyzing the impact of cyber threats on the political process, the functioning of political parties, public organizations, the institution of the presidency, and parliamentarism. The authors have examined the main challenges that arise in the field

of ensuring political stability and democratic processes in cyberspace. Attention is focused on the problems of protection against cyberattacks that can affect electoral processes, disinformation and manipulation of public opinion, as well as undermining the legitimacy of state institutions.

The scientific study also examines possible ways to overcome threats through the implementation of modern technological solutions, legal mechanisms, and international cooperation. The prospects for the development of effective cybersecurity strategies to protect political institutions in the context of a globalized world are identified.

In addition, the role of international organizations and associations in the fight against cybercrime, in particular in the sphere of politics and public administration, is given great importance in shaping cyber defense and stability in the political process. The importance of collective efforts for the formation of common security standards and the creation of effective mechanisms for countering cyber threats is analyzed.

The article also examines the possibilities of increasing the level of cybersecurity in Ukraine through the implementation of state programs, strengthening control over the information space, and developing partnerships with international organizations. It emphasizes the importance of training cybersecurity specialists and the active implementation of digital technologies in political processes.

Thus, the article contains a comprehensive approach to solving cybersecurity problems in the political sphere, emphasizing the importance of interdisciplinary cooperation for the formation of an effective strategy for countering cyber threats.

Key words: political process, cyberspace, political institutions, political parties, public organizations, the institution of the president, parliamentarian.