DOI https://doi.org/10.51647/kelm.2022.7.10

SPECYFIKA ROZWOJU KONFRONTACJI POLITYCZNEJ W SFERZE CYBERNETYCZNEJ

Yuliia Zavhorodnia
kandydat nauk politycznych, docent,
docent Katedry Teorii Politycznych Narodowego Uniwersytetu
„Odeska Akademia Prawnicza" (Odessa, Ukraina)
ORCID ID: 0000-0003-3500-8638
julija020890@gmail.com

Adnotacja. Działalność polityczna jest ważnym elementem działania systemu zarządzania kraju i systemu stosunków globalnych. W warunkach cyfryzacji społeczeństwa następuje transformacja poglądów na temat stosunków polityczno-zarządczych. Dlatego rozwój polityczny nabywa zmiany jakościowe, które są kształtowane przez współczesne wymagania ze strony społeczeństwa. Ogólnie rzecz biorąc, wszystkie decyzje polityczne są konsekwencją wyzwań, które tworzą się na globalnym lub regionalnym poziomie stosunków. Podobnie kwestia modernizacji politycznej wynika z pragnień i potrzeb obywateli, które są realizowane w postaci konstruktywnych zmian w relacjach między podmiotami politycznymi a specyfiką realizacji działalności politycznej. Ważną rolę w realizacji działalności politycznej odgrywa konflikt w kraju. Ponieważ cele nierównowagi systemu politycznego i organów zarządzających opierają się na sytuacji konfliktogennej. Przez „równowagę konfliktogenną w państwie" należy rozumieć system środków zapobiegających konfliktom oraz system środków wdrażających działania stabilizacyjne zespołu pokonfliktowego. Dlatego w warunkach wzrostu możliwości rozpowszechniania informacji istnieje potrzeba zwiększenia działań w zakresie współpracy ze społeczeństwem i organami zarządzającymi w odniesieniu do systemu działań w kierunku otwartej komunikacji i koordynacji stanowisk stron.

Słowa kluczowe: proces polityczny, konfrontacja, cyberkonflikty, cyfryzacja, wpływ cybernetyczny, działalność polityczna.

THE SPECIFICS OF THE DEVELOPMENT OF POLITICAL OPPOSITION IN THE CYBERNETIC SPHERE

Yulia Zavhorodnya
Candidate of Political Sciences, Associate Professor,
Associate Professor of the Department of Political Theories
National University "Odesa Law Academy" (Odesa, Ukraine)
ORCID ID: 0000-0003-3500-8638
julija020890@gmail.com

Abstract. Political activity is an important element of the country's management system and the system of global relations. In the conditions of digitalization of society, ideas about political and managerial relations are being transformed. Therefore, political development acquires qualitative changes, which are shaped by modern demands from society. As a rule, all political decisions are the result of challenges that will be formed at the global or regional level of relations. In the same way, the question of political modernization originates from the wishes and needs of citizens, which are realized in the form of constructive changes in the relations between political subjects and the specifics of the implementation of political activity. An important role in the implementation of political activity is played by conflict-causing balance in the country. Since, the goals of the imbalance of the political system and governing bodies rely on the conflict-causing situation. "Conflictogenic balance in the state" should be understood as a system of measures that prevent conflicts and a system of measures that carry out stabilization actions of the post-conflict syndrome. Therefore, in the conditions of increasing opportunities for the dissemination of information, there is a need to increase measures to work with society and governing bodies regarding the system of measures in the direction of open communication and the agreement of the parties' positions.

Key words: political process, opposition, cyber conflicts, digitalization, cyber influence, political activity.

СПЕЦИФІКА РОЗВИТКУ ПОЛІТИЧНОГО ПРОТИБОРСТВА В КІБЕРНЕТИЧНІЙ СФЕРІ

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

Анотація. Політична діяльність є важливим елементом діяльності системи управління країни та системи глобальних відносин. В умовах цифровізації суспільства відбувається трансформація уявлень про політико-управлінські відносини. Тому, політичний розвиток набуває якісних змін, які сформовані сучасними вимогами від суспільства. Як правило, усі політичні рішення є наслідком викликів, які сформуватись на глобальному чи регіональному рівні відносин. Так само і питання політичної модернізації походить від бажань та потреб громадян, які реалізуються у вигляді конструктивних змін у відносинах між політичними суб'єктами та специфікою реалізації політичної діяльності. Важливу роль у реалізації політичної діяльності відіграє конфліктогенна урівноваженість в країні. Оскільки, цілі дисбалансу політичної системи та органів управління опираються на конфліктогенну ситуацію. Під «конфліктогенною урівноваженістю в державі» варто розуміти систему заходів, які попереджують конфлікти та систему заходів, які здійснюють стабілізаційні дії постконфліктного синдрому. Тому, в умовах збільшення можливостей для поширення інформації виникає потреба у збільшенні заходів щодо роботи з суспільством та органами управління щодо системи вчинків в напрямку відкритої комунікації та погодженням позицій сторін.

Ключові слова: політичний процес, протиборство, кіберконфлікти, цифровізація, кібернетичний вплив, політична діяльність.

Вступ. Оскільки, політичний розвиток орієнтується на сучасні виклики та форми розвитку в умовах залучення інформаційних заходів швидкого розповсюдження інформації, відсутності кордонів для інформації та глобалізації регіональних конфронтаційних дій політичних еліт, тому політична галузь набуває нових якісних форм та методів публічної діяльності.

Звичайно, напрямок дослідження кібернетичної сфери стає все актуальнішим та потрібним, у різних галузях суспільного розвитку. Разом з тим, значна увага приділяється безпековій складовій у кіберпросторі, що говорить про елемент можливого попередження протиріч у кіберпросторі, який в демократичному суспільстві формується в рамках правових механізмів. Така правова основа знаходиться на стадії становлення та формування стратегічного планування для подальшої реалізації. Проте виникає актуальним потреба у відшуканні заходів врегулювання конфліктів та управління конфліктами у кіберпросторі, які виникають у політичній площині та формують загрозу розвитку суспільства та політичної системи управління таким суспільством.

Політичні процеси фактично трансформуються в кіберплощину та поглиблюють активну форму кіберспілкування. Розвивається аналітика та роздуми в сфері політичної стабільності, глобалізуються політичні стратегічні рішення, видозмінюються контури політичної міри відповідальності, блокуються системи зв'язку з політичними суб'єктами, які ведуть діяльність, яка порушує правила мережі комунікації та багато інших процесів, які модернізують уявлення про політичну дійсність, управлінську систему, спрощення бюрократичних процедур в інформаційній системі.

Політичний простір пронизаний актуалізацією кіберпроцесів, які мають відношення до політичного спрямування, адже в умовах суспільно-політичних потрясінь відбувається пошук думок, вчинків, аналізу, які сприяють розумінню політичної реальності, можливих подальших кроків управлінського характеру та вектору наступних суспільних змін, які можуть відбутись.

Враховуючи актуальність розвитку сучасних форм протиборства в політичній галузі та в потребі трансформації суспільно-політичного сприйняття, ***метою*** статі є характеристика прояву кіберконфліктів в політичній площині та подальше поглиблення процесу кібернетичної комунікації суб'єктів політики і цифровізації системи публічних відносин.

Основна частина. Для досягнення поставленої мети необхідно виконати ряд ***завдань,*** які сприятимуть отриманню, якісних висновків, а саме: проаналізувати існуючу систему наукових та нормативних основ кібернетичної складової політики; виокремити роль кіберконфліктів у політичних процесах; охарактеризувати існуючі негативні наслідки кібернетичного протиборства; визначити перспективи удосконалення системи контролю за формати політичного протиборства у кіберплощині.

Оцінюючи мету та завдання обраної тематики дослідження, варто відзначити, що система публічних відносин у демократичному суспільстві пронизана конфліктами, оскільки суспільство, яке видозмінює систему політичного режиму має ряд прогалин у політичній системі та органах управління. Окрім того, сучасні форми відкритого суспільства задають тренди для політиків у суспільній актуалізації інформаційного сприйняття та форм протидії. Оскільки, політики демократичної формації повинні відповідати запитам власного суспільства та відповідати на виклики глобального світу, що створює ряд завдань та інтелектуальної імпровізації для політичних діячів, то кіберконфлікти стають однією і таких форм запитів.

Разом з тим, затягування процесів нормативного врегулювання проблемних та актуальних та суспільства питань містяться фактори внутрішні та зовнішні, що збільшуються проблеми у процесі врегулювання осучаснених форм взаємовідносин.

Матеріал і методи досліджень. Для деталізації актуалізованого напрямку було досліджено нормативно складову суспільно-політичного сприйняття в українському суспільстві, яка проявлена в законних та підзаконних актах, стратегіях політико-правового планування удосконалення заданого напрямку. Окрім того, важливу роль відіграє аналіз науковцями процесу цифровізації, як поштовху до подальших суспільно-політичних перетворень. Тому, у статті проаналізовано праці зарубіжних та відчизняних авторів, а саме: Хаустової М.Г., Стеблиної Н.О., Завгородньої Ю.В., та ін.

Під час здійснення дослідження було використано загальнонаукові методи, а саме: системний метод (сприяв створенню розуміння небезпечної ролі кіберконфліктів в політичних процесах), футурологічний метод (спрогнозував значимість подальшої уваги щодо проблематики конфліктів у новітній кіберплощині), конфліктологічні теорії розвитку суспільства та політичних процесів (допомогли осягнути небезпеку та цінність конфліктологічного процесу у суспільстві та політичній взаємодії), метод біхевіоризму (сприяв здійсненню аналізу поведінки суб'єктів політики безпосередньо і опосередковано).

Окрім того, у роботі акцентуємо увагу на поглядах Д. Юм, який обґрунтував намагання скоординувати політику на створення ефективних шляхів розв'язання і пом'якшення політичних конфліктів, що власне об'єктивно вписується в сучасну політичну реальність. Тому, дана концептуалізація політики, як ядра розвитку усіх суспільно-політичних процесів пронизаних конфліктами, які потрібно пом'якшувати та вирішувати яскраво актуальна для трансформованих кіберконфліктів в політичних процесах. Фактично, даний методологічний підхід став оновою для побудови сучасної концепції щодо кіберконфліктів у політиці.

Разом з тим, метод прийняття політичних рішень досить важливий для вирішення прогалин у суспільній взаємодії та політичних процесах, як раціональна складова для сталого розвитку та розкриття інноваційного потенціалу суспільства в рамках окремої політичної системи. Адже, демократія є шляхом до швидких якісних змін в умовах політичної ефективної роботи. Оскільки, якісно видозмінювати суспільство та політичну систему можливо в умовах відкритого доступу до рекрутування політичної еліти, по інтелектуальним показникам суб'єктів, щоб еліта відповідала назві по суті, а не лише номінально. Адже, якісна політична еліта це вищий рівень конфліктологічної культури.

Окрім того, значну увагу приділено кібернетичному методу, в рамках якого у структурі кібернетичної системи виокремлюють керуючий та керований об'єкти, прямі зв'язки, по яким здійснюються команди управління, та зворотні зв'язки, по котрих рухається інформація щодо виконання команд управління, аналіз котрої сприяє можливому коригуванню команди управління. Адже, освідомлення того, що є мінімум два суб'єкти в системі кіберпротиборства з однієї та іншої сторони кіберконфлікту, бо є суб'єкт, котрий безпосередньо працює з пристроями, які розповсюджують інформацію, віруси, атакують системи та конкретний суб'єкт політики, який стоїть за цією діяльністю з метою досягнення певного політико-управлінського результату, у процесі розвитку подій цей суб'єкт може корегувати команди для виконавця.

Результати та їх обговорення. Потреба у визначені та конкретизації сучасних напрямків розвитку політичної діяльності, її розвитку, конфронтації та стабілізації політичної площини набуває усе більшого значення. Адже, швидкість отримання інформації, її розповсюдження і кібервплив на опонента та суспільство є рушійними кроками до політичних змін в системі управління. До прикладу, перед повномасштабним вторгненням рф та територію України протягом чотирьох місяців активно здійснювались кібератаки на національні електронні інформаційні ресурси, що демонструвало бажання агресора дестабілізувати систему управління в країні та швидко реалізувати військові та політичні цілі.

Під національними електронними інформаційними ресурсами варто розуміти «систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво-важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів» (Закон, 2017).

Тому, політична діяльність країни могла мати негативні наслідки під час військової агресії на самому початку повномасштабної війни, якщо б система інформаційних ресурсів була суттєво пошкоджена агресором. Падіння інформаційних ресурсів знизило б суспільно-політичну діяльність органів управління, продемонструвало низьку ефективність роботи усіх суспільно-важливих напрямків. А тому, як наслідок унеможливило б комунікацію влади з народом, що б означало падіння верхівки органів управління.

Важливу роль у напрямку інформаційно-кібернетичної трансформації відіграє міжнародна підтримка у даному напрямку. Коли спеціалісти з країн безпекового блоку активно допомагають захищати інформаційні ресурси та діють на глобальному рівні, адже в кіберпросторі війна не є регіональною, а глобальною з центром протидії на території України. А тому, як тільки ескалація війни на території України піде на стад, тоді ескалація глобальної кібервійни також знизиться.

Звичайно, сучасна система політичних зв'язків, політичної діяльності та політичної направленості трансформується в систему технологічних процесів в інформаційно-кібернетичній площині за допомогою цифровізації політичних рішень, дописів політичних діячів, публічної критики політичних уподобань на

особистих соціальних сторінках. Видозміна сучасної форми комунікації надає політичним рішенням публічності глобального спрямування, що сприяє демократичному плюралізму політичних поглядів у суспільстві, проте разом з тим, і збільшує дисбаланс у стабільності політичної системи.

У зв'язку з цим, змістовними є погляди М.Г. Хаустової, адже вона відзначає, що «розвиток принципів цифрового суспільства стимулює вдосконалення способів і методів взаємодії в рамках соціально-економічних відносин. Застосування інформаційних технологій дозволяє розширювати комунікаційні процеси, змінює склад і статус їх учасників, принципи просторової взаємодії шляхом мережевого спілкування, підвищує децентралізацію прийняття управлінських рішень в державному і приватному секторі» (Хаустова, 2022).

Окрім того, варто розуміти, що ключем будь-яких змін є нормативне врегулювання процесів життєдіяльності суспільства, яке покладено на політичну сферу публічного управління. Тому, з метою стабілізації сучасної трансформації державою регламентовано певні стратегії змін, які розраховані на діяльність органів управління та суспільства у спільній взаємодії. Така діяльність українського політика демонструє процес підготовки самих органів управління до нової форми надання послуг та підготовки суспільства до інноваційних систем отриманих послуг та споглядання на сучасні політичні процеси у новому форматі публічного менеджменту.

Інформаційно-комунікаційні технології є уже частиною щоденного політичного процесу та суспільної взаємодії. Тому, свідомість громадян та нормативна регламентація інформаційних процесів сприяють створенню меж суспільно-політичної відповідальності та регламентуванню окремих дії, як політико вмотивованих та суспільно значимих.

Сучасна інформаційна площина сприяє упровадженню цифрових технологій, котрі здійснюється в сфері цифрової трансформації. Цей процес організаційно підкріплено формуванням Комітету з питань цифрової трансформації, який діє у складі Верховної Ради України та Міністерства цифрової трансформації на рівні виконавчої влади. Воно було утворене урядом у зв'язку з реорганізацією Державного агентства з питань електронного урядування у спосіб перетворення (Стеблина, 2020: 127).

Враховуючи існуючу нормативну базу та стратегію подальшого удосконалення нормативних засад врегулювання питань кібербезпеки варто відзначити, що розвиток системи кібернетичних відносин уже розпочинається в правовому полі, проте науковці завжди у виявленні недоліків знаходяться на декілька кроків вперед та висвітлюють ключові проблемні питання, які у сучасному світі стають формою новітніх відносин.

Тому, враховуючи існуючу характеристику кіберпростору В. Бурячок формує узагальнене уявлення про новітню площину і акцентує увагу та тому, що варто розмежовувати поняття інформаційного та кібернетичного, як частина і ціле відповідно. Так, від кіберпростором автор відзначає «віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, такими як електронний інформаційний ресурс (IP), системи й мережі всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передавання інформації, котра в них циркулює, із метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони» (Бурячок, 2015: 10).

Підтримуючи повністю думку Бурячка В. варто відзначити, що автор наголошує на можливості використання віртуального середовища «для впливу на об'єкти сторони протиборства», що демонструє наукову єдність в усвідомленні подальшого розвитку такого протиборства в окремих галузях, в тому числі в політологічних процесах.

Однак, розуміючи ціннісну роль політологічних процесів та можливі негативні наслідки, які уже є в якості прикладу в світі кібернетичних форм протиборства, то виникає потреба у політологічній волі до прийняття політичних рішень, щодо механізмів впливу на дії суб'єктів політики у кіберпросторі. Проте, така політична воля – це механізм до врегулювання внутрішніх кіберконфліктів в політичній площині, однак усвідомлення зовнішніх небезпек демонструє потребу в глобальному розвитку аналізу проблеми захисту кібернетичного простору, що також містить свій прояв у глобальному впливовому політичному істеблішменті.

Проте, більшість впливових країн світу формують переважно систему боротьби, яка проявляється офіційно сформованими галузями чи органами в системі управління країни. Так, у складі збройних сил окремих країн світу існують спеціальні структури, які займаються інформаційною та кібернетичною безпекою, а саме: «об'єднане Кіберкомандування (U. S. Cyber Command-USCYBERCOM) та спеціалізований кібернетичний розвідувальний центр у США; управління мережних операцій у Німеччині; центральне управління з кібербезпеки, Оперативного центру забезпечення кібербезпеки (CSOC) та Центру державного зв'язку (GCHQ) у Великобританії; Центр інформаційних систем Служби безпеки (CISSS) та Національного агентства безпеки інформаційних систем (ANSSI) у Франції; спеціалізований центр захисту національного кіберпростору Tehila в Ізраїлі; кіберпідрозділи у складі Федеральної служби безпеки Росії тощо» (Бурячок, 2015: 11).

Зрозуміло, що функціональне призначення даних галузевих інституцій ведення боротьби в сфері кіберпростору, щодо атак на кіберпростір та інформаційний простір. «Кіберборотьба – це комплекс заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань» (Бурячок, 2015: 11).

Сучасні політичні висловлювання не оминають проблематику кібернетичного простору, оскільки самі політики розуміють цінність безпеки у політичному управлінні для суспільного сталого розвитку країн, які

вийшли на високий рівень розвитку та декламують політичну та правову стабільність, проте кіберконфлікти можуть стати дестабілізуючим фактором для таких країн.

Так, на конференції Високий представник ЄС із зовнішніх справ та політики безпеки Кетрін Ештон відзначив, що «вільний кібернетичний простір відкрив для людства безмежні можливості, водночас як каталізатор глобальних політичних подій спричиняє і серйозні зовнішньополітичні конфлікти. Тому спільною метою є вільне і безпечне гарантування кібернетичного простору» (Будапешт, 2012).

Тому, послідовність у вчинках політичних еліт провідних країн світ є демонстрацією стабільності у висловлюваннях і діях, проте в умовах швидкої модернізації кібернетичних форм боротьби та віртуальної конфронтації необхідна пришвидшена реакція та дієвість.

В узагальненій характеристиці розуміння боротьби у кіберпросторі доцільно використовувати термін «кіберконфлікти», який узагальнює систему взаємопов'язаних подій в кіберпросторі та допомагає здійснити якісний аналіз щодо обмеження негативних наслідків та попередження в подальшому можливої боротьби політичних суб'єктів такою формою.

Кіберконфлікти у політичних процесах є новітньою формою політичної боротьби та управлінського впливу на політичні рішення та процеси, тому їх вирішення та пом'якшення є невід'ємними процесами подальшого наукового дослідження, державної та глобальної статистики, яка працює на виявлення слабких напрямків безпеки та захисту загалом кібернетичної системи суспільства.

Важливим завдання для кіберентичної політики держави є моніторинг соціальних мереж в різних напрямках та аспектах активності суспільства, а саме виділяють: регулярний моніторинг, первинний моніторинг, конкурентний моніторинг, репутаційний моніторинг. Регулярний моніторинг здійснює постійне вистежування інформації в кіберпросторі, з метою виявлення конфронтаційної активності та політичної реакції на них, з метою корегування власне інформаціної політики та політики прийняття управлінських рішень. Первинний моніторинг характеризується діяльністю, з метою початку власного інформаційного формату діяльності окремих суб'єктів політики. Конкурентний моніторинг характеризується спрямованістю дослідження діяльності опонентів у мережі, їх активності та зворотного зв'язку від суспільства. В свою чергу репутаційний моніторинг приблизно охоплює рамки не менше, як шість місяців роботи партії чи політичної групи, з метою виявлення позитивних та негативних аспектів роботи (Бурячок, 2015: 93).

Загалом перша згадка про кіберконфлікти з'являється у 1985 році під час кібератаки Меркуса Гесса, який працював на КДБ на військові та дослідні лабораторії Сполучених Штатів Америки. На той момент рівень освіченості атакуючих був низьким тому наслідків для баз даних фактично не відбулось (Соціологія інтернету, Кібервійни).

Проте, уже створено основу для подальшого розвитку можливої методики впливу на опонентів, причому глобального масштабу. Тому, уже на початку XXI ст. кіберконфліктами називають такі конфлікти, що розвиваються в інтернет просторі та мають деструктивний характер. Тобто, якщо в сучасному розумінні політичного конфлікту в загальному аспекті прослідковуються і позитивна складова і негативна, проте на сучасному етапі ескалації в кіберпросторі автори акцентують увагу на негативному процесі протиборства в кіберпросторі, бо виявити та довести злочинну діяльність важко, міру відповідальності та провину сформувати та довести в рамках правового поля складно, що показує негативну частину боротьби в кіберпрострі.

Все, що не можливо ввести в правову площину одночасно стає небезпечним та складним для освідомлення, бо може ґрунтуватись лише на добросовісній договірній основі сторін протиборства.

Тому, кіберконфлікт – це форма протиборства, яка може здійснювати за допомогою технічних засобів (наприклад кібератаки) та психологічні методи (наприклад пропаганда, маніпуляція).

Основними типами кіберконфліктів у політичній сфері можна виокремити: кібервандалізм (це пошкодження даних політичної партії, окремих політичних лідерів, органів управління в кіберпросторі), інтернет-злочини (протиправні дії, які обмежують чи порушують права політичних інститутів), кібершпигунство (постійний моніторинг мереж лідерів, партій та політичних груп по інтересам, відшукання інформації суб'єктом протиборства в інформаційному просторі для використання проти опонента), кібертероризм (шкода яка здійснюється за допомогою кібертехнологій, проте наслідки можуть бути у формі навіть звичайного тероризму, що дестабілізує ситуацію у політичній площині країни де це відбулось), кібервійна(це форма сучасної війни з кібервійськом і кіберцілями).

Кожен тип кіберконфлікту для політичних процесів небезпечний по своєму та деструктивний по своїй суті, адже форма різна, але ціль одна – це негативний вплив на опонента чи на його репутацію.

Тому, загальне уявлення про кіберконфлікт між політичними опонентами індивідуальними чи груповими демонструє нову площину, яка зручна для сторін в аспекті безсуб'єктності застосування методів впливу, що з однієї сторони сповільнює політичну волю до ефективного впливу на регламентацію процесів в кіберпросторі (Завгородня, 2022: 97). Оскільки, розвиток технологічних процесів досить швидкий, однак прийняття рішень про встановлення політико-правових меж відбувається повільно, то виникає потреба уваги політичних інститутів до даного напрямку виникнення проблематики. Адже, суб'єкти політики використовують кіберпростір, лише як інструмент для задоволення політичних чи власних потреб, що обмежує можливості для осучаснення та публічного визнання технологічного прогресу в усіх сферах суспільного життя.

До прикладу, державна регуляторна політика направлена на забезпечення ефективної діяльності підприємців з унеможливленням ухиляння від сплати податків від отриманого прибутку. На підставі чого було регламентовано зобов'язання для підприємців у використанні касового апарата, за що власне підприємці

притягувались, до адміністративної відповідальності за порушення такої вимоги. Така норма трансформувалась у зручність для громадян в плані мінімального використання готівкових коштів. Проте, прикладів таких технологічних процесів в підприємництві, банківській сфері, центрах адміністративної допомоги, онлайн освіті досить багато. Тому коли противник розпочав атаки на електромережі по всій Україні, від яких стали залежні фактично усі учасники політико-суспільної системи, громадяни не могли повноцінно задовільнити продуктові потреби, бо готівку уже давно ніхто не використовує в великих масштабах. Що свідчить про уже досягнутий значний технологічний розвиток України, як держави та суспільства і індивідів, які створюють новітні програми для зручного суспільного життя, однак цей розвиток працює з низькою, або мінімальною системою захисту, що дає ворогові допомогу у вібервійні.

Разом з тим, українське суспільство уже в практичних діях зрозуміло, що інформаційна система та цивілізаційні технології стають вразливішими, в умовах повномасштабної війни на полі бою і в кіберпросторі. Тому, варто розуміти, що в умовах ескалації кіберпростір використовується для кібермоніторингу ситуації опонентом, як суспільство реагує на такі незручності в політико-суспільній системі.

Разом, з тим використання військовими технологічних засобів наведення вогню, коректування за допомогою технічних засобів у формі планшетів, телефонів також свідчать про сучасний формат використання кібернетичного простору для ведення вогневого ураження противника.

Система недоліків, щодо сприйняття кіберпростору, як політичного простору, містить широкі масштаби, адже важливо формувати механізми, які не будуть обмежувати права людини, разом з тим, які будуть зберігати форми спілкування, які якісно впливатимуть на суспільно-політичний розвиток не окремої країни, а глобального світу. Тому в аспекті відпрацювання ключових ініціатив для подальшого розвитку суспільно-політичної системи важливо приділити увагу політичній культурі, яка на теперішній час ґрунтується на публічній виваженості і латентній грубості, а доцільніше проявлялася б на відкритій позиції, яка може містити елементи дискусії, однак відкритої не заангажованої.

Політична культура сприятиме створення міжнародної системи впливу на такі атаки, що уособлюватиме протидії державам кібертерористам, що матиме глобальний характер та відкриту систему спілкування для світу, та обмеження у співпраці з країнами кібертерористами. Міжнародна система сприятиме формуванню кібердемократії, як політичного режиму майбутнього.

Окрім того, важлива інформаційна діяльність має бути направлена на кібербезпекову складову у світі зі створенням колегіальної системи кіберзахисту, котрий допомагатиме зменшенню впливу кібератак на життєдіяльність суспільства. З кіберконфліктами боротись індивідуально країнам дуже важко та ефективність нижча. Організаційно-правові норми міжнародного формату сприятимуть процесу боротьби з кіберзлочинністю та кібертероризмом, які використовують сторони у протиборстві один одному.

Яскравими формами використання кібератак на думку С. Гнатюка можна виділити «хакерська група Anonymous реалізувала КбА на сайти державних установ Ізраїлю – у результаті постраждали сайти «Моссаду», армії та спецслужб; у Швеції реалізовано потужну КбА на Міністерство оборони, «Сведбанк» та Управління залізничних доріг; американські кіберексперти провели успішну КбА на пропагандистський сайт «Аль-Каїди» у Ємені; проведено потужні вірусні КбА на електроенергетичні компанії США; зареєстровано Троянські програми Win32.Duqu та Win32.Flame, що поширюються в Інтернет через знімні носії інформації і слугують для систематичного збору та модифікації конфіденційної інформації»(Гнатюк, 2013:122).

Тому, світу уже відомі приклади багатьох кібернетичних небезпек, які відбулись та глобальним проблемам, які можуть відбутись через ескалацію в кіберпросторі. Наслідок існуючих видів конфліктної кібератівності – це економічні втрати для громадян і держав та втрати політичні, які проявляються у дискредитації політичної спільноти та системи управління з метою повалення державності загалом чи зміни правлячої еліти.

Тому, якщо проаналізувати статистику, щодо стану розвитку кібератак в умовах війни в України, то ворог лише нарощує кількість атак. Так, «якщо в лютому (з 1 по 23 лютого) на державний сектор здійснили близько 143 тисяч атак, то в наступні місяці ця цифра стрімко зросла: 3,2 мільйона атак за дві декади квітня, 42,7 мільйона атак у травні, 27,7 мільйона – в червні, 32,3 мільйона атак у липні, 28,7 мільйона атак у серпні, 25,1 мільйона у вересні» (Вдовенко, 2022).

Така, статистика демонструє значний приріст атак, які зосереджені в основному на «сканування (збір інформації про системи або мережі) – 24 308 395 атак; спроби експлуатації вразливості (спроби вторгнення з використанням вразливості у системі, компоненті чи мережі) – 639 806 випадків; шкідливе підключення (спроби з'єднання від/до IP/URL – адреси, пов'язаної з відомим шкідливим програмним забезпеченням, наприклад C2C або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі) – 151 597 спроб; спроби авторизації або входу в систему (спроба входу до служб або механізмів доступу, невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних) – 63 089 випадків; атаки на відмови в обслуговуванні DoS/DDoS (вплив на нормальну роботу системи чи сервісу, що досягається скеруваанням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів) – 1791 атак; спам (надсилання небажаних повідомлень або великої кількості повідомлень) – 708 випадків» (Вдовенко, 2022).

Такі дані, формують підтвердження актуалізації процесів дослідження кібеконфліктів, їх руйнівного характеру в кіберпросторі та суспільстві. Разом з тим, виникнення нагальної потреби у збалансованому захисті суспільно-важливих мереж.

Звичайно враховуючи усі аспекти суспільно-політичної психології варто узагальнити, що інформаційний простір та технологічні можливості сприяють різним прошаркам населення проявляти себе та озвучувати власні бажання та потреби. Великий відрив у суспільстві між бідними та багатими стає джерелом до ескалації у різних її проявах. Державна політика та міжнародна політика комплексної дії на проблемні сектори шлях до зменшення суспільно-політичної напруги в світі.

Висновки. Сучасна політична діяльність вдало трансформується в інформаційно-комунікаційну площину, з використанням позитивних аспектів для публічної політики демократичного режиму. Однак, навіть в умовах демократії та позитивних аспектів сучасного інформаційного простору виникає ряд завдань для удосконалення публічної діяльності, створення меж відповідальності та публічності через комунікаційні мережі.

Разом з тим, закриті суспільства та тоталітарні режими, стоять перед великим викликом глобальної політики та суспільної напруги, які важче стримувати в умовах цифровізації та технологічних інновацій. Усі форми суспільної активності мають бути враховані та декларовані у політичних рішеннях, щоб суспільство стабільно розвивалось, як в політичних процесах, так і в новітніх наукових розробках та якісно користувалися отриманими результатами.

Оскільки, якісний шлях попередження конфліктів це створення правових меж співіснування різних політичних поглядів, повага до іншої точки зору щодо політичних процесів, використання правових публічних методів конкурування, застосування заходів законного впливу на протиправні політичні дії, створення відповідальності за кібератаки та хакерську діяльність, що порушує суверенітет країни, недоторканість бізнесу та особистісну свободу людини.

Однак, найважливішою є політична культура ведення сучасного конфлікту та політична освіта для суб'єктів політики. Оскільки політична культура є загальноприйнятим поняттям, яке не створює сучасним політикам ніяких меж для дій. Для того, щоб така культура стала в пріоритеті для суспільного критерію політичного лідера прогресивний розвиток має отримати політична освіта для суб'єктів політики та усього суспільства. Оскільки, люди вищого рівня освіти, зневажатимуть політичну еліту, яка застосовує методи публічних бійок, штовханини, відшукання компромату на опонента, формування системи залякування через хакерські атаки та хейти в соціальних мережах. Що стане основою, для якісного рекрутування політичної еліти та системи конфліктологічних відносин.

Конфлікти не можливо викорінити з суспільно-політичної площини. Вони є шляхом до новітніх елементів розвитку, а відповідно і новітніх елементів протиборства. Проте, людина вищої політичної фундації не дозволить собі опускатись до методик протидії опоненту, які можуть вплинути негативно на його політичну кар'єру.

Розвиток політичного протиборства в кіберпросторі в сучасному сприйнятті є саме тим процесом, що демонструє збільшення суспільних груп, які можуть проаналізувати інформацію, надати власну оцінку таким процесам публічно чи сформувати індивідуалістську позицію. Така новітня модифікація суспільної дійсності, збільшення активності суспільства в кіберпросторі є шляхом до новітньої комунікації суб'єктів політики та суспільства, глобальних суб'єктів політики, окремих кандидатів на виборах, що конкурують та інших сторін комунікації в кібернетичних політичних процесах.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від Відомості Верховної Ради, 2017, № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження КМУ від 20 вересня 2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-р
3. Стеблина Н.О. Складові Цифровізації політики: цифровий форум, цифровий капітал та структура цифрових можливостей. *Науковий журнал «Політикус»*. 2020. Випуск 5. С. 126–131.
4. Національна стратегія сприяння розвитку громадянського суспільства Україні на 2021–026 роки. Затверджена Указом Президента України від 27 вересня 2021 року № 487/2021/ https://www.president.gov.ua/documents/4872021-40193
5. Стратегію реформування державного управління України на 2022-2025 роки, розпорядженням Кабінету Міністрів України від 21 липня 2021 р. № 831 р. URL: https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#Text
6. Хаустова М.Г. Державна політика в умовах цифровізації суспільства. Міжнародний досвід реалізації програм та стратегії цифровізації. *Аналітично-порівняльне правознавство.* №2. 2022. URL: http://journal-app.uzhnu.edu.ua/article/view/261881/258267
7. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. *Київ: ДУТ*, 2015. 288 с.
8. Безпеку Інтернету та боротьбу з кіберзлочинністю обговорюють у Будапешті. (2012) URL: https://www.ukrinform.ua/rubric-other_news/1404257-bezpeku_internetu_ta_borotbu_z_kiberzlochinnistyu_obgovoryuyut_u_budapeshti_1760523.html
9. Соціологія інтернету. *Кібервійни.* 2022. URL: http://elbib.in.ua/sotsiologiya-internetu-pidruchnik-online.html
10. Гнатюк С.О. Кібертироризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security*, 2013, vol. 19, issue 2, p. 118–129.
11. The National Cyber Security Strateg (NCSS): Success through cooperation URL : http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011
12. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf

13. Вдовенко О. 25 мільйонів кібератак щомісяця. Як Росія намагається зашкодити Україні в цифровому просторі. *Детектормедіа.* 2022. URL: https://detector.media/infospace/article/204308/2022-10-29-25-milyoniv-kiberatak-shchomisyatsya-yak-rosiya-namagaietsya-zashkodyty-ukraini-v-tsyfrovomu-prostori/
14. Гнатюк С.О. Теоретичні основи побудов та функціонування систем управління інцидентами інформаційної безпеки. *Захист інформації.* №1 (54). 2012. С. 121–126.
15. Завгородня Ю.В. «Кіберконфлікти» та «політичні конфлікти»: співвідношення понять. Актуальні проблеми політики : зб. наук. пр. – Одеса, 2022. – Вип. 70. С. 95–100.

References:

1. Zakon Ukrainy (2017) «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [About the main principles of ensuring cyber security of Ukraine] vid Vidomosti Verkhovnoi Rady, № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]
2. Pro skhvalennia Kontseptsii rozvytku elektronnoho uriaduvannia v Ukraini: Rozporiadzhennia (2017) [On the approval of the Concept of the development of e-governance in Ukraine] KMU vid 20 veresnia № 649-r. URL: https://zakon.rada.gov.ua/laws/show/649-2017-r. [in Ukrainian]
3. Steblyna N.O. (2022) Skladovi Tsyfrovizatsii polityky: tsyfrovyi forum, tsyfrovyi kapital ta struktura tsyfrovykh mozhlyvostei. [Components of Digitization Policy: Digital Forum, Digital Capital and Digital Capability Framework] Naukovyi zhurnal «Politykus». 2020. Vypusk 5. s. 126–131. [in Ukrainian]
4. Natsionalna stratehiia spryiannia rozvytku hromadianskoho suspilstva Ukraini na 2021 – 2026 roky. [National strategy for promoting the development of civil society in Ukraine for 2021–2026] (2021) Zatverdzhena Ukazom Prezydenta Ukrainy vid 27 veresnia 2021 roku № 487/2021/ https://www.president.gov.ua/documents/4872021-40193 [in Ukrainian]
5. Stratehiiu reformuvannia derzhavnoho upravlinnia Ukrainy na 2022–2025 roky, [The strategy of reforming the state administration of Ukraine for 2022–2025] rozporiadzhenniam Kabinetu Ministriv Ukrainy vid 21 lypnia 2021 r. № 831 r. URL: https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#Text [in Ukrainian]
6. Khaustova M.H.(2022) Derzhavna polityka v umovakh tsyfrovizatsii suspilstva.[State policy in the conditions of digitalization of society. International experience of implementation of digitalization programs and strategies] Mizhnarodnyi dosvid realizatsii prohram ta stratehii tsyfrovizatsii. Analitychno-porivnialne pravoznavstvo. №2. URL: http://journal-app.uzhnu.edu.ua/article/view/261881/258267 [in Ukrainian]
7. Buriachok, V.L. (2015) Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk. [Information and cyber security: socio-technical aspect: a textbook.] Kyiv: DUT, 288 s. [in Ukrainian]
8. Bezpeku Internetu ta borotbu z kiberzlochynnistiu obhovoriuiut u Budapeshti. [Internet security and the fight against cybercrime are discussed in Budapest.] (2012) URL: https://www.ukrinform.ua/rubric-other_news/1404257-bezpeku_internetu_ta_borotbu_z_kiberzlochinnistyu_obgovoryuyut_u_budapeshti_1760523.html [in Ukrainian]
9. Sotsiolohiia internetu.[Sociology of the Internet] Kiberviiny. (2022.) URL: http://elbib.in.ua/sotsiologiya-internetu-pidruchnik-online.html [in Ukrainian]
10. Hnatiuk S.O.(2013) Kibertyroryzm: istoriia rozvytku, suchasni tendentsii ta kontrzakhody. [Cyberterrorism: history of development, current trends and countermeasures] Ukrainian Scientific Journal of Information Security, vol. 19, issue 2, r. 118–129. [in Ukrainian]
11. The National Cyber Security Strateg (NCSS): Success through cooperation URL: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011 [in English]
12. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf [in English]
13. Vdovenko O. (2022) 25 milioniv kiberatak shchomisiatsia. [25 million cyberattacks every month.] Yak Rosiia namahaietsia zashkodyty Ukraini v tsyfrovomu prostori. Detektormedia. URL: https://detector.media/infospace/article/204308/2022-10-29-25-milyoniv-kiberatak-shchomisyatsya-yak-rosiya-namagaietsya-zashkodyty-ukraini-v-tsyfrovomu-prostori/ [in Ukrainian]
14. Hnatiuk S.O.(2012) Teoretychni osnovy pobudov ta funktsionuvannia system upravlinnia intsydentamy informatsiinoi bezpeky.[Theoretical foundations of construction and functioning of information security incident management systems] Zakhyst informatsii. №1 (54). S. 121–126. [in Ukrainian]
15. Zavhorodnia Yu.V. (2022) «Kiberkonflikty» ta «politychni konflikty»: spivvidnoshennia poniat. [«Cyber conflicts» and «political conflicts»: the relationship of concepts.] Aktualni problemy polityky : zb. nauk. pr. Odesa, Vyp. 70 S. 95–100. [in Ukrainian]