DOI https://doi.org/10.32837/app.v0i68.1293
УДК 321:316.483, 342.9

А. В. Пехник
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»

СУЧАСНІ ЗАГРОЗИ КІБЕРТЕХНОЛОГІЙ У ПОЛІТИЧНОМУ ПРОЦЕСІ

Політичні процеси в сучасному світі трансформуються у новітні форми та зв'язки. Політичні лідери виходять на нову платформу взаємодії, а саме у кіберпростір. Відповідно, створюють нові види політичних технологій, які розвиваються та функціонують у кіберпросторі та отримують назву «кібертехнології». Зростання рівня розвитку кібертехнологій як в Україні, так і у світі загалом, проявляється не тільки на рівні їх використання в підприємницькій діяльності, а й у політичних процесах (наприклад, тероризм, виборчі процеси). Зараз спостерігаємо виникнення нових загроз та тенденції до нових кіберзлочинів. Анонімність інформаційних глобальних мереж, швидкість передачі даних і легкість їх застосування – це те, що вважається головними причинами технологічного вибуху та поширення мережі Інтернет у різних сферах життя. Водночас слід зазначити, що нові кібернетичні технології вводяться швидше, ніж наука та право встигають реагувати на ці процеси. Також необхідно враховувати той факт, що кібернетична інфраструктура та критичні комунікації дуже важливі для світу, але різні кібернебезпеки можуть мати серйозні і навіть руйнівні наслідки.

Тобто, сьогодні ми бачимо, що сучасні форми активності у кіберпросторі створюють нові виклики для суспільства у вигляді новітніх загроз, оскільки трактувати та аналізувати інформацію про політичні події та процеси в суб'єктивному форматі будуть усі охочі, а тому дуже важливим стає відбір достовірної інформації та вміння сприймати політичні процеси та рішення без формування небезпеки для національної та державної цілісності.

В українському суспільстві існує постійна небезпека та військова конфронтація на Сході держави, а використання інформаційного простору та маніпулювання свідомістю людей по різні сторони активної фази протиборства підсилює небезпеку та збільшує рівень загрози та напруги у політичному та військовому протистоянні. А тому обрана тема дослідження досить актуальна у сучасному політичному процесі України та загалом у світі, оскільки глобалізація політичних процесів впливає і на політичні технології в інформаційному просторі, які поширюються та не мають територіальних меж.

У 2018 році відбулася панельна дискусія за темою «Кібербезпека та дезінформація в Україні та на Заході». Цю дискусію відкрила Енн Епплбаум, яка зазначила, що «Україна відіграє дуже важливу роль у світі в контексті розвитку технологій війни. Україна – це така собі чашка Петрі, в якій російський уряд тестував різні види технологій та стратегій, різні форми ведення війни, нові способи використання кібертехнологій та кампаній з дезінформації… Я вбачаю в українцях людей, що найкраще знаються на цій темі та які запропонують найкращі рішення у майбутньому» (Круглі столи з питань безпеки, 2018).

Існують ґрунтовні дослідження політичних технологій на етапі державотворення. Так, Т. Ринковий, досліджуючи політичні технології, надає чітку характеристику цьому поняттю, яке варто трактувати як «не тільки методологічно об'єднану сукупність процедур цілеспрямованої діяльності, мета якої – отримання бажаного заданого результату для замовника, але як послідовність дій, спрямованих на вироблення відповідних алгоритмів поведінки суб'єкта,

це особливо очевидно під час аналізу виборчих політичних технологій. Саме певні установки, які визначать вибір тієї чи іншої політичної сили суб'єктом виборчого процесу, є метою політичних технологів» (Ринковий, 2009, с. 221).

У цьому випадку автор чітко поєднує політичні технології з роллю у виборчому процесі та постановкою чітких поведінкових механізмів політичних лідерів, продуманих дій та висловлювань, створення картини лідера чи політичної сили як персонажа з мультику про добро та зло. Незважаючи на прогресивність інформаційних технологій та різноманітність публічної літератури, методика впливу на суспільну свідомість діє та продовжує вдосконалюватись. Підтвердженням цьому є наявність наукових прац0ьі протягом різних історичних періодів у названому науковому напрямку.

Дослідженням технологій впливу в політичних процесах займалися та продовжують займатись як вітчизняні, так і зарубіжні науковці. Так, серед праць зарубіжних науковців із класичними поглядами на політичні технології можна відзначити роботи В. Парсонса, М. Говлета, Р. Даля, Д. Істона, С. Хантінгтона та інших вчених. Окрім того, сучасні наукові погляди на політичні технології формуються у вітчизняній політологічній спільноті, а саме: Т. Ринковим, М. Головатим, А. Пехник, Ю. Завгородньою, А. Кройтором, І. Милосердною та іншими дослідниками, основними ідеями яких є формування новітніх форм сприйняття та використання політичних технологій.

Враховуючи особливості змін та глобалізаційні процеси, політичні технології набувають нових видозмінених форм. Якщо першоджерела політичних подій перш за все отримують поширення в інформаційному просторі та відтворюють картину політичних подій та прийнятих рішень на підставі політичних позицій, то кібертехнології – це їх суб'єктивне відтворення окремими політичними лідерами, які мають свою групу прибічників, подій з баченням та трактуванням з вигодою для себе чи політичної сили, яку вони представляють.

Тому метою наукового дослідження стали загрози, які виникають під час застосування кібертехнологій у сучасному політичному процесі.

На підставі обраної мети дослідження авторським колективом поставлено такі завдання: проаналізувати сучасні погляди на розвиток політичних технологій; охарактеризувати сучасні форми впливу на політичну свідомість у кіберпросторі; визначити можливі небезпеки під час застосування чи використання кібертехнологій.

Сутність політики полягає в боротьбі за владу та розподіл владних повноважень, тож бажанням кожного політичного та державного діяча є здобуття, збільшення влади, тоді як політичні партії метою своєї діяльності ставлять саме збільшення підтримки серед населення для можливостей збільшення політичної сили, а відповідно, і збільшення владних повноважень. Для досягнення таких цілей і партія, і лідери застосовують ряд політичних технологій, які допомагають підтримувати і навіть збільшувати підтримку серед населення. Це категорія громадян, на яких розповсюджують суб'єкти політики свій вплив для підтвердження ефективності власної політичної діяльності.

Однак науковці акцентують на тому, що варто розрізняти політичний вплив, політичну діяльність та маніпуляцію. Оскільки це різні речі за змістовним наповненням та сутністю, які повинні бути визначальними під час отримання підтримки, тобто легітимації влади у суспільстві (Ринковий, 2009, с. 221).

Тому для об'єктивізації політичних процесів виникають універсальні бачення щодо політичних технологій як невід'ємної частини політичного процесу. Важливо, на яких принципах та нормах побудована система поданої інформації для широких мас населення. На думку М. Головатого, «політичні технології варто розуміти як сукупність прийомів, методів, способів, процедур, які використовують суб'єкти політичної діяльності (особистості, політичні та суспільні групи, політичні партії, громадські об'єднання, групи тиску тощо)» (Головатий, 2009, с.222).

Актуалізуючи увагу на суспільній значимості технологій, Т. Ринковий доходить висновку, що перехід технологій у площину політики відбувається за наявності теоретичних знань про саме суспільство та особливості його розвитку. Усе це сприяє застосовуванню різноманітних закономірностей, норм, принципів, факторів щодо визначення методики, яка допоможе

ефективно впливати на свідомість суспільства. Для сучасного процесу застосування технологізації в управлінні потрібно виходити із сутнісних основ. На основі стійкості та функціонування політичної системи, яка знаходиться в стані перетворення, перебуває баланс інтересів окремих соціальних та політичних груп або суспільства загалом, що є важливим елементом розвитку громадянського суспільства.

Важливу роль у формуванні політичних технологій в сучасному суспільстві відіграють саме інформаційні технології. На думку І. Милосердної, інформаційні технології – це сукупність сучасних електронних технологічних засобів і програмного забезпечення, а також організаційних форм і методів їхнього застосування в інформаційній роботі, яка спрямована на ефективне використання інформаційних ресурсів (Милосердна, 2020, с. 64).

Окрім того, варто пам'ятати, що застосування технологій у політиці може проходити через призму ризиків, які політичним діячам/лідерам потрібно враховувати під час використання різної методики впливу на свідомість суспільства. Авторським колективом, що складається з науковців А. Пехник, А. Кройтора та Ю. Завгородньої, вдало звернено увагу на те, що «ризик пов'язаний з діяльністю в умовах, з одного боку, реально існуючої невизначеності, а з іншого – вибору зацікавленим індивідуумом певних альтернатив і розрахунком імовірності їхнього результату, тож він є діалектичною єдністю об'єктивного та суб'єктивного. З цієї точки зору ризик ототожнюється з діяльністю, пов'язаною з подоланням невизначеності в ситуації неминучого вибору, в процесі якої існує можливість кількісно та якісно оцінити ймовірність досягнення передбачуваного результату, невдачі та відхилення від мети» (Пехник, Кройтор, Завгородня, 2019, с. 35).

Тому під час використання політичних технологій варто враховувати всі можливі особливості розвитку подій, усі можливі негативні наслідки та різні напрямки розвитку політичних процесів. Відповідно, до поданої інформації в різних інформаційних ресурсах, у різних регіонах сприйняття може бути інше, а отже, й рівень підтримки може бути різним.

Як названі ризики в сучасному суспільстві можна розглядати технології у кіберпросторі, оскільки кіберпростір не містить чіткої форми ієрархії взаємовідносин, окрім того, масштаби впливу (позитивного чи негативного) також неможливо передбачити, що створює умови нестабільного впливу на політичну свідомість, відсутність сталого та тривалого впливу на суспільство.

Для того, щоб більш детально звернути увагу на сучасні загрози кібертехнологій, варто зрозуміти, що міститься в понятті кіберпростору, а отже, які межі такого простору для застосування кібертехнологій. Кіберпростір – це «середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення (ПЗ) і послуг в Інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі; сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікації та обміну даними через системи, що функціонують в мережі Інтернет, та пов'язану з ними фізичну інфраструктуру; всі форми мережної та цифрової активності, що включають у себе контент і дії з їхньої обробки; інформаційна інфраструктура, доступна через Інтернет; комунікаційне середовище, що утворюється системою зв'язків між об'єктами кіберінфраструктури, серед яких слід виділити електронні обчислювальні машини, комп'ютерні мережі, ПЗ, інформаційні ресурси» (Завгородня, 2021, с. 54).

Політичні процеси, які відбуваються в сучасному кіберпросторі, мають серйозний вплив на наддержавному рівні. Важливий вплив на кіберпростір здійснює Китай, оскільки має власні погляди на систему функціонування кіберпростору, відмежувавшись від зовнішніх інформаційних систем та формуючи внутрішньодержавну інформаційну систему. Тому такий досвід важливий для українського суспільства. Адже правляча еліта під час порушення авторських чи інших прав, особливо в мережі Інтернет, лише констатує недосконалість правової бази. Однак конкретних заходів та вдосконалення правової системи не відбувається, а розвиток інформаційних потоків стає все стрімкішим, світогляд суспільства починає формуватись окремо від політичних основ та принципів, проголошених у суспільстві. Відбувається таке відмежування влади від суспільства і навпаки.

Єдиним серйозним санкційним рішенням щодо інформаційного простору було обмеження доступу до соціальних мереж, які належали до Російської Федерації як країни-агресора на території України. Проте в суспільстві існували неоднозначні погляди на такі обмеження, і супроводжувались вони протестами та обговореннями. Таким чином ми демонструємо можливість держави вплинути на агресора, навіть якщо таке політичне рішення буде непопулярним та зменшить рейтинги політичної еліти.

Значна кількість населення збільшує інтелектуальний потенціал, а відповідно, збільшується загальна картина економічної могутності держави. Звичайно, разом з позитивними аспектами виникає і ряд негативних, що спонукає органи управління до оподаткування перебільшення кількості дітей в одній сім'ї, що також можна споглядати як певне обмеження у праві на власний вибір подружжя. Сьогодні це питання не є загрозою для національних інтересів чи кардинальної зміни свідомості громадян, однак у випадку нашарування різних питань може слугувати одним із складових елементів суспільного невдоволення чи емоційного обурення.

Офіційна політична освіта серйозно впливає на політичну свідомість усіх суб'єктів політичного процесу. Вони не виходять за загальновстановлені межі дозволених політологічних знань, суб'єктивних припущень та власного бачення розвитку політичної системи Китаю. Чіткі межі для демократичної освітньої системи обмежують можливість здобувачів власному баченню та сприйняттю політичних рішень та подій. Однак на прикладі Китаю бачимо, що для формування нових ідей та планів громадяни Китаю обирають напрямки для прогресивного інформаційно-технологічного напрямку.

Враховуючи загальну позицію Китайської Народної Республіки щодо індивідуального бачення захисту національних інтересів та цінностей держави, чітко прослідковується стратегія сприйняття влади, політики, органів управління, політичного устрою та загалом політичної системи. Хоча механізм захисту ще не сформований в повному обсязі через об'єктивно-суб'єктивні причини, які важко вирішити з задоволенням інтересів суб'єктів політики внутрішніх та зовнішніх, а також і громадян країни.

Проте навіть такі досягнення є досить високими порівняно з іншими країнами світу. Великий відсоток країн дотепер не визначився з офіційною позицією щодо правового статусу кіберпростору та особливостей його функціонування всередині держави. Більшість держав світу продовжує діяти хаотично та ситуативно, у разі виникненні проблеми, яка набула публічного розголосу, намагаючись вплинути, обмежити, заборонити, але оскільки така діяльність не має чіткої системи дій, то вказаний процес стає довготривалим та неефективним.

Ще одним проблемним аспектом залишаються кібератаки, які можна розцінювати як сучасну форму нападу, що досить вдало застосовується суб'єктами політики, переважно мається на увазі наддержавна форма взаємного впливу. Агресора можливо виявити, але важко притягнути до будь-якої форми відповідальності, будь-які каральні форми впливу на міжнародній арені діють суб'єктивно, залежно від статусу на міжнародній арені такого політичного актора. Кібератаки, які використовуються під час проведення кібероперацій, можуть привести до дуже відчутних негативних наслідків. Наприклад, така атака, як вандалізм, «завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат. До таких кібернетичних атак можна віднести псування офіційних Інтернет-сторінок, заміну змісту образливими чи пропагандистськими малюнками» (Кібербезпека як важлива складова всієї системи захисту держави, 2018); атака-пропаганда проявляється в «розсилці спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення» (Кібербезпека як важлива складова всієї системи захисту держави, 2018). Так сталося на території Криму, на Донбасі. І слід зазначити, що ця атака у вигляді пропаганди почалася ще «задовго до 2014 року, велася постійно й була зосереджена на певній верстві населення, так званій цільовій аудиторії» (Кібербезпека як важлива складова всієї системи захисту держави, 2018); атака-збір інформації проявляється у формі «злому приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні. У цьому випадку дезінформація та викрадення даних, наприклад, відомостей щодо пересування наших військ у районі

ведення бойових дій, призведе до неминучих людських втрат. Інша назва — кібершпигунство» (Кібербезпека як важлива складова всієї системи захисту держави, 2018). Ще можна додати такі атаки, як відмова сервісу, втручання в роботу обладнання, вплив на об'єкти критичної інфраструктури тощо.

Враховуючи можливості КНР, її потенціал в інформаційно-технологічному напрямку, політичні лідери різних країн світу звертали увагу на можливість участі Китаю у кібератаках, однак будь-яких фактичних доказів та реальних санкцій публічно не оголошувалось. За таких обставин проєкти, які розроблені на міжнародній арені щодо кіберсфери та правил поведінки в інформаційному просторі, його захисту та безпеки продовжує перебувати у формі обговорення та дискусії. Усі ці кібератаки направлені на те, щоб дестабілізувати ситуацію в країні, а точніше: «Відключити, знищити, дестабілізувати – це їхня мета» (Кібербезпека як важлива складова всієї системи захисту держави, 2018).

Водночас позиція Китаю щодо індивідуального захисту формує протилежні моделі розвитку глобального кіберпростору. Перша модель можливого спрямування зосереджена на демілітаризацію кіберпростору та обмеження можливостей щодо створення віртуального поля військового та політичного протиборства. Друга модель спрямована на процес обговорення та висунення гіпотез можливого міжнародного, тобто наднаціонального захисту кіберпростору. Наукова спільнота також продовжує дискутувати та обговорювати різні можливі варіанти розвитку подій щодо захисту інформаційного простору. Такі дві позиції показують, що національні інтереси усіх країн світу будуть під серйозною загрозою, коли замовники будуть ламати системи та руйнувати інформаційні бази даних.

Сучасні міжнародні організації демонструють свою неспроможність впливати на цей процес. Наприклад, в Організації об'єднаних націй розроблено ряд рішень та резолюцій, однак фактично відсутній дієвий міжнародний документ, який ефективно допоможе врегулювати кібербезпеку у світі. Своєю чергою, індивідуальні бачення захисту, розроблені прогресивними країнами (наприклад США, КНР), також більшою мірою бажають підвищити захист власних держав, але на вищому наддержавному рівні. А отже, такі форми бачення захисту буде дуже важко регламентувати.

Для України важливою подією є розроблення та затвердження «Стратегії кібербезпеки України» (2021). Як зазначає А. Задубінний: «Стратегія кібербезпеки України визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» (Задубінний, 2021). У Стратегії визначено, що гарантування кібербезпеки «є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі». Стратегія акцентує на тому, шо «кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі» («Стратегія кібербезпеки України», 2021).

Аналізуючи ситуацію в кіберпросторі, роль прогресивних країн світу, особливості використання кібертехнологій в інформаційному просторі, можемо дійти висновку, що вітчизняна система взаємовідносин між суб'єктами політики та громадянами не може повністю перейти на цифрові форми впливу, для ефективності результату впливу потрібно застосовувати змішані форми впливу (загальноприйняті та кібертехнології). Необхідно користуватися та застосовувати зарубіжний досвід та практику. Тут слід погодитися з думкою К. Александера, який наголошує, що «говорити про проблему і зрозуміти її – це вже частина рішення. Ми говоримо про кібертехнології дуже неоднаково. Ми бачимо, які речі відбуваються, але ми не бачимо загальної картини. Необхідно разом працювати компаніям між собою, компаніям і секторам – з урядом, разом працювати і державам, аби вирішити цю проблему. Цю проблему нікому з нас в односторонньому порядку не вирішити. Вона може бути вирішеною лише

завдяки спільній роботі. Нам необхідно знайти відповіді на ці проблеми, адже виклик постане перед кожною країною. Ми повинні це вирішити не лише для України, але й для всього світу» (Круглі столи з питань безпеки, 2018).

Окрім того, під час застосування технологій в інформаційному просторі варто пам'ятати про різні рівні небезпек, які чекають на суб'єктів політики. Загрози у кіберпросторі можуть проявлятись у конфліктних формах активності та спонукати до агресивних дій окремі активістські групи. Попередженням таких негативних заходів є раціональна, об'єктивна та достовірна інформація, яка надходить з офіційних сторінок окремих політичних лідерів та формує об'єктивну інформацію про сучасний стан політичних подій та рішень.

Література

Ринковий Т. Політичні технології як складова публічної політики та управління на сучасному етапі державотворення. *Політологія і право.* 2009. № 11. С. 221–230.

Головатий М. Мистецтво здобувати владу. *Політ. менеджмент.* 2009. № 4(37). С. 221–230.

Каретна О.О., Милосердна І.М., Ігнатьєва І.І. Роль та особливості інформаційно-комунікаційних технологій у взаємодії органів державної влади з громадянським суспільством. *Політикус*. № 5. 2020. С. 62–66.

Пехник А.В., Кройтор А.В., Завгородня Ю.В. Теорія ризику: історія та сучасні підходи. Актуальні проблеми політики. № 63. 2019. С. 33–47.

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.

Круглі столи з питань безпеки: новини. Фонд Віктора Пінчука провів публічну панельну дискусію на тему кібербезпеки та дезінформації. URL: https://pinchukfund.org/ua/projects/25534/news/20271/

Задубінний А. Стратегія кібербезпеки України: цілі та пріоритети. 2021. URL: https://armyinform.com.ua/2021/08/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/.

«Стратегія кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021 / *Президент України*. URL: https://www.president.gov.ua/documents/4472021-40013

Кібербезпека як важлива складова всієї системи захисту держави, 2018. URL : https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

References

Rynkovyi T. (2009) Politychni tekhnolohii yak skladova publichnoi polityky ta upravlinnia na suchasnomu etapi derzhavotvorennia. [Political technologies as a component of public policy and management at the present stage of state formation] *Politolohiia i pravo.* no 11. pp. 221–230.

Holovatyi M. (2009) Mystetstvo zdobuvaty vladu. [The art of gaining power] *Polit. menedzhment*. no 4. pp. 221–230.

Karetna O.O., Myloserdna I.M., Ihnatieva I.I. (2020) Rol ta osoblyvosti informatsiino-komunikatsinykh tekhnolohii u vzaiemodii orhaniv derzhavnoi vlady z hromadianskym suspilstvom.[The role and features of information and communication technologies in the interaction of public authorities with civil society] *Politykus.* no 5. pp. 62–66.

Pekhnyk A.V., Kroitor A.V., Zavhorodnia Yu.V. (2019) Teoriia ryzyku: istoriia ta suchasni pidkhody.[Risk theory: history and modern approaches] *Aktualni problemy polityky*. no 63. pp. 33–47.

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". pp. 53–56.

Kruglyi stoly z pitan' bezpeki: novini. Fond Viktora Pinchuka proviv publichnu panel'nu diskusiyu na temu kiberbezpeki ta dezinformacii [The Victor Pinchuk Foundation held a public panel discussion on cybersecurity and misinformation]. URL: https://pinchukfund.org/ua/projects/25534/news/20271/

Zadubinnii A. (2021) Strategiya kiberbezpeki Ukraïni: cili ta prioriteti. [Ukraine's cybersecurity strategy: goals and priorities.] URL: https://armyinform.com.ua/2021/08/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/.

Ukaz Prezidenta Ukraïni vid 26 serpnya 2021 roku № 447/2021 «Strategiya kiberbezpeki ukraïni» [Cybersecurity strategy of Ukraine] URL: https://www.president.gov.ua/documents/4472021-40013

Kiberbezpeka yak vajliva skladova vsiєï sistemi zahistu derjavi (2018). [Kiberbezpeka yak vajliva skladova vsiї sistemi zahistu derjavi] URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

Анотація

Пехник А. В., Завгородня Ю. В. **Сучасні загрози кібертехнологій у політичному процесі. –** Стаття.

У колективному дослідженні здійснюється аналіз вітчизняних наукових поглядів щодо ролі політичних технологій у розвитку органів управління. Сучасні політичні процеси потрібно перелаштовувати під нові форми та різновиди політичного впливу на громадянське суспільство. Враховуючи особливості розвитку онлайн процесів спілкування, взаємодії, коментарів щодо різних дописів, підтримки або непідтримки у формі лайків окремих політичних діячів є ознакою інформатизації політичних процесів та долучення до політики в інформаційному просторі.

У зв'язку з цим у статті приділено увагу розвитку кібертехнологій як новітньої сфери взаємодії з суспільством. Однак цей напрям не містить нагромадженого наукового досвіду, а тому формує ряд загроз у використанні під час фактичного впливу на свідомість суспільства, що може містити різного роду ризики для самих суб'єктів політики. Така непередбачена реакція, публічна критика, спами, боти – це нові перешкоди, з якими потрібно зіткнутись на інформаційній платформі для політичних діячів.

Нинішня практика діяльності політичних груп у сучасних методах та заходах впливу на свідомість громадян зіштовхується з різними видами агресії та конфліктним сприйняттям, критикою політичної діяльності, оскільки політичні лідери можуть демонструвати вплив та досягнення на суспільно важливі рішення, які не входять до сфери їхніх прямих повноважень.

Використання кібертехнологій є сучасною формою впливу на свідомість суспільства. У кіберпросторі використовується позитивна та негативна форма технологічних прийомів. Вітчизняна кіберплатформа не забезпечує належного захисту прав та інтересів як суб'єктів політики, так і громадян, що демонструє потребу в удосконаленні чинного законодавства. Політичні процеси виходять на глобальний рівень з використанням кібертехнологій та інформаційного простору загалом.

Ключові слова: кіберпростір, кібертехнології, політичні конфлікти, політична свідомість, кібератака, громадянське суспільство, політичні суб'єкти.

Summary

Pekhnik A. V., Zavgorodnya Yu. V. **Modern threats of cyber technologies in political process. –** Article.

The collective research analyzes domestic scientific views on the role of political technologies in the development of government. Modern political processes need to be readjusted to new forms and varieties of political influence on civil society. Given the peculiarities of the development of online processes of communication, interaction, comments on various posts, support or disapproval in the form of likes of individual politicians is a sign of informatization of political processes and involvement in politics in the information space.

In this regard, the article focuses on the development of cyber technology as a new area of interaction with society. However, this area does not contain the accumulated scientific experience, and therefore creates a number of threats in the use of the actual impact on the consciousness of society, which may contain various risks for the policy actors themselves. Such unpredictable reaction, public criticism, spam, bots, these are new obstacles that need to be faced on the information platform for politicians.

The current practice of political groups in modern methods and measures to influence the minds of citizens is faced with various types of aggression and conflict perception, criticism of political activity, as political leaders can demonstrate influence and achievement on socially important decisions outside their direct authority.

The use of cyber technologies is a modern form of influencing the consciousness of society. In cyberspace, the call sign and the negative form of technological techniques are used. Domestic cyber platform does not provide adequate protection of the rights and interests of politicians and citizens, which demonstrates the need to improve existing legislation. Political processes are reaching the global level with the use of cyber technologies and the information space in general.

Key words: cyberspace, cyber technologies, political conflicts, political consciousness, cyberattack, civil society, political actors.