УДК 351.82:004.056:316.774

https://doi.org/10.52058/2786-5274-2026-2(54)-177-189

Климчук Олександр Васильович доктор економічних наук, професор, професор кафедри публічного управління та менеджменту, Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, https://orcid.org/0000-0002-9427-9561

Лазор Оксана Дмитрівна доктор наук з державного управління, професор, професор кафедри публічного управління та менеджменту, Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, https://orcid.org/0000-0001-7699-8338

Яременко Олександр Іванович кандидат наук з державного управління, доцент, декан факультету права, публічного управління і менеджменту, Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, https://orcid.org/0000-0002-3053-2257

ІННОВАЦІЙНІ МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ПРОТИДІЇ ДЕСТРУКТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ В ІНТЕРНЕТ-СЕРЕДОВИЩІ: КОНЦЕПТУАЛЬНИЙ АСПЕКТ

Анотація. У статті досліджено теоретико-методологічні та концептуальні засади формування інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам в інтернет-середовищі в умовах цифрової трансформації та гібридних загроз. Обґрунтовано, що деструктивні інформаційні впливи становлять одну з ключових загроз національній безпеці України, демократичним інститутам і стабільності суспільства, а ефективна протидія їм потребує переходу від реактивних до проактивних управлінських підходів.

Визначено, що традиційні адміністративно-правові та комунікаційні інструменти публічного управління є недостатніми в умовах високої динаміки цифрового середовища, що зумовлює необхідність інтеграції інноваційних технологій, зокрема предиктивних інструментів штучного інтелекту, у систему державного управління інформаційною безпекою. Доведено, що ефективність таких рішень можлива лише за умови нормативно-правової гармонізації, узгодженої з європейськими та міжнародними стандартами, а також дотримання принципів законності, прозорості й захисту прав людини.

Запропоновано концептуальну модель інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам, що поєднує предиктивний технологічний, нормативно-правовий, соціально-

комунікаційний та інституційний блоки. Обґрунтовано, що важливою складовою цієї моделі є формування соціальної стійкості суспільства шляхом розвитку медіаграмотності, критичного мислення та стратегічних комунікацій. Реалізація запропонованих підходів сприятиме підвищенню ефективності реагування органів публічної влади на інформаційні загрози, зміцненню довіри громадян та формуванню безпечного і стійкого інформаційного простору України.

Ключові слова: публічне управління, інформаційна безпека, деструктивні інформаційні впливи, гібридні загрози, інноваційна діяльність, штучний інтелект, цифрова трансформація, національна стійкість.

Klymchuk Oleksandr Vasylovych Doctor of Economics, Professor, Professor of the Department of Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, https://orcid.org/0000-0002-9427-9561

Lazor Oksana Dmytrivna Doctor of Sciences in Public Administration, Professor, Professor of the Department of Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, https://orcid.org/0000-0001-7699-8338

Yaremenko Oleksandr Ivanovych Candidate of Sciences in Public Administration, Associate Professor, Dean of the Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, https://orcid.org/0000-0002-3053-2257

INNOVATIVE MECHANISMS OF PUBLIC GOVERNANCE IN COUNTERING DESTRUCTIVE INFORMATION INFLUENCES IN THE INTERNET ENVIRONMENT: A CONCEPTUAL ASPECT

Abstract. The article examines the theoretical, methodological, and conceptual foundations for the formation of innovative mechanisms of public governance in the field of countering destructive information influences in the Internet environment under conditions of digital transformation and hybrid threats. It is substantiated that destructive information influences constitute one of the key threats to Ukraine’s national security, democratic institutions, and social stability, and that effective counteraction to them requires a shift from reactive to proactive governance approaches.

It is determined that traditional administrative, legal, and communication instruments of public governance are insufficient in the context of the high dynamics of the digital environment, which necessitates the integration of innovative technologies—particularly predictive artificial intelligence tools—into the system of state governance of information security. It is proved that the effectiveness of such

solutions is possible only under conditions of regulatory and legal harmonization aligned with European and international standards, as well as adherence to the principles of legality, transparency, and protection of human rights.

A conceptual model of innovative mechanisms of public governance in countering destructive information influences is proposed, combining predictive technological, regulatory-legal, socio-communication, and institutional components. It is substantiated that an important element of this model is the formation of societal resilience through the development of media literacy, critical thinking, and strategic communications. The implementation of the proposed approaches will contribute to improving the effectiveness of public authorities' responses to information threats, strengthening public trust, and forming a safe and resilient information space in Ukraine.

Keywords: public governance, information security, destructive information influences, hybrid threats, innovation activity, artificial intelligence, digital transformation, national resilience.

Постановка проблеми. У сучасному цифровізованому суспільстві інформаційна сфера стала одним із ключових вимірів у системі національної безпеки та публічного управління, адже саме в інтернет-середовищі формуються суспільні настрої, політичні уподобання та моделі соціальної поведінки. Стрімкий розвиток інформаційно-комунікаційних технологій, соціальних мереж і цифрових платформ суттєво розширив можливості доступу до інформації, проте водночас створив передумови для поширення деструктивних інформаційних впливів, зокрема дезінформації, маніпулятивного контенту, інформаційно-психологічних операцій та кібератак. Такі явища становлять серйозну загрозу для демократичних інститутів, суспільної стабільності та ефективності публічного управління.

Для України, яка вже досить тривалий період перебуває в умовах гібридної війни, цифрової трансформації державного управління та глибоких соціально-політичних змін, проблема протидії деструктивним інформаційним впливам в інтернет-середовищі набуває особливої актуальності. Систематичні інформаційні атаки спрямовані на підрив довіри громадян до органів публічної влади, дестабілізацію суспільно-політичної ситуації, маніпулювання громадською думкою та спотворення стратегічних пріоритетів подальшого державного розвитку. Водночас традиційні адміністративно-правові та комунікаційні інструменти публічного управління часто виявляються недостатньо ефективними в умовах високої швидкості поширення інформації та складності цифрових комунікаційних мереж. За таких умов особливої значущості набуває впровадження інноваційних механізмів публічного управління, що поєднують цифрові технології, аналітичні інструменти, міжсекторальну взаємодію та проактивні управлінські підходи у сфері інформаційної безпеки. В Україні й досі спостерігається фрагментарність державної політики у цій сфері, недостатня

координація між органами публічної влади, обмежене використання штучного інтелекту, великих даних і стратегічних комунікацій, а також відсутність цілісної концептуальної моделі публічного управління протидією деструктивним інформаційним впливам.

Відтак, існує об'єктивна необхідність теоретичного осмислення та наукового обґрунтування інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам в інтернет-середовищі. Розв'язання цієї проблеми безпосередньо пов'язане з важливими науковими та практичними завданнями, зокрема розвитком теорії публічного управління в умовах цифровізації, формуванням ефективної державної інформаційної політики, удосконаленням системи стратегічних комунікацій, підвищенням стійкості суспільства до інформаційних загроз та забезпеченням належного рівня національної безпеки. Впровадження концептуально обґрунтованих інноваційних управлінських механізмів сприятиме підвищенню ефективності діяльності органів публічної влади, зміцненню довіри громадян та формуванню сталого і безпечного інформаційного простору України.

Аналіз останніх досліджень і публікацій. Проведений аналіз наукових досліджень і публікацій вказує на те, що проблематика публічного управління у сфері протидії деструктивним інформаційним впливам, зокрема в інтернет-середовищі, перебуває у фокусі уваги як українських, так і зарубіжних учених. Теоретико-методологічні засади інформаційної безпеки держави, управління інформаційними процесами та протидії інформаційним загрозам розкрито у працях таких науковців, як І. Андрушко, Ю. Битяк, О. Буряченко, А. Войціховський, С. Глобенко, В. Горбулін, О. Дзьобань, І. Єфименко, Г. Заворітня, О. Коваль, Г. Красноступ, В. Ліпкан, О. Пархоменко-Куцевіл, С. Петькун, Г. Почепцов, І. Рущенко, Г. Ситник, О. Сосніна, С. Телешун, О. Ткаченко, М. Требін, Ю. Уздєнової а також зарубіжних дослідників: Б. Бімбера, М. Кастельса, Дж. Ная, Г. Лассвелла, М. Маклюена, Т. Ріда, К. Санстейна та інших. У наукових публікаціях зазначених авторів ґрунтовно досліджуються питання інформаційної безпеки, стратегічних комунікацій, інформаційно-психологічного впливу, цифрових загроз та гібридних форм інформаційного протиборства. Значна увага приділяється ролі державних інституцій у забезпеченні інформаційного суверенітету, формуванню нормативно-правових механізмів протидії дезінформації, а також розвитку системи публічних комунікацій в умовах цифровізації суспільства. Окремий пласт досліджень присвячено аналізу впливу соціальних мереж, онлайн-платформ та цифрових медіа на суспільно-політичні процеси, громадську думку та державну стабільність.

Водночас, попри значну кількість наукових напрацювань, низка аспектів означеної проблематики залишається недостатньо дослідженою. Зокрема, потребують подальшого наукового осмислення інноваційні механізми публічного управління, спрямовані на системну та проактивну протидію деструктивним

інформаційним впливам саме в інтернет-середовищі, з урахуванням сучасних цифрових технологій, алгоритмічних систем, штучного інтелекту та мережевої динаміки інформаційних процесів. Недостатньо розробленими залишаються концептуальні підходи до інтеграції інноваційних управлінських інструментів у діяльність органів публічної влади у сфері інформаційної безпеки. Саме ці невирішені раніше складові загальної проблеми зумовлюють необхідність подальших досліджень і визначають наукову спрямованість статті.

Мета статті – теоретичне обґрунтування та розробка концептуальної моделі інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам в інтернет-середовищі, що базуються на інтеграції предиктивних технологій штучного інтелекту, нормативно-правової гармонізації та стратегій соціальної стійкості в умовах сучасних викликів для підвищення ефективності реагування органів публічної влади на існуючі інформаційні загрози та зміцнення інформаційної безпеки держави.

Виклад основного матеріалу. Наразі світова спільнота опинилася в епіцентрі безпрецедентної трансформації інформаційного простору, де межі між фізичною реальністю та цифровим середовищем стали остаточно розмитими.

Стрімка цифровізація всіх сфер життєдіяльності, що стала ключовим пріоритетом публічного управління в Україні та провідних країнах світу, принесла не лише колосальні переваги у вигляді прозорості та ефективності державних послуг, а й створила нове поле для глобальних конфліктів. Інтернет-середовище перетворилося на основний театр воєнних дій у межах гібридної агресії, де деструктивні інформаційні впливи (ДІВ) використовуються як високоточна зброя для підриву національної стійкості, дестабілізації суспільних інститутів та маніпулювання масовою свідомістю.

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням ролі інтернет-середовища як ключового простору формування суспільної свідомості, політичних наративів і соціальних практик. Поряд із позитивними можливостями цифровізації, інформаційно-комунікаційні технології стали інструментом масштабних деструктивних інформаційних впливів, що становлять серйозну загрозу національній безпеці, демократичним інститутам та соціальній стабільності держави. У цих умовах традиційні адміністративні та правові механізми публічного управління виявляються недостатньо ефективними, що зумовлює потребу в розробці інноваційних управлінських підходів, здатних забезпечити проактивне реагування на інформаційні загрози, які виникають під час гібридної війни.

Ефективна боротьба з гібридними загрозами в сучасному світі вимагає застосування постійної адаптації та широкого спектру заходів. Використання противником різних дієвих інструментів – від дезінформації до кібератак, вказує на необхідність формування гнучкої гібридної оборони. Така боротьба неодмінно потребує співпраці на міжнародному рівні та використання міжнародного досвіду (зокрема, співпраця з Європейським Союзом, НАТО та іншими

демократичними країнами, що вже мають відпрацьовані на практиці моделі реагування на різного роду інформаційні загрози) [1, 2].

Гібридні загрози і війну потрібно розглядати як багатофакторний процес із застосуванням сучасних інформаційних систем і технологій в управлінській діяльності, що передбачає комплексне використання агресором різноманітних комбінацій: передусім таких, як політичних, економічних, організаційних, соціальних, інформаційних, військових, кібернетичних, конвенційних, іррегулярних, терористичних та підривних важелів впливу [3, 4]. Для удосконалення державних механізмів запобігання та протидії небезпекам, які виникають в умовах гібридної війни, застосовують досить широкий спектр питань, вирішення яких спрямовані на забезпечення стійкості державних інституцій та посилення їх безпекового потенціалу. Однак, гібридна війна створює нові небезпеки Україні, на які неможливо ефективно реагувати лише використовуючи інституційні засоби. Тому за таких умов критично важливою стає роль громадянського суспільства як активного суб'єкта, здатного підтримувати й зміцнювати національну стійкість [5].

Інформаційний простір перетворився на ключову арену ведення гібридної війни, де застосовувані дезінформаційні та маніпулятивні кампанії стали одним з основних інструментів зовнішнього та внутрішнього впливу на державу [6]. З позицій публічного управління протидія таким загрозам не може обмежуватися реактивними заходами або виключно силовими інструментами. Вона потребує системного підходу, що передбачає інтеграцію управлінських рішень, нормативно-правового регулювання, цифрових технологій та соціальних механізмів підвищення стійкості суспільства. Саме тому концепція інноваційних механізмів публічного управління набуває особливого значення, оскільки дозволяє поєднати технологічні новації з управлінською логікою та публічними цінностями. Для публічного управління сфера протидії деструктивним інформаційним впливам є критично важливою, оскільки вона напряму пов'язана зі здатністю держави забезпечувати правопорядок, соціальну злагоду та довіру громадян до владних інституцій. Глобальний звіт про ризики минулого 2025 р. визначає процеси дезінформації та мізінформації як одну з топ-загроз на період найближчого десятиліття, що здатні провокувати соціальну поляризацію та здійснювати ерозію прав людини.

Проблематика різного роду дезінформаційних і маніпулятивних впливів в інформаційному просторі України відзначається комплексним і багатовимірним характером, а тому потребує використання системного підходу у сфері публічного управління. Інформаційна безпека сьогодні є вагомою складовою національної безпеки, а її якісне забезпечення в умовах гібридної війни має визначальний вплив на політичну стабільність, суспільну довіру та ефективність державного управління [7]. В умовах України, яка понад десятиліття перебуває під прицілом потужної інформаційної машини агресора, ця проблема набуває екзистенційного характеру. Використовувані традиційні ієрархічні моделі

державного управління, засновані на лінійному регулюванні та вертикальних взаємозв'язках, демонструють свою неспроможність у динамічному та анонімному інтернет-середовищі. Сьогодні ми спостерігаємо ситуацію, коли швидкість поширення деструктивного контенту, згенерованого штучним інтелектом, випереджає здатність бюрократичних систем до адекватного реагування. Це ставить перед наукою та практикою публічного управління нагальне завдання розробки нових, гнучких концептуальних аспектів управління, які б інтегрували технологічні інновації із соціальними стратегіями захисту національних інтересів країни.

За умов існуючого воєнного стану та негативного впливу війни на українське суспільство інформаційна безпека, насамперед, зосереджена на захисті критично важливої цифрової інфраструктури, захисті даних громадян від компрометації та контролі вхідного потоку інформації, щоб запобігти її використанню у якості зброї зловмисниками. Така ситуація вимагає вдосконалення законодавства для захисту державних інформаційних систем, посилення заходів кібербезпеки громадян та державних установ, а також використання технологій шифрування для забезпечення конфіденційності даних в умовах існуючих гібридних загроз [8, 9]. Оновлення нормативно-правової бази є ключовим елементом розвитку та забезпечення інформаційної безпеки, оскільки ефективне регулювання у сфері інформаційної безпеки вимагає чітких стандартів і процедур, які б одночасно враховували технічні, організаційні та етичні аспекти [10].

Також в сучасних умовах необхідно враховувати ефективність публічно-управлінських інструментів щодо забезпечення інформаційної безпеки організацій та підприємств України на основі розвитку інформаційних систем і технологій. Її доцільно розкривати у вигляді комплексної характеристики, що поєднує в собі нормативно-правову визначеність, інституційну спроможність, наглядові та стимулюючі механізми, якісну координацію реагування, а також практичну здатність усіх секторів національної економіки підтримувати безперервність критичних процесів, зокрема платежів і соціально значущих сервісів. Результативність буде зростати лише тоді, коли правила стають зрозумілими й вимірюваними, контроль переходить від формальної перевірки документації до реального оцінювання процесів і фактичної готовності, а корпоративні стимули орієнтовані на інвестиції в стійкість, включно з резервним живленням, дублюванням каналів зв'язку, безпечною хмарною інфраструктурою, навчанням персоналу та перевіркою постачальників [11, 12].

Ефективна протидія наявним фейковим повідомленням неможлива без налагодження довіри суспільства до органів публічної влади, що вимагає прозорості у прийнятті відповідних управлінських рішень та послідовності у комунікаційній політиці [13]. Наші реалії полягають у переході від "масової дезінформації" до "персоналізованої маніпуляції". Завдяки використанню великих даних (Big Data) та алгоритмів штучного інтелекту, деструктивні

суб'єкти отримують можливість сегментувати аудиторію за психотипами, ціннісними орієнтирами та емоційними тригерами, доставляючи кожному користувачу саме той контент, який з найбільшою ймовірністю змінить його поведінку. При цьому інноваційні механізми публічного управління у сфері протидії деструктивним інформаційним впливам доцільно розглядати як сукупність взаємопов'язаних інструментів, методів і процесів, спрямованих на запобігання, виявлення, нейтралізацію та мінімізацію негативного впливу інформаційних загроз. Їх ключовою ознакою є орієнтація не лише на усунення наслідків, а й на прогнозування потенційних ризиків.

На сучасному етапі деструктивні інформаційні впливи (ДІВ) перестали бути лише побічним продуктом політичної боротьби. В контексті публічного управління ДІВ необхідно розглядати як системну, а іноді й автоматизовану діяльність суб'єктів, що чітко спрямована на поширення викривленого контенту з метою завдання шкоди національним інтересам, дестабілізації державного управління або порушення соціальної єдності. Особливу роль у цьому контексті відіграють предиктивні технології штучного інтелекту, які дозволяють аналізувати великі масиви даних з відкритих джерел, соціальних мереж та онлайн-платформ, виявляти аномальні інформаційні патерни та прогнозувати розвиток інформаційних кампаній. Використання таких технологій у публічному управлінні створює передумови для переходу від реактивної до проактивної моделі управління інформаційною безпекою.

Водночас масове впровадження штучного інтелекту в управлінську практику органів публічної влади потребує чіткого нормативно-правового забезпечення, щоб гарантувати дотримання таких основних принципів, як законність, прозорість, захист персональних даних та прав людини. Тому інноваційні технології повинні функціонувати в межах гармонізованої правової системи, узгодженої з міжнародними стандартами та європейськими підходами у сфері цифрового врядування.

Саме тому нормативно-правова гармонізація у сфері протидії деструктивним інформаційним впливам передбачає узгодження національного законодавства з міжнародними правовими актами, а також міжгалузеву координацію правових норм, що регулюють інформаційну, кібернетичну та національну безпеку. В умовах євроінтеграційного курсу України особливої актуальності набуває адаптація правових механізмів до стандартів Європейського Союзу у сфері боротьби з дезінформацією та захисту цифрового простору.

Гармонізація нормативно-правової бази дозволяє створити єдине інституційне середовище для впровадження інноваційних управлінських рішень, мінімізувати правові колізії та підвищити ефективність взаємодії між органами публічної влади. Вона також сприяє формуванню чітких процедур використання технологій штучного інтелекту в управлінській діяльності, що є необхідною умовою їх легітимності та суспільної довіри.

Важливим компонентом інноваційних механізмів публічного управління виступають стратегії соціальної стійкості, які спрямовані на підвищення здатності суспільства протистояти деструктивним інформаційним впливам. Соціальна стійкість включає розвиток критичного мислення, медіаграмотності, довіри до публічних інституцій та ефективної системи стратегічних комунікацій.

З позицій публічного управління формування соціальної стійкості є довгостроковим завданням, що потребує комплексних міжсекторальних зусиль. Органи публічної влади мають виступати координаторами взаємодії державного, приватного та громадського секторів у сфері інформаційної безпеки, забезпечуючи синергію управлінських рішень і суспільних ініціатив.

На основі проведеного теоретичного аналізу доцільно запропонувати концептуальну модель інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам в інтернет-середовищі. Її ключовими складовими є такі:

1) предиктивний технологічний блок, який заснований на використанні штучного інтелекту та аналітики великих даних;

2) нормативно-правовий блок, що забезпечує правову визначеність і гармонізацію управлінських рішень органів публічної влади;

3) соціально-комунікаційний блок, орієнтований на підвищення соціальної стійкості та ефективності публічних комунікацій між зацікавленими сторонами;

4) інституційний блок, який забезпечує координацію суб’єктів публічного управління.

Запропонована модель дозволяє інтегрувати інноваційні технології в систему публічного управління з урахуванням правових і соціальних обмежень, що сприяє підвищенню ефективності реагування органів публічної влади на наявні інформаційні загрози. Це дозволяє розглядати протидію деструктивним інформаційним впливам як комплексне управлінське завдання, а не сукупність розрізнених заходів.

Відтак, за сучасних умов публічне управління має еволюціонувати від ролі “державного цензора” до ролі “архітектора безпечної екосистеми”, де механізми управління спрямовані не лише на блокування шкідливого контенту, а на формування когнітивного імунітету суспільства. Практичне значення результатів дослідження полягає у можливості їх використання органами публічної влади при формуванні державної політики у сфері інформаційної безпеки, розробці стратегій цифрового врядування та вдосконаленні механізмів міжінституційної взаємодії.

Висновки. Підсумовуючи отримані результати необхідно відзначити, що в умовах стрімкої цифровізації та тривалої гібридної агресії проти України деструктивні інформаційні впливи в інтернет-середовищі перетворилися на один із ключових чинників загроз національній безпеці, демократичним інститутам і ефективності публічного управління. Інформаційний простір набув ознак самостійного середовища стратегічного протиборства, у якому традиційні

адміністративно-правові інструменти державного управління демонструють обмежену результативність. Доведено, що протидія деструктивним інформаційним впливам не може ґрунтуватися виключно на реактивних або заборонних підходах. Вона потребує системного, проактивного та інноваційного характеру, що передбачає інтеграцію сучасних цифрових технологій, передусім предиктивних інструментів штучного інтелекту, з управлінськими, нормативно-правовими та соціально-комунікаційними механізмами публічного управління.

У межах дослідження уточнено наукове розуміння інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам як комплексної системи взаємопов'язаних інструментів, процесів і інституційних рішень, спрямованих не лише на нейтралізацію інформаційних загроз, а й на їх раннє виявлення, прогнозування та мінімізацію потенційних негативних наслідків для держави й суспільства. Обґрунтовано ключову роль нормативно-правової гармонізації як інституційної основи впровадження інноваційних управлінських рішень. Встановлено, що ефективне використання технологій штучного інтелекту в діяльності органів публічної влади можливе лише за умови наявності чітких, прозорих і узгоджених із міжнародними стандартами правових рамок, які забезпечують баланс між безпековими потребами держави та захистом прав і свобод людини.

Визначено, що важливою складовою протидії деструктивним інформаційним впливам є формування соціальної стійкості суспільства, яка передбачає розвиток критичного мислення, медіаграмотності, довіри до інститутів публічної влади та ефективних стратегічних комунікацій. З позицій публічного управління соціальна стійкість розглядається як довгостроковий управлінський ресурс, що суттєво знижує вразливість суспільства до маніпулятивних та дезінформаційних кампаній.

На основі узагальнення теоретичних підходів і практичних викликів запропоновано концептуальну модель інноваційних механізмів публічного управління у сфері протидії деструктивним інформаційним впливам в інтернет-середовищі, яка включає предиктивний технологічний, нормативно-правовий, соціально-комунікаційний та інституційний блоки. Запропонована модель дозволяє розглядати протидію інформаційним загрозам як цілісне управлінське завдання та створює передумови для підвищення ефективності реагування органів публічної влади на сучасні виклики інформаційної безпеки. Практичне значення результатів дослідження полягає у можливості їх використання при формуванні та реалізації державної інформаційної політики, удосконаленні системи стратегічних комунікацій, розробці національних програм цифрового врядування, а також у процесі підвищення інституційної спроможності органів публічної влади в умовах гібридних загроз.

Перспективними напрямами подальших наукових досліджень у даній сфері є проведення поглибленого аналізу практичних механізмів інтеграції предиктивних технологій штучного інтелекту в управлінські процеси органів

публічної влади з урахуванням етичних, правових і організаційних обмежень. Доцільним є розроблення методик оцінювання ефективності інноваційних механізмів публічного управління у сфері інформаційної безпеки, зокрема показників соціальної стійкості та рівня довіри до публічних інституцій. Окремої уваги потребують дослідження інституційних моделей міжсекторальної взаємодії держави, бізнесу і громадянського суспільства у протидії деструктивним інформаційним впливам та вивчення впливу генеративних технологій штучного інтелекту на трансформацію дезінформаційних практик та розробка адаптивних управлінських рішень у відповідь на ці процеси для формування ефективної, стійкої й безпечної системи державного управління інформаційним простором України.

Література:

1. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління.* 2024. №о 2 (74), С. 24–31. DOI: https://doi.org/10.32689/2523-4625-2024-2(74)-3.

2. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна.* 2020. Вип.29. 2020. С. 281–288. DOI: https://doi.org/10.26565/2075-1834-2020-29-38.

3. Климчук О. В. Сучасні аспекти використання інформаційних систем і технологій в управлінні. *Бізнес, інновації, менеджмент: проблеми та перспективи:* збірник тез доповідей II Міжнародної науково-практичної конференції. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. С. 170–171.

4. Уздєнова Ю. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування.* 2024. Том 35 (74). № 4. С. 172–178. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/26.

5. Ситник Г. П., Заворітня Г. В. Гібридна війна як виклик національній стійкості: державно-управлінські механізми реагування у контексті досвіду України. *Успіхи і досягнення у науці*. 2025. № 3 (13). С. 601–613. DOI: https://doi.org/10.52058/3041-1254-2025-3(13)-601-613.

6. Глобенко С. В. Публічне управління захистом інформаційного простору в умовах надзвичайних ситуацій: дис. ... д-ра філософії: 28 – Публічне управління та адміністрування; Інститут державного управління та наукових досліджень з цивільного захисту ДСНС України. Київ, 2024.177 с.

7. Петькун С., Андрушко І. Механізми інформаційної безпеки у сфері публічного управління для протидії дезінформаційним і маніпулятивним кампаніям в Україні. *Успіхи і досягнення у науці*. 2025. № 8 (18). С. 646–654. DOI: https://doi.org/10.52058/3041-1254-2025-8(18)-646-654.

8. Самборська О.Ю., Климчук О.В. Негативний вплив війни на зайнятість та доходи українців. *Інноваційна економіка.* 2023. №3 (95). С. 63–69. DOI: https://doi.org/10.37332/2309-1533.2023.3.8.

9. Єфименко І. Інформаційна безпека держави в умовах воєнного стану: особливості забезпечення. *Успіхи і досягнення у науці*. 2025. № 10 (20). С. 96–105. DOI: https://doi.org/10.52058/3041-1254-2025-10(20)-96-105.

10. Пархоменко-Куцевіл О. Концептуальні засади впровадження цифровізації як виклику для формування інформаційної безпеки. *Успіхи і досягнення у науці*. 2025. № 8 (18). С. 599–608. DOI: https://doi.org/10.52058/3041-1254-2025-8(18)-599-608.

11. Климчук О.В. Сучасні процеси розвитку в Україні інформаційних систем і технологій в управлінні підприємствами. *Актуальні проблеми, пріоритетні напрямки та стратегії розвитку України:* тези доповідей І Міжнародної науково-практичної онлайн-конференції. Ред. колегія О. С. Волошкіна та ін. Київ: ІТТА, 2021. С. 199–201.

12. Ткаченко О. Ефективність публічно-управлінських інструментів забезпечення інформаційної безпеки організацій та підприємств України. *Успіхи і досягнення у науці*. 2025. № 12 (22). С. 1440–1450. DOI: https://doi.org/10.52058/3041-1254-2025-12(22)-1440-1450.

13. Красноступ Г.М. Нова стратегія інформаційної безпеки: правова відповідь на російське інформаційне маніпулювання та втручання. *Інформація і право.* 2025. № 2(53). С. 136-146. DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334149.

References:

1. Buriachenko, O. (2024). Hibrydna viina yak nova forma hlobalnoho protystoiannia [Hybrid war as a new form of global confrontation]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia – Scientific Works of the Interregional Academy of Personnel Management. Political Sciences and Public Administration, 2 (74),* 24–31. Retrieved from DOI: https://doi.org/10.32689/2523-4625-2024-2(74)-3. [in Ukrainian].

2. Voitsikhovskyi, A. V. (2020). Informatsiina bezpeka yak skladova systemy natsionalnoi bezpeky (mizhnarodnyi i zarubizhnyi dosvid) [Information security as a component of the national security system (international and foreign experience)]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina – Bulletin of V. N. Karazin Kharkiv National University, 29,* 281–288. Retrieved from DOI: https://doi.org/10.26565/2075-1834-2020-29-38. [in Ukrainian].

3. Klymchuk, O. V. (2021). Suchasni aspekty vykorystannia informatsiinykh system i tekhnolohii v upravlinni [Modern aspects of using information systems and technologies in management]. *Biznes, innovatsii, menedzhment: problemy ta perspektyvy: zbirnyk tez dopovidei II Mizhnarodnoi naukovo-praktychnoi konferentsii – Business, innovation, management: problems and prospects: collection of abstracts of the II International scientific and practical conference.* Kyiv: KPI im. Ihoria Sikorskoho, Vyd-vo «Politekhnika», 170-171 [in Ukrainian].

4. Uzdienova, Yu. (2024). Hibrydna viina: sutnist, skladovi ta kliuchovi poniattia [Hybrid war: essence, components and key concepts]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia – Scientific Notes of V. I. Vernadsky Taurida National University. Series: Public Administration, Vol. 35 (74), 4,* 172–178. Retrieved from DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/26. [in Ukrainian].

5. Sytnyk, H. P., & Zavoritnia, H. V. (2025). Hibrydna viina yak vyklyk natsionalnii stiikosti: derzhavno-upravlinski mekhanizmy reahuvannia u konteksti dosvidu Ukrainy [Hybrid war as a challenge to national resilience: public administration response mechanisms in the context of Ukraine's experience]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science, 3 (13),* 601–613. Retrieved from DOI: https://doi.org/10.52058/3041-1254-2025-3(13)-601-613 [in Ukrainian].

6. Hlobenko, S. V. (2024). Publichne upravlinnia zakhystom informatsiinoho prostoru v umovakh nadzvychainykh sytuatsii [Public administration of information space protection under emergency conditions] (Doctor of Philosophy dissertation, Specialty 28 – Public Administration and Management). Institute of Public Administration and Research in Civil Protection of the State Emergency Service of Ukraine, Kyiv, 177 p. [in Ukrainian].

7. Petkun, S., Andrushko, I. (2025). Mekhanizmy informatsiinoi bezpeky u sferi publichnoho upravlinnia dlia protydii dezinformatsiinym i manipulatyvnym kampaniiam v Ukraini [Information security mechanisms in public administration to counter disinformation and manipulative campaigns in Ukraine]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science, 8 (18),* 646–654. Retrieved from DOI: https://doi.org/10.52058/3041-1254-2025-8(18)-646-654 [in Ukrainian].

8. Samborska, O.Yu., & Klymchuk, O.V. (2023). Nehatyvnyi vplyv viiny na zainiatiist ta dokhody ukraintsiv [Negative impact of war on employment and incomes of Ukrainians]. *Innovatsiina ekonomika – Innovative Economy, 3(95),* 63–69. Retrieved from DOI: https://doi.org/10.37332/2309-1533.2023.3.8 [in Ukrainian].

9. Yefymenko, I. (2025). Informatsiina bezpeka derzhavy v umovakh voiennoho stanu: osoblyvosti zabezpechennia [State information security under martial law: features of provision]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science, 10 (20),* 96–105. Retrieved from DOI: https://doi.org/10.52058/3041-1254-2025-10(20)-96-105 [in Ukrainian].

10. Parkhomenko-Kutsevil, O. (2025). Kontseptualni zasady vprovadzhennia tsyfrovyzatsii yak vyklyku dlia formuvannia informatsiinoi bezpeky [Conceptual foundations of digitalization implementation as a challenge for information security formation]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science, 8 (18),* 599–608. Retrieved from DOI: https://doi.org/10.52058/3041-1254-2025-8(18)-599-608 [in Ukrainian].

11. Klymchuk, O. V. (2021). Suchasni protsesy rozvytku v Ukraini informatsiinykh system i tekhnolohii v upravlinni pidpryiemstvamy [Current development processes of information systems and technologies in enterprise management in Ukraine]. In O. S. Voloshkin et al. (Eds.), Aktualni problemy, priorytetni napriamky ta stratehii rozvytku Ukrainy: tezy dopovidei I Mizhnarodnoi naukovo-praktychnoi onlain-konferentsii [Topical issues, priority directions, and development strategies of Ukraine: Proceedings of the 1st International Scientific and Practical Online Conference], 199–201. Kyiv: ITTA [in Ukrainian].

12. Tkachenko, O. (2025). Efektyvnist publichno-upravlinskykh instrumentiv zabezpechennia informatsiinoi bezpeky orhanizatsii ta pidpryiemstv Ukrainy [Effectiveness of public administration tools for ensuring information security of organizations and enterprises in Ukraine]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science, 12 (22),* 1440–1450. Retrieved from DOI: https://doi.org/10.52058/3041-1254-2025-12(22)-1440-1450 [in Ukrainian].

13. Krasnostup, H. M. (2025). Nova stratehiia informatsiinoi bezpeky: pravova vidpovid na rosiiske informatsiine manipuliuvannia ta vtruchannia [New information security strategy: legal response to Russian information manipulation and interference]. *Informatsiia i pravo – Information and Law, 2(53),* 136–146. Retrieved from DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334149 [in Ukrainian].