DOI: 10.61718/nsn29.01
УДК 351.862:334.021:351.746.1(477)

Бєліх Ігор Володимирович
ORCID: 0000-0001-5545-3021
Запорізький національний університет

ТЕХНОЛОГІЧНІ РІШЕННЯ ДЛЯ РЕАЛІЗАЦІЇ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

У наданих матеріалах дослідження оприлюднено аналіз технологічних рішень щодо реалізації публічно-приватного партнерства у сфері цивільного захисту на рівні місцевих громад. На основі проведеного аналізу дванадцяти складних цифрових рішень, що застосовуються для впровадження публічно-приватного партнерства, було створене підґрунтя для розробки комплексної моделі інституційного дизайну публічно-приватного партнерства у сфері цивільного захисту. Запропоновано концепцію «Центру цивільної стійкості та безпеки (CCSB)», яка поєднує всі досліджені рішення в єдину синергетичну структуру та здатна формувати надсистемну координаційну інституцію. *Ключові слова: публічно-приватне партнерство, цивільний захист, інфраструктурний проект, державно-приватне партнерство, синергія, механізми публічного управління.*

Вступ. Представлені матеріали є продовженням дослідження що до публічно приватного партнерства (Далі – ППП) на рівні місцевих громад у якості механізму управління, застосування якого може посилити стан цивільного захисту (Далі – ЦЗ) цих громад. Попередні комплексні дослідження теоретико-методологічних засад, механізмів та інструментів ППП, аналіз міжнародного та українського досвіду його застосування та організаційно-управлінських механізмів впровадження ППП у сфері ЦЗ на рівні місцевих громад вже привели до ряду висновків стосовно ефективної реалізації ППП [1, 2, 3, 4, 5]. Шляхом їх узагальнення було сформовано пріоритетні напрямки вдосконалення організаційно-управлінських механізмів. В їх основі лежать три кластери, зокрема такі як цифрова трансформація, правова уніфікація та фінансова інженерія. Шляхом такого структурування було створено єдине інноваційне аналітичне поле, в якому концептуалізація ключових механізмів реалізації ППП в парадигмі «розумного» партнерства являють собою підґрунтя для розробки комплексної моделі інституційного дизайну ППП у сфері ЦЗ на рівні місцевих громад.

Мета дослідження. На основі комплексного аналізу існуючих технологічних рішень публічно-приватного партнерства розробити його концептуальну модель для посилення цивільного захисту на рівні місцевих громад.

Завдання дослідження:

1. Провести комплексний аналіз існуючих технологічних рішень впровадження ППП у сфері ЦЗ.
2. Розробити комплексну модель інституційного дизайну ППП, яка може бути застосована у сфері ЦЗ на рівні місцевих громад.

Методи дослідження. Системний аналіз технологічних рішень за встановленими критеріями оцінювання; метод синтезу для інтеграції дванадцяти цифрових рішень у єдину концептуальну модель; структурно-функціональний аналіз компонентів цифрової архітектури ППП; метод моделювання для проектування координаційної інституції; порівняльний аналіз.

Виклад основного матеріалу. Було проведено комплексне дослідження технологічно складних рішень впровадження ППП, які можуть бути застосовані у сфері ЦЗ. Основні критерії дослідження: функціональне призначення, модель реалізації ППП, основні зацікавлені сторони, ключові технології та інструменти, напрями використання у системі ЦЗ, соціально-організаційний ефект. У дослідженні було виділено ППП, що містять сучасні цифрові технології. В рамках єдиної державної системи цивільного захисту (ЄДС ЦЗ) такі рішення здатні забезпечити оперативність, ефективність і сталість реагування на надзвичайні ситуації. Було проведено аналіз дванадцяти наступних рішень цифрової реалізації ППП: платформа передикативної аналітики на базі штучного інтелекту для управління ризиками [6]; цифрові «двійники» критичної інфраструктури (Digital Twins) [7]; інтегрована система смарт-дронів для моніторингу та реагування [8]; кібербезпечна хмарна платформа управління надзвичайними ситуаціями [9]; система мобільного попередження з гіперлокалізацією (Next-Gen Public Alert) [10]; платформа краудсорсингу для швидкого реагування та залучення волонтерів [11]; IoT-система раннього виявлення небезпек на базі Smart City [12]; мобільні інтероперабельні комунікаційні вузли [13]; система «цифрового резилієнсу» громад [14]; система «Розумне укриття» [15]; AR-навігація до найближчих укриттів у реальному часі [16]; цифрова мережа бізнес-хабів стійкості [17].

Висновки. На основі проведеного аналізу було прийнято рішення про доцільність створення концепції «Центру цивільної стійкості та безпеки (CCSB)». Запропонована концепція поєднує всі досліджені рішення в єдину синергетичну структуру та здатна формувати надсистемну координаційну інституцію. Таке партнерство може існувати як на рівні громадської організації чи невеликого приватного бізнесу, так і масштабуватись до рівня державно-приватною установи, що працює у взаємодії з міністерствами чи відомствами та з міжнародними установами і донорами. Сформовано критичну масу прикладних рішень та створено підґрунтя для стратегічного бачення переходу від фрагментованої інноваційності до інституціоналізованої цифрової стійкості.

Пропозиції. Розглядати результати дослідження як підґрунтя для розробки комплексної моделі інституційного дизайну ППП на місцевому рівні. Для реалізації ППП створити системну цифрову архітектуру, в якій кожен технологічний елемент виконує чітку функціональну роль у рамках ППП, а саме: хмарна платформа як центральний інструмент управління; інструменти блокчейн-реєстрації для забезпечення прозорості, захисту від маніпуляцій та миттєвої юридичної дійсності дій у рамках ППП; застосування IoT-інфраструктури та QR-ідентифікації для контролю в режимі реального часу запасів та розходу ресурсів у всіх структурних компонентах; застосування віртуальних симуляцій (AR/VR) для навчання, сертифікації та моделювання ситуацій; інтеграція з національним реєстром об'єктів готовності для верифікації, аудиту і класифікації учасників системи за рівнем стійкості.

Джерела.

1. Бєліх І. В. Сутність та особливості функціонування публічно-приватного партнерства у сфері цивільного захисту. *Нотатки сучасної науки*. 2025. № 28. DOI: https://doi.org/10.61718/nsn28.02
2. Бєліх І. В. Методологічні підходи до реалізації публічно-приватного партнерства у сфері цивільного захисту на рівні місцевих громад. *Advanced top technology*. 2025. № 13. DOI: https://doi.org/10.61718/att13.02
3. Бєліх І. В. Організаційні моделі реалізації публічно-приватного партнерства у сфері цивільного захисту. *Crosspoint: науковий альманах*. Харків: СГ НТМ «Новий курс», 2025. ISBN 978-617-7886-81-4. С. 23-26. DOI: https://doi.org/10.61718/cros2025
4. Бєліх І. В. Аналіз міжнародного та українського досвіду реалізації публічно-приватного партнерства у сфері цивільного захисту. *Соціально-гуманітарний вісник.* 2025. № 60. С. 31-33. DOI: https://doi.org/10.61718/sgv60.02
5. Бєліх І. В. Організаційно-управлінські механізми впровадження публічно-приватного партнерства на рівні місцевих громад. *Креативний простір.* 2025. № 32. С. 39-40. DOI: https://doi.org/10.61718/crp
6. Rauf Md. A., Jim Md. M. I. AI-Powered Predictive Analytics for IP Risk Management. Global Mainstream J. 2024. Vol. 1(4). DOI: https://doi.org/10.62304/ijse.v1i04.184
7. Itäpelto T. Digital Twin Enhanced Critical Infrastructure Security. IEEE SWC. 2023. P. 1-3. DOI: https://doi.org/10.1109/SWC57546.2023.10448804
8. Nguyen D.-D., Dang Q.-D. Intelligent Drone System for Smart City. Drones. 2024. 8(9). P. 512. DOI: https://doi.org/10.3390/drones8090512
9. Хомчак М. Оцінка ризиків кібербезпеки для хмарного провайдера. *Кібербезпека: освіта, наука, техніка.* 2025. № 3(27). С. 549-559. DOI: https://doi.org/10.28925/2663-4023.2025.27.773
10. Chovanec D. et al. Component-Based Approach to Early Warning Systems. Applied Sci. 2025. 15(6). P. 3218. DOI: https://doi.org/10.3390/app15063218
11. Бахур Н. Краудсорсинг у розвитку громад. Київ: НІСД, 2022. С. 1-8. URL: https://niss.gov.ua/sites/default/files/2022-07/bakhur.pdf
12. Тютюник В. В. та ін. Акустичний моніторинг у «Smart City». 2023. С. 58-76. DOI: https://doi.org/10.33269/nvcz.2023.2.58-76
13. Rajib Taid. Mobile Networks Troubleshooting. Wiley, 2021. P. 159-170. DOI: https://doi.org/10.1002/9781119778714.ch12
14. Пахненко О. Резильєнтність громад в контексті COVID-19. *Економіка та суспільство.* 2022. № 39. DOI: https://doi.org/10.32782/2524-0072/2022-39-51
15. Cuzzocrea A. Big Data Lakes: Models and Techniques. IEEE BigComp. 2021. P. 1-4. DOI: https://doi.org/10.1109/bigcomp51126.2021.0001016
16. Valizadeh M. et al. AR navigation for emergency evacuation. Heliyon. 2024. 10(12). e32852. DOI: https://doi.org/10.1016/j.heliyon.2024.e32852
17. Nofel M. et al. Blockchain, IoT, XBRL in Accounting Systems. J. Risk Financial Management. 2024. 17(8). P. 372. DOI: https://doi.org/10.3390/jrfm17080372

Губенко Владислав Дмитрович
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій
Національна академія Служби безпеки України
Науковий керівник: Даниленко В. М., доктор історичних наук, професор,
Національна академія Служби безпеки України

ТЕОРЕТИЧНІ ОСНОВИ ФЕНОМЕНУ БОТОФЕРМ ЯК ЕЛЕМЕНТА ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ГІБРИДНОЇ ВІЙНИ

У тезах розглядаються теоретичні аспекти ботоферм як автоматизованих мереж, що функціонують у цифровому просторі. Аналізується визначення, структура, класифікація та еволюція бот-мереж, їх роль у маніпуляції суспільною свідомістю в умовах гібридної війни. На основі аналізу наукової літератури та сучасних даних запропоновано авторську класифікацію ботів за рівнем автономності, функціональним призначенням та рівнем загрози. Тези базуються на матеріалах магістерської роботи та можуть бути використані для розробки стратегій кібербезпеки, з урахуванням актуальних тенденцій 2024-2025 років, включаючи інтеграцію штучного інтелекту (ШІ) у дезінформаційні кампанії. Ключові слова: ботоферми, бот-мережі, гібридна війна, інформаційна маніпуляція, класифікація ботів, кібербезпека, штучний інтелект.

Вступ. У сучасних умовах глобальної цифровізації та зростання ролі соціальних мереж у формуванні суспільних процесів ботоферми стали одним із найнебезпечніших інструментів інформаційних впливів. Актуальність теми зумовлена не лише світовими тенденціями, а й конкретним безпековим контекстом України,