DOI: https://doi.org/10.32689/2523-4536/77-4
УДК 352/354

Литвиненко С.М.
доктор філософії,
асистент кафедри економіки, підприємництва та бізнес-адміністрування,
Сумський державний університет
ORCID: https://orcid.org/0000-0001-5726-4080
Кубатко О.В.
доктор економічних наук, професор,
доцент кафедри економіки, підприємництва та бізнес-адміністрування,
Сумський державний університет
ORCID: https://orcid.org/0000-0001-6396-5772
Вороненко В.І.
кандидат економічних наук, доцент,
старший викладач кафедри економіки,
підприємництва та бізнес-адміністрування,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-0301-5924
Михайлов О.О.
аспірант,
Сумський державний університет
Борисенко О.В.
студентка,
Сумський державний університет

Lytvynenko Svitlana
PhD,
Assistant of the Department of Economics,
Entrepreneurship and Business Administration,
Sumy State University
Kubatko Oleksandr
Doctor of Economic Sciences, Professor,
Associate Professor at the Department of Economics,
Entrepreneurship and Business Administration,
Sumy State University
Voronenko Viacheslav
Ph.D. in Economics, Associate Professor,
Senior Lecturer of the Department of Economics,
Entrepreneurship and Business Administration,
Sumy State University
Mykhaylov Oleksiy
Postgraduate Student,
Sumy State University
Borysenko Oleksandra
Student,
Sumy State University

ОЦІНЮВАННЯ І ПРОГНОЗУВАННЯ ВПЛИВУ ЦИФРОВИХ ТРАНСФОРМАЦІЙ НА ПРОЦЕСИ ЗАБЕЗПЕЧЕННЯ ЦИВІЛЬНОГО ЗАХИСТУ В УМОВАХ ЕКОЛОГІЧНИХ І СОЦІАЛЬНИХ ВИКЛИКІВ[1]

[1]Робота виконана в рамках НДР «Цифрові трансформації для забезпечення цивільного захисту та повоєнного відновлення економіки в умовах екологічних і соціальних викликів» (№ д/р. 0124U000549)

ASSESSING AND FORECASTING THE IMPACT OF DIGITAL TRANSFORMATIONS ON CIVIL PROTECTION PROCESSES IN CONDITIONS OF ENVIRONMENTAL AND SOCIAL CHALLENGES

Стаття присвячена розробці методики оцінювання та прогнозування впливу цифрових трансформацій на систему цивільного захисту України в умовах сучасних екологічних і соціальних викликів, а також повоєнного відновлення національної економіки. Розглядаються ключові завдання цивільного захисту з акцентом на цифровий інструментарій та потенціал його використання для підвищення ефективності управління, моніторингу та реагування на надзвичайні ситуації. Окреслено сучасні тенденції впровадження інноваційних технологій, зокрема використання систем штучного інтелекту, Інтернету речей, платформ великих даних, а також мобільних додатків та чат-ботів, дронів, тепловізорів тощо. Розроблено підхід до визначення цифрової резильєнтності на основі багатовимірних індикаторів: інформаційно-комунікаційних технологій, електронної комерції, інфраструктури, кібербезпеки, цифрових навичок та електронного уряду. Описані методи оцінки цифрових трансформацій враховують показники ефективності, фінансових витрат та технічних характеристик. Відзначено високий потенціал цифрових інновацій у підвищенні стійкості та адаптації системи цивільного захисту до сучасних викликів, зокрема у швидкому реагуванні на надзвичайні ситуації, а також у оптимізації ресурсів та роботі з наслідками кризових подій. Таким чином, дослідження доводить, що впровадження цифрових технологій є ключовим фактором забезпечення ефективності системи цивільного захисту, що сприяє сталому розвитку та відновленню економіки України від наслідків війни.

Ключові слова: *цифрові трансформації, сталий розвиток, цивільна безпека, повоєнне відновлення, екологічні виклики.*

The study aims to develop a methodology for assessing and forecasting the impact of digital transformations on Ukraine's civil protection system amidst modern ecological and social challenges, as well as in the context of post-war national economic recovery. The key tasks of civil protection are examined with a focus on digital tools and their potential to enhance management, monitoring, and response efficiency. The article outlines contemporary trends in implementing innovative technologies, including artificial intelligence systems, the Internet of Things, big data platforms, mobile applications, chatbots, drones, thermal imaging devices, and more. A multidimensional approach to determining digital resilience is proposed based on indicators such as information and communication technologies, e-commerce, infrastructure, cybersecurity, digital skills, and e-government. Methods for assessing digital transformations are described, emphasising efficiency indicators, financial costs, and technical characteristics. The study identifies the high potential of digital innovations in increasing the resilience and adaptability of the civil protection system to modern challenges, particularly in rapid response to emergencies, resource optimisation, and managing the aftermath of crises. Thus, the publication demonstrates that implementing digital technologies is a key factor in ensuring the effectiveness of the civil protection system, promoting sustainable development, and facilitating Ukraine's economic recovery after the war.

Keywords: *digital transformation, sustainable development, civil security, post-war reconstruction, environmental challenges.*

Постановка проблеми. Сучасні глобальні виклики, зокрема воєнні конфлікти, екологічні катастрофи та соціальні кризи, зумовлюють необхідність удосконалення системи цивільного захисту. В умовах повоєнного відновлення економіки України важливим аспектом стає застосування цифрових технологій для підвищення ефективності цивільного захисту та управління надзвичайними ситуаціями.

Цифрові трансформації відіграють ключову роль у цивільному захисті населення, оптимізації ресурсів, моніторингу загроз і координації дій під час надзвичайних ситуацій. Впровадження цифрових технологій відкриває нові можливості для ефективного прогнозування та швидкого реагування.

Зважаючи на актуальність цієї проблематики, дослідження спрямоване на розробку методики оцінювання та прогнозування впливу цифрових трансформацій на систему цивільного захисту в Україні. Це дозволить визначити ключові фактори цифрової стійкості та запропонувати рекомендації щодо впровадження інноваційних технологій у сфері безпеки та реагування на кризові ситуації.

В умовах зростаючих викликів для системи цивільного захисту України традиційні методи управління виявляються не досить ефективними. Одним із напрямків, на які варто звернути увагу є рівень цифровізації цивільного захисту та реагування на надзвичайні ситуації. Також особливої уваги потребує процес інтеграції інформаційно-комунікаційних технологій у систему моніторингу та прогнозування ризиків. Важливою перешкодою на шляху до вдосконалення системи цивільного захисту є брак фінансування та кадрових ресурсів для впровадження інноваційних технологій, а також високі ризики кібератак чи технічних збоїв у критичних системах безпеки. З огляду на ці виклики, актуальним є розроблення ефективних

методик оцінювання та прогнозування впливу цифрових трансформацій на цивільний захист, що сприятиме підвищенню стійкості та адаптивності системи в умовах сучасних загроз.

Аналіз останніх досліджень і публікацій. Цифрові трансформації сприяють підвищенню стійкості економіки та ефективності кризового управління. Наприклад, дослідження демонструють, що використання штучного інтелекту та великих даних дозволяє швидко реагувати на надзвичайні ситуації та прогнозувати їх наслідки (Brynjolfsson E. & McAfee A. [2]). Зокрема, застосування Інтернету речей (IoT) у системах безпеки дозволяє здійснювати моніторинг навколишнього середовища та передбачати потенційні загрози (Atzori L. et al. [1]).

Післявоєнне відновлення економіки неможливе без активного впровадження цифрових рішень, зокрема електронного врядування, яке значно покращує доступність державних послуг та підвищує їх ефективність (Janssen M. & Van der Voort H. [6]). Крім того, сучасні цифрові платформи забезпечують нові можливості для малого та середнього бізнесу через електронну комерцію та фінансові технології (FinTech), що є критично важливим для стабілізації економіки (Gomber P. et al. [5]).

Окрему увагу варто приділити питанням кібербезпеки, адже цифровізація державного управління та критичної інфраструктури супроводжується зростанням ризиків кібератак. Дослідження показують, що країни, які впроваджують національні стратегії кіберзахисту, мають значно вищий рівень стійкості до цифрових загроз (Von Solms R. & Van Niekerk J. [8]).

Незважаючи на окреслені ризики та загрози, цифрові трансформаційні процеси безумовно можуть мати сильний вплив на систему цивільного захисту країни в сучасних умовах.

Мета статті полягає в розробці методики оцінювання та прогнозування впливу цифрових трансформацій на систему цивільного захисту України в умовах сучасних екологічних і соціальних викликів, а також повоєнного відновлення національної економіки.

Виклад основного матеріалу. Поняття «цивільний захисту населення» визначено Кодексом цивільного захисту України як «комплекс заходів, які реалізуються на території України в мирний час та в особливий період і спрямовані на захист населення, територій, навколишнього природного середовища, майна, матеріальних і культурних цінностей від надзвичайних ситуацій та інших небезпечних подій, запобігання виникненню таких ситуацій та подій, ліквідацію їх наслідків, надання допомоги постраждалим, здійснення державного нагляду (контролю) у сфері пожежної та техногенної безпеки» [9].

Державна система цивільного захисту має ряд завдань, визначених Кодексом цивільного захисту України. На деякі з них прямо чи опосередковано здатні впливати цифрові трансформаційні процеси. Окремі завдання цивільного захисту населення:

Завдання 1. Навчання населення щодо поведінки та дій у разі виникнення надзвичайної ситуації:

– створення онлайн-курсів чи тренінгів із розміщенням на освітніх платформах чи державних веб-порталах;

– видання електронних навчальних матеріалів (брошури, збірники, пам'ятки);

– використання технологій віртуальної/доповненої реальності (моделювання надзвичайних ситуацій (НС) та алгоритму дій у критичних ситуаціях);

– чат-боти для комунікацій громадян щодо цивільної безпеки, дій у разі виникнення НС.

Завдання 2. Прогнозування і оцінка соціально-економічних наслідків надзвичайних ситуацій, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах. Можливі рішення у контексті цифрових трансформацій:

– використання датчиків і сенсорів для постійного моніторингу стану довкілля (рівня води, показників якості повітря, сейсмічної активності тощо);

– технології "Big Data" (великих даних) та штучного інтелекту для аналізу інформації з різних джерел (дані з камер відеоспостереження, соцмережі, сенсори, датчики тощо) з метою виявлення та прогнозування НС;

– створення та використання спеціалізованих платформ, що займатимуться обробкою даних про НС допомагатимуть оперативно реагувати та координувати дії органів цивільного захисту (об'єднання інформацію від рятувальних служб, лікарень, поліції).

Завдання 3. Створення і цільове використання матеріальних резервів, необхідних для запобігання виникненню надзвичайних ситуацій та ліквідації їх наслідків. Можливі рішення у контексті цифрових трансформацій:

– ERP-системи для управління матеріальними ресурсами з метою відстеження стану та обсягів резервів у реальному часі;

– прогнозування потреб у матеріальних ресурсах та оцінка потенційних ризиків за допомогою "Big Data" (на основі історичних даних, погодних умов, демографічної інформації тощо);

– використання спеціальних програм для моделювання сценаріїв з метою оцінки можливих наслідків НС і відповідно планування матеріальних резервів;

– використання БПЛА для швидкої доставки невеликих партій життєво важливих ресурсів (медикаментів, води, продовольства) у важкодоступні місця.

Завдання 4. Оповіщення населення про загрозу та виникнення надзвичайних ситуацій, своєчасне та достовірне інформування про фактичну обстановку та вжиті заходи. Можливі впливи цифрових трансформацій:

– використання мобільних операторів для розсилки масових текстових повідомлень про загрозу або виникнення НС;

– спеціалізовані додатки для смартфонів, які надсилають push-повідомлення про поточну ситуацію;

– інтерактивні мапи, маршрути евакуації та поради щодо дій у критичних ситуаціях (наприклад через додатки) (інтерактивні геоінформаційні платформи);

– використання соціальних платформ, таких як "Facebook", "Instagram", "Telegram", "Twitter" для оперативного поширення інформації;

– чат-боти у месенджерах для надання інформації про надзвичайні ситуації;

– модернізовані системи сирен та гучномовців з інтеграцією цифрових систем можуть бути керовані дистанційно, забезпечуючи швидке інформування населення;

– використання технологій штучного інтелекту для виявлення та блокування фейкової інформації, яка може загострити кризову ситуацію.

Завдання 5. Проведення рятувальних та інших невідкладних робіт щодо ліквідації наслідків надзвичайних ситуацій, організація життєзабезпечення постраждалого населення. Можливі рішення у контексті цифрових трансформацій:

– БПЛА можуть використовуватися для огляду місць, куди рятувальники не можуть дістатися через небезпечні умови, дрони можуть допомагати в пошуку постраждалих, оцінці масштабу руйнувань та доставки екстрених товарів у важкодоступні місця;

– використання тепловізійного обладнання та сенсорів для пошуку постраждалих під завалами. Ці технології можуть бути інтегровані у дрони або використовуватися вручну рятувальними командами;

– телемедицина може використовуватися для надання медичних консультацій на відстані в зонах, де немає доступу до лікарів;

– онлайн-платформи психологічної допомоги.

Завдання 6. Здійснення заходів щодо соціального захисту постраждалого населення. Можливі рішення у контексті цифрових трансформацій:

– цифрові платформи для реєстрації постраждалих;

– електронні системи виплат допомоги;.

– цифрові сервіси соціальних послуг (консультації щодо соціальних пільг, переселення, працевлаштування та інших видів соціальної підтримки);

– цифрові платформи для пошуку житла;

– цифрові краудфандинг-платформи для збору коштів на підтримку постраждалих.

Завдання 7. Підготовка керівного складу єдиної державної системи цивільного захисту до дій у разі мобілізації та виконання завдань цивільного захисту у воєнний час з урахуванням норм міжнародного гуманітарного права. Можливі рішення у контексті цифрових трансформацій:

– створення цифрових платформ для управління мобілізаційними ресурсами, включаючи людські, технічні та матеріальні резерви;

– використання систем оповіщення для швидкої мобілізації керівного складу та персоналу;

– цифрові документообігові системи для забезпечення доступу до документів.

Завдання 8. Сповіщення органів управління та сил цивільного захисту єдиної державної системи цивільного захисту, а також населення про загрозу застосування засобів ураження. Можливі рішення у контексті цифрових трансформацій:

– автоматизовані системи моніторингу загроз (сенсори, супутники, радіолокаційні станції для виявлення ознак загрози застосування засобів ураження, таких як ракетні удари чи хімічні атаки);

– використання телевізійних і радіо-каналів для масового оповіщення населення про загрози;

– офіційні веб-сайти уряду, органів цивільного захисту та соціальні мережі можуть бути ефективно задіяні для швидкого поширення інформації про загрозу.

Завдання 9. Визначення населених пунктів та районів, що потребують проведення гуманітарного розмінування, маркування

небезпечних ділянок, проведення очищення (розмінування) територій. Можливі рішення у контексті цифрових трансформацій:

– аналіз супутникових знімків. Супутникові дані можуть допомогти ідентифікувати райони, що постраждали від військових дій, і потенційно є замінованими чи містять нерозірвані боєприпаси. Використання штучного інтелекту для аналізу цих зображень дозволяє швидко виявляти небезпечні зони;

– БПЛА також можуть використовуватися для обстеження територій на предмет мінування чи наявності вибухових залишків.

– БПЛА з тепловізійними та іншими сенсорами, що можуть виявляти вибухонебезпечні предмети під землею, тим самим полегшуючи процес планування гуманітарного розмінування.

– використання спеціальних застосунків або інтерактивних карт, де місцеві жителі та фахівці з розмінування можуть позначати небезпечні зони або підозрілі предмети.

Завдання 10. Технології дистанційного розмінування. Можливі рішення у контексті цифрових трансформацій:

– використання техніки для дистанційного розмінування, наприклад, броньованих машин, керованих на відстані, що дозволяє очищати великі території без безпосередньої присутності людей;

– спеціальні роботи можуть використовуватися для безпечного розмінування територій, особливо в районах з важким доступом або високим рівнем ризику.

Поряд з позитивними впливами існують негативні виклики та загрози, які обов'язково мають враховуватися при процесах планування та аналізу, особливо якщо мова йде про новітні технології, ризики яких оцінити до запуску важко. Авторами було проведено SWOT-аналіз для ідентифікації основних переваг та аспектів, що потребують особливої уваги при впровадженні цифрових технологій у сфері цивільного захисту (табл. 1).

Таким чином, цифрові трансформації відкривають перед Україною широкі можливості для підвищення ефективності цивільного захисту, але разом з тим вони вимагають серйозної уваги до викликів у галузі інфраструктури, безпеки та фінансування.

На сьогодні існує ряд розроблених методик та стандартів для оцінки впливу цифрових трансформацій на систему цивільного захисту. Ці методики використовуються для оцінки ефективності управління ризиками, швидкості реагування, а також захисту критичної інфраструктури. Наприклад, Індекс ризику катастроф ("Disaster Risk Index" – "DRI"), запропонований "UNDRR", покликаний оцінювати ризики та ступінь вразливості територій. Для проведення аналізу в тому числі використовуються цифрові інструменти для моніторингу. "DRI" враховує як ймовірність виникнення катастрофи, так і рівень готовності регіону [7].

"CIPRNet" (Critical Infrastructure Preparedness and Resilience Research Network) – інструмент, створений Єврокомісією для оцінки готовності критичної інфраструктури до стресових ситуацій. Він включає модулі аналізу, які визначають слабкі місця і надають рекомендації щодо підвищення їхньої стійкості [3].

Єврокомісія пропонує оцінювати резильєнтність країни, виходячи з оцінки чотирьох вимірів: соціального та економічного, екологічного, цифрового та геополітичного [4]. Говорячи про цифрову резильєнтність, варто зазначити, що вона має на меті визначення рівня успішності та ефективності подолання певних викликів суб'єктами з подальшою адаптацією до змін,

Таблиця 1

SWOT-аналіз впровадження цифрових технологій у сфері цивільного захисту

Сильні сторони	**Слабкі сторони**
• Поліпшення моніторингу та попередження • Підвищення ефективності комунікацій • Оптимізація використання ресурсів • Можливості	• Недостатня інфраструктура в деяких регіонах (особливо в сільській місцевості) • Низький рівень цифрової грамотності • Висока залежність від електропостачання • Відсутність єдиної національної платформи для централізованого управління цивільним захистом
Можливості	**Загрози**
• Впровадження національної цифрової платформи для управління кризами • Співпраця з міжнародними організаціями та обмін досвідом • Використання інноваційних технологій (таких як штучний інтелект, Інтернет речей тощо) • Розвиток цифрової грамотності серед населення	• Зростання ризику кібератак • Безпека даних • Проблеми з фінансуванням • Можливі технічні збої • Вразливість до зовнішніх залежностей (ризики зовнішніх впливів у разі використання імпортних технологій та обладнання)

відновленням до оптимального рівня, забезпечення сталого функціонування та удосконалення після кризових ситуацій завдяки використанню цифрових технологій. Визначення цифрової резильєнтності відбувається на основі чотирьох груп індикаторів: персональна діджиталізація, діджиталізація промисловості, суспільство (соціальний вимір) та кібербезпека.

Для кращої деталізації пропонується використовувати шість груп показників для визначення рівня цифрової резильєнтності:

1. Інформаційно-комунікаційні технології (частка кількості підприємств, що проводили аналіз «великих даних», кількість підприємств, які мають доступ до мережі Інтернет, кількість зайнятих працівників, які мають доступ до мережі Інтернет, частка кількості підприємств, що купують послуги хмарних обчислень, частка кількості підприємств, що використовують Інтернет речей, частка кількості підприємств, що використовують технології штучного інтелекту).
2. Електронна комерція та Інтернет-послуги (кількість підприємств, які здійснювали електронну торгівлю, використання соціальних медіа на підприємствах).
3. Інтернет-інфраструктура (кількість абонентів Інтернету, рівень покриття Інтернетом у міських і сільських районах, кількість користувачів Інтернету на сто осіб (Інтернет-проникнення), швидкість Інтернету за регіонами, що свідчить про можливості доступу до якісних цифрових послуг).
4. Кібербезпека (частка кількості підприємств, які стикалися з проблемами через інциденти з безпекою ІКТ, частка кількості підприємств, що застосовують заходи безпеки ІКТ в інформаційно-комунікаційних системах підприємства, безпека ІКТ в інформаційно-комунікаційних системах підприємств, кількість кібератак).
5. Цифрові навички та освіта (фахівці та навички у сфері ІКТ на підприємствах, частка кількості підприємств, що мають найманих фахівців, для яких ІКТ є основною роботою).
6. Цифровий уряд (кількість зареєстрованих «Е-звернень», кількість розглянутих «Е-звернень», кількість оприлюднених «Е-петицій», кількість оприлюднених «Е-консультацій»).

Наведемо алгоритм визначення Індексу цифрової резильєнтності (Idr). Він міститиме декілька етапів.

Для нормалізації даних для показників-стимуляторів (наприклад, кількість зайнятих працівників, які мають доступ до мережі Інтернет, фахівці та навички у сфері ІКТ на підприємствах та ін.) пропонується застосовувати формулу 1

$$A = \frac{x - x_{\min}}{x_{\max} - x_{\min}}, \quad (1)$$

де А – нормалізоване значення показника, х – фактичне значення показника, x_{min} та x_{max} – найменше та найбільше значення показника відповідно.

$$A = \frac{x_{\max} - x}{x_{\max} - x_{\min}}, \quad (2)$$

Формулу 2 використано для показників-дестабілізаторів (наприклад, кількість кібератак, частка кількості підприємств, які стикалися з проблемами через інциденти безпеки ІКТ та ін.).

На наступному етапі проводиться розрахунок проміжних індексів для кожної групи. Індекс інформаційно-комунікаційних технологій (I_{CT}):

$$I_{CT} = \frac{1}{n} \cdot \sum_{i=1}^{n} A_i, \quad (3)$$

Аналогічний розрахунок застосовується для всіх груп показників: індексу електронної комерції (I_{EC}), індексу Інтернет-інфраструктури (I_I), індексу кібербезпеки (I_{CS}), індексу цифрових навичок та освіти (I_{ED}), індексу цифрового уряду (I_{EG}).

Наступний етап – присвоєння вагових коефіцієнтів кожній групі (wi) методом експертних оцінок. При цьому сума вагових коефіцієнтів дорівнює одиниці.

У підсумку інтегрований індекс цифрової резильєнтності дорівнюватиме сумі шести проміжних індексів з урахуванням їхніх вагових коефіцієнтів (за формулою 3).

$$I_{dr} = w_1 \cdot I_{CT} + w_2 \cdot I_{EC} + w_3 \cdot I_I + \\ + w_4 \cdot I_{CS} + w_5 \cdot I_{ED} + w_6 \cdot I_{EG} \quad (4)$$

Показник потребуватиме подальшої оцінки в динаміці.

Для побудови економіко-математичної моделі оцінки впливу цифрових трансформацій на систему цивільного захисту в Україні необхідно визначити основні параметри, які характеризують ефективність цифрових змін у цьому секторі. Модель може бути спрямована на аналіз змін у ключових показниках, таких як швидкість реагування, якість комунікацій, ефективність управління ресурсами та стійкість критичної інфраструктури.

Авторами розроблено методику оцінювання впливу цифрових трансформацій на систему цивільного захисту в Україні. Методика у вигляді моделі побудована на релевантних показниках, обраних для оцінки

ефективності системи цивільного захисту та рівня цифрової трансформації. Показники включають:

– витрати на інформаційні технології та телекомунікації (у т.ч. витрати на цифровізацію державного сектору, витрати на обладнання, програмне забезпечення, телекомунікаційні послуги, тощо);

– витрати на цивільний захист, служби порятунку та реагування (обсяги фінансування служб цивільного захисту, включаючи аварійно-рятувальні служби, пожежну безпеку та інші послуги з ліквідації наслідків надзвичайних ситуацій);

– показники продуктивності та ефективності цивільного захисту (кількість рятувальних операцій, час реагування на надзвичайні ситуації, кількість потерпілих і врятованих, а також фінансові втрати від надзвичайних ситуацій, тощо);

– загальний рівень цифрової інфраструктури (кількість населення, що має доступ до Інтернету, покриття мобільного зв'язку, число організацій з доступом до Інтернету, тощо).

Основне рівняння для моделі оцінки ефективності цивільного захисту залежно від рівня цифровізації має наступний вигляд:

$$E=\alpha_1 D+\alpha_2 IT+\alpha_3 T+\alpha_4 C+\varepsilon, \quad (5)$$

де: E – індекс ефективності системи цивільного захисту (на основі показників швидкості реагування, кількості врятованих, часу на реагування, тощо); D – загальний рівень цифрової інфраструктури (дані про доступ до Інтернету, цифровізацію державних установ, тощо); IT – витрати на IT у секторі цивільного захисту; T – час реагування на надзвичайні ситуації; C – витрати на забезпечення ресурсами цивільного захисту (фінансування служб цивільного захисту). $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ – вагові коефіцієнти, що показують, наскільки кожен фактор впливає на ефективність; ε – стохастичний член, що враховує вплив інших неконтрольованих факторів.

Модель розширено стохастичним членом ε для врахування ймовірності збоїв чи додаткових ризиків, пов'язаних з цифровізацією.

Наведена методика дасть змогу оцінити конкретні впливи цифрових трансформацій на цивільний захист в Україні та визначити пріоритети для оптимізації ресурсів.

Таким чином, цивільний захист у контексті цифрових трансформацій і сучасних викликів демонструє важливість технологічного розвитку та адаптації для забезпечення ефективної і стійкої системи безпеки населення. Цифрові трансформації можуть значно підвищити здатність України реагувати на надзвичайні ситуації, мінімізувати наслідки кризових подій і забезпечити швидке відновлення.

Надійний стан системи цивільного захисту у сучасному світі важко уявити без цифрових трансформацій. Хоча основні функції цивільного захисту можуть працювати і без цифрових технологій, їх ефективність, швидкість реагування та можливості координації значно обмежуються. Цифрові трансформації сприяють кращому моніторингу, координації та швидкому реагуванню, зменшуючи ризики для населення та підвищуючи загальну стійкість до надзвичайних ситуацій.

Висновки. Дослідження підтвердило, що цифрові трансформації відіграють вирішальну роль у вдосконаленні системи цивільного захисту України, особливо у контексті повоєнного відновлення економіки та адаптації до сучасних екологічних і соціальних викликів. Запровадження інноваційних технологій сприяє підвищенню ефективності моніторингу, прогнозування, координації дій та оперативного реагування на надзвичайні ситуації. На основі аналізу сучасних цифрових рішень визначено ключові напрями їх впливу: покращення системи раннього оповіщення населення за допомогою мобільних додатків, чат-ботів, інтерактивних карт та автоматизованих інформаційних систем; розширення можливостей прогнозування надзвичайних ситуацій шляхом використання технологій великих даних, штучного інтелекту, Інтернету речей тощо; оптимізація управління ресурсами цивільного захисту, включаючи використання ERP-систем, автоматизованих платформ та БПЛА для швидкої доставки допомоги у критичні зони; розвиток цифрової резильєнтності через створення єдиної національної платформи для управління кризовими ситуаціями, інтеграцію інформаційних систем та підвищення рівня кібербезпеки.

Разом з тим, виявлено низку викликів, пов'язаних із недостатньою цифровою інфраструктурою в окремих регіонах, браком фінансування, низьким рівнем цифрової грамотності населення та ризиками кібератак. Для їх мінімізації необхідно розробити комплексну стратегію цифрової трансформації цивільного захисту, що включатиме нормативно-правове регулювання, фінансову підтримку та освітні ініціативи.

Таким чином, результати дослідження підкреслюють необхідність активного впровадження цифрових технологій у сферу цивільного захисту України. Це дозволить значно підвищити рівень готовності до надзвичайних ситуацій, забезпечити ефективне реагування та сприяти сталому розвитку і відновленню країни від наслідків війни.

Список використаних джерел:

1. Atzori L., Iera A., & Morabito G. The Internet of Things: A survey. *Computer Networks.* 2010. No. 54 (15). P. 2787–2805. DOI: https://doi.org/10.1016/j.comnet.2010.05.010
2. Brynjolfsson E., & McAfee A. *Machine, Platform, Crowd: Harnessing Our Digital Future*. W. W. Norton & Company, 2017.
3. CISA. (n.d.). *Methodology for assessing regional infrastructure resilience*. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/resources-tools/resources/methodology-assessing-regional-infrastructure-resilience
4. Commission of the European Union. *Dashboard report: November 2021*. November 29, 2021. URL: https://commission.europa.eu/system/files/2021-11/dashboard_report_20211129_en.pdf
5. Gomber P., Koch J.-A., & Siering M. Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics.* 2017. No. 87(5). P. 537–580. DOI: https://doi.org/10.1007/s11573-017-0852-x
6. Janssen M., & van der Voort H. Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly.* 2016. No. 33(1). P. 1–5. DOI: https://doi.org/10.1016/j.giq.2016.02.003
7. United Nations Office for Disaster Risk Reduction. (n.d.). *UNDRR*. URL: https://www.undrr.org/
8. Von Solms R., & Van Niekerk J. From information security to cyber security. *Computers & Security.* 2013. No. 38. P. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004
9. Верховна Рада України. *Про принципи запобігання та протидії дискримінації в Україні: Закон України № 5403-VI.* Відомості Верховної Ради України. 2012. URL: https://zakon.rada.gov.ua/laws/show/5403-17#n49

References:

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks,* no. 54(15), pp. 2787–2805. DOI: https://doi.org/10.1016/j.comnet.2010.05.010
2. Brynjolfsson, E., & McAfee, A. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future*. W. W. Norton & Company.
3. CISA. (n.d.). *Methodology for assessing regional infrastructure resilience*. Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/resources-tools/resources/methodology-assessing-regional-infrastructure-resilience
4. Commission of the European Union (November 29, 2021). *Dashboard report: November 2021*. Available at: https://commission.europa.eu/system/files/2021-11/dashboard_report_20211129_en.pdf
5. Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics,* no. 87 (5), pp. 537–580. DOI: https://doi.org/10.1007/s11573-017-0852-x
6. Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly,* no. 33 (1), pp. 1–5. DOI: https://doi.org/10.1016/j.giq.2016.02.003
7. United Nations Office for Disaster Risk Reduction. (n.d.). *UNDRR*. Available at: https://www.undrr.org/
8. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security,* no. 38, pp. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004
9. Verkhovna Rada Ukrainy. (2012). *Pro pryntsypy zapobihannia ta protydii dyskryminatsii v Ukraini: Zakon Ukrainy No. 5403-VI*. Vidomosti Verkhovnoi Rady Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/5403-17#n49