

ЦИФРОВІ ПЛАТФОРМИ УПРАВЛІННЯ ЯК ІНСТРУМЕНТ ТРАНСФОРМАЦІЇ ТА ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

©2025 КОВАЛЬ В. В., КАМІНСЬКИЙ О. Є., РЕДЬКВА О. З., ОНОФРІЙЧУК О. П., КАПРАНОВА Л. Г.

УДК 338.2:004.738.5(477)
JEL Classification: O33; L86; D80; H56; M15

Коваль В. В., Камінський О. Є., Редьква О. З., Онофрійчук О. П., Капранова Л. Г.

Цифрові платформи управління як інструмент трансформації та підвищення економічної безпеки підприємств

Ключовим фактором забезпечення економічної безпеки України в умовах повномасштабної війни є трансформація цифрових систем управління в державному секторі. Метою статті є аналіз сервісів цифрових платформ управління як інструменту підвищення стійкості економіки та економічної безпеки підприємств. Доведено, що цифрові платформи забезпечують безперервність цифрових послуг для громадян і підприємств, підвищують прозорість, знижують ризики корупції та сприяють економічному відновленню. У статті пропонується математична економічна модель для кількісної оцінки впливу цифровізації на економічну безпеку. Модель пояснює взаємозв'язок між ступенем цифрової трансформації, індексом сукупних загроз і рівнем економічної безпеки та включає функцію втрат для кількісної оцінки економічних втрат, спричинених недостатньою цифровізацією. Перевірка з використанням реальних даних підтверджує застосовність моделі. Результати моделювання засвідчили, що для забезпечення економічної стабільності критично важливо досягти рівня цифровізації, що перевищує 75%. Обґрунтовано необхідність системної цифровізації як стратегічного пріоритету для зниження макроекономічних ризиків і забезпечення сталого функціонування підприємств. Надалі можна використовувати мультиагентне моделювання для глибшого аналізу цифрової екосистеми у забезпеченні економічної безпеки підприємств. У світлі цифрової трансформації та гібридних загроз у статті пропонується багатоагентна економіко-математична модель для оцінки економічної безпеки держави та бізнесу. Диференціальні рівняння, що враховують вплив таких елементів, як прозорість, фінансування, доступність послуг та обсяг інцидентів, використовуються для характеристики динаміки цифрової довіри, ризиків атак і збитків. Враховуючи обмеження ризиків і ресурсів, запропонована цільова функція максимізує інтегральну міру цифрової ефективності.

Ключові слова: цифрова трансформація, економічна безпека, цифрові платформи, механізм управління, повоєнне відновлення.

DOI: <https://doi.org/10.32983/2222-0712-2025-3-176-185>

Рис.: 1. Табл.: 2. Формул: 5. Бібл.: 13.

Коваль Віктор Васильович – доктор економічних наук, професор, професор кафедри управління підприємницькою та туристичною діяльністю, Ізмаїльський державний гуманітарний університет (вул. Репіна, 12, Ізмаїл, 68601, Україна)

E-mail: victor-koval@ukr.net

ORCID: <https://orcid.org/0000-0003-2562-4373>

Researcher ID: B-8479-2018

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57209296120>

Камінський Олег Євгенович – доктор економічних наук, доцент, професор кафедри системного аналізу та кібербезпеки, Київський національний економічний університет імені Вадима Гетьмана (просп. Берестейський, 54/1, Київ, 03057, Україна)

E-mail: olkam@kneu.edu.ua

ORCID: <https://orcid.org/0000-0003-0607-8944>

Researcher ID: AAE-5167-2020

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57201253468>

Редьква Оксана Зіновіївна – доктор економічних наук, доцент кафедри менеджменту та адміністрування, Тернопільський національний технічний університет імені Івана Пулюя (вул. Руська, 56, Тернопіль, 46001, Україна)

E-mail: oksanaredkva@ukr.net

ORCID: <https://orcid.org/0000-0002-8246-4305>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56074598700>

Онофрійчук Олег Петрович – кандидат економічних наук, доцент, декан економічного факультету, Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука (вул. Академіка Степана Дем'янчука, 4, Рівне, 33027, Україна)

E-mail: lechkin1990@gmail.com

ORCID: <https://orcid.org/0009-0008-3458-7926>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57836304000>

Капранова Лариса Григорівна – кандидат економічних наук, доцент, завідувач кафедри підприємництва та торгівлі, Приазовський державний технічний університет (вул. Гоголя, 29, Дніпро, 49044, Україна)

E-mail: kapranova_l_g@pstu.edu

ORCID: <https://orcid.org/0000-0001-6014-9999>

Researcher ID: <https://www.researcherid.com/rid/N-1032-2018>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57201116674>

UDC 338.2:004.738.5(477)

JEL Classification: O33; L86; D80; H56; M15

Koval V. V., Kaminsky O. Ye., Redkva O. Z., Onofriichuk O. P., Kapranova L. H. Digital Management Platforms as a Tool for Transformation and Increasing Economic Security of Enterprises

A key factor in ensuring the economic security of Ukraine in the conditions of the full-scale war is the transformation of digital management systems in the public sector. The aim of the article is to analyze the services of digital management platforms as a tool for increasing the sustainability of the economy and improving the economic security of enterprises. It is proved that digital platforms ensure the continuity of digital services for citizens and enterprises, increase transparency, reduce the risk of corruption and contribute to economic recovery. The article proposes a mathematical economic model for quantitatively assessing the impact of digitalization on economic security. The model clarifies the relationship between the degree of digital transformation, the index of total threats and the level of economic security and includes a loss function to quantify economic losses caused by insufficient digitalization. Validation using real data confirms the applicability of the model. The modeling results showed that achieving a digitalization level exceeding 75% is critical to ensuring economic stability. The necessity of systemic digitalization as a strategic priority for reducing macroeconomic risks and ensuring sustainable functioning of enterprises is substantiated. In the future, multi-agent modeling can be used for a more in-depth analysis of the digital ecosystem in ensuring the economic security of enterprises. In light of digital transformation and hybrid threats, the article offers a multi-agent economic and mathematical model for evaluating the State's and businesses' economic security. The State services, businesses, citizens, cybersecurity organizations, IT infrastructure, attack agents, and foreign partners are all included in the model. Differential equations that consider the impact of elements like transparency, funding, service accessibility, and incident volume are used to characterize the dynamics of digital trust, attack risks, and losses. While accounting for risk and resource limitations, the suggested objective function maximizes the integral measure of digital efficiency.

Keywords: digital transformation, economic security, digital platform, governance mechanism, post-war recovery.

Fig.: 3. **Tabl.:** 2. **Formulae:** 5. **Bibl.:** 13.

Koval Viktor V. – Doctor of Sciences (Economics), Professor, Professor of the Department of Business and Tourism Management, Izmail State Humanitarian University (12 Riepina Str., Izmail, 68601, Ukraine)

E-mail: victor-koval@ukr.net

ORCID: <https://orcid.org/0000-0003-2562-4373>

Researcher ID: B-8479-2018

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57209296120>

Kaminsky Oleg Ye. – Doctor of Sciences (Economics), Associate Professor, Professor of the Department of Systems Analysis and Cybersecurity, Kyiv National Economic University named after Vadym Hetman (54/1 Beresteyskyi Ave., Kyiv, 03057, Ukraine)

E-mail: olkam@kneu.edu.ua

ORCID: <https://orcid.org/0000-0003-0607-8944>

Researcher ID: AAE-5167-2020

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57201253468>

Redkva Oksana Z. – Doctor of Sciences (Economics), Associate Professor of the Department of Management and Administration, Ternopil Ivan Pului National Technical University (56 Ruska Str., 46001, Ukraine)

E-mail: oksanaredkva@ukr.net

ORCID: <https://orcid.org/0000-0002-8246-4305>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56074598700>

Onofriichuk Oleh P. – Candidate of Sciences (Economics), Associate Professor, Dean of the Faculty of Economics, International Economics and Humanities University Academician Stepan Demyanchuk's Name (4 Akademik Stepan Demianchuk Str., Rivne, 33027, Ukraine)

E-mail: lechkin1990@gmail.com

ORCID: <https://orcid.org/0009-0008-3458-7926>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57836304000>

Kapranova Larysa H. – Candidate of Sciences (Economics), Associate Professor, Head of the Department of Entrepreneurship and Trade, Pryazovskyi State Technical University (29 Hoholia Str., Dnipro, 49044, Ukraine)

E-mail: kapranova_l_g@pstu.edu

ORCID: <https://orcid.org/0000-0001-6014-9999>

Researcher ID: <https://www.researcherid.com/rid/N-1032-2018>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57201116674>

Вступ. Сучасні умови функціонування влади, особливо під час великомасштабної війни, вимагають дієвих інструментів забезпечення економічної безпеки. Одним із таких інструментів є цифрова трансформація державного управління, яка не тільки полегшує взаємодію співтовариств з державою, а і є основою для оперативного реагування на зовнішні загрози, незважаючи на них. Інтеграція цифрових сервісів у систему управління дозволяє посилити контроль над ресурсами, підвищити прозорість процесів та уникнути корупційних ризиків, що є запорукою стабільності економіки в умовах гібридних викликів.

Після 2022 року Україна засвідчила себе як держава, котра в умовах бойових дій продовжує модернізувати цифрові послуги, насамперед цифрову платформу державних послуг «Дія». Цифрова трансформація підтримує безперервність ділових процесів. Реєстрація ФОП онлайн та спеціальний правовий режим Dii.City вже об'єднали понад 1550 резидентів, тобто значна частина IT-галузі функціонує згідно з чіткими, цифровими нормами оподаткування та відповідності вимогам [1].

Кіберстійкість також є невід'ємною частиною економічної стійкості. CERT-UA зафіксувала у 2024 році 4 315 кібератак/інцидентів (із піками в періоди енергетичних ударів) [3]. Те, що цифрові платформи продовжують функціонувати під час війни, свідчить про ефективність інвестицій в цифрову трансформацію та стійку до відмов обладнання інфраструктуру.

В умовах війни цифрова трансформація забезпечує три стратегічні задачі управління економічною безпекою:

- забезпечує безперервність функціонування базових державних економічних сервісів та платіжних систем;
- підвищує прозорість і підзвітність витрат на підприємствах (система Prozorro, електронне декларування);
- допомагає відбудові зруйнованих активів і підвищенню ділової активності в Україні (сервіси «Є-відновлення», Дія).

Це створює інфраструктуру стійкості, яка прямо зменшує макроекономічні і фінансові ризики та підвищує рівень довіри громадян, донорів та інвесторів до України. Саме цифровізація дала змогу утримати керованість країною, гарантувати соціальні виплати і навіть здійснювати вибірково мобілізацію. Натомість масштабні кібератаки, спроби введення в оману та руйнування фізичної інфраструктури породжують нові загрози. Отже, вивчення ролі державних цифрових сервісів як частини економічної безпеки є актуальним і потребує уваги наукової спільноти.

Аналіз останніх досліджень і публікацій. Протягом останнього періоду часу було проведено чимало наукових досліджень, які зосереджуються на значенні цифрової трансформації для зміцнення стійкості економічної безпеки України в умовах повномасштабної агресії.

Згідно з дослідженням Інституту Брукінгса [2], одним із найважливіших компонентів здатності країни протистояти війні є використання цифрових платформ. Було зазначено, що навіть під час бойових дій український уряд зміг зберегти свою систему управління економікою та здатність пропонувати соціальні та адміністративні послуги населен-

ню завдяки своїй стратегії цифрової трансформації. Доведено ефективність цифрових платформ «Дія», «Trembita» та «Prozorro», які стали частиною системи оборони та допомогли зберегти ланцюги управління економікою і зміцнити довіру громадян.

У звіті аналітиків організації економічного співробітництва та розвитку (OECD) [3] зосереджено увагу на важливості цифрової трансформації для регіональної економічної інклюзії, зокрема щодо підтримки малого та середнього бізнесу. Цифрові платформи в цьому контексті розглядаються як спосіб адаптації підприємств до військових умов, збереження виробництва та формування умов для економічного відновлення.

Порівнюючи витрати на надання соціальних послуг до та після появи цифрових інструментів, дослідження І. Мірошниченка та М. Копитка [4] продемонструвало, як цифрові інструменти можуть знизити транзакційні витрати, пришвидшити обробку запитів та знизити ризик корупції. У воєнний час ці ключові фактори безпосередньо впливають на економічну та інституційну стійкість держави.

Деякі питання економічної безпеки України стосувалися створення екосистеми мережі стартапів, які займаються розробкою технологій оборонного сектора економіки [5]. В результаті було в'явлено існування взаємозв'язку між інноваціями у сферу цифрової інфраструктури, розвитком нових бізнес-моделей та підвищенням обороноздатності держави.

Зокрема, такі платформи, як Brave1 та залучення венчурного капіталу, відіграють роль не лише у забезпеченні фронту, а й у підтримці внутрішньої економічної динаміки.

У роботі Т. Ларіної та Н. Лагодієнко [6] обґрунтовано, що стійкість і безпека підприємства зростає за рахунок комплексної інтеграції цифрових інструментів (таких як системи фінансового та екологічного моніторингу, платформи для управління персоналом) з методами системного аналізу ризиків та прогнозової аналітики.

У дослідженні Т. Пушкар [7] класифіковано цифрові платформи, розглянуто три основні моделі цифрової трансформації (поетапну, радикальну та гібридну), а також розглянуто фінансові аспекти впровадження цифрових платформ, такі як зниження операційних витрат і підвищення коефіцієнта рентабельності інвестицій як показники економічної стійкості підприємства.

Практика цифрової трансформації в управлінні підприємствами містить додаткові фактори захисту та збереження публічних даних (особливо ідентифікаційних) та сприяє загальній цифровій грамотності персоналу. Попри відмінності, усі розглянуті дослідження підтверджують: поєднання інституційної цифровізації, бізнес-інновацій та оборонних технологій є основою сучасної економічної стійкості держави. Відсутність наукових досліджень, які б моделювали взаємозв'язки між показниками цифровізації, впровадженням цифрових інструментів та станом економічної безпеки, підкреслює актуальність теми цієї статті.

Викадення основного матеріалу. Важливість економічної безпеки в сучасних умовах цифрової трансформації зростає та набуває ваги для ефективного функціонування підприємств. На нашу думку, економічну безпеку слід розуміти як такий стан національної економіки, за якого

можливо забезпечити високий рівень захисту інтересів кожного суб'єкта від негативного впливу зовнішніх і внутрішніх загроз.

Цифрова трансформація є важливою складовою економічної безпеки. Цифрові платформи («Дія», «Прозорро», «Трембіта») слугують адміністративними та комунікаційними інструментами і компонентами національної оборони під час війни. Навіть у випадках фізичного руйнування вони дозволяють державі продовжувати функціонувати, контролюючи ризики та зберігаючи стабільність фінансової системи.

Застосуємо кількісне моделювання для оцінки ефективності політики цифрової трансформації та з'ясуємо, чи забезпечує поточний рівень цифровізації держави необхідний ступінь економічної безпеки. Для досягнення цієї мети розробимо модель, яка кількісно продемонструє, як на економічну безпеку під час воєнного стану впливає цифрова трансформація державних послуг та інструменти цифрового управління. Ця модель буде використана як аналітичний інструмент для вивчення зв'язку між ступенем цифровізації, частотою ризикових подій та грошовими втратами, понесеними державою.

Запропонована модель ґрунтується на ідеї, що цифрова трансформація послаблює загрозу негативного впливу зовнішніх і внутрішніх факторів на економічний стан України. Модель дозволить визначити, який рівень охоплення цифровими сервісами (D) є достатнім для забезпечення стабільності економічної системи при заданому рівні ризику (R). Тоді модель зміни рівня економічної безпеки можна подати як:

$$\frac{dE(t)}{dt} = C \cdot D(t)(1 - R(t)) - \delta R(t) \cdot (1 - D(t)) - \gamma E(t), \quad (1)$$

де $E(t)$ – рівень економічної безпеки у момент часу t ;

$D(t) \in [0,1]$ – інтегральний показник поширення, доступності та ефективності використання цифрових державних сервісів. (0 – відсутність цифровізації, 1 – повна цифровізація);

$R(t) \in [0,1]$ – це інтегральний показник зовнішніх і внутрішніх загроз, які впливають на економічну систему в момент часу t . (екзогенний вплив: війна, кіберзагрози, інфляція тощо);

C – чутливість економічної системи країни до цифровізації (коефіцієнт ефективності);

γ – коефіцієнт деградації інституцій держави;

δ – швидкість деградації економічної безпеки під впливом ризиків (темп або ступінь зниження здатності інституцій держави ефективно функціонувати й виконувати свої завдання, кількісний параметр, що охоплює такі якісні явища, як бюрократія, корупція, слабка врегулювання і поступове руйнування управлінських механізмів) [13].

Перша складова формули (1) визначає зростання економічної безпеки завдяки цифровим інструментам та низькому ризику; друга складова визначає негативний вплив недостатнього рівня цифровізації, якщо ризики високі; а третя складова відображає природну деградацію державних інституцій без урахування впливу зовнішніх стимулів. Для розрахунку $R(t)$ враховуються такі фактори, як інтенсивність військових дій (наприклад, дані Геншта-

бу); кібератаки (дані CERT-UA, звіти Microsoft); інфляція, валютна нестабільність (дані НБУ, Держстату); рівень пошкодження інфраструктури. Кожен показник (фактор) нормують до шкали від 0 до 1, потім призначається певна «вага» (важливість) і, нарешті, кінцева оцінка $R(t)$ розраховується як середньозважене значення. Стаціонарний стан досягається, коли

$$\frac{dE(t)}{dt} = 0, \quad (2)$$

тобто:

$$E^* = \frac{C \cdot D(t)(1 - R) - \delta R(t) \cdot (1 - D)}{\gamma} \quad (3)$$

Модель дозволяє оцінити вплив політики цифровізації на довгостроковий стан економічної безпеки країни.

Щоб оцінити загальний вплив ризиків на економічну безпеку з урахуванням ступеня цифрової трансформації, додамо до економіко-математичної моделі функцію втрат. Економічні втрати, які держава зазнає при поєднанні високих ризиків та відсутності цифрової трансформації, характеризуються функцією втрат. Функція втрат визначається за формулою:

$$L(t) = \mu \cdot \beta \cdot R(t) \cdot (1 - D(t))^\alpha, \quad (4)$$

де $L(t)$ – функція втрат (економічні втрати від ризиків в момент часу t), визначається як частка ВВП України, грн або дол.

$\alpha \in [0,1]$ – коефіцієнт втрат, залежний від глибини цифрової трансформації (чим більша цифровізація, тим менші втрати);

$\beta \in [0,1]$ – коефіцієнт уразливості економіки до ризиків безпеки;

μ – масштабує загальний обсяг втрат у грошовому вираженні.

Високий ризик $R(t)$ та низький рівень цифровізації $D(t)$ призводять до більших втрат, але вплив глибокої цифровізації менший (через показник степеня $1 - D(t)^\alpha$). Якщо $\alpha = 1$, зменшення збитків є лінійним; якщо $\alpha > 1$, ефект «цифрового щита» зростає, і втрати швидко зменшуються. Максимальна сума збитків визначається параметром μ ; наприклад, 10 мільярдів доларів США у разі масованих кібератак, перебоїв у наданні послуг, припинення соціальних виплат населенню тощо.

Поєднавши формули (1) та (2), описуємо модель як набір рівнянь:

$$\begin{cases} \frac{dE(t)}{dt} = C \cdot D(t)(1 - R(t)) - \delta R(t) \cdot (1 - D(t)) - \gamma E(t) \\ L(t) = \mu \cdot \beta \cdot R(t) \cdot (1 - D(t))^\alpha \end{cases} \quad (5)$$

Використаємо фактичні, загальнодоступні дані для тестування моделі. За оцінками, Україна втратила близько 10 мільярдів доларів США в результаті хакерських атак 2017 року (NotPetya тощо) [8]. Коефіцієнт μ (максимальні потенційні втрати) можна розрахувати за допомогою цих даних [9]. За допомогою цього показника можна оцінити суб'єктивну складову моделі – внутрішній захист від загроз.

У 2021 році Україна посіла друге місце після Сполучених Штатів за кількістю кібератак, що підтверджує тенденцію сильної зосередженості на $R(t)$ у державній інфраструктурі [10].

Цифрові регуляторні інструменти, такі як «Дія», «Трембіта» та «Prozorro», значно підвищили ефективність уряду та здатність держави протистояти війні [2, 11]. Інакше кажучи, рекомендації щодо рівня чутливості C та рівня цифровізації D можуть ґрунтуватися на точних оцінках якості цих послуг.

Станом на 30 жовтня 2024 року понад 21 мільйон унікальних користувачів, або приблизно 50% населення України, вже користувалися додатком «Дія» [12]. Наприклад, у червні 2024 року було зареєстровано 20,5 мільйона користувачів, і, за останніми оцінками, охоплення зросло до 22,56 мільйона користувачів, або приблизно 53% населення.

За даними звіту Асоціації ІТ України, інвестиції в сектор кібербезпеки України, який включає платформи виявлення загроз та стартапи (наприклад, SOC Prime, Mantis Analytics та Osavul), зросли [10].

Таким чином, коефіцієнт μ приймаємо як потенційні максимальні втрати ~ 10 млрд USD, коефіцієнт β можна визначити як $\beta \approx 0,6$, враховуючи масштаби атаки у 2017. Оцінка інтенсивності ризику $R(t)$ за даними по 2021–2022 рр. з масивними кібернападами може триматися на рівні, наприклад, $R \approx 0,8$, враховуючи високий обсяг атак. Індекс цифровізації $D(t)$, у випадку, якщо цифровізація охоплює більшу частину громад (наприклад $> 70\%$ населення користуються «Дією»), можна взяти $D \approx 0,7$.

Тобто визначаємо, що $D = 0,55$ (середнє значення між реєстраціями та активним використанням), $C = 0,45$ (по-

мірна ефективність цифрової трансформації та частковий перехід на е-сервіси), решту параметрів визначаємо, як $R = 0,8$ (високий рівень ризику, війна, кібератаки, інфляція, деструкція), $\delta = 0,2$, $\gamma = 0,1$, $\beta = 0,6$, $\mu = 10000$.

Тоді рівняння набуде вигляду:

$$\frac{dE(t)}{dt} = 0,45 \cdot 0,55(1 - 0,8) - 0,2 \cdot (1 - 0,55) - 0,55E,$$

$$L(t) = 10000 \cdot 0,6 \cdot 0,8 \cdot (1 - 0,55)^2 \approx$$

$$\approx 10000 \cdot 0,6 \cdot 0,8 \cdot 0,2025 \approx 972 \text{ млн дол. США}$$

Розрахунок показує, що навіть при помірному рівні цифровізації (55%) та з достатньою ефективністю впровадження ($C = 0,45$) рівень економічної безпеки знижується в умовах високого ризику ($R = 0,8$). Тобто тільки цифровізації недостатньо, щоб повністю компенсувати вплив воєнних загроз.

Через високий ризик і часткову цифрову трансформацію очікуються економічні втрати у розмірі 972 мільйонів доларів США. Ці втрати можна розглядати як умовну оцінку загальної економічної шкоди, яка виникає щорічно (або протягом іншого фіксованого періоду) в результаті недостатньої цифрової адаптації державних служб (рівень D) під сильним зовнішнім тиском (R). Цифровізація критично важлива, але на рівні 50–60% охоплення населення України вона не забезпечує стійкості, потрібно прагнути $D > 0,75$, щоб компенсувати ризики війни. Втрати значні (понад 900 млн дол. на рік), навіть із відносно високою цифровізацією це означає, що цифрова трансформація має не лише поширюватися, а й бути глибокою та системною.

На рис. 1 показано результати симуляції моделі при зростанні індексу цифровізації D :

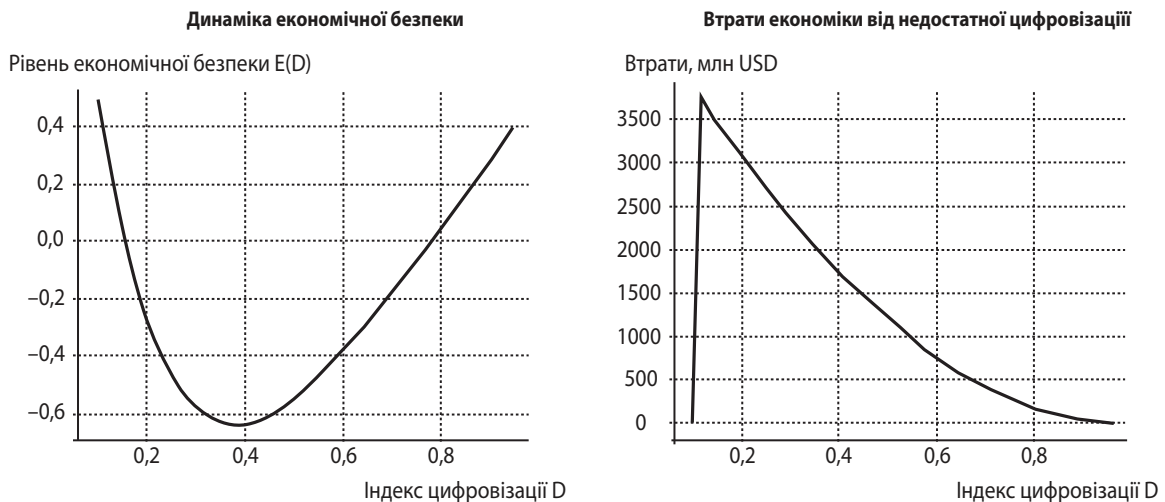


Рис. 1. Симуляція моделі при зростанні індексу цифровізації D

Джерело: сформовано авторами

Графіки показують, що при низькому рівні цифровізації ($D < 0,3$) економічна безпека знижується через високий ризик і слабкий цифровий захист, але починаючи приблизно з $D \approx 0,6$ рівень безпеки стабілізується. Спостерігається стійка тенденція до зростання економічної безпеки при $D > 0,75$. Збитки стають незначними при $D > 0,85$ та зменшуються експоненціально зі збільшенням D .

Для подальшого розвитку моделі було використано методологію мультиагентного моделювання, тобто коли система моделюється як сукупність автономних агентів, кожен із яких має свої правила поведінки, стратегії і взаємодії з іншими, що дозволить суттєво поглибити динамічну картину взаємодії між різними учасниками цифрової екосистеми та їх впливу на економічну безпеку.

Окрім можливості тестування сценаріїв, обґрунтування політики та адаптації моделі до конкретних даних, цей тип моделювання покращує розуміння механізмів економічної безпеки в умовах воєнного часу. Модель дозволяє досліджувати, як різні групи агентів – громадяни, бізнес, уряди, міжнародні організації тощо – взаємодіють у цифровому середовищі, та як це впливає на економічну стійкість, ступінь цифрової довіри, ризики кібератак та можливі втрати. Модель дозволяє тестувати такі сценарії: "Що буде, якщо зросте вплив дезінформації в країні?", "Які агенти найбільше знижують втрати?", "Як цифрова грамотність зменшує ризики?". Групи автономних агентів

мультіагентної економіко-математичної моделі для оцінки впливу цифрової трансформації на економічну безпеку наведено в табл. 1.

Цільова функція мультіагентної економіко-математичної моделі матиме такий вигляд:

$$\max E(t) = \alpha_1 D(t) - \alpha_2 D(t) - \alpha_3 L(t),$$

де $E(t)$ – ефективність цифрової трансформації на момент часу t ;

$D(t)$ – індекс цифрової довіри, узагальнений динамічний показник, що характеризує ступінь залучення користувачів до цифрових платформ;

Таблиця 1

Групи автономних агентів для оцінки впливу цифрової трансформації на економічну безпеку

Агенти	Роль	Вплив на змінні
Громадяни	Користувачі "Дії", які приймають рішення щодо довіри до сервісу	$D(t), R(t)$
Бізнес-структури	Інвестують у цифрову інфраструктуру	$D(t), E(t)$
Урядові агенти	Впроваджують цифрові сервіси, визначають політики безпеки	$D(t), E(t), R(t)$
Кіберзагрози	Імітують кібератаки, фішинг, DDOS-атаки	$R(t), L(t)$
Міжнародні організації	Інвестують у безпеку, реформи	$R(t), D(t), E(t)$
Освітні інституції	Підвищують цифрову грамотність	$R(t), D(t)$
Фінансові інституції	Просувають системи е-платежів, банківських послуг	$D(t), E(t), R(t)$
Деструктивні актори	Дезінформація, підлив довіри до цифрових платформ	$R(t), D(t), L(t)$
Медіа / Інфлюенсери	Впливають на сприйняття безпеки	$D(t), R(t)$
CSIRT / CERT-UA	Знижують втрати та ризики	$L(t), R(t)$
Регулятори	Запроваджують кіберстандарти	$R(t), D(t)$

Джерело: розроблено авторами

$R(t)$ – індекс цифрових ризиків, агрегований показник, що відображає рівень вразливості цифрових платформ до кіберзагроз;

$L(t)$ – інтегральний показник економічних, соціальних та інформаційних втрат, спричинених цифровими ризиками в умовах війни;

α_i – вагові коефіцієнти впливу (розраховуються за методикою АНР).

При обмеженнях:

$0 \leq D(t) \leq 1$ – цифрова довіра, частка користувачів;

$0 \leq R(t) \leq R_{max}$ – ризики атак не можуть бути негативними;

$0 \leq L(t) \leq L_{max}$ – втрати обмежено можливими ресурсами.

$\alpha_1, \alpha_2, \alpha_3 > 0$.

Динаміка цифрової довіри:

$$\frac{dE(t)}{dt} = \beta_1 U(t) + \beta_2 B(t) + \beta_3 F(t) + \beta_4 M(t) + \beta_5 A(t),$$

де $U(t)$ – індекс, який відображає вплив активної участі громадян у цифрових платформах;

$B(t)$ – індекс бізнес-інтеграції, показує, наскільки бізнес бере участь у цифровій економіці;

$F(t)$ – індекс ролі банків, фінтеху в підтримці цифрових платформ;

$M(t)$ – індекс, що вимірює вплив медіа на населення щодо популяризації цифрових платформ;

$A(t)$ – індекс дезінформації, вказує, наскільки сильно ворожа пропаганда та фейки зменшують цифрову довіру;

β_i – вагові коефіцієнти впливу.

Динаміка ризиків визначається формулою:

$$\frac{dR(t)}{dt} = \gamma_1 A(t) - \gamma_2 G(t) + \gamma_3 I(t) + \gamma_4 CSIRT(t),$$

де $G(t)$ – показник неефективності державного управління (наскільки бюрократія знижує економічну безпеку);

$I(t)$ – показник впливу міжнародних криз, інфляції, санкцій на цифрову економіку тощо;

$CSIRT(t)$ – показник ефективності кіберзахисту. Зазвичай має негативне значення у рівнянні, бо витрати на кіберзахист платформ зменшують ресурсну базу, хоча й підвищують стійкість.

γ_i – вагові коефіцієнти впливу.

Інтегральна залежність втрат визначається за формулою:

$$L(t) = \int_0^t \delta_1 R(\tau) \cdot \delta_2 (1 - D(\tau)) d\tau,$$

де $R(\tau)$ – рівень ризику атак і вразливостей у момент часу τ ;

τ – змінна інтегрування, враховує накопичення втрат протягом часу від початку періоду ($t = 0$) до поточного моменту t ;

δ_1 – ваговий коефіцієнт ризику;

δ_2 – ваговий коефіцієнт недовіри.

$G(t) + I(t) + CSIRT(t) \leq B_{res}$ – обмеження ресурсів бюджету на захист платформ.

Модель є детерміновано-стохастичною, тобто частина поведінки задається формулами, а частина – ймовірнісними правилами. Аналіз динаміки поведінки агентів у запропонованій мультиагентній моделі наведено в табл. 2.

Модель показує наявність складної мережі взаємозалежностей між суб'єктами економічної безпеки, можливість моделювання поведінки кожного агента в умовах цифрових загроз, виявлення вразливих місць (наприклад, недостатній зворотний зв'язок від громадян до CERT-UA), а також можливість оцінки ефектів впровадження політик безпеки або змін обсягу інвестицій у певного агента (наприклад, в освіту чи CERT-UA) на загальну стійкість системи.

Матрицю взаємодії агентів цифрової екосистеми економічної безпеки України, яка відображає вплив одних агентів на інших, наведено на рис. 2.

Таблиця 2

Динаміка поведінки агентів системи економічної безпеки в умовах війни

Агенти	Правила поведінки	Змінні стану
1	2	3
Громадяни	Підключаються до цифрових платформ з імовірністю $I(t)$, яка зростає при: - позитивному медіафоні; - зниженні кількості кібератак; - зростанні підтримки від освітніх агентів	Рівень довіри до системи. Припиняють використання платформ, коли $R(t) > \theta_r$ (порог ризику), або поширюється негативна дезінформація $M(t) > \theta_m$
Бізнес-структури	Інвестують у цифрову інфраструктуру, якщо: - довіра громадян зростає $D(t) > \theta_d$, або - спостерігається стабільність $R(t)$, $L(t)$	Розмір інвестицій
Урядові агенти	Розширюють сервіси, якщо: - зростає цифрова довіра; - отримують зовнішню допомогу; - падає ефективність старих рішень	кількість нових сервісів; активні користувачі урядових сервісів
Кіберзагрози	Здійснюють атаки з інтенсивністю, що залежить від: - зростання довіри громадян, атаки частішають, - активності CERT-UA, атаки зменшуються	Ddos атаки, фішинг, злом реєстрів, deepfake-кампанії
Міжнародні організації	Інвестують при: - зростанні кіберзагроз; - наявності відкритої цифрової звітності; - запиті з боку уряду	обсяг підтримки; тип підтримки (технологічна, інституційна, освітня)
Освітні інституції	Реагують на: - падіння цифрової довіри, активізують кампанії; - зростання атак, запроваджують нові курси	охоплення громадян освітніми ініціативами; рівень цифрової обізнаності
Фінансові інституції	Збільшують використання цифрових платформ, якщо: - уряд просуває криптовалюту; - інші агенти не знижують довіру	Обсяг цифрових послуг
Деструктивні актори	Поширюють дезінформацію коли: - спостерігається позитивний тренд довіри; - міжнародна підтримка зростає	кількість фейків; обсяг охоплення аудиторії недовірою
Медіа та інфлюенсери	Поширюють наративи на основі: - активності уряду; - поведінки атакуючих агентів; - міжнародного тиску	Обсяг охоплення аудиторії

1	2	3
CSIRT / CERT-UA	- здійснюють заходи при перевищенні рівня кібератак; - ефективність залежить від бюджету та міжнародної підтримки	Стан системи кіберзахисту
Регулятори	Змінюють нормативні документи, коли: - зростає інцидентність; - міжнародні партнери рекомендують зміни	- рівень нормативного захисту - відповідність стандартам

Джерело: розроблено авторами

Матриця впливу агентів одне на одного (1 = є вплив)

Громадяни	0	1	1	0	0	0	0	0	0	0	0
Бізнес	0	0	1	0	0	0	0	1	0	0	0
Уряд	0	0	0	0	0	0	0	0	1	0	0
Кібератаки	1	0	1	0	0	0	0	0	0	0	0
Дезінфо	1	0	0	0	0	0	0	0	0	0	0
Освіта	1	0	0	0	0	0	0	0	0	0	0
Міжнародні організації	0	0	1	0	0	0	0	0	1	0	0
Фінанси	0	0	0	0	0	0	0	0	0	0	0
CERT-UA	0	0	0	1	0	0	0	0	0	0	0
Регулятори	0	1	1	0	0	0	0	0	0	0	0
Медіа	1	1	0	0	0	0	0	0	0	0	0
	Громадяни	Бізнес	Уряд	Кібератаки	Дезінфо	Освіта	Міжнародні організації	Фінанси	CERT-UA	Регулятори	Медіа

Рис. 2. Матриця взаємодії агентів цифрової екосистеми економічної безпеки України

Джерело: сформовано авторами

Матриця дає можливість формування сценаріїв стійкості, наприклад, як зміниться система, якщо посилити фінансування CERT-UA або якщо зменшиться активність медіа, а також для верифікації економіко-математичної моделі, де кожен агент має власну динаміку впливу на цільову функцію (економічну безпеку).

Граф взаємозв'язків агентів цифрової екосистеми економічної безпеки на основі цієї матриці наведено на рис. 3.

Вузли (агенти) показані на графі, це громадяни, бізнес, уряд, CERT-UA, медіа, освітні установи, міжнародні організації, фінансові установи, регулятори, актори дезін-

формації, кіберзагрози. Направлені ребра графа показують, хто на кого впливає. Наприклад: Уряд впливає на CERT-UA, CERT-UA реагує на кіберзагрози, освіта формує свідомість громадян, медіа впливає на сприйняття цифровізації як громадянами, так і бізнесом, дезінформація впливає на громадян. Цей граф дозволяє виявляти критичні вузли, які є найбільш пов'язаними (наприклад, уряд, громадяни, CERT-UA), моделювати каскадні ефекти (наприклад, послаблення кіберзахисту впливає на бізнес та уряд через CERT-UA) та планувати політику кібер- та інформаційної безпеки держави, наприклад, шляхом підсилення впливу освіти або міжнародної підтримки.

Граф взаємодії агентів цифрової економічної безпеки

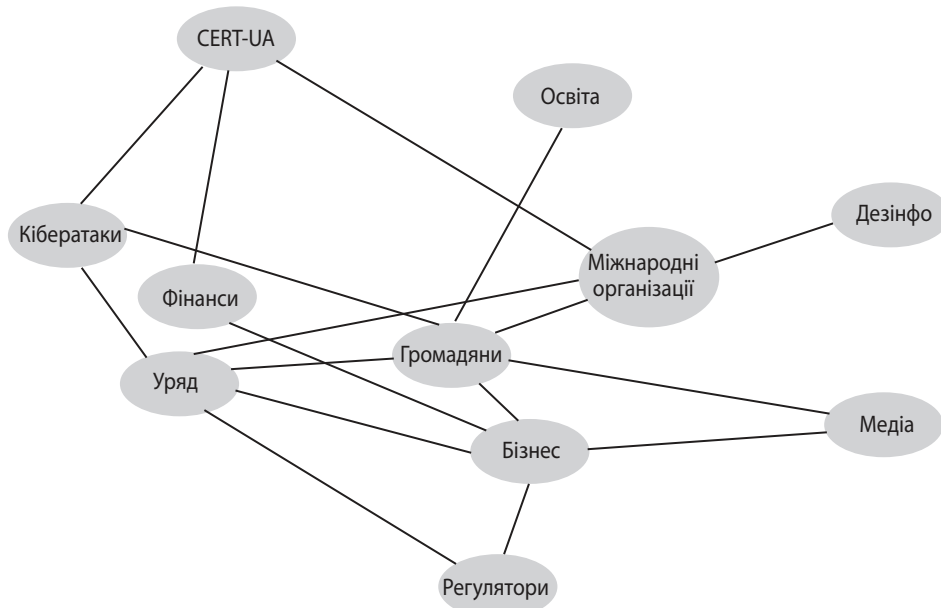


Рис. 3. Граф взаємодії агентів цифрової екосистеми економічної безпеки України

Джерело: сформовано авторами

Це спрощена модель, яка ігнорує тривалість інцидентів, асиметричний вплив подій (наприклад, втрата бази даних реєстру є більш критичною, ніж інцидент із збоєм вебсайту) та різні типи збитків (прямі економічні, втрата даних та соціальні наслідки). Оскільки умови воєнного стану пов'язані з раптовими зовнішніми факторами, модель також потребує додаткових досліджень і вдосконалення.

Висновки. За допомогою запропонованої моделі можна кількісно оцінити, як цифрова трансформація впливає на фінансову стабільність українського бізнесу під час конфлікту. Для розширення моделі, яка включає системну динаміку та функцію збитків, можна використовувати багатоагентне моделювання.

Результати моделювання підтверджують, що для підтримки економічної стабільності критично важливим є рівень цифровізації, що перевищує 75%. Модель, що використовується, дозволяє визначити коефіцієнт охоплення цифровими послугами (коефіцієнт D), необхідний для забезпечення економічної стабільності при певному рівні ризику (коефіцієнт R).

Державні органи можуть використовувати модель для обґрунтування інвестицій у цифрову інфраструктуру як засобу зниження втрат (коефіцієнт $L(t)$). Це важливо для: бюджетного планування; розробки стратегій цифровізації; адаптації сервісів до регіональних особливостей.

Під час конфлікту цифрові послуги зменшують наслідки соціальних маніпуляцій, дезінформації та кібератак. Аналіз цього впливу дозволяє нам оцінити очікувані фінансові втрати у разі недостатньої цифровізації та створити сценарії для відбиття загроз.

Типи агентів, моделювання їхньої адаптивної поведінки, вивчення каскадних сценаріїв відмов та оптимізація ресурсів мають бути основними цілями майбутніх досліджень багатоагентної моделі, запропонованої у статті. По-

єднання моделі з платформами цифрової безпеки для візуалізації ризиків у режимі реального часу є перспективним напрямком. Це дозволить створити базу даних для розробки інструментів раннього попередження про ризики та стратегічного планування заходів безпеки.

ЛІТЕРАТУРА

1. Кабачинський І. Diia.City – 3 роки: Як новий податковий простір трансформує IT-індустрію України // UNITED24 Media. 2025. URL: <https://united24media.com/business/diacity-3-years-how-the-new-tax-space-is-transforming-ukraines-it-industry-5814>
2. Digital Resilience in Ukraine During War // Brookings Institution. URL: <https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war>
3. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine // OECD. 2024. URL: <https://www.oecd.org/>
4. Мірошниченко І., Копитко М. Економічна ефективність електронного урядування в умовах війни. *Економіка та держава*. 2023. № 10. С. 41–45.
5. Mysyshyn A. Ukraine's WarTech Ecosystem: How Tech Startups Power Defense and Economy // GMFUS. 2024. URL: <https://www.gmfus.org>
6. Ларіна Т., Лагодієнко Н., Уваров С. Інтеграція цифрових інструментів в процес забезпечення економічної безпеки підприємства. *Актуальні питання економічних наук*. 2024. № 3-4. DOI: <https://doi.org/10.5281/zenodo.14613693>
7. Пушкар Т. Цифрові платформи як інструмент оптимізації стратегічних рішень. *Сталий розвиток економіки*. 2025. № 2 (53). С. 213–220. DOI: <https://doi.org/10.32782/2308-1988/2025-53-29>
8. The Threat of Russian Cyberattacks Looms Large // The New Yorker. URL: <https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large>

9. Ukraine's IT Army: The World's First Cyberwarfare Force – But a Gamble // Business Insider. URL: <https://www.businessinsider.com/ukraines-it-army-world-first-cyberwarfare-but-a-gamble-2024-7>

10. Ukraine Cybersecurity Market Review 2023 // IT Ukraine Association. URL: <https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf>

11. 21 млн українців користуються Дією // Міністерство цифрової трансформації України. URL: <https://diia.gov.ua/>

12. Скільки українців користуються застосунком «Дія» // Speka. URL: <https://speka.media/skilki-ukrayinciv-koristuyutsya-zastosunkom-diya-9wnzj3>

13. Інституційна (не)спроможність держави в Україні: як розірвати замкнене коло : монографія / наук. ред. Г. І. Зеленько. Київ : ІПіЕнД ім. І. Ф. Кураса НАН України, 2025. 480 с.

REFERENCES

Brookings Institution. (n.d.). Digital Resilience in Ukraine During War. Retrieved from <https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war>

Business Insider. (n.d.). Ukraine's IT Army: The World's First Cyberwarfare Force – But a Gamble. Retrieved from <https://www.businessinsider.com/ukraines-it-army-world-first-cyberwarfare-but-a-gamble-2024-7>

IT Ukraine Association. (n.d.). Ukraine Cybersecurity Market Review 2023. Retrieved from <https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf>

Kabachynskyi, I. (2025). Diia.City – 3 roky: Yak novyi podatkovyi prostir transformuie IT-industriiu Ukrainy [Diia.City – 3 years: How the new tax space is transforming Ukraine's IT industry]. *UNIT-ED24 Media*. Retrieved from <https://united24media.com/business/diiacity-3-years-how-the-new-tax-space-is-transforming-ukraines-it-industry-5814>

Larina, T., Lahodiienko, N., & Uvarov, S. (2024). *Intehratsiia tsyfrovyykh instrumentiv v protses zabezpechennia ekonomichnoi*

bezpeky pidpriemstva [Integration of digital tools in the process of ensuring the economic security of the enterprise]. *Aktualni pytannia ekonomichnykh nauk*, 3-4. <https://doi.org/10.5281/zenodo.14613693>

Ministerstvo tsyfrovoi transformatsii Ukrainy. (n.d.). 21 mln ukraintsiiv korystuiutsia Diieiu [21 million Ukrainians use Diia]. Retrieved from <https://diia.gov.ua/>

Miroshnychenko, I., & Kopytko, M. (2023). *Ekonomichna efektyvnist elektronnoho uriaduvannia v umovakh viiny* [Economic efficiency of e-governance in the context of war]. *Ekonomika ta derzhava*, 10, 41–45.

Mysyshyn, A. (2024). Ukraine's WarTech Ecosystem: How Tech Startups Power Defense and Economy. *GMFUS*. Retrieved from <https://www.gmfus.org>

The New Yorker. (n.d.). The Threat of Russian Cyberattacks Looms Large. Retrieved from <https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large>

OECD. (2024). Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Retrieved from <https://www.oecd.org/>

Pushkar, T. (2025). *Tsyfrovii platformy yak instrument optymizatsii stratehichnykh rishen* [Digital platforms as a tool for optimizing strategic decisions]. *Stalyi rozvytok ekonomiky*, 2(53), 213–220. <https://doi.org/10.32782/2308-1988/2025-53-29>

Speka. (n.d.). Skilky ukraintsiiv korystuiutsia zastosunkom «Diia» [How many Ukrainians use the Diia app]. Retrieved from <https://speka.media/skilki-ukrayinciv-koristuyutsya-zastosunkom-diya-9wnzj3>

Zelenko, H. I. (Ed.). (2025). *Instytutsiina (ne)spromozhnist derzhavy v Ukraini: yak rozirvaty zamknene kolo* [Institutional (in)ability of the state in Ukraine: how to break the vicious circle]: monohrafiia. IPiEnD im. I. F. Kurasa NAN Ukrainy. Kyiv.

Стаття надійшла до редакції 29.08.2025 р.
Статтю прийнято до публікації 13.09.2025 р.