# МАТЕМАТИЧНА МОДЕЛЬ ЕКОНОМІЧНОЇ СТІЙКОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З УРАХУВАННЯМ ПОКАЗНИКІВ ВІДМОВОСТІЙКОСТІ

# MATHEMATICAL MODEL OF THE ECONOMIC RESILIENCE OF TELECOMMUNICATION SYSTEMS CONSIDERING FAULT-TOLERANCE INDICATORS

УДК 330.4:004.056.5

DOI: https://doi.org/10.32782/dees.19-66

**Янко А.С.**[1]
к.т.н., доцент,
доцент кафедри комп'ютерних та інформаційних технологій і систем,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
**Маслій О.А.**[2]
к.е.н., доцент,
доцент кафедри фінансів, банківського бізнесу та оподаткування,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

**Yanko Alina**
National University «Yuri Kondratyuk Poltava Polytechnic»
**Maslii Oleksandra**
National University «Yuri Kondratyuk Poltava Polytechnic»

*У статті досліджено взаємозв'язок між відмовостійкістю телекомунікаційних систем та економічною ефективністю їх функціонування. Особливу увагу приділено визначенню оптимального балансу між технічними показниками надійності та фінансовими витратами. Запропоновано математичну модель коефіцієнта економічної стійкості (КЕС), яка інтегрує ключові технічні параметри (інтенсивність відмов, середня тривалість простою) з економічними чинниками. Модель дозволяє кількісно оцінити економічну доцільність інвестицій у надійність, визначити критичні точки невиправданих витрат та прогнозувати вплив технічних удосконалень на фінансові результати. Отримані результати особливо актуальні для формування безпекоорієнтованого інформаційного середовища національної економіки та підвищення стійкості мереж і критичної інфраструктури до зовнішніх та внутрішніх загроз в умовах воєнних дій.*
**Ключові слова:** *телекомунікаційна система, відмовостійкість, резервування, економічна ефективність, коефіцієнт економічної стійкості, надійність, економічна безпека, критична інфраструктура.*

*This article explores the relationship between fault tolerance in telecommunication systems and their economic efficiency, focusing on balancing technical reliability with financial costs in critical infrastructures. A mathematical model of the Economic Resilience Coefficient (ERC) is proposed, integrating technical parameters (failure intensity, downtime duration) with economic factors (capital/operational expenditures, downtime losses, SLA penalties). This model enables quantitative evaluation of reliability investments, identification of cost-justification thresholds, and prediction of how technical improvements impact financial outcomes. It supports sensitivity analysis of key parameters, providing a methodological basis for optimal network development strategies under uncertainty – particularly vital in sectors where downtime causes significant financial and reputational damage. The ERC model facilitates formation of a security-oriented information environment that strengthens telecommunication network resilience against external and internal threats. Practically, it enables operators and policymakers to optimize investment allocation, minimize unnecessary expenditures, and enhance system disruption resistance. This is especially critical for Ukraine under ongoing military aggression, where information and communication stability directly supports national economic security. The model also serves post-war reconstruction by guiding development of reliable, economically sustainable telecommunication infrastructures underpinning digital transformation. By linking fault tolerance with economic performance within a systemic security framework, this research advances theoretical and applied foundations for national economic resilience. Results emphasize integrating reliability management, economic efficiency, and information security into unified strategies that reinforce financial and communication system stability. The study demonstrates that fostering security-oriented information environments is essential for enhancing economic security during wartime and ensuring long-term post-war recovery and sustainable development.*
**Key words:** *telecommunications system, fault tolerance, redundancy, economic efficiency, economic sustainability coefficient, reliability, economic security, critical infrastructure.*

**Постановка проблеми.** Сучасні процеси цифрової трансформації супроводжуються інтенсифікацією ризиків і загроз в інформаційному просторі та підвищенням уразливості інформаційних систем, що зумовлює необхідність забезпечення функціонування національної економіки на засадах інформаційної захищеності. Забезпечення економічної безпеки держави та безперервності функціонування стратегічно важливих секторів в умовах воєнних дій вимагає формування безпекоорієнтованого інформаційного середовища суспільних відносин, яке базується на використанні високонадійних систем захисту даних, підвищенні резистентності телекомунікаційних мереж і об'єктів критичної інфраструктури до деструктивних впливів зовнішніх та внутрішніх загроз.

Сучасні телекомунікаційні мережі – це основа цифрової економіки та суспільного життя, адже вони забезпечують постійний обмін інформацією між бізнесом, державою і громадянами. Через дедалі більшу залежність різних сфер від надійності цифрових сервісів навіть короткий збій може призвести до серйозних проблем для компаній чи навіть усієї країни, особливо під час воєнних дій [1]. Якщо ключові елементи мережі виходять з ладу, це спричиняє низку негативних наслідків:

– прямі фінансові втрати через зупинку сервісів та недоотриманий дохід;

[1] ORCID: https://orcid.org/0000-0003-2876-9316
[2] ORCID: https://orcid.org/0000-0003-2184-968X

– непрямі економічні втрати у вигляді штрафів за невиконання умов договорів та компенсацій клієнтам;

– репутаційні ризики, що знижують довіру споживачів та інвесторів;

– підвищення витрат на відновлення працездатності мережі та її елементів.

Надійність телекомунікаційних систем залежить від їхньої здатності працювати без збоїв навіть під час аварій [2]. У сучасній цифровій економіці, де фінансові операції, бізнес-процеси та державні послуги повністю залежать від стабільного зв'язку, навіть короткочасний збій може призвести до колосальних збитків. За даними дослідження Uptime Institute, понад 60% організацій повідомляють про збитки понад 100 000 доларів від однієї серйозної аварії, а 16% – понад 1 мільйон доларів. Останні гучні інциденти, як-от збій програмного забезпечення CrowdStrike у 2024 році, призвели до втрат понад 5,4 мільярда доларів для компаній зі списку Fortune 500 лише за один день, при цьому найбільш постраждалими стали сектори охорони здоров'я та фінансів. Ці випадки наочно демонструють, як вразлива структура мережі та недостатня надійність критично важливих компонентів посилюють збитки [3]. У практичній моделі резервування банківських сервісів дослідження показало, що вкладення в надлишкові сервіси покращують операційну ефективність і задоволеність клієнтів, але надмірне дублювання без обґрунтування призводить до невиправданих витрат [4].

Традиційні технічні метрики, такі як середній час безвідмовної роботи та доступність, ефективно описують технічний стан мережі, але не враховують економічні наслідки аварій. У сучасних умовах цього недостатньо, адже може призвести до великих фінансових втрат, особливо у сферах з високими вимогами до Угода про рівень обслуговування (УРО, з анг.мови – Service Level Agreement). Потреба у комплексній моделі також зумовлена розвитком сучасних методів захисту та зберігання даних, які стають ключовим елементом у забезпеченні відмовостійкості [5]. Дослідження IBM Global Services, зазначає, що середня вартість простою або несподіваного збою програмного застосування становить понад 400 000 доларів за годину для великих організацій [6]. Це створює потребу у комплексній моделі, яка поєднує технічні та економічні аспекти управління надійністю.

**Аналіз останніх досліджень і публікацій.** У сучасному світі, де цифрова трансформація набирає обертів, вимоги до якості послуг зростають, а умови контрактів стають більш суворими, що змушує операторів шукати нові способи управління надійністю та економічною ефективністю мереж. Тому в наукових дослідженнях дедалі більше уваги приділяється інтегрованим моделям, які об'єднують технічні й економічні параметри. Так, Юрчич В. та співавтори [7] розробили комплексну модель оцінки технічно-економічного потенціалу телекомунікаційних операторів, що поєднує технологічні характеристики, економічні показники та вплив ринкових умов. Модель аналізує простої в мережах та серверах, підвищуючи точність стратегічного планування й знижуючи економічні ризики. Бішт С. та ін. [8] пропонують показники для оцінки важливості мережевих вузлів, що допомагає виявляти критичні точки та розробляти стратегії резервування, скорочуючи витрати через простої. Русек К. та ін. [9] рекомендують застосовувати параметр Value-at-Risk для оцінки бізнес-ризиків у телекомунікаційних мережах, перетворюючи технічні збої на фінансові показники з урахуванням штрафів за порушення сервісів, що особливо важливо в кризових умовах.

Гіларі Франк та ін. [10] розглядають архітектури приватних 5G-мереж з точки зору інвестиційної привабливості, операційних витрат і ризиків простоїв, ілюструючи співвідношення витрат на обслуговування, енергоресурси та управління несправностями. Дослідження демонструє, що вдалий вибір архітектури знижує фінансові ризики під час збоїв, показуючи практичне застосування КЕС для порівняння архітектур і знаходження оптимального балансу між надійністю та економічною ефективністю. Звіт TUM [11] систематизує підходи для повної оцінки вартості володіння мережею з урахуванням капітальних та експлуатаційних витрат, енергоспоживання та відновлення, акцентуючи на життєвому циклі інфраструктури та економічних ризиках, що дозволяє узгодити параметри КЕС з довгостроковими прогнозами. Кумар А. та ін. [12] аналізують модель із апаратним та програмним забезпеченням, демонструючи залежність прибутку і доступності від параметрів відмов: витрати зростають із частотою збоїв, а середній час до відмови падає зі збільшенням коефіцієнтів відмов, але зростає при вищих коефіцієнтах ремонту. Байрон Дж. та ін. [13] показують експоненційне зростання витрат при підвищенні надійності: перехід від 99,9% до 99,999% доступності може збільшити витрати в рази. Моделі демонструють, що дешевші диски без резервування можуть бути економічно вигіднішими за 25 років, ніж дорогі надійні носії, допомагаючи визначити доцільність інвестицій у надлишковість. Для підтвердження значення оцінки простоїв щодо витрат у дослідженні Ванга Г. та ін. [14] проаналізовано понад 290000 випадків збоїв обладнання в дата-центрах й здійснено оцінювання частоти відмов серверів, втрати продуктивності та вплив на показники УРО.

З огляду на активну розробку у сучасних дослідженнях методології інтеграції технічних параметрів надійності телекомунікаційних систем з економічними показниками ефективності, моделювання

взаємозв'язків між архітектурою мережі, частотою відмов, операційними витратами та фінансовими ризиками простоїв, актуалізується проблематика розробки комплексного коефіцієнта економічної стійкості телекомунікаційних систем.

**Постановка завдання.** Мета дослідження – розроблення математичної моделі оцінювання економічної стійкості телекомунікаційних систем на основі інтеграції показників відмовостійкості для оптимізації інвестиційних рішень у сфері критичної інфраструктури в умовах підвищених безпекових ризиків.

**Виклад основного матеріалу дослідження.** Надійність телекомунікаційних систем суттєво впливає на економічну безпеку компаній і держави загалом [19]. Процедура забезпечення відмовостійкості на основі альтернативних математичних моделях є одним із прикладів технічних рішень, що підвищують надійність системи [6, 15]. У сучасних умовах збій мережі може призвести до серйозних наслідків. Тому необхідна комплексна модель, яка враховує не лише технічні аспекти надійності, а й економічні фактори.

Розглянемо поетапне створення математичної моделі коефіцієнта економічної стійкості (КЕС), що об'єднує показники надійності та економічні дані в єдину систему.

Телекомунікаційні системи мають два основні типи витрат:

*КВ* – капітальні вкладення в інфраструктуру (мережеве обладнання, сервери, будівництво веж, канали зв'язку);

*ЕВ* – експлуатаційні витрати (короткострокові витрати, які компанія несе для ведення бізнесу).

Формула для базових витрат виглядає так:

$$M_б = M_{КВ} + M_{ЕВ}(t), \quad (1)$$

де $M_{КВ}$ – початкові інвестиції (не змінюються з часом); $M_{ЕВ}(t)$ – накопичені операційні витрати до часу $t$.

Ця формула відображає базовий рівень економічних витрат без урахування збоїв і ризиків. Несправність компонентів телекомунікаційної мережі спричиняє додаткові витрати, пов'язані з простоями сервісів, ремонтом і штрафами за порушення умов контрактів. Для їх обчислення вводиться поняття інтенсивності відмови $\lambda(t)$, яка описує середню кількість відмов на одиницю часу:

$$M_{втр}(t) = \lambda(t) \times T(t) \times M_{пр}, \quad (2)$$

де $\lambda(t)$ – інтенсивність відмов на момент часу $t$; $T(t)$ – середня тривалість одного простою; $M_{пр}$ – економічні втрати за одиницю часу простою.

Ця формула дає змогу оцінити витрати на простої залежно від рівня надійності мережі та важливості сервісів. Отже, загальна вартість володіння системою на момент часу $t$ виглядатиме як сума рівнянь (1) та (2):

$$M_в = M_б(t) + M_{втр}(t) \quad (3)$$

Імовірність безперебійної роботи системи описується класичною функцією надійності: зі зростанням надійності $R(t)$ фінансові втрати від збоїв скорочуються, що прямо впливає на доходи оператора.

Щоб врахувати вплив надійності на прибуток, вводимо поняття очікуваного економічного результату:

$$E = N(t) \times L(t), \quad (4)$$

де $N(t)$ – ймовірність безвідмовної роботи у момент часу $t$; $L(t)$ – загальний дохід від надання послуг до моменту часу $t$, €.

У реальних системах частина збитків пов'язана з контрактними зобов'язаннями перед клієнтами, зокрема УРО. Запроваджуємо коефіцієнт штрафів і репутаційних втрат $k_{УРО}$, який визначає масштаби загальних втрат:

$$M_ш = k_{уро} \times M_{втр}(t), \quad (5)$$

де $k_{УРО}$ – коефіцієнт штрафів і репутаційних втрат, безрозмірний $k_{УРО} > 1$. Наприклад, якщо компанія має жорсткі контрактні зобов'язання, навіть невеликий простій може призвести до великих штрафів, і тоді $k_{УРО}$ може бути 2–3. Таким чином, формула повних витрат з урахуванням УРО є сумою рівнянь (3) та (5):

$$M_б = M_{КВ} + M_{ЕВ}(t) + k_{УРО} \times M_{втр}(t) \quad (6)$$

Підсумовуючи всі попередні кроки, вводимо базове рівняння коефіцієнту економічної стійкості:

$$KEC(t) = \frac{N(t) \times L(t)}{M_{КВ} + M_{ЕВ}(t) + k_{УРО} \times \lambda(t) \times T(t) \times M_{пр}}, \quad (7)$$

де $N(t)$– ймовірність безвідмовної роботи системи у момент часу $t$; $L(t)$ – дохід від надання послуг за час $t$, €; $M_{КВ}$ – капітальні інвестиції, €; $M_{ЕВ}(t)$ – накопичені операційні витрати, €; $\lambda(t)$ – інтенсивність відмов у момент часу $t$, [відмов/год]; $T(t)$ – середня тривалість простою, [години]; $M_{пр}$ – економічні втрати за 1 годину простою, €/год; $k_{УРО}$ – коефіцієнт штрафів та репутаційних втрат.

Вихідні значення коефіцієнту можна розглядати так: якщо $KEC(t) > 1$ – система економічно вигідна: доходи перевищують витрати та збитки; якщо $KEC(t) = 1$ – система функціонує на рівні беззбитковості; якщо $KEC(t) < 1$ – система економічно нестійка, потрібна оптимізація витрат або підвищення надійності.

Формулювання задачі оптимізації для оператора має такий вигляд:

$$\max_{x \in X} KEC(t), \quad (8)$$

де $x$ – вектор керуючих змінних (рівень резервування, топологія мережі, УРО, графік технічного обслуговування); $X$ – область допустимих рішень.

Графік (див. рис. 1) ілюструє, як змінюється КЕС залежно від рівня надійності системи у сценарії, коли інші економічні та технічні параметри залишаються фіксованими.

Для репрезентативного прикладу масштабу доходів та інвестицій використовуємо показники групи Deutsche Telekom за 2024 рік: дохід від послуг склав 96,5 мільярдів євро, а КВ становив приблизно 16,0 мільярдів євро (як орієнтир для інвестицій) – дані з офіційного річного звіту [16].

Вартість простоїв. Аналіз понад 290 000 випадків збоїв, проведений у дослідженні Ванга та ін. [14], дозволив встановити частоту відмов обладнання та їхній вплив на сукупні втрати продуктивності. Ці дані були зіставлені з результатами щорічних досліджень Uptime Institute [17], які підтверджують, що вартість інцидентів значно зросла. Замість загальних відсоткових показників (які вже згадані у вступі), у нашій моделі $M_ч$ – вартість години простою – може бути визначена з урахуванням цих реальних інцидентів.

Для оцінки розподілу простоїв за частотою та тривалістю збоїв використовуємо відкриту статтю з моделлю дискретного ланцюга Маркова, що базується на 1211 записах щоденних збоїв мобільних мереж: більшість збоїв – «незначні», а серйозні чи тяжкі трапляються рідко (2–5%). Це підтверджує доцільність сценарного підходу з фокусом на кількох «значущих» інцидентах на рік [18].

Щоб поєднати статистику простоїв з економічними показниками інцидентів, детальніше розкладемо складову втрат рівняння (2):

$$M_{втр}(t) = \lambda_i(t) \times T \times M_ч , \quad (9)$$

де $\lambda_i(t)$ – кількість значущих інцидентів на рік; $T$ – середня тривалість такого інциденту на рік; $M_ч$ – вартість години простою (€/год) з урахуванням штрафів/компенсацій/репутаційних ефектів. Діапазони $M_ч$ узгоджуємо з часом. Наприклад, для серйозних збоїв вона може сягати сотень тисяч або навіть мільйонів євро на годину, що дозволяє визначити реалістичні межі для економічних втрат у моделі.

З урахуванням рівняння (9) виведемо оновлене рівняння (7):

$$KEC(t) = \frac{N(t) \times L(t)}{M_{КВ} + M_{EB}(t) + k_{уро} \times \lambda_i(t) \times T \times M_ч} \quad (10)$$

Графік (див. рис. 2) показує, як змінюється коефіцієнт економічної стійкості залежно від величини ефективних втрат від простоїв при фіксованому рівні надійності системи $R$ = 0,97. Навіть за стабільної технічної надійності зростання штрафів або вартості години простою швидко знижує КЕС. Це підкреслює важливість інвестування у заходи, що скорочують тривалість та частоту збоїв.

На графіку (див. рис. 3) наводяться криві байдужості КЕС у площині двох ключових економічних параметрів КВ та ЕВ, демонструючи компроміс між модернізацією та економією ресурсів.

Графік (див. рис. 4) демонструє різницю між новою економічною метрикою КЕС і класичною технічною метрикою доступності у просторі двох змінних, де червоні зони: КЕС значно вищий за доступність – економічні фактори стають визначальними, а сині зони: різниця між КЕС та доступністю мінімальна – технічна надійність домінує.

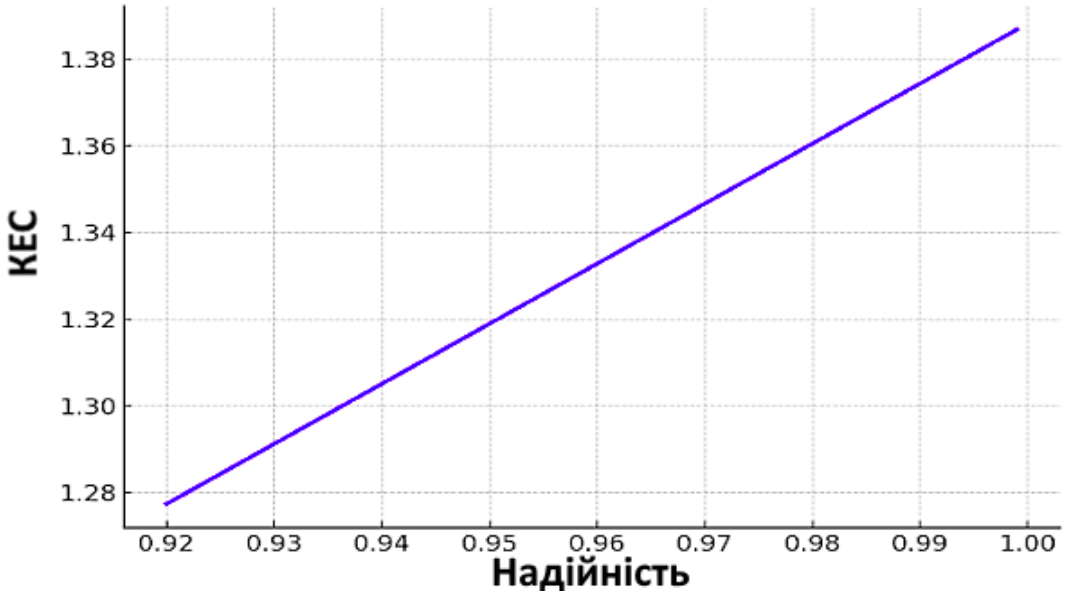


**Рис. 1. Відношення КЕС до надійності**

*Джерело: сформовано авторами*

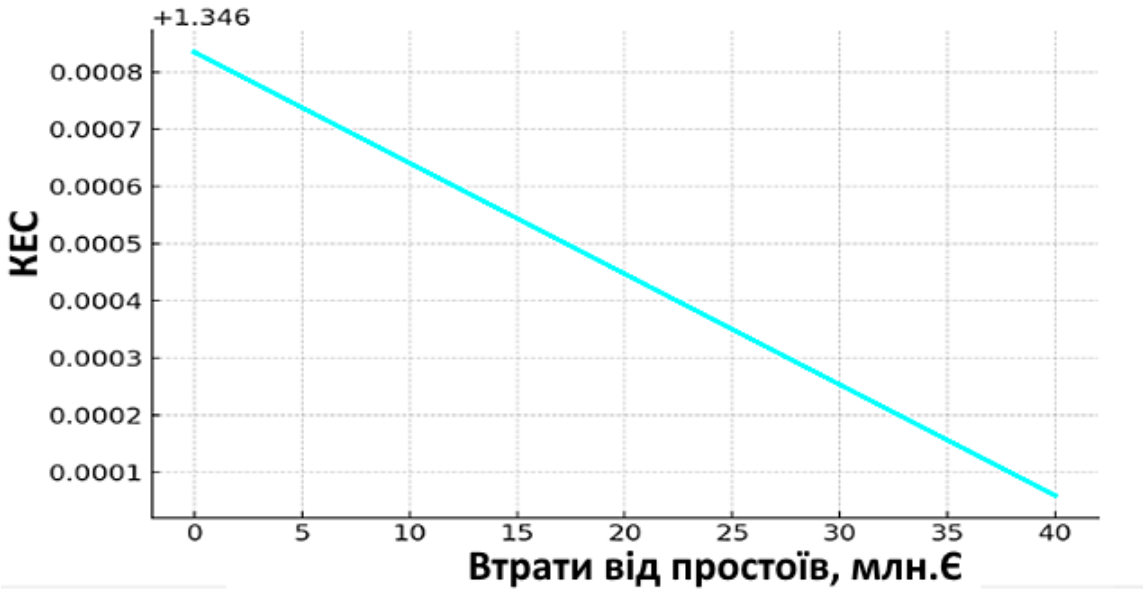


**Рис. 2. Оцінка чутливості КЕС до змін у втраті від простоїв та штрафів**

*Джерело: сформовано авторами*

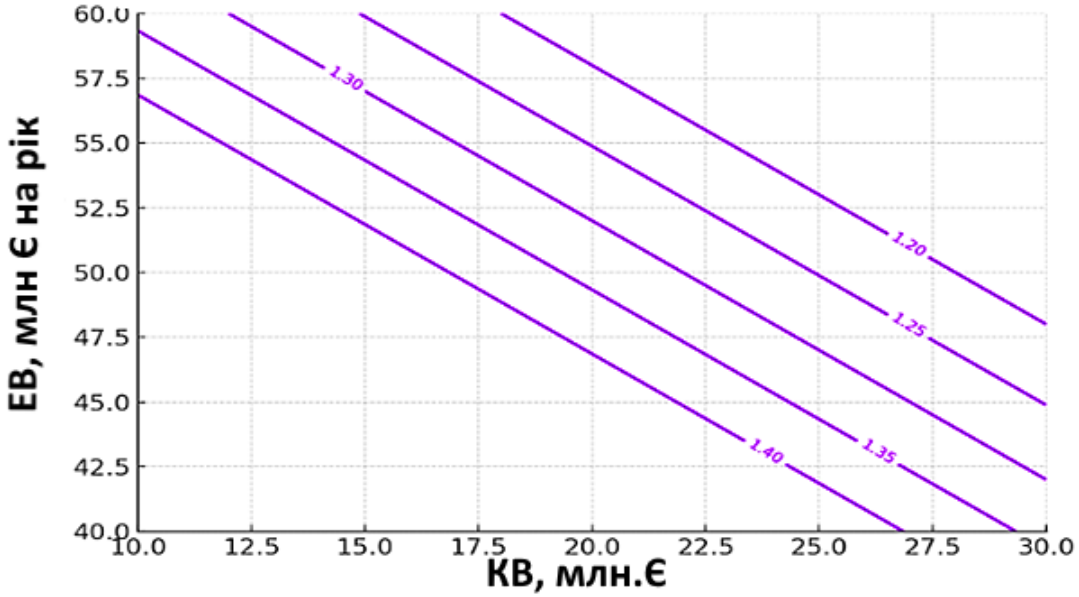


**Рис. 3. Криві байдужості КЕС для компромісу між КВ та ЕВ**

*Джерело: сформовано авторами*

Під час воєнних дій телекомунікаційні системи набувають статусу критичної національної інфраструктури, що зумовлює підвищені вимоги до їхньої стійкості та надійності. Зміни в зовнішніх умовах впливають на всі складові формули КЕС. Тому пропонується додати до КЕС (7) спеціальний коефіцієнт $k_в$, що враховує додатковий ризик воєнних дій:

$$KEC_в(t) = \frac{N(t) \times L(t)}{M_{KB} + M_{EB}(t) + k_{УРО} \times \lambda(t) \times T(t) \times M_{пр} + k_в \times M_в(t)}, \quad (11)$$

де $k_в$ – коефіцієнт впливу війни на економіку системи, $k_в > 1$; $M_в(t)$ – прямі витрати на відновлення обладнання після фізичного руйнування.

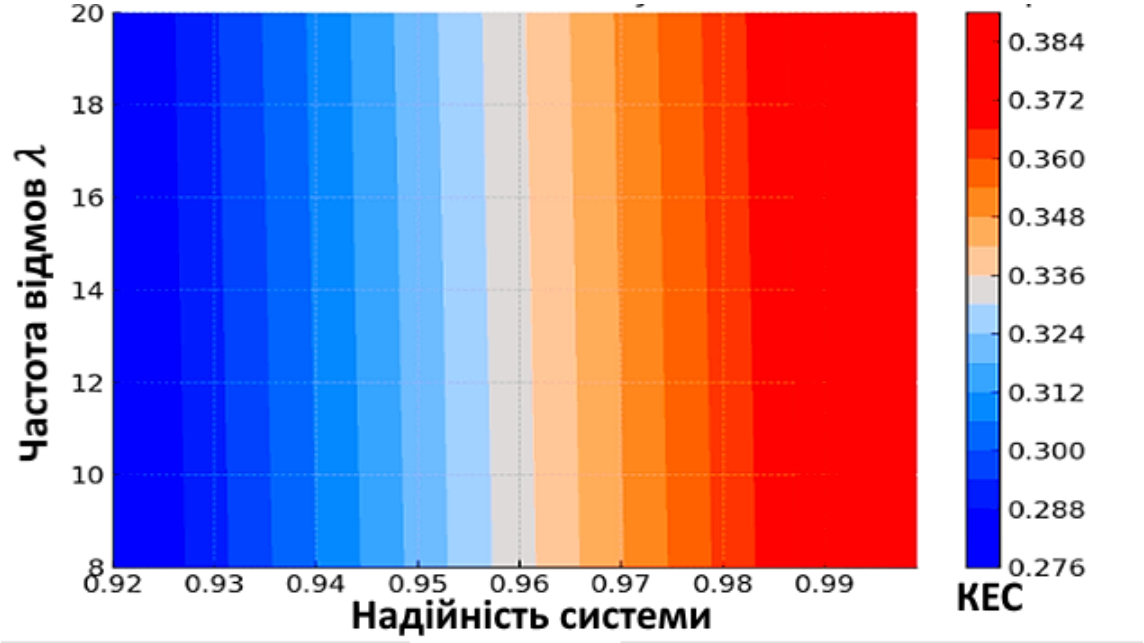


**Рис. 4. Різниця між КЕС та доступністю**

*Джерело: сформовано авторами*

Це дозволяє відобразити, що у воєнний період система вимагає додаткових ресурсів, а економічні ризики мають нелінійний характер, що можна побачити на тепловій карті представленій на рис. 5.

Запропонований коефіцієнт економічної стійкості поєднує технічну надійність телекомунікаційної мережі з економічними наслідками відмов та витратами на підтримку. Це дозволяє операторам:

1. Кількісно оцінювати баланс між КВ та ЕВ. Замість абстрактних показників надійності оператор бачить, наскільки додаткові інвестиції у резервування чи нову технологію реально впливають на економічну ефективність.

2. Аналізувати УРО та репутаційні ризики. Високе значення коефіцієнта kУРО у формулі демонструє, к жорсткі контракти посилюють вразливість компанії до збоїв. Це дає можливість

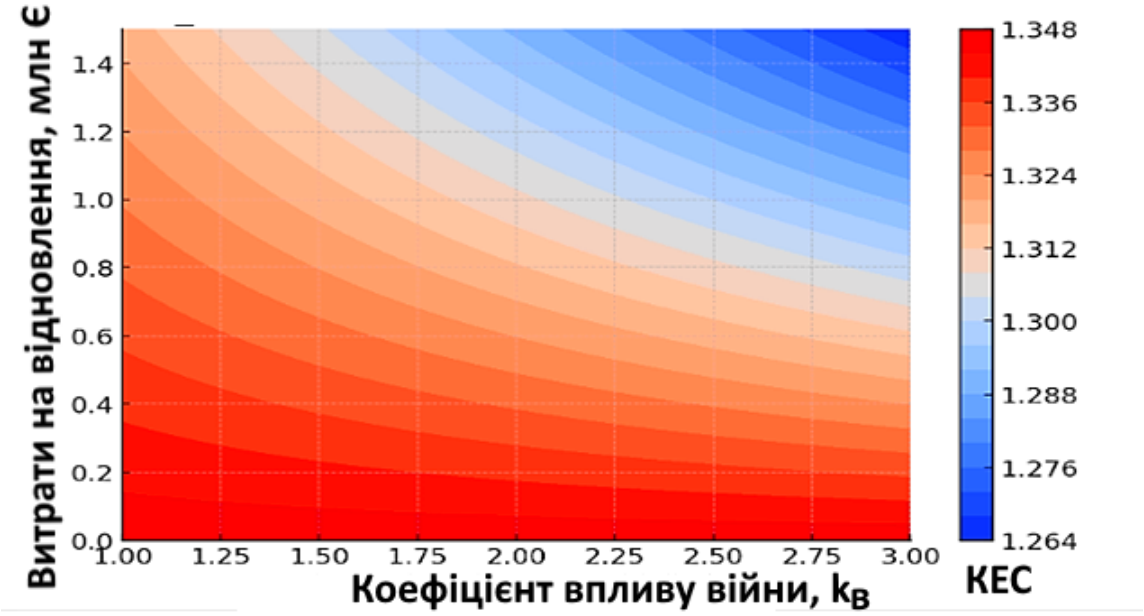


**Рис. 5. Теплова карта КЕС проти параметрів впливу війни**

*Джерело: сформовано авторами*

коригувати політику УРО залежно від прийнятного рівня ризику.

3. Встановлювати пріоритети для розвитку мережі. Моделювання дозволяє оцінити, що економічно вигідніше: підвищувати ймовірність безперебійної роботи *R* через модернізацію мережі чи зосередитися на зменшенні тривалості простоїв шляхом оптимізації операційних процесів.

**Висновки.** Класичні підходи, що розглядають технічну надійність та економічні показники окремо, не надають повної картини фінансових втрат, спричинених збоями, що унеможливлює формування ефективного безпекоорієнтованого інформаційного середовища. Запропонована модель КЕС усуває цю проблему, об'єднуючи обидва аспекти в єдину метрику, що особливо актуально для забезпечення економічної безпеки держави та функціонування сучасних високонадійних систем критичної інфраструктури. Моделювання, проведене на основі відкритих фінансових даних, показало, що навіть незначне зменшення середньої тривалості простоїв може значно підвищити КЕС, що часто є економічно вигіднішим, ніж значні капітальні вкладення у підвищення ймовірності безперебійної роботи. Модель КЕС дозволяє операторам та державним установам кількісно оцінювати баланс між капітальними та експлуатаційними витратами, аналізувати репутаційні ризики та встановлювати пріоритети для розвитку мережі в контексті зміцнення економічної безпеки. Таким чином, модель стає ефективним інструментом для стратегічного планування безпекоорієнтованого інформаційного середовища, що дозволяє прогнозувати економічні наслідки інцидентів та приймати обґрунтовані інвестиційні рішення для підвищення стійкості критичної інфраструктури до зовнішніх і внутрішніх загроз.

**БІБЛІОГРАФІЧНИЙ СПИСОК:**


1. Глушко А., Янко А., Білько С. Цифрова трансформація бізнес-процесів: безпековий аспект. *Цифрова економіка та економічна безпека*. 2025. № 2 (17). С. 160–166. URL: https://doi.org/10.32782/dees.17-26

2. Onyshchenko S., Yanko A., Hlushko A., Sabelnikova P. Assessment of information protection level against unauthorized access. *ScienceRise.* 2023. № 2. С. 36–44. URL: https://doi.org/10.21303/2313-8416.2023.003211

3. Uptime Institute. *Uptime Institute Global Data Center Survey Results 2024*. URL: https://uptimeinstitute.com

4. Mohseni Mehr K., Niky Isfahan H., Aali S. Validation of the Banking Services Redundancy Model in Sepah Bank. *Digital Transformation and Administration Innovation.* 2024. № 2(3). С. 90–101. URL: https://www.journaldtai.com/index.php/jdtai/article/download/91/126

5. Yanko A., Mychailichenko O., Hlushko A. Modern methods for protecting and storing data in computer systems to ensure their fault tolerance. *Theoretical and Applied Cyber Security*. 2024. № 6 (1). С. 72–81. URL: https://doi.org/10.20535/tacs.2664-29132024.1.315086

6. Onyshchenko S., Yehorycheva S., Furmanchuk O., Maslii O. Ukraine construction complex innovation-oriented development management. *Proceedings of the 2nd International Conference on Building Innovations.* 2019. P. 687–700. URL: https://doi.org/10.1007/978-3-030- 42939-3_68

7. Jurčić V., Gotovac S. A comprehensive techno-economic model for fast and reliable analysis of the telecom operator potentials. *Applied Sciences*. 2022. № 12(20). 10658. URL: https://doi.org/10.3390/app122010658

8. Bisht S., Kumar V., Pandey S. Analysis of network reliability characteristics and importance of components in a communication network. *Mathematics.* 2021. № 9(12). 1347. URL: https://doi.org/10.3390/math9121347

9. Rusek K., Walkowiak K., Pióro M. Effective risk assessment in resilient communication networks. *Journal of Network and Systems Management*, 2016. № 24. P. 123–148. URL: https://doi.org/10.1007/s10922-016-9370-3

10. Frank H., Smolka J., Mathew J. Techno-economic analysis of 5G non-public network architectures. *IEEE Access*. 2022. № 10. 70204–70218. https://research-information.bris.ac.uk/ws/portalfiles/portal/328132669/Full_text_PDF_final_published_version_.pdf

11. Technical University of Munich. *Techno-economic studies of telecom-munication networks*. URL: https://mediatum.ub.tum.de/doc/1764484/1764484.pdf

12. Kumar A., Malik S. C., Kumar N. Cost analysis of a computer system with hardware repair subject to inspection and arbitrary distributions for hardware and software replacement. *International Journal of Systems Assurance Engineering and Management*, 2013. № 4(1). P. 39–49. https://www.researchgate.net/publication/259476072

13. Byron J., Miller E., Darrell L. Measuring the Cost of Reliability in Archival Systems. *UCSD Center for Research in Storage Systems*. 2008. URL: https://crss.us/media/pubs/916f5482d2c0dfd400923bd43a0f6299f3aa4a81.pdf

14. Wang G., Xu W., Zhang L. What can we learn from four years of data center hardware failures? *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2017. P. 25–36. URL: https://people.iiis.tsinghua.edu.cn/~weixu/Krvdro9c/dsn17-wang.pdf

15. Янко А. С., Краснобаєв В. А., Любченко Р. О., Сабельнікова П. С. Процедура забезпечення відмовостійкості комп'ютерної системи на основі використання модулярної арифметики. *Системи управління, навігації та зв'язку*. 2023. № 4(74). С. 125–128. URL: https://doi.org/10.26906/SUNZ.2023.4.125

16. Deutsche Telekom. *Annual report 2024 data*. URL: https://www.telekom.com/resource/blob/1085970/9e25d438580a5e3f39521fd94ed5e48c/dt-24-annual-report-data.pdf

17. Uptime Institute. *Resiliency survey executive summary*. URL: https://datacenter.uptimeinstitute.com

18. ACCENTS Journals. Modeling downtime severity of telecommunication networks using DTMC.

*International Journal of Advanced Technology and Engineering Exploration*. 2023. № 10 (101). С. 70–78. https://accentsjournals.org/paperinfo.php?journalPaperId=1529

19. Onyshchenko S., Maslii O., Ivaniuk B. The Impact of External Threats to the Economic Security of the Business. *7th International Conference on Modeling, Development and Strategic Management of Economic System: Collection of scientific articles.* Atlantis Press, Paris, France, 2019. С. 156–160.

**REFERENCES:**

1. Glushko A., Yanko A., Bilko S. (2025) Tsyfrova transformatsiia biznes-protsesiv: bezpekovyi aspekt [Digital transformation of business processes: security aspect]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, no 2 (17), pp. 160–166. Available at: https://doi.org/10.32782/dees.17-26 (in Ukrainian)

2. Onyshchenko S., Yanko A., Hlushko A., Sabelnikova P. (2023) Assessment of information protection level against unauthorized access. *ScienceRise*, no (2), pp. 36–44. https://doi.org/10.21303/2313-8416.2023.003211

3. Uptime Institute (2024) Uptime Institute Global Data Center Survey Results 2024. Available at: https://uptimeinstitute.com/resources/research-and-reports/uptime-institute-global-data-center-survey-results-2024

4. Mohseni Mehr K., Niky Isfahan H., Aali S. (2024) Validation of the Banking Services Redundancy Model in Sepah Bank. *Digital Transformation and Administration Innovation*, no 2(3), pp. 90–101. Available at: https://www.journaldtai.com/index.php/jdtai/article/download/91/126

5. Yanko A., Mychailichenko O., Hlushko A. (2024) Modern methods for protecting and storing data in computer systems to ensure their fault tolerance. *Theoretical and Applied Cyber Security*, no 6(1), pp. 72–81. Available at: https://doi.org/10.20535/tacs.2664-29132024.1.315086

6. Onyshchenko S., Yehorycheva S., Furmanchuk O., Maslii O. (2019) Ukraine construction complex innovation-oriented development management. *Proceedings of the 2nd International Conference on Building Innovations,* pp. 687–700. Available at: https://doi.org/10.1007/978-3-030- 42939-3_68

7. Jurčić V., Gotovac S. (2022) A comprehensive techno-economic model for fast and reliable analysis of the telecom operator potentials. *Applied Sciences*, no 12(20), 10658. Available at: https://doi.org/10.3390/app122010658

8. Bisht S., Kumar V., Pandey S. (2021) Analysis of network reliability characteristics and importance of components in a communication network. *Mathematics*, no 9(12), 1347. Available at: https://doi.org/10.3390/math9121347

9. Rusek K., Walkowiak K., Pióro M. (2016) Effective risk assessment in resilient communication networks. *Journal of Network and Systems Management*, no 24, pp. 123–148. Available at: https://doi.org/10.1007/s10922-016-9370-3

10. Frank H., Smolka J., Mathew J. (2022) Techno-economic analysis of 5G non-public network architectures. *IEEE Access*, no 10, 70204–70218. Available at: https://research-information.bris.ac.uk/ws/portalfiles/portal/328132669/Full_text_ PDF_final_published_version_.pdf

11. Technical University of Munich (2022) *Techno-economic studies of telecommunication networks*. Available at: https://mediatum.ub.tum.de

12. Kumar A., Malik S. C., Kumar N. (2013) Cost analysis of a computer system with hardware repair subject to inspection and arbitrary distributions for hardware and software replacement. *International Journal of Systems Assurance Engineering and Management*, no 4(1), pp. 39–49. Available at: https://www.researchgate.net/publication/259476072

13. Byron J., Miller E., Darrell L. (2008) Measuring the Cost of Reliability in Archival Systems. *UCSD Center for Research in Storage Systems*. Available at: https://crss.us/media/pubs/916f5482d2c0dfd400923bd43a0f6299f3aa4a81.pdf

14. Wang G., Xu W., Zhang L. (2017) What can we learn from four years of data center hardware failures? *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 25–36. Available at: https://people.iiis.tsinghua.edu.cn/~weixu/Krvdro9c/dsn17-wang.pdf

15. Yanko A. S., Krasnobaev V. A., Lyubchenko R. O., Sabelnikova P. S. (2023). Protsedura zabezpechennia vidmovostiikosti kompiuternoi systemy na osnovi vykorystannia moduliarnoi aryfmetyky [Procedure for ensuring fault tolerance of a computer system based on the use of modular arithmetic]. *Systemy upravlinnia, navihatsii ta zviazku*, no 4(74), pp. 125–128. Available at: https://doi.org/10.26906/SUNZ.2023.4.125 (in Ukrainian)

16. Deutsche Telekom (2024). *Annual report 2024 data*. Available at: https://www.telekom.com/resource/blob/1085970/9e25d438580a5e3f39521fd94ed5e48c/dt-24-annual-report-data.pdf

17. Uptime Institute (2024) *Resiliency survey executive summary*. Available at: https://datacenter.uptimeinstitute.com

18. ACCENTS Journals (2023) Modeling downtime severity of telecommunication networks using DTMC. *International Journal of Advanced Technology and Engineering Exploration*, no 10(101), pp. 70–78. Available at: https://accentsjournals.org/paperinfo.php?journalPaperId=1529

19. Onyshchenko S., Maslii O., Ivaniuk B. (2019) The Impact of External Threats to the Economic Security of the Business. *7th International Conference on Modeling, Development and Strategic Management of Economic System: Collection of scientific articles*. Paris: Atlantis Press, pp. 156–160.