

С. М. Лисенко, проф., д-р техн. наук, **А. В. Качур**, **Л. О. Корецька**, доц., канд. техн. наук

Хмельницький національний університет, м. Хмельницький, Україна

e-mail: sirogyk@ukr.net, kachurav@khnmu.edu.ua, koretskal@khnmu.edu.ua

Метод синтезу резильєнтних архітектур систем віртуальної та доданої реальності

У статті розглядається проблема забезпечення стійкості систем доповненої (AR) та віртуальної (VR) реальності, які характеризуються високою чутливістю до порушень продуктивності та збоїв апаратного й програмного забезпечення. Більшість існуючих підходів зосереджені на аналізі фіксованих архітектур, залишаючи відкритим питання автоматизованого синтезу систем, стійких за своєю побудовою.

Запропоновано новий метод аналітичного синтезу архітектур AR/VR, який базується на формальній моделі, що пов'язує 20-вимірний вектор параметрів пом'якшення негативних впливів із сімома ключовими метриками стійкості: надійністю, готовністю, відмовостійкістю, цілісністю, часом відновлення, стабільністю продуктивності та безпекою користувача. Задача проектування сформульована як проблема багатокритеріальної оптимізації, для вирішення якої застосовано генетичний алгоритм.

Експериментальна валідація, проведена у середовищі Simulink, підтвердила ефективність методу. Результати показали, що синтезована архітектура забезпечує покращення загального показника стійкості на 19,4% порівняно з базовою конфігурацією в умовах жорстких експлуатаційних обмежень. Зокрема, досягнуто суттєвого приросту показників готовності (+82,2%) та часу відновлення (+39,9%). Запропонований підхід дозволяє кількісно оцінювати та оптимізувати архітектурні рішення на етапі проектування.

віртуальна реальність, резильєнтність, синтез архітектури, оптимізація проектування, моделювання деградації, метрики стійкості, генетичні алгоритми

Постановка проблеми. Сучасні системи доповненої (AR) та віртуальної (VR) реальності стрімко трансформуються з інструментів розваг у критично важливі технології для промисловості, медицини та освіти. Функціонування цих систем базується на складному та безперервному циклі взаємодії між апаратним забезпеченням, програмними модулями, мережевими даними та кінцевим користувачем [1]. Порушення цього циклу – апаратні збої, мережеві затримки або помилки програмного коду – призводять не лише до погіршення досвіду користувача, але й можуть спричинити такі серйозні наслідки для його здоров'я, як кіберхвороба [2]. Вплив такого роду робить питання надійності архітектури таких систем першочерговою задачею.

Резильєнтність в контексті систем віртуальної та доданої реальності вважають здатність архітектури функціонувати під впливом негативних факторів, адаптуватись до динамічних змін умов використання, та швидко відновлювати працездатність без критичних втрат у якості досвіду користувача. Існуючі методи проектування зосереджені переважно на аналізі поведінки вже існуючих архітектур у стресових умовах. Важливим є перехід до превентивного синтезу, і проблема полягає у відсутності єдиного методу, який дозволив би кількісно об'єднати стратегії підвищення надійності на всіх рівнях ще на етапі проектування.

Таким чином, актуальним завданням є розробка методу синтезу, який трансформує процес створення AR/VR архітектури в задачу багатокритеріальної оптимізації [27] для досягнення максимального рівня стійкості в умовах впливу деструктивних факторів.

Аналіз останніх досліджень та публікацій. Ряд публікацій був присвячений проблемі стійкості на різних архітектурних рівнях середовищ AR/VR. Дослідження, орієнтовані на апаратне забезпечення ([15]-[17], [23]), зосереджуються на відмовостійкості та енергоефективності з використанням таких методів як динамічне масштабування напруги та частоти, планування з урахуванням теплового режиму та апаратна надлишковість. Підходи програмного рівня ([18], [19]) концентруються на механізмах контрольних точок і перезапуску (checkpoint-restart), віртуалізації та адаптивному відмовостійкому виконанні для забезпечення відновлення після перехідних збоїв.

Методи, орієнтовані на дані ([20]-[22]), спрямовані на підвищення надійності та цілісності передачі за допомогою багатошляхової маршрутизації, прямого виправлення помилок (FEC) та надлишкового кодування для інтенсивних робочих навантажень потокової передачі з ефектом занурення. Стійкість, пов'язана з користувачем ([24], [25], [30]), підкреслює поведінкову стабільність, комфорт і безпеку шляхом моделювання шаблонів людської взаємодії та оптимізації ергономіки в інтерфейсах VR/AR. Нарешті, системні та інтегративні дослідження ([26], [28], [29]) пропонують комплексні фреймворки оптимізації та синтезу, які поєднують апаратне, програмне забезпечення та фактори навколишнього середовища для досягнення глобальної стійкості в усій екосистемі віртуальної реальності. Основні підходи узагальнені в таблиці 1.

Таблиця 1 – Опис методів мінімізації негативних впливів

Компонент	Тип змінної	Автори	Метод мінімізації	Застосування у синтезі
Апаратне забезпечення (H)	Мережеві умови	Y. Sun et al. [15]	Обчислювальне розвантаження (offloading) важких завдань на хмару/периферію для зменшення локального термічного стресу.	Включення змінної рішення для порогу розвантаження; зменшує інтенсивність відмов пристрою lh.
Апаратне забезпечення (H)	Екологічні змінні	X. Zhang et al. [16]	Предиктивне управління тепловим режимом динамічно обмежує обчислення для запобігання перегріву.	Додавання параметра термічного ліміту та запуск шляху резервування при його перевищенні для підвищення надійності.
Апаратне забезпечення (H)	Поведінка користувача	J. Gomez et al. [17]	Динамічна вибірка сенсорів та масштабування потужності на основі інтенсивності руху.	Використання порогу чутливості до руху для активації режиму низького енергоспоживання; знижує частоту відмов.

Продовження Таблиці 1

Апаратне забезпечення (H)	Системне навантаження	J. Gomez et al. [17]	Розподілені обчислення на сенсорах розділяють завдання між CPU / GPU для запобігання насиченню.	Введення змінної паралельних потоків для балансування навантаження та підтримки стабільності PSh.
Апаратне забезпечення (H)	Апаратні обмеження	J. Xiong et al. [18]	Малопотужні мікро-LED дисплеї зменшують теплове навантаження та енергоспоживання.	Додавання змінної архітектури дисплея (OLED / μ LED), пов'язаної з термічними параметрами.
Програмне забезпечення (S)	Мережеві умови	A. Hazarika [19]	Адаптивне проміжне ПЗ для стрімінгу коригує роздільну здатність залежно від затримки та джиттера.	Додавання порогу якості стрімінгу, що керує динамічною адаптацією ПЗ.
Програмне забезпечення (S)	Зміни середовища	A. Hazarika [19]	Корекція пози та сцени в реальному часі компенсує зміни освітлення та оклюзії.	Додавання режиму відкату ПЗ (fallback), що знижує точність при поганому освітленні для збереження надійності трекінгу.
Програмне забезпечення (S)	Поведінка користувача	J. Gomez et al. [17]	Предиктивна пакетна обробка вводу згладжує сплески взаємодії для запобігання пікам CPU.	Додавання змінної інтервалу пакетування для стабілізації продуктивності PSs.
Програмне забезпечення (S)	Системне навантаження	K. T. Foerster et al. [20]	Створення контрольних точок (checkpoint/restore) забезпечує швидке відновлення під навантаженням.	Встановлення частоти контрольних точок та фактора реплікації контейнерів для максимізації As.
Програмне забезпечення (S)	Апаратні обмеження	Y. Sun et al. [15]	Програмне розвантаження обчислень зменшує стрес на обмежені локальні ресурси.	Включення змінної коефіцієнта розвантаження, що координується з апаратними та мережевими моделями.
Дані / Зв'язок (D)	Мережеві умови	B. Zhao et al. [21]	Багатошляхове планування агрегує кілька каналів 5G для маскування джиттера та втрат.	Додавання змінної кількості паралельних каналів зв'язку.

Продовження таблиці 1

Дані / Зв'язок (D)	Екологічні змінні	V. Kelkkanen [22]	Периферійна локалізація підтримує трекінг при завадах або оклюзії.	Змінна вибору між периферійним та хмарним трекінгом; зменшує затримку та RT.
Дані / Зв'язок (D)	Поведінка користувача	P. Yang et al. [23]	Предиктивна попередня вибірка даних (pre-fetching) передбачає рух користувача.	Додавання змінної розміру буфера попередньої вибірки; покращує безперервність та PSD.
Дані / Зв'язок (D)	Системне навантаження	Y. Sun et al. [15]	Спільна архітектура зв'язку-обчислень-кешування (3C) балансує навантаження.	Використання змінних розміру кешу та периферійних вузлів для посилення AD.
Дані / Зв'язок (D)	Апаратні обмеження	A. Hazarika [19]	Адаптивна модуляція та кодування (AMCS) підтримує надійність при зміні SNR.	Змінна рівня модуляції/кодування підлаштовується під радіоумови для покращення ID.
Користувачі (U)	Мережеві умови	V. Kelkkanen [22]	Предикція руху та інтерполяція кадрів компенсують затримку для зменшення кіберхвороби.	Додавання змінної буфера інтерполяції; знижує сприйману затримку, покращуючи PSU та US.
Користувачі (U)	Екологічні змінні	M. Park et al. [25]	Адаптивна яскравість інтерфейсу та придушення аудіо реагують на освітлення та шум.	Змінна порогів адаптації інтерфейсу; підвищує комфорт та стабільність.
Користувачі (U)	Поведінка користувача	S. Weech et al. [26]	Адаптивна локомоція (телепортація) зменшує кіберхворобу від інтенсивного руху.	Змінна режиму локомоції / обмеження швидкості взаємодії; підсилює US та PS.

Закінчення таблиці 1

Користувачі (U)	Системне навантаження	J. Xiong et al. [18]	Динамічний рендеринг рівня деталізації (LOD) масштабує якість залежно від кількості користувачів.	Змінна макс. кількості користувачів / LOD; запобігає перевантаженню та зберігає PS.
Користувачі (U)	Апаратні обмеження	J. Xiong et al. [18]	Ергономічні, легкі HMD та управління живленням зменшують втому та перегрів.	Змінні ваги пристрою / ємності батареї / термічного порогу; покращують US.

Джерело: розроблено авторами

Кожен з розглянутих методів спрямований на окремий клас негативних впливів на систему – нестабільне функціонування мережі, зміна навколишнього середовища, тощо. За допомогою відображення цих стратегій мінімізації впливу у контрольовані змінні проектування, можливою стає кількісна оцінка їхнього внеску у ключові метрики резильєнтності системи. Незважаючи на значний приріст у забезпеченні стійкості окремих компонентів систем віртуальної та доданої реальності, більшість з розглянутих методів обмежені своєю областю застосування – рішення, орієнтовані на дані, спрямовані на надійність передачі, але працюють незалежно від апаратних обмежень і динаміки системного навантаження; а дослідження на рівні користувача насамперед стосуються комфорту та ергономіки без зв'язку цих факторів із системними метриками продуктивності. Ця фрагментація створює проблему: наразі не існує уніфікованого методу синтезу, здатного поєднувати методи підвищення стійкості з усіх архітектурних шарів і максимізувати їх спільно під впливом динамічних факторів навколишнього середовища, поведінки та робочого навантаження. Наш метод спрямований на усунення цієї прогалини шляхом впровадження комплексної багатокритеріальної структури синтезу.

Постановка завдання. В імерсивних системах стійкість визначається як здатність техногенного середовища підтримувати прийнятну продуктивність, незважаючи на збої, деградацію або зовнішній стрес, що охоплює етапи передбачення, протистояння, відновлення та адаптації. Оскільки системи AR/VR поєднують у собі апаратне забезпечення, програмне забезпечення, мережі передачі даних та користувачів, стійкість є емерджентною властивістю, що виникає внаслідок їхньої взаємодії, а не властивістю окремого шару. Метою завдання синтезу є розробка методу, який дозволяє проектувати архітектурні конфігурації, здатні підтримувати функціональний вихід вище мінімально допустимого рівня протягом усього часу виконання місії. Процес синтезу розглядається як зворотне відображення від цільових показників стійкості до конкретних параметрів проектування. Завдання синтезу зводиться до пошуку оптимального 20-вимірною вектора пом'якшення впливів (M_Vector), який максимізує кожен критерій стійкості незалежно при одночасному мінімізуванні часу відновлення. Це формулюється як багатокритеріальна задача оптимізації:

$$\max_x \begin{pmatrix} R_{\text{sys}}(T; x), \\ A_{\text{sys}}(x), \\ FT(k, n, T; x), \\ I(x), \\ PS(x), \\ US(x), \\ RT^{-1}(x), \\ MTTR^{-1}(x) \end{pmatrix}. \quad (1)$$

Для кількісної оцінки та чисельної оптимізації в межах методу використовуються такі формалізовані критерії як надійність, доступність, відмовостійкість, цілісність, час відновлення, стабільність продуктивності та безпека користувача.

Надійність визначається як ймовірність того, що система виконує покладені на неї функції без збоїв з перебігом часу [5]:

$$R(t) = P\{T_f > t\} = e^{-\lambda t}, \quad (2)$$

T_f показує час функціонування системи до першого збою, λ – показник збоїв, що показує середню кількість відмов у період часу.

Доступність – це відсоток часу, коли система працює [6]:

$$A = \frac{MTTF}{MTTF + MTTR}, \quad (3)$$

$MTTF$ та $MTTR$ – середній час відмови та середній час відновлення відповідно.

Відмовостійкість – це здатність системи продовжувати функціонування безперервно навіть у випадку, коли один або більше з її компонентів перестає функціонувати. Для конфігурації k-з-n (система функціонує, якщо принаймні k з n ідентичних елементів функціонують) [3][7]:

$$FT(k, n, t) = \sum_{i=k}^n \binom{n}{i} R(t)^i [1 - R(t)]^{n-i}. \quad (4)$$

Якщо елементи системи нерівноцінні, доцільно використати вагові коефіцієнти [8].

Цілісність показує протидію системи пошкодженню даних під час передачі або зберігання [8]. E_d та E_c – кількість виявлених та виправлених помилок відповідно:

$$I = 1 - \frac{E_d - E_c}{E_d}. \quad (5)$$

Час відновлення – це затрачений час від виникнення несправності до повного відновлення [9][10].

$$RT = t_{\text{restore}} - t_{\text{fail}}, \quad (6)$$

$$MTTR = \frac{1}{N} \sum_{i=1}^N (t_{restore,i} - t_{fail,i}) \cdot \quad (7)$$

Стабільність продуктивності вимірює відхилення від номінальної продуктивності (наприклад, кількість кадрів на секунду, затримки, тощо) [11][12]:

$$PS = 1 - \frac{|P(t) - P_0|}{P_0} \quad (8)$$

Змінна безпеки користувачів вимірює ймовірність того, що небезпечні умови не виникнуть, при цьому ρ – умовна ймовірність шкоди користувачеві у раз відмови системи [13][14]:

$$US = 1 - P_{hazard} = 1 - \rho(1 - R_{sys}) \quad (9)$$

Теоретична база для оцінки резильєнтності в середовищах AR/VR ґрунтується на кількісних параметрах, що відображають стабільність та адаптивність системи. Надійність, доступність, відмовостійкість, цілісність, час відновлення, стабільність продуктивності та безпека користувача разом утворюють цілісну сукупність показників, що описують здатність системи підтримувати прийнятну роботу в мінливих умовах. Кожна метрика забезпечує окремий погляд на поведінку рівнів апаратного забезпечення, програмного забезпечення, даних та взаємодії з користувачем, тоді як їхнє математичне формулювання дозволяє пряму інтеграцію в аналітичні та симуляційні структури. Отримана структура встановлює уніфікований фундамент для синтезу та чисельної оптимізації стійких архітектур AR/VR.

Виклад основного матеріалу. Забезпечення резильєнтності середовищ AR/VR вимагає системного підходу, спрямованого на покращення стабільності продуктивності та відмовостійкості кожного архітектурного шару. Основною метою запропонованого методу є максимізація всіх критеріїв стійкості шляхом ідентифікації та посилення параметрів, що мають на них найбільш суттєвий вплив. Методологічна структура розглядає ці критерії як взаємозалежні цілі оптимізації. Наприклад, зниження часу відновлення підвищує доступність, а зменшення частоти помилок покращує цілісність та стабільність продуктивності.

Процедура синтезу спрямована на пошук багатовимірного оптимуму, де комбінація проектних рішень (рівні надмірності, політика DVFS, частота контрольних точок, рівень FEC тощо) забезпечує максимальну ефективність системи.

Етапи реалізації методу:

1. Верифікація та базова «контрольна карта»:
 - Визначення часу місії та профілів роботи
 - Структурна модель надійності – побудова діаграм надійності та використання ланцюгів Маркова для розрахунку доступності
 - Валідація параметрів: розрахунок інтенсивності відмов та відновлення
 - Інструментарій затримки та безпеки
 - Визначення мінімально допустимих значень для кожної метрики
2. Застосування методів мінімізації впливів
3. Інтеграція та синтез.

Кожен шар архітектури – апаратне забезпечення, програмне забезпечення, дані та користувачі – моделюється як напівзалежна підсистема, внутрішні параметри якої реагують на зовнішні змінні:

$$E = \{E_n, E_{env}, E_b, E_s, E_{hw}\} \quad (10)$$

В даному випадку E_n – мережеві умови, E_{env} – зміни середовища, E_b – зміни поведінки користувача, E_s – зміни навантаження системи, E_{hw} – умови, пов'язані з апаратним забезпеченням [27]. Ці фактори впливають на зв'язки між внутрішніми компонентами системи.

Таким чином, кожна підсистема $C_j = \{H, S, D, U\}$ підтримує вектор параметрів проектування $x_j = [x_{j1}, x_{j2}, \dots, x_{jm}]$, який визначає її роль в загальній резильєнтності системи.

Для оцінки практичної ефективності запропонованого методу синтезу та демонстрації взаємодії окремих механізмів стійкості в межах повної архітектурної конфігурації, аналітичну структуру було інтегровано у виконуваний чисельний робочий процес. Цей процес поєднує в собі оптимізацію, відображення параметрів та повну оцінку системи. Розглянемо концептуальну модель з [27]:

$$VR = \{H, S, D, U\}, E = \{E_n, E_{env}, E_b, E_s, E_{hw}\} \quad (11)$$

Застосуємо дану модель у вищеописаному методі. Для цього встановимо відповідність між функціями оцінки $f_{i,j}(E_i, C_j)$ з [27], та відповідними метриками резильєнтності $R_{sys}(T; x)$, $A_{sys}(x)$, $FT(k, n, T; x)$, $I(x)$, $PS(x)$, $US(x)$. Метод синтезу вибудовує конфігурації, що дозволяють досягти необхідного рівня резильєнтності. Формально синтез відображає обернену відповідність параметрів резильєнтності і параметрів проектування:

$$x^* = \underset{x \in X}{argmax} R_{VR}^{(final)}(x, E) \quad (12)$$

Кожен з критеріїв резильєнтності M_k залежить від внутрішніх параметрів системи та впливу зовнішніх факторів. Для того, щоб оцінити ці залежності, кожен компонент C_j описується номінальним значенням $M_{k,j}^{nom}(x_j)$ і функціями деградації $f_{i,j}(x_j, E_i)$. У моделі синтезу впроваджуються коефіцієнти чутливості $\gamma_{k,i,j}$, що визначають, наскільки кожен i -й зовнішній фактор впливає на критерій k компоненту j :

$$M_{k,j}(x, E) = M_{k,j}^{nom}(x_j) \prod_{i \in E} [f_{i,j}(x_j, E_i)]^{\gamma_{k,i,j}} \quad (13)$$

Кожен фактор $f_{i,j} \in [0, 1]$ відображає ступінь впливу зовнішньої умови на можливість підтримувати очікувану продуктивність. Для кожного з критеріїв k , значення на рівні системи отримується з відповідної агрегаційної функції:

$$M_k(x, E) = \Phi_k(M_{k,H}, M_{k,S}, M_{k,D}, M_{k,U}) \quad (14)$$

Φ – відповідний структурний оператор для надійності, відмовостійкості, тощо. Загальна ціль синтезу тоді визначається як нормалізований, зважений показник усіх критеріїв:

$$R_{VR}^{final}(x, E) = \sum_{k=1}^8 \beta_k v_k(M_k(x, E)) \quad (15)$$

v_k приводить генерогенні фактори до загального показника: лінійного або обернено-лінійного для часових вимірів, та експоненційного для критеріїв, що динамічно змінюються. Таким чином, оптимізація може бути сформульована як:

$$\begin{aligned} & \text{Максимізація : } R_{VR}^{final}(x, E) \\ & \text{При : } g(x, E) \leq 0, h(x, E) = 0 \end{aligned} \quad (16)$$

Для підтвердження ефективності запропонованого методу аналітичного синтезу було проведено чисельне оцінювання. Метою експерименту є демонстрація здатності моделі орієнтуватися у багатовимірному просторі проектування стратегій пом'якшення впливів та ідентифікувати оптимальну архітектуру. На додаток до аналітичного формулювання, процедура синтезу реалізована безпосередньо в середовищі Simulink, що дозволяє проводити високоточну оцінку стійкості в умовах динамічної зміни робочих параметрів. Simulink забезпечує структуроване представлення всіх компонентів, функцій впливу та механізмів агрегації на рівні блоків. Шляхом вбудовування конвеєра обчислення стійкості в Simulink та представлення ключових архітектурних параметрів як конфігурованих змінних, генетичний алгоритм (ГА) може оцінювати кожен кандидатний вектор мітигації на основі реалістичного моделювання поведінки системи. Процес синтезу був реалізований як задача одноцільової оптимізації під керуванням стандартного генетичного алгоритму. Функція придатності (fitness function) для ГА виконує повну аналітичну модель за наступною схемою: вектор зменшення впливів, розрахунок метрик, функції деградації та агрегація.

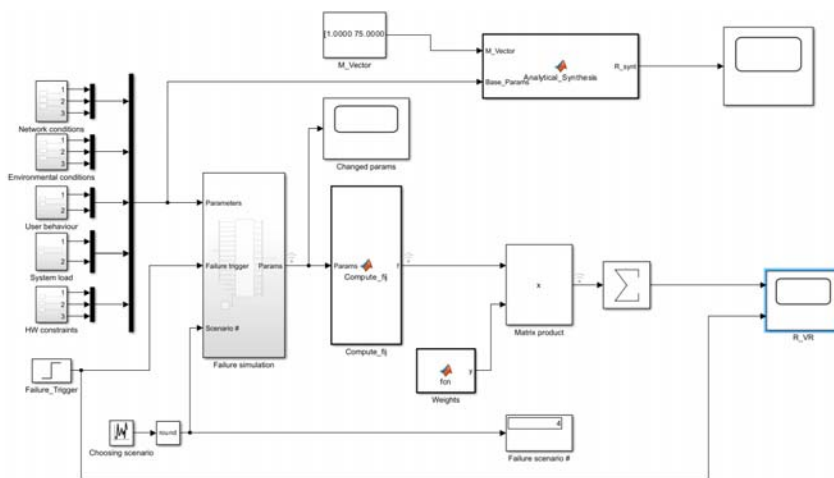


Рисунок 1 – реалізація системи в середовищі Simulink

Джерело: розроблено авторами

Інтеграція підходу в модель дала змогу отримати вектор зменшення впливів з середнім балом стійкості 0,477268 при базових вхідних параметрах. Результати порівняльного аналізу базової архітектури (з мінімальними заходами пом'якшення) та синтезованої оптимальної архітектури в умовах важкого сценарію експлуатації наведено в Таблиці 2.

Таблиця 2 – Результати експериментів

Метрика	Базова оцінка	Оптимізована оцінка	Покращення (%)
Надійність	0,5893	0,7728	+31,1%
Доступність	0,0001	0,0002	+82,2%
Відмовостійкість	0,5878	0,6931	+17,9%
Цілісність	0,5981	0,6514	+8,9%
Час відновлення	0,6666	0,9327	+39,9%
Стабільність продуктивності	0,0001	0,0002	+18,6%
Безпека коритувача	0,7286	0,7331	+0,6%
Інтегральний показник	0,4822	0,5756	+19,4%

Висновки. У роботі представлено формально обґрунтований метод автоматизованого синтезу стійких архітектур AR/VR. Встановлено суворий математичний зв'язок між архітектурними проектними рішеннями низького рівня та емерджентними властивостями стійкості високого рівня. Запропонована аналітична модель перетворює складне якісне завдання проектування стійких систем на кількісну проблему багатокритеріальної оптимізації. Експериментальні результати, отримані як шляхом синтезу на основі генетичного алгоритму, так і за допомогою інтеграції в Simulink у реальному часі, підтверджують ефективність цього підходу.

Майбутня робота може бути зосереджена на розширенні бібліотеки стратегій пом'якшення впливів, уточненні моделей чутливості за допомогою емпіричних даних з фізичних випробувальних стендів та дослідженні застосування цього методу синтезу до інших класів кіберфізичних систем. Критично важливим напрямком для майбутніх досліджень є протидія просунутим загрозам безпеці в таких взаємопов'язаних системах. Це включає адаптацію нашої моделі стійкості для врахування ботнетів і поліморфного шкідливого програмного забезпечення [28-34], а також вирішення унікальних проблем безпеки та приватності, притаманних імерсивним середовищам, таким як автентифікація користувачів, конфіденційність даних та захист від неімерсивних атак [34-45].

Список літератури

1. Resilience engineering. *Wikipedia*. URL: [https://en.wikipedia.org/wiki/Resilience_engineering] (https://en.wikipedia.org/wiki/Resilience_engineering) (дата звернення: 13.02.2026).
2. System Resilience. *SEBoK Wiki*. URL: [https://sebokwiki.org/wiki/System_Resilience] (https://sebokwiki.org/wiki/System_Resilience) (дата звернення: 13.02.2026).
3. The k-out-of-n System Model. *Wiley*. URL: [<https://catalogimages.wiley.com/images/db/pdf/047139761X.07.pdf>] (<https://catalogimages.wiley.com/images/db/pdf/047139761X.07.pdf>) (дата звернення: 13.02.2026).
4. RBDs and Analytical System Reliability. *ReliaSoft*. URL: [https://help.reliasoft.com/reference/system_analysis/sa/rbds_and_analytical_system_reliability.html] (https://help.reliasoft.com/reference/system_analysis/sa/rbds_and_analytical_system_reliability.html) (дата звернення: 13.02.2026).
5. Reliability analysis of a k-out-of-n:F system under a linear model. Ann. Inst. Stat. Math. URL: [<https://www.ism.ac.jp/editsec/aism/71/0537.pdf>] (<https://www.ism.ac.jp/editsec/aism/71/0537.pdf>) (дата звернення: 13.02.2026).
6. Availability. *Wikipedia*. URL: [<https://en.wikipedia.org/wiki/Availability>] (<https://en.wikipedia.org/wiki/Availability>) (дата звернення: 13.02.2026).
7. k-out-of-n Systems. *ReliaSoft*. URL: [https://help.reliasoft.com/articles/content/reference_examples/blocksim/k-out-of-n_systems.html] (https://help.reliasoft.com/articles/content/reference_examples/blocksim/k-out-of-n_systems.html) (дата звернення: 13.02.2026).
8. Multi-Blockchain-Based IoT Data Processing Techniques for Big Data Integrity Verification. *Sensors*. 2021. Vol. 21, no. 10. Art. no. 3515. URL: [<https://www.mdpi.com/1424-8220/21/10/3515>] (<https://www.mdpi.com/1424-8220/21/10/3515>) (дата звернення: 13.02.2026).
9. Recovery Time Objective (RTO). *NIST CSRC*. URL: [https://csrc.nist.gov/glossary/term/recovery_time_objective] (https://csrc.nist.gov/glossary/term/recovery_time_objective) (дата звернення: 13.02.2026).
10. Mean time to recovery. *Wikipedia*. URL: [https://en.wikipedia.org/wiki/Mean_time_to_recovery] (https://en.wikipedia.org/wiki/Mean_time_to_recovery) (дата звернення: 13.02.2026).
11. Measuring System Visual Latency through Cognitive Tests. *Proc. IEEE VR 2020*. URL: [https://www.microsoft.com/en-us/research/wp-content/uploads/2020/01/ieee_vr_2020_latency.pdf] (https://www.microsoft.com/en-us/research/wp-content/uploads/2020/01/ieee_vr_2020_latency.pdf) (дата звернення: 13.02.2026).
12. Measuring motion-to-photon latency for sensorimotor experiments with VR. *PLOS ONE*. 2022. URL: [<https://pmc.ncbi.nlm.nih.gov/articles/PMC10616216/>] (<https://pmc.ncbi.nlm.nih.gov/articles/PMC10616216/>) (дата звернення: 13.02.2026).
13. Investigating guardian awareness techniques to promote VR user safety. *SMU*. URL: [https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=9024&context=sis_research] (https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=9024&context=sis_research) (дата звернення: 13.02.2026).

14. Exploring Metaphorical Transformations of a Safety Boundary Wall for VR. **Applied Sciences**. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11125283/ (дата звернення: 13.02.2026).
15. Communication, Computing and Caching for Mobile VR Delivery: Modeling and Trade-off / Sun Y. et al. **arXiv preprint arXiv:1804.10335**. 2018. URL: https://arxiv.org/abs/1804.10335 (дата звернення: 13.02.2026).
16. Zhang X., Xia Y., Ali M. A Smartphone Thermal Temperature Analysis for Virtual and Augmented Reality : National Science Foundation Technical Report. 2020. URL: https://par.nsf.gov/servlets/purl/10219090 (дата звернення: 13.02.2026).
17. Distributed On-Sensor Compute System for AR/VR Devices: A Semi-Analytical Simulation Framework for Power Estimation / Gomez J. et al. **arXiv preprint arXiv:2203.07474**. 2022. URL: https://arxiv.org/abs/2203.07474 (дата звернення: 13.02.2026).
18. Augmented Reality and Virtual Reality Displays: Emerging Technologies and Future Perspectives / Xiong J. et al. **Light: Science & Applications**. 2021. Vol. 10, no. 1. Art. no. 215. URL: https://www.nature.com/articles/s41377-021-00658-8 (дата звернення: 13.02.2026).
19. Hazarika A. Towards an Evolved Immersive Experience: Exploring 5G. **Sensors**. 2023. Vol. 23, no. 7. P. 3682. URL: https://www.mdpi.com/1424-8220/23/7/3682 (дата звернення: 13.02.2026).
20. Transparent Fault Tolerance for Stateful Applications in Kubernetes with Checkpoint/Restore / Foerster K. T. et al. **Proc. IEEE SRDS 2023**. URL: https://ktfoerster.github.io/paper/2023-srds.pdf (дата звернення: 13.02.2026).
21. Zhao B., Guo S., Liu X. A Multipath Scheduler Based on Cross-Layer Information for Cloud VR in 5G Edge Networks. **Computer Networks**. 2024. Vol. 244. P. 110333. DOI: https://doi.org/10.1016/j.comnet.2024.110333.
22. Kelkkanen V. Evaluation and Reduction of Temporal Issues in Remote VR : Master's Thesis / Univ. of Oulu. Oulu, Finland, 2023. URL: https://www.diva-portal.org/smash/get/diva2:1744902/FULLTEXT02.pdf (дата звернення: 13.02.2026).
23. Feeling of Presence Maximization: mmWave-Enabled Virtual Reality Meets Deep Reinforcement Learning / Yang P. et al. **arXiv preprint arXiv:2107.01001**. 2021. URL: https://arxiv.org/abs/2107.01001 (дата звернення: 13.02.2026).
24. Exploring Metaphorical Transformations of a Safety Boundary Wall for VR / Qin H. et al. **Applied Sciences**. 2024. Vol. 14, no. 6. Art. no. 2520. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11125283/ (дата звернення: 13.02.2026).
25. Recent Advances in Wearable Thermal Devices for Virtual and Augmented Reality / Park M. et al. **Micromachines**. 2025. Vol. 16, no. 3. Art. no. 338. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12029164/ (дата звернення: 13.02.2026).
26. Weech S., Kenny S., Barnett-Cowan M. Presence and Cybersickness in Virtual Reality Are Negatively Related: A Review. **Frontiers in Psychology**. 2019. Vol. 10. P. 158. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2019.00158/full (дата звернення: 13.02.2026).
27. Lysenko S., Kachur A. A Resilience Assurance Process Model for Enhancing Virtual Reality Architectural Design. **Proc. 14th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT)**. Athens, Greece, 2024. P. 1–9. DOI: https://doi.org/10.1109/DESSERT65323.2024.11122129.
28. A Technique for Detection of Bots which are Using Polymorphic Code / Pomorova O. et al. **Communications in Computer and Information Science**. 2014. Vol. 431. P. 265–276.
29. Botnet Detection Technique for Corporate Area Network / Savenko O. et al. **Proc. 7th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2013)**. Berlin, Germany, 2013. P. 363–368.
30. Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture / Kashtalian A. et al. **International Journal of Computing**. 2025. Vol. 24, no. 1. P. 35–51. DOI: 10.47839/ijc.24.1.3875.

31. Evaluation Criteria of Centralization Options in the Architecture of Multicomputer Systems with Traps and Baits / Kashtalian A. et al. *Radioelectronic and Computer Systems*. 2025. No. 1. P. 264–297. DOI: 10.32020/reks.2025.1.18.
32. Multi-Computer Malware Detection Systems with Metamorphic Functionality / Kashtalian A. et al. *Radioelectronic and Computer Systems*. 2024. No. 1. P. 152–175. DOI: 10.32020/reks.2024.1.13.
33. A Botnet Detection Approach Based on the Clonal Selection Algorithm / Lysenko S. et al. *Proc. 2018 IEEE 9th Int. Conf. on Dependable Systems, Services and Technologies (DeSSerT 2018)*. Kyiv, Ukraine, 2018. P. 424–428.
34. A Technique for the Botnet Detection Based on DNS-Traffic Analysis / Pomorova O. et al. *Proc. 22nd Int. Conf. Computer Networks (CN 2015)*. Brunów, Poland, 2015. Vol. 522. P. 127–138.
35. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception / Di Geronimo L. et al. *Proc. CHI*. 2020. P. 1–14. DOI: 10.1145/3313831.3376600.
36. Alshehri A., Alrehili K., Alhumaid F., Alessa A. Exploring the Privacy Concerns of Bystanders in Smart Homes. *Proc. Priv. Enhancing Technol. (PoPETs)*. 2022. Vol. 2022, no. 4. P. 253–270. DOI: 10.56553/popets-2022-0064.
37. Lin H., Bergmann N. W. IoT Privacy and Security Challenges for Smart Home Environments. *Information*. 2016. Vol. 7, no. 3. Art. 44. DOI: 10.3390/info7030044.
38. Wang Q., Cai Z., Li R., Fang X. A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis. *Sensors*. 2020. Vol. 20, no. 24. Art. 7030. DOI: 10.3390/s20247030.
39. Yao Y., Zimmermann T., Chin A., Schaub F. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.–Comput. Interact. (CSCW)*. 2019. Vol. 3, no. CSCW. P. 1–24. DOI: 10.1145/3359161.
40. Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions / Saqib E. et al. *ACM Trans. Comput.–Hum. Interact. (TOCHI)*. 2025. P. 1–?. DOI: 10.1145/3731755.
41. Marky K., Prange S., Krell F., Mühlhäuser M., Alt F. ‘You Just Can’t Know About Everything’: Privacy Perceptions of Smart Home Visitors. *Proc. MUM*. 2020. P. 1–13. DOI: 10.1145/3428361.3428464.
42. Android Permissions: User Attention, Comprehension, and Behavior / Felt A. P. et al. *Proc. SOUPS@CHI*. 2012. P. 3–14. DOI: 10.1145/2335356.2335360.
43. Zimmermann V., Gerber P., Marky K., Böck L., Kirchbuchner F. Assessing Users’ Privacy and Security Concerns of Smart Home Technologies. *i-com*. 2019. Vol. 18, no. 3. P. 197–216. DOI: 10.1515/icom-2019-0015.
44. Alshamsi O., Shaalan K., Butt U. Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. *Information*. 2024. Vol. 15, no. 10. Art. 631. DOI: 10.3390/info15100631.
45. Ogonji M. M., Okeyo G., Wafula J. M. A Survey on Privacy and Security of Internet of Things. *Computer Science Review*. 2020. Vol. 38. Art. 100312. DOI: 10.1016/j.cosrev.2020.100312.

References

1. Resilience engineering," *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/Resilience_engineering
2. "System Resilience," *SEBoK Wiki*. [Online]. Available: https://sebokwiki.org/wiki/System_Resilience
3. "The k-out-of-n System Model," *Wiley*. [Online]. Available: <https://catalogimages.wiley.com/images/db/pdf/047139761X.07.pdf>
4. "RBDs and Analytical System Reliability," *ReliaSoft*. [Online]. Available: https://help.reliasoft.com/reference/system_analysis/sa/rbds_and_analytical_system_reliability.html
5. "Reliability analysis of a k-out-of-n:F system under a linear model," *Ann. Inst. Stat. Math.* [Online]. Available: <https://www.ism.ac.jp/editsec/aism/71/0537.pdf>
6. "Availability," *Wikipedia*. [Online]. Available: <https://en.wikipedia.org/wiki/Availability>
7. "k-out-of-n Systems," *ReliaSoft*. [Online]. Available: https://help.reliasoft.com/articles/content/reference_examples/blocksim/k-out-of-n_systems.html
8. "Multi-Blockchain-Based IoT Data Processing Techniques for Big Data Integrity Verification," *Sensors*, vol. 21, no. 10, 2021, Art. no. 3515. [Online]. Available: <https://www.mdpi.com/1424-8220/21/10/3515>
9. "Recovery Time Objective (RTO)," *NIST CSRC*. [Online]. Available: https://csrc.nist.gov/glossary/term/recovery_time_objective
10. ["Mean time to recovery," *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/Mean_time_to_recovery
11. "Measuring System Visual Latency through Cognitive Tests," in *Proc. IEEE VR 2020*. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2020/01/ieee_vr_2020_latency.pdf

12. "Measuring motion-to-photon latency for sensorimotor experiments with VR," *PLOS ONE*, 2022. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10616216/>
13. "Investigating guardian awareness techniques to promote VR user safety," *SMU*. [Online]. Available: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=9024&context=sis_research
14. "Exploring Metaphorical Transformations of a Safety Boundary Wall for VR," *Applied Sciences*. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11125283/>
15. Y. Sun, Z. Jiang, C. Xu, S. Zhou, and Z. Niu, "Communication, Computing and Caching for Mobile VR Delivery: Modeling and Trade-off," *arXiv preprint arXiv:1804.10335*, 2018. [Online]. Available: <https://arxiv.org/abs/1804.10335>
16. X. Zhang, Y. Xia, and M. Ali, "A Smartphone Thermal Temperature Analysis for Virtual and Augmented Reality," National Science Foundation Technical Report, 2020. [Online]. Available: <https://par.nsf.gov/servlets/purl/10219090>
17. J. Gomez, S. Raghunathan, and K. Chowdhury, "Distributed On-Sensor Compute System for AR/VR Devices: A Semi-Analytical Simulation Framework for Power Estimation," *arXiv preprint arXiv:2203.07474*, 2022. [Online]. Available: <https://arxiv.org/abs/2203.07474>
18. J. Xiong, Y. Li, K. Liu, X. Liu, and Z. Liu, "Augmented Reality and Virtual Reality Displays: Emerging Technologies and Future Perspectives," *Light: Science & Applications*, vol. 10, no. 1, 2021, Art. no. 215. [Online]. Available: <https://www.nature.com/articles/s41377-021-00658-8>
19. A. Hazarika, "Towards an Evolved Immersive Experience: Exploring 5G," *Sensors*, vol. 23, no. 7, p. 3682, 2023. [Online]. Available: <https://www.mdpi.com/1424-8220/23/7/3682>
20. K. T. Foerster, H. Schmidt, and D. P. van der Meer, "Transparent Fault Tolerance for Stateful Applications in Kubernetes with Checkpoint/Restore," in *Proc. IEEE SRDS 2023*. [Online]. Available: <https://ktfoerster.github.io/paper/2023-srds.pdf>
21. B. Zhao, S. Guo, and X. Liu, "A Multipath Scheduler Based on Cross-Layer Information for Cloud VR in 5G Edge Networks," *Computer Networks*, vol. 244, p. 110333, 2024. [Online]. Available: <https://doi.org/10.1016/j.comnet.2024.110333>
22. V. Kelkkanen, "Evaluation and Reduction of Temporal Issues in Remote VR," Master's Thesis, Univ. of Oulu, Oulu, Finland, 2023. [Online]. Available: <https://www.diva-portal.org/smash/get/diva2:1744902/FULLTEXT02.pdf>
23. P. Yang, Y. Zhao, J. Wu, and J. Zhang, "Feeling of Presence Maximization: mmWave-Enabled Virtual Reality Meets Deep Reinforcement Learning," *arXiv preprint arXiv:2107.01001*, 2021. [Online]. Available: <https://arxiv.org/abs/2107.01001>
24. H. Qin, Z. Sun, S. Yao, and C. Zhang, "Exploring Metaphorical Transformations of a Safety Boundary Wall for VR," *Applied Sciences*, vol. 14, no. 6, 2024, Art. no. 2520. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11125283>
25. M. Park, J. Kim, and D. Kang, "Recent Advances in Wearable Thermal Devices for Virtual and Augmented Reality," *Micromachines*, vol. 16, no. 3, 2025, Art. no. 338. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12029164>
26. S. Weech, S. Kenny, and M. Barnett-Cowan, "Presence and Cybersickness in Virtual Reality Are Negatively Related: A Review," *Frontiers in Psychology*, vol. 10, p. 158, 2019. [Online]. Available: <https://www.frontiersin.org/articles/10.3389/fpsyg.2019.00158/full>
27. S. Lysenko and A. Kachur, "A Resilience Assurance Process Model for Enhancing Virtual Reality Architectural Design," *Proc. 14th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2024, pp. 1–9. doi: <https://doi.org/10.1109/DESSERT65323.2024.11122129>
28. [O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, and A. Nicheporuk, "A Technique for Detection of Bots which are Using Polymorphic Code," *Communications in Computer and Information Science*, vol. 431, pp. 265–276, 2014. ISSN 1865-0929.
29. O. Savenko, S. Lysenko, A. Kryshchuk, and Y. Klots, "Botnet Detection Technique for Corporate Area Network," in *Proc. 7th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2013)*, Berlin, Germany, Sept. 12–14, 2013, pp. 363–368. ISBN 978-1-4799-1426-5.
30. A. Kashtalian, S. Lysenko, T. Kysil, A. Sachenko, O. Savenko, and B. Savenko, "Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture," *International Journal of Computing*, vol. 24, no. 1, pp. 35–51, 2025. doi: 10.47839/ijc.24.1.3875.
31. A. Kashtalian, S. Lysenko, A. Sachenko, B. Savenko, O. Savenko, and A. Nicheporuk, "Evaluation Criteria of Centralization Options in the Architecture of Multicomputer Systems with Traps and Baits," *Radioelectronic and Computer Systems*, no. 1, pp. 264–297, 2025. doi: 10.32620/reks.2025.1.18.
32. A. Kashtalian, S. Lysenko, O. Savenko, A. Nicheporuk, T. Sochor, and V. Avsiyevych, "Multi-Computer Malware Detection Systems with Metamorphic Functionality," *Radioelectronic and Computer Systems*, no. 1, pp. 152–175, 2024. doi: 10.32620/reks.2024.1.13.

33. [S. Lysenko, K. Bobrovnikova, and O. Savenko, "A Botnet Detection Approach Based on the Clonal Selection Algorithm," in Proc. 2018 IEEE 9th Int. Conf. on Dependable Systems, Services and Technologies (DeSSerT 2018), Kyiv, Ukraine, May 24–27, 2018, pp. 424–428.
34. O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, and K. Bobrovnikova, "A Technique for the Botnet Detection Based on DNS-Traffic Analysis," in Proc. 22nd Int. Conf. Computer Networks (CN 2015), Brunów, Poland, June 16–19, 2015, vol. 522, pp. 127–138.
35. L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, and A. Bacchelli, "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception," in *Proc. CHI*, 2020, pp. 1–14. doi: 10.1145/3313831.3376600.
36. A. Alshehri, K. Alrehili, F. Alhumaid, and A. Alessa, "Exploring the Privacy Concerns of Bystanders in Smart Homes," *Proc. Priv. Enhancing Technol. (PoPETs)*, vol. 2022, no. 4, pp. 253–270, 2022. doi: 10.56553/popets-2022-0064. (Open PDF available.)
37. H. Lin and N. W. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," *Information*, vol. 7, no. 3, art. 44, 2016. doi: 10.3390/info7030044.
38. Q. Wang, Z. Cai, R. Li, and X. Fang, "A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis," *Sensors*, vol. 20, no. 24, art. 7030, 2020. doi: 10.3390/s20247030.
39. Y. Yao, T. Zimmermann, A. Chin, and F. Schaub, "Privacy Perceptions and Designs of Bystanders in Smart Homes," *Proc. ACM Hum.–Comput. Interact. (CSCW)*, vol. 3, no. CSCW, pp. 1–24, 2019. doi: 10.1145/3359161.
40. E. Saqib, S. He, J. Choy, R. Abu-Salma, J. Such, J. Bernd, and M. Javed, "Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions," *ACM Trans. Comput.–Hum. Interact. (TOCHI)*, pp. 1–?, 2025. doi: 10.1145/3731755.
41. K. Marky, S. Prange, F. Krell, M. Mühlhäuser, and F. Alt, "'You Just Can't Know About Everything': Privacy Perceptions of Smart Home Visitors," in *Proc. MUM*, 2020, pp. 1–13. doi: 10.1145/3428361.3428464. (Open PDF available.)
42. A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," in *Proc. SOUPS@CHI*, 2012, pp. 3–14. doi: 10.1145/2335356.2335360.
43. V. Zimmermann, P. Gerber, K. Marky, L. Böck, and F. Kirchbuchner, "Assessing Users' Privacy and Security Concerns of Smart Home Technologies," *i-com*, vol. 18, no. 3, pp. 197–216, 2019. doi: 10.1515/icom-2019-0015.
44. O. Alshamsi, K. Shaalan, and U. Butt, "Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach," *Information*, vol. 15, no. 10, art. 631, 2024. doi: 10.3390/info15100631.
45. M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A Survey on Privacy and Security of Internet of Things," *Computer Science Review*, vol. 38, art. 100312, 2020. doi: 10.1016/j.cosrev.2020.100312.

Sergii Lysenko, Prof, Dr tech. sci., **Artem Kachur**, **Liudmyla Koretska**, Assoc. Prof., PhD tech sci.
Khmelnytskyi National University, Khmelnytskyi, Ukraine

Method for Synthesising Resilient Architectures of Virtual and Augmented Reality Systems

The article considers the problem of ensuring the stability of augmented (AR) and virtual (VR) reality systems, which are characterized by high sensitivity to performance violations and hardware and software failures. Most existing approaches focus on the analysis of fixed architectures, leaving open the issue of automated synthesis of systems that are stable by design.

A new method for analytical synthesis of AR/VR architectures is proposed, which is based on a formal model that links a 20-dimensional vector of mitigation parameters with seven key stability metrics: reliability, availability, fault tolerance, integrity, recovery time, performance stability, and user safety. The design problem is formulated as a multi-criteria optimization problem, for the solution of which a genetic algorithm is used.

Experimental validation conducted in the Simulink environment confirmed the effectiveness of the method. The results showed that the synthesized architecture provides an improvement in the overall resilience index by 19.4% compared to the base configuration under strict operational constraints. In particular, a significant increase in the availability indicators (+82.2%) and recovery time (+39.9%) was achieved. The proposed approach allows for quantitative assessment and optimization of architectural solutions at the design stage.

virtual reality (VR), resilience, VR architecture, fault tolerance, error mitigation, system reliability

Одержано (Received) 12.02.2026

Прорецензовано (Reviewed) 20.02.2026

Прийнято до друку (Approved) 24.02.2026