https://orcid.org/0000–0001–7756–0004
https://orcid.org/0009–0008–2309–7569

УДК 519.718

О.В. ФЕДУХІН[*], О.О. СКРИПНІКОВА[*]

ГАРАНТОЗДАТНІСТЬ КІБЕРФІЗИЧНИХ КОМП'ЮТЕРНИХ СИСТЕМ ІЗ ВБУДОВАНИМИ МІКРОПРОЦЕСОРАМИ

[*]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *У статті проведено системний аналіз сучасного стану теорії та практики забезпечення гарантоздатності кіберфізичних комп'ютерних систем із вбудованими мікропроцесорами. Розглянуто еволюцію концепції гарантоздатності від класичної таксономії Авіженіуса-Лапрі-Ренделла до сучасних підходів. Проаналізовано основні виклики, зумовлені широким впровадженням технологій інтернету речей, штучного інтелекту, хмарних і периферійних обчислень, розподілених сервісів та цифрових двійників. Показано, що традиційні методи оцінювання надійності не повною мірою враховують динамічний характер сучасних кіберфізичних систем, взаємозалежність програмних компонентів, ресурсні обмеження IoT-пристроїв та нові кіберзагрози. Узагальнено сучасні архітектурні підходи до підвищення гарантоздатності, зокрема модельно-орієнтовану інженерію, інтегрований аналіз функціональної та кібербезпеки, технології цифрових двійників, методи ін'єкції відмов, прогнозне технічне обслуговування та шаблони проєктування гарантоздатності. Розглянуто сучасні інструментальні засоби формальної верифікації, моделювання, аналізу ризиків і тестування відмовостійкості. Систематизовано програмні та апаратні механізми забезпечення гарантоздатності, включаючи резервування, активну реплікацію, N-версійне програмування, контрольні точки, блоки відновлення, механізми моніторингу працездатності та реконфігуровані архітектури. Обґрунтовано необхідність переходу від статичних моделей оцінювання до адаптивних методів підтримки гарантоздатності в реальному часі з використанням машинного навчання, аналізу експлуатаційної телеметрії та автоматизованого прогнозування відмов.*
Ключові слова: *гарантоздатність, кіберфізичні системи, вбудовані мікропроцесори, інтернет речей, функціональна безпека, відмовостійкість, цифровий двійник, прогнозування відмов, самовідновлювані системи, резервування, формальна верифікація.*

Abstract. *The paper presents a systematic analysis of the current state of the theory and practice of ensuring the dependability of cyber-physical computer systems with embedded microprocessors. The evolution of the concept of dependability from the classical Avizienis-Laprie-Randell taxonomy to contemporary approaches is examined. The major challenges arising from the widespread adoption of the Internet of Things (IoT), artificial intelligence, cloud and edge computing, distributed services, and digital twins are analyzed. It is shown that traditional reliability assessment methods do not fully address the dynamic nature of modern cyber-physical systems, the interdependencies among software components, the resource constraints of IoT devices, or emerging cybersecurity threats. Contemporary architectural approaches to improving dependability are summarized, including Model-Based Systems Engineering (MBSE), integrated safety and security analysis, digital twin technologies, fault injection techniques, predictive maintenance, and dependability design patterns. Modern tools for formal verification, modeling, risk analysis, and fault-tolerance testing are also reviewed. Software and hardware mechanisms for ensuring dependability are systematized, including redundancy, active replication, N-version programming, checkpointing, recovery blocks, health monitoring mechanisms, and reconfigurable architectures. The necessity of transitioning from static assessment*

models to adaptive run-time dependability assurance methods based on machine learning, operational telemetry analysis, and automated failure prediction is substantiated.
Keywords: *dependability, cyber-physical systems, embedded microprocessors, Internet of Things, functional safety, fault tolerance, digital twin, failure prediction, self-healing systems, redundancy, formal verification.*

DOI: 10.34121/1028-9763-2026-3-112-125

1. Аналіз стану проблеми

Гарантоздатність комп'ютерних систем кіберфізичних комп’ютерних систем із вбудованими мікропропроцесорами (dependability) є комплексною системною властивістю, що інтегрує безвідмовність, готовність, функціональну безпеку, конфіденційність, цілісність даних, ремонтопридатність, живучість та відмовостійкість.

Фундаментальна таксономія, розроблена Алгірдасом Авіженіусом, Жан–Клодом Лапрі та Браяном Ренделлом ще в 1980-х роках, продовжує слугувати теоретичним підґрунтям [1]. Згодом вона була розширена з урахуванням аспектів інформаційної безпеки (security), що дозволило комплексно враховувати як випадкові відмови, так і навмисні кібератаки.

Однак аналіз сучасного стану проблеми виявляє низку суттєвих прогалин між класичними теоретичними моделями та практичними викликами, зумовленими глобальними технологічними тенденціями останніх років.

Інтеграція штучного інтелекту (ШІ) у критичні застосунки породжує нові виклики щодо передбачуваності, інтерпретованості та стійкості до невизначеності. Як зазначається в оглядовій статті «Design for dependability — State of the art and trends» (Journal of Systems and Software, 2024), більшість наявних результатів зосереджена на невеликих, статичних системах, критичних до безпеки, і не може бути безпосередньо перенесена на великі автономні системи з динамічними гетерогенними архітектурами та ШІ-компонентами.

Стрімкий розвиток IoT-систем потребує нових методів забезпечення гарантоздатності в реальному часі (run–time assurance), оскільки неможливо повністю передбачити всі ризики на етапі проєктування.

Зростання складності розподілених архітектур (хмарні обчислення, мікросервіси, туманні та периферійні обчислення) призводить до появи каскадних відмов через програмні залежності, де збій одного сервісу поширюється на десятки взаємопов'язаних компонентів. Понад 90 % сучасного програмного коду базується на open-source компонентах, що підвищує ризики атак на ланцюги постачання (supply chain attacks) та неконтрольованого поширення дефектів.

Загострення кібербезпекових загроз вимагає одночасного врахування випадкових збоїв і цілеспрямованих атак, що потребує спільного моделювання безпеки (safety) та кібербезпеки (security).

Отже, актуальність проблематики гарантоздатності зросла, а існуючі методологічні підходи потребують суттєвого оновлення. Це зумовлює необхідність проведення системного аналізу та визначення нових напрямів досліджень.

2. Постановка мети дослідження

Метою даного дослідження є системний аналіз сучасного стану теорії та практики забезпечення гарантоздатності комп’ютерних систем, кіберфізичних комп’ютерних систем із вбудованими мікропропроцесорами, ідентифікація ключових прогалин між класичними підходами та новими технологічними викликами, а також визначення перспективних напрямів розвитку методів, моделей та інструментальних засобів гарантоздатності.

Для досягнення поставленої мети необхідно вирішити такі завдання:

• Провести структурований аналіз сучасних досліджень IoT-кіберфізичних систем із урахуванням їх стрімкої інтеграції з технологіями на основі ШІ, хмарним та розподіленими сервісами.

• Виявити та класифікувати основні виклики, що обмежують застосування традиційних методів дизайну для гарантоздатності.

• Узагальнити сучасні методологічні підходи, зокрема модель-орієнтований аналіз, шаблони проєктування та інтеграцію методів машинного навчання.

• Сформулювати науково обґрунтовані рекомендації щодо розвитку теорії та практики гарантоздатності.

3. Аналіз сучасного стану теорії та практики забезпечення гарантоздатності комп'ютерних систем

3.1. Фундаментальні концепції та еволюція класифікації загроз

Класифікація загроз гарантоздатності (відмови, помилки, збої) активно розвивається з урахуванням специфіки прикладних доменів. Зокрема, характерними для IoT-систем є дефіцит енергетичних ресурсів, зовнішні фізичні збурення та кібератаки. Така домен-специфічна деталізація є характерною рисою сучасних робіт, оскільки універсальні моделі часто виявляються недостатніми для динамічних гетерогенних середовищ.

3.2. Актуальні напрями досліджень за прикладними доменами

3.2.1. Гарантоздатність систем на основі штучного інтелекту

Інтеграція компонентів ШІ суттєво впливає на методи забезпечення гарантоздатності. Ключовими проблемами є відсутність інтерпретованості (explainability) моделей ШІ, що ускладнює застосування традиційних модель-орієнтованих технік верифікації. Це зумовлює необхідність розвитку методів забезпечення гарантоздатності в реальному часі (run–time assurance), включаючи гібридні підходи, що поєднують аналітичні моделі з data-driven техніками. На конференціях, як-от DepCoS–RELCOMEX, підкреслюється роль когнітивних систем і глибокого навчання для адаптивного управління гарантоздатністю.

3.2.3. Гарантоздатність хмарних та розподілених систем

У хмарних середовищах гарантоздатність визначається стійкістю всієї сервісної екосистеми. Мікросервісні архітектури, контейнеризація, Kubernetes-оркестрація та multi-cloud інфраструктури створюють нові виклики щодо управління відмовами. Особливо небезпечними є каскадні відмови через програмні залежності, які можуть бути спричинені помилками API, перевантаженням черг повідомлень, деградацією баз даних, відмовами балансувальників навантаження або конфігураційними помилками CI/CD. У сучасних дослідженнях активно розглядаються chaos engineering, fault injection, observability-підходи, self-healing архітектури та автоматизоване прогнозування деградації сервісів.

3.2.4. Гарантоздатність вбудованих систем реального часу та IoT-систем

Стрімке поширення інтернету речей (Internet of Things, IoT) зумовлює необхідність переосмислення класичних підходів до забезпечення гарантоздатності. Масштаби розгортання IoT-систем — від «розумних будинків» і промислових сенсорних мереж до критичної інфраструктури «розумних міст» — досягли такого рівня, за якого традиційні моделі надійності виявляються недостатньо ефективними. Гарантоздатність IoT-систем (dependability of IoT) як комплексна властивість охоплює безвідмовність, готовність, функціональну безпеку, живучість та захищеність, однак реалізація цих атрибутів у середовищі масових дешевих пристроїв з обмеженими ресурсами стикається з низкою фундаментальних обмежень [2].

Особливістю IoT-систем є їхня тісна інтеграція з фізичним середовищем: збої в роботі можуть призводити не лише до втрати даних, а й до реальних фізичних наслідків — зупинки виробництва, аварійних ситуацій, загрози життю людей. При цьому динамічна топологія мережі, гетерогенність пристроїв (від сенсорів із мінімальними обчислювальними можливостями до шлюзів з обмеженими ресурсами), а також суттєві енергетичні обмеження для акумуляторних пристроїв створюють принципово нові виклики.

Як показують дослідження, розгортання IoT-проєктів стикається з критичною проблемою забезпечення безперервності функціонування: лише близько 2 % розгорнутих рішень досягають достатнього рівня надійності для виконання критичних застосунків, а три чверті невдалих IoT-проєктів спричинені проблемами на рівні апаратного забезпечення [3].

Систематизація загроз для IoT-середовища вимагає врахування додаткових категорій порівняно з класичними системами. Зокрема, більшість IoT-пристроїв мають обмежену обчислювальну потужність, об'єм пам'яті та енергоспоживання, що унеможливлює застосування стандартних механізмів відмовостійкості та безпеки (наприклад, повноцінного шифрування чи складних протоколів узгодження). Системи IoT об'єднують пристрої різних виробників із різними технічними характеристиками та протоколами зв'язку, що ускладнює створення єдиної політики управління відмовами. При цьому для IoT-систем втрата мережевого зв'язку, поява нових пристроїв, вихід із ладу окремих вузлів є нормою функціонування, а не винятком. Така специфіка при використанні атрибутивної моделі гарантоздатності вимагає враховувати, які з атрибутів мають впливати на кінцеву оцінку. Крім того, IoT-пристрої часто фізично доступні для зловмисника, що створює ризики компрометації апаратного забезпечення, перехоплення даних та атак на ланцюги постачання.

Архітектурні стратегії підвищення відмовостійкості

Відмовостійкість IoT-систем забезпечується комбінацією різнорівневих механізмів. На рівні пристроїв застосовуються методи резервування (replication, cold standby sparing redundancy), що підвищують готовність системи в умовах апаратних відмов. Для мережевого рівня розробляються алгоритми відмовостійкого розміщення вузлів (fault tolerant node placement), які забезпечують альтернативні шляхи комунікації у разі виходу з ладу окремих елементів. На рівні системи в цілому застосовуються комбіновані підходи, що включають прогнозування збоїв, ізоляцію несправних компонентів та самовідновлення (self-healing).

Особливої уваги заслуговують методи оцінки робастності IoT-систем через ін'єкцію відмов (fault injection). Наприклад, для систем на основі RS–485 запропоновано підходи, що дозволяють виявляти приховані дефекти шляхом впровадження відмов у повідомлення, якими обмінюються пристрої [4].

Класичні моделі аналізу відмов (дерева відмов, FMEA) виявилися недостатньо адаптованими для IoT-середовищ, оскільки вони не враховують одночасну дію випадкових апаратних збоїв та кібератак. Для подолання цього обмеження запропоновано інтеграцію FTA (Fault Tree Analysis) із моделями кібербезпекових загроз, що дозволяє здійснювати спільну оцінку ризиків безпеки (safety) та кібербезпеки (security) [5]. Також у сфері оцінки ризиків IoT активно розвиваються фреймворки, що базуються на методології MITRE ATT&CK для Edge-IoT-середовищ, які дозволяють виявляти та пріоритезувати атаки в реальному масштабі часу. Для малих та середніх підприємств пропонуються легковагові ризик-орієнтовані фреймворки, що інтегрують класифікацію активів, STRIDE-моделювання загроз та CVSS-оцінку вразливостей.

Периферійні та хмарні обчислення як засіб підвищення гарантоздатності

Розвиток концепцій edge та fog computing розглядається як один із найперспективніших напрямів підвищення гарантоздатності IoT. Розміщення обчислювальних ресурсів ближче до джерел даних дозволяє знизити затримки, зменшити залежність від нестабільних каналів зв'язку з хмарою, а також підвищити конфіденційність за рахунок локальної обробки чутливих даних. Дослідження показують, що використання edge-вузлів (наприклад, Raspberry Pi, Nvidia Jetson) для раннього виявлення відмов дозволяє підвищити стійкість IoT-мереж до збоїв, зменшуючи затримки та мінімізуючи залежність від централізованих систем. Особливу увагу привертають підходи з використанням багаторівневих edge-архітектур, що забезпечують планування завдань із різним рівнем критичності (mixed-criticality) з урахуванням обмежень енергоспоживання та вимог до затримок. Перспективними напрямами також є легковагові методи вибору edge-серверів, що поєднують прогнозування затримок з адаптивною оцінкою надійності.

Використання блокчейн-технологій для підвищення надійності

Систематичний огляд ключових досліджень із блокчейн-орієнтованих IoT-мереж класифікує методи підвищення надійності та довіри на чотири групи: підходи з використанням машинного навчання, edge-обчислень, легковагових блокчейн-рішень та багаторівневих механізмів. Блокчейн дозволяє створювати незмінний, верифікований реєстр транзакцій між пристроями, що забезпечує цілісність даних та можливість аудиту навіть за наявності певної частки зловмисних вузлів. Інтеграція блокчейну з системами управління довірою на основі репутації дозволяє підтримувати високу надійність навіть за умови, що до 40 % вузлів проявляють зловмисну поведінку.

Проте застосування блокчейну в IoT стикається з проблемами масштабованості та енергоефективності, що стимулює розробку легковагових консенсусних механізмів і гібридних архітектур.

Механізми безпеки для обмежених середовищ

Забезпечення безпеки є критичним аспектом гарантоздатності IoT. Технологія Trusted Execution Environment (TEE) розглядається як ефективний засіб підвищення безпеки та надійності IoT-пристроїв, надаючи захищене середовище виконання для критичного коду та даних навіть у разі компрометації основної операційної системи. Для ресурсо-обмежених пристроїв розробляються легковагові програмні рішення, що забезпечують захист без необхідності встановлення спеціалізованого апаратного забезпечення, що сприяє масовому впровадженню технологій безпеки в IoT.

Метрики та моделі оцінювання гарантоздатності IoT

Формування системи метрик для оцінювання гарантоздатності IoT залишається відкритою науковою проблемою. Традиційні показники (наприклад, MTBF, середній час відновлення) часто не враховують специфічних особливостей IoT: розподілений характер, енергетичні обмеження, динамічну топологію. У сучасних дослідженнях пропонуються композитні метрики, що містять показники стійкості до переривань зв'язку, ефективність механізмів самовідновлення, а також енергетичну ефективність протоколів забезпечення надійності.

Для кількісного аналізу гарантоздатності використовуються як аналітичні моделі (дерева відмов, марковські процеси), так і методи статистичного моделювання. Інтеграція цих підходів у гібридні моделі, що поєднують традиційний надійнісний аналіз із методами машинного навчання для прогнозування відмов, є одним із перспективних напрямів подальших досліджень.

Перспективні напрями та відкриті проблеми

Незважаючи на значний прогрес у сфері гарантоздатності IoT, низка проблем залишаються невирішеними. Очевидна необхідність стандартизації методів оцінки. Існуючі міжнародні стандарти (зокрема серія IEC 62443) розроблялися для промислових систем автоматизації та потребують адаптації до специфіки IoT-середовищ. Відсутність уніфікованих вимог до надійності та безпеки IoT-компонентів ускладнює сертифікацію та порівняння рішень від різних виробників.

Преспективним напрямом є автоматизація управління відмовами в реальному часі. Розгортання великомасштабних IoT-систем потребує розвитку механізмів автоматичного виявлення, локалізації та відновлення після збоїв без участі людини. Особливо актуальними є self-adaptive-архітектури, що динамічно змінюють конфігурацію системи у відповідь на зміну умов середовища.

Ще одним із методів покращення метрик гарантоздатності є використання методів машинного навчання для аналізу телеметрії IoT-пристроїв. Такий підхід дозволяє здійснювати прогнозування відмов до їх настання, що відкриває можливості для проактивного технічного обслуговування.

При цьому необхідно знаходити компроміси між гарантоздатністю та енергоефективністю. Балансування вимог до надійності з обмеженими енергетичними ресурсами автономних пристроїв потребує розробки адаптивних стратегій, що змінюють інтенсивність використання механізмів контролю залежно від поточного стану заряду батареї та критичності виконуваної функції.

Важливою складовою є складність ланцюгів постачання компонентів IoT (від апаратних модулів до програмних бібліотек), що створює ризики внесення вразливостей на всіх етапах життєвого циклу.

Отже, гарантоздатність IoT-систем становить самостійний та динамічно розвинутий напрям досліджень, який вимагає поєднання методів класичної теорії надійності, кібербезпеки, розподілених систем та енергоефективних обчислень. Подальший прогрес у цій сфері значною мірою визначатиме можливість масового впровадження IoT-рішень у критичних сферах життєдіяльності суспільства.

3.3. Методологічні підходи та інструментальні засоби

Можна виділити три основні напрями розвитку інструментальних засобів у сфері забезпечення гарантоздатності програмно-технічних та кіберфізичних систем, які концентруються на трьох взаємодоповнюючих напрямах, що визначають еволюцію методів аналізу, проєктування та експлуатації складних систем.

• ***Модельно-орієнтована інженерія (Model-Based Systems Engineering, MBSE)*** забезпечує формалізований опис архітектури, поведінки та функціональних взаємозв'язків системи протягом усього життєвого циклу. Застосування мов моделювання, зокрема SysML (Systems Modeling Language) та AADL (Architecture Analysis and Design Language), дозволяє створювати єдину цифрову модель системи, що слугує основою для аналізу її гарантоздатності [6]. На відміну від традиційних документо-орієнтованих підходів, MBSE забезпечує автоматизовану перевірку вимог, трасування залежностей між компонентами, моделювання сценаріїв функціонування та аналіз поширення відмов ще на ранніх стадіях проєктування. Особливе значення мають механізми моделювання потоків помилок (Error Propagation Analysis), що дозволяють оцінити каскадний вплив локальних несправностей на функціонування всієї системи [7]. Інтеграція моделей із засобами формальної верифікації, імітаційного моделювання та автоматизованого генерування тестових сценаріїв сприяє скороченню вартості розроблення, зменшенню кількості проєктних помилок та підвищенню рівня гарантоздатності складних систем [8].

• ***Інтегрований аналіз функціональної та кібербезпеки. (Safety-Security Co-engineering).*** Традиційно питання функціональної та інформаційної безпеки розглядалися як незалежні напрями досліджень. Проте цифровізація критичної інфраструктури, поширення кіберфізичних систем, інтернету речей та автономних технологій продемонстрували необхідність комплексного аналізу цих аспектів. Сучасна концепція Safety-Security Co-engineering базується на припущенні, що порушення кібербезпеки можуть бути безпосередньою причиною виникнення небезпечних відмов, тоді як механізми забезпечення функціональної безпеки повинні враховувати можливі навмисні зовнішні впливи. Однією з найбільш перспективних методологій цього напряму є STPA-SafeSec, яка розширює системно-теоретичний аналіз процесів (STPA) [9] шляхом одночасного дослідження небезпечних сценаріїв функціонування, людського фактора, програмних помилок та кіберзагроз. Такий інтегрований підхід дозволяє виявляти взаємозалежності між випадковими відмовами, програмними дефектами та цілеспрямованими кібератаками, що особливо важливо для транспортних систем, промислової автоматизації, енергетичних мереж.

• ***Динамічна гарантоздатність на основі цифрових двійників (Dynamic Dependability with Digital Twins).*** Перехід від періодичного контролю технічного стану до безперервного моніторингу в режимі реального часу є однією з ключових тенденцій сучасної інженерії гарантоздатності. Центральне місце в цьому напрямі займає концепція цифрового двійника (Digital Twin) [10], яка передбачає створення високоточної цифрової моделі фізичної системи, синхронізованої з її реальним станом за допомогою потоків даних від сенсорів та інформаційно-вимірювальних систем. Цифровий двійник забезпечує можливість безперервного оцінювання технічного стану обладнання, аналізу деградації компонентів, прогнозування розвитку несправностей та моделювання можливих сценаріїв експлуатації без втручання у функціонування реального об’єкта. Інтеграція цифрових двійників із методами машинного навчання, аналізу часових рядів та технологіями штучного інтелекту створює основу для реалізації концепції Predictive Maintenance (прогнозного технічного обслуговування), яка дозволяє прогнозувати момент виникнення потенційної відмови, оптимізувати графіки обслуговування та мінімізувати ризик незапланованих простоїв. У сучасних дослідженнях цифрові двійники дедалі частіше розглядаються не лише як інструмент експлуатаційного моніторингу, а й як важливий елемент підтримки прийняття рішень щодо забезпечення гарантоздатності складних кіберфізичних систем протягом усього їх життєвого циклу.

Для реалізації зазначених підходів використовуються класи інструментів, які наведені в табл. 1.

Таблиця 1 — Основні інструментальні засоби у сфері забезпечення гарантоздатності програмно-технічних та кіберфізичних систем

Категорія	Приклади інструментів	Функціональне призначення
Формальна верифікація	PRISM, UPPAAL	Перевірка ймовірнісних моделей та часових параметрів
Аналіз надійності	BlockSim, SAPHIRE	Побудова дерев відмов (FTA) та діаграм надійності (RBD)
Тестування на стійкість	Chaos Mesh, Gremlin	Впровадження штучних збоїв (Chaos Engineering)

Рисунок 1 — Центральний щит системи протидимного захисту

Як приклад оцінки складної кіберфізичної системи за допомогою пакета SAPHIRE можна навести моделювання відмов та розрахунок мінімального перерізу розподіленої обчислювальної структури, яка реалізує систему протидимного захисту висотних будівель (рис. 1) [11].

Як приклад використання підходу Chaos Engineering можна навести методику імітаційного моделювання із заміною контролерів програмними моделями та інжекцією помилок для комплексної оцінки відмовостійкості програмного забезпечення диспетчеризації розподілених систем керування інженерним обладнанням [4].

У загальних випадках оцінка гарантоздатності часто спирається на комбіновані моделі Маркова та напівмарковські процеси. Для систем із самовідновленням (self-healing) використовується функція доступності:

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

де $MTTF$ — середній час до відмови, $MTTR$ — середній час відновлення.

При цьому розвиток інструментальних засобів зміщується від статичного аналізу коду до створення моніторів реального часу, які забезпечують гарантоздатність системи безпосередньо під час експлуатації. Майбутнє галузі полягає в автоматизації верифікації за допомогою «Explainable AI» (XAI), що дозволить аналізувати причини відмов у нейромережевих компонентах.

Дизайн для гарантоздатності

Процес дизайну для гарантоздатності охоплює три взаємопов’язані діяльності: аналіз ризиків, їх пом’якшення та оцінювання ефективності прийнятих рішень. Його основною метою є забезпечення здатності системи виконувати визначені функції навіть за умов виникнення відмов, несправностей або зовнішніх дестабілізуючих впливів.

Перший етап передбачає систематичну ідентифікацію потенційних загроз, джерел відмов і вразливостей системи, а також оцінювання ймовірності їх виникнення та можливих наслідків. Для цього застосовуються методи аналізу ризиків, зокрема FMEA (Failure Modes and Effects Analysis), FTA (Fault Tree Analysis), STPA (System-Theoretic Process Analysis), аналіз сценаріїв відмов та інші підходи, що дозволяють формалізувати критичні ситуації ще на ранніх етапах проєктування.

Другий етап полягає у виборі та реалізації механізмів зменшення ризиків. До таких механізмів належать архітектурна надлишковість, відмовостійкі алгоритми, резервування ресурсів, засоби виявлення та локалізації помилок, автоматичне відновлення після відмов, застосування захисних бар’єрів, а також використання перевірених шаблонів проєктування гарантоздатності. Реалізація зазначених механізмів здійснюється з урахуванням компромісу між рівнем гарантоздатності, продуктивністю системи та вартістю її розроблення.

Третім компонентом процесу є оцінювання гарантоздатності, що містить моделювання, формальну верифікацію, імітаційне моделювання, тестування, аналіз експлуатаційних даних та кількісне визначення показників надійності, готовності, безпечності та ремонтопридатності. Отримані результати використовуються для коригування архітектурних рішень та уточнення моделей ризиків, що забезпечує ітеративний характер процесу проєктування.

Поточний етап розвитку методології дизайну для гарантоздатності характеризується активною інтеграцією компонентів штучного інтелекту. Застосування моделей машинного навчання відкриває нові можливості для прогнозування відмов, адаптивного керування ризиками, автоматичного виявлення аномалій, підтримки прийняття рішень та оптимізації процесів технічного обслуговування. Водночас використання ШІ створює нові виклики, пов'язані з недостатньою пояснюваністю моделей, можливими помилками навчання, невизначеністю поведінки в нештатних ситуаціях та необхідністю забезпечення довіри до результатів функціонування інтелектуальних компонентів. Це зумовлює появу нового напряму досліджень, присвяченого забезпеченню гарантоздатності систем штучного інтелекту (Dependable AI).

Важливою віхою розвитку галузі стало опублікування у 2023-му році першого систематичного огляду шаблонів гарантоздатності (dependability patterns) [12], який узагальнив сучасні архітектурні рішення щодо забезпечення основних атрибутів гарантоздатності. Дослідження охопило шаблони забезпечення відмовостійкості (fault tolerance), безвідмовності (reliability), функціональної безпеки (safety), готовності (availability), а також їх комбінації для складних кіберфізичних і програмно-апаратних систем. Результати аналізу підтвердили, що використання стандартизованих шаблонів дозволяє повторно застосовувати перевірені рішення, скорочувати час проєктування та підвищувати якість архітектурних рішень.

Аналіз сучасних досліджень свідчить, що модель-орієнтовані підходи (Model-Based Engineering, MBSE) залишаються домінуючою методологією забезпечення гарантоздатності. Вони забезпечують формалізоване представлення структури системи, її поведінки та взаємозв'язків між компонентами, що створює можливості для автоматизованої верифікації, генерації тестів і проведення аналізу ризиків. Одночасно спостерігається активне доповнення класичних моделей сучасними методами аналізу даних. Зокрема, дедалі ширше застосовуються exploratory data analysis для дослідження експлуатаційної інформації, методи візуальної аналітики для підтримки експертного аналізу складних процесів, а також спеціалізовані алгоритми аналізу рідкісних подій (rare event analysis), які дозволяють оцінювати ймовірність виникнення критичних, але малоймовірних сценаріїв функціонування систем.

Отже, сучасний розвиток дизайну для гарантоздатності характеризується переходом від ізольованого використання класичних методів аналізу ризиків до комплексного поєднання модель-орієнтованого проєктування, аналізу великих обсягів експлуатаційних даних, технологій штучного інтелекту та стандартизованих архітектурних шаблонів. Така інтеграція створює передумови для підвищення рівня гарантоздатності складних програмно-технічних систем в умовах зростаючої складності їх архітектури та невизначеності експлуатаційного середовища.

Кіберфізичні комп’ютерні системи з вбудованими мікропроцесорами тісно поєднують як програмну складову, так і апаратні засоби. Це вимагає комплексного підходу до дизайну для гарантоздатності таких систем. Розглянемо апаратну складову.

Діаграма (рис. 2) відображає ієрархію та взаємозв'язки між різними методами забезпечення надійності апаратного забезпечення. Вона включає такі категорії:

• Активна реплікація — це процес одночасного виконання операцій на кількох вузлах.

• Активно-пасивне резервування передбачає, що коли один вузол працює, інший перебуває в режимі очікування. Механізми підтвердження верифікують отримання або виконання операцій.

• Рівні активної реплікації включають модель надмірності з *N*-модулями.

Рисунок 2 — Діаграма забезпечення надійності апаратного забезпечення

Подвійна надмірність використовується переважно для виявлення помилок, але не завжди для їх автоматичного виправлення без додаткових механізмів.

Квазімісткова структура — це високонадійна двоканальна архітектура відмовостійких обчислювальних систем та електроніки критичного застосування. Вона поєднує безперервне самоперевірення та реконфігурацію, забезпечуючи вищу ймовірність безвідмовної роботи за значно меншої апаратної надмірності, ніж традиційні мажоритарні схеми [13].

До керуючих елементів відноситься «Оцінювач», який аналізує результати від рівнів активної реплікації. На основі аналізу «Оцінювача» може відбуватися перемикання на систему активно-пасивного резервування, якщо активні модулі вийшли з ладу або видають суперечливі дані.

Розглянемо програмну складову. Для підвищення гарантоздатності інформаційних систем необхідне застосування комплексу методів, спрямованих на своєчасне виявлення

відмов, локалізацію несправностей, збереження працездатності та відновлення функціонування системи без втрати критично важливої інформації. Використання таких методів є особливо актуальним для автоматизованих систем керування об’єктами критичної інфраструктури, де навіть короткочасне порушення функціонування може призвести до значних матеріальних збитків або створити загрозу безпеці людей.

Важливу роль у забезпеченні безперервної роботи відіграє механізм періодичного контролю працездатності компонентів системи, який ґрунтується на регулярному обміні службовими повідомленнями між її елементами. Аналіз своєчасності надходження таких повідомлень дає змогу оперативно виявляти відмови окремих програмних модулів, каналів зв'язку або апаратних засобів та своєчасно ініціювати процедури резервування чи відновлення.

Для мінімізації наслідків можливих відмов застосовується механізм збереження контрольного стану системи. Його сутність полягає у періодичній фіксації поточного стану програмного забезпечення, службових даних та результатів виконання обчислень. У разі виникнення збою це забезпечує можливість швидкого повернення до останнього коректного стану без необхідності повторного виконання всього технологічного процесу.

Підвищення достовірності результатів досягається також шляхом використання структурної надлишковості програмного забезпечення. Для цього створюються кілька незалежно реалізованих програмних модулів, які виконують однакові функції. Отримані результати порівнюються спеціальним модулем прийняття рішення, який визначає найбільш достовірний результат на основі принципу більшості або інших критеріїв узгодженості. Такий підхід істотно зменшує ймовірність виникнення помилок, пов'язаних із недоліками окремої програмної реалізації.

Іншим ефективним методом забезпечення відмовостійкості є застосування альтернативних програмних реалізацій. Спочатку виконується основний алгоритм, після завершення якого здійснюється перевірка правильності отриманого результату за встановленими критеріями. Якщо результат не відповідає вимогам, автоматично активізується альтернативний алгоритм, який забезпечує виконання тієї ж функції іншим способом. У сучасних інформаційних системах можливе як одночасне виконання кількох альтернативних алгоритмів із подальшим вибором найкращого результату, так і їх розподілене виконання на різних обчислювальних вузлах, що додатково підвищує стійкість системи до відмов.

Перспективним напрямом розвитку гарантоздатних інформаційних технологій є поєднання структурної програмної надлишковості з механізмами автоматичного відновлення. Такий комплексний підхід дозволяє одночасно забезпечити високу достовірність результатів обчислень, своєчасне виявлення програмних помилок, автоматичне усунення наслідків відмов та збереження безперервності функціонування інформаційної системи навіть за наявності несправностей окремих компонентів.

Необхідною складовою зазначених методів є спеціалізований модуль оцінювання результатів обчислень, який виконує функції контролю їх правильності, аналізу відповідності встановленим критеріям та формування рішення щодо подальшого функціонування системи. Залежно від застосованого підходу цей модуль реалізує або порівняння результатів незалежних програмних реалізацій, або перевірку їх відповідності визначеним умовам правильності, забезпечуючи тим самим підвищення надійності та гарантоздатності програмного забезпечення.

Розглянемо діаграму класів, яка відображає архітектурні патерни та механізми надійності програмного забезпечення (рис. 3). Вона ілюструє взаємозв'язки між різними стратегіями виявлення та виправлення помилок.

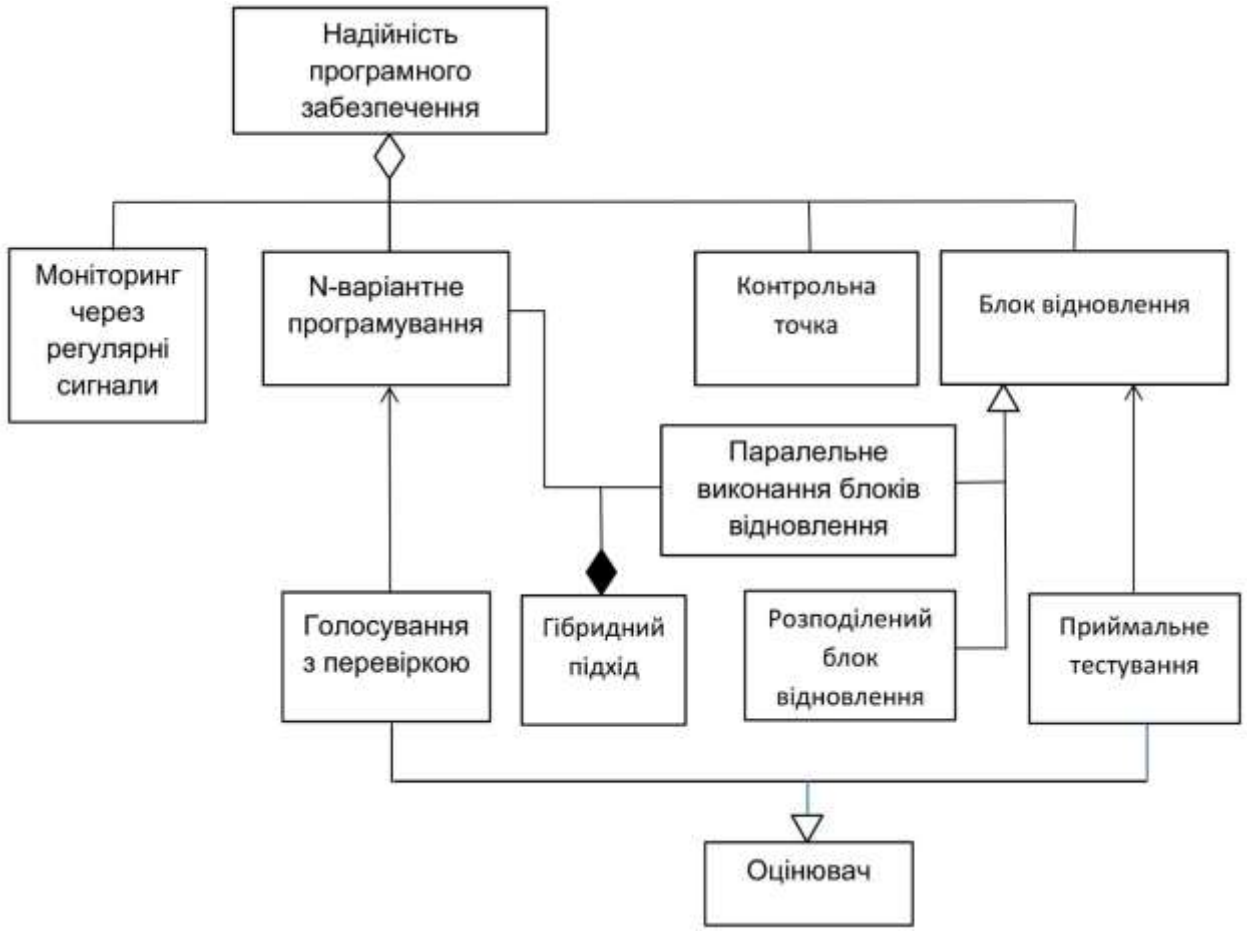

Рисунок 3 — Діаграма забезпечення надійності програмного забезпечення

Основні компоненти та їхні ролі:

• Механізм моніторингу працездатності системи через регулярні сигнали.

• Контрольна точка. Збереження стану системи для можливості відновлення у разі збою.

• *N*-варіантне програмування. Метод надлишковості, де декілька незалежних версій програми виконують одне завдання. Рішення приймається компонентом «Голосування з перевіркою».

• Блок відновлення. Метод відмовостійкості, де альтернативні блоки коду виконуються, якщо основний не пройшов «Приймальне тестування»:

– паралельне виконання блоків відновлення;

– розподілені блоки відновлення.

• Гібридний підхід, що поєднує елементи *N*-версійного програмування та блоків відновлення.

• «Оцінювач» — базовий компонент (узагальнення), від якого успадковуються механізми перевірки результатів.

4. Практична цінність

Практична цінність отриманих результатів полягає в можливості їх безпосереднього використання.

Для інженерів та архітекторів ПЗ надано систематизований огляд шаблонів проєктування для гарантоздатності. Визначено пріоритетні напрями впровадження chaos engineering та self-healing-архітектур.

Для програмного забезпечення рекомендовано використовувати комплекс механізмів підвищення відмовостійкості, що включає контроль працездатності компонентів, періодичне збереження стану системи, структурну програмну надлишковість, альтернативні програмні реалізації та автоматичне відновлення після відмов.

На рівні апаратного забезпечення доцільно застосовувати комбіновані схеми резервування, квазімісткові структури, активну реплікацію, реконфігуровані відмовостійкі архітектури та механізми безперервного самоконтролю, які дозволяють підтримувати працездатність системи навіть за виникнення множинних несправностей.

Перспективним напрямом подальших досліджень є створення адаптивних методів оцінювання гарантоздатності, що використовують методи машинного навчання, аналіз експлуатаційної телеметрії та прогнозування відмов у режимі реального часу.

5. Висновки та рекомендації

У роботі виконано системний аналіз сучасного стану досліджень у сфері забезпечення гарантоздатності кіберфізичних комп'ютерних систем із вбудованими мікропроцесорами. Показано, що класичні моделі гарантоздатності залишаються теоретичною основою аналізу складних систем, однак їх практичне застосування потребує суттєвого розширення з урахуванням розвитку технологій штучного інтелекту, інтернету речей, розподілених обчислень та цифрових двійників.

Проведений огляд дозволив встановити, що сучасні дослідження зміщуються від забезпечення окремих властивостей надійності до інтегрованого підходу, який одночасно враховує функціональну безпеку, кібербезпеку, відмовостійкість, адаптивність та безперервний моніторинг технічного стану систем. Особливого значення набувають модельно–орієнтоване проєктування, цифрові двійники, методи ін'єкції відмов, Chaos Engineering, автоматизоване прогнозування відмов та технології самовідновлення.

Встановлено, що для кіберфізичних систем із вбудованими мікропроцесорами ефективне забезпечення гарантоздатності можливе лише за умови комплексного використання програмних і апаратних механізмів резервування, контролю працездатності, відновлення після відмов, структурної надлишковості та постійного аналізу експлуатаційних даних.

Перспективи подальших досліджень полягають у розробленні єдиних моделей оцінювання гарантоздатності для складних кіберфізичних систем, створенні адаптивних механізмів підтримки гарантоздатності в режимі реального часу, інтеграції методів штучного інтелекту з формальними моделями аналізу ризиків, а також стандартизації метрик оцінювання гарантоздатності сучасних IoT та кіберфізичних систем.

СПИСОК ДЖЕРЕЛ

1. Avizienis A., Laprie J.C., Randell B. Fundamental concepts of dependability. *Journal of Systems and Software*. 1980. P. 5–12. URL: https://pld.ttu.ee/IAF0530/16/avi1.pdf.
2. URL: https://journals.nupp.edu.ua/sunz/en/article/view/3823.
3. URL: https://eng.iotexpo.com.cn/industry–news/iot–connectivity–ai–adoption–2025.html.
4. Скрипнікова О.О., Ґедзь О.В., Оцун Б.М. Елементи імітаційного моделювання відмовостійкості програмного забезпечення диспетчеризації розподіленої системи керування інженерним обладнанням висотних будівель. *Global Trends in Science: Research, Innovation and Development:* Proc. of the 2nd Intern. Scient. and Pract. conf. (Sep. 29 – Oct. 1, 2025). Varna, Bulgaria, 2025. P. 160–165. URL: https://www.eoss–conf.com/wp–content/uploads/2025/09/Varna_Bulgaria_29.09.25.pdf.
5. Mohammad Rezaul Karim1, Sohag Kabir2, Ci Lei3 , Raluca Lefticaru4, and Mohammad Abdul Baset. A Combined Approach to Safety and Security of IoT by Applying Fault Tree Analysis and Attack Trees with Minimal Cut Sets. *Aviation Electronics, Information Technology, Telecommunications, Electricals, and Controls (AVITEC).* 2025. Vol. 7, N 2. P. 113–127. DOI: https://doi.org/10.28989/avitec.v7i2.2918.
6. Friedenthal S., Moore A., Steiner R. *A Practical Guide to SysML: The Systems Modeling Language*. 3rd ed. Burlington: Morgan Kaufmann, 2015. 640 p.

7. Feiler P.H., Gluch D.P. Model-Based Engineering with AADL: An Introduction to the SAE Architecture Analysis and Design Language. Boston: Addison-Wesley, 2013. 760 p.
8. Madni A.M., Purohit S., Madni C.C. Exploiting Digital Twins in MBSE to Enhance System Modeling and Life Cycle Coverage. *Handbook of Model-Based Systems Engineering*. Cham: Springer. 2023. DOI: https://doi.org/10.1007/978–3–030–93582–5_33.
9. Abdulkhaleq A., Wagner S. STPA-Sec: Safety Meets Security. *Computer Safety, Reliability, and Security (SAFECOMP Workshops)*. Springer, 2015. P. 33–48.
10. Larsen P.G., Fitzgerald J., Woodcock J. How Do We Engineer Trustworthy Digital Twins? *Research Directions: Cyber-Physical Systems*. 2023. Vol. 1. e3. DOI: https://doi.org/10.1017/cbp.2023.3.
11. Begun V., Hedz O., Begun S., Analysis of the Importance of Electronic Components in Automated Smoke Protection Systems for Modern High–Rise Buildings. *SCIREA Journal of Information Science and Systems Science*. 2025. Vol. 9, Issue 2, April 2025. P. 60–85. DOI: https://doi.org/10.54647/isss1204.
12. URL: https://www.mdpi.com/2073–431X/12/10/214.
13. Муха Ар.А., Федухин А.В. К вопросу о достоверности функционирования компьютерных систем с квазимостиковой структурой. URL: https://www.immsp.kiev.ua/publications/articles/2019/_2019_3/03_Feduchin_19.pdf.

Стаття надійшла до редакції 26.05.2026 / прийнята до друку 13.08.2026