https://orcid.org/0000-0001-6591-2199
https://orcid.org/0000-0002-9068-5837

УДК 519.718

П.Д. СЕСПЕДЕС ГАРСІЯ*, Н.В. СЕСПЕДЕС ГАРСІЯ*

СУЧАСНІ НАПРЯМИ ЗАРУБІЖНИХ ДОСЛІДЖЕНЬ У ГАЛУЗІ ГАРАНТОЗДАТНОСТІ СИСТЕМ

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

Анотація. *Стаття присвячена аналізу сучасних напрямів розвитку теорії і практики гарантоздатності комп'ютерних та інших систем. У багатьох країнах світу використання гарантоздатних комп'ютерних систем та питання розробки методів для розрахунку показників гарантоздатності обговорюються на спеціалізованих національних і міжнародних форумах і конференціях. Актуальними, як і раніше, є визначення, уточнення і формулювання базових понять і таксономії теорії забезпечення гарантоздатності. В усьому світі проводяться інтенсивні наукові дослідження, практичні науково-технічні розробки комп'ютерних систем та мереж для забезпечення гарантоздатності в авіаційних, ракетно-космічних і військово-промислових комплексах, керуючих системах на атомних електростанціях, залізничному транспорті, в системах охорони здоров'я, а також у фінансовій сфері бізнес-критичного застосування. Теорія гарантоздатності актуальна, але все ще недостатньо розвинена у сферах систем кібербезпеки; виявлення аномалій у мережевому трафіку; систем автоматизованого проєктування; систем доповненої і віртуальної реальності; самовідновлювальних систем; робототехніки; кіберфізичних датчикових систем; методів і засобів ідентифікації людини (біометрія); моніторингу екологічного стану; аналітики крупномасштабних даних та інтелектуального аналізу даних для бізнес-областей і цифрового банкінгу; баз даних; комп'ютерних систем охорони здоров'я; систем бездротового зв'язку. Підвищення рівня гарантоздатності набирає актуальності у таких сферах: хмарні сховища і обчислення; шифрування, квантові обчислення і криптографічні методи; збереження конфіденційності та контроль доступу до особистих даних; безпека і надійність блокчейну. Підсумки, що отримані у роботі, можуть бути корисні для широкого кола фахівців, які займаються дослідженнями в галузі гарантоздатності в усіх сферах її застосування.*

Ключові слова: *гарантоздатність комп'ютерних систем, загрози, апаратні та програмні засоби, безпека, конфіденційність, цілісність.*

Abstract. *This article analyzes modern trends of the development of the theory and practice of dependability of computer and other systems. The use of dependable computer systems and the development of methods for dependability indicators calculation are discussed at specialized national and international forums and conferences in many countries around the world. It is still relevant to define, clarify and formulate the basic concepts and taxonomy of the dependability theory. All over the world intensive scientific research, practical scientific and technical development of computer systems and networks are carried out with the aim of ensuring dependability in aviation, rocket, space and military-industrial complexes, control systems at nuclear power plants, railway transport, healthcare systems and also in the financial sphere of business-critical application. Dependability theory is relevant, but still underdeveloped in the following areas: cybersecurity systems, network traffic anomalies detection, computer-aided design systems, augmented and virtual reality systems, self-healing systems, robotics, cyber-physical sensor systems, methods and means of human identification (biometrics), environmental monitoring, large-scale data analytics and data mining for business areas and digital banking, databases, healthcare computer systems, wireless communication systems. The following areas are still gaining relevance towards improving their dependability level: cloud storage and computing, encryption, quantum computing and cryptographic methods, maintaining confidentiality and personal data access control, blockchain security and reliability. The results obtained in the paper can be useful for a wide range of experts that are involved in the research of dependability in all areas of its application.*

Keywords: *computer systems dependability, threats, hardware and software, security, confidentiality, integrity.*

DOI: 10.34121/1028-9763-2021-2-95-101

1. Вступ

Вже понад 30 років у багатьох країнах використання гарантоздатних комп'ютерних систем (ГКС) і питання розробки методів для розрахунку показників гарантоздатності обговорюються на спеціалізованих національних і міжнародних форумах та конференціях. Актуальними, як і раніше, є визначення, уточнення і формулювання базових понять і таксономії теорії забезпечення гарантоздатності.

В усьому світі проводяться інтенсивні наукові дослідження, практичні науково-технічні розробки і використовується накопичений досвід роботи з КС та мережами для забезпечення гарантоздатності в авіаційних, ракетно-космічних і військово-промислових комплексах, керуючих системах на атомних електростанціях, залізничному транспорті, у системах охорони здоров'я, а також у фінансовій сфері бізнес-критичного застосування. Це звісно передбачає оцінку продуктивності систем, методи моделювання, експерименти, порівняльні аналізи і аналізи апостеріорних даних.

Для забезпечення відмовостійкості КС розглядається необхідність використання різного роду надлишковості (функціональної та структурної) і питання розробки й мінімізації терміну тестування програмного забезпечення та операційних систем [1].

Набирає актуальності тема забезпечення гарантоздатності при низьких витратах для доступності високонадійних КС у повсякденному житті [2].

Серед дослідників у галузі гарантоздатності, відмовостійкості, надійності, живучості та безпеки необхідно відзначити великий внесок вітчизняних вчених: д.т.н., професора В.С. Харченка (НАУ ім. М.Є. Жуковського «ХАІ»); д.т.н., професорів В.О. Романкевича і Ю.Г. Савченка (НТУ України «КПІ імені Ігоря Сікорського»); д.т.н., професора О.В. Дрозда (ОНПУ України); д.т.н., професора В.О. Романова (ІК імені В.М. Глушкова НАН України) та д.т.н. В.П. Стрельнікова і О.В. Федухіна (ІПММС НАН України).

Основні напрями роботи з гарантоздатності вітчизняних фахівців: розробка теоретичних основ і прикладних методів створення гарантоздатних комп'ютерних засобів, систем високого рівня надійності, спеціалізованих систем, теорії багатоверсійних систем, методів і засобів оцінки і забезпечення надійності і функціональної безпеки, технологій створення та експертизи гарантоздатних комп'ютерних систем для критичних інфраструктур (атомні електростанції, аерокосмічні комплекси, авіація, військово-промислові комплекси, залізничний транспорт, бізнес-критичні системи), засоби верифікації програмного забезпечення та системи програмованої логіки.

Великий інтерес представляє інформація про напрями досліджень і отримані результати в області теорії і практики гарантоздатності відомих зарубіжних дослідників.

Метою статті є аналіз сучасних напрямів досліджень і практичного застосування теорії гарантоздатності комп'ютерних та інших систем за кордоном.

2. Області та напрями, актуальні для теорії гарантоздатності

Аналізуючи матеріали міжнародних наукових конференцій і завдяки глибокому і всебічному розгляду проблем у роботі апаратно-програмної частини різних систем, можна виділити такі області і напрями, в яких необхідно застосовувати існуючі і розробляти нові методи і методології при проєктуванні, оцінці, перевірці та забезпеченні гарантоздатності комп'ютерних систем і мереж.

2.1. Збої, помилки, аномалії

У великомасштабних високопродуктивних обчислювальних системах відмови компонентів стають нормою, а не винятком. Виникнення збоїв, а також їх вплив на продуктивність системи і експлуатаційні витрати стають все більш важливою проблемою для розробників і адміністраторів системи. Однак складно ефективно ідентифікувати аномалії з великої кількості даних, а виявлення їх вручну вимагає занадто багато часу і може викликати помилки. Тому особлива увага приділяється питанням оцінки помилок у проєктуванні, різних умов експлуатації, створення інструментів щодо виявлення випадкових збоїв, аномалій у забезпеченні безпеки мережевого трафіка, датчикових, хмарних системах і системах з великим об'ємом даних [3]. Активно розвивається напрям автоматично створюваних статистичних моделей, що застосовуються для виявлення мережевих аномалій [4].

У 2020 році була отримана премія Вільяма К. Картера за докторську дисертацію в області гарантоздатності вченим Bo Fang. У дисертації порушено проблему тимчасових апаратних збоїв у системах високопродуктивних обчислень. Вважається, що більшість короткочасних апаратних збоїв не роблять значного впливу на програмному рівні. В роботі Bo Fang запропонована модель визначає, які збої дійсно мають значення, особливо ті, які можуть викликати непомітне пошкодження даних для того, щоб вибірково виконати дії по відновленню. Так само в роботі пропонується інноваційна ідея застосування схеми відновлення, що дозволяє підвищити ефективність щодо продуктивності, так і в енергозбереженні [5].

2.2. Кібератаки, загрози

Для класичних інформаційних систем проблеми кібербезпеки знаходяться в цифровому полі, вони можуть проявлятися у вигляді відмов при обслуговуванні, крадіжки даних (порушення конфіденційності), знищення даних (порушення цілісності). Вплив на інтелектуальну систему шкідливого програмного забезпечення або кібератак може бути направлений на дистанційне управління об'єктом із метою відключення або зміни виконання закладених функцій, що призводить до катастрофічних наслідків (нещасні випадки, смерть та ін.).

Проблема навмисних кібератак вимагає розробки протоколів і алгоритмів для виявлення, запобігання, діагностики, усунення випадкових і зловмисних загроз, виявлення ботнетів і кібератак. Крім цього, існує потреба у створенні універсального методу для аналізу та усунення шкідливих програм, а також виявлення метаморфічних шкідливих програм.

Особлива увага спрямована на створення методів і оптимальної персоналізованої стратегії виявлення DoS- і DDoS-атак у мережевих системах [6].

2.3. Апаратні, програмні системи і забезпечення

Сучасні технічні системи являють собою сукупність кінцевого числа взаємопов’язаних апаратних і програмно-апаратних компонентів. Це досить складні об'єкти, безвідмовна робота яких вимагає комплексного вирішення питань, пов’язаних із гарантоздатністю. Тому приділяється велика увага гарантоздатності, безпеці та відмовостійкості систем, хмарних, туманних, росистих і гібридних обчислень, програмно визначених мереж, периферійних обчислень, забезпеченню якості програмного і проміжного програмного забезпечення комп'ютерних систем, мереж та IT-інфраструктур, наднадійних мереж із малою затримкою, розробці гарантоздатних методів обміну інформацією та додатків для датчикових систем і роботів [7].

Приділяється значна увага забезпеченню якості та валідації апаратного забезпечення (мікропроцесори, пам'ять постійна і динамічна, однокристальні системи, периферійні пристрої введення-виведення), розробці високонадійної електроніки та промислової робототехніки [8]. З появою нових технологій виникають і нові напрями досліджень для фахів-

ців із гарантоздатності. Як приклад можна привести роботи по підвищенню надійності систем бездротового зв'язку за рахунок використання технології FSO/RF [4].

Актуальними є питання надійності, уразливості, перевірки та валідації програмного забезпечення та операційних систем, хмарних сховищ і кіберфізичних вбудованих систем [8]. Також увага спрямована на проєктування та виробництво надійних самовідновлювальних, самозахисних відмовостійких систем і мереж. Як приклад самовідновлювальної мережі можна розглянути автоматизовану систему розподілу електроенергії з інтелектуальними індикаторами поширення відмови. Така система дозволяє ідентифікувати місце відмови, автоматично ізолювати його і відновити постачання електроенергії.

2.4. Оцінка, аналітика, аналіз, тестування

Одним із важливих наукових і практичних завдань є оцінка, аналітика, аналіз, перевірка, тестування моделей, методів, методологій в області забезпечення гарантоздатності інформаційних систем.

Основні зусилля фахівців із гарантоздатності сконцентровані в таких напрямах:

– розробка моделей і методологій для проєктування, оцінки, перевірки, забезпечення гарантоздатності і безпеки систем (оцінка продуктивності, аналітичні методи, моделювання, експерименти, порівняльний аналіз і аналіз польових даних) [8];

– розробка методів проєктування, моделювання, перевірки, тестування апаратних засобів, програмного забезпечення і компонентів комп'ютерних систем, мереж та інфраструктур для критично важливих областей;

– розробка методів забезпечення гарантоздатності електрообладнання: оцінка технічного стану з використанням програмно-інформаційних засобів;

– розробка методів забезпечення гарантоздатності, аналіз безпеки процесу експлуатації електронних систем, що використовуються у критично важливих інфраструктурах, у випадку сильного електромагнітного імпульсного впливу [4].

2.5. Безпека, захист, конфіденційність

Основою роботи сучасних обчислювальних систем є безпека роботи даних систем, захист від зовнішнього несанкціонованого впливу і/або проникнення в систему. Це досягається за рахунок використання надійних компонентів, структур, процедур та ін. У цьому напрямі велика увага приділяється питанням інформаційної безпеки, збереження конфіденційності та контролю доступу, розробці методів і засобів ідентифікації людини (біометрія), розробці захищених систем управління персональними даними, а також безпеці і конфіденційності баз даних [9].

2.6. Штучний інтелект, нейромережі

Системи штучного інтелекту все більше впроваджуються у професійну і повсякденну діяльність людини. До таких систем можна віднести, наприклад, методи розпізнавання образів (включаючи як більш складні і спеціалізовані, так і нейронні мережі), які широко використовують при оптичному і акустичному розпізнаванні (в тому числі тексту й мови), у медичній діагностиці. Область застосування штучного інтелекту досить широка: це і фінанси, і військова справа, і важка промисловість, і управління людськими ресурсами, і видавнича діяльність, і медицина, і технічне обслуговування телекомунікацій, розвага та ігри, транспорт, інтернет речей та ін. У комп'ютерних науках проблеми штучного інтелекту розглядаються з позицій проєктування експертних систем та баз знань.

Фахівців із гарантоздатності штучний інтелект цікавить у першу чергу для проєктування, забезпечення безпеки, кібербезпеки і захисту інтелектуальних систем [7]. Як і раніше, актуальні питання впливу методів штучного інтелекту на промисловість залізниць, ро-

зробки додатків і інтелектуальних систем для аналізу даних на основі машинного навчання, розвиток машинного навчання, створення комп'ютерних програм високої точності [6]. Ці питання тісно перетинаються із проблемами штучного інтелекту в автоматизованому керуванні, а саме із проблемами, що виникають після подання концепцій автоматизованого водіння і використання в них глибоких нейронних мереж [10].

2.7. Криптографія, шифрування, блокчейн

Сучасна криптографія, крім методів шифрування даних, стала включати в себе і методи забезпечення конфіденційності (неможливості прочитування інформації сторонніми), цілісності даних (неможливості непомітної зміни інформації), аутентифікації (перевірки справжності авторства чи інших властивостей об’єкта). Традиційна криптографія утворює розділ симетричних криптосистем, в яких зашифрування і розшифрування проводиться з використанням одного і того ж секретного ключа. Однак сучасна криптографія включає в себе також і асиметричні криптосистеми, системи електронного цифрового підпису (ЕЦП), хеш-функції, управління ключами, отримання прихованої інформації, квантову криптографію.

Фахівців в області гарантоздатності цікавлять такі напрями: квантові обчислення і післяквантова криптографія; криптографічні методи і набори інструментів; електронне голосування з шифруванням підпису; безпеку і надійність блокчейна для критично важливих систем (у тому числі систем реального часу) і бізнес-областей [6].

Щодо питання на тему шифрування та криптографії, в 2020 році лауреатом Премії Лапрі була обрана наукова стаття авторів Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, і Gene Tsudik на тему: «Масштабоване і ефективне доказове володіння даними». В їх роботі розглянута проблема ступеня довіреності з точки зору безпеки і надійності зберігання даних у хмарних сховищах і створення безпечної техніки, заснованої на криптографії з симетричним ключем, яке не потребує масового шифрування [11], що свідчить про високу актуальність даного напряму в питанні гарантоздатності.

2.8. Транспорт

Сучасна транспортна інфраструктура включає в себе додаткові підсистеми, від роботи яких залежить безпека руху транспортних засобів. До цих додаткових систем відносяться як апаратні, так і програмні засоби, забезпеченням гарантоздатності яких займаються фахівці в цій галузі і самі розробники. Ведуться серйозні роботи щодо забезпечення гарантоздатності і безпеки інтелектуальних транспортних систем, безпілотних автомобілів, дронів [7].

Все більше уваги приділяється проблемам і можливості забезпечення гарантоздатності громадського транспорту (автономні шатли, допоміжні системи для водіїв поїздів). Наприклад, у дослідницькій лабораторії автономного водіння Intel Labs проводять вимір і стандартизацію поняття безпеки в області автоматизації транспортних засобів [10].

В інфраструктурі безпеки польотів розробники і фахівці посилено займаються питаннями забезпечення гарантоздатності багатоканальних систем зв'язку і операцій технічного обслуговування для організації повітряного руху. Приділяється увага моделюванню рівнів безпеки транспортного обладнання, схильного до впливу сильних електромагнітних імпульсів. Актуальними є питання надійності і безпеки інтелектуальних транспортних телекомунікаційних мереж, що підтримують транспортні послуги [1].

2.9. Критична область

Для забезпечення функціонування різних систем у критично важливих галузях потрібні все більш потужні і інтегровані автономні системи. У зв'язку з цим приділяється велика

увага питанням безпеки і захисту при розробці критично важливих відмовостійких систем, а також супутнього програмного забезпечення. У зв'язку з цим утворюється потреба у створенні ефективних методів перевірки подібних систем.

Також залишаються актуальними питання захисту критичних інфраструктур від кібератак і стійкості розумних мереж (smart grid) [7].

В окрему галузь досліджень виділяють моделювання та оцінку безпеки інформаційних і керуючих систем атомних електростанцій на базі програмованої платформи з урахуванням прихованих фізичних і конструктивних недоліків [1].

2.10. Великі обсяги даних

Людство активно входить в інформаційну епоху, що супроводжується величезними обсягами даних, які генеруються кожен день із датчиків, окремих архівів, соціальних мереж, інтернету речей і інтернету в різних масштабах і форматах, що є серйозною проблемою для гарантоздатності систем. Саме тому вже довгий час дуже актуальні питання безпеки і конфіденційності баз даних, моніторингу центру обробки даних, основи і управління системами баз даних і великими обсягами даних, розробки методів інтелектуального аналізу даних для бізнесу і критичних областей [7].

2.11. Інфраструктура

Інформаційні технології з кожним днем все більше впроваджуються в різні системи інфраструктури міст, спільнот, підприємств та ін. Питання гарантоздатності таких систем є надто актуальними для розробників. Створюються гарантоздатні рішення для інтелектуальних енергосистем і енергоефективних проєктів [9], інтелектуальних транспортних систем і мереж, «розумних» міст, екологічного моніторингу та підтримки прийняття рішень [7].

2.12. Кіберфізичні системи

Кіберфізичні системи знаходяться на перетині декількох сфер і в залежності від реалізації здатні впливати на різні аспекти нашого життя. До кіберфізичних систем можна віднести «розумні» мережі електропостачання, системи управління «розумним» транспортом, автоматизовані системи управління у виробництві і сільському господарстві, аерокосмічні системи, а також медичне обладнання. Важливим аспектом у роботі надійних кіберфізичних систем є достовірність даних. Найбільша увага в цій сфері приділяється гарантоздатності кіберфізичних систем охорони здоров'я, кібербезпеки медичних пристроїв і систем охорони здоров'я [7].

3. Висновки

Тема гарантоздатності найбільш актуальна у сфері розвитку інтелектуальних технологій і систем із використанням штучного інтелекту і нейронних мереж. Найбільш дослідженими є такі питання: безпека транспортних систем, моделювання руху транспорту і оцінка ризиків; безпека прийняття рішень в автоматизованих транспортних засобах і з використанням нейронних мереж; допоміжні системи для запобігання небажаних подій на залізничному транспорті; системи зв'язку для інфраструктури безпеки польотів і організація повітряного руху.

Активно проводяться дослідження у сфері «розумного» міста, а саме у питаннях інтеграції фізичних, цифрових і людських систем у штучне середовище заради сталого, благополучного і всебічного майбутнього. Нині концепція «розумного» міста включає в себе гарантоздатні рішення для інтелектуальних і комунікаційних мереж, систем накопичення енергії, аналізів і прогнозування електроспоживання.

З’явилися міжнародні та галузеві стандарти, узгоджені з концепцією гарантоздатності. Вони присвячені гарантоздатності КС, мереж і програмного забезпечення. Але аналіз концепції і сучасного стану теорії ГКС свідчить про те, що теорія не в повній мірі враховує особливості нового класу інформаційно-обчислювальних систем, заснованих на принципах сервіс-орієнтованої архітектури. В межах сучасних тенденцій рішення проблем створення ГКС зводиться до необхідності застосування комплексного підходу до їх вирішення на платформі нової відмовостійкої структури.

СПИСОК ДЖЕРЕЛ

1. Zamojski W., Mazurkiewicz J., Sugier **J.,** Walkowiak T., Kacprzyk J. Engineering in Dependability of Computer Systems and Networks. *Proc. of the Fourteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX* (Brunów, Poland July 1–5, 2019). Brunów, Poland, 2019. URL: https://www.springer.com/gp/book/9783030195007.
2. DSN 2020 Rising Star in Dependability Award: Karthik Pattabiraman. *Electrical and Computer Engineering UBC*. URL: https://www.ece.ubc.ca/news/202006/karthik-pattabiraman-wins-award-dependable-computing .
3. The 6th IEEE International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (Dependsys, 14–16 December, 2020). Fiji, 2020. URL: https://tc.computer.org/tccld/2020/08/20/6th-ieee-international-conference-dependability-snsor-cloud-big-data-systems-applications-dependsys-2020-14-16-december-2020-fiji/ .
4. Theory and Applications of Dependable Computer Systems, Proceedings of the Fifteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX (Brunów, Poland, June 29 – July 3, 2020). Brunów, Poland. URL: https://www.springer.com/gp/book/9783030482558.
5. DSN 2020 The William C. Carter PhD Dissertation Award in Dependability: Bo Fang. *Electrical and Computer Engineering UBC*. URL: https://www.ece.ubc.ca/news/202005/bo-fang-wins-award-dependable-computing.
6. Dependability in Sensor, Cloud and Big Data Systems and Applications, *5th International Conference, DependSy*s (Guangzhou, China, November 12–15, 2019). URL: https://www.springer.com/gp/book/9789811513039.
7. DESSERT'2020 11th International IEEE Conference Dependable Systems, Services and Technologies (Ukraine, Kyiv, May 14–18, 2020). Kyiv, 2020. URL: www.dessert.ieee.org.ua/dessert-2020.
8. The 50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2020) (Valencia, Spain, Jun 29, 2020 – Jul 2, 2020). Valencia, Spain, 2020. URL: https://sn.committees.comsoc.org/call-for-papers/the-50th-ieee-ifip-international-conference-on-dependable-systems-and-networks-dsn-2020.
9. The 2021 IEEE Conference on Dependable and Secure Computing Aizuwakamatsu (Fukushima, Japan, 30 Jan – 2 Feb., 2021). Fukushima, Japan, 2021. URL: http://nsclab.org/dsc2021.
10. 17th European Dependable Computing Conference (Munich, Germany, 13–16 September, 2021). Munich, Germany, 2021. URL: http://edcc.dependability.org/keynotes.html.
11. Ateniese G., Di Pietro R., Mancini L.V., Tsudik G. DSN 2020 Laprie Award Winner. Scalable and Efficient Provable Data Possession. *Proc. 4th Intl. Conf. on Security and Privacy in Communication Networks (SecureComm)* (Istanbul, Turkey, September, 2008). Istanbul, Turkey, 2008. Art. N 9. P. 1–10. URL: https://doi.org/10.1145/1460877.1460889.

Стаття надійшла до редакції 20.01.2021