НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МАТЕМАТИЧНИХ МАШИН І СИСТЕМ

МУХА АРТЕМ АНДРІЙОВИЧ

УДК 004.05

МОДЕЛІ, МЕТОДИ ТА ТЕХНІЧНІ ЗАСОБИ СТВОРЕННЯ ГАРАНТОЗДАТНИХ КЕРУЮЧИХ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ З ДВОКАНАЛЬНОЮ СТРУКТУРОЮ ОБРОБКИ ДАНИХ

05.13.06 - інформаційні технології

Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук

Київ – 2020

Дисертацією є рукопис
Робота виконана в Інституті проблем математичних машин і систем НАН України

Науковий керівник доктор технічних наук,
старший науковий співробітник
Федухін Олександр Вікторович,
Інститут проблем математичних машин і систем
НАН України,
завідувач лабораторії гарантоздатних комп'ютерних
систем для критичних технологій та інфраструктур

Офіційні опоненти: доктор технічних наук, професор
Романкевич Віталій Олексійович,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»,
завідувач кафедри системного програмування і спеціалізованих комп'ютерних систем

кандидат технічних наук
Бабешко Євген Васильович,
Національний аерокосмічний університет імені М.Є. Жуковського «Харківський авіаційний інститут»,
доцент кафедри комп'ютерних систем, мереж і кібербезпеки

Захист відбудеться "16" вересня 2020 р. о 16-00 на засіданні спеціалізованої вченої ради Д 26.204.01 в Інституті проблем математичних машин і систем НАН України за адресою: 03187, м. Київ-187, проспект Академіка Глушкова, 42.

З дисертацією можна ознайомитись у бібліотеці Інституту проблем математичних машин і систем НАН України за адресою: 03187, м. Київ-187, проспект Академіка Глушкова, 42.

Автореферат розісланий "16 " серпня 2020 р.

Вчений секретар
спеціалізованої вченої ради М.Г. Ієвлєв

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У зв’язку зі стрімким розвитком інформаційних технологій (ІТ) сучасне суспільство стає все більш залежним від якості послуг, що надаються. Важливою складовою такої залежності є рівень надійності і безпеки сервісів і систем, що базуються на ІТ. Це обумовлено тим, що недостатній рівень надійності та безпеки комп'ютерних систем (КС) як засобів, що реалізують ІТ, призводить або до матеріальних втрат і зниження конкурентоспроможності, або до більш серйозних наслідків, пов'язаних із загибеллю людей, техногенними та екологічними катастрофами при експлуатації КС у системах критичного призначення. На сьогоднішній день важко знайти область людської діяльності, де б не були потрібні КС високої надійності і безпеки. Це, в першу чергу, енергетика, транспорт, космос, військово-промисловий комплекс, медицина, фінанси і т.д.

Узагальненою властивістю таких систем є властивість гарантоздатності (dependability), базовою платформою якої є відмовостійкість, а атрибутами – безвідмовність, готовність, обслуговуваність, живучість, достовірність, безпека, конфіденційність і цілісність. Іншими словами, гарантоздатні системи – це відмовостійкі, високонадійні, безпечні та живучі системи з гарантовано достовірними обчисленнями. Складність і масштабність вирішення проблеми забезпечення гарантоздатності КС ставить принципово нові завдання з організації істотно більш ефективних відмовостійких архітектурних рішень, реалізації нових підходів щодо забезпечення високої надійності, живучості та безпеки, розробки нових методів і засобів прогнозування, діагностики та самоконтролю програмних і апаратних засобів, розвитку комплексних технологій автоматизації проектування, статистичного та імітаційного моделювання.

На цей час над вирішенням проблем розробки гарантоздатних інформаційно-керуючих КС спеціального та критичного призначення працює значна кількість учених, цьому питанню присвячено багато наукових робіт, проводяться профільні наукові конференції, фінансуються державою відповідні дослідження науково-дослідних, навчальних університетів та інститутів.

Серед дослідників в галузі гарантоздатності, відмовостійкості, надійності, живучості та безпеки необхідно відзначити великий внесок зарубіжних та вітчизняних вчених: A. Avizienis, B. Randell, J.-C. Laprie, д.т.н., професора В.С. Харченко (НАКУ ім. М.Є. Жуковського «ХАІ»), д.т.н., професорів В.О. Романкевича і Ю.Г. Савченко (НТУ України «КПІ ім. І. Сікорського»), д.т.н., професора О.В. Дрозда (ОНПУ України), д.т.н., професора В.О. Романова (ІК ім. акад. В.М. Глушкова НАН України), д.т.н, професора О.Г. Додонова (ІПРІ НАН України), д.т.н., професора О.Д. Азарова (ВНТУ України) та д.т.н. В.П. Стрельнікова і О.В. Федухіна (ІПММС НАН України).

У ряді промислово розвинених країн світу вимоги до гарантоздатності КС, що керують і забезпечують життєдіяльністю суспільства, стають національними пріоритетами розвитку ІТ найвищого рівня, регулярно оновлюються відповідні стандарти у сфері гарантоздатності, надійності та безпеки.

У роботі розглянуто створення деяких базових методів інжинірингу КС спеціального призначення, основною галуззю застосування яких є управління об’єктами критичних інфраструктур і технологій, а саме, військова сфера, транспорт, енергетика та інші.

Зв’язок роботи з науковими програмами, планами, темами

Результати дисертаційної роботи були отримані в ІПММС НАН України в межах держбюджетних науково-дослідних тем: “Розробка теоретичних засад створення та дослідження живучих гарантоздатних систем керування, на основі ймовірнісно-фізичного підходу, шифр “Живучість”, номер державної реєстрації теми 0110 U001005 (2010-2014 рр.); «Розробка теоретичних основ і прикладних методів створення комп’ютерних засобів і систем із гарантованою надійністю і безпекою для критичних технологій і інфраструктур», шифр “Безпека”, номер державної реєстрації теми 0115U000035 (2015-2019 рр.).

Дослідження виконувались і виконуються сьогодні відповідно до Пріоритетного напряму розвитку науки і техніки в Україні «Інформаційні та комунікаційні технології, включаючи розвиток нових апаратних рішень для перспективних засобів обчислювальної техніки, інформаційних та комунікаційних технологій, розробку базових компонент та комплексів керування складними системами», «Розробка і дослідження моделей і методів оцінки якості і підвищення надійності, функціональної безпеки і живучості керуючих систем, а також інформаційних технологій для створення гарантоздатних автоматизованих систем обробки інформації та управління критичного застосування» паспорта спеціальності 05.13.06 – інформаційні технології.

Мета і завдання дослідження. Метою досліджень є розробка моделей, методів і технічних засобів для проектування ефективних гарантоздатних КС із мінімальною надлишковістю на основі двоканальної обробки даних щодо використання у критичних інфраструктурах і технологіях.

Для досягнення поставленої мети в дисертаційній роботі передбачається вирішення таких завдань:

1. Удосконалення атрибутивної моделі гарантоздатності КС, на основі якої стане можливим проведення її параметризації (кількісної оцінки атрибутів і метрик).
2. Розробка методів обчислення кількісної оцінки загального рівня гарантоздатності КС та проведення порівняльної оцінки КС за загальним рівнем гарантоздатності.
3. Здійснення аналізу і класифікації за властивостями надійності, безпеки, ефективності використання відмовобезпечних структур КС із двоканальною обробкою даних. На основі отриманих результатів проведення структурного синтезу і аналізу нового класу двоканальних КС із квазімістковою структурою (КМС) та реконфірацією у процесі функціонування.
4. Проведення аналізу ефективності методів інфраструктурного резервування і оптимізації на основі КМС як напряму забезпечення високого рівня функціональної безпеки і живучості.
5. Розробка гарантоздатної мікропроцесорної контрольно-інформаційної системи для залізничних переїздів.

Об'єктом дослідження є процеси інжинірингу (розробки, аналізу та порівняння) сучасних керуючих комп'ютерних систем критичного призначення, що забезпечують високий рівень гарантоздатності.

Предметом дослідження є методи і засоби забезпечення високого рівня гарантоздатності керуючих КС критичного призначення із двоканальною обробкою даних.

Методи дослідження. У відповідності з метою та зазначеними завданнями використовувалися основні положення таких теорій, як гарантоздатності комп'ютерних систем, надійності цифрових схем і систем, теорія ймовірностей і математичної статистики; методологія математичного та статистичного моделювання, методи булевої алгебри та ін.

Перевірка правильності теоретичних пропозицій здійснюється методами аналітичних розрахунків, проведення комп'ютерних експериментів шляхом моделювання та порівнянням цих методів.

Наукова новизна отриманих результатів полягає в тому, що:

- вдосконалено АМГ КС та здійснено розгорнуту декомпозицію її понять на атрибути, метрики і критерії рівня реалізації, яка відрізняється від відомих включенням до її складу атрибуту достовірність, аналітичних оцінок кількісних метрик та критеріїв реалізації якісних метрик, що надає можливості дослідження й управління гарантоздатністю КС;

- вперше розроблено метод кількісного оцінювання рівня реалізації атрибутів, метрик та критеріїв рівня реалізації, що дозволяє здійснити параметризацію АМГ. Завдяки цьому розроблено скалярну математичну модель комплексного оцінювання загального рівня гарантоздатності КС та реалізовано процедуру порівняльної оцінки КС з боку досягнутого рівня гарантоздатності для різних варіантів їх виконання в період проектування. Такий метод, на відміну від відомих, дозволяє здійснювати аналітичне оцінювання рівня гарантоздатності та робити вибір варіантів реалізації гарантоздатної КС при її інжинірингу;

- вперше на основі аналізу та класифікації відмовобезпечних структур КС із двоканальною структурою обробки даних запропоновано новий клас двоканальної КС із квазімістковою структурою та можливістю реконфігурації при відмовах її складових частин, що дозволяє створювати відмовобезпечі і відмовостійкі КС підвищеної надійності, безпеки і живучості з мінімальною надмірністю технічних засобів. Завдяки аналітичним розрахункам та статистичному моделюванню надійності КМС, показано переваги запропонованої структури з боку надійності та достовірності від 10 до 30 % перед класичною дубльованою структурою;

- дістала подальшого розвитку стратегія відмовобезпеки як альтернатива дорогої стратегії повної відмовостійкості при проектуванні гарантоздатних КС за рахунок встановлення критеріїв небезпечних відмов та захисних станів, які використовуються при доказі безпеки КС і дозволяють створювати ефективні реалізації КС без втрати безпеки функціонування;

- набув подальшого розвитку метод інжинірингу безпечної КС із високим рівнем живучості на основі КМС кластерного типу, що дозволяє підвищити безпеку і живучість КС розподіленого типу з розвиненою топологією в декілька разів.

Практичне значення отриманих результатів. Отримані теоретичні результати досліджень і практично підтверджені прикладні методи побудови гарантоздатних комп'ютерних засобів і систем мають міжгалузеву направленість та можуть бути впроваджені при розробці й проектуванні конкурентоздатних вітчизняних керуючих КС із двоканальною структурою обробки даних щодо критичних технологій та інфраструктур.

Потенційний економічний ефект від впровадження результатів наукових досліджень полягає у зменшенні витрат на роботи спеціалістів по проведенню ремонтів та технічному обслуговуванню складових частин гарантоздатних систем завдяки введенню функцій відмовостійкості, самодіагностики і самовідновлення та ін. Також практичним чинником є скорочення збитків від простоїв із причини відмов обладнання за рахунок високої надійності і готовності систем.

У межах конкурсу науково-технічних проектів наукових установ НАН України в ІПММС НАН України було проведено структурний синтез, технічне проектування та виготовлення з використанням методів забезпечення гарантоздатності дослідного зразка «Контрольно-інформаційної системи для залізничних переїздів (КІСЗП) «Благовіст»». Система «Благовіст» забезпечує зменшення аварійних ситуацій на залізничних переїздах за рахунок повної інформованості водіїв автотранспорту про ситуацію на переїзді. Основною відмінністю інноваційної системи є надання водіям інформації про: наближення моменту закриття автоматичного шлагбауму (за наявності); зайнятість потягом ділянки наближення до переїзду; напрямок руху поїзду через переїзд; швидкість руху поїзду, що наближається; час, що залишився до проходження потягу по переїзду; вільність контрольної ділянки за переїздом; ситуація на переїзді у вигляді інформаційної стрічки, що біжить.

Розробка системи проводилася у співпраці з Департаментом автоматики, телемеханіки і зв'язку Укрзалізниці та Державним науково-дослідним центром залізничного транспорту України. Виконання іноваційного проекту було підтримано Національним транспортним університетом та департаментом ДАІ МВС України, які дали згоду на обладнання залізничних переїздів. Отримано дозвіл на встановлення дослідного зразка системи на магістральній ділянці у гірській місцевості залізних доріг Грузії

Особистий внесок здобувача. Особистий внесок полягає в розробці нових методів, алгоритмів і програм, що забезпечують розв'язання поставлених задач. Основні результати роботи одержані автором особисто.

У роботі [1] запропоновано для управління процесом розробки систем використовувати FMEA-аналіз. У роботі [2] запропоновано здійснювати дослідження алгоритмів функціонування відмовостійких систем засобами імітаційного моделювання в інструментальному середовищі Matlab Simulink. У роботі [3] описано вирішення задачі підвищення живучості систем протиаварійної автоматики, запропоновано принцип інфраструктурного резервування. У роботах [4, 5] виконано аналіз технічних засобів та рішень з точки зору забезпечення атрибутів гарантоздатності КІСЗП «Благовіст». У роботі [6] наводяться додаткові аспекти вирішення проблем забезпечення гарантоздатності в системах критичного призначення.

У публікаціях, написаних у співавторстві, здобувачеві належить: у роботі [7] запропонована ідея реалізації апаратно-керованого відновлення, блоку контролю, часткового блокування та маскування відмов на базі одного кристалу ПЛІС, що дозволяє реалізувати апаратну надлишковість і надає можливість ефективного використання відмовостійких квазімісткових структур. У роботі [8] здійснено аналіз резервування комбінаційних схем у вигляді цифрових блоків за топологією мажоритарного резервування з відновленням. У роботі [9] запропонована реалізація резервованої двоканальної системи з реконфігурацією та відновленням, яка далі згадується як квазімісткова, за допомогою мультиплексорів. У роботах [10, 11] виконано імітаційне моделювання квазімісткової системи. У роботах [12-14] запропоновані варіанти апаратної реалізації інноваційних гарантоздатних систем автоматичної переїзної сигналізації для залізничних переїздів, відпрацьовано відмовостійкий алгоритм роботи системи, розроблена імітаційна модель системи та з використанням методу кінцевих автоматів описана у вигляді діаграм станів, відпрацьовано алгоритм створення відмовостійких систем на базі пакета Matlab Simulink. У роботі [15] виконано аналіз логічної функції квазімісткової структури. У роботах [16, 17] запропоновано ділити метрики на дві групи, що мають виключно кількісні та якісні оцінки, проведено аналітичні розрахунки вагових коефіцієнтів метрик, запропоновано використання відносних значень різноманітних параметрів у відносних величинах, нормованих на їх граничні значення. У серії робіт [17-20, 27] було впроваджено нові технічні рішення та алгоритми, що застосовані при розробці гарантоздатних КІСЗП серії «Благовіст», запропоновано використання бездротової передачі даних у системі, алгоритм розрахунку швидкості потяга на базі двоканальних колійних датчиків підрахунку осей, проведено аналіз ряду натурних експериментів. У роботі [21] запропоновано інформаційний підхід щодо підвищення безпеки проїзду автотранспорту через залізничні переїзди. У роботах [22, 29] запропоновано алгоритм моделювання надійності та проведено статистичне моделювання засобами пакета RELIABmod. У роботах [23, 24] здійснено аналіз положень стратегій побудови гарантоздатних систем, а саме відмовобезпеки та відмовостійкості. У роботі [25] запропоновано використання імітаційного моделювання у доказі функціональної безпеки систем. У роботі [26] запропоновано новий підхід, пов'язаний з функцією DN-розподілу, що дозволяє отримати оцінку ймовірності тривалості безвідмовного функціонування об'єкта. У роботі [28] проведено розрахунки показників достовірності та ймовірності безвідмовної роботи різних надлишкових структур комп'ютерних систем. У роботах [29, 30] виконано аналітичний розрахунок надійності квазімісткової структури. У роботі [31] запропоновані приклади елементів гравітаційної автоматики з високим рівнем гарантування відключення при відмові та теоретичні основи їх використання, розглянуто приклад розробки живучої системи на основі квазімісткової структури. У роботі [32] проведено розрахунок функції середнього напрацювання на відмову відновлювального виробу у межах гіпотези про дифузійний закон розподілу (DN-розподіл).

Апробація результатів дисертації. Результати роботи доповідалися на науково-технічних семінарах «Надійність, якість, сертифікація засобів обчислювальної техніки та автоматизації» ІПММС НАН України, на науково–

практичних конференціях з міжнародною участю «Математичне та імітаційне моделювання систем. МОДС» (м. Київ, 2010 р.; м. Київ, 2013 р.; м. Київ, 2016 р.; м. Чернігів 2017 р.), IX International conference "Strategy of Quality in Indastry and Education" (Varna, Bulgary, 2013 р.), Міжнародній науково-практичній конференції «Актуальні питання розвитку технічних наук в умовах глобальної нестабільності» (м. Київ, 2013 р.), III Міжнародній конференції «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища» INUDECO (м. Славутич, 2018 р.).

Публікації. За темою дисертації опубліковано 32 наукові роботи, у тому числі 26 статей у наукових журналах, які включені до різних міжнародних наукометричних баз даних, із них 20 статей опубліковано в наукових журналах, які входять також до переліку ДАК України як фахові, з них 4 одноосібні, та 6 тез доповідей на міжнародних конференціях.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, чотирьох розділів, висновків, списку використаних джерел із 123 найменувань та п'яти додатків. Загальний обсяг дисертаційної роботи становить 235 сторінок, із яких 168 сторінок основного тексту та 54 сторінки додатків, 36 рисунків, 22 таблиці, що дорівнює 4,75 облікових аркуша.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується актуальність проблеми, формулюються мета і задачі дослідження, наукова новизна та практична цінність одержаних результатів, показано зв'язок поставлених задач із науковими дослідженнями.

Перший розділ дисертації містить у собі розгорнутий аналіз основних характеристик (атрибутів) гарантоздатних КС, а саме: безвідмовність, готовність, обслуговуваність, живучість, достовірність, функціональну безпеку, конфіденційність, цілісність з детальним описом їх метрик та методів їх кількісної оцінки (табл. 1).

Як базову модель безвідмовності для надлишкових структур пропонується використовувати феноменологічну модель ймовірності безвідмовної роботи виду ${}^{f}_{c}R^{q}_{s} = c^{s}(1-{}^{f}F^{q}_{s})$, де ${}^{f}F^{q}_{s}$ – функція ймовірності відмови з урахуванням параметрів f, q та s, s - кількість резервів, спочатку доступних для підключення, q - кількість модулів, що забезпечують задану продуктивність системи (характеристика актуальна для систем, продуктивність яких залежить від кількості одночасно працюючих ресурсів), c - ступінь компенсації наслідків відмови (умовна ймовірність того, що при виникненні відмови у працюючій системі остання здатна відновити інформацію і продовжити її обробку без довготривалої втрати даних), f - здатність модуля допускати f одиничних відмов до того, як він стане непрацездатним.

Приймаючи гіпотезу про DN - розподіл напрацювання до відмови елементів, модулів і системи в цілому, ймовірність відмови будемо обчислювати таким чином:

${}^{f}F_{s}^{q} = DN(x; v, f, q, s)$, де v – коефіцієнт варіації напрацювання до відмови; x – відносне напрацювання ($x = \frac{t}{T_1}$), t – час експлуатації (напрацювання), T_1 – середнє напрацювання (до відмови). Функція ймовірності відмови для DN-розподілу має такий вид: $DN(x;v) = \Phi\left(\frac{x-1}{v\sqrt{x}}\right) + \exp\left(2v^{-2}\right)\Phi\left(-\frac{x+1}{v\sqrt{x}}\right)$, де $\Phi(*)$ – функція нормованого нормального розподілу.

Таблиця 1 – Атрибути та метрики гарантоздатної КС

№	Найменування атрибута	Метрики
1	Безвідмовність	Ймовірність безвідмовної роботи відмовостійкої системи ${}^{f}_{c}R_{s}^{q}$
		Ймовірність безвідмовної роботи ненадлишкового каналу системи $R_к(t)$
		Коефіцієнт відмовостійкості $K_{ВС}$
2	Готовність	Коефіцієнт готовності $K_г(t)$
		Коефіцієнт оперативної готовності $K_{ог}(t)$
3	Обслуговуваність	Тривалість технічного обслуговування, $T_{то}$
		Середній час відновлення, $T_в$
		Коефіцієнт технічного використання $K_{тв}$
4	Живучість	Коефіцієнт живучості $G(q^i)$
		Коефіцієнт деградації $D(q^i)$
		Виживаність системи $R(n)$
5	Достовірність	Ймовірність отримання достовірного результату D
6	Функціональна безпека	Ймовірність безпечної роботи $R_{БР}(t)$
		Ймовірність небезпечної відмови $Q_{НВ}(t)$
		Середнє напрацювання на небезпечну відмову $T_{НВср}$
		Коефіцієнт безпеки $K_Б$
7	Конфіденційність	Ймовірність порушень $P_П$
		Рівень доступності $L_Д$
		Рівень секретності $L_С$
8	Цілісність	Рівень цілісності обчислювальних ресурсів $L_{ОР}$
		Рівень цілісності програмних ресурсів $L_{ПР}$
		Рівень цілісності інформації $L_{ЦІ}$

На основі моделі ${}_c^f R_s^q$ пропонується феноменологічна модель достовірності функціонування виду $D = [d_M \cdot {}_c^f R_s^q] \cdot k$, де d_M – достовірність обчислень модуля, ${}_c^f R_s^q$ – ймовірність безвідмовної роботи системи за час t, k – коефіцієнт, що враховує кратність порівняння інформації між каналами в процесі функціонування системи або поріг порівняння послідовно включеного порівняльного пристрою.

Введено такі визначення.

Визначення 1. Атрибутивна модель гарантоздатності КС (АМГКС) **(**Attributive model dependability of computer systems, AMDCS) – модель гарантоздатності КС, яка повністю описує комплексну властивість КС за допомогою атрибутів і метрик.

Визначення 2. Метрика гарантоздатної КС – міра, що дозволяє отримати чисельне значення деякої властивості гарантоздатної КС.

Атрибутивну модель довільної ГКС позначимо у вигляді досягнутого рівня гарантоздатності G_{AM}, що складається з оцінок атрибутів A_i, $A_i \in G_{AM}$, $i = 1,...,n$. У свою чергу, оцінки метрик i-го атрибута складають його оцінку $M_{ij} \in A_i$, $j = 1,...,m$.

Визначення комплексу метрик атрибутів гарантоздатності дозволило вирішити задачу формалізації узагальненої (скалярної) оцінки досягнутого рівня гарантоздатності КС, що розробляється. Як математичну модель пропонується використовувати функціонал G_{AM}, складовими якого є нормовані значення кількісних оцінок рівнів реалізації атрибутів із метрик з відповідними ваговими коефіцієнтами: $G_{AM} = \sum_{i=1}^{n} B_i A_i$, де n - кількість атрибутів, B_i – коефіцієнт впливу i-го атрибута, A_i – кількісна оцінка рівня виконання i-го атрибута у відносних величинах: $A_i = \sum_{j=1}^{m_i} \beta_{ij} M_{ij}$, де m_i – кількість метрик i-го атрибута, β_{ij} – вага j-ї метрики i-го атрибута, M_{ij} – кількісна оцінка рівня виконання j-ї метрики i-го атрибута у відносних величинах. Кількісні оцінки рівня виконання метрики представляють собою відносні величини, нормовані на нормативні або граничні значення або отримані експертним методом. У результаті підстановки отримаємо скалярну математичну модель рівня гарантоздатності КС: $G_{AM} = \sum_{i=1}^{n} B_i \sum_{j=1}^{m_i} \beta_{ij} M_{ij}$.

Величини вагових коефіцієнтів B_i, β_{ij} залежать від особливостей застосування кожної конкретної системи і можуть бути обчислені експертним або аналітичним методом.

У дисертаційній роботі запропоновано експертний метод оцінювання вагових коефіцієнтів β_{ij} для випадку, коли значення метрик мають тільки якісні оцінки (наприклад, атрибути конфіденційність і цілісність). У цьому випадку використовуються складові критерії реалізації метрик та рівні їх виконання у діапазоні {0-1}.

У роботі також пропонуються два способи аналітичної оцінки ваг метрик. У зв'язку з тим, що створення ГКС є дуже витратним проектом, то, беручи до уваги специфіку функціонування КС, немає сенсу реалізовувати кожен атрибут і кожну метрику з однаковим, максимально високим рівнем. Логічно припустити, що найбільш важливу метрику деякого атрибута слід реалізовувати з найбільшим рівнем. Наступним припущенням є те, що найбільш важлива метрика, яка має найвищу реалізацію, повинна мати найвищу вагу. На цій основі розроблені два аналітичних методи оцінки ваг метрик в АМГКС.

Наприклад, якщо система описується кінцевим числом атрибутів і деякий її атрибут описується трьома метриками з оцінками M_1, M_2, M_3, то вирази для розрахунку вагових коефіцієнтів $\beta_i (i = 1,2,3)$ мають такий вигляд:

$$\beta_1 = \frac{(M_1 + M_2)(M_1 + M_3)}{(M_1 + M_2)(M_1 + M_3) + (M_2 + M_1)(M_2 + M_3) + (M_3 + M_1)(M_3 + M_2)} = \frac{(M_1 + M_2)(M_1 + M_3)}{S_Z},$$

де S_Z – позначення знаменника виразу з лівої частини ланцюжка,

$\beta_2 = \frac{(M_2 + M_1)(M_2 + M_3)}{S_Z}; \beta_3 = \frac{(M_3 + M_1)(M_3 + M_2)}{S_Z}$. Причому $\sum_{i=1}^{3} \beta_i = 1$. Другий метод передбачає ранжування метрик у такий спосіб: $M_1 \geq M_2 \geq M_3$. Вирази для розрахунку вагових коефіцієнтів β_i будуть мати такий вигляд: $\beta_1 = \frac{2 - a - c}{3}$, $\beta_2 = \frac{a + 1 - c}{3}$, $\beta_3 = \frac{b + c}{3}$, де $a = \frac{1}{1 + M_1/M_2}$, $b = \frac{1}{1 + M_1/M_3}$, $c = \frac{1}{1 + M_2/M_3}$. Обидва методи дають збіжність результатів обчислень і можуть використовуватися рівноправно.

Для порівняльного оцінювання двох КС з боку рівня гарантоздатності сформульована така постановка завдання. Нехай є дві системи S_1 та S_2 з описаним вище набором атрибутів гарантоздатності. При цьому якісні метрики систем S_1 та S_2 збігаються кількістю критеріїв виконання, а кількісні – описуються однаковими аналітичними виразами f_{ij1} та f_{ij2}, що являють собою результати підстановок чисельних значень параметрів, відповідно, в системі S_1 та S_2. Ставиться завдання вибору системи з найвищим рівнем гарантоздатності (РГС). Позначимо співвідношення $\frac{f_{ij1}}{f_{ij2}}$ як Q_{ij}, де i – позначення атрибута, j – позначення метрики. У випадку кількісних атрибутів і метрик $Q_{ср.\text{і}} = \sum_{j=1}^{n_{ij}} Q_{ij} \cdot b_{ij}$ та $Q_{ср.кіл.} = \sum_{i=1}^{6} Q_{ср.i} \cdot B_i$,

де $\sum_{i=1}^{6} B_i = 1$ за всіма кількісними атрибутами для значень $B_i\,(i = 1,..6)$.

Кожній якісній метриці відповідає набір критеріїв оцінки, кількість яких дорівнює k_{ij}. Рівень виконання критерію оцінки визначається величиною U_l (або K_l) $(l = 1,\ldots,k_{ij})$, яка знаходиться в діапазоні значень {0-1}. Кількісною оцінкою якісної метрики є усереднена оцінка рівнів виконання її критеріїв, наприклад, $L_{ij} = \frac{\sum_{l=1}^{k_{ij}} U_l}{k_{ij}}$, де i – номер якісного атрибута, j – номер якісної метрики. У цьому випадку $Q_{ср.i} = \sum_{i=1}^{2} \frac{L_{j1}}{L_{j2}} \cdot b_{ij}$ за всіма якісними метриками двох якісних атрибутів та $Q_{ср.як.} = \sum_{i=1}^{2} Q_{ср.i} \cdot B_i$ за всіма якісними атрибутами для значень $B_i\,(i = 1,2)$. Отримані величини $Q_{ср.кіл.}$ та $Q_{ср.як.}$ служать для порівняння систем S_1 та S_2 за сукупністю оцінок, відповідно, кількісних і якісних атрибутів. Сума цих величин $R = Q_{ср.кіл.} + \mathrm{Q}_{\text{ср.як.}}$ дозволяє зробити висновок про перевагу тієї чи іншої системи з точки зору гарантоздатності.

Нагадаємо, що під час розгляду співвідношення чисельних значень показників чисельник співвідношення відповідає системі S_1, його знаменник – системі S_2. Якщо $\mathrm{R} \geq 1$, слід віддати перевагу системі S_1, в іншому випадку – системі S_2. При прийнятті рішення про перевагу тієї чи іншої системи необхідно мати на увазі, що для одних метрик зростання їх показника призводить до збільшення рівня РГС, а для інших метрик - до зменшення РГС, тому вклади цих метрик беруться зі знаком «-».

Другий розділ дисертації присвячений аналізу концепцій створення відмовостійких та відмовобезпечних систем. Вводиться твердження, що коли існує безпечна можливість призупинення надання системою послуг або надання її не в повному обсязі, доцільною є заміна повної відмовостійкості на часткову відмовостійкість з метою зменшення затрат на розробку та реалізацію проекту. Таку часткову відмовостійкість пропонується означити як відмовобезпеку.

Визначення 3. Відмовобезпека – властивість технічної системи при відмові її деяких частин переходити в режим роботи (безпечний стан, Safe state), що не представляє небезпеки для людей, навколишнього середовища або матеріальних цінностей.

Використання підходу, при якому стратегія повної відмовостійкості замінюється стратегією відмовобезпеки, дозволяє будувати економічно ефективні ГКС з меншими технічними витратами. Такі системи доцільно доповнювати попереджувальним і поточним технічним обслуговуванням з метою скорочення часу відновлення.

У розділі також проводиться детальна класифікація відмовобезпечних дубльованих структур КС. Завдяки аналізу різного типу структур, стало можливим

на базі дубльованої структури синтезувати систему підвищеної експлуатаційної готовності, а саме квазімісткову структуру з реконфігурацією (КМС).

Нова структура будується за принципом декомпозиції (дихотомії - ділення навпіл) блоків дубльованої структури, що складається із двох ЕОМ. КМС завжди залишається готовою до роботи при будь-яких подіях – відмовах або збоях у роботі складових частин. Якщо ЕОМ дубльованої структури розбивається на умовно рівнонадійні функційні субблоки (ФСБ) (наприклад, ЕОМ1.1 і ЕОМ1.2, ЕОМ2.1 і ЕОМ2.2), то середнє напрацювання до відмови такого ФСБ може бути орієнтовно оцінено таким чином: $T_{in}^{EOM} = \sqrt{n} \cdot T_{EOM}$. Висока експлуатаційна готовність досягається за рахунок організації двоканальної КМС із рівнонадійних дубльованих вузлів, що мають перехресні зв'язки між ними за допомогою схем реконфігурації (СР) зі змінною логічною функцією І/АБО (рис.1).

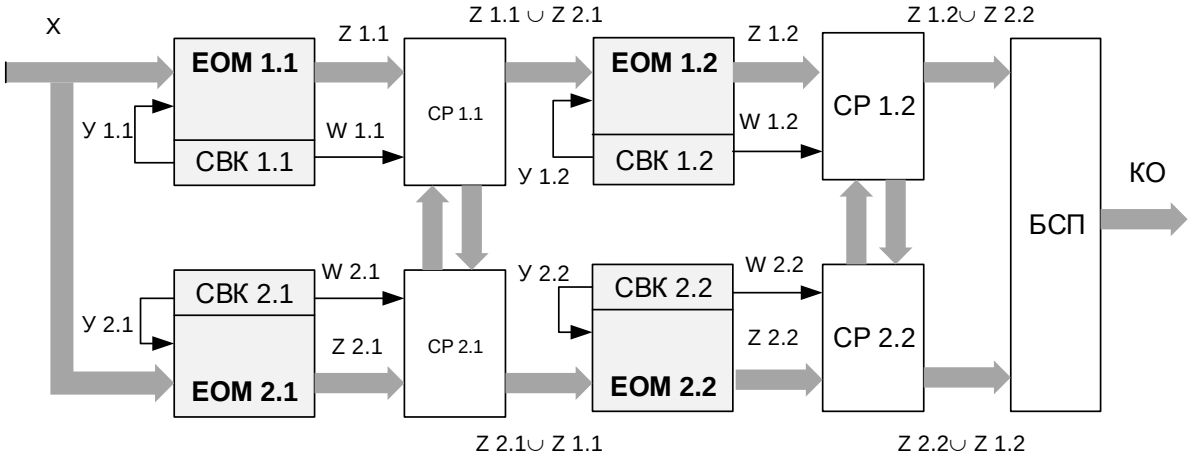

Рисунок 1 – Двовузлова КМС

Кожен ФСБ має схему внутрішнього контролю (СВК), вихід якої керує роботою СР, змінюючи її логічну функцію. Функціонування каналів КМС на виході також контролюється безпечною схемою порівняння (БСП) з логічною функцією І/АБО, яка здатна передавати керуючі впливи на керований об'єкт (КО) навіть у тому випадку, коли в результаті відмов ФСБ КМС перетворюється із двоканальної в одноканальну.

Логічна функція справної двовузлової КМС виглядає таким чином: $F_{КМС} = z_1 \cup z_2 \cup z_1 \cdot z_2 \cup z_1 \cdot z_{1.2} \cdot z_{2.1} \cup z_1 \cdot z_{1.1} \cdot z_{2.2} \cup z_2 \cdot z_{1.1} \cdot z_{2.2} \cup z_2 \cdot z_{1.2} \cdot z_{2.1} \cup z_{1.1} \cdot z_{2.2} \cup z_{1.2} \cdot z_{2.1}$, де $z_1 = z_{1.1} \cdot z_{1.2}$; $z_2 = z_{2.1} \cdot z_{2.2}$. Неважко бачити, що КМС характеризується більш високим рівнем відмовостійкості і, як наслідок, експлуатаційної готовності, тому що має значно більшу кількість працездатних станів, ніж проста дубльована структура. Наявність працездатних станів на імпліканті $z_1 \cup z_2$ свідчить про те, що КМС здатна до автоматичної реконфігурації в одноканальну структуру без додаткового втручання і зміни функції БСП. КМС залишається працездатною при виході з ладу одного з чотирьох ФСБ або двох, підключених послідовно або перехресно. Тільки одночасний вихід із ладу ФСБ в одному вузлі КМС призводить до втрати її працездатності та переходу в безпечний стан.

Перевагою КМС є те, що з ростом кількості вузлів зростає надійність системи, зменшується складність ФСБ, з яких складається вузол, що спрощує програмну І/АБО технічну реалізацію СВК, підвищує точність контролю і діагностики несправностей структури, що, як наслідок, призводить до зменшення часу відновлення та додаткового зростання показників надійності відновлювальної квазімісткової структури в цілому. Виявлений позитивний ефект від розбиття системи на рівнонадійні дубльовані вузли та використання реконфігурації структури в разі відмови ФСБ дозволяє більш ефективно здійснювати структурний синтез високонадійних відмовостійких і безпечних КС критичного призначення.

КМС є зручним вирішенням проблеми підвищення живучості КС, оскільки відомі в теорії живучості систем способи забезпечення даної властивості базуються на властивості відмовостійкості. КМС є пластичною структурою, дозволяє будувати типові кластери та використовувати методи інфраструктурного резервування й топологічної оптимізації з метою підвищення живучості.

Третій розділ присвячено дослідженню надійності КМС та порівнянню її кількісних показників з іншими надлишковими відмовостійкими структурами.

Дослідження надійності запропонованої КМС здійснювалось шляхом проведення розрахунків надійності такими способами: стандартизованим методом (СМ) із використанням формул для послідовно-паралельних структур із довідників по надійності, класичним методом (КМ) із використанням базових формул теорії ймовірностей, логіко-ймовірнісним методом (ЛЙМ) із використанням формул булевої алгебри, ймовірносно-фізичним методом (ЙФМ) із використанням *DN*-розподілу наробітку до відмови.

1. Порівняльна оцінка надійності КМС із класичною дубльованою структурою СМ продемонструвала виграш КМС у плані ймовірності безвідмовної роботи (при $R_{ФБ} = 0{,}9$) $R_{ДС} = 0{,}99$, двовузлова КМС $R_{КМС} = 0{,}996$, трихвузлова КМС $R_{КМС} = 0{,}997$ і т.д., тенденція зростання не визиває сумнівів.

2. Порівняльна оцінка надійності КМС (рис. 2а) із різними структурами змішаного дублювання (рис. 2б,в) та структурою з системним дублюванням (рис. 2г).

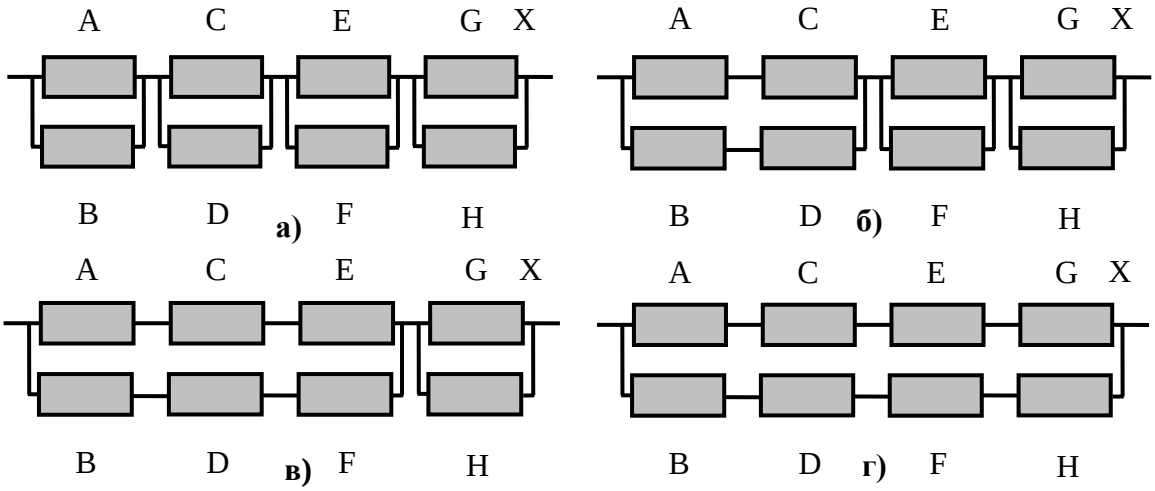

Рисунок 2 – Структурні схеми надійності досліджуваних систем

Обчислення ймовірностей безвідмовної роботи для функцій виходу X_1, X_2, X_3, X_4 (R_X) здійснювалось ЛЙМ та ЙФМ.

Результати розрахунків (для контрольного прикладу 2) (рис. 3) демонструють переваги КМС (функція виходу X_1) з боку R_X порівняно зі структурами зі змішаним дублюванням та дублюванням на рівні системи (найбільш програшний варіант із функцією виходу X_4 – дублювання на рівні системи).

3. Аналіз надійності КМС від кількості дубльованих вузлів ЙФМ показав (для контрольного прикладу 3), що з ростом кількості вузлів у КМС відзначається зростання $R_{КМС}$ структури: двовузлова КМС $R_{КМС}$=0,99558, тривузлова КМС $R_{КМС}$=0,99913, що в обох випадках перевищує ймовірность безвідмовної роботи класичної дубльованої структури $R_{ДС}$=0,97851.

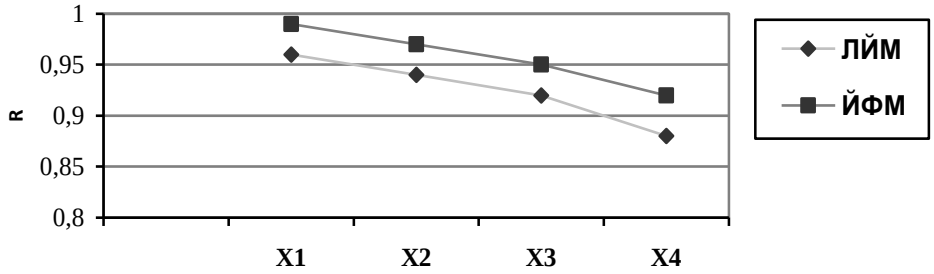

Рисунок 3 – Залежність ймовірності безвідмовної роботи структур від способу введення надлишковості

4. Аналіз надійності КМС від кількості дубльованих вузлів КМ показав (для контрольного прикладу 4), що з ростом кількості вузлів у КМС відзначається також зростання $R_{КМС}$ структури. Для цього були складені таблиці станів структур та отримано такі вирази і кількісні результати: дубльована структура при $R_{ФБ}$=0,7452, $R_{ДС} = 2R_{ФБ} - R^2_{ФБ}$=0,9351, двовузлова КМС при $R_{ФСБ}$=0,8875, $R_{КМС} = R^4_{ФСБ} + 4\cdot(1-R_{ФСБ})\cdot R^3{}_{ФСБ} + 4\cdot(1-R_{ФСБ})^2\cdot R^2{}_{ФСБ}$=0,9749, трихвузлова КМС $R_{ФСБ}$=0,9361, $R_{КМС} = R^6_{ФСБ} + 6\cdot(1-R_{ФСБ})\cdot R^5{}_{ФСБ} + 12\cdot(1-R_{ФСБ})^2\cdot R^4{}_{ФСБ} + 6\cdot(1-R_{ФСБ})^3\cdot R^3{}_{ФСБ} =$ = 0,9874.

Аналіз залежності $R_{КМС}$ КМС від кількості дубльованих вузлів КМ також показав, що з ростом кількості вузлів у КМС відзначається зростання $R_{КМС}$ структури та перевищення над $R_{ДС}$ класичної дубльованої структури. Також показано, що найбільший виграш за ймовірністю безвідмовної роботи КМС досягається при рівності надійності ФСБ і дубльованих вузлів.

5. Для статистичного моделювання надійності систем був використаний модернізований пакет програм RELIABmod v.2.0, який включає в себе чотири генератора випадкових чисел, розподілених відповідно до *DN*-розподілу, розподілу Вейбулла, логарифмічно-нормального і експоненційного розподілам, які параметризовані у двох параметрах: v – коефіцієнт варіації наробітку до відмови і

x – відносний наробіток, де $x = t_н / T_1$, T_1 – середній наробіток до відмови, $t_і$ – час експлуатації.

При моделюванні основним законом розподілу приймається дифузійний розподіл (*DN*-розподіл) наробітку до відмови (на відмову). Дослідження надійності проводилось як невідновлюваної КМС та КМС з відновленням. Графічна інтерпретація результатів статистичного моделювання невідновлюваної КМС наведена на рис. 4.

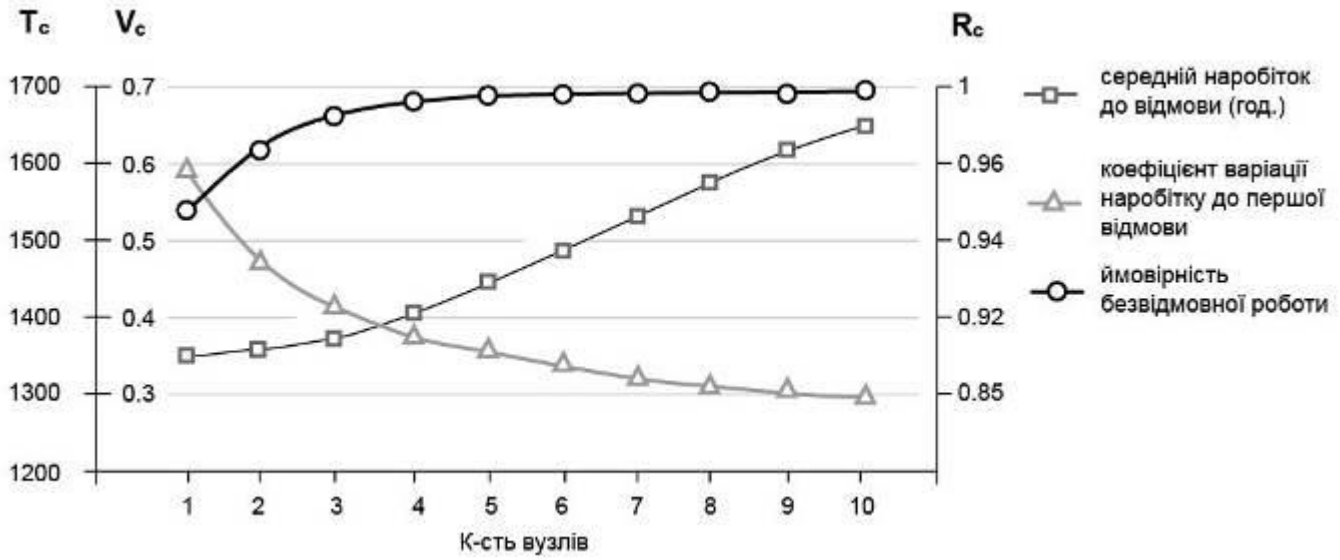

Рисунок 4 – Результати моделювання надійності невідновлювальної КМС

Графічна інтерпретація результатів статистичного моделювання КМС із відновленням наведена на рис. 5.

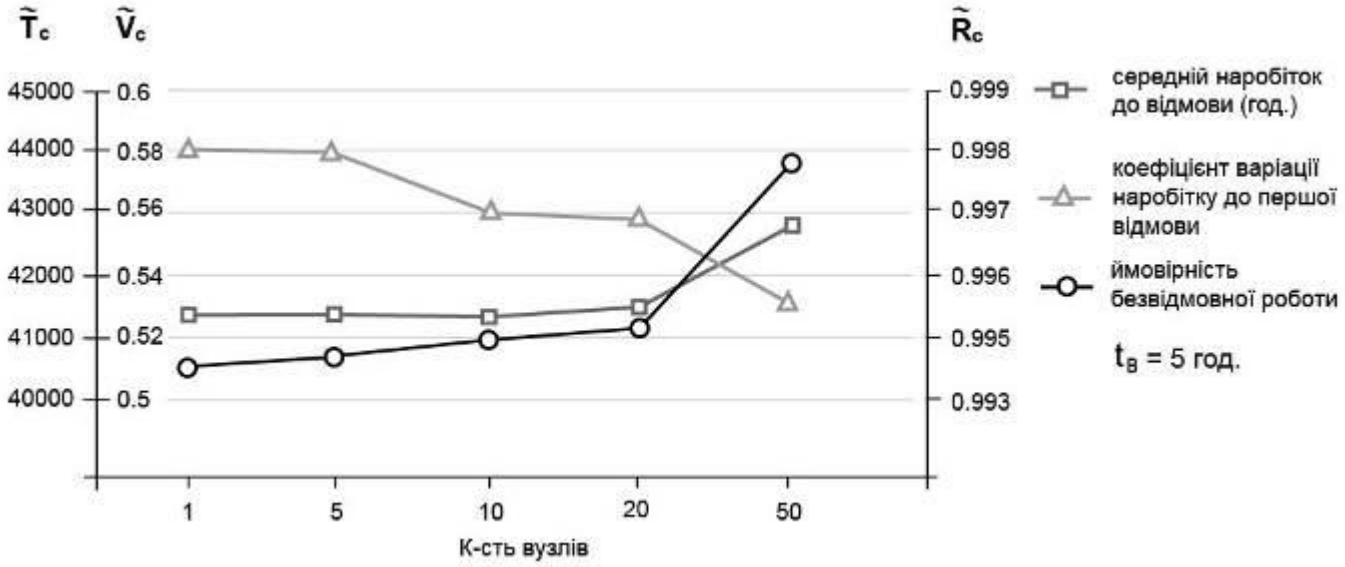

Рисунок 5 – Результати моделювання надійності відновлювальної КМС

При моделюванні відновлюваної КМС та з метою врахування впливу залежності середнього наробітку на відмову ФСБ від часу його віртуального функціонування пропонується феноменологічна модель виду

$$T_2\left(t_{\Sigma ФСБ}\right) = T_1\left\{0{,}05 + 0{,}95\exp\left[\frac{(t_{\Sigma ФСБ} - T_1)}{(5\cdot 10^5 - T_1)}\cdot\left(0{,}05 + \ln\left(T_1\right)^{-1}\right)\right]\right\},$$

де $t_{\Sigma ФСБ}$ – сумарне напрацювання ФСБ, T_1 – середній наробіток до відмови ФСБ, $T_2\left(t_{\Sigma ФСБ}\right)$ – середній наробіток на відмову ФСБ.

У цілому, основні, найбільш важливі, результати статистичного моделювання надійності двох КМС показали, що:

- для відновлюваних надлишкових структур, що складаються з малої кількості надлишкових блоків (у нашому випадку - дубльованих вузлів), такий показник, як середній наробіток до відмови (на відмову) є не інформативним, що підтверджує гіпотезу, висловлену А. Авіженісом;
- зі зростанням кількості вузлів надійність обох систем підвищується, що найбільш яскраво виражено при розподілі класичної дубльованої структури на рівнонадійні вузли відповідно до принципу дихотомії;
- зі зростанням кількості вузлів зменшується значення коефіцієнта варіації наробітку до відмови структури.

Аналізуючи останній результат моделювання, можна зробити дуже важливий висновок. Зі зростанням кількості вентилів у сучасних мікропроцесорах (Intel, AMD та інш.) з 1 до 10 млн їх надійність не зменшується, а розкид по надійності від зразка до зразка не виявляється за результатами тривалої експлуатації великої кількості складних мікропроцесорів ПЕОМ. Це можна обґрунтувати малим коефіцієнтом варіації напрацювання до відмови цих виробів. Причиною цього явища є всеосяжне поелементне і поблокове резервування з утворенням великої кількості дубльованих вузлів, що і підтверджено результатами моделювання надійності КМС.

Дослідження достовірності функціонування двовузлової КМС та її прототипів з використанням феноменологічної моделі $D = [d_M \cdot {}^f_c R^q_s]\cdot k$ показали (для контрольного прикладу 7) такі результати: КМС – $D_{КМС}$=0,995, дубльована структура з навантаженим резервом – $D_{ДС1}$=0,989, дубльована структура з ненавантаженим резервом – $D_{ДС2}$=0,940. Переваги КМС визначаються високими значеннями ймовірності безвідмовної роботи ${}^f_c R^q_s$=0.99992 та коефіцієнта k=0,99998, що враховує кратність порівняння інформації між каналами.

Четвертий розділ присвячено питанням впровадження запропонованого інформаційного підходу для забезпечення безпеки на залізничних переїздах, який полягає в підвищенні інформованості учасників руху про ймовірну небезпеку на шляху їх руху. Для реалізації запропонованого підходу розроблено КІСЗП «Благовіст». Робота системи (рис. 6, 7) заснована на фіксації місцезнаходження поїзда за допомогою підрахунку осей на лічильних пунктах (ЛП) із використанням

колійних датчиків (КД). Інформація з ЛП передається через радіоканал на центральний пункт (ЦП) і далі відображається на інформаційному табло (ІТ).

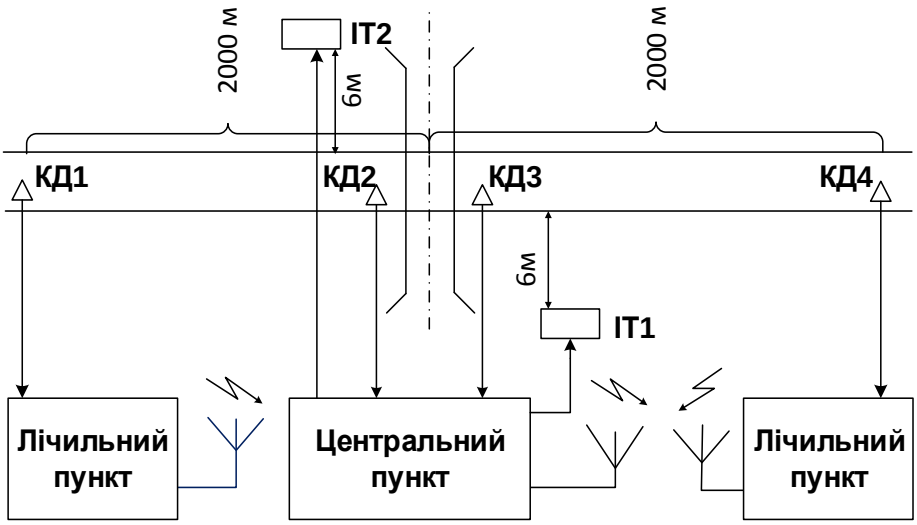

Рисунок 6 – Структурна схема КІСЗП «Благовіст»

Рисунок 7 – Загальний вид складових частин (зліва – лічильний пункт, праворуч – центральний пункт та інформаційне табло) системи КІСЗП «Благовіст»

КІСЗП «Благовіст» призначена для своєчасного інформування автотранспортних засобів (АТЗ), що перетинають переїзд, про основні показники руху поїзда, який слідує через зону переїзду. До таких показників відносяться напрямок руху, швидкість руху поїзда, а також відлік часу наближення поїзда до переїзду. Ці характеристики система відображає на інформаційному табло (рис. 8), а також виводить повідомлення шляхом рядка, що біжить, про наближення поїзда,

його фактичний рух через переїзд і про підвищену небезпеку в разі його затримки щодо прибуття або зупинки на ділянці наближення (рис. 9). Таким чином КІСЗП «Благовіст» підвищує інформованість водіїв АТЗ, які рухаються через переїзд, що в цілому забезпечує підвищення безпеки руху.

У розділі детально описано структурний синтез системи, її алгоритмічне та програмне забезпечення, описано елементну базу і методи забезпечення гарантоздатності КІСЗП «Благовіст».

Рисунок 8 – Інформаційне табло

Рисунок 9 – Приклад розміщення системи на переїзді

ВИСНОВКИ

У дисертаційній роботі викладено рішення низки важливих завдань у теорії і практиці забезпечення гарантоздатності КС із двоканальною структурою обробки даних, а саме:

1. Вдосконалено АМГ КС та здійснено розгорнуту декомпозицію її понять на атрибути, метрики і критерії рівня реалізації, яка відрізняється від відомих включеним до її складу атрибуту достовірность, аналітичних оцінок кількісних метрик та критеріїв реалізації якісних метрик, що надає можливості дослідження й управління гарантоздатністю КС;

2. Вперше розроблено метод кількісного оцінювання атрибутів, метрик та критеріїв рівня реалізації, що дозволяє здійснити параметризацію АМГ. Завдяки цьому, розроблено скалярну математичну модель комплексного оцінювання загального рівня гарантоздатності КС та реалізовано процедуру порівняльної оцінки КС для різних варіантів їх реалізації. Такий метод, на відміну від відомих, дозволяє здійснювати аналітичне оцінювання рівня гарантоздатності та робити вибір варіантів реалізації гарантоздатної КС при її інжинірингу

3. Вперше на основі аналізу та класифікації відмовобезпечних структур КС із двоканальною структурою обробки даних запропоновано новий клас двоканальної КС із квазімістковою структурою та можливістю реконфігурації при відмовах її

складових частин, що дозволяє створювати відмовобезпечі і відмовостійкі КС підвищеної надійності, безпеки і живучості з мінімальною надмірністю технічних засобів. Завдяки аналітичним розрахункам та статистичному моделюванню надійності КМС, показано переваги запропонованої структури з боку надійності та достовірності від 10 до 30 % перед класичною дубльованою структурою;

4. Дістала подальшого розвитку стратегія відмовобезпеки як альтернатива дорогої стратегії повної відмовостійкості при проектуванні гарантоздатних КС за рахунок встановлення критеріїв небезпечних відмов та захисних станів, які використовуються при доказі безпеки КС і дозволяють створювати ефективні реалізації КС без втрати безпеки функціонування;

5. Набув подальшого розвитку метод інжинірингу безпечних КС критичного призначення з високим рівнем живучості на основі КМС кластерного типу, що дозволяє підвищити безпеку і живучість КС розподіленого типу з розвиненою топологією в декілька разів на прикладі систем протиаварійної автоматики ГЕС.

6. Розроблено методи аналітичного розрахунку і алгоритми статистичного моделювання надійності КМС, показано їх переваги з боку надійності і достовірності функціонування перед класичною дубльованою структурою. Доведено, що КМС дозволяють підвищити безвідмовность і експлуатаційну готовність існуючих двоканальних резервованих систем обробки даних шляхом декомпозиції їх дубльованих каналів на рівнонадійні вузли, об'єднані схемами контролю та реконфігурації.

7. Доведено, що безвідмовність КМС зростає зі збільшенням кількості дубльованих вузлів, з яких складається структура. З ростом кількості вузлів КМС зменшується складність вузлів, що спрощує програмну та/або технічну реалізацію схем внутрішнього контролю, підвищується точність діагностики несправностей структури, що призводить до зменшення часу відновлення та зростання показників надійності відновлювальних квазімісткових структур у цілому.

8. Запропоновано інформаційний підхід до забезпечення безпеки руху залізничними переїздами, оснований на інформуванні учасників руху про швидкість руху поїзду, напрям руху і час, що залишився до моменту його проходження через переїзд. Для реалізації цього підходу та з метою впровадження отриманих у дисертації результатів на основі КМС розроблено експериментальний зразок Контрольно-інформаційної системи для залізничних переїздів «Благовіст», що не має аналогів в Україні. Значну перспективу та потенціал впровадження розробленої системи відзначено Департаментом ДАІ МВС України, Департаментом Автоматики, телемеханіки та зв’язку «Укрзалізниці», Національним транспортним університетом та спеціалістами залізничного транспорту Грузії, Вірменії та Польщі.

СПИСОК ОПУБЛИКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Муха Ар.А. Управление процессом разработки сложных технических систем и процессов, особенности применения FMEA-анализа. *Математичні машини і системи.* 2012. № 2. С. 168–176.
2. Муха Ар.А. Моделирование и разработка алгоритма работы АПС-РМПГ средствами пакета Matlab Similink+ Statefolw. *Молодий вчений*. 2014. № 5 (8). С. 10–14.
3. Муха Ар.А. К вопросу о живучести систем противоаварийной автоматики на гидроэлектрических станциях. *Молодий вчений.* 2018. № 3 (55). С. 399–405.
4. Муха Ар.А. Практические аспекты гарантоспособности контрольно-информационной системы для железнодорожных переездов «Благовест». *Математичні машини і системи*. 2018. № 4. С. 109–116.
5. Федухин А.В., Муха Ар.А., Муха А.А. ПЛИС-системы как способ повышения отказоустойчивости информационно-управляющих комплексов. *Математичні машини і системи.* 2010. № 1. С. 198–204.
6. Федухин А.В., Муха Ар.А. К вопросу об аппаратной реализации избыточных структур. Резервирование цифровых функциональных блоков. *Математичні машини і системи.* 2010. № 2. С. 138–143.
7. Федухин А.В., Муха Ар.А. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией. *Математичні машини і системи.* 2010. № 4. С. 156–159.
8. Федухин А.В., Муха Ар.А. Имитационное моделирование отказоустойчивой резервированной двухканальной системы в интегрированной инструментальной среде Matlab Simulink. *Математичні машини і системи.* 2011. № 2. С. 178–181.
9. Федухин А.В., Гладков А.В., Муха Ар.А. Новый подход к автоматизации переездов на железнодорожном транспорте. *Математичні машини і системи.* 2011. № 3. С. 135–141.
10. Муха Ар.А., Пасько В.П. Структурный синтез отказоустойчивых компьютерных систем. *Математичні машини і системи.* 2013. № 2. С. 202–206.
11. Федухин А.В., Ярошенко В.Н., Сухомлин А.И., Сеспедес Гарсия Н.В., Муха Ар.А. К вопросу о сравнительной оценке гарантоспособных систем. *Математичні машини і системи.* 2014. № 1. С. 185–194.
12. Федухин А.В., Муха Ар.А. Радиомикропроцессорные информационные системы для железнодорожных переездов серии «Благовест». *Математичні машини і системи.* 2014. № 2. С. 137–141.
13. Федухин А.В., Муха Ар.А. Беспроводные микропроцессорные системы для железнодорожных переездов серии «Благовест». *Молодий вчений.* 2014. № 11. С. 16–19.
14. Федухин А.В., Муха Ар.А. Беспроводные микропроцессорные системы для

железнодорожных переездов серии «Благовест». *Приборы и системы. Управление, контроль, диагностика.* 2015. № 2. С. 1–5.

15. Федухин А.В., Ярошенко В.Н., Муха Ар.А. К вопросу о взаимосвязи величин метрик и их весов. *Математичні машини і системи.* 2015. № 3. С. 191–200.

16. Федухин А.В., Муха Ар.А. Информационный подход к повышению безопасности движения по железнодорожным переездам. *Математичні машини і системи.* 2015. № 4. С. 145–151.

17. Федухин А.В., Пасько В.П., Муха Ар.А. К вопросу моделирования надежности, восстанавливаемой квазимостиковой структуры с учетом тренда параметров надежности составных частей. *Математичні машини і системи.* 2016. № 1. С. 158–167.

18. Федухин А.В., Муха Ар.А. Стратегия отказобезопасности как альтернатива полной отказоустойчивости при проектировании гарантоспособных компьютерных систем. Ч. 1. *Молодий вчений.* 2016. № 8 (35). С. 169–173.

19. Федухин А.В., Муха Ар.А. Стратегия отказобезопасности как альтернатива полной отказоустойчивости при проектировании гарантоспособных компьютерных систем. Ч. 2. *Молодий вчений*. 2016. № 10 (37). С. 23–27.

20. Федухин А.В., Муха Ар.А., Сеспедес Гарсия Н.В. Доказательство безопасности компьютерных систем. *Математичні машини і системи.* 2016. № 3. С. 93–101.

21. Федухин А.В., Ярошенко В.Н., Муха Ар.А. О важных следствиях из формулы DN-распределения наработки до отказа. *Молодий вчений.* 2016. №11 (38). С. 42–46.

22. Федухин А.В., Лутов С.Д., Сеспедес Гарсія Н.В., Ґедз О.В., Муха Ар.А. Система інформаційного сповіщення для залізничних переїздів «Благовіст». *Наука та Інновації.* 2017. № 13 (2). С. 29-35; Fedukhin A.V., Lutov S.D., Cespedes Garcia N.V., Gedz A.V., Mukha Ar. A. Blagovist: Information Warning System for Railroad Crossings. *Science and Innovation.* 2017. N 13 (2). P. 27–32.

23. Федухин А.В., Сеспедес Гарсия Н.В., Муха Ар.А. К вопросу о связи надежности и достоверности функционирования компьютерных систем. *Математичні машини і системи.* 2017. № 2. С. 145–155.

24. Федухин А.В., Сеспедес Гарсия Н.В., Муха Ар.А. К вопросу о надежности невосстанавливаемой системы с квазимостиковой структурой элементов. *Математичні машини і системи.* 2017. № 4. С. 160–168.

25. Федухин А.В., Муха Ар.А. Обеспечение живучести систем противоаварийной автоматики ГЭС. *Математичні машини і системи.* 2018. № 2. С. 169–194.

26. Федухин А.В., Стрельников В.П., Сеспедес Гарсия Н.В., Муха Ар.А. Приближенная оценка надежности восстанавливаемых изделий на этапе эскизного проектирования. *Математичні машини і системи.* 2018. № 3. С. 149–155.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

27. Mukha Ar.A. Develoment of safety FPGA-based systems for automatic crossing signals for lavel crossing. *Strategy of Quality in Indastry and Education:* IX international conference (Varna, Bulgary, 2013). Varna, 2013. Vol. 1. P. 345–346.
28. Муха Ар.А. Гарантоспособность компьютерных систем – способность предоставлять требуемые услуги с высоким уровнем доверия. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища INUDECO 18:* тези доп. III міжнар. конф. (м. Славутич, 25-27 квітня 2018 р.). Славутич, 2018. С. 258–265.
29. Федухин А.В., Муха Ар.А. Имитационное моделирование отказоустойчивой резервированной двухканальной системы в интегрированной инструментальной среде Matlab Simulink. *Математичне та імітаційне моделювання систем. МОДС -2010:* тези доп. 5-ої наук.-практ. конф. з міжнар. участю (м. Київ, 25-29 червня 2010 р.). Київ, 2010. С. 225–226.
30. Федухин А.В., Муха Ар.А. Структурный синтез отказоустойчивых компьютерных систем. *Актуальні питання розвитку технічних наук в умовах глобальної нестабільності:* тези доп. Міжнар. наук.-практ. конф. (м. Київ, 13-14 квітня 2013 р.). Київ, 2013. С. 61–64.
31. Ґедз О.В., Муха Ар.А. Моделирование работы и отладка алгоритма функционирования контрольно-информационной системы для железнодорожных переездов «Благовест». *Математичне та імітаційне моделювання систем. МОДС-2016:* тези доп. 11-ої наук.-практ. конф. з міжнар. участю (м. Київ, 25-29 червня 2016 р.). Київ, 2016. С. 246–247.
32. Федухин А.В., Муха Ар.А., Сеспедес Гарсия Н.В. Моделирование и аналитическая оценка надежности квазимостиковой структуры. *Математичне та імітаційне моделювання систем. МОДС-2017:* тези доп. Міжнар. наук.-практ. конф. (м. Чернігів, 25–29 червня 2017 р.). Чернігів, 2017. С. 282–288.

АНОТАЦІЯ

Муха Ар.А. Моделі, методи та технічні засоби створення гарантоздатних керуючих комп'ютерних систем критичного призначення з двоканальною структурою обробки даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології. – Інститут проблем математичних машин і систем НАН України. Київ, 2020.

Дисертація присвячена створенню базових методів інжинірингу комп'ютерних систем (КС) спеціального призначення із двоканальною структурою обробки даних. У роботі удосконалено атрибутивну модель гарантоздатності КС та сформульовано метод кількісного оцінювання рівня реалізації атрибутів, метрик та критеріїв оцінки. Розроблено скалярну математичну модель кількісного оцінювання загального рівня

гарантоздатності КС та розроблено метод порівняльної оцінки КС з боку досягнутого рівня гарантоздатності різних варіантів їх виконання.

Запропоновано новий клас двоканальних КС із квазімістковою структурою (КМС) та можливістю її реконфігурації при відмовах. Завдяки аналітичним розрахункам та статистичному моделюванню надійності КМС, показано її переваги з боку надійності, достовірності функціонування і живучості.

З метою практичної реалізації запропоновано інформаційний підхід до забезпечення безпеки залізничних переїздів, виготовлено дослідний зразок Контрольно - інформаційної системи для залізничних переїздів «Благовіст».

Ключові слова: гарантоздатність, відмовостійкість, відмовобезпека, атрибутивна модель гарантоздатності, квазімісткова структура, кількісна оцінка рівня гарантоздатності.

ABSTRACT

Mukha Ar. A. Models, methods and technical means of creation of reliable controllers of computer systems of critical application with two-channel data structure. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of a candidate of technical sciences (doctor of philosophy) in specialty 05.13.06 – Information Technologies – Institute of Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine, Kyiv, 2020.

The dissertation addresses the new current tasks of creating, maintaining and evaluating the computer systems' security.

The work consists of an introduction, four sections, conclusions, a list of sources used and three applications. The work presented relates to the field of computer systems warranty theory.

The first section, "Developing an Attribution Model for Computer Systems Warranty," discusses the current problems of creating a computer-based computer security system and concludes that a comprehensive approach is needed to address them on the platform of a new fault-tolerant structure. The section provides an in-depth analysis of the main characteristics (attributes) of a CS, namely: uptime, availability, serviceability, survivability, reliability, functional security, confidentiality, integrity with a detailed description of their metrics and methods for quantifying them. Based on the attributive model of the CS (AMGCS), using the metric approach, a methodology for quantifying the level of implementation of attributes, metrics and criteria for evaluating the level of implementation has been developed. In order to analytically evaluate the security level of computer systems, in general, a mathematical model in the form of functional type is proposed.

By considering the attribution model of the guarantee as a set of metric indicators, a methodology for the comparative assessment of computer systems by the achieved level

of guarantee of different variants of their implementation has been developed. The basic methods of guaranteeing are described.

The second section, “Designing and Analyzing a Faulty Computer System with a Quasi-Content Structure,” first describes the approach to developing a fault-tolerant computer system for the case where the system created is a critical infrastructure and has the potential for any single failure to suspend execution. its function (in whole or in part) without going into a critical state. Thus, complete fault tolerance is transformed into partial fault tolerance, namely fault tolerance, which enables the design of more efficient systems of critical application.

Basic software requirements for fault-tolerant computer systems have been developed and the ability to achieve a high degree of security for management programs, software bugs and hardware failures has been demonstrated through the use of error prevention, detection, and fault tolerance techniques.

The classification of two-channel fault-tolerant structures of computer systems has been improved, the advantages and disadvantages of each of the structures considered with the logical function of the restoring body "I" are shown. In order to improve the operational readiness of the existing structures, a new quasi-self-repairing two-channel structure was developed with reconfiguration of component parts, consisting of equally reliable duplicate units with restoring bodies having the "AND / OR" function.

It is proved that by decomposition of functional blocks into equally reliable parts and addition of control and reconfiguration circuits it is possible to increase the overall probability of trouble-free operation of the system as a whole. The quasi-content structure easily scales in the direction of increasing the number of duplicate nodes and has a high potential for use in the construction of trouble-free systems of high availability.

In the field of creation of computer systems with high survivability, the application of the principle of infrastructure redundancy and topological optimization is demonstrated, using the example of a quasi-capacitive structure in the construction of a hydroelectric power station automatic safety system. A high survivability cluster structure has been developed, which has significant prospects for the development of endurance critical cluster systems.

In the third section, "Ensuring the failover of fault-tolerant computer systems", we investigated the reliability and reliability of a Quasi-Bridge Structure (QBS), and its advantages over other dual-channel structures. This is confirmed by analytical calculations by several methods and by statistical modeling. The reliability of the QBS functioning was evaluated using the original phenomenological model, which demonstrated its advantages over other two-channel redundant structures.

Section 4, Microprocessor Control and Information System for Blagovest Railroad Crossings, discusses the problems of accident at railroad crossings, and addresses their solutions through the introduction of a new model-based control and information system that enhances traffic through railroad crossings.

Within the framework of competition of scientific and technical projects of scientific institutions of NAS of Ukraine in IPMMS of NAS of Ukraine.

Keywords: dependability, fault-tolerance, fail safety, attributive model of dependability, quasi-bridge structure, quantitative assessment of the level of dependability.

АННОТАЦИЯ

Муха Ар.А. Модели, методы и технические средства создания гарантоспособных управляющих компьютерных систем критического назначения с двухканальной структурой обработки данных. – Квалификационная научная работа на правах рукописи.

Диссертация на соискание научной степени кандидата технических наук по специальности 05.13.06 – информационные технологии. – Институт проблем математических машин и систем НАН Украины. Киев, 2020.

Диссертация посвящена созданию базовых методов инжиниринга компьютерных систем (КС) специального назначения с двухканальной структурой обработки данных. В работе усовершенствована атрибутивная модель гарантоспособности КС и сформулирован метод количественной оценки уровня реализации атрибутов, метрик и критериев оценки. Разработана скалярная математическая модель количественной оценки общего уровня гарантоспособности КС и метод сравнительной оценки КС со стороны достигнутого уровня гарантоспособности различных вариантов их выполнения.

Предложен новый класс двухканальных КС с квазимостиковой структурой (КМС) и возможностью реконфигурации при отказах составных частей. Благодаря аналитическим расчетам и статистическому моделированию надежности КМС, показано ее преимущества по надежности, достоверности функционирования и живучести.

Предложен информационный подход к обеспечению безопасности железнодорожных переездов, проведен структурный синтез, изготовлен опытный образец Контрольно - информационной системы для железнодорожных переездов «Благовест».

Ключевые слова: гарантоспособность, отказоустойчивость, отказобезопасность, атрибутивная модель гарантоспособности, квазимостиковая структура, количественная оценка уровня гарантоспособности.