

Голові разової спеціалізованої вченої ради
Харківського аерокосмічного університету
«Харківський авіаційний інститут»
доктору технічних наук, професору
Фесенку Герману Вікторовичу

ВІДГУК

ОФІЦІЙНОГО ОПОНЕНТА

професора кафедри математичної інформатики факультету комп'ютерних наук
та Київського національного університету імені Тараса Шевченка
доктора технічних наук, професора
ЗАСЛАВСЬКОГО Володимира Анатолійовича
на дисертаційну роботу Панаріна Артема Сергійовича
«Методи і засоби забезпечення функційної безпечності інформаційно-керуючих
систем АЕС на програмовних платформах з використанням комбінованої
диверсності», представлену на здобуття ступеня доктора філософії
у галузі знань 12 «Інформаційні технології»
за спеціальністю 123 «Комп'ютерна інженерія»

1. Загальна характеристика та актуальність теми

1.1. Атомна енергетика традиційно висуває до інформаційно-керуючих систем (ІКС) найвищі вимоги функційної безпечності серед усіх промислових галузей, оскільки ціна відмови контурів аварійного захисту реактора вимірюється не лише економічними, а й екологічними та соціальними наслідками. Перехід ІКС АЕС на програмовні платформи типу FPGA та SoC розширює функціональні можливості систем, проте одночасно створює нову площину ризику — можливість того, що дефект проектування, спільний для кількох формально незалежних каналів багатoversійної системи, спричинить одночасну відмову всіх каналів (відмову за загальною причиною (ВЗЗП)).

1.2. Диверсність традиційно розглядається як основний архітектурний засіб протидії ВЗЗП, однак практичне застосування цього принципу здебільшого спирається на якісні рекомендації класифікаторів NUREG-6303 та NUREG-7007, які не дають інженеру формалізованого інструменту для обґрунтованого вибору конкретної комбінації видів диверсності під задані обмеження вартості й безпечності. Саме усуненню цієї прогалини присвячена дисертаційна робота А. С. Панаріна, в якій запропоновано перехід від описової класифікації диверсності до її графового та матричного формалізованого представлення, алгоритмічного методу вибору диверсних рішень та методу модельно-базованої верифікації, що замикає цикл «вибір диверсності — реалізація — підтвердження коректності». Таким чином, обраний здобувачем напрям дослідження є своєчасним і має

суттєве прикладне значення для проєктування та модернізації систем безпеки АЕС, зокрема на платформах Radiy та RadICS.

2. Аналіз змісту дисертації

Робота має логічну структуру, яка складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків, що послідовно розкривають зміст дослідження.

2.1. У першому розділі виконано аналіз вимог міжнародних стандартів (ІЕС 61513, ІЕС 60880, ІЕС 62138, ІЕС 61508) та національних нормативних документів до функційної безпечності ІКС АЕС, класифіковано відмови ІКС, зокрема відмови за загальною причиною, і проаналізовано принцип диверсності та наявні класифікаційні схеми її видів.

2.2. У другому розділі побудовано розширену чотирирівневу класифікацію видів і підвидів диверсності, її графову модель та дві матричні форми — булеву матрицю суміжності і матрицю інцидентності «вершина–ребро». На основі експертного анкетування визначено метрики диверсності й відносної вартості, які через формули адитивної згортки дозволяють обчислювати інтегральні показники для окремих шляхів та комбінацій шляхів графа а також розроблено алгоритми їх вибору. Також виконано ймовірнісну оцінку безвідмовної та безпечної роботи двоверсійної системи аварійного захисту реактора з використанням моделей.

2.3. У третьому розділі розроблено методи реалізації програмно-апаратної диверсності програмовних платформ: метод диверсної синхронізації каналів, метод структурно-просторової диверсності матриць логічних елементів і таймінгів сигналів, а також підходи до диверсифікації контрольних сум і механізмів контролю цілісності пам'яті. В розділі також наведено детальне моделювання кортежу тактування трьох каналів до і після застосування раціональних фазових зсувів, яке кількісно демонструє зниження узагальненого показника кількості одночасних перемикачів каналів майже на 40 %.

2.4. У четвертому розділі: розроблено метод модельно-базованої верифікації систем програмної логіки, що поєднує моделювання в середовищі ForSyDe із синтезом у VHDL; наведено результати експериментальної перевірки на прикладі еталонної реалізації soft-процесора Nios, узагальнену технологічну схему розроблення двоверсійних систем та матрицю комплексування методів диверсності; описано впровадження результатів на платформах Radiy, RadICS.

3. Наукова новизна результатів

3.1. Найбільш вагомими новими науковими результатами дисертаційного дослідження, на думку опонента, є такі:

- вперше запропоновано розширену чотирирівневу класифікацію видів і підвидів диверсності для програмовних платформних рішень ІКС АЕС

(архітектурний, апаратний, програмно-алгоритмічний, експлуатаційний рівні; понад 60 підвидів), доведено до формалізованих графової та матричної моделей, придатних для алгоритмічної обробки;

- запропоновано метод модельно-базованої верифікації систем програмної логіки ІКС АЕС, що інтегрує формальне моделювання поведінки (ForSyDe, VHDL) з апаратною реалізацією компонентів верифікації безпосередньо у складі FPGA-проєкту;

- удосконалено метод вибору видів диверсності для програмовних платформ, що поєднує експертне оцінювання метрик ефективності диверсності й відносної вартості з алгоритмами пошуку шляхів та їх комбінацій у графовій моделі за критеріями максимізації диверсності, мінімізації витрат та компромісу «диверсність/вартість»; методи реалізації програмно-апаратної диверсності — метод диверсної синхронізації каналів на основі варіації тактових параметрів і фазових зсувів та метод структурно-просторової диверсності матриць логічних елементів і таймінгів сигналів;

- отримало подальший розвиток технологічна схема розроблення та верифікації двоверсійних і багатоверсійних систем безпеки АЕС з комплексним застосуванням запропонованих моделей диверсності та модельно-базованого тестування.

3.2. Формулювання наукової новизни результатів опонентом у цілому узгоджується з авторським викладом у вступі та висновках дисертації.

4. Обґрунтованість наукових положень і їх достовірність

4.1. Сформульовані в дисертації наукові положення, висновки та практичні рекомендації достатньо обґрунтовані застосуванням апробованого математичного апарату — теорії множин і графів для побудови моделей диверсності, теорії надійності для оцінки ймовірності безвідмовної роботи двоверсійної системи аварійного захисту, а також відповідністю прийнятих архітектурних рішень вимогам міжнародних стандартів ІЕС 61513, ІЕС 60880, ІЕС 62138, ІЕС 61508.

Побудована здобувачем система моделей є внутрішньо узгодженою: розширений класифікатор диверсності послідовно трансформується у графову й матричну форми, на основі яких формалізовано метрики та алгоритми вибору диверсних рішень, а отримані комбінації диверсності далі підтверджуються методами програмно-апаратної реалізації та модельно-базованої верифікації. Такий наскрізний зв'язок моделей, методів і засобів реалізації є свідченням методологічної цілісності дослідження.

4.2. Достовірність результатів підтверджена експериментальною перевіркою на реальних FPGA-платформах: моделюванням кортежу тактування для методу диверсної синхронізації та порівнянням еталонної й диверсної реалізацій засобами ForSyDe з розрахунком інтегрального коефіцієнта

диверсності $K_d = 0,9$, підтвердженого додатковою перевіркою часових діаграм у середовищі ModelSim на трьох рівнях опису (алгоритмічному, функціональному, апаратному). Отримані результати експериментальної перевірки узгоджуються з підсумковими оцінками, наведеними автором у висновках дисертації, і в сукупності підтверджують практичну ефективність запропонованих методів диверсності та верифікації.

5. Практичне значення отриманих результатів

5.1. Теоретичні результати доведено автором до методичних рекомендацій з вибору стратегій диверсності для платформ Radiu та RadICS, програмних засобів автоматизованого аналізу графової моделі диверсності та апаратних прототипів двоверсійних модулів з реалізованими методами диверсної синхронізації й контролю цілісності.

5.2. Отримані наукові результати мають підтверджене практичне застосування за трьома напрямками: в освітньому процесі ХАІ — при викладанні дисциплін з комп'ютерної інженерії та ядерної безпеки; у виробничій діяльності — у складі науково-дослідних і дослідно-конструкторських робіт з модернізації ІКС АЕС на платформах Radiu та RadICS; а також у нормативно-методичній роботі — при підготовці документації для систем сертифікації безпеки АЕС. Кожен із напрямів підтверджено окремим актом впровадження.

6. Повнота висвітлення основних результатів дисертації

Кількісні та якісні вимоги до оприлюднення результатів дисертаційного дослідження виконано: 16 публікацій охоплюють 8 статей у фахових виданнях України категорії «Б», статтю у виданні Springer (Q4 Scopus), участь у трьох колективних монографіях (одна індексується Scopus) та чотири доповіді, опубліковані в матеріалах конференцій рівня Scopus. Здобувач представляв результати роботи на конференціях «Dependable Systems, Services and Technologies», «DepCoS-RELCOMEX», «Information and Digital Technologies», «International Conference on Nuclear Engineering» та «IDAACS».

7. Оцінка оформлення дисертації, дотримання вимог академічної доброчесності

Робота А. С. Панаріна в цілому оформлена згідно з чинними вимогами Міністерства освіти і науки України. Виклад матеріалу послідовний і логічний, кожен розділ супроводжується висновками. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, списку використаних джерел (138 найменувань) та додатків; повний обсяг становить 218 сторінок, робота містить 46 рисунків, 12 таблиць та 32 формули. Перевірка роботи на текстові збіги підтвердила, що дисертація є результатом самостійного дослідження здобувача,

ознак фальсифікації, фабрикації, плагіату чи некоректних запозичень без посилань не виявлено.

8. Зауваження до дисертаційної роботи

1. Розроблена система метрик диверсності та відносної вартості спирається на усереднені експертні оцінки вагових коефіцієнтів, при цьому кваліфікація й досвід окремих експертів у розрахунках не диференціюються. Варто додати коефіцієнт компетентності експерта (стаж, профільна кваліфікація), який враховувався б при агрегуванні індивідуальних оцінок у підсумкові метрики диверсності.

2. Немає розгорнутої оцінки економічного ефекту впровадження методів диверсності (наприклад, порівняння вартості реалізації диверсних рішень з вартістю усунення наслідків потенційної ВЗЗП), а також рекомендацій щодо адаптації методів до умов воєнного часу — живучості й відновлюваності систем безпеки АЕС в умовах зовнішніх впливів на критичну інфраструктуру.

3. В моделях фактично не враховується можлива різниця в безвідмовності елементів двох- або багатоверсійної архітектури, що може вплинути на вибір кращого варіанту.

4. В дисертаційній роботі йде мова про життєвий цикл систем, що досліджуються, але не розглянуто питання старіння та остаточного ресурсу об'єктів, що теж вимагає застосування філософії диверсності при проведенні технічного обслуговування систем.

5. В дисертаційній роботі відсутні посилання на публікації опонента, оскільки питання диверсності - різнотипне резервування складних систем розглядалось з 1983 року, є публікації в українських та міжнародних виданнях, працях конференцій та монографіях.

6. В роботі використовуються різноманітні математичні формули та моделі прийняття рішень, в представлених моделях прямих і обернених задач оптимізації необхідно вказувати параметри оптимізації та умови для вагових коефіцієнтів показників. Доцільно більш детально пояснювати параметри формул наприклад на стор. 83 формули (2.4)-(2.7) та (2.21)-(2.27) на стор. 109, а також в інших місцях, а також звертати увагу при посиланні на формули, так у прикладі розрахунків на стор.95 є посилання на формули (2.16), (2.17) які знаходяться на стор. 104, а не поруч з прикладом.

7. В дисертації на сторінках є пусті місця, наприклад стор. 130, 136 та багато великих відступів та пропусків між рядками тексту, назвами параграфів. На стор.107 є посилання на представлений на стор. рис. 2.9, який є ідентичним із рис.1.1 на стор.30. Деякі рисунки та тексти програм можна винести в додатки. В тексті зустрічаються багато разів слова (рисунок, таблиця) які можна написати скорочено рис., табл., все вище сказане приведе до скорочення кількості сторінок роботи.

Перелічені зауваження не знижують рівень дисертаційної роботи і не впливають на загальну позитивну характеристику дисертації.

9. Висновки щодо дисертаційної роботи

9.1. На основі детального аналізу роботи вважаю, що дисертаційна робота Панаріна Артема Сергійовича «Методи і засоби забезпечення функційної безпечності інформаційно-керуючих систем АЕС на програмовних платформах з використанням комбінованої диверсності» є завершеним, самостійним і цілісним науковим дослідженням, яке вирішує актуальне науково-технічне завдання підвищення функційної безпечності багатOVERсійних ІКС АЕС на програмовних платформах.

9.2. За своїм науково-методичним рівнем, обґрунтованістю висновків та практичною цінністю робота повністю задовольняє вимоги пп. 6–9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44. Її автор, Панарін Артем Сергійович, заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 123 «Комп'ютерна інженерія».

Офіційний опонент,
професор кафедри математичної інформатики
факультету комп'ютерних наук та кібернетики
Київського національного університету
імені Тараса Шевченка,
доктор технічних наук, професор

Володимир А. ЗАСЛАВСЬКИЙ

30 вересня 2026 р.