МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.Н. КАРАЗІНА

ОДАРУЩЕНКО Олег Миколайович

УДК 004.05,004.415.5

МЕТОДИ І ЗАСОБИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ З УРАХУВАННЯМ ФІЗИЧНИХ І ПРОЄКТНИХ ДЕФЕКТІВ КОМПОНЕНТІВ

05.13.05 – комп’ютерні системи та компоненти

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня

доктора технічних наук

Харків–2021

Дисертацією є рукопис.

Робота виконана на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор,
ХАРЧЕНКО Вячеслав Сергійович,
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», завідувач кафедри комп'ютерних систем, мереж і кібербезпеки.

Офіційні опоненти: доктор технічних наук, професор,
ДРОЗД Олександр Валентинович,
Одеський національний політехнічний університет, професор кафедри комп'ютерних інтелектуальних систем та мереж;

доктор технічних наук, професор,
КРИВУЛЯ Геннадій Федорович,
Харківський національний університет радіоелектроніки, професор кафедри автоматизації проектування обчислювальної техніки;

доктор технічних наук, професор,
ОПАНАСЕНКО Володимир Миколайович,
провідний науковий співробітник відділу мікропроцесорної техніки Інституту кібернетики імені В.М. Глушкова НАН України.

Захист відбудеться «06» травня *2021 року о* 15-00 *годині* на засіданні спеціалізованої вченої ради Д 64.051.29 Харківського національного університету імені В.Н. Каразіна за адресою: 61022, м. Харків, майдан Свободи, 6, ауд. 234.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету імені В.Н. Каразіна за адресою: 61022, м. Харків, майдан Свободи, 4.

Автореферат розісланий «05» квітня *2021року.*

Учений секретар
спеціалізованої вченої ради Євгенія КОЛОВАНОВА

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В забезпеченні безпеки АЕС, авіаційних і ракетно-космічних комплексів та інших критичних об'єктів важливу роль відіграють інформаційні-керуючі системи (ІКС), ядром яких є програмно-технічні комплекси (ПТК). Вартість відмов ПТК ІКС АЕС, є надзвичайно високою. Кількість експлуатаційних подій за даними сайту Державного науково-технічного центру з ядерної та радіаційної безпеки, які викликані відмовами ІКС в період 2015-2018 рр. становить 46%.

Найважливішою характеристикою ІКС є функційна безпечність, яка відповідно до міжнародних і національних стандартів (IEC61508, IEC26262) визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та/або його наслідки. Для України актуальність нормування, моніторингу, оцінювання та забезпечення функціональної безпечності підтверджується наявністю великої кількості аварійно небезпечних об'єктів, перш за все, реакторів АЕС.

Це зумовлює необхідність: по-перше, гарантованого виконання вимог до стійкості до відмов програмних, програмовних, апаратних засобів, збурень різної природи та змін характеристик фізичного та інформаційного середовища; по-друге, забезпечення якості розроблення і точності відтворення реальних потреб використання ПТК ІКС за призначенням; по-третє, мінімізації часових, енергетичних та інших ресурсів, які використовуються.

Сучасні процеси модернізації існуючих та розробки перспективних ПТК ґрунтуються на використанні нової елементної бази, сучасних технологіях створення їх апаратної та програмної компонент. Це, з одного боку, розширює можливості ІКС, приводить до підвищення ефективності технологічних процесів, знижує ресурсоємність виробництва, а з іншого – до зростання ризиків підвищення залежності функціональності, надійності й безпеки від якості проєктних рішень. Впровадження індустріальних технологій розроблення програмного забезпечення не призвело до такого ж прогресу в проектуванні ПТК із гарантованим рівнем надійності та безпеки.

Слід зазначити, що такий стан речей склався, не зважаючи на інтенсивні дослідження впродовж останніх десятиліть, які виконувалися в Україні та за її межами, зокрема, за напрямами:

- розвитку теоретичних засад, загальних методів оцінювання та підвищення надійності та функційної безпечності (A. Avizienis, J.-C. Laprie, G. Johnson, B. Randell, E. Zaitseva, Б.Ю. Волочий, Б.М. Конорєв, В.С. Харченко, М.О. Ястребенецький та інші);
- розроблення методів і засобів оцінювання та забезпечення надійності програмного забезпечення для різних застосунків (B. Littlewood, P. Popov, A. Romanovsky, S. Russo, L. Strigini, J. Vain, В.В. Ліпаєв, Д.А. Маєвський, В.С. Яковина та інші);
- розроблення й дослідження моделей та методів діагностування і забезпечення стійкості інформаційно-керуючих систем і ПТК до фізичних та проєктних дефектів (T. Anderson, F. Saglietti, K. Trivedi, О.В. Дрозд, В.А. Краснобаєв, Г.Ф. Кривуля, В.М. Опанасенко, О.М. Романкевич, В.О. Романкевич, В.В. Скляр, В.І. Хаханов та інші).

Зокрема, залишається низка нерозв'язаних задач і обмежень існуючих методів і засобів, а саме:

- моделі, які описують надійнісну і безпекову (як інформаційну, так і функційну) складові, не ураховують реальну розмірність задач оцінювання з огляду на складність індустріальних ІКС та їх ПТК, змінність параметрів відмов і відновлень;

- у методах оцінювання функційної безпечності, насамперед, аспекти безвідмовності апаратних і програмних засобів розглядаються відокремлено, без спільного кількісного аналізу результатів верифікації, а також змінності параметрів, які впливають на точність оцінки;

- методи розроблення й забезпечення відмовостійкості ПТК з використанням програмовних платформ недостатньо ураховують можливості, обмеження і похибки вбудованих засобів контролю і діагностування на рівні електронних проєктів, модулів і каналів тощо.

Таким чином, можливо зробити висновок про існування **протиріччя,** яке полягає у невідповідності між розширенням множини причин порушення працездатності програмно-технічних комплексів інформаційно-керуючих систем атомних станцій, аерокосмічних комплексів та інших індустріальних об'єктів критичного застосування (КЗ) внаслідок фізичних і проєктних дефектів їх апаратних, програмних і програмовних компонентів, зміною параметрів потоків їх відмов і відновлень, ***з одного боку,*** і рівнем розвитку концептуальних засад, сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпечності, які не враховують повну множину причин і характеристик відмов і порушень ПТК, – ***з іншого боку***. Подолати це протиріччя можливо шляхом вирішення **актуальної науково-прикладної проблеми** комплексного оцінювання і забезпечення надійності і функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування в процесі розроблення, верифікації, валідації та використання за призначенням з урахуванням відмов, обумовлених проєктними, фізичними дефектами і вразливостями програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» в рамках держбюджетних науково-дослідних робіт МОН України: «Розробка науково-методичних основ й інформаційних технологій оцінки і забезпечення відмовостійкості та безпеки комп'ютеризованих систем аерокосмічних комплексів, інших комплексів критичного застосування» (№Г503-42/2003, №104U003502, 2003-2004); «Теоретичні основи, методи та інструментальні засоби аналізу, розробки та верифікації гарантоздатних інформаційно-управляючих систем для аерокосмічних об'єктів і комплексів критичного застосування» (ДР № №0106U001071, 2006-2008); «Теоретичні основи, методи та технології забезпечення гарантоздатності еволюціонуючих комп'ютеризованих інфраструктур для аерокосмічних і критичних об'єктів» (ДР№0108U010994, 2009-2011); «Теоретичні основи, методи та інформаційні технології розробки програмно-технічних комплексів критичного застосування в умовах ресурсних обмежень» (ДР№

0112U001058, 2012-2014); Наукові основи, методи і засоби зеленого комп'ютингу і комунікацій (ДР№0115U000996, 2015-2017).

Мета і завдання дослідження. Метою дисертаційного дослідження є розвиток методологічних основ, розроблення методів і засобів оцінювання та забезпечення надійності та функційної безпечності програмно-технічних комплексів на різних етапах життєвого циклу з урахуванням відмов, обумовлених фізичними та проєктними дефектами і вразливостями, а також їх практичне впровадження в інформаційно-керуючих системах критичного застосування для зниження ризиків небезпечних відмов.

Досягнення поставленої мети передбачає вирішення таких завдань:

1. Аналіз принципів, методів і засобів оцінювання та забезпечення надійності та функційної безпечності ПТК ІКС критичного застосування;
2. Розвиток методології оцінювання і забезпечення надійності та функційної безпечності ПТК для ІКС критичного застосування;
3. Вдосконалення ймовірнісних моделей надійності програмних засобів з урахуванням вторинних дефектів;
4. Розроблення методу оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю;
5. Розроблення моделей оцінювання надійності та функційної безпечності ПТК на самодіагностованих платформах;
6. Розроблення методів верифікації і валідації програмовних платформ і ПТК на їх основі;
7. Вдосконалення методу забезпечення функційної безпечності ПТК на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності);
8. Розроблення методу оцінювання та забезпечення функційної безпечності при створенні та ліцензуванні модулів і платформ для ІКС на програмовних логічних інтегральних схемах;
9. Розроблення та впровадження інструментальних програмно-апаратних засобів підтримки процесів ліцензування програмовних платформ та ПТК ІКС, забезпечення їх відповідності вимогам національних і міжнародних стандартів.

Об'єкт дослідження – програмно-технічні комплекси інформаційно-керуючих систем критичного застосування, а також процеси забезпечення їх надійності та функційної безпечності на різних етапах життєвого циклу.

Предмет дослідження – принципи, методи і засоби оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування при розробленні, верифікації та використанні за призначенням.

Методи дослідження. При розв'язанні науково-прикладної проблеми було використано наступні методи. При удосконаленні ймовірнісних моделей оцінювання надійності (безвідмовності) програмних засобів було використано методи теорії надійності програмних засобів та математичної статистики. При розробленні методу оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю було використано методи теорії надійності, теорії множин і графів, марковських випадкових процесів з

дискретними станами і неперервним часом. При розробленні математичних моделей оцінювання готовності та функційної безпечності ПТК на самодіагностовних платформах було використано методи теорії надійності і технічної діагностики, теорії ймовірностей та марковських випадкових процесів. При розробленні методів верифікації і валідації програмовних платформ і ПТК на їх основі було використано методи аналізу видів, наслідків і критичності відмов, теорії множин, методи системного аналізу. При розробленні методу забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах було використано теорії надійності і технічної діагностики, теорії множин і графів, марковського аналізу. При розробленні методу оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і програмовних платформ було використано методи теорії надійності і технічної діагностики, теорії множин і графів, марковського аналізу, системного аналізу. Оцінка експериментальних даних, отриманих у ході роботи, проводилася з використанням методів математичної статистики.

Наукова новизна одержаних результатів обумовлена розробленими методологією, моделями та методами оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного застосування, які надали подальший розвиток відповідному науковому напряму та в межах яких отримані такі нові наукові результати:

уперше розроблено:

- метод оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю, який на відміну від відомих враховує різні сценарії зміни параметрів потоків відмов і відновлень програмних, програмовних і апаратних засобів, що забезпечує підвищення точності розрахунку функції готовності та імовірності відмов за загальною причиною;
- моделі оцінювання готовності та функційної безпечності програмно-технічних комплексів на самодіагностовних платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функційної безпечності, можливість обґрунтування вимог до засобів контролю й діагностування та формування рекомендацій щодо їх виконання;
- методи верифікації і валідації програмовних платформ і програмно-технічних комплексів на їх основі, які на відміну від відомих, базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов та ін’єктування фізичних і проєктних дефектів, що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності за рахунок збільшення імовірності виявлення прихованих дефектів;
- метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах, який на відміну від відомих ураховує фізичні та проєктні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3;

удосконалено:

- ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та аналізу різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання кількісних показників;

набули подальшого розвитку:

- методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушень внаслідок проєктних і фізичних дефектів і дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і повне виконання вимог до відповідних показників;
- метод забезпечення функційної безпечності програмно-технічних комплексів на самодіагностовних програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною.

Достовірність нових наукових положень і висновків дисертаційної роботи підтверджується:

- збігом з результатами, отриманими з використанням відомих моделей і методів теорії надійності; обґрунтованістю припущень, прийнятих при розробленні моделей і методів, виходячи з досвіду експлуатації ПТК ІКС;
- працездатністю та ефективністю апаратних рішень та інструментальних засобів, отриманих із застосуванням запропонованих методів і моделей, підтвердженою на низці підприємств;
- результатами практичного використання розроблених моделей, методів та інструментальних засобів при створенні, сертифікації та експлуатації ПТК на програмовних платформах та ІКС різного призначення.

Практичне значення одержаних результатів полягає в тому, що розроблені моделі та методи доведено до прикладних інженерних методик та процедур, рекомендацій щодо побудови архітектур ПТК, використанням інструментальних засобів оцінювання, програмно-апаратних засобів забезпечення надійності та функційної безпечності ПТК в організаціях, які займаються розробленням, виробництвом, модернізацією та експлуатацією інформаційно-керуючих систем, важливих для безпеки. Це дозволило покращити показники надійності і функційної безпечності ПТК ІКС, які використовуються у атомній енергетиці, авіаційних системах та інших критичних системах, а також обгрунтувати вимоги до них.

Результати досліджень впроваджено на наступних підприємствах:

1. Публічному акціонерному товаристві «Науково-виробниче підприємство «Радій» (м. Кропивницький) при оцінюванні надійності і функційної безпечності перспективної цифрової інформаційно-управляючої платформи RadICS в процесі її SIL-3 сертифікації на відповідність вимогам стандарту IEC 61508 (акт впровадження 17.09.2020);
2. Товаристві з обмеженою відповідальністю «Науково-виробниче підприємство «Радікс» в ході розроблення процедур і інструкцій системи

менеджменту якості підприємства і виконанні низки проєктів (I&C Test Platform for Electricite de France, Франція; I&C system of IEA-R1 Research Reactor Control Console and Nuclear Channels Modernization, Бразилія; Embalse Refurbishment, MCR and SCA Window Annunciators, Аргентина) (акт впровадження 16.09.2020);

3. Державному науково-виробничому підприємстві «Об'єднання «Комунар» СКБ «Полісвіт» при розробленні бортових інформаційно-керуючих систем для літаків АН-70, АН-148, що підвищило значення показників надійності і функційної безпечності з урахуванням різних типів дефектів і відмов програмно-апаратних засобів, ПЛІС і засобів контролю і самодіагностування (акт впровадження 28.08.2020);

4. Державному підприємстві «Державний науково-технічний центр з ядерної та радіаційної безпеки» в процесі розроблення проєктів нормативних документів і методик оцінювання відповідності ІКС АЕС вимогам стандартів, що надало змогу покращити повноту оцінювання і якість відповідних документів (акт впровадження 29.09.2020);

5. Приватному підприємстві ЛітСофт в ході розроблення технології модельної розробки і тестування апаратного забезпечення (програмовних плат, чіпів, систем електроніки) з використанням комбінації методів машинного навчання та алгебраїчного підходу , що дозволяє звільнитись від суб'єктивності синтезу тестових наборів, підвищити ефективність тестування і відповідно рівень надійності і функційної безпечності (акт впровадження 23.09.2020);

6. Національному аерокосмічному університеті ім. М.Є. Жуковського «ХАІ» при виконанні 5 науково-дослідних робіт за держазомвленням (акт впровадження 24.08.2020), при виконанні міжнародних проєктів за програмою Європейського Союзу: «MASTAC» (Msc and PhD Studies in Aerospace Critical Computing , 2006-2009 pp); «SAFEGUARD» (National Safeware Engineering Network of Centres of Innovative Academia-Industry Handshaking , 2010-2013 pp); SEREIN» (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains , 2013-2016 pp), а також в навчальному процесі для розроблення навчального контенту навчальних дисциплін: «Технології забезпечення якості ПТК»; «Технології проєктування програмних систем»; «Теорія ризиків та технології управління безпекою ІКС»; «Технології розроблення та забезпечення функційної безпеки ІУС» (акт впровадження 25.09.2020).

Публікації. За результатами досліджень опубліковано 68 наукових праць, 5 монографій [1-5], з яких одну індексовано у науково-метричній базі Scopus, підручник [67], 2 навчальних посібника [61, 62], настанова Національного космічного агентства України [64], 25 статей у наукових фахових виданнях України та інших держав [6-30], з яких 3 індексовано у науково-метричній базі Scopus, 30 тез доповідей в збірниках матеріалів конференцій [31-60], з яких 12 індексовано у науково-метричній базі Scopus, отримано свідоцтво про реєстрацію авторського права на твір [63].

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи отримано особисто. Робота [30] і розділи роботи [3] написано без соавторів. В опублікованих із співавторами здобувачеві належить такі результати: [1]-моделювання і оцінка готовності ПТК з урахуванням зміни параметрів процессів

відмов та відновлень; [2]-методи визначення параметрів потоків відмов та відновлення ПЗ та величин їх зміни, послідовність розробки і аналіз моделей готовності ІТ-інфраструктур з змінними параметрами; [3]-методи контроля випадкових відмов обладнання, методи виключення систематичних відмов обладнання; [4]-методика оцінювання енергоспоживання ПЛК; [5]-аналіз недоліків IEC 61508, багатофрагментні марковські моделі та розв'язання систем диференційних рівнянь; [6]-багатофрагментна марковська модель; [7]-алгоритм модифікованого експоненційного методу розв'язання систем лінійних алгебраїчних рівнянь; [8]-визначення термінів дефект ПЗ, відмова ПЗ; [9]-визначення термінів дефект ПЗ, відмова ПЗ; [10]-МНПЗ з урахуванням недетермінованого числа вторинних дефектів; [11]- модель інформаційно-технічного стану з урахуванням рівней працездатності, показники гарантоздатності; [12]-марковські моделі з урахуванням прояву вторинних дефектів ПЗ; [13]-модель подій, показники гарантоздатності; [14]-елементи технології модельної розробки апаратного забезпечення з використанням комбінації методів машинного навчання та алгебраїчного підходу; [15]- визначення параметрів функцій ризику МНПЗ для урахування вторинних дефектів; [16]-список параметрів параметрів, які застосовуються в МНПЗ для урахування вторинних дефектів; [17]- етапи розроблення багатофрагментних марковських моделей; [18]-метод оцінювання надійності ПЗ з урахуванням прояву вторинних дефектів; [19]-інструментальні засоби функціонального покриття для електронних проектів ПЛІС в ході виконання їх функціонального тестування; [20]-модель функціонального покриття для електронних проєктів ПЛІС);[21]-марковські моделі оцінювання готовності комп'ютерних систем; [22]-структурна схема надійності відмовостійкості системи, система диференційних рівнянь; [23]-алгоритм обрання інструментальних засобів; [24]-однофрагментні та багатофрагментні моделі оцінювання надійності комп'ютерних систем; [25]-базова марковська модель відмов ІКС, структурна модель системи контроля та діагностики на основі самодіагностовних програмовних платформ; [26]-однофрагмента та багатофрагментна марковські моделі оцінювання надійності двохканальної комп'ютеризованої системи; [27]-постановка завдання розроблення моделей математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів; [28]-структурні схеми систем нормальної експлуатаціїта аварійного захисту, дерева відмов, багатофрагментні моделі з урахуванням помилок засобів контролю; [29]-модифікована МНПЗ Джелінські-Моранди; [31]-математичні моделі готовності критичних інфраструктур з змінними параметрами; [32]-структурна схема надійності, багатофрагмента марковська модель; [33]-процедура тестування з внесенням дефектів; [34]-етапи оцінювання готовності ПТК; [35]-оптимальна FIT – процедура, алгоритм та приклад виконання процедури; [36]-багатофрагментна марковська модель, індустріальний приклад; [37]-результати аналізу недоліків стандарту IEC 61508, структурна схема надійності та марковська модель системи аварійного захисту; [38]-етапи виконання HW FIT процедури; [39]-основні етапи реалізації процедури тестування АК з внесенням мультидефектів; [40]-індустріальний приклад виконання процедури тестування з внесення мультидефекту; [41]-етапи автоматизації техніки FMEDA;. [42]- процедура обрання

інструментальних засобів для оцінювання надійності ПТК; [43]-визначення FIT – здатності, SW та HW процедури з внесенням дефектів; [44]-процедура SW FMEA; [45]-модель оцінювання надійності відновлюваних управлючих систем з урахуванням засобів контролю; [46]-методика оцінка надійності обчислювальних систем;[47]-визначення надійності як критерія якості програмного забезпечення; [48]-багатофрагментна модель для дубльованої архітектури ПТК; [49]-модифікація МНПЗ Джелинського-Моранди; [50]-приклад формування кореляційної залежності; [51]-визначенння інформаційно-технічного стану, елементи методології; [52]-перелік параметрів оцінювання надійності ПЗ з урахуванням вторинних дефектів; [53]-визначення етапів метода оцінювання надійності програмних засобів; [54]-аналіз IEC 61508, перелік недоліків стандарта, підходи до їх усунення; [55]-етапи оцінювання надійности ПТК в контексті 61508; [56]-деталізована процедура тестування ПЗ з внесенням дефектів; [57] - Концепція і принципи оцінювання і забезпечення надійності та функціональної безпеки програмно-технічних комплексів; [58] - метод оцінювання та забезпечення функційної безпеки; [59]-багатофрагментні марковські моделі критичних інфраструктур; [60] – марковські моделі; [61] - моделювання та оцінка комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ; [62]-практичні заняття змоделювання та оцінки комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ; [63] - алгоритм рішення марковських ланцюгів; [64]-поняття про інформаційно-технічний стан, дефекти та уразливості, що призводять до порушення працездатності; [65]-опис методів контроля відмов обладнання, опис функційного тестування, аналіз процесів валідації FPGA систем; [66] - опис створення spin-off компанії із задачами забезпечення та оцінювання безпеки ІКС; [67]-загальна характеристика процесу побудови автоматизованих систем управління; [68]-принципи забезпечення безпеки.

Результати дисертаційної роботи повністю відображено в публікаціях. Всі співавтори згодні із внеском здобувача. Робота не містить плагіату та запозичень. У докторській дисертації не містяться результати кандидатської дисертації.

Апробація результатів дисертації.

Основні положення і результати дисертаційної роботи доповідалися та обговорювалися на міжнародних, всеукраїнських та регіональних конференціях: Всеукраїнському науково-технічному семінарі «Критичні комп’ютерні технології та системи» на кафедрі комп’ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ» (м. Харків, 2003÷2019 рр.); DepCos-RELCOMEX 2010: International Conference on Dependability of Computer Systems, Brunow Palace, Poland, 2010; IDT 2013: 7th International Conference on Digital Technologies, Circuits, Systems and Signal Processing, Žilina, Slovak Republic, 2010; ICTERI 2013: 9th International Conference on ICT in Education, Research, and Industrial Applications, Kherson, Ukraine, 2013; 6th International Workshop on the Applications of FPGA in Nuclear Power Plants, Kirovograd, Ukraine, 2013; CrISS 2013: 3rd International Workshop Critical Infrastructure Safety and Security, Sevastopol, Ukraine, 2013; EWDTS 2013: East-West Design&Test Symposium, Ростов-на-Дону, Росія, 2013; МОДС 2013: Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання», Чернігів-Жукин, Україна, 2013; DT 2014: 10th International Conference

on Digital Technologies, Zilina, Slovak Republic, 2014; PSAM 12: 12th International Conference on Probabilistic Safety Assessment and Modeling, Hawaii, Honolulu, USA, 2014; ICONE 22: 22nd International Conference on Nuclear Engineering, Prague, Czech Republic, 2014; NPIC and HMIT 2015: 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC, USA, Charlotte, 2015; ICONE 23: 23rd International Conference on Nuclear Engineering, Chiba, Japan, 2015; SMRLO 2016: 2nd International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management, Beer Sheva, Israel, 2016; ICONE 26: 26th International Conference on Nuclear Engineering, London, United Kingdom, 2018; міжнародна науково-технічна конференція НТК "Гарантоздатні (надійні і безпечні) системи, сервіси і технології (DESSERT – Dependable Systems, Services and Technologies)" (м. Полтава, 2006 р., м. Кіровоград, 2007-2010 рр., м. Севастополь, 2012 р., 2014 р., м. Київ, 2016 р., 2018 р., 2020 р.).

Структура та обсяг дисертації. Дисертаційна робота складається з анотацій двома мовами, вступу, шести розділів, висновків, списку використаних джерел та додатків, де: додаток А - показники, параметри системні позначення; додаток Б – результати оцінювання готовності ПТК дубльованих архітектур; додаток В – загальна процедура верифікації і валідації; додаток Г – акти впровадження; додаток Д – список опублікованих праць за темою дисертації. Загальний обсяг дисертації становить 429 сторінок; робота містить 112 рисунків (з них 16 на окремих сторінках); 35 таблиць; список використаних джерел, що включає 317 найменувань на 36 сторінках; 4 додатки на 41 сторінці.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ містить загальну характеристику роботи, актуальність проблеми, мету та завдання дослідження, відомості про зв'язок роботи з науковими програмами, планами, темами, відзначені наукова новизна й практична цінність отриманих результатів, особистий внесок здобувача в роботах у співавторстві, відомості про апробацію результатів роботи.

У **першому розділі** проведено аналіз методів і засобів оцінювання та забезпечення надійності та функційної безпечності ПТК ІКС критичного використання. Проведено аналіз факторів впливу різної природи на надійність, функційну безпечність ІКС критичного використання. Визначена вартість наслідків відмов ПТК ІКС критичного використання. Систематизовано вимоги державних та міжнародних стандартів до надійності і функційної безпечності ПТК та вимоги до організації процесів розробки, верифікації та валідації для забезпечення виконання цих вимог. Розглянуто узагальнені структури ПТК та ІКС як об’єктів моделювання. Виконано огляд методів і засобів оцінювання надійності і функційної безпечності ІКС критичного використання, прокласифіковано моделі і методи. Проведено аналіз математичного апарату та обмежень використання існуючих методів оцінювання. Визначено протиріччя та сформульовано науково-прикладну проблему. Обґрунтовано задачі, математичний апарат, етапи і методику досліджень.

Основні положення розділу викладені у публікаціях автора [1, 2, 3, 7, 23, 46, 60, 62 ,64, 65].

Другий розділ присвячено розробці методології оцінювання і забезпечення

надійності і функційної безпечності ПТК ІКС критичного застосування. Методологія оцінювання і забезпечення надійності та функційної безпечності ПТК ІКС критичного застосування базується на використанні системи принципів, об'єднаних загальною концепцією і покладених в основу розроблених в дисертації моделей і методів.

Базові ідеї досліджень грунтуються на парадигмі фон Неймана створення надійної системи із ненадійних елементів, яка розвивається стосовно ПТК ІКС критичного застосування шляхом їх комплексного оцінювання і забезпечення надійності і функційної безпечності.

Комплексність базується, по-перше, на розширенні поняття технічного стану системи до інформаційно-технічного стану (ІТС), де під ІТС розуміється сукупність властивостей і ознак як технічного, так і інформаційного характеру, притаманних системі в певний момент часу. Застосування поняття ІТС дозволяє врахувати такі властивості системи, як безвідмовність, готовність, функційну безпечність. По-друге, комплексність базується на врахуванні:

- множини компонентів: МК={АК, ПК, ПвК} (апаратних (АК), програмних (ПК), програмовних (ПвК);
- множини дефектів: МД={ДФ, ДП, ДВФ, ДВІ} (фізичні дефекти АК – (ДФ), дефекти проектування (ДП), дефекти взаємодії фізичної природи (ДВФ), дефекти взаємодії інформаційні (ДВІ));
- множини відмов: МВ={ВК, ВН} (відмови критичні (ВК), відмови некритичні (ВН));
- множини змінних параметрів: МЗП={ЗІВм, ЗІВн, ЗКВн} (змінні інтенсивності відмов (ЗІВм – $\Delta\lambda_d$, $\Delta\lambda_{дв}$), змінні інтенсивності відновлень (ЗІВн – $\Delta\mu_d$, $\Delta\mu_{дв}$), запас компонент для відновляння (ЗКВн));
- множини властивостей (атрибутів): МА={АБ, АГ, АФБ, АІБ,АГз} (атрибути безпеки (АБ), атрибути готовності (АГ), атрибути функційної безпечності (АФБ), атрибути інформаційної безпеки (АІБ), атрибути гарантоздатності (АГз)).

Отже, комплексність дорівнює декартовим добутком множин

$$М = МК \times МД \times МВ \times МЗП \qquad (1)$$

та подається у трьохмірному просторі (рис. 1).

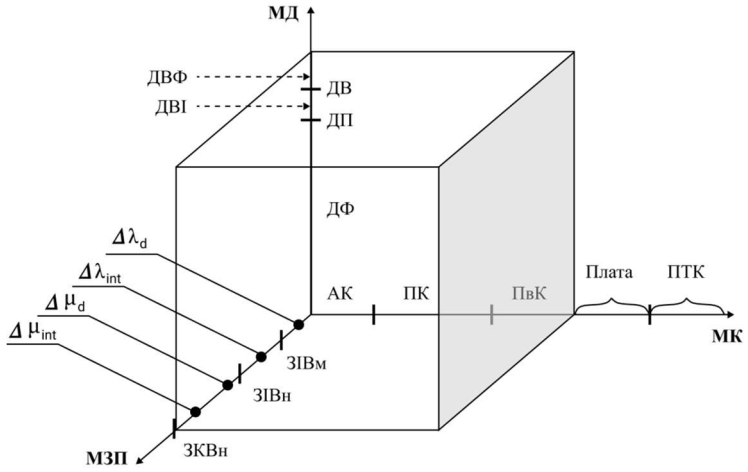

Рис. 1 Трьохмірний куб врахування множин компонент, дефектів та змінності параметрів

Структура методології оцінювання і забезпечення надійності і функційної безпечності ПТК ІКС критичного використання, яка ієрархічно поєднує обрану концепцію, обгрунтовані принципи та розроблені на їх основі моделі, методи та інструментальні засоби наведено на рис. 2.

Розроблено модель «система-фізичне та інформаційне середовище».

$$S(t) = \{S_0(t), E_{int}(t), E_{ext}(t)\}, \quad (2)$$

де $S_0(t)$ – працезданий стан, $E_{int}(t)$ – вектор internal (внутрішніх) впливів, $E_{ext}(t)$ – вектор external (зовнішніх) впливів.

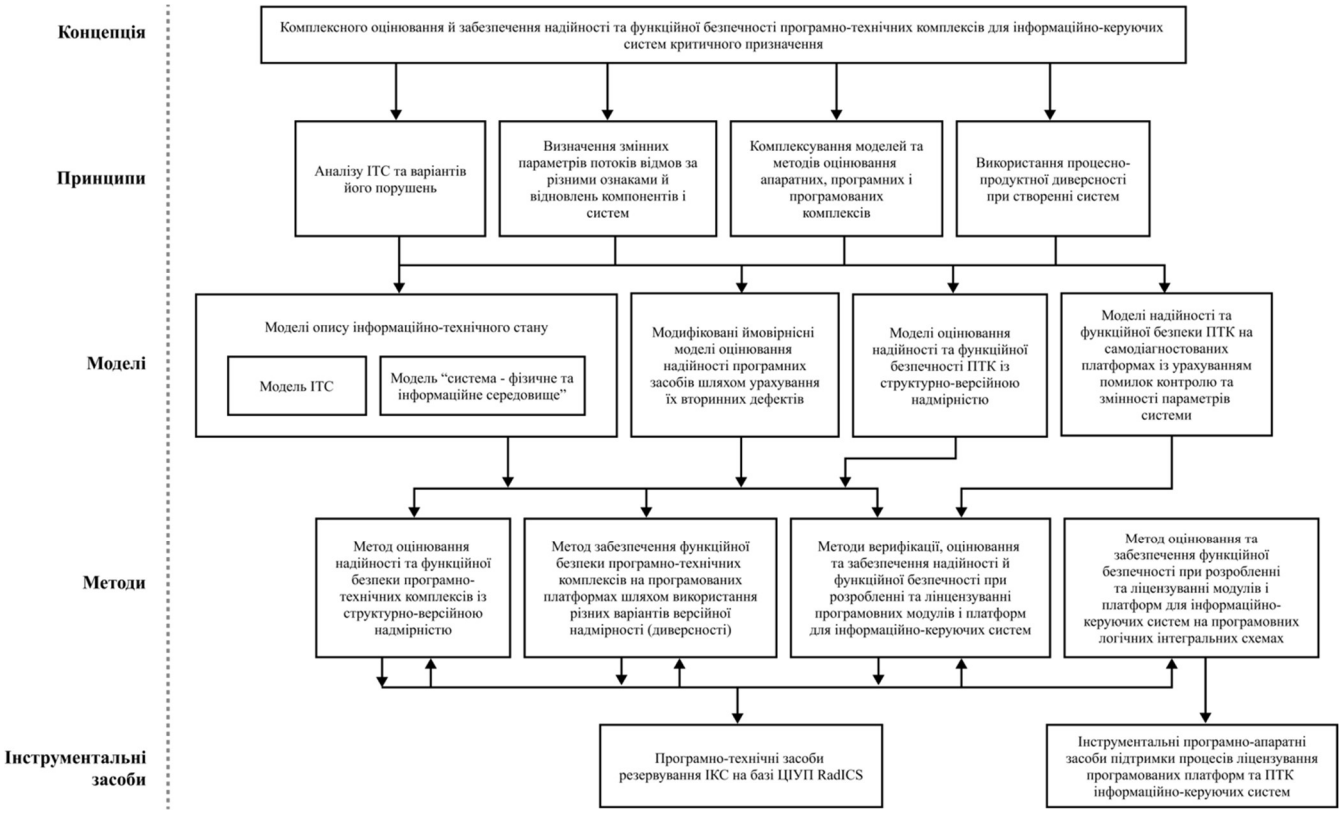

Рис. 2 Структура методології оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів з урахуванням проєктних і фізичних дефектів

$$E_{int}(t) = \{E_{int.phs}(t), E_{int.des}(t)\}, \quad (3)$$

де $E_{int.phs}(t)$ – вектор внутрішніх фізичних впливів на систему, який обумовлює виникнення або прояв фізичних дефектів (ДФ) апаратних засобів; $E_{int.des}(t)$ – вектор внутрішніх проектних впливів, який обумовлює прояв проектних дефектів (ДП) програмних (ДПП) і апаратних (ДПА) засобів.

$$E_{ext}(t) = \{E_{ext.inf}(t), E_{ext.phs}(t)\}, \quad (4)$$

де $E_{ext.inf}(t)$ – вектор зовнішніх інформаційних впливів (ДВІ), $E_{ext.phs}(t)$ – вектор зовнішніх фізичних впливів.

Реакція системи на внутрішні і зовнішні фізичні впливи проявляється тим, що система формує помилкову вихідну інформацію в даний момент часу або один з наступних моментів часу. Реакція системи на зовнішні інформаційні впливи проявляється тим, що порушується внутрішня інформація, що циркулює або зберігається в системі, або середовище (зовнішня система) отримує несанкціонований доступ до цієї інформації в даний або один з наступних моментів часу. Тоді вектор стану системи в момент $t+\Delta t$ можливо записати:

$$S(t+\Delta t) = \{S_{Eint}(t+\Delta t), S_{Eext}(t+\Delta t)\} \quad (5)$$

Модель «система-фізичне та інформаційне середовище» деталізовано моделлю інформаційно-технічного стану:

$$S(t+\Delta t) = \{S_{tec}(t+\Delta t), S_{inf}(t+\Delta t)\} \quad (6)$$

де $S_{tec}(t+\Delta t)=\{S_0(t)//\{E_{int.phs}(t), E_{int.des}(t), E_{ext.phs}(t)\}\}$ – технічний стан, $S_{inf}(t+\Delta t)=\{S_0(t)//E_{ext.inf}(t)\}$ - інформаційний стан. При $E_{int}(t) = Ø$, $E_{ext}(t) = Ø$ $S(t+\Delta t) = S_0(t)$ і стан $S(t+\Delta t)$ є справним ІТС, при якому виконуються всі вимоги до системи. При $E_{int}(0) \neq Ø$, $E_{ext}(0) \neq Ø$ стан $S(t+\Delta t)$ є непрацездатним. Модель ІТС дозволила визначити розширену множину станів, які враховуються в подальшому моделюванні. Відповідно це множини: $MS_0(t) = MS_{0tec}(t) \cap MS_{0inf}(t)$ –справних ІТС; $MS_П(t) = MS_{Птес}(t) \cap MS_{Пinf}(t)$ – працездатних ІТС; $MS^i_{чПtec}(t) = U\ MS^i_{чПtec}(t)$ – частково працездатних технічних станів; $MS_{чПinf}(t) = U\ MS^j_{чПinf}(t)$ - частково працездатних інформаційних станів; $MS_{ПНtec}(t) – MS_{ПНinf}(t)$ - інформаційних технічних; $MS_{ПНinf}(t)$ - $MS_{ПНinf}(t)$ - інформаційних. До складу $MS_{ПН}(t)$ входять: $MS_{НРБtec}(t)$, $MS_{НРБinf}(t)$ – непрацездатні, але безпечні стани. До складу $MS_{НРБ}(t)$ входять: $MS_{НРНБtec}(t)$, $MS_{НРНБinf}(t)$ – непрацездатні, небезпечні (аварійні або критичні).

За результатами досліджень обгрунтовано концепцію, принципи, комплекс моделей і методів, які утворюють структуру методології оцінювання і забезпечення надійності та функційної безпечності ПТК ІКС критичного призначення. З метою розширення простору станів, які враховуються в процесі оцінювання показників надійності і функційної безпечності введено поняття інформаційно-технічного стану. В наслідок цього отримана модель ІТС, яка дозволила розробити моделі і методи оцінювання надійності і функційної безпечності ПТК ІКС з урахуванням впливу зовнішніх і внутрішніх факторів з різним ступенем їх урахування та деталізації.

Таким чином, в розділі отримано перший науковий результат, а саме методологію оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушень внаслідок проектних і фізичних дефектів і дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і повне виконання вимог до відповідних показників.

Основні положення розділу викладені у публікаціях автора [8, 11, 13, 16, 47, 48, 50, 56, 60, 62].

Третій розділ присвячено розробленню моделей оцінювання надійності програмних засобів (МНПЗ) (англ. SRGM Software Reliability Growth Models).Спираючись на досвід розроблення, рефакторинга та тестування програмних проєктів і базуючись на твердженні про внесення вторинних дефектів ПЗ в ході реалізації цих процесів розроблено множину сценаріїв внесення-усунення вторинних дефектів, що дало можливість виконати уточнення поведінки ПЗ в умовах відповідного сценарію за рахунок перебору співвідношень параметрів, що

сценарій описують. З метою аналізу впливу процесів внесення-усунення вторинних дефектів на кількісні значення надійнісних параметрів ПЗ постало завдання вибору типу SRGM. Для цього було виконано аналіз SRGM різних класифікаційних ознак (емпірічних, статистичних, ймовірнісних), який дозволив сформулювати висновок про те, що для оцінювання надійності ПЗ з урахуванням фактора вторинних дефектів доцільно використовувати імовірнісні моделі, оскільки вони містять параметр, який характеризує інтенсивність їх прояву, яка обчислюється за допомогою функції ризику моделі. Виконано спрямований аналіз з метою вибору функцій ризику моделей, які можливо модифікувати для урахування встановленого фактору. За результатами цього аналізу обрано та модифіковано функції ризику наступних SRGM: Джелінського-Моранди; Муси; простої експоненційної; Шика-Уолвертона.

Модифікацію виконано за рахунок включення параметра n^{in} – кількості вторинних дефектів, де складовими функцій ризику є наступні величини: N_d - залишкове число ДППЗ після розробки і тестування; К - коефіцієнт пропорційності; t – довільна точка часу між виявленням (i-1)-го та i-го ДППЗ; $N(t)$ – число виявлених ДППЗ до моменту часу t; X_i – час тестування від t_{i-1} (час виявленя i-1 дефекту ПЗ) до t_i; F_{i-1}- загальна кількість скорегованих дефектів к моменту часу t_i. Модифіковані функції ризику представлено в таблиці 1.

Таблиця 1

Модифікація функцій ризику ймовірнісних МНПЗ

МНПЗ	Функції ризику	Модифіковані функції ризику
Джелінського-Моранди	$\lambda(t)=K(N_d-(i-1))$	$\lambda(t)=K(N_d-i+1+n^{in})$
Проста експоненційна	$\lambda(t)=K(N_d-N(t))$	$\lambda(t)=K(N_d-N(t)+n^{in})$
Шика-Уолвертона	$\lambda(t)=K(N_d-i+1)X_i$	$\lambda(t)=K(N_d-i+1+n^{in})X_i$
Модель Ліпова	$\lambda(t)=K(N_d-F_{i-1})$	$\lambda(t_i)=K(N_d-F_{i-1}+n^{in})$
Модель Муси	$\lambda(t)=K(N_d-F_{i-1})$	$\lambda(t_i)=K(N_d-F_{i-1}+n^{in})$

Вихідними даними для обчислення інтенсивності прояву ДППЗ із урахуванням фактору вторинних дефектів є прогнозоване число вторинних дефектів, яке є результатом застосування розробленої послідовності прогнозування кількості вторинних дефектів за результатами збору статистичних даних про прояв «первинних дефектів». Алгоритм цієї послідовності складається з наступної послідовності етапів: збору статистичних даних про ДППЗ; побудови кореляційного поля, а саме залежності числа ДППЗ від часу; визначення рівняння лінії регресії; визначення вибіркового коефіцієнту кореляції; обчислення прогнозованого числа дефектів на інтервалах часу, що досліджується.Дану послідовність застосовано для прогнозування кількості вторинних дефектів за результатами функціонального тестування (поведінкового тестування) електронного проекту модуля LM (Logic Module) цифрової інформаційно-керуючої платформи (ЦІКП) RadICS. Кореляційне поле статистики дефектів наведено на рис. 3. За допомогою метода найменших квадратів визначено рівняння лінії регресії:

$$y = 12.66/x + 2.31 \quad (7)$$

Лінія регресії за даними кореляційного поля має вигляд (рис. 4).

Шукана величина n^{in} обчислюється за виразом (8):

$$\delta = \left| y - \frac{a}{x} - b \right| - \frac{1}{n+1-x}\sigma_y, \quad (8)$$

де y - дослідне число виявлених дефектів за інтервал часу; x – номер інтервалу часу (в місяцях); a, b – коефіцієнти рівняння лінії регресії; n – число інтервалів часу, що досліджуються; σ_y - середнє квадратичне відхилення по y; δ - шукана величина відхилення (n^{in} - шукана величина відхилення округлена до цілого).

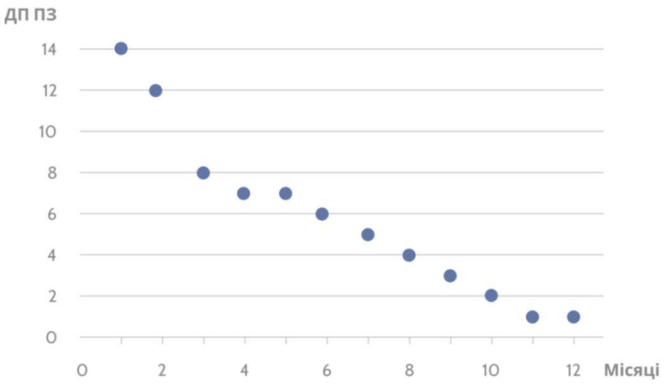

Рис. 3 Кореляційне поле статистики дефектів

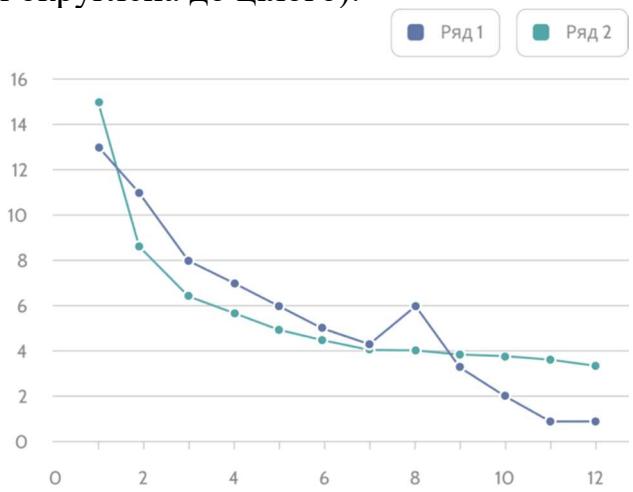

Рис. 4 Лінія регресії (ряд 2)

Результати розрахунку числа вторинних дефектів наведено в таблиці 2.

Таблиця 2

Результати розрахунку числа вторинних дефектів

x	y	$a+\frac{b}{x}$	$\left\|y-a-\frac{b}{x}\right\|$	$\left\|y-a-\frac{b}{x}\right\|-\frac{1}{13-x}\sigma_y$	n^{in}
1	13	14,96916	1,969157	1,667813	2
2	11	8,639352	2,360648	2,031909	2
3	8	6,529417	1,470583	1,10897	1
4	7	5,474449	1,525551	1,123758	1
5	6	4,841469	1,158531	0,706515	1
6	5	4,419482	0,580518	0,063928	
7	4	4,118063	0,118063	–0,48463	
8	6	3,891998	2,108002	1,384776	1
9	3	3,71617	0,71617	–0,18786	
10	2	3,575508	1,575508	0,370132	
11	1	3,460421	2,460421	0,652356	
12	1	3,364514	2,364514	–1,25161	

Далі, використовуючи отриману оцінку кількості вторинних дефектів за допомогою модифікованих моделей здійснюється оцінювання інтенсивності прояву

ДППЗ, яка є одним із параметрів, що використовується в оцінюванні надійності і функційної безпечності ПТК ІКС в цілому. Інтенсивності ДППЗ обчислені з використанням МНПЗ Джелінського-Моранди. Результати наведено в таблиці 3.

В додаток до цього результату запропоновано варіанти комплексування SRGM, які на основі запропонованого принципу комплексування моделей, дозволяють поєднати переваги моделей різних класифікаційних ознак. Прикладами такого комплексування є послідовне використання моделей М. Холстеда (емпірична), М.Мілса (статистична), Дж Д. Муси (ймовірнісна) та М. Холстеда, моделі фірми IBM (емпірична), Джелінського-Моранди (ймовірнісної). У варіантах комплексування також застосовано модифіковані ймовірнісні моделі. Отримані модифіковані МНПЗ, послідовність прогнозування кількості вторинних дефектів ПЗ та варіанти комплексування моделей дозволили отримати уточнені значення інтенсивностей прояву ДППЗ та підвищити точність оцінок надійності та функційної безпечності ПТК в цілому.

Таблиця 3

Результати розрахунку інтенсивності прояву ДППЗ λ_d

Інтервал часу	Виявленні дефекти	Прогнозоване число вторинних дефектів	λ_d без урахування вторинних дефектів	λ_d з урахуванням вторинних дефектів
1	13	2	0,01358	0,013979
2	11	2	0,011183	0,011583
3	8	1	0,009286	0,009486
4	7	1	0,007788	0,007988
5	6	1	0,00649	0,00669
6	5		0,005392	0,005392
7	4		0,004493	0,004493
8	6	1	0,003495	0,003694
9	3		0,002596	0,002596
10	2		0,002097	0,002097
11	1		0,001797	0,001797
12	1		0,001598	0,001598
Середня інтенсивність прояву дефектів			0,005816	0,005949
Середня зміна інтенсивності прояву дефектів			0,001089	0,001126

Таким чином, в розділі отримано другий новий науковий результат, а саме ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та аналізу різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання кількісних показників.

Основні положення розділу викладені у публікаціях автора [8, 10, 12, 15, 16, 18, 29, 47, 48, 50, 52, 57, 57-59, 64, 65].

Четвертий розділ присвячено розробленню моделей та методу оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю. Було виконано систематизацію змінних параметрів, що враховують відповідні моделі (рис. 6). Систематизацію виконано за послідовністю: множина дефектів – група змінних параметрів відповідної множини дефектів – групи причин дефектів –

коефіцієнти зміни. Для множин обраних дефектів у спрощеному вигляді причинно-наслідкові зв'язки дозволяють описати узагальнені моделі зміни параметрів.

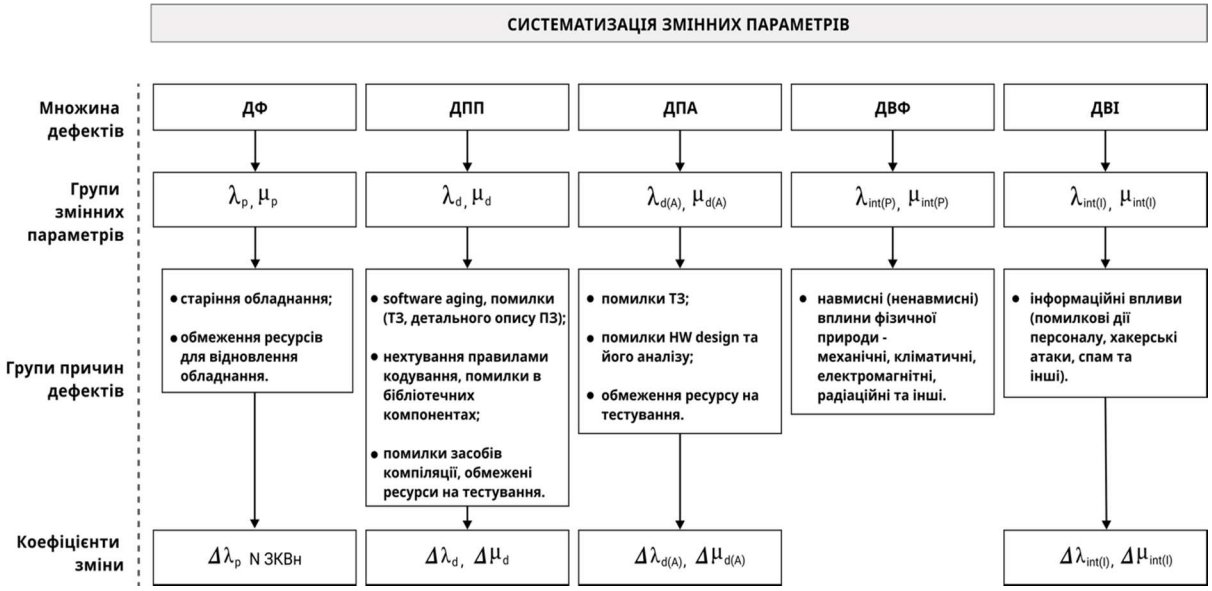

Рис. 5 Систематизація змінних параметрів

Процес прояву, усунення та зміни параметрів дефектів проектування λ_d (9) і λ_{int} (10), де λ_{int} є узагальненим виразом інтенсивності прояву групи дефектів взаємодії (ДВ):

$$\lambda_d(t_i + 1) = \lambda_d(t_i) - \Delta\lambda_d \quad (9)$$

$$\lambda_{int}(t_j + 1) = \lambda_{int}(t_j) - \Delta\lambda_{int}\ , \quad (10)$$

де $\Delta\lambda_d$ і $\Delta\lambda_{int}$ – величини зміни відповідних параметрів після усунення дефекта, який проявився.

Крім переліченої множини дефектів на надійність та функційну безпечність мають вплив існуючі вразливості, тобто «мякі» дефекти, використання яких може порушити працездатність. Було розроблено узагальнену модель прояву дефектів та вразливостей, яка описує можливі сценарії порушення працездатності досліджуваних систем (рис. 6), в якій впливи на систему та її реакція позначені наступним чином: X(t) – вихідні дані, які викликають вірну реакцію системи Z(t); $X(t_i)$ - вихідні дані, які викликають прояв дефекту та ініціюють вихідну реакцію, яка відрізняється від очикуваної $Z_p(t_i) \neq Z_0(t_i)$; $A(t_j)$ атака на вразливість, які ініціюють вихідну реакцію, відрізняється від очикуваної $Z_p(t_j) \neq Z_0(t_j)$.

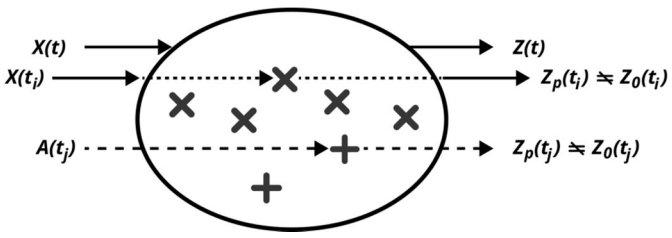

Рис. 6 Модель прояву дефектів та вразливостей

Спираючись на узагальнені моделі розроблено сценарії зміни параметрів в моделі, які базуються на їх комбінаціях параметрів моделей та величинах змін. Це дозволило перейти до розробки множини базових макромоделей, які є макромоделями для типових архітектур ПТК ІКС з фіксованими варіантами зміни параметрів потоків відмов і відновлень їх програмно-апаратних засобів. Макромоделі дозволили розробити та класифікувати

багатофрагментні марковські моделі (БММ), де під БММ розуміється, деталізований марковський граф, що складається із множини внутрішніх підграфів (фрагментів) Моделі було прокласифіковано за наступними ознаками: число зв'язків між фрагментами (моделі можуть бути однозв'язковими або багатозв'язковими); характер зв'язків між фрагментами (лінійні моделі та деревоподібні); структура фрагментів (однорідні та неоднорідні); кількості фрагментів (випадковою або детермінованою кількістю). Дані моделі дозволили досліджувати надійність та функційну безпечність ПТК ІКС як функції часу в умовах зміни обраної множини параметрів.

Прикладом із розробленої множини БММ є модель для архітектури двоканального двохверсійного ПТК аварійного та попереджувального захисту (АЗ ПЗ) з двокаскадною схемою голосування (перший каскад голосування 2/3, другий каскад голосування 1/2) виробництва ТОВ «НВП «Радій» м. Кропивницький.

Архітектура такого ПТК наведено на рис. 7.

Даний комплекс використовує дві функціонально ідентичні версії ПЗ (V1, V2). Дана архітектура ПТК є однією з базових для побудови ІКС АЕС. На даний момент ПТК АЗ-ПЗ успішно експлуатується на блоках №1 та №3 Запорізької АЕС (3 комплекти), блоці №3 і №4 Рівненської АЕС (3 комплекти), блоці №1 та №3 Южно-Української АЕС (2 комплекти). До складу ПТК входе два комплекти обладнання, кожний із яких має у своєму складі:

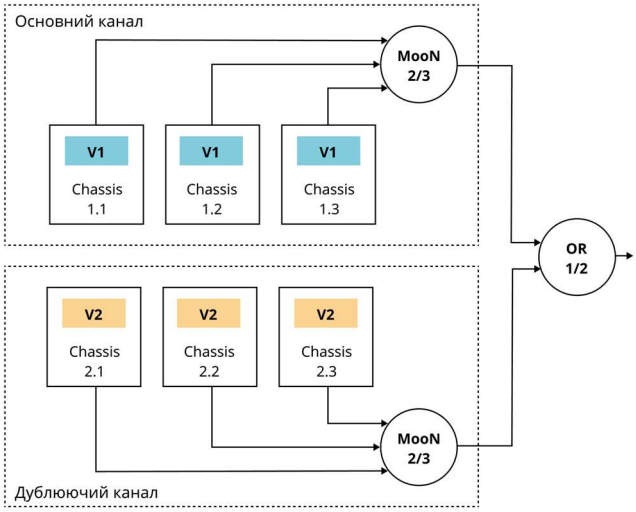

Рис. 7 Архітектура двоканального 2-версійного ПТК АЗ ПЗ з 2-каскадною схемою голосування (2-з-3 та 1-з-2)

- три ідентичних шафи формування сигналів, які утворюють три незалежні канали захисту та взаємно резервують один одного:
- кросова вихідна шафа, яка формує вихідні сигнали комплекту на основі даних отриманих від шаф формування сигналів;
- робоча станція, що архівує, відображає й реєструє дані;
- автоматизоване робоче місце оператора, призначене для відображення контрольованих параметрів, станів дискретних входів і виходів, а також причин, що викликали спрацьовування захистів. Структурна схема надійності (ССН) такого комплексу наведена на рис. 8.

Для розроблення БММ задіяно наступний сценарій зміни параметрів у відповідності до якого величина зміни інтенсивності прояву ДП ПЗ ($\Delta\lambda_d$) є сталою для кожного фрагмента, $\Delta\lambda_{di}$ = const, і $\in 1\ldots N$, де N – кількість фрагментів. Задіяна наступна система означень системи $S^{p}{}_{22}$ ($S^{x3}{}_{x1x2}$): S (ознака архітектури системи), x1 – кількість апаратних каналів; x2 – кількість версій ПЗ; x3 – ознака наявності програмно-апаратних засобів канального реконфігурування. Макрограф БММ наведено на рис. 9.

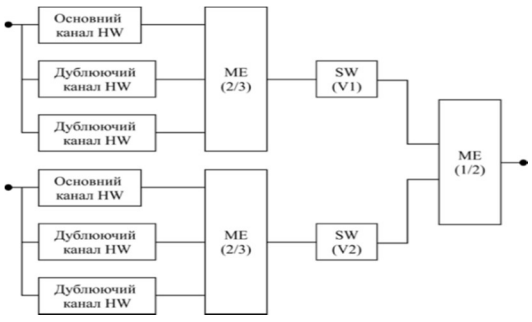

Рис. 8 ССН ПТК «2-з-3» та «1-з-2»

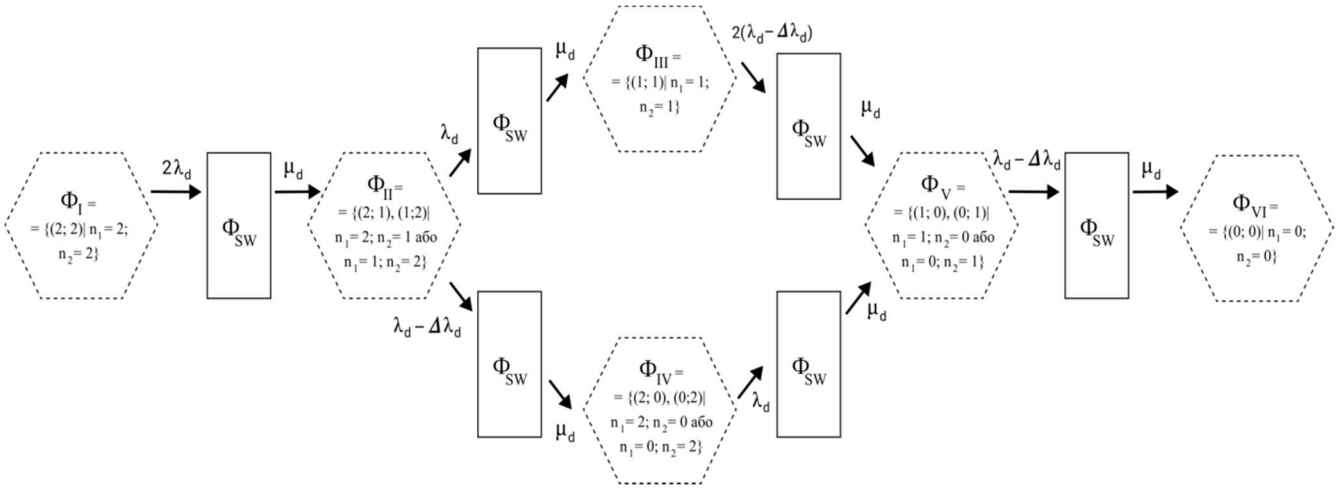

Рис. 9 – Макрограф ББМ 2-версійної ПТК з 2-каскадною логікою «2-з-3» та «1-з-2»

Модель складається із множини фрагментів: першого фрагменту Φ_I, внутрішніх фрагментів Φ_{II} - Φ_{VI}, та внутрішніх фрагментів Φ_{SW}, який розподілений між Φ_I - Φ_{VI} та включає в себе множину станів у яких проявився ДППЗ. БММ, що враховує зміну та усунення проєктних дефектів в обох комплектах комплексу наведено на рис. 10.

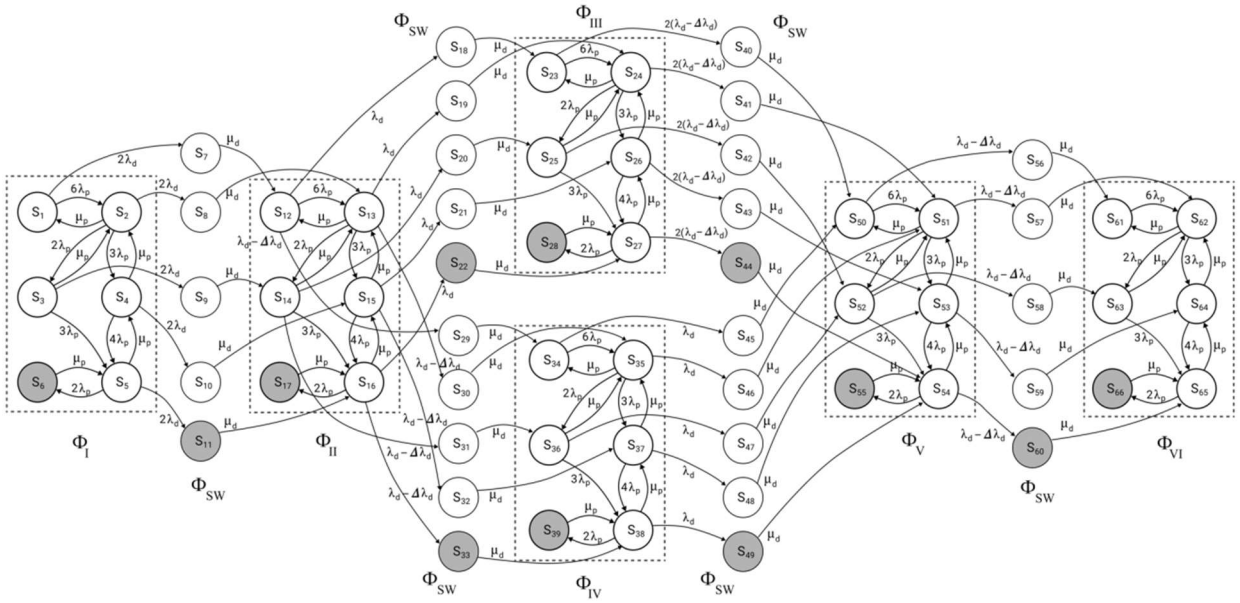

Рис. 10 ББМ двоверсійної ПТК з двокаскадною логікою «2-з-3» та «1-з-2»

Результати обчислення функції готовності наведено на рис. 11, кількісні значення параметрів дано у таблиці 4.

Таблиця 4

Кількісні значення інтенсивностей відмов і відновлень ПТК АЗ і ПЗ

№ п/п	λ_d, 1/год	$\Delta\lambda_d$, 1/год	λ_p, 1/год	μ_d, 1/год	μ_p, 1/год
1	0.00001	0.000005	0.0001	0.01	1
2	0.000025	0.0000125	0.0001		
3	0.00005	0.000025	0.0001		
4	0.000075	0.0000375	0.0001		

Графіки функції готовності для трьохканального двоверсійного ПТК з двокаскадною архітектурою «1-з-2» та «2-з-3» наведено на рис. 12.

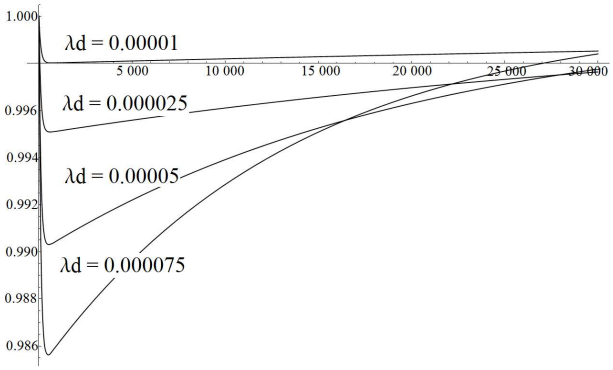

Рис. 11 Результати оцінювання надійності двоверсійного ПТК з двокаскадною архітектурою «2-з-3» та «1-з-2»

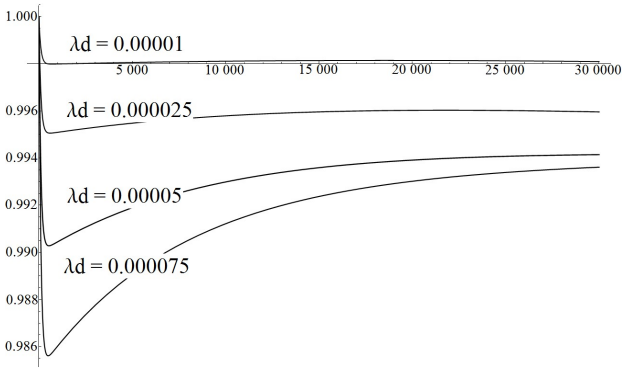

Рис. 12 Результати оцінювання надійності двоверсійного ПТК з двокаскадною архітектурою «1-з-2» та «2-з-3»

Аналіз результатів моделювання для двохкаскадних архітектур «2-з-3» та «1-з-2» і «1-з-2» та «2-з-3» виявив наступні особливості. Перша архітектура демонструє більш високу швидкість зростання функції готовності для однакових значень параметрів у порівнянні з другою і відповідно більші фінальні значення шуканого показника. Трьохканальна архітектура демонструє більш швидкий перехід до сталого стану за шуканою функцією.

Виконані дослідження базових архітектур ПТК дозволили побудувати їх пріоритетні ряди (рис. 13), де під цим терміном розуміється послідовність архітектур побудована за зростаючими кількістними значенями показників надійності та функційної безпечності.

Аналіз наведених вище пріорітетних рядів дозволяє сформулювати наступні висновки. Найкращий результат за значеннями обчислених показників в усьому діапазоні застосованого параметру демонструє дубльована двохверсіна архітектура з засобами реконфігурації. Крім того, за умови застосування різних програмних версій, достовірність виявлення дефектів для такої архітектури є високою.

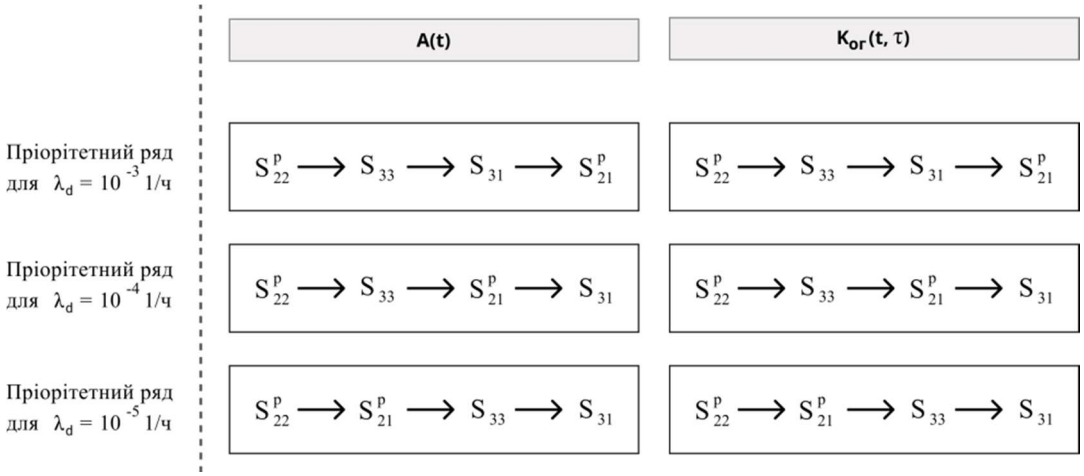

Рис. 13 Пріоритетні ряди базових архітектур побудови ПТК для функцій готовності і оперативної готовності

Далі за пріоритетом кращий результат демонструє мажоритарно резервована архітектура, хоча із зменшенням значення λ_d її випереджає дубльована одноверсійна архітектура з вбудованими засобами реконфігурації.

Основними перевагами розроблених моделей і метода є наступні:

систематизація змінних у часі параметрів моделей дозволяє врахувати зміну кількості дефектів та одержати більш точні показники надійності та функційної безпечності ПТК; отримані сценарії зміни параметрів ПТК з різною архітектурою дозволяють підвищити адекватність розроблених моделей з метою отримання більш точних результатів обчислення шуканих показників; множина багатофрагментних макромоделей та марковських моделей, які побудовано для множини базових архітектур ПТК ІКС дозволяє розмістити їх у пріоритетному порядку та надати рекомендації особі, що приймає рішення щодо структурно-версійної їх побудови для забезпечення необхідного рівня надійності та функційної безпечності.

Таким чином, в розділі отримано новий науковий результат, а саме метод оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю, який на відміну від відомих враховує різні сценарії зміни параметрів потоків відмов і відновлень програмних, програмовних і апаратних засобів, що забезпечує підвищення точності розрахунку функції готовності та імовірності відмов за загальною причиною

Основні положення розділу викладені у публікаціях автора [1 – 3, 6, 9, 16, 17, 18, 21, 22, 23, 24, 28, 31, 35, 61, 64, 65].

П'ятий розділ присвячено розробці моделей оцінювання готовності та функційної безпечності ПТК на самодіагностованих платформах (СДПП). СДПП (англ. SDPP - Self-diagnostic Programmable Platform) це трійка – SDPP = {SPM, SCF, SD}, де SPM - множина програмовних модулів платформи (англ. SPM – Set of Programmable Module) , SFC - множина функцій конфігурування (англ. SCF – Set of Configuration Functions, SD – множина дефектів (англ. Set of defects). Розглянуто СДПП на ПЛІС, як такі, що найбільш ефективним засобом реалізують функції захисту, блокувань, управління та регулювання. Використання ПЛІС для ПТК ІКС дозволяє на етапі проектування закласти алгоритми самодіагностування, які виконуються окремою функціональною підсистемою, яка називається системою контролю і діагностики (СКД). В результаті дослідження моделі СКД програмовної платформи на основі СДПП встановлено, що її складові (програмно-апаратні модулі) можуть бути представлені у вигляді структурної схеми, де центром інформаційного обміну є логічний модуль (англ. LM – Logic Module) та діагностичний модуль(англ. DM - Diagnostic Module) (рис. 14).

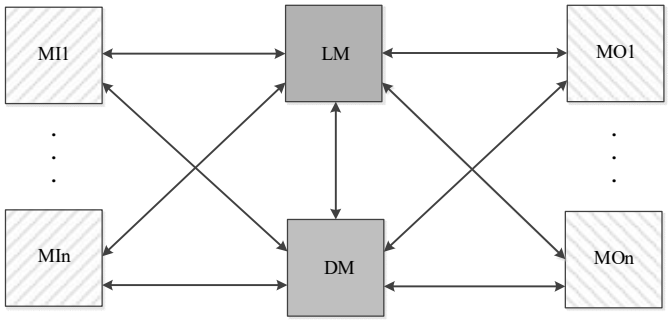

Рис. 14 Структура СДПП

Множиною модулів є: M = {LM, DM, MI, MO}, де LM логічний модуль, DM – діагностичний модуль, MI = {MI1,...,MIi,...,MIN} – множина модулів входу (англ. MI – Module Inputs), SOM = {MO1,...,MOi,...,MON} - множина модулів виходу (англ.SOM – Set of Ouputs Modules).

Дана модель СКД для СДПП враховує наступні види самодіагностики (рис. 15):

- HW SD (Hardware Self-Diagnostics) – вбудована апаратна самодіагностика, яка поділяється на HWU SD (HW Units SD)– самодіагностика рівня вузла модуля, HWM SD (HW Modules SD)– самодіагностика рівня модуля;
- IF SD (Interfaces SD) – програмна самодіагностика для інтерфейсів передачі

даних, яка включає DTP SD (Data Transmission Protocols)–самодіагностика для протоколів передачі даних.

- вбудована програмна самодіагностика для електронних проектів ED (Electronic Design SD) ПЛІС, яка поділяється на RAD SD (Random Access Data SD)–самодіагностика даних, що зберігаються в оперативній пам'яті ПЛІС; PD SD (Packet Data SD) – самодіагностика пакетів даних; MED SD (Modules Electronic Design SD) – самодіагностика електронного проекту модуля. У відповідності із прийнятим підходом на поділ відмов на безпечні і небезпечні було визначено множина і підмножини таких відмов, а саме: M_{DD} – множину небезпечних детектованих СКД відмов (detected dangerous_failure), M_{DU} – множину небезпечних недетектованих відмов (undetected dangerous failure). Означені відмови характеризуються параметрами λ_{DD} и λ_{DU} (інтенсивностями небезпечних детектованих та не детектованих відмов). Оцінювання цих параметрів здійснюється за процедурою аналізу видів і наслідків відмов, їх ефектів та діагностики (англ. FMEDA – Failure Mode Effect and Diagnostic Analysis). Після виділення підмножин небезпечних детектованих і небезпечних детектованих відмов компонент ІКС будується її модель функціонування. Для ІКС з простою структурою інтенсивності відмов системи в цілому визначають як відповідні суми, тобто $\sum\lambda_{DD}$ та $\sum\lambda_{DU.}$

Для випадку, коли відомі значення інтенсивностей відмов і відновлень системи розроблено марковскую модель відмов ПТК в загальному вигляді (рис. 16).

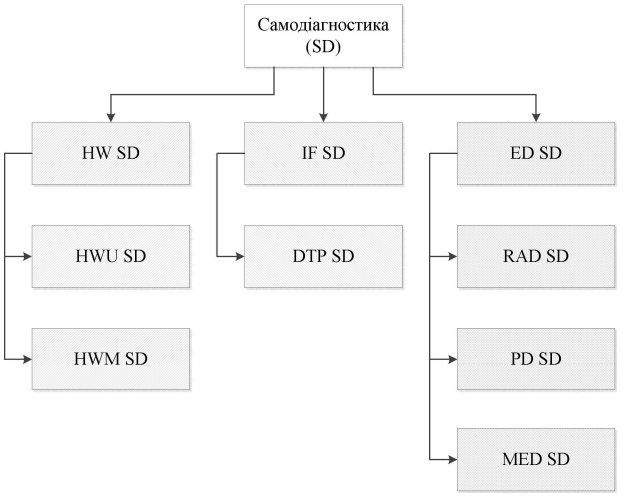

Рис. 15 Класифікація вбудованої самодіагностики ПТК на СДПП

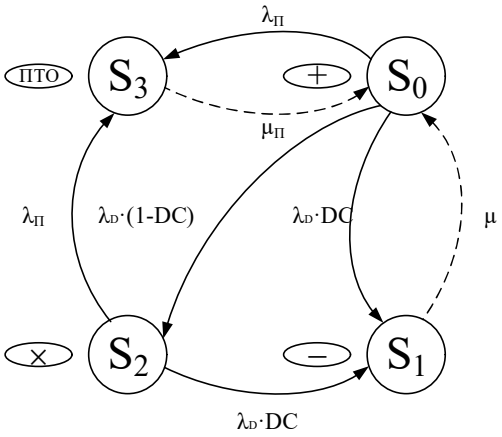

Рис. 16 Марковська модель відмов ПТК

На рис.16 використано наступні позначення: DC – показник діагностичного покриття (diagnostic coverage); S_0 - працездатний стан; S_1 - стан відмови (небезпечна детектована відмова); S_2 - стан прихованої відмови (небезпечна недетектована відмова); S_3 - стан профілактичного технічного обслуговування. Частина небезпечних відмов, що виявляється автоматичними діагностичними тестами в неавтономному режимі визначається як діагностичне охоплення.

$$DC = \frac{\sum_{i=1}^{N} \lambda_{DDi}}{\sum_{i=1}^{N} \lambda_{total_i}} \tag{11}$$

де λ_{DDi} - інтенсивність детектованої небезпечної відмови *i*-го програмно-апаратного юніта та/або модуля; λ_{totali} є сумою λ_{DDi}, λ_{DUi} – інтенсивності недетектованих небезпечних відмов *i*-го програмно-апаратного юніту модуля, λ_{SDi} - інтенсивності детектованих безпечних відмов *i*-го програмно-апаратного юніту модуля, λ_{SUi} - інтенсивності недетектованих безпечних відмов *i*-го програмно-апаратного юніту та/або модуля. Для моделі на рис. 19 використовуються наступні припущення: небезпечні відмови детектуються з ймовірністю виявлення, рівній DC; відмови, недетектовані СКД, виникають з ймовірністю, яка дорівнює доповненню величини діагностичного покриття до одиниці (1 - DC); після прояву відмов, недетектованих СКД, система в подальшому може перейти або в стан відмови, детектованої СКД, (після його прояву) або в стан періодичного технічного обслуговування (ПТО); ПТО проводиться з періодичністю $T_{ПТО} = 1/\lambda_П$, $\lambda_П$ - інтенсивність проведення ПТО та з тривалістю $T_{ПТО} = 1/\mu_П$. Особливістю даної моделі є врахування небезпечного стану, стану недетектованої, тобто прихованої небезпечної відмови, що дає змогу більш точно відслідкувати надійнісну поведінку системи та оцінити показники надійності та функційної безпечності ПТК.

Розроблений підхід, який враховує вплив СКД на рівень надійності і функційної безпечності ПТК, а математичні моделі містять стани прихованих небезпечних відмов було застосовано при розробленні марковських моделей оцінювання надійності та функційної безпечності ПТК для систем нормальної експлуатації (СНЕ) та системи аварійного і попереджувального захисту виробництва ТОВ «НВП «Радій» м. Кропивницький, Україна, архітектура ПТК СНЕ наведена на рис. 17.

Наведена СНЕ, має архітектуру 2oo3. Передбачається, що будь-яке діагностичне тестування тільки фіксує знайдені збої або відмови і не може змінити ні вихідні стани каналів, ні результат. Першим етапом побудови моделей є розробка дерева відмов (ДВ) (рис. 18), де ДВ є діаграмою, яка відображає відмови компонент системи, події або їх комбінації, що призводять до зміни стану системи.

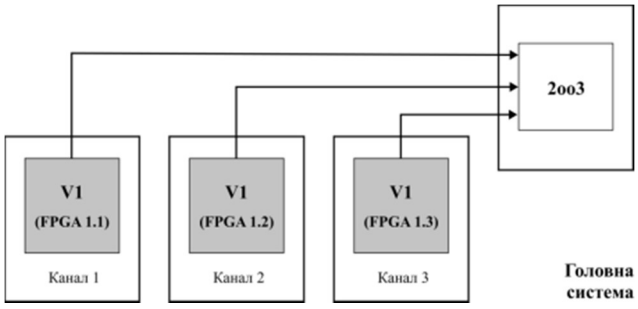

Рис. 17 Архітектура ПТК СНЕ

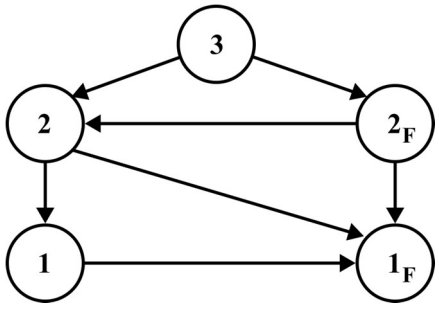

Рис. 18 ДВ СНЕ

Кожна вершина ДВ відповідає конкретному стану системи. Причому кожна система може знаходитись в одному з п’яти станів, а саме: стан 3 – система справна; стан 2 – система працездатна, відмовив канал (система несправна), відмова виявлена і канал відновлюється; стан 1 – система непрацездатна, відмовили два канали,

відмови виявлені і канал відновлюється; стан 2_F – система працездатна, відмовив канал (система несправна), відмова не виявлена і канал не відновлюється; стан 1_F – система непрацездатна, відмовили два канали, виявлена відмова одного каналу і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється.

ДВ відображає переходи із одного вузла в інший і за своєю суттю є першим фрагментом БММ. Далі розроблюється БММ (рис. 19). З'єднуючою ланкою між фрагментами моделі є стани, коли відмовляє ПЗ (стани S_5, S_6, S_7). Суцільною лінією позначені ребра, що визначають перехід за умови прояву відповідного типу дефекту (апаратного або програмного) і показує відмови, а штрихова лінія – відновлення каналу СНЕ.

Вершини БММ СНЕ відповідають функціональним станам системи.

Всі стани діляться на категорії справний стан, працездатний та непрацездатний стани, а саме: стани, в яких система справна (S_0 (3), S_8 (3)); в яких система працездатна (S_1 (2), S_2 (2_F), S_9 (2), S_{10} (2_F)); стани, в яких система непрацездатна (S_3 (1), S_4 (1_F), S_5 (2), S_6 (3), S_7 (2_F), S_{11} (1), S_{12} (1_F)). Більш детальний опис станів є наступний: S_0 (3) – система справна, працюють 3 канали; S_1 (2) – система працездатна, відмовив 1 канал, відмова виявлена і канал відновлюється;S_2 (2_F) – система працездатна, відмовив 1 канал, відмова не виявлена і канал не відновлюється; S_3 (1) – система непрацездатна, відмовили 2 канали, відмови виявлені і канал відновлюється; S_4 (1_F) – система непрацездатна, відмовили 2 канали, відмова одного каналу виявлена і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється;

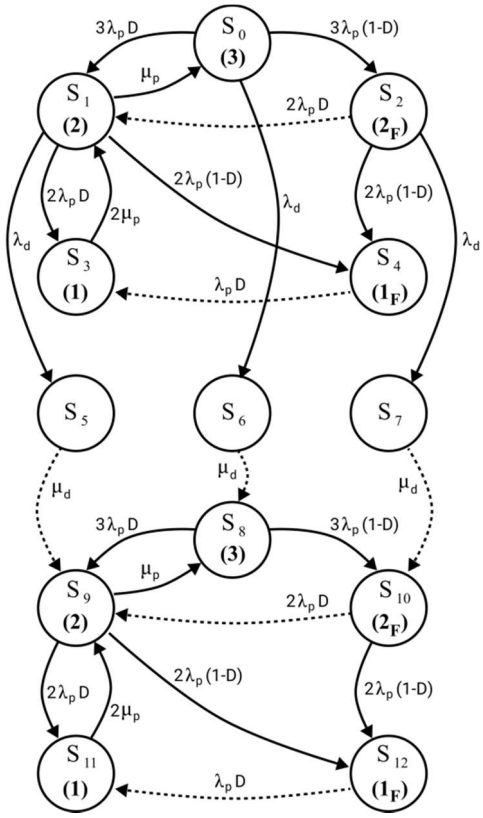

Рис. 19 БММ СНЕ

S_5 (2) – система непрацездатна, при виявленій відмові одного каналу відмовила програмна частина системи, відмова виявлена і програмна частина відновлюється; S_6 (3) – система непрацездатна, при роботі трьох каналів відмовила програмна частина системи, відмова виявлена і програмна частина відновлюється; S_7 (2_F) – система непрацездатна, при невиявленій відмові одного каналу відмовила програмна частина системи, відмова виявлена і програмна частина відновлюється; S_8 (3) – система справна, після відновлення програмної частини системи працюють 3 канали; S_9 (2) – система працездатна, після відновлення програмної частини відмовив 1 канал, відмова виявлена і канал відновлюється; S_{10} (2_F) – система працездатна, після відновлення програмної частини відмовив 1 канал, відмова не виявлена і канал не відновлюється; S_{11} (1) – система непрацездатна, відмовили 2 канали, відмови виявлені і канал відновлюється; S_{12} (1_F) – система непрацездатна, відмовили 2 канали, відмова одного каналу виявлена і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється. Далі відповідно до БММ

складено СДР Колмогорова. За результатами аналізу властивостей матриць коефіцієнтів СДУ (жорсткості, розрідженості, розмірності) було задіяно інструментальні засоби ExpMeth та MATLAB і відповідно використано експоненціальний чисельний метод та метод Рунге-Кутта. Розрахунки виконано на проміжку часу $t \in [0;10000]$ (годин) із точністю $\varepsilon = 10^{-6}$. За подібним алгоритмом досліджено ПТК системи аварійного захисту (САЗ). САЗ має двухкаскадну схему голосування (перший каскад 2/3, другий 1/2). Побудовано ДВ, БММ та отримано оцінки показників надійності та функційної безпечності.

Графіки функції готовності (ФГ) наведені на рис. 20. Результати моделювання отримані за допомогою обох чисельних методів в основному збігаються, за виключенням того, що метод Рунге-Кутта на параметрі *DC=0,99* дає значне відхилення від експоненційного методу на інтервалі інтегрування [0;1000] годин, що може бути в результаті неадаптивного кроку інтегрування, який використовується даним методом. Застосований експоненціальний метод має вбудовану процедуру адаптивного вибору кроку інтегрування. Тому можливий висновок про більш доцільне застосування експонеціального методу на часових інтервалах дослідження систем від 0 до 1000 годин.

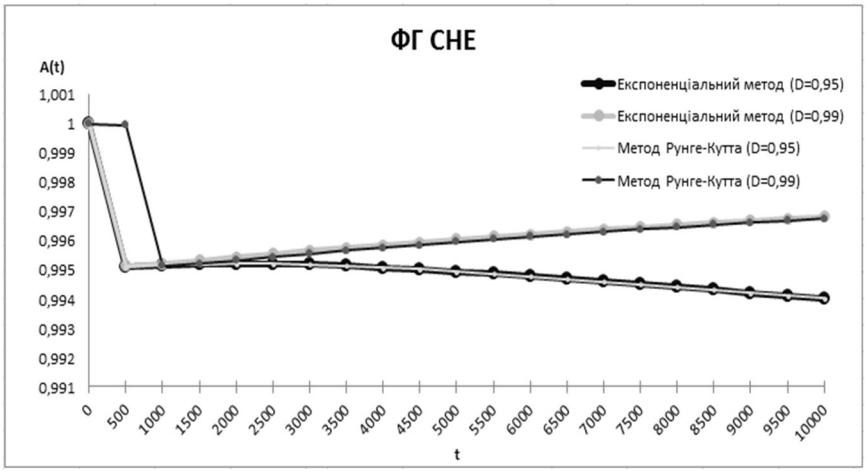

Рис. 20 Функція готовності СНЕ для $DC_1=0,95$ та $DC_2=0,99$

Після 1000 годин спостерігається співпадання результатів обчислень для обох значень параметра DC. За графіками найбільш «сприятливою» при обрахунку обома методами є модель із параметром *DC=0,99*.

Тому справедливим є висновок про необхідність забезпечення високого рівня діагностичного покриття в ході розроблення систем важливих для безпеки. Забезпечення цього досягається за рахунок розроблення концепції програмно-апаратного діагностування на рівні від окремого апаратного компоненту, юніту, модуля, системи до технік розроблення програмного забезпечення з використанням спеціалізованих вбудованих методів самодіагностування.

Розроблені моделі є інструментом метода забезпечення функціональної безпеки ПТК на СДПП.

Таким чином в розділі отримано четвертий і шостий нові наукові результати, а саме: моделі оцінювання готовності та функційної безпечності програмно-технічних комплексів на самодіагностовних платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функційної безпечності, можливість обґрунтування вимог до засобів контролю й діагностування та формування рекомендацій щодо їх виконання; метод забезпечення функційної безпечності

програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною.

Основні положення розділу викладені у публікаціях автора [25, 27, 28, 30, 57, 64, 65].

Шостий розділ присвячено методам верифікації та валідації програмовних платформ і ПТК побудованих на їх основі, а також методу забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах. Виконано модифікацію процедури аналізу видів і наслідків відмов (FMEDA), яка є одним із етапів виконання верифікації і валідації модулів програмовних платформ. Модифікація дозволила покращити ефективність процедури, а саме зменшити обсяг рутинної складної роботи при аналізі простих та складних апаратних компонент вузлів модулів і модулів в цілому за рахунок впровадження засобів автоматизації FMEDA, що дозволило зменшити час на виконання процедури. Було автоматизовано наступні етапи процедури: генерації списків електронних компонент та вузлів схеми; генерації анкети для аналізу режимів відмов; визначення параметрів інтенсивностей відмов (failure rate – λ) для простих та складних апаратних компонент; класифікації встановлених інтенсивностей відмов на множини: λ_{sd} – безпечні діагностовані; λ_{su} – безпечні недіагностовані; λ_{dd} - небезпечні діагностовані; λ_{du} - небезпечні недіагностовані; визначення рівня діагностичного покриття схеми засобами вбудованої самодіагностики; формування фінального звіту FMEDA. Модифікована процедура дозволяє визначити рівні внесення дефектів, саме на рівні ПЛІС; окремих вузлів модуля і модуля в цілому, набору модулів для внесення мультидефектів; на рівні засобів конфігурування системи, що дозволило більш точно встановлювати рівень реалізації підсистем самодіагностування модулів і систем в цілому побудованих на програмовних платформах. Фінальний звіт модифікованої процедури є вихідними даними для розроблених базових методів верифікації і валідації програмовних платформ, які є основою для побудови систем критичного використання і які в свою чергу потребують обов’язкової сертифікації (Safety Integrity Level – SIL сертифікації) на відповідність заданим рівням функційної безпечності, а саме: метода (процедури) із внесенням апаратних дефектів (англ. HW FIT – Hardware Fault Insertion Testing); метода (процедури) із внесенням програмних дефектів (англ. SW FIT – Software Fault Insertion Testing).

Базуються дані методи на введеному понятті FIT – придатності, де FIT – придатність - це придатність системи до ін’єктування дефектів у її електричні схеми та окремі компоненти (HW FIT-придатність) або програмного коду (SW FIT-придатність). Для SIL - орієнтованого процесу сертифікації СДПП концепція SW&HW FIT - придатності визначена як придатність виконати тест на введення (ін'єкцію) за результатами FMEA або FMEDA на різному рівні ієрархії системи: (модуль, підсистема, система) FMEDA; системний SW, реалізований з кодом HDL (Chip) - FMEDA; програми SW -конфігураційні файли, що генеруються інтегрованим середовищем розробки) – FMEA (рис. 21).

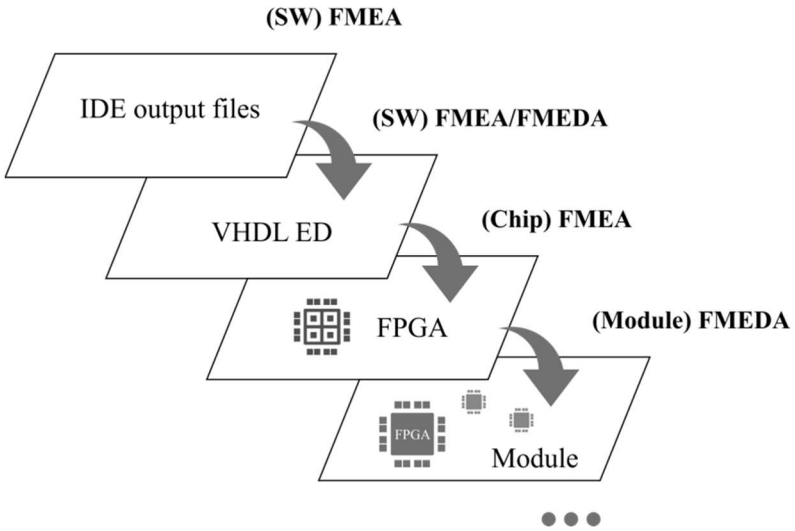

Рис. 21 Рівні внесення дефектів на основі результатів виконання модифікованої процедури FMEDA

Таким чином для HW FIT маємо:

$$FMEDA = (Chip)FMEDA \cup (Module)FMEDA \cup (Cabinet)FMEDA \cup (System)FMEDA, \quad (12)$$

де *(Chip)FMEDA* - виконаний аналіз для ПЛІС, *(Module)FMEDA* – виконаний аналіз для модуля ПЛК, *(Cabinet)FMEDA* - виконаний аналіз для набора модулів, що уможливлює виконання процедури мульті - FIT (одночасне внесення двох і більше дефектів), *(System)FMEDA* – виконаний аналіз для системи в цілому. Наступним кроком процедури є визначення позиції (точки схеми) pf_i та засобів mf_i внесення для всіх встановлених при виконанні FMEDA дефектів f_i. Загалом pf_i і mf_i - це множини $pf_i = \{pf_{ij}\}$, $mf_i = \{mf_{ik}\}$, $j = 1,\ldots, npf_i$; $k = 1,\ldots, nmf_i$ і тоді маємо:

$$\exists i,v,\ i \neq v: pf_i \cap pf_v \neq \varnothing,\ mf_i \cap mf_v \neq \varnothing. \quad (13)$$

Повний простір FIT покриття для дефекта f_i (Full FIT covered space - $FFCSf_i$), є множина, яка є декартовим добутком:

$$FFCSf_i = pf_i \times mf_i.. \quad (14)$$

Повний простір FIT покриття дефектів для схеми (Full FIT covered space of scheme (FFCS)) є об'єднання:

$$FFCSS = \cup FFCSf_i, ,\ i = 1,\ldots,F. \quad (15)$$

Імплементований простір покриття для схеми (Implemented FIT covered space of scheme (IFCS)) є підмножиною *FFCS* і визначається*:*

$$IFCS \subseteq FFCS \quad (16)$$

та має бути розроблений у відповідності до множини обмежень(*r*- restrictions) $FITR = \{r_z\}$ для різних рівнів системи. Цими обмеженнями є : *r1* - параметри елементів не мають змінюватись при температурних та механічних впливах; *r2* - введення дефекту для елемента $a_x \in A$ (у просторі елементів a_x) не має спричиняти новий дефект або неприйнятну зміну параметрів інших елементів a_q; *r3* - будь-який елемент $a_x \in A$ повинен бути технологічно прийнятним для внесення дефекту. Отже, маємо наступне:

$$IFCS = FITR \blacklozenge FFCS, \quad (17)$$

де $\blacklozenge$ - операція фільтрації набору FFCS набором FITR. IFCS описується наборами позицій внесення $Ipf_i = \{Ipf_{ij}\}$ і значень внесення $Imf_i = \{Imf_{ik}\}, j = 1,\ldots, Ipf_i; k = 1,\ldots, nmf_i$. Зрозуміло, що $\forall Ipf_{ij} \subseteq pf_{ij}$, $\forall Imf_{ik} \subseteq mf_{ik}$.

Вихідними даними для процедури SW FIT є результати аналізу видів і наслідків відмов (англ. FMEA- Failure Mode and Effects Analysis). Під час FMEA проводиться аналіз джерел ризиків, які можуть виникнути під час роботи з IDE (Integrated Development Environment) та формування файлів конфігурації програмованого логічного контролера. Результатами цього аналізу є список типів відмов ПЗ. Таким чином для SW FIT маємо:

$$FMEA = \cup(SW\ Components)FMEA, \quad (18)$$

де *SW Components* – є окремими компонентами комплексу ПЗ. Для кожної окремої компоненти визначається підмножина режимів відмов (дефектів) та ефекти їх впливу на працездатність ПЗ та ПЛК в цілому. Кількість підмножин відмов відповідає кількості тестованих компонентів SW. Тоді $F = \{f_i\}$ - це повний набір SW-дефектів, а SWComp = $\{SWComp_i\}$ - множина протестованих компонентів SW. Тоді маєм відображення набору SW компонентів на набір дефектів:

$$f: SWComp \rightarrow F \quad (19)$$

За аналогією з HW FIT, для кожної пари f_i - $SWComp_i$ встановлюється точка внесення дефекту pf_i і значення mf_i цієї вставки. Загалом pf_i and mf_i є множини $pf_i = \{pf_{ij}\}$, $mf_i = \{mf_{ik}\}$, $j = 1,\ldots, npf_i$; $k = 1,\ldots, nmf_i$, і ідповідно повний простір SW FIT покриття дефектів (SW FIT covered space of f_i (Full FIT covered space SW FF_SWCSf_i)) є декартовим добутком:

$$FF\_SWCSf_i = pf_i \times mf_i. \quad (20)$$

Відповідно повний простір SW FIT покриття SW (FF_SWCS) є об'єднання всієї множини FF_SWCSf_i:

$$FF\_SWCS = \cup FF\_SWCSf_i, , i = 1,\ldots,F. \quad (21)$$

Реалізований простір покриття для програмного компонента (IF_SWCS - Implemented SW FIT covered space of component) - є підмножиною FF_SWCS, відповідно IF_SWCS розробляється з урахуванням основного обмеження SW FITR - введення несправності SW для SWComp повинно бути технологічно прийнятним. Дані методи (процедури) було об'єднано в загальний метод верифікації і валідації програмовних платформ і ПТК побудованих на їх основі.

З метою практичної реалізації розроблених методів верифікації і валідації було розроблено низку інструментальних програмно-апаратних засобів підтримки процесів ліцензування програмованих платформ та ПТК ІКС критичного використання, а саме: інструментальні засоби апаратної підтримки виконання HW FIT (тестові панелі), які зазнали декілька етапів еволюції у відповідності до зростаючого функціоналу. Тестова панель V1.0 дозволяє виконувати замикання окремих ланцюгів вузлів окремого електронного модуля ((рис.23 б). Тестова панель V2.0 додатково дозволяє виконувати тести з можливістю зміни електричних параметрів схеми (підвищення, зменшення опору). Панель V3.0 монтується безпосередньо на модуль, що дозволяє виконувати тести для окремого модуля у складі повноцінно діючої платформи (разом з іншими модулями) та розширює можливості виконання мульті - HW FIT; інструментальні засоби програмної підтримки RPCT outputs FIT (RFIT), який дозволяє: виконувати аналіз та редагувати

тестувальником (верифікатором) вміст вихідних файлів, які генеруються спеціалізованим програмним засобом розроблення користувацької логіки ПЛК; перерахунок контрольних сум команд, які редагуються в ході SW FIT; зберігати файли, які містять внесені дефекти; мережевий програмний засіб внесення дефектів, який забезпечує мережеву роботу з компонентами платформи, які оснащені інтерфейсами LAN; формує та надсилає через інтерфейси LAN кадри протоколу, які містять внесені дефекти.

Таким чином отримані моделі, методи і інструментальні засоби дозволяють: забезпечувати етапи тестування програмовних платформ і ПТК, які будуються на їх основі і в ході цього забезпечувати перевірку здатності діагностичних підсистем виявляти різнотипні програмно-апаратні дефекти та ініціювати запуск захисних дій на рівні системи відповідно до типу виявленого дефекту; підтверджувати рівень надійності та функційної безпечності системи, рівень стійкості системи до зовнішніх вторгнень та збільшувати діагностичне покриття в ході тестування.

Отримані в ході попередніх досліджень множини моделей, методів, інструментальних програмно-апаратних засобів було об’єднано у загальний метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем критичного використання на програмовних логічних інтегральних схемах, який об’єднав усі переваги попередніх результатів та дозволив гарантувати виконання вимог національних та міжнародних нормативних документів до рівня функційної безпечності SIL3 (рис. 22).

Системи сертифіковані за даним рівнем функційної безпечності SIL-3 допускаються для побудови систем безпеки і систем важливих для безпеки на об’єктах критичної інфраструктури.

Таким чином в розділі отримано п’ятий і сьомий нові наукові результати, а саме: методи верифікації і валідації програмовних платформ і програмно-технічних комплексів на їх основі, які на відміну від відомих, базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов та ін’єктування фізичних і проєктних дефектів, що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності за рахунок збільшення імовірності виявлення прихованих дефектів; метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах, який на відміну від відомих ураховує фізичні та проєктні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3.

Основні положення розділу викладені у публікаціях автора [19, 20, 33, 34, 39, 40, 42, 43, 45, 48, 62, 63,68].

У додатках наведено: список показників, параметрів, системних позначень та визначень; результати обчислень; документи, що підтверджують практичне значення і впровадження результатів дисертаційної роботи; а також список публікацій.

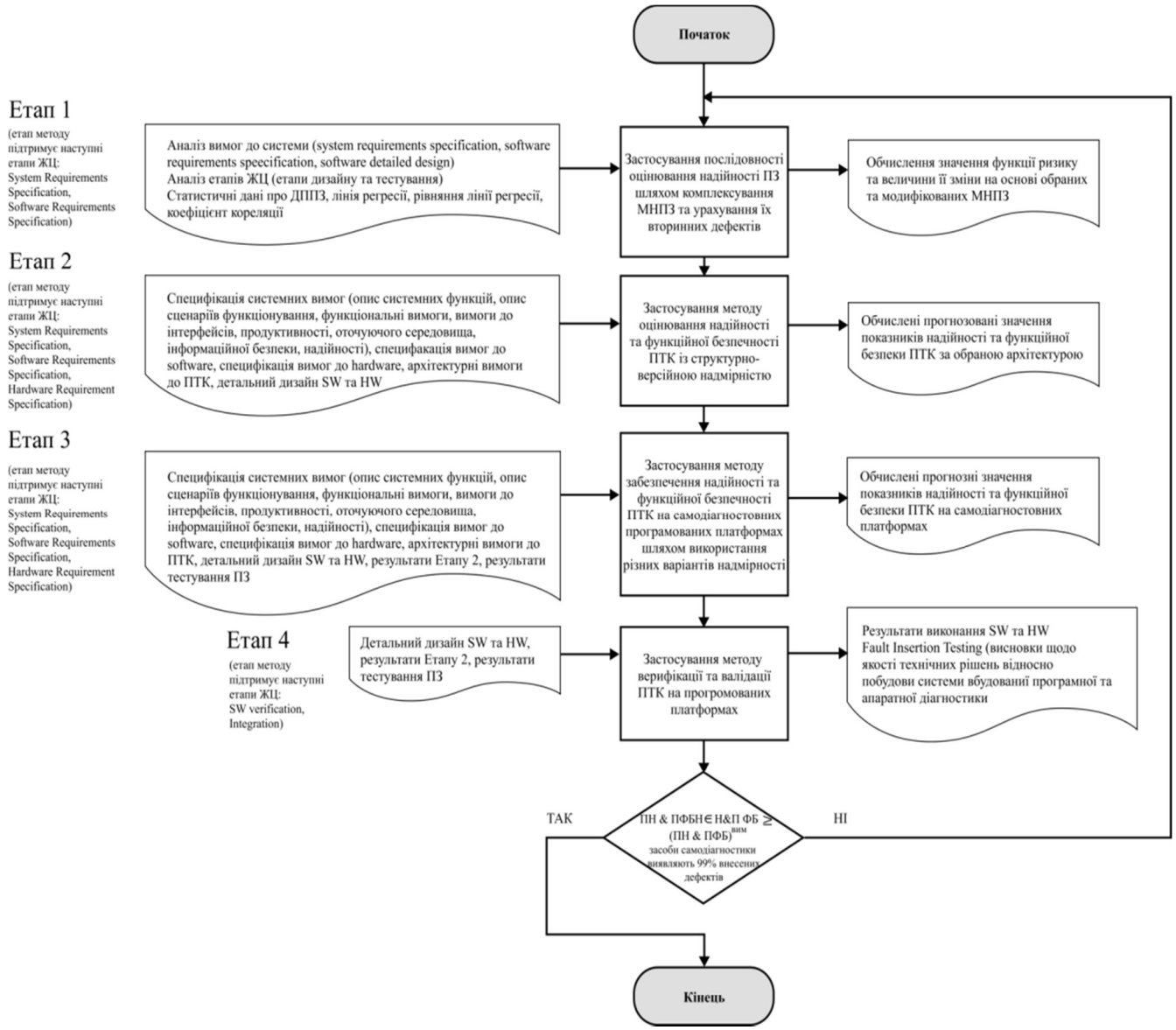

Рис. 22 Алгоритм метода оцінювання та забезпечення надійності і функційної безпечності ПТК ІКС КВ

ВИСНОВКИ

1. У дисертаційній роботі вирішена актуальна науково-прикладна проблема комплексного оцінювання і забезпечення надійності і функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування в процесі розроблення, верифікації, валідації та використання за призначенням з урахуванням відмов, обумовлених проєктними, фізичними дефектами і вразливостями програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень, що полягає у вирішенні об'єктивного протиріччя, а саме в усунені невідповідності між встановленою розширенною множиною причин порушення працездатності програмно-технічних комплексів інформаційно-керуючих систем атомних станцій, аерокосмічних комплексів та інших індустріальних об’єктів критичного застосування внаслідок фізичних і проєктних дефектів їх апаратних, програмних і програмовних компонентів, зміною параметрів потоків відмов і відновлень з одного

боку, і рівнем розвитку концептуальних засад, сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпечності, які не повно враховують причини і характеристики відмов і порушень ПТК, - з іншого боку.

2. У дисертації одержані наступні нові наукові результати:

1) уперше розроблено метод оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю, який на відміну від відомих враховує різні сценарії зміни параметрів потоків відмов і відновлень програмних, програмовних і апаратних засобів, що забезпечує підвищення точності розрахунку функції готовності та імовірності відмов за загальною причиною;

2) уперше розроблено моделі оцінювання готовності та функційної безпечності програмно-технічних комплексів на самодіагностовних платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функційної безпечності, можливість обґрунтування вимог до засобів контролю й діагностування та формування рекомендацій щодо їх виконання

3) уперше розроблено методи верифікації і валідації програмовних платформ і програмно-технічних комплексів на їх основі, які на відміну від відомих, базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов та ін'єктування фізичних і проєктних дефектів, що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності за рахунок збільшення імовірності виявлення прихованих дефектів;

4) уперше розроблено метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах, який на відміну від відомих ураховує фізичні та проєктні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3;

5) удосконалено ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та аналізу різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання кількісних показників;

6) набула подальшого розвитку методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушень внаслідок проєктних і фізичних дефектів і дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і повне виконання вимог до відповідних показників. В рамках методології сформульована концепція комплексного оцінювання й забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного застосування, яка є розвитком концепції синтезу надійних систем із ненадійних компонентів, яку запропонував Джон фон-Нейман, яка розвивається стосовно ПТК ІКС критичного застосування шляхом їх комплексного оцінювання і забезпечення

надійності і функційної безпечності. Концепція базується на принципах:

- аналізу інформаційно-технічного стану та варіантів його порушення, який відрізняється тим, що дозволяє урахувати системні властивості і ознаки як технічного, так і інформаційного характеру, які притаманні системі в певний момент часу;

- визначення змінних параметрів потоків відмов за різними ознаками й відновлень компонентів і систем, який відрізняється тим, що дозволяє виконувати оцінювання надійності і функційної безпечності ПТК ІКС критичного застосування з урахуванням змінності параметрів потоків відмов і відновлень їх програмно-апаратних компонент, спираючись на аналіз опису: системних функцій; сценаріїв функціонування системи; вимог до оточуючого середовища, вимог до інформаційної безпеки; вимог до надійності і функційної безпечності; архітектури системи; детального дизайну програмно-апаратних компонент ПТК;

- комплексування моделей та методів оцінювання апаратних, програмних і програмовних компонент, який відрізняється тим, що дозволяє поєднувати переваги розроблених моделей і методів з метою більш точного оцінювання надійності і функційної безпечності ПТК ІКС критичного застосування;

- використання процесно-продуктивної диверсності при створенні систем, який відрізняється тим, що дозволяє застосовувати різні продуктові (програмно-апаратні) і процесні засоби для реалізації ідентичних функцій з метою розробки ПТК, які є стійкими дефектів різної природи, завдяки: застосуванню в резервованих каналах системи різних програмно-апаратних версій, що знижує імовірність відмови за загальною причиною; застосуванню диверсних незалежних процесів і засобів проєктування і тестування.

7) набув подальшого розвитку метод забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною.

3. Практичне значення одержаних результатів полягає в тому, що розроблені моделі та методи доведено до прикладних інженерних методик та процедур, рекомендацій щодо побудови архітектур ПТК, використанням інструментальних засобів оцінювання, програмно-апаратних засобів забезпечення надійності та функційної безпечності ПТК в організаціях, які займаються розробленням, виробництвом, модернізацією та експлуатацією інформаційно-керуючих систем, важливих для безпеки. Це дозволило покращити показники надійності і функційної безпечності ПТК ІКС, які використовуються у атомній енергетиці, авіаційних системах та інших критичних системах, а також обгрунтувати вимоги до них.

4. Результати досліджень впроваджено в процесі:

- оцінювання надійності і функційної безпечності перспективної цифрової інформаційно-управляючої платформи RadICS в процесі її SIL-3 сертифікації на відповідність вимогам стандарту IEC 61508 («Науково-виробниче підприємство «Радій» (м. Кропивницький));

- розроблення процедур і інструкцій системи менеджменту якості підприємства і виконання низки міжнародних проєктів із розроблення відповідних інформаційно-керуючих систем (I&C Test Platform for Electricite de France, Франція; I&C system of

IEA-R1 Research Reactor Control Console and Nuclear Channels Modernization, Бразилія; Embalse Refurbishment, MCR and SCA Window Annunciators, Аргентина) (Товариство з обмеженою відповідальністю «Науково-виробниче підприємство «Радікс» (м. Кропивницький);

- розроблення бортових інформаційно-керуючих систем для літаків АН-70, АН-148, що підвищило значення показників надійності і функційної безпечності з урахуванням різних типів дефектів і відмов програмно-апаратних засобів, ПЛІС і засобів контролю і самодіагностування (Державне науково-виробниче підприємство «Об'єднання «Комунар» СКБ «Полісвіт»);

- розроблення структур і вимог нормативних документів до ПТК ІКС АЕС, що надало змогу покращити повноту оцінювання і якість відповідних документів (Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки»);

- розроблення технології модельної розробки і тестування апаратного забезпечення (програмовних плат, чіпів, систем електроніки) з використанням комбінації методів машинного навчання та алгебраїчного підходу, що дозволяє звільнитись від суб'єктивності синтезу тестових наборів, підвищити ефективність тестування і відповідно рівень надійності і функційної безпечності (Приватному підприємстві ЛітСофт);

- виконання 5 науково-дослідних робіт за держзамовленням, міжнародних проєктів за програмою Європейського Союзу: «MASTAC» (MSc and PhD Studies in Aerospace Critical Computing, 2006-2009 pp.); «SAFEGUARD» (National Safeware Engineering Network of Centres of Innovative Academia-Industry Handshaking, 2010-2013 pp.); SEREIN» (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains, 2013-2016 pp.); «ERASMUS+ALIOT» (Internet of Things: Emerging Curriculum for Industry and Human Application, 2018-2019 pp.), а також в навчальному процесі для розроблення навчального контенту навчальних дисциплін: «Технології забезпечення якості ПТК»; «Технології проєктування програмних систем»; «Теорія ризиків та технології управління безпекою ІКС»; «Технології розроблення та забезпечення функційної безпеки ІУС» (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»).

5. Виконана в дисертації кількісна оцінка ефективності запропонованих методів, підтверджена результатами практичного впровадження, свідчить про їх переваги, порівняно з існуючими методами, а саме вдосконалено процеси розроблення, верифікації та валідації СДПП і систем, які будуються на їх основі, що забезпечло досягнення системами рівня функційної безпечності SIL-3 і зменьшило відповідно часові і фінансові затрати на ці процеси до 10%; підвищена точність оцінювання та значення показників надійності і функційної безпечності з урахуванням різних типів дефектів і відмов програмно-апаратних засобів бортових ІКС літаків АН-70, АН-148 до 5%; підвищена ефективність тестування (число виявлених дефектів) до 10%.

6. Достовірність нових наукових положень і висновків дисертаційної роботи підтверджується:

- збігом з результатами, отриманими з використанням відомих моделей і методів теорії надійності; обґрунтованістю припущень, прийнятих при розробленні моделей і методів, виходячи з досвіду експлуатації ПТК ІКС;
- працездатністю та ефективністю апаратних рішень та інструментальних засобів, отриманих із застосуванням запропонованих методів і моделей, підтвердженою на низці підприємств;
- результатами практичного використання розроблених моделей, методів та інструментальних засобів при створенні, сертифікації та експлуатації ПТК на програмовних платформах та ІКС різного призначення.

7. Основні положення і результати дисертації можуть бути використані державними та закордонними підприємствами, що виконують розробку, тестування, супроводження і експлуатацію програмно-технічних комплексів інформаційно-керуючих систем критичного застосування.

8. Подальші дослідження слід проводити в наступних напрямках:

- вдосконалення інструментальних засобів виконання процедури аналізу видів, наслідків і критичності відмов з урахуванням ненадійності, що вносять програмні компоненти;
- вдосконалення інструментальних засобів автоматизації процеса прийняття рішень при розробці ПТК ІКС КЗ, а також створення інформаційних технологій підтримки експлуатації систем, важливих для безпеки, атомних станцій, аерокосмічних комплексів та інших індустріальних об’єктів критичного застосування на всіх етапах життєвого циклу.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації:

1. Харченко В.С., Одарущенко О.Н., Поночовный Ю.Л., Одарущенко Е.Б., Скляр В.В. Технологии высокой готовности для программно-технических комплексов космических систем : монография. Харьков, 2010. 372 с. *(Особистий внесок здобувача: моделювання і оцінка готовності ПТК з урахуванням зміни параметрів процессів відмов та відновлень).*

2. Боярчук А.В., Брежнев Е.В., Горбенко А.В., Дубницкий В.Ю., Епифанов А.С., Зайцева Е.В., Засуха С.А., Иванченко О.В., Кочкарь Д.А., Левашенко В.Н., Одарущенко О.Н., Орехов А.А., Резчиков А.Ф., Сиора А.А., Скатков А.В., Скляр В.В., Тарасюк О.М. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : монография. Харьков, 2011. 641с. *(Особистий внесок здобувача: методи визначення параметрів потоків відмов та відновлення ПЗ та величин їх зміни, послідовність розробки і аналіз моделей готовності ІТ-інфраструктур з змінними параметрами).*

3. Одарущенко О.Н., Харченко В.С., Маевский Д.А., Поночовный Ю.Л., Руденко А.А, Одарущенко Е.Б., Засуха С.А., Жадан В.О., Живило С.В. CASE-оценка критических программных систем. Надежность: монография. Т.2. Харьков, 2012. 292с. *(Особистий внесок здобувача: методи контроля випадкових відмов обладнання, методи виключення систематичних відмов обладнання).*

4. Odarushchenko O., Sklyar V., Bulba E., Horbenko R., Ivasyuk A., Kotov D. Assessment of Energy Consumption for Safety-Related PLC-based Systems. *Green IT*

Engineering: Concepts, Models, Complex Systems Architectures, Studies in Systems, Decision and Control series. Springer. Springer International Publishing Switzerland, 2017. P. 269 – 281. *(Особистий внесок здобувача: методика оцінювання енергоспоживання ПЛК).* (Видання входить до міжнародної наукометричної бази Scopus).

5. Odarushchenko, O. Odarushchenko, E, .Butenko, V., Ruchkov, E. Tool-Based Assessment of Reactor Trip Systems Availability and Safety Using Markov Modeling. *Cyber Security and Safety of Nucler Power Plant Instrumentation and Control Systems*. Hershey, Pennsylvania, United States of America, IGI Global, 2020. P. 175-203. *(Особистий внесок здобувача: аналіз недоліків IEC 61508, багатофрагментні марковські моделі та розв'язання систем диференційних рівнянь).*

6. Одарущенко О.Н., Одарущенко Е.Б., Стороженко А.В., Гроза П.Н. Оценка надежности программно-технических комплексов на основе многофрагментных марковских моделей. *Системи обробки інформації*. 2001. Вип. 3(13). С. 110-116. *(Особистий внесок здобувача: багатофрагментна марковська модель).*

7. Одарущенко О.Н., Одарущенко Е.Б., Поночовный Ю.Л. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем. *Авіаційно-космічна техніка і технологія*. 2002. Вип. 35. С. 187-191. *(Особистий внесок здобувача: алгоритм модифікованого експоненційного методу розв'язання систем лінійних алгебраїчних рівнянь).*

8. Одарущенко О.Н., Поночовный Ю.Л. Одарущенко Е.Б. Терминологические аспекты теории надежности программных средств. *Радіоелектронні і комп'ютерні системи*. 2004. Вип. 2(6), С. 88-94. *(Особистий внесок здобувача: визначення термінів дефект ПЗ, відмова ПЗ).*

9. Харченко В.С., Одарущенко О.Н., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов. *Радіоелектронні і комп'ютерні системи*. 2006. Вип. 5(17). С.62-70. *(Особистий внесок здобувача: визначення термінів дефект ПЗ, відмова ПЗ).*

10. Руденко А.А., Одарущенко О.Н., Харченко В.С. Модели оценки надежности программных средств с учетом недетерминированного числа вторичных дефектов. *Радіоелектронні і комп'ютерні системи.* 2010. Вип.6(47). С.197-203. *(Особистий внесок здобувача: МНПЗ з урахуванням недетермінованого числа вторинних дефектів).*

11. Харченко В.С., Одарущенко О.Н., Модель информационно-технического состояния компьютерной системы. *Системи обробки інформації.* 2008. Вип. 7(74). С.128-130. *(Особистий внесок здобувача: модель інформаційно-технічного стану з урахуванням рівней працездатності, показники гарантоздатності).*

12. Харченко В.С., Одарущенко О.Н., Руденко А.А., Одарущенко Е.Б., Поночовный Ю.Л. Моделирование обслуживаемых компьютерных систем с учетом вторичных дефектов программных средств. *Радіоелектронні і комп'ютерні системи*. 2009. № 7. С.245-249. *(Особистий внесок здобувача*: *марковські моделі з урахуванням прояву вторинних дефектів ПЗ).*

13. Одарущенко О.Н., Харченко В.С. Информационно-технические состояния компьютеризированных систем: модель событий и показатели гарантоспособности. *Системи управління, навігації та зв'язк*. 2009. Вип. 3(11). С.156-159. *(Особистий внесок здобувача: модель подій, показники гарантоздатності).*

14. Летичевский О.О., Песчаненко В.С., Харченко В.С., Волков В.А.. Одарущенко О.М. Модельний спосіб розроблення алгоритмів цифрових систем на програмованих логічних інтегральних схемах. *Кібернетика і системний аналіз*. 2020. Т. 56. №5. С.29-37. *(Особистий внесок здобувач: елементи технології модельної розробки апаратного забезпечення з використанням комбінації методів машинного навчання та алгебраїчного підходу).* (Видання входить до міжнародної наукометричної бази Scopus).

15. Одарущенко О.Н.. Руденко А.А., Харченко В.С. Учет вторичных дефектов в моделях надежности программных средств. *Математичні машини і системи.* 2010. Вип.1. С.205-217. *(Особистий внесок здобувача*: *визначення параметрів функцій ризику моделей надійності програмних засобів для урахування вторинних дефектів).*

16. Харченко В.С., Одарущенко О.Н., Руденко А.А., Одарущенко Е.Б. Анализ сценариев и определение параметров для оценки надежности программных средств с учетом вторичных дефектов. *Системи управління, навігації та зв'язку.* 2011. Вип.3(11). С.273-280. *(Особистий внесок здобувача*: *список параметрів, які застосовуються в моделях надійності програмних засобів для урахування вторинних дефектів).*

17. Odarushchenko O., Kharchenko V., Popov P., Zhadan V. Empirical evaluation accuracy of mathematical software used for availability assessment of fault-tolerant computer systems. *Electronic Jornal Reliability & risk Analysis: Theory & Applications*. 2012. 3(26), Vol.7. P.85-97. *(Особистий внесок здобувача*: *етапи розроблення багатофрагментних марковських моделей).*

18. Одарущенко О.Н., Руденко А.А., Харченко В.С. Метод оценивания надежности программных средств с учетом вторичных дефетков. *Радіоелектронні і комп'ютерні системи*. 2012. Вип.7(59). С.313-318. *(Особистий внесок здобувача*: *метод оцінювання надійності ПЗ з урахуванням прояву вторинних дефектів).*

19. Ивасюк А.О., Одарущенко О.Н., Фадеева Е.К., Барвинко А.П. Модель и инструментальная поддержка анализа сигналов при оценке функциональной безопасности FPGA-модулей. *Системи обробки інформації.* 2013. Вип. 4(111). С.20-23. *(Особистий внесок здобувача*: *інструментальні засоби функціонального покриття для електронних проектів ПЛІС в ході виконання їх функціонального тестування).*

20. Скляр В.В.. Резуненко А.А., Одарущенко О.Н., Гудзь А.С., Щербаченко С.С., Сенаторо А.А, Вовк Е.Д. Обеспечение тестового покрытия для электронных проектов FPGA при оценивании функциональной безопасности по критериям SIL3. *Системи обробки інформації.* 2013. Вип. 5(112). С. 62-65. *(Особистий внесок здобувача*: *модель функціонального покриття для електронних проєктів ПЛІС).*

21. Odarushchenko O., Kharchenko V., Butenko V. Metric-based analysis of Markov models for computer systems availability assessment. *Радіоелектронні і комп'ютерні системи*. 2013. Вип. 5(64). С.214-220. *(Особистий внесок здобувача*:

марковські моделі оцінювання готовності комп'ютерних систем).

22. Одарущенко О.Н., Харченко В.С., Руденко А.А., Одарущенко Е.Б. Учет фактора вторичных дефектов при оценке надежности программных средств. *Научные ведомости Белгородского государственного университета. "История. Политология. Экономика. Информатика".* 2013. №22(165). Вып. 28/1. С.153-160. *(Особистий внесок здобувача: сценарії внесення та усунення дефектів програмних засобів, аналіз моделей надійності програмних засобів з метою визначення переліку моделей для модифікації їх функцій ризику).*

23. Харченко В.С., Бутенко В.О., Одарущенко О.Н. Метрико-интервальные модели и инструментальные средства для оценивания готовности информационно-управляющих систем с использованием марковских процессов. *Системи обробки інформації.* 2014. Вип. 9(125). С.59-64. *(Особистий внесок здобувача: алгоритм обрання інструментальних засобів).*

24. Kharchenko V, Butenko V, Odarushchenko O., Sklyar V. Multi-fragmentation Markov Modeling of a Reactor Trip System. *Journal of Nuclear Engineering and Radiation Science*. 2015. Vol. 1, Iss. 3. 031005 (10 pages). URL: https: // asmedigitalcollection.asme.org/ nuclearengineering/ articleabstract/1/3/031005/472772/ Multifragmentation-Markov-Modeling-of-a-Reactor?redirectedFrom=fulltext (дата звернення: 18.01.2021). *(Особистий внесок здобувача: однофрагментні та багатофрагментні моделі оцінювання надійності комп'ютерних систем).* (Видання входить до міжнародної наукометричної бази Scopus).

25. Скляр В.В., Одарущенко О.Н., Поночовный Ю.Л., Бульба Е.Н., Ивасюк А.О. Модели отказов информационно-управляющих систем на основе самодиагностируемых программируемых платформ в системах аварийной защиты реакторов. *Радіоелектронні і комп'ютерні системи науково-технічний журнал.* 2015. №4. С.19-24. (*Особистий внесок здобувача: базова марковська модель відмов ІКС, структурна модель системи контроля та діагностики на основі самодіагностовних програмовних платформ).*

26. Kharchenko V., Odarushchenko O., Butenko V., Moskalets V., Odarushchenko E., Strjuk O. Application of Markov Modeling for Safety Modeling for Safety Assessment of Self-Diagnostic Programmable Instrumentations and Control Systems. *Central European Researchers Journal*. 2016. Vol.2, Iss. 2. P. 61-69. URL: http://ceres-journal.eu/iss160202 (дата звернення: 18.01.2021). *(Особистий внесок здобувача: однофрагмента та багатофрагментна марковські моделі оцінювання надійності двохканальної комп'ютеризованої системи).*

27. Одарущенко О.Б., Одарущенко О.М., Бутенко В.О., Москалець В.В., Стрюк О.Ю. Моделі математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів. *Системи управління, навігації та зв'язку.* 2017. Вип. 4(44). С.40-45. *(Особистий внесок здобувача: постановка завдання розроблення моделей математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів).*

28. Одарущенко О.М., Одарущенко О.Б., Харченко В.С. Марковьскі моделі оцінювання функціональної безпеки програмно-технічних комплексів на

самодіагностовних програмовних платформах з урахуванням помилок засобів контролю. *Радіоелектронні і комп'ютерні системи.* 2019. №4(92). С.17-29. *(Особистий внесок здобувача: структурні схеми систем нормальної експлуатаціїта аварійного захисту, дерева відмов, багатофрагментні моделі з урахуванням помилок засобів контролю).*

29. Руденко О.А., Одарущенко О.М., Руденко З.М., Одарущенко О.Б. Оцінювання кількості вторинних дефектів програмних засобів шляхом комплексування модифікованих моделей росту надійності Джелінські-Моранди і Шика-Волвертона. *Системи управління, навігації та зв'язку.* 2020. Вип.1(59). С.97-100. *(Особистий внесок здобувача: модифікована МНПЗ Джелінські-Моранди).*

30. Одарущенко О.Н. Оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для програмно-технічних комплексів інформаційно-керуючих систем. *Системи управління, навігації та зв'язку.* 2020.Вип.3(61). С.90-93.

Праці апробаційного характеру:

31.Odarushchenko, O., Kharchenko, V. Availability models of critical infrastructures with variable system dependability parameters. *Proceedings of the first International Workshop Critical Infrastructure Safety and Security. CrISS-DESSERT,* May 11-13, 2011, Kirovograd, Ukraine, 2011. P. 319-330. (*Особистий внесок здобувача: математичні моделі готовності критичних інфраструктур з змінними параметрами).*

32. Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Selecting mathematical software for dependability assessment of computer systems described by stiff Markov chains. *ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer. ICTERI 2013: Procceding of the 9th International Conference,* June 19-22, 2013, Kherson, Ukraine, 2013. P. 146 – 162. (*Особистий внесок здобувача: структурна схема надійності, багатофрагмента марковська модель).* (Видання входить до міжнародної наукометричної бази Scopus).

33.Odarushchenko O., Ivasyuk O., Bulba E. Fault injection-based technique and tool for FPGA modules safety assessment. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013,* May 23-26, 2013, Sevastopol, Ukraine, 2013. P.14. (*Особистий внесок здобувача: процедура тестування з внесенням дефектів).*

34. Butenko V., Odarushchenko O., Kharchenko V. Analysis of markov chains for high availability systems: metric-based approach. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013,* May 23-26, 2013, Sevastopol, Ukraine, 2013. P.16. (*Особистий внесок здобувача: етапи оцінювання готовності ПТК).*

35. Odarushchenko O., Kharchenko V., Sklyar V, Ivasuyk A. Fault-Injection Testing: FIT-Ability. *Proceedings of East-West Design&Test Symposium EWDTS"2013*, September 27-30, 2013, Ростов-на-Дону, Росссия, 2013. P.188-192. (*Особистий внесок здобувача: – оптимальна FIT – процедура, алгоритм та приклад виконання процедури).*

36. Odarushchenko, O., Kharchenko, V, Butenko, D, Butenko V. Assessment of the Reactor Trip System Dependability Two Markov Chains - based Cases. *Proceedings of the 10th International Conference on Digital Technologiesю,* July 9-11, 2014, Zilina, Slovakia, 2014. P. 103-109. (*Особистий внесок здобувача: багатофрагментна марковська модель, індустріальний приклад).* (Видання входить до міжнародної наукометричної бази Scopus).

37. Butenko V., Kharchenko V., Odarushchenko O., Popov P., Sklyar V., Odarushchenko E. Markov's Model and Tool-Based Assessment of Safety-Critical I&C Systems: Gaps of the IEC 61508. *12-th International Conference on Probabilistic Safety Assessment and Modeling*: *Proceeding of 12-th International conference on probabilistic safety assessment and modeling,* June 22-27, 2014, Honolulu, Hawaii, USA, 2014. P. 455-458. URL: http: // iapsam.org/ psam12/ proceedings/paper/ paper_455_1.pdf (дата звернення 18.01.2021). (*Особистий внесок здобувача: результати аналізу недоліків стандарту IEC 61508, структурна схема надійності та марковська модель системи аварійного захисту).* (Видання входить до міжнародної наукометричної бази Scopus).

38. Odarushchenko O., Kharchenko V, Sklyar V, Ivasyuk A. Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues. *Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication ICONE22*, July 7-11, 2014, Prague, Czech Republic, 2014. Vol. 6: Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. URL: https: // asmedigitalcollection.asme.org /ICONE/ICONE22/volume/45967. ICONE22-31163, V006T13A022; 5 pages. (Дата звереннння: 18.01.2021). (*Особистий внесок здобувача: етапи виконання HW FIT процедури).* (Видання входить до міжнародної наукометричної бази Scopus).

39. Odarushchenko O., Kharchenko V, Gordieiev O., Vilkomir S. t-Wise-Based Multi-Fault Injection Technique for the Verification of Safety Critical I&C Systems. *Procceding of 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT,* February 22-26, 2015, Charlotte, USA, 2015. P. 1827-1836. (*Особистий внесок здобувача: основні етапи реалізації процедури тестування АК з внесенням мультидефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

40. Odarushchenko O., Kharchenko, Sklyar, V. Multi-Fault Injection Testing: Cases for FPGA-Based NPP I&C Systems. *Proceedings of 23rd International Conference on Nuclear Engineering ICONE-23*, May 17-21, 2015, Chiba, Japan, 2015. URL: https://inis.iaea.org/search/search.aspx?orig_q=RN:48025087 (Дата звереннння: 18.01.2021). (*Особистий внесок здобувача: індустріальний приклад виконання процедури тестування з внесення мультидефекту).* (Видання входить до міжнародної наукометричної бази Scopus).

41. Odarushchenko O., Babeshko E., Kharchenko V., Sklyar V. Toward automated FMEDA for complex electronic products. *Proceedings of the International Conference on Information and Digital Technologies,* July 7-9, 2015, Zilina, Slovakia, 2015. P. 17-22. (*Особистий внесок здобувача: етапи автоматизації техніки FMEDA).* (Видання входить до міжнародної наукометричної бази Scopus).

42. Odarushchenko O., Kharchenko, V. Butenko V., Odarushchenko, E. Markov's Modeling of NPP I&C Reliability and Safety Optimization of tool-and-technique selection. *Proceeding of Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management,* February 15-18, 2016, Beer Sheva, Israel, 2016. P. 328 – 336. (*Особистий внесок здобувача: процедура обрання інструментальних засобів для оцінювання надійності ПТК).* (Видання входить до міжнародної наукометричної бази Scopus).

43. Odarushchenko O., Strjuk O., Bulba Y., Leontiiev K., Ivasyuk A., Kharchenko V. Fault insertion software and hardware testing for safety PLC-based system SIL certification. *Proceeding of the 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018,* May 24-27, 2018, Kyiv, Ukraine, 2018. P. 202-206. (*Особистий внесок здобувача: визначення FIT –здатності, SW та HW процедури з внесенням дефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

44. Babeshko, E., Kharchenko, V., Odarushchenko, O., Leontiiev, K., Strjuk, O. NPP I&C Safety Assessment by Aggregation of Formal Techniques. *Proceedings of the 2018. 26th International Conference on Nuclear Engineering ICONE26,* July 22-26, 2018, London, England, 2018. P. 1-6. (*Особистий внесок здобувача:процедура SW FMEA).* (Видання входить до міжнародної наукометричної бази Scopus).

45. Одарущенко О.Н., Одарущенко Е.Б. Оценка надежности восстанавливаемых управляющих и вычислительных систем с учетом характеристик средств контроля в условиях дефектов программных и аппаратных средств // Науково-технічна конференція, 10-11 лист. 1999р.:тези доп. Харків, 1999. С.38-39. (*Особистий внесок здобувача: модель оцінювання надійності відновлюваних управлючих систем з урахуванням засобів контролю).*

46.Одарущенко О.Н., Одарущенко Е.Б., Яковлев В.И. Оценка надежности вычислительных систем с учетом изменения параметров отказов и восстановлений их программных средств // 8-я Международная конференция «Теория и техника передачи, приема и обработки информации» (Интегрированные информационные системы, сети и технологии), 17-19 сентября 2002р.: тез. докл. Харьков, 2002. С. 269-271. (*Особистий внесок здобувача*: *методика оцінка надійності обчислювальних систем).*

47. Одарущенко О.Н., Поночовный Ю.Л. Надежность, как критерий качества программного обеспечения// Матеріали Міжнародної науково-технічної конференції «Інтегровані комп'ютерні технології в машинобудуванні – ІКТМ-2003», тези доп. Харків, 2003. С.221. (*Особистий внесок здобувача*: *визначення надійності як критерія якості програмного забезпечення).*

48. Одарущенко О.Н., Харченко В.С., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем// Матеріали 1-ої Міжнар. науково-техн. конф. „Гарантоспроможні (надійні та безпечні) системи, сервіси та технології - DESSERT-2006", 25-28 квітня 2006р.: тези доп. Полтава, 2006. С. 12. (*Особистий внесок здобувача*: *багатофрагмента модель для дубльованої архітектури ПТК).*

49. Одарущенко О.Н., Руденко А.А. Модель Джелинского-Моранды с учетом недетерминированного числа вторичных дефектов. Матеріали Третьої міжнародної науково-технічної конференції „Комп'ютерна математика в інженерії, науці та освіті“ (CMSEE-2009), 1-31 жовтня 2009р: тези доп. Київ, 2009. С. 49-50. (*Особистий внесок здобувача*: *модифікація МНПЗ Джелинського-Моранди).*

50. Одарущенко О.Н., Руденко А.А. Использование корреляционных зависимостей при прогнозировании числа вторичных дефектов программных средств// Матеріали Четвертої міжнародної науково-технічної конференції „Комп'ютерна математика в інженерії, науці та освіті“ (CMSEE-2010), 1-31 жовтня 2010р.: тези доп. Полтава, 2010. С. 53-54. (*Особистий внесок здобувача*: *приклад формування кореляційної залежності).*

51. Одарущенко О.Н., Живило С.В. Методология оценки гарантоспособности на основе фактического информационно-технического состояния// Материалы междунар одной научно-практической конференции «Информационные технологии и информационная безопасность в науке, технике и образовании (ИНФОТЕХ -2011), 05-10 вер. 2011р.: тези доп. Севастополь, 2011. С.38-39. (*Особистий внесок здобувача*: *визначенння інформаційно-технічного стану, елементи методології).*

52. Одарущенко О.Н., Руденко А.А. Определение параметров оценки надежности программных средств с учетом вторичных дефектов// Шоста науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання систем. МОДС '2011'', 27-30 черв. 2011р.: тези доп. Чернігів, 2010. С. 391-392. (*Особистий внесок здобувача*: *перелік параметрів оцінювання надійності ПЗ з урахуванням вторинних дефектів).*

53. Одарущенко О.Н., Руденко А.А., Руденко З.Н., Мельник М.А. Метод оценивания надежности программных средств с учетом вторичных дефектов// Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013», 24-27 червня 2013р.: тези доп. Чернігів-Жукин, 2013. С. 336-339. (*Особистий внесок здобувача*: *визначення етапів метода оцінювання надійності програмних засобів).*

54. Одарущенко О.Н., Харченко В.С. Моделирование и оценивание функциональной безопасности программно-технических комплексов в контексте стандарта IEC 61508. Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013», 24-27 червня 2013р.: тези доп. Чернігів-Жукин, 2013. С. 339-339. (*Особистий внесок здобувача*: *аналіз IEC 61508, перелік недоліків стандарта, підходи до їх усунення).*

55.Odarushchenko O., Kharchenko V., Butenko V., Odarushchenko E. Assessing of programmable system availability in context of the IEC 61508. *Program 7th International conference - Dependable Systems, Services and Technologies DESSERT2014*, May 16-18, 2014. Kiev, Ukraine. 2014. P.21. (*Особистий внесок здобувача*: *етапи оцінювання надійности ПТК в контексті 61508).*

56. Odarushchenko O., Odarushchenko E, Strjuk O., Leontiiev K., Software Fault Insertion Testing for SIL Certification of Safety PLC-based System. *Proceeding of The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020,* May 14-18, 2020. Kiev, Ukraine. 2020. P.80-84. (*Особистий внесок*

здобувача: *деталізована процедура тестування ПЗ з внесенням дефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

57. Одарущенко О.М., Одарущенко О.Б. Концепція і принципи оцінювання і забезпечення надійності та функціональної безпеки програмно-технічних комплексів. //Сьома міжнародна науково-технічна конференція «Проблеми інформатизації», 13-15 листопада 2019р.: тези доп. Черкаси-Харків-Баку-Більско-Бяла, 2019. С.5. *(Особистий внесок здобувача: Концепція і принципи оцінювання і забезпечення надійності та функціональної безпечності ПТК).*

58.Одарущенко О.М., Одарущенко О.Б. Метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах// Десята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», 9-19 квітня 2020р.: тези доп. Баку-Харків-Жиліна, 2020. С.20. (*Особистий внесок здобувача*: *метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах).*

59.Odarushchenko O., Kharchenko V., Odarushchenko V. Multi-fragmental availability models of critical infrastructures with variable parameters of system dependability, information & security. *Information and Security. An International Journal*. 2012, Vol. 28, № 2. P. 248 – 265. *(Особистий внесок здобувача*: *багатофрагментні марковські моделі критичних інфраструктур).*

60.Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Availability assessment of computer systems described by stiff Markov chains: case study. *Springer.CCIS (412)*. 2013. P. 112 – 135. *(Особистий внесок здобувача: структурна схема надійності відмовостійкості системи, система диференційних рівнянь).* (Видання входить до міжнародної наукометричної бази Scopus).

Праці, які додатково відображають наукові результати дисертації:

61. Одарущенко О.Н., Харченко В.С., Поночовный Ю.Л., Одарущенко Е.Б., Бутенко В.О., Харыбин А.В. Системы и технологии высокой готовности. Харьков, 2013. 273с. (*Особистий внесок здобувача*: *моделювання та оцінка комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ).*

62. Одарущенко О.Н., Поночовный Ю.Л., Одарущенко Е.Б., Бутенко В.О., Харыбин А.В. Системы и технологии высокой готовности. Харьков, 2013. 96 с. *(Особистий внесок здобувача*: *практичні заняття змоделювання та оцінки комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ).*

63. Комп’ютерна програма «MSMC-Method selector for Markov chains»: Свідоцтво про реєстрацію авторського права на твір №57120. - Дата реєстрації 05.10.2014. *(Особистий внесок здобувача*: *алгоритм рішення марковських ланцюгів).*

64. Гарантоздатність програмно-технічних комплексів критичного призначення /Ю. Алексеєв, Б. Конорев, В. Скляр, О. Одарущенко, В. Харченко, Г. Чертков// СОУ-Н НКАУ 0060:2010. Настанова національного космічного агенства

України. *(Особистий внесок здобувача*: *поняття про інформаційно-технічний стан,, дефекти та уразливості, що призводять до порушення працездатності).*

65.Харченко В.С., Андрейченко Д.К., Антощук С.Г., Дрозд М.А., Одарущенко О.Н., Бульба Е.Н., Стрюк А.Ю., Ивасюк А.О. Зеленая ИТ-инженерия. В 2-х томах. Том 1. Принципы, компоненты, модели. Харьков, 2014. 594с. *(Особистий внесок здобувача*: *опис методів контроля відмов обладнання, опис функційного тестування, аналіз процесів валідації FPGA систем).*

66. Харченко В.С., Скляр В.В.. Одарущенко О.М., Одарущенко О.Б. Університетсько-індустріальна кооперація. Модельно-орієнтований підхід. Практичне керівництво та приклади. Харків, 2017. 363 с. *(Особистий внесок здобувача*: *опис створення spin-off компанії із задачами забезпечення та оцінювання безпеки ІКС).*

67. Барсов В.І., Одарущенко О.М., Краснобаєв В.А., Тиртишніков О.І., Барсова З.В. Основи побудови АСУ. Полтава, 2012. 400с. *(Особистий внесок здобувача: загальна характеристика процесу побудови автоматизованих систем управління).*

68. Харченко В.С., Одарущенко О.Н., Иванченко О.В. Принципы анализа и управления безопасностью критических инфраструктур. *Вісник Хмельницького національного університету*. 2010. Вип.5. С. 218-221. *(Особистий внесок здобувача*: *принципи забезпечення безпеки).*

АНОТАЦІЯ

Одарущенко О.М. Методи і засоби забезпечення надійності та функційної безпечності програмно-технічних комплексів з урахуванням фізичних і проектних дефектів компонентів. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» Міністерства освіти і науки України; Харківський національний університет імені В.Н. Каразіна Міністерства освіти і науки України. – Харків, 2021.

На основі розвитку парадигми фон Неймана і гіпотези про можливість побудови надійних і функційно безпечних систем із недостатньо надійних програмно-апаратних компонентів розроблена методологія оцінювання і забезпечення надійності та функційної безпечності ПТК ІКС КЗ за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушень внаслідок проєктних і фізичних дефектів і дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання шуканих показників. Удосконалено ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів. Розроблено метод оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю, що забезпечує підвищення точності розрахунку функції готовності та імовірності відмов за загальною причиною. Розроблено моделі оцінювання готовності та функційної безпечності ПТК на самодіагностовних платформах та метод забезпечення функційної безпечності шляхом використання різних варіантів

версійної надмірності (диверсності), що підвищило точність оцінок до 5%. Розроблено методи верифікації і валідації програмовних платформ і ПТК на їх основі і результуючий метод оціювання та забезпечення надійності і функційної безпечності ПТК ІКС КЗ, який акумулює всі попередні наукові результати та їх переваги. Він дозволяє виконувати комплексне оцінювання вказаних властивостей і забезпечує досягнення системами рівня функційної безпечності SIL-3.

Отримані результати дозволили вирішити науково-прикладну проблему комплексного оцінювання і забезпечення надійності і функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування.

Ключові слова: інформаційні-керуючі системи, програмно-технічні комлекси, надійність та функційна безпечність, апаратні засоби, програмні засоби, множина дефектів, дефект проєктування програмних засобів, моделі надійності програмних засобів.

АННОТАЦИЯ

Одарущенко О.Н. Методы и средства обеспечения надежности и функциональной безопасности программно-технических комплексов с учетом физических и проектных дефектов компонент. - На правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05 - компьютерные системы и компоненты. - Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт» Министерства образования и науки Украины; Харьковский национальный университет имени В.Н. Каразина Министерства образования и науки Украины. - Харьков, 2021.

На основе развития парадигмы фон Неймана и гипотезы о возможности построения надежных и функционально безопасных систем из недостаточно надежных программно-аппаратных компонентов разработана методология оценки и обеспечения надежности и функциональной безопасности программно-технических комплексов информационно-управляющих систем критического назначения (ПТК ИУС КН) за счет описания их информационно-технического состояния, совершенствование принципов уменьшения и оценки рисков его нарушений в результате проектных и физических дефектов и дефектов взаимодействия с учетом изменения параметров потоков отказов и восстановлений, что обеспечивает повышение точности оценки искомых показателей. Усовершенствованы вероятностные модели оценки надежности (безотказности) программных средств путем учета вторичных дефектов. Разработан метод оценки надежности и обеспечения функциональной безопасности ПТК со структурно-версионной избыточностью, что обеспечивает повышение точности расчета функции готовности и вероятности отказов по общей причине. Разработаны модели оценки готовности и функциональной безопасности ПТК на самодиагностирующихся платформах и метод обеспечения функциональной безопасности путем использования различных вариантов версионной избыточности (диверсности), что повысило точность оценок до 5%. Разработаны методы верификации и валидации программируемых платформ и ПТК на их основе и результирующий метод оценивания и обеспечения

надежности и функциональной безопасности ПТК ИУС КН, который аккумулирует все предыдущие научные результаты и их преимущества. Он позволяет выполнять комплексную оценку указанных свойств и обеспечивает достижение системами уровня функциональной безопасности SIL-3.

Полученные результаты позволили решить научно-прикладную проблему комплексной оценки и обеспечения надежности и функциональной безопасности ПТК ИУС КН.

Ключевые слова: информационные управляющие системы, программно-технические комлексы, надежность и функциональная безопасность, аппаратные средства, программные средства, множество дефектов, дефект проектирования программных средств, модели надежности программных средств.

ANNOTATION

Odarushchenko O.M. Methods and means for ensuring reliability and functional safety of instrumentation and control systems with considering the physical and design defects of the components.- As the manuscript.

Dissertation for the degree of Doctor of Technical Sciences in the specialty of 05.13.05 – Computer Systems and Components. – National Aerospace University “Kharkiv Aviation Institute” Ministry of Education and Science of Ukraine; V.N. Karazin Kharkiv National University Ministry of Education and Science of Ukraine. – Kharkiv, 2021.

The safety of nuclear power plants, aerospace and other critical facilities depends to a large extent on the instrumentation and control systems (I&C). The cost of failures of hardware, software, software and communication (network) facilities of I&C is extremely high. The most important property of I&C is functional safety (FS), which in accordance with international and national standards (IEC 61508, IEC 26262) determines the ability of systems to minimize the risks of transition to an emergency (dangerous) state and/or its consequences. Modern processes of modernization of existing and development of promising I&C are based on the use of a new element base, modern technologies for the development of their hardware and software components. This, on the one hand, expands the capabilities of I&C, leads to increased efficiency of technological processes, reduces the resource intensity of production, and on the other hand - to increase the risks of increasing the dependence of functionality, reliability and safety on the quality of design solutions. That is, the increase in the capabilities of the modern element base, the introduction of industrial software development technologies (software) has not led to the same progress in the design of I&C with the necessary and guaranteed level of reliability and safety. Modern I&C of critical application retain a set of "safety deficits", which are determined by: insufficient level of reliability and FS of hardware and software; insufficient level of diagnosis of hardware and software; incomplete satisfaction of seismic requirements; variety of element base and technical solutions for different I&C.

During the analytical research of the subject area it was found that despite intensive research on selected topics in recent decades, in the areas of: development of theoretical foundations, general methods of evaluation and improving reliability and functional safety (A. Avizienis, J.-C. Laprie , G. Johnson, B. Randell, E. Zaitseva, B.Yu. Volochy, B.M. Konorev, V.S. Kharchenko, M.O. Yastrebenetsky and others); development of methods

and tools for evaluating and ensuring the reliability of software for various applications (V. Littlewood, P. Popov, A. Romanovsky, S. Russo, L. Strigini, J. Vain, V.V. Lipayev, D.A. Maevsky, V.S. Yakovina and others); development and research of models and methods for diagnosing and ensuring the stability of information control systems and I&C to physical and design defects (T. Anderson, F. Saglietti, K. Trivedi, O.V. Drozd, V.A. Krasnobaev, G.F. Kryvulya, V.M. Opanasenko, O.M. Romankevich, V.O. Romankevich, V.V. Sklyar, V.I. Khakhanov and others), there are a number of unsolved problems and limitations of existing methods and means of evaluation and provision the required level of properties, namely: models that describe the reliable and safe (both informational and functional) components, do not take into account the real dimension of the evaluation tasks given the complexity of industrial I&C; variability of failure and recovery parameters; in the Reliability ans FS (RFS) assessment methods, first of all, the aspects of hardware and software reliability are considered separately, without a joint comprehensive quantitative analysis; methods of developing and ensuring the resilience of I&Cs using software platforms do not sufficiently take into account the capabilities, limitations and errors of embedded control and diagnostic tools at the level of electronic projects, modules and channels, etc.

Based on the development of von Neumann's paradigm and the hypothesis of the possibility of building reliable and functionally safe systems from insufficiently reliable software and hardware components, a methodology for assessing and ensuring the reliability and functional safety of I&Cs by describing their information and technical condition, improving the principles of risk reduction and assessment its violations due to design and physical defects and defects of interaction taking into account the variability of the parameters of the flows of failures and recoveries, which provides an increase in the accuracy of estimating the required indicators. Probabilistic models for assessing the reliability of software (SRGM - software reliability growth models) by taking into account secondary defects have been improved. A method for assessing the reliability and functional safety of I&C with structural-version redundancy has been developed, which provides an increase in the accuracy of calculating the readiness function and the probability of failure for a common cause. Models for assessing the readiness and functional safety of I&C on self-diagnostic platforms and a method for ensuring functional safety by using different options for version redundancy (diversity), which increased the accuracy of estimates to 5%. Methods of verification and validation of software platforms and I&C based on them and the resulting method of evaluation and ensuring the reliability and functional safety of I&C, which accumulates all previous scientific results and their benefits, have been developed. It allows to carry out complex estimation of the specified properties and provides achievement by systems of a level of functional safety of SIL-3.

The obtained results allowed to solve the scientific and applied problem of complex evaluation and ensuring the reliability and functional security of software and hardware complexes of information and control systems of critical application.

Keywords: instrumentation and control systems, reliability and functional safety, hardware, software, set of defects, verification and validation, software design defect, software reliability models.

Підп. до друку 02.04.2021. Формат 60х90 1/16. Папір офсетний.
Ум. друк. арк. 1,9. Тираж 100 пр. Зам. № 34.
Гарнітура Times New Roman Cyr.

Друк – Редакційно-видавничий відділ Полтавської державної аграрної академії
Свідоцтво суб'єкта видавничої справи ДК №2174 від 26.04.2005 р.
Адреса: 36003, м. Полтава, вул. Г. Сковороди, 1/3.