МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ОЗІРКОВСЬКИЙ ЛЕОНІД ДЕОНІСІЙОВИЧ

УДК 629.039.58, 621.396.9

РОЗВИТОК ТЕОРЕТИЧНИХ ЗАСАД ОЦІНЮВАННЯ ПОКАЗНИКІВ ФУНКЦІОНАЛЬНОЇ БЕЗПЕЧНОСТІ РАДІОЕЛЕКТРОННИХ СИСТЕМ ВІДПОВІДАЛЬНОГО ПРИЗНАЧЕННЯ

05.12.17 – радіотехнічні та телевізійні системи

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Львів 2020

Дисертацією є рукопис.

Робота виконана у Національному університеті «Львівська політехніка» Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор **Волочій Богдан Юрійович,** Національний університет «Львівська політехніка», професор кафедри теоретичної радіотехніки та радіовимірювань.

Офіційні опоненти: доктор технічних наук, професор **Толюпа Сергій Васильович,** Київський Національний університет ім. Т.Г. Шевченка, професор кафедри кібербезпеки та захисту інформації.

доктор технічних наук, професор **Жук Сергій Якович,** Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського», завідувач кафедри радіотехнічних пристроїв та систем.

доктор технічних наук, професор **Краснобаєв Віктор Анатолійович,** Харківський національний університет імені В. Н. Каразіна, професор кафедри електроніки і управляючих систем.

Захист відбудеться «10» грудня 2020 р. о 14^{15} годині на засіданні спеціалізованої вченої ради Д.35.052.10 у Національному університеті «Львівська політехніка», 79013, м. Львів, вул. С. Бандери, 12, ауд. 217 головного корпусу.

З дисертацією можна ознайомитися у бібліотеці Національного університету «Львівська політехніка», 79013, м. Львів, вул. Професорська, 1.

Автореферат розісланий «4» листопада 2020 р.

Вчений секретар спеціалізованої вченої ради, к.т.н., М.І. Бешлей

Дисертаційна робота присвячена проблемі підвищення рівня функціональної безпечності радіоелектронних систем відповідального призначення (Safety Critical Systems) на етапі їх системотехнічного проектування. Особливістю радіоелектронних систем відповідального призначення є те, що їх функціональна безпечність залежить не тільки від надійності апаратних чи програмних засобів, але й від алгоритму поведінки (функціонування), наявності та різновиду відмовостійкої структури системи та процедур її технічного обслуговування. Проте моделі, методи та методики, які дозволяють оцінити рівень їх безпечності з врахуванням вищезазначених особливостей – відсутні.

Актуальність теми. Радіоелектронна система відповідального призначення (РЕСВП) – це програмно-апаратна система, яка є складовою системи керування складними технічними системами (телекомунікаційні системи, транспорт (авіація, залізниця, трубопроводи), медичні системи, робототехнічні системи, енергетичні системи, військова техніка, технологічні лінії тощо), вихід з ладу яких призводить до втрати працездатності системи керування, а це в свою чергу – до аварійної ситуації складної технічної системи. Функціональною безпечністю, згідно стандартів IEC 61508, ISO 26262, називають властивість системи, при виході з ладу її окремих підсистем чи модулів, переходити в такий режим роботи, в якому вона не несе загрози життю людей, навколишньому середовищу чи іншим системам.

Стрімке впровадження штучного інтелекту у системи керування призводить до того, що кінцеве рішення про управляючу дію приймає система керування, а не людина. Крім цього, такі системи стають повністю автономними (роботизовані безпілотні літальні апарати, пристрої та системи Інтернету речей, розподілені хмарні телекомунікаційні системи, системи індустріального Інтернету речей тощо), і помилки в проектуванні їх структури та алгоритмів поведінки, які згодом реалізують як програмне забезпечення, призводять до відмов чи збоїв. А вони в свою чергу призводять до появи аварійної ситуації, яку вже неможливо усунути за допомогою оператора. Відповідно, зважаючи на потенційні наслідки аварійних ситуацій, проблема забезпечення функціональної безпечності РЕСВП на етапі системотехнічного проектування виходить на перше місце.

Проблемою підвищення функціональної безпечності РЕСВП займається велика кількість фахівців та вчених, найвідомішими з яких є Н. Бар, З. Блувбанд, А. Верма, Б. Волочій, К. Еріксон, І. Кнєзевич, Х. Кумамото, А. Можаев, І. Рябінін, Х. Фам, В. Харченко, Е. Хенлі, М. Чепін. В їх працях розглянуто різні методи забезпечення та аналізу функціональної безпечності, що заклало теоретичні підвалини для розроблення сучасних програмно-інформаційних комплексів (Safety Commander, RAM Commander, ReliaSoft Suite, ITEM ToolKit, AttackTree, Reliability Workbench).

Зокрема, в працях Е. Хенлі та Х. Кумамото розроблена методологія оцінювання ризику експлуатації технічних систем на базі дерев відмов, що дало поштовх для подальшого розвитку теорії безпечності в працях Н. Бара, А. Верма та І. Кнєзевича. Теорія функціональної безпечності апаратних засобів докладно розвинута в працях В. Харченко, а програмних засобів – в працях Х. Фама. Для систем, які складалися з декількох підсистем чи модулів дані підходи були прийнятними. Однак, із збільшенням складності технічних систем ці підходи вимагали побудови громіздких моделей і потребували значних часових затрат на їх валідацію та аналіз. Спроби

автоматизувати цей процес були здійснені З. Блувбандом, А. Можаєвим та І. Рябініним. Крім цього, основним недоліком методики аналізу безпечності за допомогою дерева відмов виявилось те, що отримані моделі є статичними і не відображають можливості активного резервування, особливості стратегій технічного обслуговування, вплив засобів контролю та діагностики. Частково усунути ці недоліки вдалося М. Чепіну завдяки застосування динамічних дерев відмов для оцінювання функціональної безпечності систем. Однак на сьогодні застосування динамічних дерев відмов не реалізовано в жодному з доступних спеціалізованому програмному забезпеченні для оцінювання функціональної безпечності.

Наблизитись до динамічних моделей безпечності дав змогу метод автоматизованої побудови дискретно-неперервних стохастичних моделей у вигляді графа станів і переходів на основі структурно-автоматної моделі, запропонований Б. Волочієм та В. Беляєвим. Даний метод покладено в основу інформаційної технології аналізу надійнісної та функціональної поведінки радіоелектронних систем та комплексів і дає змогу автоматизовано будувати динамічні ймовірнісні моделі без обмеження на їх розмірність.

Незважаючи на розвиток теорії та практики, вирішення проблеми підвищення рівня функціональної безпечності РЕСВП призводить до зменшення рівня надійності таких систем. Це породжує протиріччя, оскільки до сучасних РЕСВП висуваються однаково високі вимоги, як до рівня функціональної безпечності, так і до рівня надійності. Справа в тому, що засоби забезпечення функціональної безпечності проектують як окрему додаткову підсистему і з точки зору надійності вона є послідовним з'єднанням з основною системою, що зменшує надійність РЕСВП в цілому.

Тому актуальною проблемою є розвиток теоретичних засад, а на їх основі методів, моделей та методик, які дадуть змогу визначати слабкі місця в РЕСВП з точки зору функціональної безпечності. В ці місця вносять необхідні види надлишковості, щоб підвищити функціональну безпечність і підвищувати або принаймні не знижувати надійність. Причому моделі та методи повинні враховувати як особливості підключення різних видів надлишковості і наявність засобів контролю та діагностики, так і особливості стратегій технічного обслуговування та ремонту.

Таким чином, в дисертаційній роботі розв'язана важлива науково-прикладна проблема розвитку теоретичних засад комплексного забезпечення рівня функціональної безпечності та надійності радіоелектронних систем відповідального призначення на етапі їх системотехнічного проектування.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження виконувалися у відповідності до наукового напряму кафедри теоретичної радіотехніки та радіовимірювань Національного університету «Львівська політехніка» – «Теорія і методи проектування радіотехнічних кіл, систем і комплексів та забезпечення їх якості», в рамках низки держбюджетних науково-дослідних робіт: ДБ Вербаль (2004 – 2006) «Розробка комп'ютерних моделей відмовостійких радіоелектронних засобів», № держ. реєстрації 0104U002291; ДБ КРОКІТ (2007 – 2009) «Розробка комп'ютерних макромоделей радіоелектронних систем та їх функціональних вузлів, адаптованих до задач надійнісного проектування», № держреєстрації 0107U000836; ДБ ПНРЛ (2010 − 2012)

«Розроблення моделей, методів та алгоритмів для автоматизованої оцінки показників надійності радіоелектронних та електромеханічних пристроїв та систем», № держреєстрації 0110U001098; ДБ Трикаф (2013 – 2014) «Розроблення моделей надійності, ризику та безпечності програмно–апаратних технічних систем», № держреєстрації 0113U001371; ДБ/Ризик (2017 – 2018) «Розробка математичного забезпечення для програмного засобу аналізу функціональної безпечності та надійності програмно-апаратних систем відповідального призначення», № держреєстрації 0117U004458.

Мета і завдання дослідження. Метою роботи є підвищення ефективності процедур синтезу радіоелектронних систем відповідального призначення шляхом розвитку теоретичних засад, а на їх основі створення нових методів для побудови комплексних моделей, які дають змогу оцінювати, як рівень функціональної безпечності, так і рівень надійності РЕСВП з урахуванням їх відмовостійкої структури, специфіки алгоритму поведінки та різновиду стратегії технічного обслуговування.

Для досягнення поставленої мети в межах дисертаційних досліджень були сформульовані і розв’язані такі завдання:

1. Проаналізувати сучасний стан теоретичних підходів та практичних методик забезпечення заданого рівня безпечності систем відповідального призначення на етапі їх системотехнічного проектування.
2. Удосконалити існуючі теоретичні засади побудови моделей РЕСВП, з яких можна отримувати, як показники функціональної безпечності, так і показники надійності шляхом розділення простору непрацездатних станів на непрацездатні безпечні стани, критичні та катастрофічні стани.
3. Розробити методи та моделі оцінювання показників функціональної безпечності РЕСВП, які дають змогу синтезувати доцільну, з точки зору безпечності, стратегію технічного обслуговування та ремонту.
4. Розробити моделі для синтезу безпечних відмовостійких радіоелектронних систем відповідального призначення з мажоритарною структурою з реконфігурацією ядра, з дворівневим принципом мажоритарного резервування, з технічним обслуговуванням та ремонтом і з системою контролю та діагностики.
5. Запропонувати характеристики функціональної безпечності, які дають змогу синтезувати безпечні алгоритми поведінки РЕСВП з доцільним рівнем часової та функціональної надлишковості та розробити методи та методики синтезу таких алгоритмів.

Об’єктом дослідження є процес синтезу радіоелектронних систем відповідального призначення із заданим рівнем функціональної безпечності та надійності.

Предмет дослідження: методи, моделі, алгоритми і методики аналізу та синтезу відмовостійкої структури безпечних радіоелектронних систем відповідального призначення, алгоритму її поведінки та стратегії технічного обслуговування.

Наукова новизна отриманих результатів.

Вперше запропоновано:

1. Функцію аварійності, яка на відміну від існуючих кількісних показників функціональної безпечності, відображає взаємозв’язок між показниками

безпечності та надійності, що дає змогу синтезувати із заданими рівнем функціональної безпечності та надійності наступні складові РЕСВП: відмовостійкі структури, алгоритми поведінки з часовою та функціональною надлишковістю, процедури стратегій технічного обслуговування та ремонту.

2. Метод визначення функції аварійності на підставі розділення непрацездатних станів на непрацездатні безпечні стани, непрацездатні критичні та непрацездатні катастрофічні стани, який на відміну від існуючих підходів, дає змогу отримати мінімальні січення (слабкі місця системи) з моделі у вигляді графа станів і переходів без побудови дерева відмов. Це забезпечує врахування впливу на показники функціональної безпечності: динаміку підключення та різновиди активного резерву (гарячий, холодний, теплий); функціонування засобів контролю, діагностики та комутації; різновид стратегії технічного обслуговування; часову та функціональну надлишковість, введену в алгоритм поведінки радіоелектронної системи відповідального призначення.
3. Метод розрахунку середнього значення ймовірності існування мінімального січення, який на відміну від існуючих, враховує дію прихованих відмов не тільки в кінці інтервалу планово-профілактичного обслуговування, а в будь-який момент часу на інтервалі експлуатації, що дає змогу отримати достовірні значення ймовірностей існування мінімальних січень для випадків, коли мінімальне січення містить виключно приховані відмови або комбінації прихованих та явних відмов. Разом з цим, за допомогою середніх значень ймовірностей появи мінімальних січень можна отримати середнє значення ймовірності появи аварійної ситуації РЕСВП за наявності прихованих відмов.
4. Показники безпечності для відмовостійких РЕСВП з мажоритарною структурою: ймовірність потрапляння РЕСВП в передаварійну ситуацію та частоту потраплянь в аварійну ситуацію, які на відміну від існуючих кількісних показників, дають змогу визначити момент здійснення реконфігурації мажоритарної структури та вибрати доцільні варіанти резервування та стратегії технічного обслуговування. А це, насамперед, дає змогу синтезувати безпечні РЕСВП з мажоритарною структурою, які з мінімальною кількістю надлишковості забезпечують задані показники функціональної безпечності та надійності.
5. Характеристику безпечності експлуатації алгоритму поведінки РЕСВП – частоту потрапляння у стани неуспішного завершення, яка на відміну від існуючих показників, відображає зв'язок між надлишковістю (часовою і функціональною) введеною в алгоритм і функціональною безпечністю. Це дало змогу підчас розв’язання задачі синтезу алгоритму поведінки оцінювати вплив введеної часової і функціональної надлишковості на показники ефективності РЕСВП, а врахування замість абсолютних значень від’ємних приростів частоти потрапляння в стани неуспішного завершення алгоритму поведінки забезпечує можливість не завищувати вимоги до апаратних засобів РЕСВП.

Набули подальшого розвитку:

1. Метод простору станів з використанням структурно-автоматної моделі, в якому, на відміну від існуючого, запропоновано удосконалену структуру вектора стану та маску аварійної ситуації, що дало змогу автоматизовано розділити простір непрацездатних станів в залежності від рівня критичності відмови, що

забезпечило отримання траєкторії розвитку аварійних ситуацій і в результаті отримати комплексну модель, з якої визначати як показники надійності, так і функціональної безпечності.

2. Метод побудови дерева відмов, згідно якого, на відміну від існуючого, дерево відмов формується на базі функції аварійності і дає змогу перейти до логіко-ймовірнісної моделі від моделі у вигляді графа станів і переходів, що забезпечує візуалізацію аварійної ситуації і полегшує валідацію логіко-ймовірнісної моделі проектантом.
3. Моделі стратегій технічного обслуговування для планово-профілактичного обслуговування та аварійно-відновлювальних робіт, які, на відміну від існуючих, дають змогу враховувати вплив на показники функціональної безпечності: виникнення прихованих відмов в будь-який момент часу; простою РЕСВП при відключенні її підсистем під час проведення процедур технічного обслуговування; аварій, спричинених раптовими відмовами; і призначені для розв’язання задач синтезу стратегії технічного обслуговування із заданим рівнем функціональної безпечності та мінімізувати вплив на безпечність прихованих відмов.
4. Моделі відмовостійких систем з мажоритарною структурою для РЕСВП, які на відміну від існуючих, забезпечують врахування впливу на функціональну безпечність наявність резерву, можливість реконфігурації мажоритарної структури, використання технічного обслуговування і ремонту, і дають змогу синтезувати структуру РЕСВП із заданим рівнем функціональної безпечності і доцільним рівнем структурної надлишковості, що є особливо важливим для бортових інформаційно-керуючих систем літальних апаратів, зокрема безпілотних, для яких масо-габаритні показники є критичними.
5. Метод синтезу параметрів стратегії технічного обслуговування за заданим значенням показника функціональної безпечності, в основу якого покладено визначення функції готовності з врахуванням ймовірності появи аварійної ситуації і, на відміну від існуючих методів, враховує в тривалостях простою не тільки зупинку РЕСВП при проведенні аварійно-відновлювальних робіт, а й примусову зупинку роботи РЕСВП підчас проведення планово-профілактичних обслуговувань для пошуку та усунення прихованих відмов, що дає змогу уникнути завищення значень функції готовності при розрахунках, а відповідно підвищити достовірність.

Практичне значення одержаних результатів. Основним практичним результатом дисертації є зменшення інтелектуального навантаження на розробника РЕСВП за рахунок розроблення низки методик і алгоритмів. Ці методики і алгоритми дали змогу: автоматизувати окремі етапи процесу оцінювання ризику експлуатації РЕСВП; підвищити достовірність, отриманих показників функціональної безпечності та надійності за рахунок підвищення ступеня адекватності моделей у вигляді графа станів та переходів; зменшити затрати часу розробника на розв'язання проектних завдань синтезу відмовостійкої структури, алгоритму поведінки та процедур стратегії технічного обслуговування та ремонту РЕСВП. Серед одержаних практичних результатів слід відзначити:

1) Методику синтезу моделі стратегії технічного обслуговування сукупності

РСВП у вигляді системи диференційних рівнянь Колмогорова – Чепмена. Розроблена методика, на відміну від існуючих, дає змогу проектантові отримувати модель, в якій враховано вплив на показники функціональної безпечності РЕСВП (ймовірність появи аварійної ситуації та ймовірності існування мінімальних січень) наступних параметрів стратегії технічного обслуговування: періодичності фази моніторингу прихованих відмов; середнє значення тривалості фази проведення планово-профілактичного обслуговування; періодичності фаз проведення планово-профілактичного обслуговування; середнє значення тривалості фази проведення аварійно-відновлювальних робіт; швидкість переходу ремонтної бригади від планово-профілактичного обслуговування до аварійно-відновлювальних робіт; кількість РЕСВП, які можуть бути на обслуговуванні одної ремонтної бригади. А також враховано показники надійності РЕСВП.

2) Методики надійнісного параметричного синтезу РЕСВП з мажоритарною структурою з реконфігурацією та дворівневою мажоритарною структурою. Показано, що середнє значення тривалості безвідмовної роботи відмовостійкої РЕСВП з використанням дворівневої мажоритарної структури, з умовою збереження її працездатності, коли справним залишається 1 ядро із 3, є більшим, зокрема в порівнянні з відмовостійкою РЕСВП на основі мажоритарної структури з фіксованим правилом прийняття рішення типу «2 із 3» на 9480 годин (або на 114 %), а в порівнянні з відмовостійкою РЕСВП з використанням дворівневої мажоритарної структури, з умовою збереження її працездатності, коли справними залишаються 2 ядра із 3, на 10937 год. (або на 159 %).

3) Методологію синтезу безпечних алгоритмів поведінки РЕСВП, в яких на відміну від існуючих врахована часова надлишковість, у вигляді циклів повторного виконання критичних функцій, та функціональну надлишковість у вигляді передачі виконання задачі іншим підсистемам РЕСВП. Ця методологія дає змогу проектантам створювати методики синтезу безпечних алгоритмів поведінки для кожного конкретного типу РЕСВП, в яких є можливість використовувати названі вище види надлишковості і досягти заданого рівня ймовірності виконання задачі при жорстких обмеженнях на тривалість виконання задачі.

4) Методику підтвердження достовірності отриманого результату синтезу безпечного алгоритму поведінки. Дана методика забезпечує підтвердження достовірності отриманого результату синтезу безпечного алгоритму поведінки РЕСВП шляхом його отримання принципово іншим методом, оскільки на етапі системотехнічного проектування отримати результати експериментальним шляхом є неможливим.

Основні результати дисертаційної роботи використано і впроваджено:

- Компанія МС Зв’язок, при розробленні стратегій технічного обслуговування коміркових станцій мобільного зв’язку.
- ТОВ «Поліном–Стиль» – для оцінювання безпечності системи автоматизованого керування.
- Науковий центр Академії сухопутних військ імені гетьмана Петра Сагайдачного – для оцінювання функціональної безпечності та надійності безпілотних літальних апаратів, для аналізу ефективності розвідувальних комплексів.

- У держбюджетних науково-дослідних роботах , що виконувалися на кафедрі теоретичної радіотехніки та радіовимірювань з 2004 по 2018 рік.
- У навчальний процес спеціальності 172 «Телекомунікації та радіотехніка» в курс лекцій з дисциплін «Надійнісне проектування телекомунікаційних систем та мереж», «Методи забезпечення надійності великих систем», «Технологія моделювання ТК систем».

Особистий внесок здобувача. Основні наукові результати дисертаційної роботи отримано автором самостійно. У працях, опублікованих у співавторстві, авторові належить: [1, 4, 6, 26, 47, 51, 54] – обґрунтування необхідності розділення простору непрацездатних станів на безпечні, критичні та аварійні, поняття функції аварійності, метод визначення функції аварійності, удосконалення структури вектора станів, поняття маски аварійної ситуації, концепція автоматизації процедур вибору різних типів непрацездатних станів; [7] – метод отримання середніх значень ймовірності існування мінімальних січень для випадку, коли вони містять комбінації прихованих та явних відмов або виключно приховані відмови; [5, 12] – метод отримання дерева відмов з функції аварійності, алгоритм автоматизованої побудови дерева відмов; [8, 11, 14, 15, 16] – метод синтезу безпечних алгоритмів РЕСВП, поняття функції безпечності для алгоритмів поведінки; [2, 9, 18, 19, 39] — представлення процесу технічного обслуговування РЕСВП у вигляді системи масового обслуговування, метод синтезу параметрів стратегії технічного обслуговування за заданим значенням показника її ефективності, моделі стратегій планово-профілактичного обслуговування та аварійно-відновлювальних робіт, алгоритми автоматизованого синтезу стратегій технічного обслуговування; [10] – моделі відмовостійких систем з мажоритарною структурою; [3] – структурна схема надійності РЕСВП безпілотного літального апарата; [13, 20, 26, 35, 54, 55, 56] – комплексна модель у вигляді станів для отримання з неї мінімальних січень, поняття бінарної структурно-автоматної моделі; [17, 53] – методика валідації методу синтезу безпечних алгоритмів поведінки за допомогою схеми шляхів; [21, 22, 57, 58] – математична модель стратегії технічного обслуговування з врахуванням виникнення аварійних ситуацій, спричинених явними та прихованими відмовами; [37] – метод визначення функції готовності з врахуванням ймовірності появи аварійної ситуації; у роботах [27] – метод синтезу параметрів стратегії технічного обслуговування за заданим значенням показника її ефективності; [32, 33, 34, 41] – методика та моделі синтезу моделі стратегії технічного обслуговування групи РЕСВП у вигляді системи диференційних рівнянь Колмогорова – Чепмена для випадків експоненційного та неекспоненційного розподілу ймовірності для тривалостей перебування у станах; [29, 49] – модель та методика дослідження функції готовності, ймовірності появи аварійної ситуації та функцій аварійності РЕСВП; [24, 31] – модель безпечної відмовостійкої РЕСВП з реконфігурацією ядра мажоритарної структури; [28, 40] – алгоритми автоматизації для методики синтезу показників ефективності стратегії технічного обслуговування та розрахунку функції готовності РЕСВП за допомогою програмного забезпечення MatLab; [23, 39] – модель та методика визначення показників надійності для синтезу структури РЕСВП із заданим рівнем безпечності; [30, 38] – модель та методика синтезу безпечної відмовостійкої РЕСВП з використанням дворівневої мажоритарної структури; [43 – 46, 48, 50, 52, 59] –метод та моделі для розв’язання задачі синтезу

безпечних алгоритмів поведінки РЕСВП; [36, 42] – модель та методика введення часової та функціональної надлишковості в алгоритм поведінки.

Апробація результатів дисертації. Основні наукові результати і положення дисертаційної роботи представлялися, доповідалися та були обговорені на 30-ти міжнародних та всеукраїнських науково-технічних конференціях: міжнародна науково-технічна конференція «Сучасні проблеми радіоелектроніки, телекомунікацій та комп'ютерних наук TCSET» (Україна, Славське–Львів, 2004, 2006, 2008, 2010, 2016, 2018, 2020), міжнародна науково-технічна конференція CADSM «Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці» (Україна, Поляна 2003, 2005, 2011), міжнародна науково-технічна конференція «International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management, SMRLO» (Ізраїль, Бер–Шева, 2016), міжнародний симпозіум «Надёжность и качество» (Росія, Пенза, 2003, 2004, 2006, 2007, 2008, 2011, 2012), міжнародна науково-технічна конференція «Modelowanie i symulacja komputerowa w technice» MiS'2003, (Польща, Лодзь, 2003), міжнародна науково–технічна конференція «Uradzenia i systetemy radioelektroniczne UiSR'09» (Польща, Варшава, 2009), міжнародна науково–технічна конференція «ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer: ICTERI» (Україна, 2015, 2019), міжнародна науково–технічна конференція «Радіотехнічні поля, сигнали, апарати та системи, РТПСАС» (Україна, Київ 2012, 2013, 2014), міжнародна науково–технічна конференція «Фізико–технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано– та мікроелектроніки PREDT», (Україна, Чернівці, 2011, 2012, 2013, 2014, 2017, 2018, 2019); міжнародна науково–технічна конференція «Dependable Systems, Services & Technologies DeSSerT» (Україна, Київ, 2018); міжнародна конференція з інформаційно–телекомунікаційних технологій та радіоелектроніки УкрМіКо'2017 (Україна, Київ, 2017); міжнародна науково–технічна конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій» (Україна, Запоріжжя 2012, 2014), міжнародна науково-технічна конференція «Computer Science & Engineering CSE» (Україна, Львів, 2013), міжнародна конференція з автоматичного управління «Автоматика» (Україна, Львів, 2011), міжнародна науково-практична конференція «Информационно-телекомуникационные системы» (Росія, Москва, 2005), міжнародна науково-технічна конференція «Современные информационные системы. Проблемы и тенденции развития» (Росія, Туапсе, 2007), всеукраїнські науково–практичні конференції «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій СПТЕЛ» (Львів, 2011, 2012, 2013, 2014), «Проблеми та перспективи розвитку економіки і підприємництва та комп′ютерних технологій в Україні» (Львів, 2006, 2008, 2011, 2013), «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування СПРТП» (Вінниця, 2009, 2011).

Публікації. За результатами досліджень, які викладені в дисертаційній роботі, опубліковано 118 наукових праць, серед них монографій – 2, патент України на винахід – 1, статей у іноземних періодичних виданнях – 5 (з них 5 – у науковій періодиці, що входить до міжнародних наукометричних баз різного рівня Scopus, Index Copernicus, Infobase Index, Academic Research Index), статей у фахових виданнях

України – 36 (з них 13 – у науковій періодиці, що входить до міжнародної наукометричної бази Index Copernicus), у періодичних наукових виданнях України – 1, у збірниках матеріалів міжнародних та всеукраїнських конференцій – 73, (з них – 27 індексованих у наукометричних базах Scopus та Web of Science).

Структура та обсяг роботи. Робота складається з переліку умовних скорочень, розширеної анотації українською та англійською мовами, вступу, п’яти розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи складає 353 сторінки друкарського тексту, з яких 245 сторінок основного тексту, 61 рисунок, 17 таблиць, список використаних джерел із 253 найменувань, 4 додатки на 76 сторінках. Додатки містять структурно-автоматні моделі та алгоритм автоматизації синтезу показників ефективності стратегій технічного обслуговування РЕСВП, акти впровадження та список наукових праць автора.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** наведена загальна характеристика роботи, обґрунтовано актуальність теми дисертації, показано зв’язок роботи з науковими програмами, темами, сформульовано мету та основні завдання, об’єкт, предмет та методи дослідження, подано наукову новизну, практичну цінність отриманих результатів. Подано відомості про впровадження результатів роботи, вказано особистий внесок автора і наведено відомості про апробацію результатів дисертаційної роботи та про публікації за темою роботи, подано короткий опис структури і обсягу дисертації.

Перший розділ – «Сучасний стан та тенденції розвитку теорії синтезу безпечних радіоелектронних систем відповідального призначення на етапі системотехнічного проектування» – містить аналітичний огляд інформаційних джерел, присвячених проблемі забезпечення заданого рівня функціональної безпечності РЕСВП на етапі системотехнічного проектування. Особливістю етапу системотехнічного проектування РЕСВП є те, що він має обмежену тривалість – два-три місяці. За цей час потрібно сформувати конкурентні варіанти реалізації системи і на основі аналізу вибрати доцільний. При формуванні структури та алгоритму поведінки РЕСВП, на етапі системотехнічного проектування, необхідно вирішити дві важливі задачі: забезпечення заданого рівня функціональної безпечності та заданого рівня надійності. Під час вирішення цих задач виникає протиріччя (рис. 1). Для досягнення заданого рівня функціональної безпечності визначають слабкі місця РЕСВП і вводять засоби підвищення безпечності. Однак при введенні в систему

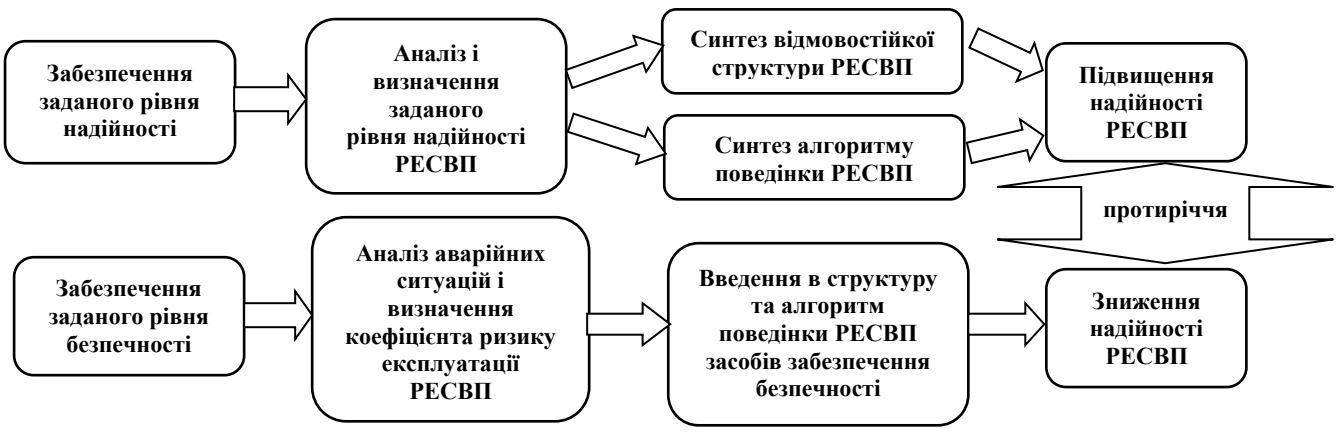


Рис. 1. Протиріччя між надійністю та функціональною безпечністю РЕСВП

додаткових засобів для забезпечення безпечності знижується надійність системи, оскільки додаткові елементи будуть, з точки зору надійності, послідовно з'єднані з іншими елементами системи.

За результатами огляду сучасних методів оцінювання функціональної безпечності та надійності РЕСВП на етапі системотехнічного проектування встановлено, що всі методи оцінювання функціональної безпечності (дерева відмов, динамічні дерева відмов, дерева подій, бінарні діаграми рішень) для встановлення слабких місць системи передбачають визначення мінімальних січень для кожної конкретної аварійної ситуації РЕСВП. Однак, всі ці методи не дають змоги враховувати вплив на функціональну безпечність РЕСВП застосування відмовостійких мажоритарних структур з реконфігурацією, з дворівневим мажоритарним резервуванням; стратегій технічного обслуговування (з багатофазним обслуговуванням, з контролем явних та прихованих відмов); часової, інформаційної та функціональної надлишковості алгоритму поведінки. Але найвагомішим недоліком існуючих методів є те, що вони не дозволяють на основі одної моделі отримати показники функціональної безпечності і показники надійності. Також ці методи малопридатні для багатоваріантного аналізу впродовж короткого часу, що є визначальним на етапі системотехнічного проектування.

Тому, необхідно розробити метод побудови комплексної моделі РЕСВП, на основі якої можна отримати і показники надійності, і показники функціональної безпечності. Метод побудови моделі повинен бути орієнтований на багатоваріантний аналіз РЕСВП. Побудова моделі, після внесення змін в технічні рішення РЕСВП, має здійснюватися автоматизовано.

Аналіз інформаційних джерел показав, що суттєвий вплив на функціональну безпечність РЕСВП має технічне обслуговування (ТО). Причому стратегії ТО також треба розробляти на етапі системотехнічного проектування. Тому, підчас розроблення стратегії ТО необхідно мати модель, яка дасть змогу оцінити частоту потрапляння РЕСВП в аварійну ситуацію в залежності від різновиду стратегії. При цьому, важливим аспектом є врахування впливу прихованих відмов на показники безпечності.

Як показують інформаційні джерела, що забезпечення високого рівня функціональної безпечності складних технічних систем покладається на інформаційно-керуючу систему. Вона реалізується, як правило, в різних варіантах мажоритарної конфігурації (з реконфігурацією структури і відповідною зміною правила голосування, з дворівневою мажоритарною структурою) і має визначальний вплив на безпечність складної технічної системи в цілому. Тому необхідно розробити моделі, які дають-змогу визначати як частоту потрапляння в аварійну ситуацію, так і показники надійності (ймовірність безвідмовної роботи, функцію готовності тощо). На таких моделях проектант зможе отримати залежність зменшення значення частоти потрапляння в аварійну ситуацію від збільшення значень показників надійності і ТО.

Заданий рівень функціональної безпечності РЕСВП, крім відмовостійких конфігурацій та ТО, визначає її алгоритм поведінки (АП). Оскільки, алгоритм поведінки реалізовується в РЕСВП у вигляді програмного забезпечення, то підвищення рівня безпечності РЕСВП здійснюється введенням в АП часової, інформаційної та функціональної надлишковостей. Тому, необхідно розробити підхід

для побудови моделі АП, яка б дала змогу враховувати потрапляння АП в стан неуспішного виконання завдання і обчислювати кількісно частоту потрапляння РЕСВП в аварійну ситуацію в залежності від кількості циклів повторного виконання функцій, параметрів апаратних засобів, послідовності використання підсистем тощо.

Другий розділ роботи – **«Розвиток теоретичних засад оцінювання показників функціональної безпечності радіоелектронних систем відповідального призначення на основі методу простору станів»** присвячений розробленню методів, які дали можливість використовувати представлення РЕСВП у вигляді графа станів і переходів (ГСП) як комплексну модель для визначення і показників функціональної безпечності, і показників надійності. Основною перевагою такого підходу, на відміну від існуючих, є те, що він забезпечує урахування зв'язку між властивостями надійності та безпечності РЕСВП і дає змогу розв'язувати протиріччя між ними, шляхом знаходження компромісних рішень.

У формуванні підходу прийнято до уваги, що для оцінювання функціональної безпечності складних систем за допомогою дерев відмов чи інших логіко-ймовірнісних методів (динамічних дерев відмов, бінарних діаграм рішень, дерев подій) використовується поняття «мінімальне січення», яке відображають у вигляді логічних функцій. Мінімальні січення дають змогу визначати слабкі місця системи для конкретної аварійної ситуації. Можливості визначати мінімальні січення за допомогою використання методу простору станів на сьогодні не відомо. Однак, досвід використання моделей у вигляді ГСП дав підстави передбачити, що така можливість існує. Для отримання можливості визначати мінімальні січення з ГСП в дисертації введено нову характеристику функціональної безпечності – **«Функція аварійності»**.

Функція аварійності (ФА) – це залежність ймовірності виникнення в РЕСВП непрацездатних станів, які призводять до аварійної ситуації, від тривалості експлуатації. Властивості функції аварійності:

- функція аварійності – невід'ємна гладка функція:

$$Q_A(t) = \begin{cases} 0, t = 0 \\ f(t), 0 \le t \le \infty \\ 1, t \to \infty \end{cases} \quad (1)$$

- для конкретної РЕСВП кількість функцій аварійності $Q_A(t)$ дорівнює кількості мінімальних січень, що призводять до аварійної ситуації;
- значення функції аварійності для конкретного інтервалу тривалості експлуатації РЕСВП дорівнює значенню ймовірності виникнення мінімального січення, яке отримано за допомогою дерева відмов (ДВ) для такої ж тривалості її експлуатації;
- об'єднання усіх функцій аварійності $Q_{Ai}(t)$ відповідає ймовірності появи аварійної ситуації $Q_{AC}(t)$ на цьому інтервалі:

$$Q_{AC}(t) = 1 - \prod_{i=1}^{k}(1 - Q_{Ai}(t)), \quad (2)$$

де $Q_{Ai}(t)$ – і-та функція аварійності,

k – кількість функцій аварійності.

Для формування виразу ФА необхідно встановити сукупність непрацездатних станів, які призводять до аварійної ситуації. Оскільки одні й ті

ж стани можуть входити в склад різних аварійних ситуацій і відповідно у різні ФА, то необхідно мати засоби для їх однозначної ідентифікації. Для цього в роботі запропоновано метод розділення усіх можливих непрацездатних станів, в яких може перебувати система, на такі групи (рис. 2):

- Непрацездатні безпечні стани – це сукупність станів, в які переходить система в результаті відмови підсистем чи модулів, однак з цих станів система безпосередньо не потрапляє в аварійну ситуацію.
- Критичні (передаварійні) стани – це стани, в які переходить система з безпечних непрацездатних станів і які передують аварійній ситуації. Наступним переходом система потрапляє у аварійну ситуацію.
- Катастрофічні (аварійні) стани – це стани, які відповідають власне аварійній ситуації.

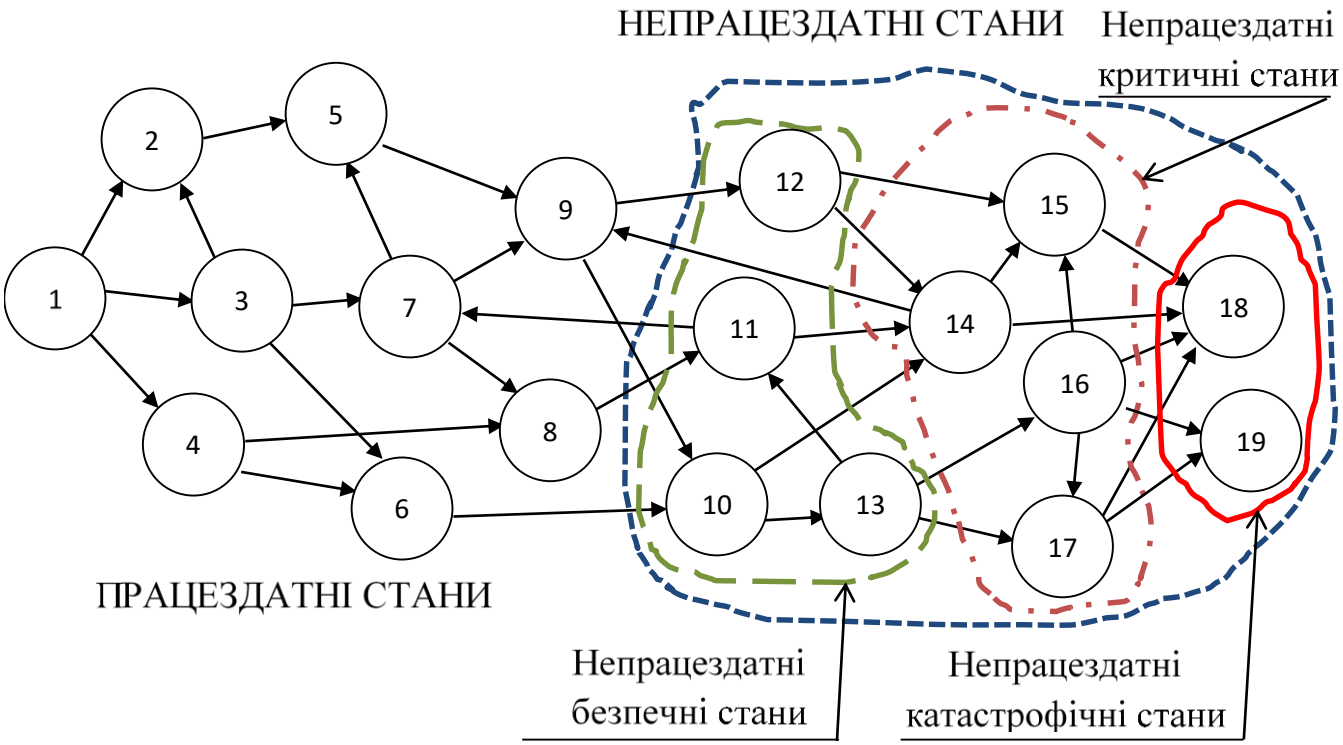


Рис. 2. Граф станів і переходів РЕСВП з розділеним простором непрацездатних станів для визначення функції аварійності

Така класифікація дає змогу з розподілу ймовірностей перебування в непрацездатних безпечних, критичних та катастрофічних станах сформувати ФА, показники функціональної безпечності та показники надійності РЕСВП безпосередньо з ГСП. Значення функції аварійності визначається як сума ймовірностей перебування в безпечних непрацездатних станах, критичних та катастрофічних станах. Переходи між цими станами показують траєкторію переходу (еволюцію) системи від несуттєвої відмови до аварії. Причому, чим менше переходів від непрацездатного безпечного стану до катастрофічного, тим гірші показники функціональної безпечності має система, і відповідно є менше можливостей уникнути аварійної ситуації.

Для визначення функції аварійності на основі ГСП в дисертації розроблено

низку методів та методик.

Першим з них є метод розділення непрацездатних станів системи. Структурна схема методу представлена на рис. 3. Суть цього методу полягає в генерації повного простору станів (без об'єднання непрацездатних станів в один стан), і розділення підпростору непрацездатних станів на три групи станів, описаних вище.

Для цього необхідно замінити структурно-автоматну модель бінарною структурно-автоматною моделлю. Бінарний опис стану передбачає введення окремої компоненти вектора стану для опису працездатного/непрацездатного стану кожного елемента (підсистеми, модуля тощо) РЕСВП, що забезпечить однозначну ідентифікацію як працездатного/непрацездатного стану, так і різновиду непрацездатного стану.

Крім цього, запропоновано ввести додаткові компоненти вектора станів, щоб

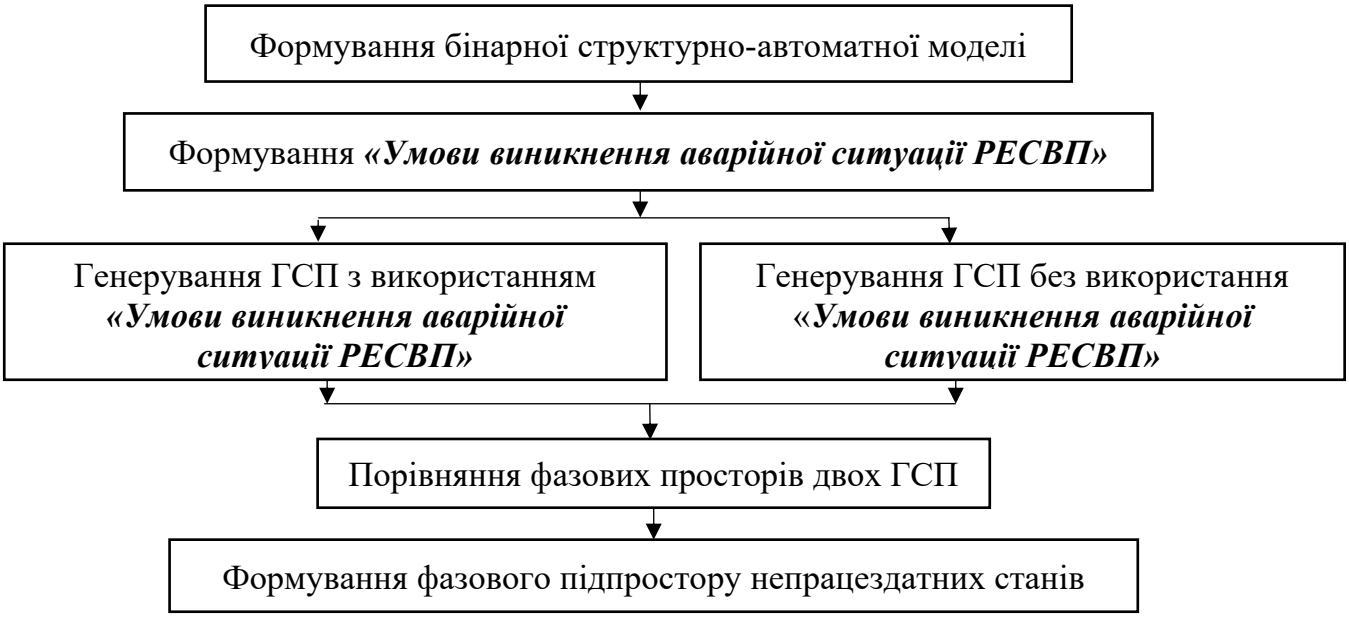


Рис. 3. Структурна схема методу розділення станів РЕСВП на працездатні та непрацездатні

відобразити вплив на функціональну безпечність параметрів стратегії ТО, засобів контролю і діагностики, засобів комутації (при активному резервуванні, реконфігурації тощо), ідентифікації режиму роботи системи (різновид резервування). Структура вектора станів (ВС) представлена на рис. 4.

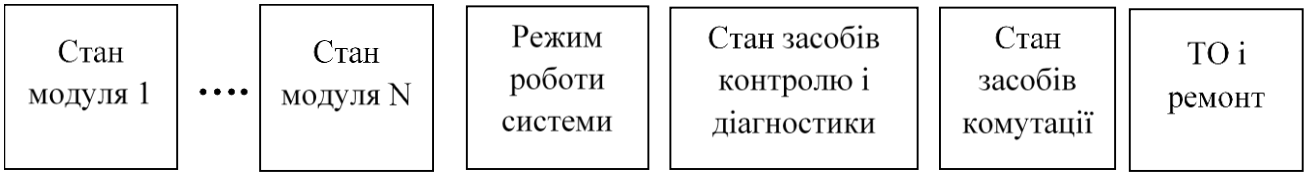


Рис. 4. Удосконалена структура вектора стану РЕСВП

Таким чином, за допомогою методу розділення станів (рис. 3) з графа станів та переходів (рис. 2) можна отримувати значення як показників безпечності (з непрацездатних станів) так і значення показників надійності системи (з працездатних станів). Зауважимо, що така комплексна модель у вигляді графа станів і переходів з удосконаленим описом стану дає змогу проводити дослідження залежностей впливу засобів підвищення надійності на значення показників безпечності і навпаки.

Для однозначного визначення з графа станів і переходів мінімальних січень, а з їх сукупностей – функцію аварійності, в дисертації запропоновано метод формування

функції аварійності в підпросторі непрацездатних станів.

На першому етапі метод передбачає формування масок аварійної ситуації. З їх допомогою здійснюється вибір непрацездатних станів, які формують конкретну аварійну ситуацію. ***Маска аварійної ситуації*** – це логічний вираз, сформований з компонент ВС. Слід зауважити, що необхідною і достатньою умовою для виникнення аварійної ситуації є рівність нулю всіх компонент вектора станів. Маска аварійної ситуації отримується з «Умови аварійної ситуації РЕСВП» шляхом її мінімізації за правилами алгебри логіки. Маска аварійної ситуації має наступні властивості:

- Якщо логічний вираз, який описує аварійну ситуацію, складається з компонент ВС, об'єднаних тільки оператором «AND», то для РЕСВП властива одна функція аварійності:

$$(Vg=0)\wedge(Vh=0)\wedge\ldots\wedge(Vk=0) \qquad (3)$$

- Якщо логічний вираз, який описує аварійну ситуацію, складається з N груп складових, об'єднаних операторами «OR», причому в кожній з груп компоненти ВС об'єднано тільки оператором «AND», то для РЕСВП властиві N функцій аварійності:

$$((Vm=0)\wedge(Vn=0)\wedge\ldots\wedge(Vq=0))\vee\ldots..\vee((Vs=0)\wedge(Vt=0)\wedge\ldots\wedge(Vy=0)) \qquad (4)$$

На другому етапі необхідно створити матрицю, яка складається з трьох стовпчиків: у перший стовбчик заносяться порядкові номера ФА – N, в другий – заносяться компоненти ВС та їх значення, у третій – заносяться номери станів, що формують відповідну ФА. Значення функції аварійності дорівнює сумі ймовірностей перебування у тих станах, що відповідають масці аварійної ситуації:

$$Q_{Ai}(t)=\sum_{j=m}^{q}P_j(t)+\ldots\ , \qquad (5)$$

де $P_j(t)$ – ймовірності перебування РЕСВП у групі непрацездатних станів m … q, у яких значення компонент ВС дорівнює нулю у відповідності до *i* – ї маски аварійної ситуації. Група непрацездатних станів в найпростішому випадку може включати усі непрацездатні стани. Для РЕСВП таких груп станів може бути декілька.

Третій розділ – «Модель та метод для розв'язання задачі синтезу стратегії технічного обслуговування, яка забезпечує заданий рівень функціональної безпечності радіоелектронної системи відповідального призначення». Технічне обслуговування полягає у проведенні двох видів робіт: аварійно-відновлювальних робіт (АВР) з ліквідації аварійних ситуацій, спричинених явними (діагностованими) відмовами та планово-профілактичного обслуговування (ППО) для усунення прихованих (не діагностованих) відмов. Явні відмови призводять до появи аварійної ситуації і відповідно до катастрофічних наслідків, а приховані – знижують ефективність засобів забезпечення відмовостійкості і зменшують запас безпечності системи.

Існуючі, на сьогодні, методи дають змогу оцінити тільки інтегральний показник функціональної безпечності за наявності прихованих та явних відмов. Це середнє значення ймовірності появи аварійної ситуації. Водночас відомі методи не дають змоги врахувати вплив стратегії ТО на безпечність РЕСВП в цілому. Відсутні методи та моделі, які дають змогу порівнювати окремі стратегії ТО між собою для вибору кращої з точки зору безпечності. А також для вибраної стратегії вирішувати задачу

параметричної оптимізації за критерієм мінімального середнього значення частоти потрапляння РЕСВП в аварійну ситуацію. Основна причина такого стану речей в тому, що при аналізі аварійних ситуацій існуючі методи дають змогу отримати достовірні значення ймовірностей існування мінімальних січень лише для випадку, якщо всі відмови є явними. Якщо ж мають місце приховані відмови, то існуючі методи дають змогу оцінити мінімальні січення лише для найгіршого випадку. А це, в свою чергу, знижує достовірність визначення слабких місць в процедурах технічного обслуговування РЕСВП на початкових інтервалах часу її експлуатації.

Правильне представлення в моделі явних і прихованих відмов є важливим для розв'язання задачі синтезу стратегії технічного обслуговування одною бригадою багатьох РЕСВП, які функціонують одночасно. Для вирішення цієї проблеми в роботі запропоновано модель процесу ТО багатьох РЕСВП, які функціонують одночасно, у вигляді системи масового обслуговування (рис. 5) з врахуванням АВР, ППО та наявності прихованих відмов.

Запропонована система масового обслуговування включає в себе три черги заявок та канал обслуговування. Першу чергу формують заявки на проведення ППО. Другу чергу – заявки на усунення прихованих відмов. Третю чергу – заявки на проведення АВР, тобто усунення явних відмов. Черга заявок на усунення прихованих відмов відображає поточну кількість підсистем та модулів РЕСВП, на яких виникли приховані відмови. Черга заявок на проведення АВР відображає поточну кількість аварійних ситуацій, які виникли в підсистемах та модулях РЕСВП.

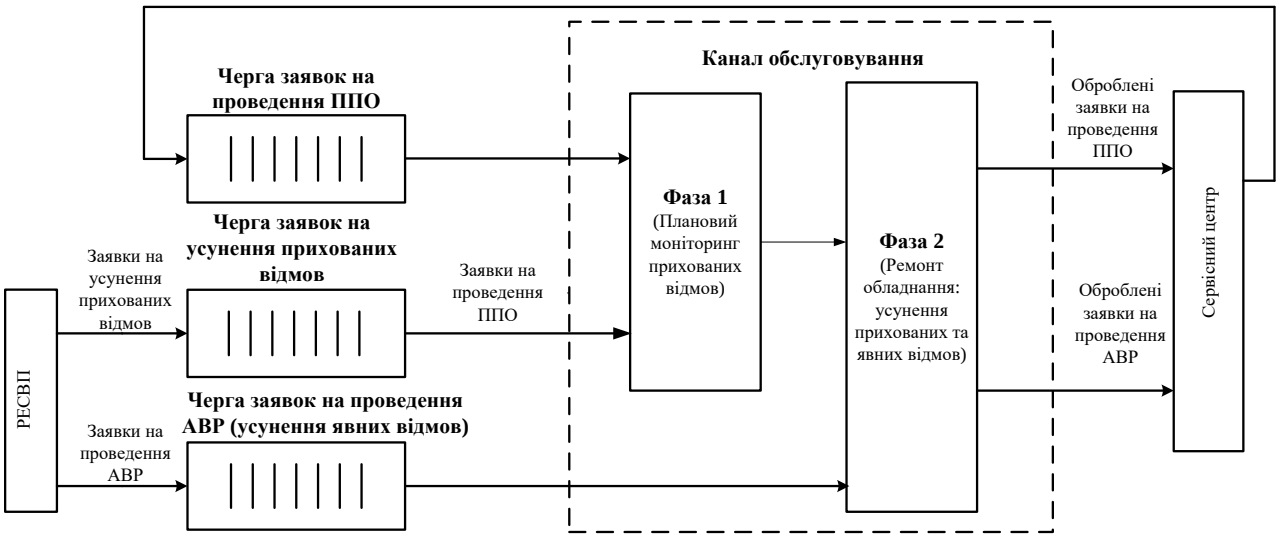


Рис. 5. Модель процесу технічного обслуговування сукупності РЕСВП, які функціонують одночасно, у вигляді системи масового обслуговування з трьома чергами та одноканальним багатофазним обслуговуванням

Оскільки для кожної РЕСВП властива одна аварійна ситуація, то максимальний розмір черги заявок на проведення АВР залежить від кількості РЕСВП, які знаходяться на обслуговуванні одної ремонтної бригади. Процес проведення ППО і АВР, в запропонованій моделі, представлено каналом з багатофазним обслуговуванням, кожна фаза якого відображає відповідний етап проведення відновлювальних робіт.

В даному розділі запропоновано новий метод визначення середнього значення ймовірності існування мінімального січення, яке включає в себе комбінацію

прихованих та явних відмов або виключно приховані відмови. Згідно цього методу модель для знаходження середнього значення ймовірності існування мінімального січення для загального випадку буде мати такий вигляд:

$$MCScep(y) = \frac{\sum_{i=1}^{N}((Le_1 \cdot t_{МЯ}) \cdot \ldots \cdot (Le_k \cdot t_{МЯ}) \cdot (Ll_1 \cdot t_{МП_i}) \cdot \ldots \cdot (Ll_r \cdot t_{МП_i}))}{N}, \quad (6)$$

де Le_k – інтенсивність появи явної k-ї відмови;

Ll_r – інтенсивність появи r-ї прихованої відмови;

$t_{МЯ}$ – інтервал часу від початку чергового застосування РЕСВП до моменту появи явної відмови (тривалість одноразового (безперервного) застосування РЕСВП);

$t_{МП}$ – інтервал часу від попереднього планового ТО до моменту наступного чергового планового ТО згідно ППО;

i – *i*-те застосування (місія) РЕСВП;

N – кількість застосувань РЕСВП, що припадає на один інтервал моніторингу прихованих відмов; *N = Tin/tm , де Tin – ……. , tm – ……. ;*

$Le*t_{МЯ}$ – ймовірність появи *i–ї* явної відмови;

$Ll*t_{МП}$ – ймовірність появи *i*–ї прихованої відмови.

Згідно результатів валідації методу визначення середнього значення ймовірності існування мінімального січення, твердження, що ***середнє значення ймовірності появи аварійної ситуації є сумою середніх значень ймовірностей існування мінімальних січень*** можна вважати правильним. На основі цього твердження запропоновано удосконалену формулу для визначення середнього значення ймовірності появи аварійної ситуації, яку можна представити як суму середніх значень ймовірностей існування мінімальних січень:

$$Qcep(x) = \sum_{j=1}^{Q} \frac{\sum_{i=1}^{N}((Le_1 \cdot t_{МЯ}) \cdot \ldots \cdot (Le_k \cdot t_{МЯ}) \cdot (Ll_1 \cdot t_{МН_i}) \cdot \ldots \cdot (Ll_r \cdot t_{МН_i}))_j}{N}, \quad (7)$$

де Q – кількість мінімальних січень

В розділі 3 розроблено структурно-автоматну модель стратегії ТО, представленої на рис. 5 системою масового обслуговування. На основі структурно-автоматної моделі автоматизовано отримується модель у вигляді графа станів та переходів, а відтак і модель у вигляді системи лінійних диференційних рівнянь. Ці моделі дають змогу створити методику синтезу стратегії ТО. Отримана за методикою стратегія ТО буде забезпечувати задані значення показників функціональної безпечності та готовності РЕСВП. Результатом розв'язання задачі синтезу стратегії ТО є значення таких її параметрів та показників: періодичності фази моніторингу прихованих відмов; середнє значення тривалості фази проведення ППО; періодичності фази проведення ППО; середнє значення тривалості фази проведення АВР; швидкості переходу ремонтної бригади від ППО до АВР; інтенсивності відмов для кожної РЕСВП; кількості РЕСВП, які можуть бути на обслуговуванні одної ремонтної бригади. Модель стратегії ТО у вигляді графа станів і переходів подано на рис. 6 для випадку, коли на обслуговуванні ремонтної бригади є одна РЕСВП. При цьому частина підсистем цієї РЕСВП перебуває під постійним моніторингом, а частина – перевіряється по завершенню заданого інтервалу часу. Дана стратегія ТО передбачає проведення ППО з певним періодом для усунення прихованих відмов та АВР для

усунення аварійних ситуацій, спричинених явними відмовами.

Розроблена структурно-автоматна модель дає змогу автоматизовано побудувати модель для загального випадку, коли на обслуговуванні одної ремонтної бригади є до декількох десятків РЕСВП. В цьому випадку кількість станів може сягати до $10^3 \ldots 10^4$.

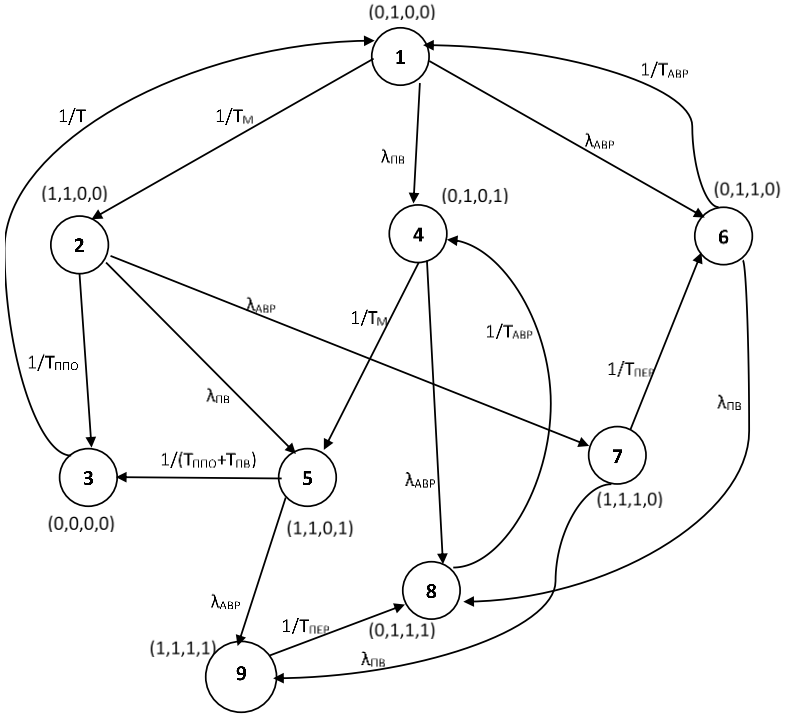
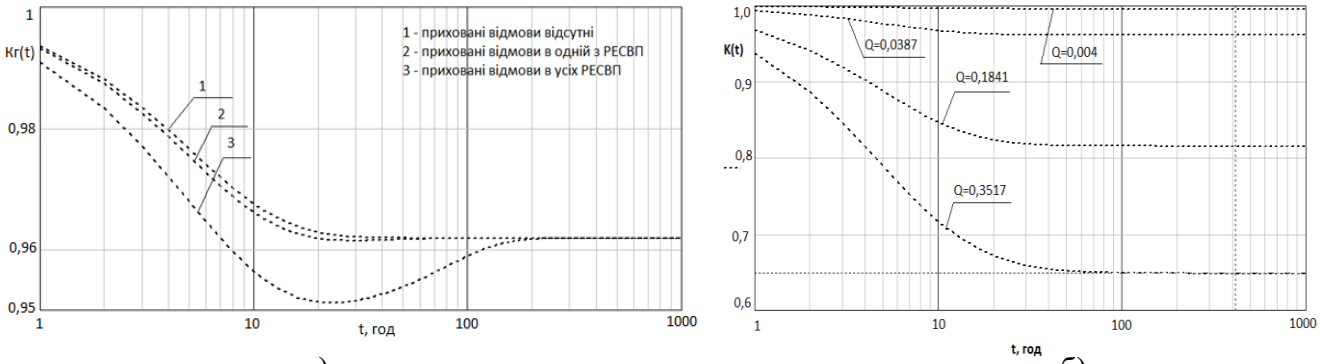


Рис. 6. Модель стратегії ТО у вигляді графа станів і переходів, в якій представлено проведення ППО та АВР для усунення прихованих та явних відмов

Результати порівняльного дослідження залежності функції готовності 5-ти РЕСВП від тривалості їх експлуатації для трьох варіантів наявності прихованих відмов, які обслуговує одна ремонтна бригада подано на рис. 7а. Результати порівняльного дослідження залежності функції готовності 5-ти РЕСВП від тривалості їх експлуатації для чотирьох значень ймовірності появи аварійної ситуації, викликаної явними відмовами, подано на рис. 7б.



а) б)

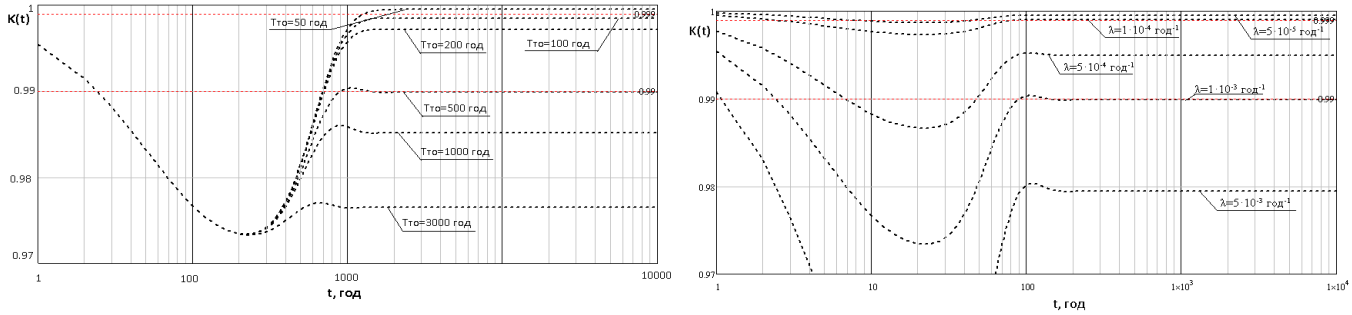
Рис.7. Залежності функції готовності сукупності з 5-ти РЕСВП від тривалості їх експлуатації для трьох варіантів наявності прихованих відмов (а) та для чотирьох значень ймовірності появи аварійної ситуації (б)

З проведених досліджень видно, що не врахування прихованих відмов призводить до завищення значення функції готовності на 1,5…2,1%, а не врахування аварійних ситуацій призводить до завищення значення функції готовності до 45%.

Залежності функції готовності сукупності з 5-ти РЕСВП від тривалості їх експлуатації для шести варіантів значень періодичності проведення ППО показані на рисунку 8а і для п’яти варіантів значень показника їх надійності (інтенсивності появи явних відмов) при періодичності проведення ППО 500 годин показані на рисунку 8б.

Отже запропонована модель дає змогу вибрати доцільну періодичність

проведення ППО і значення показника надійності кожної РЕСВП для забезпечення необхідного значення коефіцієнта готовності сукупності РЕСВП на заданому інтервалі їх експлуатації. На основі запропонованої структурно-автоматної моделі було розроблено і реалізовано в програмному забезпеченні MatLab методику синтезу параметрів стратегії обслуговування сукупності РЕСВП для забезпечення необхідного значення коефіцієнта готовності на заданому інтервалі їх експлуатації.



а) б)

Рис. 8. Залежності функції готовності сукупності з 5-ти РЕСВП від тривалості їх експлуатації для шести варіантів значень періодичності проведення ППО (а) і для п’яти варіантів значень інтенсивності появи явних відмов (б) при періодичності проведення ППО 500 годин

Четвертий розділ – «Синтез безпечних радіоелектронних систем відповідального призначення з використанням мажоритарних структур». В складних технічних системах (зв’язок, атомна енергетика, авіація, космічна галузь, наземний транспорт тощо) найбільш критичною, з точки зору функціональної безпечності, є інформаційно-керуюча система. Від надійності інформаційно-керуючої системи залежить безпечність експлуатації складної технічної системи. Вихід з ладу інформаційно-керуючої системи призводить до аварії складної технічної системи. Аварія складної технічної системи тягне за собою тяжкі наслідки, пов'язані із значними матеріальними втратами, загибеллю людей, екологічними катастрофами тощо. Тому інформаційно-керуючі системи є одним із різновидів РЕСВП.

Безпечність та надійність РЕСВП такого класу традиційно забезпечують використанням мажоритарних структур. Така структура складається з непарної кількості модулів ядра, резервних модулів та мажоритарного елемента. В якості модулів можуть використовуватися РЕСВП в цілому або її окремі підсистеми. В подальшому РЕСВП з мажоритарною структурою будемо називати відмовостійкою РЕСВП. Використання РЕСВП з мажоритарною структурою обґрунтовано тим, що даний різновид відмовостійких систем, крім високої надійності забезпечує: високий рівень функціональної безпечності завдяки апаратному захисту від збоїв; відсутність перерв у роботі після відмов окремих модулів; простоту процедури контролю та діагностики для виявлення несправних модулів.

В більшості сучасних РЕСВП використовується мажоритарна структура (МС) з фіксованим правилом прийняття рішення. Однак, в сучасних умовах, функціональна безпечність, яку вони забезпечують, є недостатньою. Введення додаткових засобів для підвищення функціональної безпечності знижує рівень надійності РЕСВП, і відповідно знижується тривалість її безперервної, безвідмовної експлуатації. Тому для подолання протиріччя між надійністю і безпечністю одним з найбільш перспективних методів підвищення рівня функціональної безпечності складних

технічних систем є підвищення надійності відмовостійкої РЕСВП з використанням МС без введення додаткових засобів забезпечення безпечності. В дисертації розглядаються три способи підвищення надійності відмовостійкої РЕСВП:

- Використання реконфігурації мажоритарної структури (зі зміною правила голосування). Цей спосіб дає змогу вийти з передаварійного стану і таким чином забезпечити довготривале функціонування з іншим правилом голосування для мажоритарного елемента.
- Використання дворівневої МС. Це дозволяє підвищити рівень безпечності з одночасним підвищенням рівня надійності без зміни правила голосування для мажоритарних елементів. В склад дворівневої МС в якості модулів входять РЕСВП з МС.
- Додавання до МС резервних модулів та використання технічного обслуговування та ремонту, що дозволяє збільшити тривалість безвідмовної роботи РЕСВП та не допускати тривалих простоїв складної технічної системи.

Однак, кількісно визначити на скільки кожен із вищезазначених способів підвищує безпечність за рахунок підвищення надійності відмовостійкої РЕСВП з використанням МС за допомогою відомих в практиці проектування моделей немає змоги. Причина в тому, що відомі моделі враховують тільки одне певне фіксоване правило прийняття рішення мажоритарним елементом (наприклад 2 із 3-х, 4 із 7-ми, 5 із 9-ти тощо). І в жодній з них не передбачена можливість оцінювання впливу різновиду МС на функціональну безпечність. Розв'язання таких завдань експериментальним шляхом потребує тривалої експлуатації і тому не прийнятне в принципі, оскільки втрати (матеріальні, людські) при виникненні аварійної ситуації є, як правило, дуже суттєвими.

В розділі показано вирішення проблеми оцінювання рівня функціональної безпечності РЕСВП з використанням МС шляхом використання запропонованих аналітичних надійнісних моделей, в яких враховано: поведінку відмовостійкої РЕСВП при втраті працездатності її модулів, тобто реконфігурацію мажоритарної структури, яка супроводжується зміною правила голосування; параметри стратегії аварійного відновлення; параметри засобів контролю, діагностики та комутації; ненадійність мажоритарного елемента; дворівневий мажоритарний принцип резервування (використання трьох мажоритарних структур вкладених в мажоритарну структуру).

Першим кроком, для вирішення вищезазначеної проблеми, було введено два нових показники функціональної безпечності для відмовостійких РЕСВП з використанням МС:

- ймовірність потрапляння РЕСВП в передаварійну ситуацію – $P_{pas}(t)$;
- частота потраплянь в аварійну ситуацію – $W_{as}(t)$.

Ймовірність потрапляння в передаварійну ситуацію $P_{PAS}(t)$ – визначається як сума ймовірностей перебування в передаварійних станах, для яких наступна відмова хоча б одного елемента МС призведе до втрати працездатності РЕСВП і відповідно до аварії складної технічної системи в цілому:

$$P_{pas}(t) = \sum_{i=1}^{x}\{P_i(t)\}, \quad (8)$$

де x – кількість передаварійних станів;

$P_i(t)$ – ймовірність перебування в *i-му* передаварійному стані за час експлуатації.

Даний показник необхідний для того, щоб оцінювати доцільність реконфігурації або враховувати підчас формування стратегії технічного обслуговування.

Частота потраплянь в аварійну ситуацію $W_{as}(t)$ – це густина розподілу ймовірності для випадкових інтервалів часу, в момент закінчення яких відмовостійка РЕСВП з використанням МС і відповідно складна технічна система потрапляє в аварійну ситуацію:

$$W_{as}(t) = \frac{dQ(t)}{dt} = \sum_{i=1}^{x}\{P_i(t) \cdot L_{i,F}\} \quad , \tag{9}$$

де $P_i(t)$ – ймовірність перебування в *i-му* передаварійному стані за час експлуатації;

$L_{i,F}$ – інтенсивності переходів з *i*-го передаварійного стану в аварійний стан F.

Для практичного визначення ймовірності потрапляння РЕСВП в передаварійну ситуацію та частоти потрапляння в аварійну ситуацію надійнісної моделі відмовостійкої РЕСВП з МС у вигляді графа станів та переходів, за допомогою методів розроблених в розділі 2, вибираються лише стани критичної відмови, після яких відмовостійка РЕСВП з МС переходить в стан катастрофічної відмови (аварійна ситуація складної технічної системи). На рис. 9 показано як збільшення надійності складових РЕСВП з МС забезпечує зростання функціональної безпечності. Наприклад, на інтервалі часу експлуатації 100 год, при зменшенні інтенсивності відмов модулів, що входять в склад РЕСВП, з 10^{-2} до 10^{-6}, частота Was(t) зменшується з $8 \cdot 10^{-2}$ до $3 \cdot 10^{-7}$.

Збільшення надійності РЕСВП з МС без застосування резервних модулів, а відповідно зменшення $W_{as}(t)$, можна досягти наступними способами, а саме: здійснити реконфігурацію мажоритарної структури або застосовувати дворівневу мажоритарну структуру або/і вводячи технічне обслуговування і ремонт складових системи. Ознакою (тригером) для здійснення реконфігурації буде попадання відмовостійкої РЕСВП з МС у передаварійний стан.

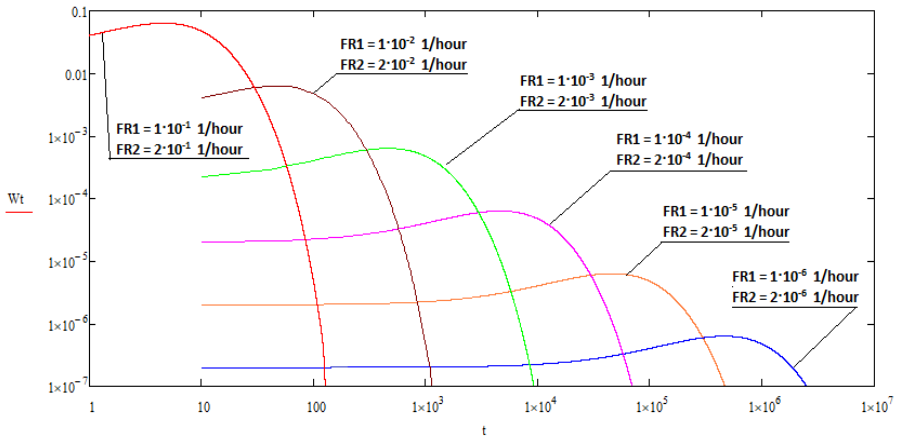


Рис.9 Залежності частоти потраплянь у аварійну ситуацію від тривалості експлуатації РЕСВП для шести значень інтенсивності відмов (FR) модулів МС

Для таких відмовостійких РЕСВП в дисертації запропоновано нові моделі для розв'язання задач синтезу показників і параметрів їх складових. Ці моделі розроблено у вигляді структурно-автоматних моделей з символьним представленням параметрів та показників надійності та функціональності складових відмовостійкої РЕСВП.

Для відмовостійкої РЕСВП з реконфігурацією структурно-автоматна модель представлена в табл. 1, а система диференційних рівнянь має вигляд (10).

Таблиця 1. – Структурно-автоматна модель відмовостійкої РЕСВП з реконфігурацією мажоритарної структури

Базові події	**Умови та обставини**	**Формули розрахунку інтенсивностей базових подій**	**Формули розрахунку ймовірностей альтернативних переходів**	**Правила модифікації компонент вектора станів**
Відмова модуля в ядрі МС	(V1>0) AND (V7=0)	$V1*\lambda_n$	1	V1:=V1–1; V2:=V2+1; V7:=1
Закінчення процедури підключення модуля з гарячого резерву в ядро МС	(V2>0) AND (V3=1) AND (V7=1)	$1/T_h$	P_h	V1:=V1+1; V2:=V2–1; V3:=0; V7:=0
			$1–P_h$	V2:=V2–1; V7:=0
	(V2>0) AND (V3=0) AND (V7=1)		1	V2:=V2–1; V7:=0
Закінчення процедури переведення модуля з холодного резерву в гарячий резерв	(V3=0) AND (V4>0) AND (V7=0)	$1/T_c$	P_c	V3:= 1; V4:=V4–1
			$1–P_c$	V4:=V4–1
Відмова резервного модуля, гарячий резерв	(V3=1)	λ_n	1	V3:=0
Закінчення процедури реконфігурації МС	(V1=V6) AND (V1>=3) AND (V2=0) AND (V3=0) AND (V8=1)	$1/T_{rec}$	P_{rec}	V1:=V1–1; V3:=1; V6:=V6–2
			$1–P_{rec}$	V1:=V1–1; V2:=V2+1; V7:=1
	(V1=V6) AND (V1>=3) AND (V2=0) AND (V3=1) AND (V8=1)		P_{rec}	V1:=V1–1; V4:=V4+1; V6:=V6–2
			$1–P_{rec}$	V1:=V1–1; V2:=V2+1; V7:=1
Критерій виникнення аварійної ситуації: (V1<V5)				

Після розв’язання системи рівнянь (10) отримується розподіл ймовірностей перебування у кожному стані, з якого компонуються формули для визначення показників надійності та функціональної безпечності РЕСВП. На рис. 10 подано результати порівняльного дослідження показників надійності відмовостійкої РЕСВП з використанням МС без реконфігурації і з реконфігурацією (а) та при різних значеннях ймовірності успішної реконфігурації (б).

Також за допомогою цієї ж моделі проектант має змогу отримувати показники функціональної безпечності. На рис. 11 представлено залежності ймовірності виникнення передаварійної ситуації (а) та частоти попадання (б) в аварійну ситуацію від тривалості експлуатації для чотирьох варіантів реалізації правила голосування.

Отримані результати дослідження (рис. 11) показують однозначний зв’язок між показниками надійності та безпечності для відмовостійкої РЕСВП з МС: чим більша кількість модулів в ядрі МС і відповідно більш висока її надійність, тим меншим є значення ймовірності потрапляння в критичні передаварійні стани і тим нижче значення частоти потрапляння відмовостійкої РЕСВП в аварійну ситуацію.

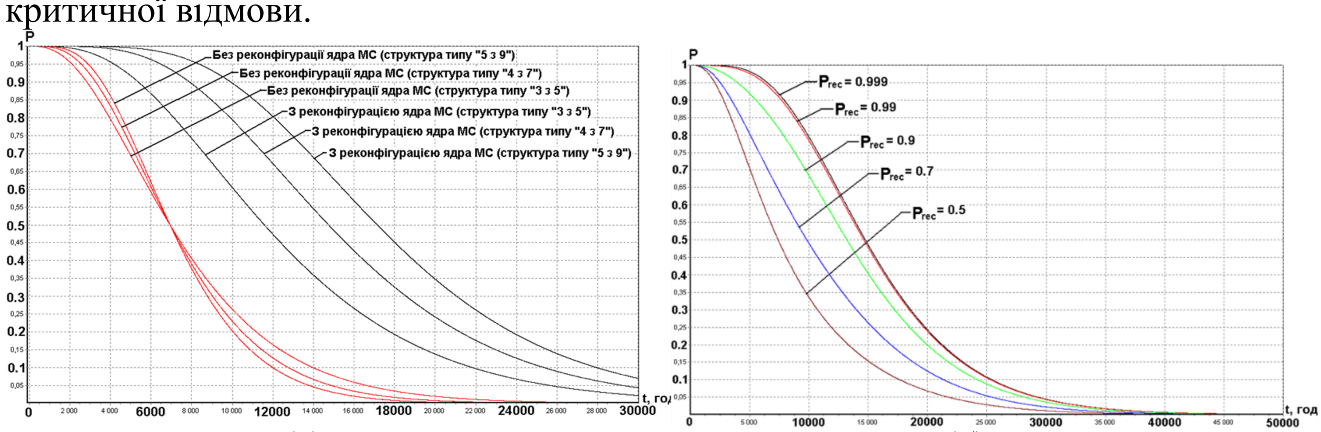
Зауважимо, що спадні ділянки залежностей не треба приймати до уваги, так як вони належать стану критичної відмови РЕСВП. Наведені вони для того, щоб показати наявність помилкових результатів при визначенні запропонованих показників функціональної безпечності за рахунок неправильного вибору тривалості

експлуатації РЕСВП.

В розроблених моделях враховано формування в процесі експлуатації РЕСВП ковзного резерву з працездатних модулів, які залишаються після втрати працездатності мажоритарних структур нижчого (першого) рівня. Якщо відмовляє мажоритарний елемент, то в ковзний резерв переходять три модулі. Якщо відмовляють два модулі ядра, то в ковзний резерв переходить один модуль.

$$\begin{cases} \dfrac{dP_1(t)}{dt} = -7\lambda \cdot P_1(t) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ \dfrac{dP_4(t)}{dt} = -6 \cdot \lambda \cdot P_4(t) + \dfrac{P_{rec}}{T_{rec}} \cdot P_3(t) \\ \dfrac{dP_5(t)}{dt} = -\dfrac{1}{T_h} \cdot P_5(t) + \dfrac{1-P_{rec}}{T_{rec}} \cdot P_3(t) \\ \dfrac{dP_6(t)}{dt} = -\left(\dfrac{P_h}{T_h} + \dfrac{1-P_h}{T_h}\right) \cdot P_6(t) + 5\lambda \cdot P_4(t) \\ \dfrac{dP_7(t)}{dt} = -5\lambda \cdot P_7(t) + \lambda \cdot P_4(t) + \dfrac{P_h}{T_h} \cdot P_6(t) \\ \dfrac{dP_8(t)}{dt} = -\left(\lambda + \dfrac{P_{rec}}{T_{rec}} + \dfrac{1-P_{rec}}{T_{rec}}\right) \cdot P_8(t) + \dfrac{1-P_h}{T_h} \cdot P_6(t) \\ \dfrac{dP_9(t)}{dt} = -5\lambda \cdot P_9(t) + \dfrac{1}{T_h} \cdot P_5(t) \\ \dfrac{dP_{10}(t)}{dt} = -\left(\dfrac{P_{rec}}{T_{rec}} + \dfrac{1-P_{rec}}{T_{rec}}\right) \cdot P_{10}(t) + \lambda \cdot P_8(t) + \dfrac{P_h}{T_h} \cdot P_{14}(t) + \dfrac{1}{T_h} \cdot P_{15}(t) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ \dfrac{dP_{29}(t)}{dt} = -\dfrac{1}{T_h} \cdot P_{29}(t) + 3\lambda \cdot P_{20}(t) \end{cases} \qquad (10)$$

Ковзний резерв призначений для підтримання працездатності мажоритарних структур нижчого (першого) рівня, що залишилися (залишаються) працювати до критичної відмови.



(а) (б)

Рис. 10. Залежності ймовірності безвідмовної роботи РЕСВП від тривалості експлуатації з використанням МС без реконфігурації і з реконфігурацією (а) та ймовірності успішної реконфігурації (б)

Дана модель дає змогу порівнювати надійність відомої відмовостійкої РЕСВП з використанням МС з фіксованим правилом голосування та відмовостійкої

РЕСВП з використанням дворівневої мажоритарної структури. Результати порівняння представлено на рис. 12 та в табл. 2. Середнє значення тривалості безвідмовної роботи відмовостійкої РЕСВП №6 на основі МС з фіксованим правилом голосування «2 із 3» плюс 6 модулів в резерві є більшим, в порівнянні з: відмовостійкою РЕСВП № 1 (табл. 2) на 241%; відмовостійкою РЕСВП № 2 на 213%; відмовостійкою РЕСВП № 3 на 131%; відмовостійкою РЕСВП № 4 на 60%; відмовостійкою РЕСВП № 5 на 28%.

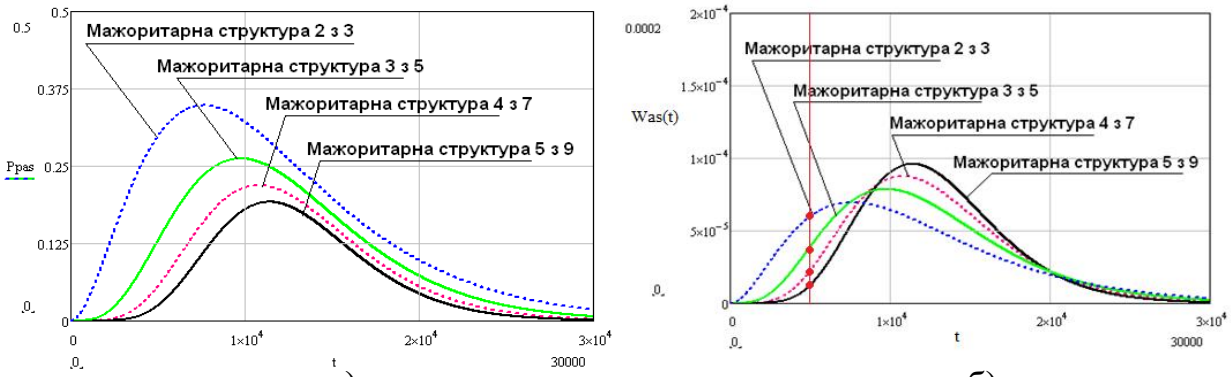


Рис. 11. Залежність ймовірності потрапляннння в передаварійні стани (а) та частоти попадання відмовостійкої РЕСВП в аварійну ситуацію (б) від тривалості її експлуатації для 4–х варіантів реалізації правила голосування

На рис. 13 показано взаємозв’язок між запланованою кількістю ремонтів на задану тривалість терміну експлуатації РЕСВП та значенням показника функціональної безпечності (ймовірністю потрапляння в передаварійний стан відмовостійкої РЕСВП з МС). Із збільшенням кількості ремонтів безпечність РЕСВП з МС зростає, оскільки максимум ймовірності перебування в передаварійній ситуації зменшується і наближається до закінчення терміну її експлуатації.

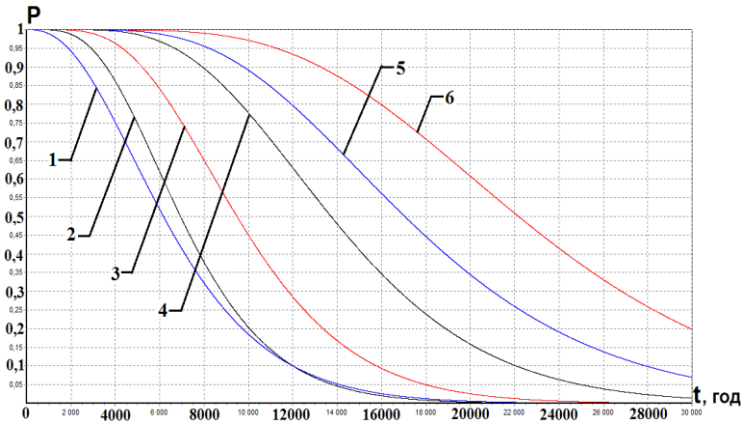


Рис. 12. Порівняння надійності 4-х варіантів побудови (реалізації) відмовостійкої РЕСВП з МС з фіксованим правилом голосування (криві 1, 3, 4, 6) та 2-х варіантів побудови (реалізації) відмовостійкої РЕСВП з використанням дворівневої мажоритарної структури (криві 2 і 5)

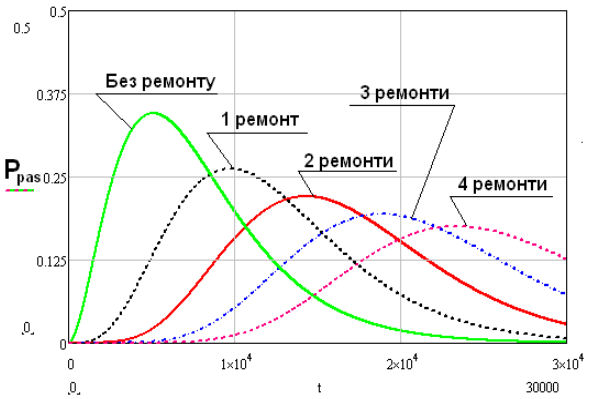


Рис. 13. Залежності ймовірностей виникнення передаварійної ситуації у відмовостійкій РЕСВП з МС з правилом голосування «3 із 5» і з різною кількістю ремонтів, від тривалості її експлуатації

На основі розроблених моделей в роботі сформовано дві методики надійнісного

синтезу відмовостійких РЕСВП з реконфігурацією мажоритарної структури та відмовостійких РЕСВП з дворівневою мажоритарною структурою. В таблиці 2 показані результати порівняння надійності РЕСВП, для якої розглядається використання 6 варіантів забезпечення відмовостійкості. В таблиці використано такі позначення: Nr – кількість робочих модулів в МС; Nz – загальна кількість модулів; G і M – кількість модулів в гарячому і холодному резерві. Тсер – середній час роботи до відмови. Для коректності порівняння у всіх варіантах однакова загальна кількість модулів – 9.

Таблиця 2 – Порівняння надійності РЕСВП, для якої використано 6 варіантів забезпечення відмовостійкості

Тип відмовостійкої РЕСВП	**N_r/N_z**	**G**	**M**	**Тсер, год**	**К-ть станів**	**К-ть переходів**
РЕСВП №1. Дворівнева мажоритарна структура з правилами голосування на обох рівнях «2 із 3», яка втрачає працездатність після втрати працездатності двох ядер	**9/9**	**0**	**0**	**6840**	**80**	**308**
РЕСВП №2. МС з фіксованим правилом голосування «5 із 9»	**9/9**	**0**	**0**	**7460**	**9**	**18**
РЕСВП №3. МС з фіксованим правилом голосування «4 із 7» (2 модулі в резерві)	**7/9**	**1**	**1**	**10099**	**28**	**78**
РЕСВП №4. МС з фіксованим правилом голосування «3 із 5» (4 модулі в резерві).	**5/9**	**1**	**3**	**14502**	**40**	**118**
РЕСВП №5. Дворівнева мажоритарна структура з правилами голосування на обох рівнях «2 із 3», яка втрачає працездатність з втратою працездатності останнього ядра	**9/9**	**0**	**0**	**18131**	**200**	**794**
РЕСВП №6. МС з фіксованим правилом голосування «2 із 3» (6 модулів в резерві)	**3/9**	**1**	**5**	**23266**	**36**	**110**

В **розділі 5** – **«Синтез безпечних алгоритмів поведінки радіоелектронних систем відповідального призначення»** розроблено методологію синтезу безпечних алгоритмів поведінки, на основі якої проектант може створювати свою методику синтезу для конкретного варіанту реалізації алгоритму поведінки. Методологія доповнена моделями та методами, які адекватно враховують усі особливості алгоритму поведінки, що визначають функціональну безпечність РЕСВП. Створені на основі методології методики дадуть змогу проектанту за короткий час (в рамках тривалості етапу системотехнічного проектування РЕСВП) здійснювати розв’язання задачі синтезу безпечного алгоритму через багатоваріантний аналіз.

Функціональна безпечність РЕСВП визначається як її відмовостійкою структурою, так і функціональною поведінкою. Функціональна поведінка визначається алгоритмом, який задає умови і послідовність дій підсистем та модулів РЕСВП при виконанні нею своїх функцій. Алгоритм поведінки для РЕСВП розробляється на етапі її системотехнічного проектування. Прикладом таких АП є алгоритми пошуку і виявлення цілей, алгоритми отримання, запису та передавання телеметричних даних, алгоритми отримання навігаційних даних тощо.

Особливістю алгоритмів поведінки РЕСВП є те, що для них притаманне як успішне так й неуспішне завершення. Неуспішне завершення АП призводить до

аварійних ситуацій. Неуспішне завершення АП зумовлюється помилками оператора, втратою працездатності апаратних чи програмних засобів, неточними вхідними даними, неправильним спрацюванням засобів контролю та діагностики тощо. Для мінімізації кількості неуспішних завершень роботи РЕСВП, а відповідно для забезпечення заданого рівня функціональної безпечності РЕСВП, використовується часова та функціональна надлишковості.

Часова надлишковість передбачає повторне виконання сукупності операційних блоків АП, якщо в результаті зовнішніх (завад, помилок оператора) чи внутрішніх (відмов і збоїв) випадкових чинників не вдалось виконати задану функцію за першим разом. Функціональна надлишковість передбачає переключення (перехід) на інший спосіб виконання задачі (переключення на іншу систему), якщо дана система після заданої кількості повторних циклів не змогла виконати завдання, або тривалість виконання циклу перевищила граничне значення.

Характерною особливістю РЕСВП є граничне значення тривалості виконання кожної функції АП. Якщо це значення перевищить гранично допустиме, то АП не успішно завершує свою роботу і РЕСВП потрапить у критичну відмову. А складна технічна система, в складі якої функціонує ця РЕСВП, в аварійну ситуацію. Таким чином введення часової надлишковості при певних вимогах до тривалості виконання АП може бути не прийнятним. Для мінімізації ймовірності потрапляння у стан неуспішного завершення АП, а відповідно потрапляння у аварійну ситуацію необхідно визначити граничну кількість повторень кожного циклу. Якщо РЕСВП після кількох повторних циклів не змогла виконати завдання, а тривалість виконання циклу перевищила граничне значення,-то відбувається переключення на інший спосіб виконання невиконаної функції (переключення на іншу підсистему, що входить в склад РЕСВП). Якщо і ця підсистема не змогла виконати свою функцію, то здійснюється переключення на наступну. Якщо всі функції РЕСВП, передбачені алгоритмом поведінки, виконано, то маємо успішне його завершення. Якщо ні, то неуспішне завершення. Відповідно складна технічна система, в складі якої функціонує ця РЕСВП, попадає в аварійну ситуацію.

Перевірка доцільності введення кожного з різновидів надлишковості повинна виконуватися на етапі системотехнічного проектування РЕСВП. Відсутність такої можливості у сучасних засобів проектування змушує здійснювати перевірку на предмет безпечності лише на етапі випробувань складної технічної системи. Однак такий підхід не завжди є прийнятним, оскільки за наявності помилок в алгоритмі поведінки РЕСВП в аварійну ситуацію потрапляє і складна технічна система в цілому.

В основу методології синтезу безпечних алгоритмів покладено удосконалену стохастичну модель АП у вигляді графа станів і переходів, в якій розрізняються групи станів, що визначають функціональну безпечність РЕСВП. Стани поточного виконання АП визначаються детермінованими чинниками (кількість операційних блоків, тривалість виконання операційного блоку, кількість циклів, кількість шляхів від одного операційного блоку до іншого тощо). А стани успішного завершення та аварійні стани визначаються випадковими чинниками, які призводять до невиконання чи зупинки АП (вихід з ладу підсистем, не спрацювання окремих підсистем, помилки оператора, тривалість виконання АП ($T_{ВИК}$) перевищує граничне значення ($T_{ГР}$), зовнішні завади тощо). Таким чином повний простір станів буде складатися з трьох

груп станів:

- стани першої групи будуть відображати процес переходу від одного операційного блоку АП до наступного в процесі виконання РЕСВП своєї задачі;
- стани другої групи – це стани успішного завершення АП;
- стани третьої групи – це стани неуспішного завершення АП.

В процесі виконання алгоритму поведінки, РЕСВП буде знаходитись в першій групі станів певний час, значення якого ($T_{ВЗ}$) не повинно перевищувати граничне значення тривалості виконання ($T_{ГР}$) задачі. В залежності від зовнішніх та внутрішніх чинників РЕСВП буде переходити в стани групи 2 або 3. Якщо тривалість перебування РЕСВП в першій групі станів перевищить граничне значення ($T_{ГР}$), то РЕСВП не виконає свого завдання і складна технічна система потрапить в аварійну ситуацію. Якщо РЕСВП за час $T_{ВЗ} \leq T_{ГР}$ переходить у групу станів 2, то свою функцію РЕСВП виконала успішно. Якщо РЕСВП потрапляє в групу станів 3, то для них існує два варіанти наслідків:

- при $t < T_{ГР}$, РЕСВП може повертатись в групу станів 1 в результаті повторного виконання частини АП. Причому, кількість потраплянь в групу станів 3 з групи станів 1 і назад при виконанні вищезазначеної умови може бути декілька.
- при $t \geq T_{ГР}$, РЕСВП залишається в групі станів 3, тому що АП потрапляє у стан неуспішного завершення. В цьому варіанті РЕСВП спричиняє аварійну ситуацію.

Перебування РЕСВП в групах станів 1 та 2 характеризується ймовірністю успішного виконання задачі – $P_{ВЗ}(t)$. Потрапляння РЕСВП в групу станів 3 характеризується ймовірністю неуспішного (аварійного) завершення АП – Q(t).

Однак, ймовірність неуспішного завершення АП за час t є інтегральною характеристикою алгоритму і визначене з неї середнє значення тривалостей неуспішного завершення АП не дає змоги оцінити як часто РЕСВП потрапляє в аварійний стан. Тому в дисертації запропоновано ввести нову характеристику функціональної безпечності експлуатації АП – **частоту потрапляння у стани неуспішного** завершення за час, необхідний (витрачений) для виконання алгоритму поведінки (11). Це обумовлено тим, що використані під час проектування (синтезу) АП і часова, і функціональна надлишковості «вимагають» збільшення часу на виконання алгоритму поведінки.

$$w(t) = \frac{dQ(t)}{dt} = \sum_{q=0}^{z-1} \lambda_{z,z-q} \cdot P_{z-q}(t), \qquad (11)$$

де $\lambda_{z,z-q}$ – інтенсивність переходів в стан неуспішного завершення АП z з стану z – q,

$P_{z-q}(t)$ – ймовірність перебування РЕСВП в стані z – q,

Характеристика функціональної безпечності експлуатації АП має вигляд, показаний на рис. 14. Якщо РЕСВП не має ні функціональної, ні часової надлишковості, то максимум характеристики функціональної безпечності w(t) буде в точці t = 0.

За наявності надлишковості характеристика w(t) в момент t = 0 приймає значення нуль і далі зростає до певного максимального значення, а тоді спадає до нуля. Чим

більше часу буде додано до номінальної тривалості виконання АП на виконання процедур часової та функціональної надлишковості тим нижчим буде максимальне значення характеристики w(t) і тим далі вправо цей максимум переміститься. Тобто, при збільшенні часу на виконання процедур часової і функціональної надлишковості, частота потрапляння в аварійний стан зменшується.

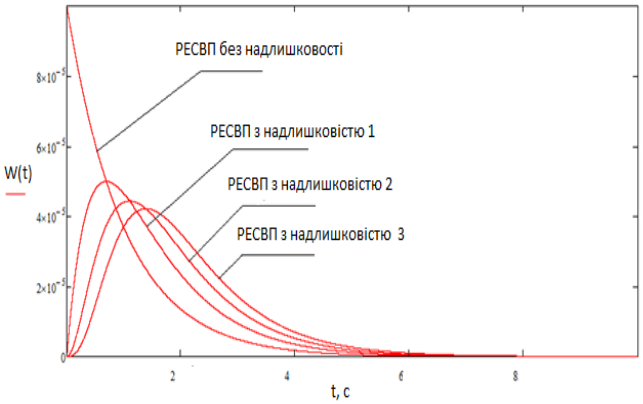


Рис. 14. Варіанти вигляду характеристики безпечності АП

Для синтезу безпечних алгоритмів поведінки РЕСВП розроблено методологію, суть якої полягає у визначенні вимог до параметрів і показників функціональності часової та функціональної надлишковостей, які забезпечать мінімальне значення максимуму характеристики w(t). Задача синтезу АП вирішується з урахуванням обмежень на: граничне (мінімальне) значення ймовірності успішного завершення АП – $P_{ГР}(t)$; граничне значення ймовірності неуспішного завершення АП – Q(t); граничне значення допустимого середнього значення тривалості виконання АП – $T_{ГР.}$

Методологія синтезу безпечних АП базується на запропонованих в дисертації методах та стохастичних моделях і представлена схемою на рис. 15. Для розроблення методик синтезу АП конкретних РЕСВП методологія рекомендує проектантам провести деталізацію виконання п’яти етапів.

Етап 1: Евристичний синтез алгоритму поведінки РЕСВП. Формування еквівалентного алгоритму на основі його оригіналу. Еквівалентний алгоритм – це модель оригіналу у вигляді блок-схеми, в якому враховано блоки неуспішного/успішного завершення та стохастичні перевірочні блоки.

Етап 2. Розроблення структурно-автоматної моделі алгоритму поведінки на основі еквівалентного алгоритму. Структурно-автоматна модель дає змогу здійснювати формалізовану (автоматизовану) побудову моделей у вигляді графа станів і переходів для будь-яких значень показників функціональності та параметрів АП.

Етап 3. Формування аналітичної моделі алгоритму поведінки у вигляді системи диференціальних рівнянь Колмогорова-Чепмена та її розв’язання. Даний етап вирішується застосуванням методу простору станів.

Етап 4. Компонування формул для визначення показників ефективності алгоритму поведінки. Формули компонуються евристичним методом.

Етап 5. Розв’язання задач синтезу безпечних алгоритмів поведінки РЕСВП. Метод розв’язання – багатоваріантний аналіз доцільних варіантів реалізації (побудови) АП. Процедура знаходження мінімального значення максимуму характеристики w(t) є *двоетапною*. На *першому етапі* для різних значень ймовірності виконання підсистемою своєї функції здійснюється зміна тривалості її виконання і знаходиться при якому значенні тривалості виконання, значення від’ємного приросту частоти потрапляння в аварійну ситуацію буде найбільшим. Ця процедура

виконується для кожної підсистеми РЕСВП. На *другому етапі* фіксується знайдене значення тривалості виконання функції кожною підсистемою і аналогічно знаходиться ймовірність її виконання, при якій значення від'ємного приросту частоти потрапляння в аварійну ситуацію буде найбільшим. З графіка (рис. 16) видно, що при значенні тривалості t = 0,02 с від'ємний приріст частоти потрапляння в аварійну ситуацію збільшується максимально для усіх значень (0,98; 0,99; 0,999) ймовірності виконання функції підсистемами РЕСВП.

В результаті отримаємо АП, який при конкретних параметрах апаратних та програмних засобів забезпечує задану ймовірність успішного завершення і разом з цим отримаємо найменше значення частоти потрапляння в аварійну ситуацію.

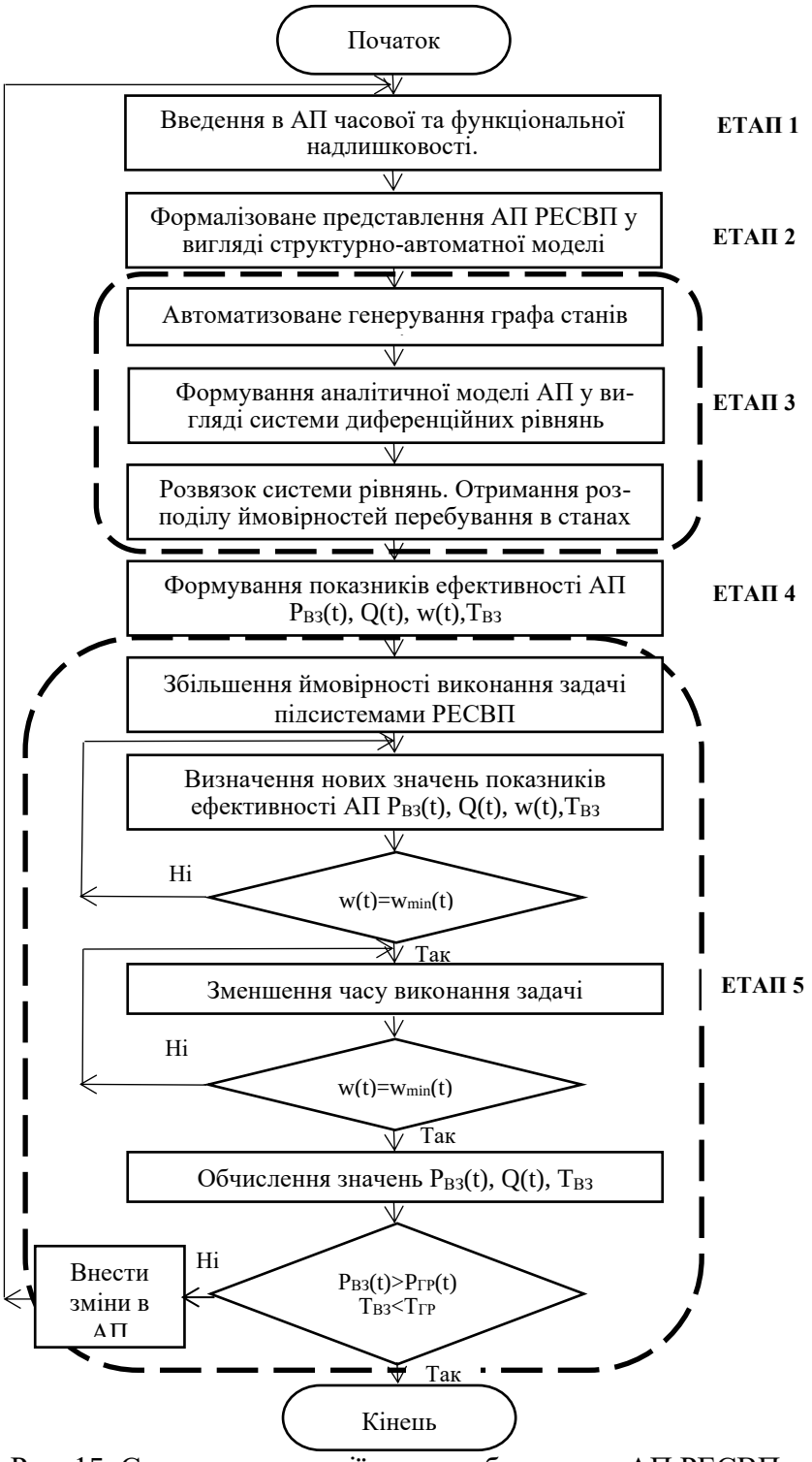


Рис. 15. Схема методології синтезу безпечних АП РЕСВП

Зв'язок характеристики безпечності експлуатації АП з показником ефективності РЕСВП приведено на рис. 17.

Перевірку правильності одержаного в результаті розв'язання задачі синтезу алгоритму поведінки РЕСВП необхідно здійснювати шляхом моделювання АП принципово іншим методом з подальшим порівнянням отриманих результатів. Альтернативний метод повинен дати змогу враховувати неуспішні виконання АП та наявність стохастичних та детермінованих переходів в алгоритмі. Так як серед відомих методів моделювання АП не виявлено метода, який би відповідав цим вимогам, було запропоновано новий метод – «метод схеми шляхів». Схема шляхів є

формалізованим представленням функціональної поведінки РЕСВП в компактній формі, що відображає сукупність всіх шляхів в АП, які ведуть до виконання або невиконання завдання РЕСВП. На відміну від методу простору станів, метод схеми шляхів не дає змоги отримати показники ефективності у вигляді залежності від тривалості експлуатації, а лише у вигляді точкових значень ймовірності потрапляння РЕСВП в стан критичної відмови при неуспішному завершенні АП та середнє значення тривалості виконання завдання РЕСВП.

Ці точкові значення будуть порівнюватися з відповідними значеннями, отриманими за допомогою моделі у вигляді графа станів та переходів. При їх співпадінні можна зробити висновок про правильність розв'язання задачі синтезу АП.

Застосування характеристики функціональної безпечності експлуатації АП w(t)

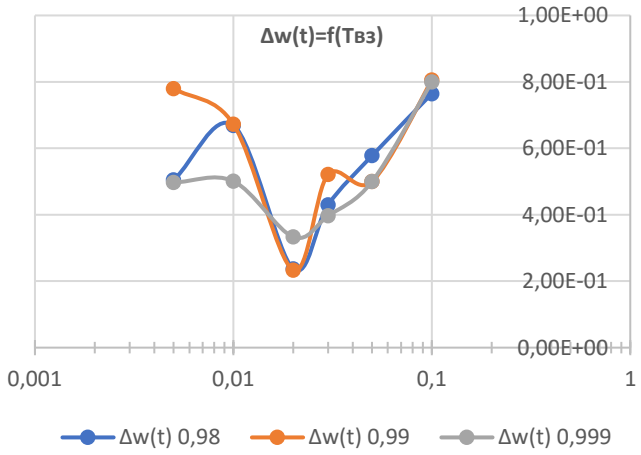


Рис. 16. Залежність від'ємного приросту частоти потрапляння в аварійну ситуацію від тривалостей виконання підсистемами РЕСВП своїх функцій

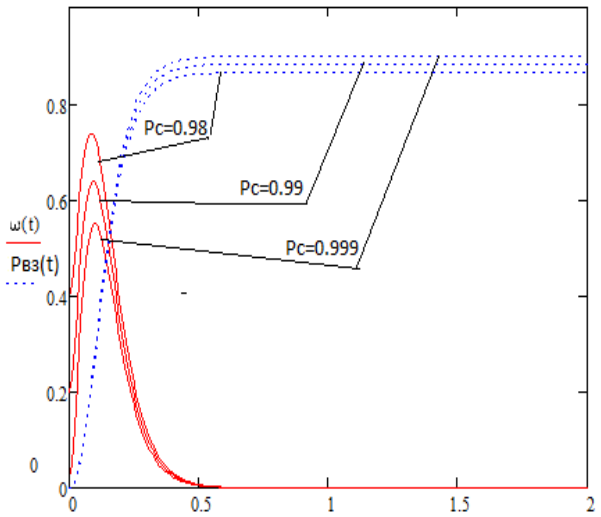


Рис. 17. Зв'язок характеристики безпечності експлуатації АП з показником ефективності РЕСВП

дало змогу по частоті потрапляння в стани неуспішного виконання АП оцінювати вплив введеної часової і функціональної надлишковостей на показники ефективності РЕСВП. А врахування замість абсолютних значень від'ємних приростів частоти потрапляння в стани успішного завершення АП, дає змогу не завищувати вимоги до апаратних засобів РЕСВП.

Основні результати та висновки

В дисертації розв'язано науково-прикладну проблему підвищення ефективності процедур синтезу радіоелектронних систем відповідального призначення шляхом розвитку теоретичних засад комплексного забезпечення заданого рівня функціональної безпечності та надійності на етапі системотехнічного проектування. Ефективність процедур синтезу полягає, з одного боку, в скороченні витрат часу на розроблення моделей для двох і більше варіантів побудови РЕСВП, а з іншого – в підвищенні ступеня достовірності отриманих показників функціональної безпечності. Підвищення достовірності забезпечується врахуванням впливу на функціональну безпечність: відмовостійких структур зі складною поведінкою, алгоритмів поведінки із часовою та функціональною надлишковістю та стратегій технічного обслуговування. А високий рівень формалізації запропонованих методів

та моделей дає змогу автоматизувати процедури синтезу РЕСВП із заданим рівнем функціональної безпечності.

В дисертації отримано наступні наукові результати:

1. На основі проведеного аналізу відомих методів оцінювання функціональної безпечності РЕСВП встановлено, що використані в них моделі не дають можливості отримати разом з показниками функціональної безпечності, ще і показники надійності та оцінювати їх взаємозв'язок. Також відомі методи не призначені для багатоваріантного аналізу, що важливо на етапі системотехнічного проектування РЕСВП. Разом з цим встановлено, що обов'язковим показником, на основі якого здійснюється оцінювання функціональної безпечності, FMEA/FMECA–аналіз та PHA/HAZOP/LOPA–аналіз, є мінімальні січення.

2. Запропоновано метод розділення непрацездатних станів на непрацездатні безпечні стани, критичні та катастрофічні стани. В основу метода покладено методику класифікації непрацездатних станів, удосконалено структуру вектора станів та введено поняття маски аварійної ситуації, що дало змогу однозначно класифікувати різновиди непрацездатних станів. Разом з цим розроблено методику побудови бінарної структурно-автоматної моделі.

3. Введено поняття функції аварійності для оцінювання функціональної безпечності РЕСВП та принципи її формування з простору непрацездатних станів за допомогою маски аварійності. Для цього розроблено метод формування функції аварійності в підпросторі непрацездатних станів, який передбачає визначення груп станів, що відповідають кожній функції аварійності, містить процедури сортування компонент масок аварійних ситуацій, знаходження функцій аварійності, порівняння станів у функціях аварійності та формування виразів для функцій аварійності. Для візуалізації результату побудови функції аварійності розроблено метод побудови дерева відмов на основі функцій аварійності.

4. Розроблено метод визначення середнього значення ймовірності виникнення мінімального січення за наявності прихованих відмов. Метод дає змогу отримати середнє значення ймовірності появи аварійної ситуації як суму середніх значень мінімальних січень, які містять як комбінації явних та прихованих відмов, так і виключно приховані відмови. Слід відзначити, що відомі методи визначення середнього значення ймовірності виникнення мінімального січення враховують тільки явні відмови. В процесі валідації розробленого методу встановлено, що середнє значення ймовірності виникнення мінімального січення, яке містить виключно явні відмови, визначене існуючим та запропонованим методами – співпадають. Цим підтверджується правильність запропонованого методу. Середні значення ймовірностей виникнення мінімальних січень, які містять комбінації явних та прихованих відмов та значення ймовірностей виникнення мінімальних січень, визначених відомими методами, відрізняються в 3,9 рази, причому відомі методи дають завищені значення цих ймовірностей. Середні значення ймовірностей виникнення мінімальних січень, які містять виключно приховані відмови та значення ймовірності виникнення мінімальних січень, визначених існуючими методами відрізняються на два порядки (в 107,9 рази).

5. Запропоновано нове представлення стратегії технічного обслуговування сукупності РЕСВП одною ремонтною бригадою у вигляді системи масового

обслуговування. На основі цього представлення отримано математичну модель стратегії технічного обслуговування РЕСВП з врахуванням виникнення аварійних ситуацій, спричинених явними та прихованими відмовами. На базі моделі розроблено два методи для автоматизованого визначення функції готовності з врахуванням ймовірності появи аварійної ситуації та автоматизованого синтезу параметрів стратегії технічного обслуговування за заданим значенням коефіцієнта готовності. Не врахування прихованих відмов завищує коефіцієнт готовності від 3 до 5%, якщо кількість РЕСВП, які знаходяться на обслуговуванні у одної ремонтної бригади, не перевищує 10. При збільшенні кількості РЕСВП завищення значення коефіцієнта готовності зростає.

6. Розроблено методику розв'язання задачі синтезу стратегії технічного обслуговування сукупності РЕСВП. Методика дає змогу проводити дослідження функції готовності, ймовірності появи аварійної ситуації та функцій аварійності РЕСВП. Оскільки ця методика призначена для багатоваріантного аналізу, то створено алгоритм автоматизованого розрахунку функції готовності РЕСВП за допомогою програмного забезпечення MatLab та алгоритм автоматизації розв'язання задач синтезу показників стратегії її технічного обслуговування та ремонту.

7. Для синтезу безпечних РЕСВП з використанням мажоритарної структури з реконфігурацією та дворівневої мажоритарної структури розроблено математичні моделі, які дають змогу отримати нові показники функціональної безпечності відмовостійких систем цього класу: ймовірність потрапляння РЕСВП в передаварійну ситуацію та частоту потраплянь в аварійну ситуацію. Це дало змогу оцінювати вплив різних способів підвищення надійності РЕСВП з використанням мажоритарним структур на її безпечність. На основі цих моделей розроблено методику надійнісного синтезу відмовостійкої РЕСВП з реконфігурацією мажоритарної структури та методику синтезу відмовостійкої РЕСВП з використанням дворівневої мажоритарної структури. Ці методики дозволяють скоротити витрати часу для розв'язання задачі синтезу кожного наступного варіанту побудови РЕСВП на 85 – 112%, причому з контролем заданого рівня функціональної безпечності.

8. Запропоновано нову характеристику функціональної безпечності експлуатації алгоритму поведінки – частоту потрапляння у стани неуспішного завершення за час, необхідний для виконання алгоритму поведінки. Розроблено методологію синтезу безпечних алгоритмів поведінки РЕСВП, яка забезпечує визначення ймовірність його аварійного завершення та частоту потрапляння у стан неуспішного завершення. На базі методології сформовано методику введення часової та функціональної надлишковості в алгоритм поведінки РЕСВП та методику синтезу алгоритмів поведінки, призначених для розроблення програмного забезпечення програмно-апаратної реалізації РЕСВП.

Список основних праць, в яких опубліковано результати дисертації

<u>Колективні монографії:</u>

1. Бобало Ю.Я. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем// Монографія / Ю.Я. Бобало, Б.Ю. Волочій, О.Ю. Лозинський, Б.А. Мандзій, Л.Д. Озірковський, Д.В. Федасюк, С.В.

Щербовських, В.С. Яковина. Львів: Видавництво Львівської політехніки, 2013. – 300 с., ISBN 978-617-607-468-7

2. Волочий Б. Проектирования эффективных стратегий технического обслуживания. Математические модели, алгоритмы и методики // Монография / Богдан Волочий, Леонид Озирковский, Игорь Кулык/ LAP LAMBERT Academic Publishing, Germany, 2015. – 160 с., ISBN 978-3-659-63366-9

Патенти:

3. Патент на винахід № 126099 Україна, МПК (2006): H02J 1/00. Система електропостачання малогабаритного безпілотного літального апарата / Пащук Ю. М., Корольов В.М., Озірковський Л.Д., Васінович В.Ю., Сальник Ю.П. (Україна); заявник – Національна академія сухопутних військ імені гетьмана Петра Сагайдачного. – № u201712061; заявл. 07.12.2017; опубл. 11.06.2018, бюл. № 11/2018.

Статті у наукових періодичних виданнях України та наукових періодичних виданнях інших держав, що входять до міжнародних наукометричних баз даних:

4. Volochiy B. The New Method of Building a Safety Model for Quantitative Risk Assessment of Complex Technical Systems for Critical Application/B. Volochiy, B. Mandziy, L. Ozirkovskyy//Communications in Computer and Information Science. – 2016. - Vol. 594. – P. 56 – 70. (ISSN: 1865-0929 (print), SCOPUS, Web of science)
5. Ozirkovskyy L., The Algorithm of Automated Development of Fault Trees for Safety Exploitation Assessment of Complex Technical Systems // L. Ozirkovskyy, A. Mashchak, O. Shkiliuk, S. Volochiy / Central European Researchers Journal, Volume 2, Issue 2, –2016, –P. 1 – 10 (ISSN: 2453-7314, Infobase Index, Academic Resource Index)
6. Volochiy B. Improvement of fidelity of moving objects classification in guard signaling complexes with seismic sensors / Mykhailo Zmysnyi, Leonid Ozirkovskyy, Volodomyr Onyschchenko, Yuriy Salnyk // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 8(4), –2018, – P. 36 – 39 (ISSN: 2391-6761 (Online) DOI: 10.35784, Index Copernicus)
7. Ozirkovskyy L. Adequacy Increase of Assessment of Minimal Cut Sets Considering Latent Failures / Leonid Ozirkovskyy, Bohdan Volochiy, Andriy Mashchak, Ihor Kulyk // Central European Researchers Journal, Vol.5 Issue 2, 2019, P. 58 – 66 (ISSN: 2453-7314, Infobase Index, Academic Resource Index)
8. Ozirkovskyy L. Synthesis of safe behavior algorithms of radioelectronic systems for critical applications /Leonid Ozirkovskyy, Bohdan Volochiy, Mykhailo Zmysnyi, Oleksandr Shkiliuk // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, volume 10 №1, –2020, – P. 28 – 31 (ISSN: 2391-6761)
9. Volochiy B. The maintanance strategy optimization of base stations of communication cellular network / B. Volochiy, L. Ozirkovskyy, I. Kulyk, M. Zmysnyi // Радіоелектронні і комп'ютерні системи. – 2016. – № 5 (79). – С. 120 – 129. (ISSN: 2663-2012, Index Copernicus, РІНЦ)
10. Volochiy B. Designing of fault-tolerant radio electronic systems with complex majority structures / B. Volochiy, L. Ozirkovkyy, M. Zmysnyi, I. Kulyk // Радіоелектронні і комп'ютерні системи. – 2016. – № 6 (80). – С. 43–53. (ISSN: 2663-2012, Index Copernicus, РІНЦ)

11. Мандзій Б.А. Технологія аналітичного моделювання дискретно-неперервних стохастичних систем на основі блок-схем алгоритмів їх поведінки / Мандзій Б.А., Волочій Б.Ю., Озірковський Л.Д. // Вісник Нац. ун-ту “Львів. політехніка”. – 2008. № 621: Інформаційні системи та мережі. – С.171–181 (ISSN 0321-0499)
12. Волочій Б.Ю. Методика побудови дерева відмов складної технічної системи на основі графу станів і переходів/Б.Ю. Волочій, Л.Д. Озірковський, А.В. Мащак, О.П. Шкілюк//Вісник академії митної служби України, серія "Технічні науки". – 2014. – №1(51), С. 10 – 19., (ISSN 2310-9645)
13. Волочій Б.Ю. Оцінка ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарату / Б.Ю. Волочій, Л.Д. Озірковський, Ю.М. Пащук, А.В. Мащак, В.А. Онищенко // Військово-технічний збірник : зб. наук. пр./Акад. сухопутних військ ім. гетьмана Петра Сагайдачного. – 2015. – Вип. 13. – С. 77 – 87. (ISSN: 2312-4458)
14. Волочій Б.Ю. Метод аналізу ефективності алгоритмів поведінки радіоелектронних комплексів відповідального призначення / Волочій Б.Ю., Озірковський Л.Д., Шкілюк О.П, Мащак А.В. // Науково-технічний журнал «Радіоелектронні і комп’ютерні системи». – 2014, №6 (70), – С. 130 – 134. (ISSN 1814-4225, Index Copernicus)
15. Волочій Б.Ю. Оцінка надійності програмно-апаратних систем за допомогою моделі їх поведінки / Волочій Б.Ю., Озірковський Л.Д., Чопей Р.С., Мащак А.В., Шкілюк О.П. // Вісник Національного університету «Львівська політехніка». Радіоелектроніка та телекомунікації. – 2014, № 796, – С. 222 – 231. (ISSN 0321-0499)
16. Волочій Б.Ю. Порівняння методів оцінки показників ефективності алгоритмів поведінки радіоелектронних комплексів / Б.Ю. Волочій, Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак // Вісник НТУУ "КПІ". Серія Радіотехніка. Радіоапаратобудування. – 2014, – №59, – С. 29 – 39. (ISSN 2310-0389, Index Copernicus)
17. Volochiy B. Technique of Construction Models of Behavior Algorithms of Radio Electronic Complex System using the Scheme of Paths Method / Bohdan Volochiy, Leonid Ozirkovskyi, Oleksandr Shkiliuk, Andriy Mashchak // International Journal of Computing, Vol. 13, Issue 3, 2014, – P. 183 – 190. (ISSN 1727-6209)
18. Мандзій Б. А. Оцінка ефективності комбінованої стратегії технічного обслуговування мережі коміркового зв’язку / Б. А. Мандзій, Б. Ю. Волочій, Л. Д. Озірковський, С. І. Гнатів, І. В. Кулик // Східно-Європейський журнал передових технологій. Інформаційно-керуючі системи. – Том 1, № 9 (61), 2013. – С. 40 – 44. (ISSN 1729-3774)
19. Мандзій Б. А. Дослідження впливу профілактичного технічного обслуговування на надійність відмовостійкого джерела безперебійного електроживлення / Б. А. Мандзій, Б. Ю. Волочій, Л. Д. Озірковський, Д. С. Кузнєцов, І. В. Кулик // Східно-Європейський журнал передових технологій. Енергозберігаючі технології та обладнання. – Том 1, №8 (61), 2013. – С. 8 – 12. (ISSN 1729-3774)
20. Волочій Б. Ю. Методика розрахунку мінімальних січень для відмовостійких систем на основі структурно-автоматної моделі / Б. Ю. Волочій, Л. Д. Озірковський, А. В. Мащак, О. П. Шкілюк, І. В. Кулик // Вісник Національного технічного університету

України “Київський політехнічний інститут” Серія – Радіотехніка. Радіоапаратобудування. – Київ. − 2013. вип. 52 – С. 38 – 45. (ISSN 2310-0389, Index Copernicus)

21. Волочій Б.Ю. Надійнісна модель відмовостійкої багатопроцесорної систем з відновленням працездатності програмного забезпечення / Б.Ю. Волочій, Л.Д. Озірковський, О.В. Муляк, М.М. Змисний, Т.І. Панський // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2013. – № 54. – С. 33 – 43. (ISSN 2310-0389, Index Copernicus)
22. Мандзій Б.А. Оцінка економічної ефективності технічного обслуговування та ремонту систем регіональних радіоелектронних комплексів / Б.А. Мандзій, Б.Ю. Волочій, С.І. Гнатів, Л.Д. Озірковський, І.В. Кулик // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2013. – № 54. – С. 160 – 170. (ISSN 2310-0389, Index Copernicus)
23. Волочій Б.Ю. Методика визначення показників надійності відмовостійких програмно-апаратних радіоелектронних систем / Б.Ю. Волочій, Л.Д. Озірковський, Т.І. Панський, О.В. Муляк // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2013. – № 55. –С. 71 – 79. (ISSN 2310-0389, Index Copernicus)
24. Волочій Б.Ю. Надійнісна модель відмовостійкої програмно-апаратної системи на основі мажоритарної структури з ковзним резервуванням та автоматичним перезавантаженням програмного забезпечення / Б.Ю. Волочій, Л.Д. Озірковський, О.В. Муляк, М.М. Змисний // Радіоелектронні і комп’ютерні системи. – 2013. – №5 (64). – С. 221 – 226. (ISSN 1814-4225, Index Copernicus)
25. Волочій Б.Ю. Методика оцінки показників ефективності радіоелектронного комплексу моніторингу повітряного простору / Волочій Б.Ю., Озірковський Л.Д., Шкілюк О.П, Мащак А.В. // Вісник Національного університету «Львівська політехніка». Радіоелектроніка та телекомунікації. – 2013, № 766, – С. 194 – 203. (ISSN 0321-0499)
26. Озірковський Л.Д., Модель поведінки програмно-апаратних електронних систем / Озірковський Л.Д., Панський Т.І. // Вісник Національного університету «Львівська політехніка», Електроніка. – 2013, № 764, – С.36 – 43 (ISSN 0321-0499)
27. Волочій Б.Ю. Визначення впливу оновлення програмного забезпечення на показники надійності відмовостійкої багатопроцесорної системи / Б.Ю. Волочій, В.-М.В. Міськів, О.В. Муляк, Л.Д. Озірковський // Восточно-Европейский журнал передовых технологий. – 2013, № 3/9 (63), – С. 55 – 59 (ISSN 1729-3774)
28. Мандзій Б.А. Автоматизація побудови моделей надійності резервованих та відновлюваних складних технічних систем / Б.А. Мандзій, Л.Д. Озірковський // Восточно-Европейский журнал передовых технологий. – 2013, № 2/4 (62), – С. 44 – 49 (ISSN 1729-3774)
29. Mandziy Bohdan Analytical Reliability Model of a Redundant Repairable System with Limited Number of Restorations/Bohdan Mandziy, Leonid Ozirkovskyy // Computational Problems Of Electrical Engineering. – 2013 – Vol. 3, No. 2, – P. 54 – 60 (ISSN 2224-0977, Index Copernicus)
30. Мандзій Б.А. Порівняльна оцінка надійності трьох конфігурацій відмовостійкої системи з мажоритарною структурою / Б.А. Мандзій, Б.Ю. Волочій, Л.Д.

Озірковський, М.М. Змисний, О.В. Муляк // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С. 44 − 50. (ISSN 1607-3274)
31. Волочій Б.Ю. Оцінка ефективності використання відмовостійкої системи з реконфігурацією ядра мажоритарної структури / Б.Ю. Волочій, Л.Д. Озірковський, М.М. Змисний // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2012. – № 48. – С. 117–125. (ISSN 2310-0389, Index Copernicus)
32. Volochiy Bohdan Extending The Features of Software For Reliability Analysis of Fault-tolerant Systems / Bohdan Volochiy, Bohdan Mandziy, Leonid Ozirkovskyy // Computational Problems of Electrical Engineering, Lviv Politechnic National University, 2012. - Volume 2, number 1. – P. 113 – 121 (ISSN 2224-0977)
33. Волочій Б.Ю. Метод побудови моделей поведінки складних систем немарковського типу у вигляді графа станів і переходів / Волочій Б.Ю., Озірковський Л.Д., Кулик І.В. // Міжнародний науковий журнал "Комп'ютинг" Науково-дослідний інститут Інтелектуальних комп'ютерних систем. Тернопільський Національний Економічний Університет, том 11, випуск №3. Тернопіль. – 2012. – С. 262 – 271. (ISSN 1727-6209)
34. Волочій Б.Ю. Формалізація побудови моделей дискретно-неперервних стохастичних систем з використанням методу фаз Ерланга / Волочій Б.Ю., Озірковський Л.Д., Кулик І.В.//Відбір і обробка інформації. Національна академія наук України. Міжвідомчий збірник наукових праць. Вип. №36 (112). – Львів: 2012. – С. 39 – 47. (ISSN 0474-8662)
35. Озірковський Л. Д. Оцінка показників надійності та безпечності інформаційно-керуючої системи RTP 3000 з викормстанним RAM Commander / Л. Д. Озірковський, Т. І. Панський, О. В. Сидорчук, І. В. Кулик // Східно-Європейський журнал передових технологій. Радіотехнічні інформаційні засоби. – Том 6, № 11(60), 2012. – С. 37 – 40. (ISSN 1729-3774)
36. Волочій Б.Ю. Марковська модель як засіб комплексного моделювання інформаційних систем з функціональним резервуванням / Волочій Б.Ю., Озірковський Л.Д., Улибін Д.О. // Вісник Нац. ун-ту „Львівська політехніка” №470. Комп’ютерні системи проектування. Теорія і практика. – Львів. – Вид-во Нац. ун-ту „Львівська політехніка”, 2003. – С. 101–109 (ISSN 0321-0499)
37. Мандзій Б.А., Визначення параметрів стратегії аварійного відновлення для відмовостійких систем на основі мажоритарної структури/Б.А. Мандзій, Б.Ю. Волочій, Л.Д. Озірковський, М.М. Змисний, І.В. Кулик //Вісник НУ «Львівська політехніка». Радіотехніка та телекомунікації. – 2011. – №705. – С. 216 – 224. (ISSN 0321-0499)
38. Волочій Б.Ю. Моделі відмовостійкої системи з використанням трьох мажоритарних структур, вкладених у мажоритарну структуру, для розв’язання задач надійнісного проектування / Волочій Б.Ю., Озірковський Л.Д., Змисний М.М., Муляк О.В. // Вісник НУ «Львівська політехніка». Радіотехніка та телекомунікації. – 2012. –№738. – С. 223 – 230. (ISSN 0321-0499)
39. Озірковський Л.Д. Оцінка імовірності простою резервованих систем з технічним обслуговуванням / Л.Д. Озірковський, Т.І. Панський, О.В. Сидорчук //Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2012. – № 49. – С. 151–156. (ISSN 2310-0389, Index Copernicus)

40. Волочій Б.Ю. Удосконалення технології моделювання дискретно-неперервних стохастичних систем з використанням методу фаз Ерланга / Б.Ю. Волочій, Л.Д. Озірковський, І.В. Кулик // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2012. – № 48. – С. 159 – 167. (ISSN 2310-0389, Index Copernicus)
41. Волочій Б.Ю. Модель цифрової системи комутації вузла телекомунікаційної мережі / Волочій Б.Ю., Матічин О.В., Озірковський Л.Д., Стецюк С.О., Улибін Д.О. // Вісник Нац. ун-ту „Львівська політехніка”, № 508, Радіоелектроніка та телекомунікації, Львів. – Вид-во Нац. ун-ту „Львівська політехніка”, 2004. – С. 144 – 152 (ISSN 0321-0499)
42. Мандзій Б.А. Програмні моделі для інтерактивного проектування відмовостійких систем з комбінованим структурним резервуванням / Мандзій Б.А., Волочій Б.Ю., Озірковський Л.Д. // Міжнар. наук.-техн. ж-л “Комп’ютинг”. – 2008. – Т.7. - Вип.1. – С. 153 – 160 (ISSN 1727-6209)
43. Мандзій Б. А. Моделювання дискретно-неперервних стохастичних систем у задачах дослідження їх відмово стійкості / Мандзій Б. А., Волочій Б. Ю., Озірковський Л. Д. // Міжвідомчий збірник наукових праць “Відбір і обробка інформації”. - Львів: Вид-во ФМІ НАНУ. – 2008, вип. 28. – С. 39 – 47 (ISSN 0474-8662)
44. Мандзій Б.А. Методи оцінювання структурної живучості ієрархічних інформаційних мереж регіональних радіоелектронних комплексів / Мандзій Б.А., Волочій Б.Ю., Озірковський Л.Д. // Міжвідомчий збірник наукових праць “Відбір і обробка інформації”. - Львів: Вид-во ФМІ НАНУ.- 2009, вип. 30. – С. 104 – 112 (ISSN 0474-8662)
45. Волочій Б.Ю. Моделі для надійнісного проектування вузла пам’яті сервера та джерела безперебійного живлення / Б.Ю. Волочій, Л.Д. Озірковський, О.В. Муляк, В.Д. Гила//Вісник НУ «Львівська політехніка». Радіотехніка та телекомунікації. – 2011. –№680. – С. 206 – 216. (ISSN 0321-0499)

<u>Публікації у матеріалах конференцій, які індексуються в міжнародних науково-метричних баз даних:</u>

46. Ozirkovskyy L. Increasement of Functional Safety of the Behavior Algorithms of Radio Electronic Safety-Critical Systems /Leonid Ozirkovskyy, Bohdan Volochiy, Mykhailo Zmysnyi, Oleksandr Shkiliuk // Proceedings 15 th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2020, Lviv-Slavsko, Ukraine, February 25 – 29, 2020 (SCOPUS)
47. Ozirkovskyy L. Methodology of Defining the Accident Rate Function for Fault Tolerant System with High Responsibility Purpose / Leonid Ozirkovskyy, Bohdan Volochiy, Mykhailo Zmysnyi, Andriy Maschak // Proc eedings of 15th International Conference ICTERI-2019, 5th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (TheRMIT 2019), Kherson, Ukraine, June 12-15, 2019, P. 778 – 793 (SCOPUS)
48. Ozirkovskyy, L., Analysis of the maintenance strategy effectiveness based on the reliability/cost ratio / Ozirkovskyy, L., Kulyk, I., Mazur, A., Petryshyn, N., Malynovska, Y. // Proceedings 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018, P. 810 – 814. (SCOPUS,

Web of Science)
49. Volochiy, B. Research of efficiency indexes of radio telemetry system with short-term use / B. Volochiy, L. Ozirkovskyy, O. Shkiliuk, V.-M. Miskiv // Proceedings 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018. – P. 1268 – 1271 (SCOPUS, Web of Science)
50. Volochiy B. Method of developing unified model for estimating safety and reliability of complex systems for critical application / B. Volochiy, L. Ozirkovskyy // Proceedings 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018. – P. 801 – 804 (SCOPUS, Web of Science)
51. Volochiy B. The scheme of paths method based technique for evaluating of the behavior algorithms efficiency / B. Volochiy, L. Ozirkovskyy, O. Shkiliuk, V. Kharchenko // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, – P. 397 – 401 (SCOPUS)
52. Ozirkovskyy L. The Automation of the Exploitation Risks Assessment of the Navigation Information System of Air Drones / L. Ozirkovskyy, Yu. Pashchuk, A. Mashchak, S. Volochiy // Modern Problems of Radio Engineering, Telecommunications, and Computer Science: proc. of the XIIIth Intern. Conf. TCSET'2016, Lviv-Slavsko, Ukraine, February 23 – 26, 2016. – P. 140 – 144. (SCOPUS, Web of Science)
53. Volochiy B. Automation of Quantitative Requirements Determination to Software Reliability of Safety Critical NPP I&C Systems / Bohdan Volochiy, Oleksandr Mulyak, Leonid Ozirkovskyi, Vyacheslav Kharchenko // Proceedings of the Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management, SMRLO 2016, 15 – 18 February 2016, Israel, Beer Sheva. – IEEE, 2016. – P. 337 – 346. (SCOPUS, Web of Science)
54. Volochiy B. Safety Estimation of Critical NPP I&C Systems via State Space Method / Bohdan Volochiy, Leonid Ozirkovskyi, Oleksandr Mulyak, Sergiy Volochiy // Proceedings of the Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management, SMRLO 2016, 15 – 18 February, 2016, Israel, Beer Sheva. – IEEE, 2016. – P. 347 – 356. (SCOPUS, Web of Science)
55. Volochiy B. Automation of Building the Safety Models of Complex Technical Systems for Critical Application / B. Volochiy, B. Mandziy, L. Ozirkovskyy // ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer: proc. of the 11th Intern. Conf. ICTERI 2015, Lviv, Ukraine, May 14-16, 2015. - Lviv, 2015. – P. 550 – 565. – CEUR-WS.org, online (SCOPUS)
56. Volochiy B. Estimation of Indexes of Efficiency of Radioelectronic Hardware-Software Systems Based on the Algorithm of Behavior / B. Volochiy, L. Ozirkovskyy, O. Shkiliuk, A. Mashchak // Матеріали 11-ої Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та комп'ютерної інженерії TCSET-2012», Львів – Славсько, 2012. – С. 322 – 323. (SCOPUS) .
57. Structure of «K of N» / B. Volochiy, L. Ozirkovskyy, M. Zmysnyi // Modern problems of radio engineering, telecommunications and computer science: proceedings of the XI– th. International Conference TCSET'2012, Lviv–Slavsko, Ukraine.: Publishing National University «Lviv Politechnic». – 2012. – P. 89 – 90, (SCOPUS).
58. Volochiy B. Estimation of Indexes of Efficiency of Radioelectronic Hardware–Software

Systems Based on the Algorithm of Behavior /B. Volochiy, L. Ozirkovskyy, O. Shkiliuk, A. Mashchak // Матеріали 11–ої Міжнародної науково–технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та комп'ютерної інженерії TCSET–2012», Львів – Славсько, 2012. – С. 322 – 323, (SCOPUS).

59. Volochiy Bohdan Designing of Fault–Tolerant Radioelectronic Systems with Majority Structure / Bohdan Volochiy, Leonid Ozirkovskyy, Mykhailo Zmysnyi, Ihor Kulyk // Modern Problems of Radio Engineering, Telecommunications and Computer Science: Proceedings of the International Conference TCSET'2010, February 23 – 27, 2010, Lviv – Slavsko, Ukraine. – P. 35 – 39, (SCOPUS).

АНОТАЦІЯ

Озірковський Л.Д. Розвиток теоретичних засад для оцінювання показників функціональної безпечності радіоелектронних систем відповідального призначення. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи. – Національний університет «Львівська політехніка» Міністерства освіти і науки України, Львів, 2020.

В дисертації розв'язано актуальну науково-прикладну проблему розвитку теоретичних засад комплексного забезпечення заданого рівня функціональної безпечності та надійності радіоелектронних систем відповідального призначення (РЕСВП). Розроблені засоби (методи, моделі, алгоритми та методики) дають змогу, на етапі системотехнічного проектування, визначати слабкі місця РЕСВП з точки зору функціональної безпечності. Це дає змогу проектанту обґрунтовано ввести необхідні види надлишковості (структурної, часової, функціональної), щоб підвищити, як функціональну безпечність, так і надійність РЕСВП.

В дисертації, запропоновано новий метод для автоматизованого визначення різновидів непрацездатних станів. На основі цього методу запропоновано методику розроблення комплексних динамічних моделей РЕСВП у вигляді графа станів і переходів, які на відміну від існуючих, дають змогу без побудови дерева відмов, визначати як мінімальні січення, так і показники надійності РЕСВП.

Для відображення взаємозв'язків між показниками функціональної безпечності і надійності відмовостійких структур, алгоритмів поведінки та стратегій технічного обслуговування запропоновано нові показники та характеристики функціональної безпечності: функція аварійності; частота потрапляння в аварійну ситуацію; ймовірність потрапляння в передаварійну ситуацію; середнє значення ймовірності існування мінімального січення.

Розроблено нові моделі та методику синтезу стратегій технічного обслуговування, що дало змогу гарантовано підтримувати заданий рівень функціональної безпечності РЕСВП на етапі її експлуатації.

В роботі запропоновано моделі відмовостійких РЕСВП з використанням мажоритарних структур, які на відміну від існуючих, дають змогу враховувати вплив на функціональну безпечність використання реконфігурації мажоритарної структури, дворівневої мажоритарної структури та технічного обслуговування і ремонту

Розроблено методологію синтезу безпечних алгоритмів поведінки РЕСВП, в якій

на відміну від існуючих, враховано вплив часової та функціональної надлишковості на функціональну безпечність РЕСВП.

Ключові слова: функціональна безпечність, надійність, надійнісне проектування, радіоелектронна система відповідального призначення, відмовостійкі системи, алгоритм поведінки, технічне обслуговування, мажоритарна система.

АННОТАЦИЯ

Озирковский Л.Д. Развитие теоретических основ оценки показателей функциональной безопасности радиоэлектронных систем ответственного назначения. – На правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.12.17 - радиотехнические и телевизионные системы. - Национальный университет «Львовская политехника» Министерства образования и науки Украины, Львов, 2020.

В диссертации решена актуальная научно-прикладная проблема развития теоретического базиса комплексного обеспечения заданного уровня функциональной отказобезопасности и надежности радиоэлектронных систем ответственного назначения (РЭСОН). Разработанные средства (методы, модели, алгоритмы и методики) позволяют на этапе системотехнического проектирования, определять слабые места РЭСОН с точки зрения функциональной отказобезопасности. Это дает возможность разработчику обоснованно вводить необходимые виды избыточности (структурной, временной, функциональной), чтобы повысить, как функциональную отказобезопасность, так и надежность РЭСОН.

В диссертации, предложен новый метод для автоматизированного определения разновидностей неработоспособных состояний. На основе этого метода предложена методика разработки комплексных динамических моделей РЭСОН в виде графа состояний и переходов, которые в отличие от существующих, позволяют без построения дерева отказов, определять как минимальные сечения, так и показатели надежности РЭСОН. Для отображения взаимосвязей между показателями функциональной безопасности и надежности отказоустойчивых структур, алгоритмов поведения и стратегий технического обслуживания предложены новые показатели и характеристики функциональной безопасности: функция аварийности; частота попадания в аварийную ситуацию; вероятность попадания в предаварийное состояние; среднее значение вероятности существования минимального сечения.

Разработаны новые модели и методика синтеза стратегий технического обслуживания, что позволило гарантированно поддерживать заданный уровень функциональной безопасности РЭСОН не этапе ее эксплуатации.

В работе предложены модели отказоустойчивых РЭСОН с использованием мажоритарных структур, которые в отличие от существующих, позволяют учитывать влияние на функциональную отказобезопасность использование реконфигурации мажоритарной структуры, двухуровневой мажоритарной структуры и технического обслуживания.

Разработана методология синтеза отказобезопасных алгоритмов поведения РЭСОН, в которой в отличие от существующих, учтено влияние временной и функциональной избыточности на функциональную отказобезопасность РЭСОН.

Ключевые слова: функциональная отказобезопасность, надежность, надежностное проектирование, радиоэлектронная система ответственного назначения, отказоустойчивые системы, алгоритм поведения, техническое обслуживание, мажоритарная система.

SUMMARY

Ozirkovskyy L.D. Development of theoretical basis for empowering assessment of functional safety indicators of safety critical radio electronic systems. - On the rights of the manuscript.

A thesis submitted in fulfilment of the Doctor of Engineering Science Degree in Specialty 05.12.17 – Radio and Television Systems. – Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2020.

This thesis presents the solution of the actual scientific problem of development the theoretical basis of complex maintenance of safety critical radio electronic system (SCRES) with a required level of functional safety and reliability. The developed means (methods, models, algorithms and techniques) enable an identifying the weaknesses in the SCRES design in terms of functional safety at the stage of system design. This allows an engineer to reasonably induce necessary types of redundancy (structural, temporary, functional) to increase both functional safety and reliability of SCRES. Thus, the developed tools give the opportunity to synthesize a fault-tolerant structure, behavior algorithm and maintenance strategy, which ensure that the SCRES will not fall into an emergency.

Modern methods of assessing functional safety indexes are based on the determination of minimal cut sets, which show the weaknesses of the SCRES. To obtain minimal cut sets, these methods use fault trees, dynamic fault trees, event trees, or binary decision diagrams. However, the known methods don't allow to take into account the impact on the SCRES functional safety of fault-tolerant majority structures with reconfiguration, fault-tolerant two-tier majority structures, maintenance strategies, temporary and functional redundancy in behavior algorithms. Also, a significant disadvantage of existing methods is that they don't give the opportunity to obtain both functional safety indexes and reliability indexes on the basis of a single model. So, it can lead to the condition when the reliability of the SCRES is reduced with the induction of additional tools for increasing functional safety. Also, these methods aren't suitable enough for solving synthesis tasks via multivariate analysis for a short period time, what is very important at the stage of system design.

In the dissertation, a new method is proposed for automated definition of types of inoperable states. This method provides a classification of inoperable states of the SCRES according to the level of critical failures and allows obtaining trajectories of accidents. Based on this method, a new technique is proposed for development of complex dynamic models of SCRES in the form of a graph of states and transitions. This technique, unlike the existing ones, allows determining both minimal cut sets and reliability indexes of SCRES without constructing appropriate fault tree.

To reflect the relationship between indexes of functional safety and reliability of fault-tolerant structures, behavior algorithms and maintenance strategies, new indexes and characteristics of functional safety are proposed: the accident function; frequency of fall into an accident state; probability of fall into a pre-accident state; the average value of the probability of a minimal cut set existence.

New models of strategies for planned and preventive maintenance and emergency recovery have been developed to take into account the impact of SCRES downtime on functional safety indexes during maintenance and repair procedures.

These models enabled the development of method for synthesizing a maintenance strategy which guarantees to maintain a required level of functional safety of the SCRES. New method was developed to calculate the average value of the probability of the minimal cut set existence that gives an opportunity to solve the problem of minimizing impact of latent failures on the functional safety. This method makes it possible to obtain dependable values of the probabilities of the minimal cut sets existence for cases when the minimal cut set contains only latent failures or a combination of latent and active failures.

New models of fault-tolerant SCRESs with majority structures were developed, which, in contrast to the existing ones, allow to take into account the impact of the use of reconfiguration of the majority structure, two-tier majority structure, maintenance and repair on the functional safety. The proposed models make it possible to solve the problem of synthesis of fault-tolerant systems for SCRES with a required level of functional safety and appropriate level of structural redundancy, that is especially important for onboard information and control systems of aircrafts, including unmanned vehicles, for which mass and size restrictions are critical.

New methodology for the synthesis of safe behavior algorithms of the SCRES was developed, which, in contrast to the existing ones, takes into account the impact of time and functional redundancy on the functional safety of SCRES. This methodology shows the way to achieve a required level of probability of the task execution with the minimum value of the frequency of accidents.

Keywords: functional safety, reliability, reliable engineering, safety critical radio electronic system, fault–tolerant systems, behavior algorithm, maintenance, majority system.

СПИСОК СКОРОЧЕНЬ

АВР – аварійно-відновлювальні роботи
АП – алгоритм поведінки
ВС – вектор станів
ГСП – граф станів і переходів
МС – мажоритарна структура
ППО – планово-профілактичне обслуговування
РЕСВП – радіоелектронна система відповідального призначення
САМ – структурно-автоматна модель
ТО – технічне обслуговування
ФА – функція аварійності