МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

На правах рукопису

Мащак Андрій Володимирович

УДК 629.039.58, 621.396.9

МОДЕЛІ ДЛЯ ОЦІНКИ РИЗИКУ ЕКСПЛУАТАЦІЇ СИСТЕМИ РАДІОУПРАВЛІННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

05.12.17 - радіотехнічні та телевізійні системи

Дисертація на здобуття наукового ступеня
кандидата технічних наук

Науковий керівник
Озірковський Леонід Деонісійович
кандидат технічних наук,
доцент

Ідентичність всіх примірників дисертації,
поданих до ради
ЗАСВІДЧУЮ
Вчений секретар спеціалізованої
вченої ради Д 35.052.10

Бондарєв А.П.

Львів – 2016

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БпЛА - безпілотний літальний апарат
ВВШП – вимірювачі висотно-швидкісних параметрів
ВС – відмовостійка система
ДВ – дерево відмов
ІМ - імітаційне моделювання
ЛІМ – логіко - імовірнісне моделювання
МКП - мікропроцесор
ММ - магнітометр
МС – мінімальні січення
НОС – навігаційно-обчислювальна система
НП - навігаційна підсистема
ПЕЖ - підсистема електроживлення
ПМКВС – правила модифікації компонент вектора стану
ОП - обчислювальна підсистема
САМ – структурно-автоматна модель
СЛДР – система лінійних диференційних рівнянь
СС – січення системи
ФРІАП – формула розрахунку імовірності альтернативного переходу
ФРІБП – формула розрахунку інтенсивності базової події
FMEA – аналіз видів та потенційних наслідків та несправностей (Failure mode and effects analysis)
FMECA - аналіз видів, наслідків та критичності несправностей (Failure mode, effects and criticality analysis)
RPN - значення пріоритету ризику (Risk Priority Number)

ВСТУП

Умовою якісного функціонування складних технічних систем є забезпечення заданого рівня їх надійності. Проте, цілому ряду технічних систем, а саме: системи управління транспортними засобами (авіація, залізничний, морський транспорт), системи життєзабезпечення, системи управління енергетичними об'єктами (ядерна, теплова, гідроенергетика), виробничі системи, системи військового призначення, медичні системи тощо, які відносяться до систем відповідального призначення, визначальною властивістю є заданий рівень безпечності. Безпечність – це властивість системи, після виходу її з ладу в цілому чи окремих підсистем, переходити в такий режим роботи, в якому немає загрози життю і здоров'ю людини, відсутня загроза до нанесенню шкоди навколишньому чи пошкодження інших систем [21, 74-77, 100-102]. Оцінка безпечності полягає в оцінці ризику експлуатації технічних систем на основі проведення аналізу наслідків видів відмов (FMEA), аналізу критичності наслідків видів відмов (FMECA), аналізу дерев відмов (FTA) та аналізу дерев подій (ETA), в результаті яких отримують якісні або кількісні значення показників ризику, допустимий рівень яких встановлюється відповідними міжнародними стандартами [21, 74-77]. У випадку перевищення рівня ризику гранично допустимого значення необхідно розробити рекомендації з його зниження. Рекомендації полягають в підвищенні рівня надійності апаратних засобів, ширшому застосуванні засобів контролю та діагностики, використання захисних, блокуючи систем тощо. Після реалізації даних рекомендацій здійснюють переоцінку показників ризику методом експертних оцінок і таким чином вважається, що ризик експлуатації системи відповідального призначення зменшився, а відповідно його безпечність зросла.

Радіоелектронні системи управління, а саме навігаційно-обчислювальна підсистема безпілотим літальним апаратом (БпЛА), котра входить в склад пілотажно-навігаційного комплексу, що призначений для керування БпЛА на всіх етапах польоту є одним з різновидів технічних систем відповідального призначення. Небезпека експлуатації БпЛА полягає в тому, що пасажири, які

перебувають на інших літальних апаратах, чи люди на землі можуть отримати травми у випадку зіткнення або аварійної посадки такого безпілотного літального апарата. Відмова навігаційно-обчислювальної підсистеми БпЛА також призводить до значних фінансових затрат при пошкодженні самого апарата. Одним із способів забезпечення заданого рівня надійності та зменшення потенційних ризиків при екплуатації БпЛА є моделювання надійнісної та функціональної поведінки його системи для можливості проведення прогнозування ймовірностей виникнення відмов, як окремих компонентів так і їх комбінацій і оцінювання міри важкості наслідків даних відмов. Розробка моделей дозволить визначити критичні відмови, які можуть призводити до падіння БпЛА та розрахувати ймовірності їх виникнення та врахувати критичність кожної відмови з точки зору ризику експлуатації.

Актуальність теми. При проектуванні радіоелектронних систем відповідального призначення (РСВП) недостатньо забезпечити високий рівень їх надійності, оскільки непрацездатність таких систем потенційно загрожує здоров'ю та життю людей, довкіллю, а також призводить до значних матеріальних збитків. Тому важливою задачею на етапі системотехнічного проектування є оцінка ризику експлуатації таких систем. Оцінка ризику експлуатації РСВП потребує докладного опису усіх процесів, ситуацій та чинників, які призводять до аварійної ситуації в результаті непрацездатності системи, і проводиться з метою формування рекомендацій для мінімізації з одного боку наслідків аварії, а з іншого боку – унеможливлення чи зменшення частоти виникнення аварій. Для розв'язання такої задачі необхідно здійснити розробку моделі поведінки РСВП високої складності. А це відповідно потребує використання методів побудови моделей з високим рівнем формалізації та автоматизації, оскільки для досягнення прийнятного рівня ризику потрібно розглядати багато варіантів реалізації РСВП. Відсутність таких засобів призводить до використання спрощених моделей поведінки і отримання недостовірних оцінок ризику, які в свою чергу призводять до реалізації неприйнятних з точки зору безпечності проектних рішень.

Оцінку ризику РСВП, до яких відносяться системи авіоніки і, зокрема, бортова навігаційно-обчислювальна система БпЛА котра входить до складу навігаційно-обчислювальної системи, на сьогоднішній день, здійснюють за допомогою таких методів: аналіз видів, наслідків та критичності несправностей Failure Mode, Efects and (Criticality) Analysis (FMEA/FMECA); аналіз дерева відмов (ДВ); аналіз діаграм бінарного рішення; імітаційного моделювання методом Монте-Карло. Окремі процедури побудови моделей надійності та оцінки ризику переліченими методами частково автоматизовані і реалізовані в спеціалізованих програмних продуктах таких виробників: A.L.D. Reliability Engineering Ltd. (Ізраїль), Reliasoft Corporation (США), PTC Windchill (США), ITEM Software (Великобританія, США), Isograph Ltd. (Великобританія, США).

Як показав огляд інформаційних джерел, питанням оцінки ризику та забезпечення надійності РСВП приділяється велика увага українських та зарубіжних науковців. Для детального дослідження критичності відмов та оцінки безпечності на сьогодні найбільш вживаним є аналіз видів, наслідків та критичності несправностей FMEA/FMECA, який регламентований рядом міжнародних стандартів (MIL-882, Fides Issue, Telcordia). Однак у сучасних методиках реалізації FMEA/FMECA аналізу автоматизованими є лише незначна частина процедур, а засобами автоматизації є різновид електронних таблиць, які заповнюються і перевіряються вручну. Також у цих методах не передбачено врахування особливостей технічного обслуговування, зокрема обмежена кількість ремонтів, вплив на безпечність використання відмовостійких конфігурацій, вплив засобів контролю, діагностики та самодіагностики, які властиві сучасним РСВП.

У роботах Danhua Wang, F. Mhenni, M. Takeichi, Suiran Yu, Xiangyu Han представлено методи та моделі оцінки ризику експлуатації РСВП на основі аналізу ДВ та FMEA/FMECA аналізу. Однак слід відзначити, що у представлених методах оцінка ризику є суб'єктивною, оскільки усі показники, які формують остаточні показники аналізу – Risk Priority Number (RPN) та рівень ризику Risk Level, є експертними оцінками. Існує значна ймовірність

того, що розробник може необґрунтовано занизити або завищити показник безпечності, що призведе до збільшення ризику аварії РСВП або до суттєвого і недоцільного зростання вартості системи.

У роботах Jan Maggot, L. Xing, Serhio Contini, Souza Rodrigo de Queiroz, P. Liggesmeyer, Л.С. Маєвського присвячених розв'язанню задач оцінки ризику експлуатації шляхом побудови ДВ, вказується на необхідність врахування функціональної поведінки системи. Однак у цих роботах розглядаються методики, згідно з якими передбачено, що події в системі є взаємонезалежними, що занижує достовірність оцінки ризику РСВП. У даних моделях, які розробляються на основі цих методик, не враховується функціональна поведінка РСВП, а лише перераховуються, чи визначаються, чи виявляються відмови елементів системи.

Врахувати взаємозалежність подій у РСВП дозволяють динамічні ДВ у поєднанні з методом імітаційного моделювання Монте-Карло. Можливості динамічних ДВ представлені в роботах F.Chiacchio, G.Merle, M.Skrobanek, M.Čepin. Однак слід зазначити, що використання імітаційного моделювання для аналізу динамічного ДВ значно збільшує затрати часу в порівнянні з затратами часу на аналіз статичних ДВ. Дана обставина обмежує використання цього методу на етапі системотехнічного проектування при розв'язанні задач надійнісного синтезу системи через багатоваріантний аналіз.

Для зменшення затрат часу при побудові та аналізі ДВ у роботах Danhua Wang, Pan Jingui, Xiaoqin Su, Zhaoming Lei були запропоновані методи автоматизованої побудови ДВ. В основі цих методів – побудова моделі у вигляді перехідного графа потоку відмов системи. При цьому існує висока ймовірність внесення помилки в перехідний граф через низький рівень формалізації процесу його побудови.

В роботах J. Kloosa, R. Eschbacha, T. Hussaina показано метод побудови ДВ, в якому запропонована окрема процедура верифікації ДВ. Однак дана процедура потребує значних затрат часу, що є неприпустимим на етапі

системотехнічного проектування, коли необхідно розглянути багато варіантів реалізації РСВП упродовж обмеженого часу.

В роботах J. Kloosa, R. Eschbacha, T. Hussaina представлено метод побудови ДВ, в якому запропонована окрема процедура верифікації ДВ. Однак дана процедура потребує затрати значних часових ресурсів, що є неприпустимим на етапі системотехнічного проектування, коли необхідно розглянути декілька варіантів реалізації РСВП упродовж обмеженого часу.

Отже, для оцінки ризику експлуатації навігаційно-обчислювальної системи БпЛА сучасні методи, в основу яких покладено дерево відмов, не дозволяють побудувати моделі з достатнім рівнем адекватності. Вони не враховують належності одних і тих же відмов до різних аварійних ситуацій, що виключає взаємозв'язок між надійністю та безпечністю БпЛА. А це, в свою чергу, не дозволяє кількісно оцінити вплив використання відмовостійких конфігурацій на зниження ризику експлуатації, що призводить або до надмірного резервування, а відповідно до зростання вартості, або до необґрунтованого ускладнення системи. Моделі для оцінки ризику експлуатації у вигляді ДВ, побудованих за відомою методикою, не дають змоги врахувати вплив технічного обслуговування, ремонту та функціональної поведінки на безпечність, а також вплив засобів контролю і діагностики на безпечність та надійність БпЛА. Крім цього існуючі моделі не дозволяють враховувати перебування системи у стані простою, який для навігаційно-обчислювальної системи БпЛА є аналогічним до аварійної ситуації.

Таким чином, *актуальною є науково-прикладна задача* зниження ризику експлуатації бортової навігаційно-обчислювальної системи БпЛА шляхом визначення найбільш «слабких» з точки зору безпечності підсистем і реалізації їх у вигляді відмовостійких конфігурацій. Для вирішення цієї задачі необхідно розробити нові або удосконалити існуючі моделі для кількісної оцінки ризику експлуатації навігаційно-обчислювальної системи БпЛА. Крім цього, процес побудови моделі повинен бути формалізованим, що дозволить мінімізувати ймовірність внесення помилки у модель, а відтак і автоматизувати його.

Автоматизація процесу побудови моделей зробить їх придатними для багатоваріантного аналізу багатьох реалізацій навігаційно-обчислювальної системи БпЛА в обмежені терміни етапу системотехнічного проектування.

Зв'язок роботи з науковими програмами, планами, темами. Результати дисертаційної роботи пов'язані з виконанням науково-дослідних робіт Міністерства освіти і науки України, які виконувались на кафедрі теоретичної радіотехніки та радіовимірювань Національного університету «Львівська політехніка», відповідають науковому напряму «Теорія і методи проектування радіоелектронних кіл, систем і комплексів та забезпечення їх якості» та тематиці досліджень кафедри, а саме:

- науково-дослідна робота «Розроблення моделей, методів та алгоритмів для автоматизованої оцінки показників надійності радіоелектронних та електромеханічних пристроїв та систем», № держреєстрації 0110U001098 (2010−2012);
- науково-дослідна робота «Розроблення моделей надійності, ризику та безпечності програмно-апаратних технічних систем», № держреєстрації 0113U001371 (2013-2014).

У перелічених науково-дослідних роботах автор брав участь як виконавець.

Мета та завдання дослідження. Метою дисертаційної роботи є розробка методики оцінки рівня ризику експлуатації навігаційно-обчислювальної системи котра входить до складу навігаційно-обчислювальної підсистеми безпілотного літального апарата з використанням нових моделей навігаційної та обчислювальної підсистем та на її основі створення програмного засобу, який автоматизує отримання кількісного показника ризику експлуатації.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Провести аналіз методів побудови моделей систем для оцінки ризику їх експлуатації. Здійснити вибір математичного апарата, який уможливлює побудову адекватних моделей з урахуванням усіх особливостей навігаційно-обчислювальної системи безпілотного літального апарата.

2. Здійснити розробку моделей навігаційно-обчислювальної системи безпілотного літального апарата для кількісної оцінки ризику її експлуатації з формуванням рекомендацій щодо забезпечення заданого або допустимого рівня ризику при заданому рівні надійності. Моделі повинні давати змогу визначати найбільш критичні з точки зору ризику експлуатації підсистеми та їх елементи з метою використання для них відмовостійких конфігурацій, які б знижували рівень ризику експлуатації при заданому рівні надійності.

3. Розробити методику та засіб автоматизованого отримання кількісного показника ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата для забезпечення можливості розв'язання задач надійнісного синтезу системи через багатоваріантний аналіз.

4. Здійснити розробку засобів для візуалізації причинно-наслідкових зв’язків розвитку аварійної ситуації у вигляді дерева відмов, що дозволить відслідковувати вплив критичних з точки зору безпечності підсистем на потенційну аварійну ситуацію та проводити валідацію отриманих дерев відмов шляхом порівняння з деревами відмов, отриманими за допомогою стандартизованих методик.

5. Розробити засоби автоматизованого отримання мінімальних січень на основі моделі навігаційно-обчислювальної системи безпілотного літального апарата у вигляді графа станів та переходів для проведення оцінки ризику експлуатації.

Об’єктом дослідження є процес оцінювання ризику експлуатації бортової навігаційно-обчислювальної системи БпЛА.

Предметом дослідження є моделі, методики та засоби автоматизації оцінювання ризику експлуатації бортової навігаційно-обчислювальної системи БпЛА.

Методи дослідження, що використані в дисертаційній роботі, базуються на положеннях теорії системотехнічного проектування складних технічних систем, теорії надійності складних систем, теорії випадкових процесів, теорії оцінки ризиків складних технічних систем. Для побудови математичної моделі

об'єкта дослідження у вигляді системи диференційних рівнянь Колмогорова - Чепмена та їх розв’язання використано методи теорії марковських випадкових процесів та методи чисельних розв’язків систем лінійних диференційних рівнянь. Для отримання мінімальних січень та побудови дерева відмов використано математичний апарат теорії моделювання дискретно-неперервних стохастичних систем. Для отримання показників ризику використано теорію оцінки ризиків складних технічних систем.

Наукова новизна одержаних результатів. Основні результати роботи, які визначають її наукову новизну та виносяться на захист:

1) Дістав подальший розвиток метод формалізованого представлення об’єкта дослідження у вигляді структурно-автоматної моделі, який на відміну від існуючого дозволяє виокремити всі можливі непрацездатні стани складної технічної системи, з множини яких вибираються групи станів, які представляють аварійні ситуації і на їх основі визначаються мінімальні січення без побудови дерева відмов. За допомогою мінімальних січень отримують ймовірність виникнення аварійної ситуації складної технічної системи.

2) Вперше розроблено математичну модель навігаційної підсистеми для оцінки ризику її експлуатації. В моделі відображено: показники надійності дубльованих акселерометрів та гіроскопів; показники надійності магнітометра та вимірювачів висотно-швидкісних параметрів; надійність приймача сигналів від супутникової навігаційної системи та надійність приймача каналу зв’язку БпЛА з оператором. Крім цього, враховано функціональне резервування супутникової навігаційної системи навігаційною підсистемою БпЛА. Це забезпечило високу достовірність оцінки ризику експлуатації навігаційно-обчислювальної підсистеми БпЛА.

3) Удосконалено математичну модель обчислювальної підсистеми для оцінки ризику її експлуатації, в якій, на відміну від існуючих, відображено: мажоритарну структуру та відмови і збої її мікропроцесорів; можливість автоматичного перезавантаження мікропроцесорів після виявлення збою;

ненадійність підсистеми електроживлення. Це дало змогу підвищити достовірність оцінки ризику експлуатації.

Практичне значення одержаних результатів

1. Запропонована методика визначення кількісного показника ризику обчислювально-навігаційної системи БпЛА, а саме ймовірності виникнення мінімального січення, без побудови дерева відмов. Методика дозволяє вирішувати задачі зменшення рівня ризику експлуатації навігаційно-обчислювальної системи БпЛА на етапі системотехнічного проектування. Це досягається шляхом оцінки ризику експлуатації багатьох варіантів побудови навігаційно-обчислювальної системи БпЛА з врахуванням вартості їх реалізації. Розв’язання задачі зменшення оцінки ризику експлуатації здійснюється з меншими затратами часу, ніж вимагає методика оцінки ризику експлуатації з використанням дерева відмов, що важливо на етапі системотехнічного проектування.

2. Розроблено алгоритм та прототип програмного засобу, в основу якого покладено запропоновану методику. Програмний засіб автоматизує процес отримання кількісного показника ризику, в якому враховуються: відмовостійкі конфігурації підсистем; відмови апаратних засобів; збої програмних засобів; належність певної частини відмов до двох і більше мінімальних січень; вплив ненадійності приймача сигналу від супутникової навігаційної системи; вплив ненадійності приймача системи зв’язку з оператором.

3. Розроблена методика розв'язання зворотної задачі, а саме побудова дерева відмов на основі мінімальних січень. Ступінь формалізації методики дав змогу розробити прототип програмного засобу для автоматизованої побудови дерева відмов. Практична необхідність отримання дерева відмов, після того як сформовані мінімальні січення в тому, що воно візуалізує шляхи потрапляння навігаційно-обчислювальної системи в аварійні стани. Необхідно зауважити, що дерево відмов є обов'язковим атрибутом при здійсненні сертифікації на безпечність експлуатації безпілотного літального апарата.

Результати дисертаційної роботи використані:

– в науково-дослідній роботі за шифром «Дрон» інв. №17-13 НОВ у Науковому центрі Національної Академії сухопутних військ імені гетьмана Петра Сагайдачного.

– в держбюджетній науково-дослідній роботі «Розроблення моделей, методів та алгоритмів для автоматизованої оцінки показників надійності радіоелектронних та електромеханічних пристроїв та систем»

– в держбюджетній науково-дослідній роботі «Розроблення моделей надійності, ризику та безпечності програмно-апаратних технічних систем».

– в ТОВ “Сілего Технолоджі (Україна)”.

Особистий внесок здобувача. Дисертаційна робота є самостійно виконаним науковим дослідженням. У наукових працях, опублікованих у співавторстві, авторові дисертації належить: [79] – валідація моделі алгоритму поведінки системи радіоелектронного комплексу шляхом її порівняння з моделлю у вигляді бінарної структурно-автоматної моделі; [103] – спосіб представлення непрацездатних станів радіоелекронного комплексу бінарними компонентами вектора стану; [104] - спосіб виділення непрацездатних станів із сукупності усіх станів системи для ідентифікації аварійних ситуацій; [110] – методика побудови дерева відмов складної технічної системи на основі мінімальних січень; [111]математична модель для оцінки ризику експлуатації відмовостійкої системи з мажоритарною структурою; [112] – удосконалений метод формалізованого представлення об’єкта дослідження у вигляді бінарної структурно-автоматної моделі; методика автоматизованого формування мінімальних січень; [113, 143] – спосіб представлення надійності програмного забезпечення в структурно-автоматних моделях мікропроцесорних систем; [114] - математичні моделі навігаційної та обчислювальної підсистем системи радіоуправніння БпЛА [112] - тестова бінарна структурно-автоматна модель алгоритму поведінки радіоелектронного комплексу; [79, 80-82, 106, 107] – автоматизація отримання мінімальних січень на основі методу простору станів;

[103-105] – автоматизація методики побудови дерева відмов та основі графа станів і переходів.

Апробація результатів дисертації. Основні наукові результати дисертації та основні положення роботи доповідались на дев’яти Міжнародних та чотирьох Всеукраїнських конференціях і семінарах: міжнародна науково-технічна конференція TCSET «Сучасні проблеми радіоелектроніки, телекомунікацій та комп’ютерної інженерії» (Україна, Львів-Славське, 2012, 2014); міжнародна молодіжна науково-технічна конференція «Сучасні проблеми радіотехніки та телекомунікацій (Україна, Севастополь, 2012); Національна конференція «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій» (Україна, Львів, 2013, 2014); Міжнародна науково-технічна конференція РТПСАС «Радіотехнічні поля, сигнали, апарати та системи (теорія, практика, історія, освіта)» (Україна, Київ, 2013, 2014); IX науково-практична конференція «Проблеми та перспективи розвитку економіки, підприємництва та комп'ютерних технологій в Україні» (Україна, Львів, 2013); Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (Чернівці, Україна, 2013, 2014); 7th International Conference Dependable Systems, Services and Technologies DESSERT 2014 (Ukraine, Kiev, 2014); VII Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій» (Україна, Запоріжжя, 2014); КриКТехС-2015/7/105 всеукраїнський науково-технічний семінар «Критичні комп'ютерні технології та системи» (Україна, Харків, 2015); на семінарах кафедри теоретичної радіотехніки та радіовимірювання.

Публікації. За результатами дисертаційної роботи опубліковано 17 наукових праць, з них 6 статей у фахових виданнях України, у тому числі 2 статті у виданнях України, які входять до міжнародних наукометричних баз; 9 публікацій у збірниках праць Міжнародних науково-технічних конференцій та

3 публікації у збірниках праць Всеукраїнських науково-технічних конференцій і семінарів.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, п'яти розділів, висновків, переліку літератури з 154 назв та 2 додатки. Загальний обсяг дисертаційної роботи складає 156 сторінок, з них 113 сторінок основного тексту, 12 рисунків та 21 таблиця.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА МОДЕЛЕЙ ДЛЯ ОЦІНКИ РИЗИКУ ЕКСПЛУАТАЦІЇ ТЕХНІЧНИХ СИСТЕМ

Одним з важливих показників безпечності експлуатації РСВП, до яких відносяться безпілотні літальні апарати (БпЛА), є оцінка рівня ризику експлуатації. Оцінка ризику експлуатації РСВП [96] регламентується рядом міжнародних стандартів [75-77, 97-99, 134-135] та необхідна практично на усіх етапах життєвого циклу РСВП, і перш за все, на етапі системотехнічного проектування. Крім стандартів, експлуатація БпЛА цивільного призначення регламентується рядом кодексів та наказів України [145]. Основною метою оцінки ризику є своєчасне виявлення небезпек для напрацювання, обґрунтування і реалізації проектних рішень щодо їх усунення або зменшення їх наслідків [141-143, 152].

Згідно нормативних документів [145] *аварійною ситуацією* або авійційною подією називається - подія, пов'язана з експлуатацією повітряного судна, яка відбувається у разі безпілотного повітряного судна з часу, коли повітряне судно готове рушити з місця для виконання польоту, до часу його зупинки після завершення польоту та вимкнення головної силової установки, під час якої:

а) будь-яка особа отримала тілесне ушкодження зі смертельним наслідком або тілесне ушкодження внаслідок безпосереднього контакту з будь-якою частиною повітряного судна, у тому числі частиною, що відділилася від повітряного судна;

б) повітряне судно зазнає пошкодження або відбувається руйнування його конструкції, у результаті чого: порушується міцність конструкції, погіршуються технічні чи льотні характеристики повітряного судна, та звичайно потребується значний ремонт або заміна пошкодженого компонента повітряного судна, за винятком відмови чи пошкодження двигуна, коли пошкоджено лише один двигун (у тому числі його капоти чи допоміжні агрегати), повітряні гвинти, закінцівки крила, антени, датчики, лопатки,

пневматики, гальмівні пристрої, колеса, обтічники, панелі, стулки шасі, лобове скло, обшивка повітряного судна (наприклад, незначні вм'ятини чи пробоїни) або виникли незначні пошкодження лопатей несучого гвинта, лопатей хвостового гвинта, шасі та пошкодження, що викликані градом чи зіткненням з птахами (у тому числі пробоїни в обтічнику антени радіолокатора);

в) повітряне судно зникає безвісти чи опиняється в місці, де доступ до нього абсолютно неможливий;

В подальшому авіаційну подію будемо називати аварійною ситуацією (АС).

Згідно стандартів [21, 75-77], термін *функціональна безпечність* визначається, як частина загальної безпечності, котра відноситься до обладнання, яке знаходиться під контролем, та систем контролю, і залежить від правильності функціонування електричних, електронних, електронних програмованих систем, пов'язаних з безпечністю; систем забезпечення заданого рівня безпечності, яка реалізована на інших технологіях; зовнішніх засобів зменшення ризиків [99]. Функціональна безпечність виконує дві основні функції. Перша функція - реалізація процесів функціонування, таким чином, щоб унеможливити перехід системи або її складових підсистем в потенційно небезпечний стан. Друга функція полягає в забезпеченні заходів, щодо блокування або вимкнення системи у випадку небезпеки переходу системи у аварійний стан з подальшим зменшенням наслідків від такого переходу та самої аварії.

Вважається, що абсолютної безпечності не існує - навіть після прийняття захисних рішень, все одно буде існувати певний рівень ризику [102, 68]. У відповідності до стандарту [135] *ризик* це поєднання ймовірності події та її наслідків. В окремих випадках ризик обумовлений можливістю відхилення від очікуваного результату або події. Згідно стандарту [21] ризик являє собою ймовірність небезпеки функціонуванню системи і навколишньому середовищу, а також важкості нанесеної шкоди.

1.1 Узагальнена структурна схема навігаційно-обчислювальної системи безпілотного літального апарата

Згідно [145], безпілотний літальний апарат (БпЛА) – це пристрій призначений для виконання польоту атмосфері чи космічному просторі, без пілота на борту, керування польотом якого і контроль за ним здійснюються за допомогою спеціальної станції, що розташована поза літальним апаратом.

Однією з основних систем БпЛА, яка має визначальний вплив на безпечність експлуатації є система радіуправління до складу, як правило, входить навігаційно-обчислювальна підсистема , підсистема автоматичного управління польотом, підсистема телеметрії, підсистема живлення, магнітометр та приймача сигналів від супутникової навігаційної системи та приймача сигналів зв’язку з оператором.

Склад та призначення навігаційної підсистеми розглянуто в [128, 157]. Принципи побудови обчислювальної підсистеми приведено в [89-91, 128]. Особливості підсистем живлення БпЛА докладно проаналізовано в [65, 147]. Таким чином, на основі аналізу інформаційних джерел сформовано узагальнену структурну схему навігаційно-обчислювальної підсистеми БпЛА, яка представлена на рис.1.1.

Згідно рис.1.1 типова навігаційно-обчислювальна система складається з таких складових:

1. Обчислювальна підсистема (ОП). Призначена для вирішення завдань обрахунку та видачі сигналів для навігації та просторової орієнтації БпЛА, оптимальної оцінки навігаційних параметрів і їх корекції, а також опитування датчиків та підсистем, зберігання та передачі масивів даних, забезпечення функціонування систем самоконтролю та контролю стану периферійних пристроїв тощо. Являє собою сукупність інформаційно взаємозв’язаних апаратно-програмних засобів передачі, зберігання і обробки інформації.

Архітектура ОП має багаторівневу, ієрархічну та неоднорідну побудову. На нижньому рівні ієрархії використовують спеціалізовані обчислювачі, що забезпечують первинну обробку інформації від одного датчика або групи

однорідних датчиків. Середній рівень ієрархії ОП представляють більш

Рис. 1.1. Узагальнена структурна схема навігаційно-обчислювальної системи та її взаємозв'язок з бортовими системами БпЛА

потужні мікропроцесори, які вирішують функціональні завдання на основі комплексної обробки інформації датчиків. На верхньому рівні ієрархії ОП розташовуються мікропроцесори, які призначені для вирішення завдань управління, контролю, індикації, зв’язку та фільтр калмана.

2. Навігаційний підсистема (НП). Призначена для визначення координат місцезнаходження, кутової орієнтації, висоти, лінійної швидкості та інших параметрів польоту БпЛА. Як правило, включає такі пристрої:

– приймач супутникової навігаційної системи (СНС). Забезпечує високу точність визначення координат БпЛА (до 6-10 м) за сигналами глобальної супутникової навігаційної системи (NAVSTAR/ГЛОНАСС), має малі габарити та невисоку вартість. Основним недоліком СНС є низька автономність та завадостійкість;

- систему повітряних сигналів (ВВШП), яка у своєму складі має приймач повітряного тиску (ППТ), датчики барометричної висоти (ДВ) та істинної повітряної швидкості (ДШ);
- магнітометр (ММ) або індукційний датчик, що вимірює магнітний курс БпЛА;
- акселерометри і гіроскопічні датчики кутової швидкості, яким властиві значні рівні шумів і зміщення нуля, що призводить до значних похибок вихідної інформації НП. Такі похибки, що, в основному, визначаються дрейфом гіроскопів, компенсуються за допомогою зовнішньої корекції за сигналами інших систем. Основними перевагами НП є висока інформативність (вимірювання як лінійних, так і кутових параметрів польоту БпЛА), завадостійкість та автономність. Інтеграція (комплексування) інформації від СНС, НП, ВВШП та ММ здійснюється за допомогою алгоритму калманівської фільтрації (КФ).

3. Підсистема автоматичного управління польотом (САУ) або автопілот. Призначена для оцінки відхилень поточних навігаційних параметрів польоту БпЛА від заданих параметрів згідно з запрограмованим польотним завданням та/або з командами оператора, і вироблення командних сигналів для мінімізації цих відхилень. Також САУ може використовуватися для управління корисним навантаженням та іншим обладнанням БпЛА.

4. Підсистема телеметрії, котра призначена для передачі по каналу радіозв’язку до наземної станції управління польотом (НСУ) телеметричної інформації, у т.ч. навігаційної інформації, вихідних даних систем збору інформації корисного навантаження, даних про стан систем БпЛА.

5. Система електроживлення, необхідна для функціонування інших систем БпЛА. Дана система має два блоки котрі паралельно живлять усі бортові підсистеми та модулі напругою 5 В; Корисне навантаження використовує живлення 12 В.

На етапі системотехнічного проектування важливим є вибір конфігурації навігаційно-обчислювальної системи, що забезпечить заданий рівень ризику експлуатації. Залежно від призначення БпЛА та його функцій до складу навігаційно-обчислювальної підсистеми включають ОП з одним або двома, чи трьома мікропроцесорами. Для збільшення відмовостійкості представлених систем, а також достовірності сигналів від вхідних підсистем, передбачено обов’язкове використання мажоритарної структури ОП .

Аналіз структури системи радіуправління БпЛА показав, що відмова обчислювальної підсистеми або навігаційних підсистем однозначно призводить до відмови системи радіуправління, а в результаті і до відмови всього БпЛА, що призводить до виникнення аварійної ситуації. Отже дана система є найбільш критичною при експлуатації БпЛА. Тому проведення оцінки ризику навігаційно-обчислювальної підсистеми БпЛА необхідно проводити ще на етапі її системотехнічного проектування, бо лише тут можна вносити кардинальні зміни в структуру та склад системи, а на подальших етапах рівень ризику можна тільки константувати. Таким чином, актуальною є наявність у проектантів моделей обчислювальної та навігаційної підсистем для визначення критичних комбінацій відмов системи радіоуправління БпЛА, що в свою чергу дасть можливість зменшити ризик експлуатації за рахунок резервування виявлених за допомогою цих моделей слабких місць системи.

1.2 Особливості навігаційно-обчислювальної системи безпілотним літальним апаратом з точки зору оцінки ризику експуатації

Як об'єкт дослідження навігаційно-обчислювальна підсистема характеризується рядом особливостей, котрі необхідно враховувати при моделюванні і розрахунку показників ризику. Найбільш суттєвими особливостями є:

- Сучасні навігаційно-обчислювальної системи БпЛА, як різновид РСВП, складаються, як правило, з великої кількості елементів та підсистем

[59, 119, 123, 141], надійнісну поведінку яких потрібно враховувати при оцінці ризику експлуатації БпЛА;

- Систему радіоуправління та її складові реалізують як відмовостійкі конфігурації, що характеризуються високою складністю, яка не завжди дає можливість звести їх до послідовно-паралельних з’єднань елементів. Крім цього навігаційно-обчислювальна підсистема може мати складі зв'язки між підсистемами та елементами, багатофункціональні елементи, підсистеми та елементи з залежними відмовами або елементи котрі мають обмежене відновлення [125, 150].
- Сучасні БпЛА, як правило, є багатофункціональними, тому необхідно будувати моделі і оцінювати їх ризик експлуатації по множині аварійних ситуацій [123, 155, 159, 160].
- Безпілотні літальні апарати характеризуються значними періодами простою під час їх експлуатації, з одночасною умовою підтримки заданого рівня надійності [145] за рахунок технічного обслуговування та ремонту.
- Для вибору і обґрунтування проектних рішень необхідно провести аналіз надійності та провести оцінку ризику експлуатації для реалізації БпЛА з різними варіантами видів структури, організації, режимів та умов роботи, що вимагає побудову моделі для кожної реалізації [118, 123, 148], тобто можливості проводити багатоваріантний аналіз.

Оцінка ризику експлуатації БпЛА, окрім всього вище вказаного, має специфіку, оскільки необхідно враховувати періоди коли БпЛА не використовується з одночасною необхідністю забезпечення максимального рівня надійності та мінімізацією ризику під час експлуатації апарата, технічне обслуговування і ремонт, які відбуваються після процесу польоту БпЛА [18, 26, 157].

1.3 Моделі систем управління безпілотним літальними апаратами

Для встановлення ступеня врахування вищезазначених особливостей системи радіоуправлінн БпЛА проведено огляд існуючих моделей таких систем, що дозволяють оцінити ризик експлуатації БпЛА.

В роботі [128] розроблено модель обчислювального ядра інформаційно-керуючої системи літального апарата та узагальнений граф взаємозв'язку обладнання для окремих підсистем. Для можливості проведення оцінки функціональної безпечності запропоновано метод оцінювання функціональної безпечності бортової інформаційно керуючої системи, який базується на процедурі аналізу критичності окремих елементів, що входять до її складу. Згідно методу визначається критичність окремих елементів інформаційно керуючої системи та визначаються нормовані коефіцієнти критичності. Запропонований новий коефіцієнт критичності який проградуюваний за п'ятьма рівнями та визначається на основі експертної оцінки. Проте на сьогоднішній день існують стандартизовані методи оцінки критичності (FMEA/FMECA) об'єкту, в яких вибір рівня критичності здійснюється не лише на основі експертної оцінки але й на ймовірності виникнення критичної ситуації, ймовірності виявлення та її значущості.

Автор роботи [64] проводить аналіз авіаційних катастроф та пропонує, базуючись на статистиці експлуатації пілотованих літальних апаратів, визначити основні умови безпечності експлуатації БпЛА. Також в роботі розроблено модель поведінки БпЛА, в котру закладено трансформовані для безпілотного апарата параметри отримані із статистичних даних про катастрофи пілотованих літальних апаратів. Автор представляє побудовані залежності між площею та густиною населення, використання повітряного простору в якому виконують свої завдання як БпЛа, так і пілотовані літальні апарати для можливості отримання оцінки ризику людських втрат. В результаті дослідження моделі запропоновано рекомендовані інтенсивності відмов авіаційного комплексу в залежності від території над якими здійснюється політ БпЛА. Результат роботи показав що найбільшим чинником на ймовірність

виникнення авіаційної події є людський чинник. Проте, в представленій моделі, основними чинниками впливу на літальний апарат є зовнішні чинники. Також у моделі відсутнє врахування функціональної поведінки БпЛА та не враховано ймовірності відмови програмих засобів боротвих систем апарата.

Робота [4] присвячена аналізу історії військових БпЛА, представлено основні правила оцінки безпечності. В роботі, безпечність БпЛА розглядається як декілька етапів експлуатації літальних апаратів: авіаційна подія в повітрі, аварія на землі та надійність БпЛА. Наведено рекомендації щодо часу польоту над територіями з різною густиною населеня. Наприклад час польоту великогабаритних БпЛА (MQ-9 Predator B, Global Hawk, AeroVironment Helios) над густонаселеними територіями рекомендовано скоротити до мінімуму. Також розроблено рекомендації щодо введення системи взаємного сповіщення між безпілотними літальними апаратами у повітрі та підвищення точності систем супутникової навігації. В загальному дана робота носить декларативний характер і лише подає рекомендації щодо експлуатації БпЛА та їх інтеграції в загальну авіаційну систему.

В роботі [151] автором представлено розроблено систему автоматизованого управління БпЛА тактичного призначення з докладним описом його структури. В роботі представлено один з варіантів системи автоматизованого управління польоту.

Таким чином існуючі моделі відображають одну-дві особливості систем радіоуправління БпЛА та їх окремих підсистем, а оцінка ризику експлуатації проводиться або за допомогою експертних оцінок. або за допомогою спрощених моделей, що призводить до незавжди вдалих з точки безпечності технічних рішень.

1.4 Загальна характеристика технологій моделювання для аналізу ризику експлуатації технічних систем відповідального призначення

При проектуванні РСВП, в тому числі і БпЛА, оцінку ризику експлуатації здійснюють за допомогою моделювання, і на основі моделей розраховують

відповідні показники безпечності і в тому числі показник рівня ризику. Для отримання показників ризику експлуатації на сьогоднішній час розроблена велика кількість методів, а саме - методи імітаційного моделювання (ІМ) [118], методи логіко-імовірнісного моделювання (ЛІМ) [153, 154], метод простору станів [100, 117]. Найбільш використовуваними, на сьогодні, є різновиди методу ЛІМ. До позитивних рис методів ЛІМ можна віднести те, що для них розроблені формальні алгоритми отримання моделей. Таким чином, методи ЛІМ отримали можливість їх автоматизації, і створення відповідного програмного забезпечення.

Найбільш розповсюджений метод ЛІМ, який передбачає побудову дерева відмов (ДВ) [163] . Дерево відмов (ДВ) – вид структурних схем, який дає змогу дедуктивним способом графічно описати події, котрі призводять до аварійної ситуації (катастрофічної відмови системи) [18, 26, 40, 64, 67]. Результатом аналізу ДВ є якісне та кількісне представлення подій, які можуть призвести до катастрофічної відмови системи, у вигляді січень системи і мінімальних січень та ймовірностей їх виникнення. Мінімальні січення (МС) – це така найменша комбінація подій, яка призводить до відмови системи в цілому. Якщо з МС вилучити хоча б одну подію, то відмова системи унеможливлюється [4, 40, 59, 64]. Мінімальні січення – це кількісний показник при оцінці ризику експлуатації РСВП.

Аналіз отриманих МС дає можливість представити найбільш вразливі місця РСВП. Для подальшого аналізу наслідків та критичності несправностей застосовують FMEA/FMECA-аналіз [26, 75-77, 139] на основі якого отримують якісні показники безпечності у вигляді експертних оцінок, що дозволяє зменшити потенційні наслідки небезпек та аварій, шляхом імплементації рекомендацій експертів, які полягають у введенні додаткової надлишковості, організації засобів контролю та діагностики, організації технічного обслуговування та діагностики тощо. Однак кількісна оцінка ефективності цих рекомендацій відсутня.

1.4.1 Аналіз оцінки безпечності методами логіко - імовірнісного моделювання

На сьогоднішній день великий внесок у дослідження безпечності структурно-складних систем за допомогою логіко-імовірнісного моделювання, здійснив колектив під керівництвом І. А. Рябініна та Г.Н. Черкесова, досягнення якого представлені в роботах [102, 119, 128, 137-138, 141-142, 144, 148-150, 162]. Зокрема І. А. Рябініним та Г.Н. Черкесовим написано ряд монографій присвячених логіко - імовірнісному аналізу надійності і безпечності структурно - складних систем [148 - 150, 162]. Теоретичну основу ЛІМ складають операції над функціями булевої алгебри. Для аналізу безпечності, згідно даних методів, проводиться аналіз умов попадання системи в небезпечний стан. В роботах [119, 144, 148] представлено методичні основи оцінки надійності та ризику структурно - складних систем. Основним недоліком представленого методу є значний об'єм трудомістких логічних перетворень при аналізі складних сценаріїв, а саме при переході від функції небезпечного стану до ймовірнісної функції. Тому даний метод був частково автоматизований і реалізований в програмному комплексі "АРБИТР" (КП "АСМ"), застосування даного програмного комплексу представлено в роботах [128, 142, 144]. Для оцінки безпечності, згідно даного методу, визначається ступінь ризику, який присутній в системі. Ступінь ризику - ймовірнісна величина, яка характеризує невиконання системою своєї цільової функції в рамках конкретної небезпеки. Також однією з переваг даного методу є отримання коефіцієнтів значущості кожного окремого елементу, які впливають на безпечність системи. Однак, розробка схеми функціональної цілісності, особливо з врахуванням несумісних подій, являє собою складну та трудомістку роботу. Також, саме при розробці схеми функціональної цілісності існує ймовірність внесення помилки в модель системи, які практично неможливо виправити.

1.4.2 Аналіз оцінки ризику за допомогою дерев відмов

Дерево відмов (ДВ) базується на основі логічних причинно-наслідкових зв'язків відмов системи з відмовами її елементів та іншими подіями. При аналізі імовірності виникнення відмови системи, ДВ складається з послідовностей і комбінацій порушень і несправностей системи, і таким чином представляє собою багаторівневу графічну структуру [18, 26, 40, 96]. Застосування ДВ знайшло своє місце при аналізі, моделюванні та проектуванні: технологічних об’єктів [158] а також теплоелектростанції [30], гідроелектростанції [37], цеху розливу питної води [161]; систем безпеки об’єктів водного транспорту [116]; системи приготування і роздавання кормів "людина-машина-середовище" [140]; кислотної відмови геосистеми [118]; електротравматизму на металургійних підприємствах [147]; комп'ютерних систем управління [155].

Перевагою даного методу є простота аналізу системи та наочне представлення розвитку аварійної ситуації. В даних роботах застосовується побудова статичних ДВ. В статичних ДВ вважається, що кожна подія в системі є незалежною [40]. Для врахування взаємозалежностей подій у моделі були запропоновані динамічні дерева відмов [8, 9].

В роботі [10] авторами представлено методику побудови та аналізу динамічних ДВ. Позитивна особливість методики полягає у тому, що розробник отримує ДВ з врахуванням послідовності виникнення подій в часі та подій, що повторюються. Після побудови динамічного ДВ, для можливості подальшого дослідження системи, авторами проводиться аналіз даного ДВ імітаційним моделюванням (ІМ) методом Монте - Карло. Однак, слід зазначити, що використання імітаційного моделювання для аналізу динамічного ДВ значно збільшує часові затрати в порівнянні з аналізом статичних ДВ.

Авторами роботи [1] представлено методику побудови статичного ДВ. Запропонована робота є продовженням роботи [50]. Особливістю методики побудови ДВ є введення в дерево блоків з часовими залежностями. В даних блоках створена можливість задання часового інтервалу, в якому відбудеться

відповідна подія. Розроблені авторами моделі з часовими залежностями знайшли свої застосування в оцінці надійності та безпечності:

- електричних силових систем [49];
- комп'ютерних мереж [53, 68];
- транспорту та логістики [51, 52];

Недоліком даної роботи можна назвати складність розрахунків з врахуванням визначення часових інтервалів.

У роботі [12] представлено методику, яка дозволяє проводити аналіз через декомпозицію громіздких, складних ДВ на прості. В результаті декомпозиції одного складного ДВ отримуються декілька дерев меншої розмірності, котрі піддаються аналізу. Після проведення аналізу отриманих менших ДВ, за допомогою запропонованого авторами методу, проводиться процедура об'єднання результатів аналізу менших ДВ в один. Результатом даного методу є МС системи та показник надійності - ймовірність відмови системи. Однак слід відмітити, що через проведення декомпозиції та об'єднання ДВ, представлена методика вкладає похибку у визначене значення ймовірності відмови системи.

Динамічні ДВ, в яких закладено функціональну залежність подій між собою, представлено авторами роботи [56]. До позитивних особливостей представленої методики побудови ДВ можна віднести використання в ДВ блоків з пріоритетом та блоків повторення. За допомогою такого ДВ отримується ймовірність виникнення аварійної ситуації в системі. Отримані ДВ враховують кореляцію між відмовами, однак, їх подальший аналіз вимагає використання методів ІМ або методу простору станів.

Автори роботи [48] представляють аналіз ДВ, в котрих закладений перерозподіл ймовірностей виникнення певних подій. В моделі закладено алгоритм, котрий змінює інтенсивності виникнення відмов елементів системи за умови, що в ДВ відбулись певні інші відмови. Представлений метод застосований при розробці моделі системи аварійного відключення на ядерній

електростанції. Даний підхід є достатньо складним та вимагає від розробника значних інтелектуальних та часових затрат при розробці та аналізі моделі.

Автори роботи [54] пропонують методику побудови ДВ з врахуванням перерозподілу навантаження елементів. Дана методика передбачає застосування складного математичного апарата, який базується на використанні логіко – ймовірнісної моделі та марковської моделі. Першим етапом даної методики передачається побудова динамічного ДВ. Другим етапом є побудова моделі подій на основі якого необхідно будувати марковську модель. Подальший аналіз марковської моделі дозволяє отриманти показники надійності та січення системи. Використання даної методики вимагає від розробника вміння будувати динамічні ДВ, розробляти відповідну до побудованого динамічного ДВ марковську модель, знати метод розщеплення простору станів та вміти аналізувати побудовані моделі.

В роботі [70] порівнюються два методи аналізу: аналіз на основі дерева відмов та аналіз видів, причин та наслідків відмов (FMEA). В роботі представлено результат порівняння цих двох методів аналізу, із зазначенням внеску кожного для реалізації структурованої інтелектуальної розробки системи управління гідравлічної турбіни та її технічного обслуговування.

В роботі [49] основою методики аналізу надійності телекомунікаційних систем є побудова та аналіз ДВ. В представлених методах автором, запропоновано принципи розробки моделей телекомунікаційних систем та моделей систем їх технічної експлуатації для забезпечення їх надійності та визначення критичності відмов. Побудова моделей технічної експлуатації підкреслює важливість врахування в моделях, не лише структури технічної системи, а й їх технічної експлуатації, що підвищує адекватність отриманих моделей.

Слід відзначити, що для аналізу динамічних ДВ найчастіше використовують ІМ, методом Монте-Карло, який полягає у розігруванні генератором випадкових чисел тривалостей процесів відмов та відновлення на основі їх заданих моделей. Використання імітаційних моделей при оцінці

надійності складних відновлювальних систем призводить до значних затрат машинного часу та ресурсу, особливо це відображається при збільшенні точності моделювання та при необхідності проаналізувати велику кількість варіантів реалізації РСВП.

В роботах [5, 13, 14, 58, 85] представлено авторами методики оцінки безпечності, що представляють собою комбінацію методів аналізу ДВ та FMEA/FMECA-аналізу. Такий комбінаційний підхід забезпечує зменшення внесення помилок при оцінці безпечності [70]. В роботі [85] представлено розроблений авторами частково автоматизований алгоритм верифікації результатів аналізу ДВ та FMEA/FMECA-аналізу. Також розроблений алгоритм перетворення результатів між цими двома методами аналізу. Авторами праць [13, 59, 85] запроновано методики частково автоматизованого отримання ДВ та результатів FMEA-аналізу на основі побудованої моделі у вигляді графа. Слід відзначити, що низький рівень формалізації цих методики підвищує імовірність внесення в модель помилок.

Процедура верифікації побудованих ДВ є достатньо складною задачею. Так в роботі [41] представлено алгоритм верифікації результатів FMEA-аналізу за допомогою побудованого ДВ. Однак дана методика передбачає побудову окремої верифікаційної моделі, що є часоємним та неприйнятним на етапі системо-технічного проетування.

Таким чином, сучасні методики побудови та аналізу ДВ, в більшості випадків, вимагають від розробника "ручної" побудови дерева. Потрібно зауважити, що ДВ є статичними, оскільки вважається, що усі події в системі є взаємонезалежними. Використання методів побудови динамічних ДВ, в яких закладена можливість визначення подій котрі водять в різні аварійні ситуації, вимагає, для подальшого аналізу, залучення складних методів.

Можливість визначення подій котрі водять в різні аварійні ситуації може бути закладена в моделях побудованих за допомогою методу простору станів, однак на даний момент існує необхідність збільшення рівня автоматизації процедур побудови даних моделей.

1.4.3 Аналіз оцінки ризику за допомогою дерев подій

Ризик представляє собою взаємозв'язок між ймовірністю настання події та рівнем наслідків. Тому необхідно враховувати не лише причини, які в призводять до виникнення аварійної події але й визначити усі можливі наслідки до котрих призведе дана подія. Метод побудови дерева подій дозволяє преставити сценарій виникнення усіх можливих наслідків аварійної події.

Даний метод не є автоматизованим і передбачає побудову дерева в якому закладаються певні ймовірнісні значення виникнення усіх можливих наслідків. Автоматизація даного підходу представлений у можливості введення у відповідну форму розроблених програмних засобів.

1.4.4 Аналіз оцінки ризику методом простору станів

Одним з методів оцінки безпечності є метод простору станів. В роботах [33, 130, 146] представлено основи моделювання системи у методом простору станів. Моделлю, яка отримаються згідно даного методу є дискретно-неперервна стохастична система марковського типу, графічним представленням якої є граф станів та переходів і аналітична модель у вигляді системи лінійних диференційних рівнянь (СЛДР) Колмогорова – Чепмена. Однак, слід відзначити що дані методики потребують підвищення рівня автоматизації, оскільки, передбачають ручну побудову моделі об'єкту дослідження, що є надзвичайно трудоміским процесом.

В роботі [15] автор проводить моделювання системи для оцінки безпечності методом простору станів. В результаті побудови та аналізу моделі об'єкту дослідження отримуються - безпечність в залежності від часу та середній час напрацювання на небезпечну відмову. Слід відзначити, що в даній роботі інтенсивність небезпек розподілена за законом розподілу Вейбула, що значно збільшило ступінь адекватності розробленої моделі та точність отриманих результатів моделювання. Однак, аналіз побудованої моделі вимагає від розробника значних часових затрат.

Методика автоматизованої побудови моделі об'єкту дослідження методом простору станів представлено в роботі [27]. Згідно даної методики, у створеному авторами програмному забезпеченні, будується модель елементів системи. Наступним етапом даної методики встановлюються стани, в яких відображаються небезпечні та працездатні стани системи. Наступним етапом даної методики є побудова взаємозв'язків між елементами, встановлення стратегії обслуговування та ремонту системи. На основі отриманої моделі у вигляді графу станів в автоматизованому режимі будується СЛДР. В результаті розв'язку СЛДР отримується показник безпечності ймовірність небезпечної відмови за годину та функція готовності системи. Автори роботи проводять аналіз безпечності програмного забезпечення на трьох рівнях - на системному рівні; на рівні підсистем; на рівні окремого елементу, шляхом побудови моделі об'єкту дослідження методом простору станів. У зв'язку з необхідністю врахування великої кількості станів, автори спрощують модель, що знижує рівень отриманих результатів. Також дана методика не є придатною для багатоваріантного аналізу, оскільки вимагає побудови та аналізу моделі для кожної реалізації системи.

На сьогоднішній день розроблено удосконалену технологію з високим рівнем формалізації, що дозволило автоматизувати процес побудови об'єкту дослідження у вигляді графа станів та переходів [100, 113]. Представлена технологія дозволяє детально описати надійнісну [124], функціональну [129], поведінки системи та аварійні ситуації в тому числі. Однак, на сьогоднішній час дана технологія призначена для опису функціональної та надійнісної поведінки РСВП, а для оцінки безпечності вона потребує певних вдов\сконалень, оскільки в наявному вигляді не дозволяє розрізняти стани відмови, а відповідно формувати аварійні ситуації. Крім цього слід відмітити, що на даний момент не розроблено методик для автоматизованої побудови ДВ об'єкту дослідження на основі методу простору станів, чи іншого представлення РСВП.

1.4.5 Порівняльний аналіз сучасних технологій побудови моделей для оцінки ризику, придатних для застосування на етапі системотехнічного проектування технічних систем відповідального призначення

Проведений аналіз існуючих технологій побудови моделей для оцінки ризику експлуатації показали, що переважна більшість з них не враховує в повній мірі визначальні, з точки зору безпечності, особливості сучасних систем радіоуправління БпЛА.

Моделі оцінки ризику, які базуються на методі логіко-ймовірнісних методах, дають можливість побудувати дерево відмов об'єкту дослідження та отримати МС. Слід відмітити, що у статичних ДВ не враховуються взаємозалежності між подіями, у динамічних ДВ вона враховується. Однак, для подальшого аналізу динамічного ДВ необхідно використовувати інші методи моделювання - метод простору станів або ІМ методом Монте - Карло. Однак методи, які базуються на методі ЛІМ, не придатні до багатоваріантного аналізу, що є обов’язковим при оцінці безпечності експлуатації БпЛА на системотехнічному етапі проектування, коли з декількох технічних рішень потрібно вибрати те. Яке забезпечить мінімальний ризик при експлуатації БпЛА.

Використання FMEA/FMECA-аналізу дозволяє отримати достатньо деталізовану оцінку показників безпечності і зокрема ризику експлуатації РСВП. Але слід відзначити, що показники безпечності та в тому числі показники ризику експлуатації отримуються винятково шляхом експертної оцінки, що вносить суб'єктивність в отримані результати аналізу. Особливо ступінь суб'єктивності є значною, коли необхідно зменшити значення показника ризику - RPN (FMEA) чи рівня ризику - RL (FMECA) за рахунок рекомендацій експертів, оскільки перебудова моделі з подальшою переоцінкою ризику не відбувається, і перевірити кількісно чи показники ризику є знижені чи навпаки завищені немає можливості.

Методи, в основі яких покладено ІМ методом Монте - Карло, потребують значних обчислюваних ресурсів. В більшості випадків при оцінці безпечності і зокрема ризику експлуатації РСВП дані методи призначені для аналізу моделей, побудованих за допомогою методів ЛІМ чи простору станів. Дані методи дозволяють, розробивши відповідну модель РСВП, отримати показники надійності та провести оцінку ризику експлуатації. Однак, отримана модель не надається до модифікації, при зміні її вхідних параметрів чи структури системи, що знижує ефективність використання методик оцінки ризику експлуатації БпЛА на системотехнічному етапі проектування. Слід відзначити значний рівень складності побудови та верифікації ІМ.

Методики, котрі базуються на методі простору станів, на даний момент не використовуються в повній мірі своїх можливостей через значні інтелектуальні та часові затрати при ручній розробці моделі об'єкту дослідження у вигляді графа станів та переходів. Використання удосконаленої технології моделювання дискретно-неперервних стохастичних систем [100, 113] дозволяє в автоматизованому режимі будувати модель об'єкту дослідження у вигляді графа станів та переходів. За допомогою використання даної технології потенційно можливо враховувати особливості БпЛА: обмежений ремонт окремих елементів, діагностику, враховувати залежностей між подіями, простій тощо, однак існує значна проблема в однозначній ідентифікації аварійних ситуацій. Слід відмітити, що високий рівень формалізації такого підходу дозволяє ефективно проводити багатоваріантний аналіз об'єкту дослідження при зміні вхідних даних. Однак, дана технологія потребує удосконалення і для цього необхідно внести відповідні зміни в методику побудови формалізованого представлення об'єкту.

Методи побудови дерева подій передбачають виключно ручну побудову дерева подій на основі логічного аналізу. Даний метод передбачений лише для визначення усіх можливих наслідків аварійної відмови. Автоматизація даного методу полягає лише у створеній електронній таблиці котру заповняє

розробник та після її заповнення в автоматизованому режимі формується дерево подій.

Отже, аналіз публікацій з проблеми оцінки ризику експлуатації РСВП і зокрема систем радіоуправління БпЛА показало, що:

- Моделей придатних для оцінки ризику експлуатації БпЛА з врахуванням усіх особливостей навігаційно-обчислювальної підсистеми літального апарата не розроблено.
- Методики автоматизованого отримання дерев відмов для візуалізації проблеми виникнення аварійних ситуацій при екплуатації БпЛА не розроблено.
- Всі оглянуті методи побудови моделей для оцінки ризику враховують в моделі або надійнісну поведінку або поведінку системи при настанні аварійних ситуацій. Тобто для оцінки надійності та безпечності потрібно будувати дві різні моделі, які враховують вплив надійності на безпечність і навпаки.
- Існуючі технології моделювання не дозволяють враховувати в одній моделі вплив обмеженого ремонту окремих елементів чи підсистем, діагностику, простій системи, вплив відмовостійких конфігурацій на рівень ризику експлуатації РСВП.
- Переважна більшість моделей є непридатними для багатоваріантного аналізу проектних рішень, які були прийняті після застосування рекомендацій із зменшення ризику експлуатації, отриманих в результаті здійснення FMEF/FMECA - аналізу.

Результат порівняння існуючих технологій побудови моделей оцінки безпечності, які придатні для застосування на етапі системотехнічного проектування представлено а таблиці 1.3.5:

Таблиця 1.3.5

Порівняння можливостей технологій оцінки ризику експлуатації РВСП

Технології оцінки ризику базуються на методах / Можливості технологій	Логіко-ймовірнісні методи	Імітаційне моделювання	Метод простору станів	Удосконалена технологія побудови простору станів
Визначення подій котрі водять в різні аварійні ситуації	-/+	-	+	+
Оперативно здійснювати багатоваріантний аналіз	-	-	-	+
Здійснювати побудову ДВ	+	-	-	-
Комплексно (поєднано) враховувати надійність і безпечність РСВП	-	-	-	-
Враховувати обмежений ремонт	-	+	+	+
Враховувати наявність вбудованого контролю і діагностики	+	+	+	+
Враховувати простій системи	+	+	+	+

Висновки до розділу 1

1. На основі проведеного аналізу сучасних інформаційних джерел можна стверджувати про відсутність математичних моделей радіоелектронних систем відповідального призначення, які б давали змогу оцінити ризик експлуатації навігаційно-обчислювальної підсистеми безпілотного літального апарата в залежності від того, які відмовостійкі конфігурації використано при її побудові.
2. Переважна більшість методів оцінки безпечності, включаючи стандартизовані FMEA/FMECA методології, за винятком моделей на базі дерев відмов та дерев подій, дозволяють отримати лише якісні експертні оцінки ризику експлуатації систем відповідального призначення. В багатьох випадках це завищує реальний рівень ризику, а подальші процедури його зниження призводять до необґрунтованого ускладнення проектованих систем.
3. При використанні різновидів методу логіко-імовірнісного моделювання, за винятком динамічних дерев відмов, для кількісної оцінки ризику є

неможливим врахування взаємовз'язку між подіями які призводять до аварійної ситуації, що знижує точність оцінки показників ризику експлуатації систем відповідального призначення. Використання динамічних дерев відмов потребує одночасного застосування разом з ними або методу простору станів, або методу імітаційного моделювання, що при відсутності засобів автоматизації побудови дерев відмов суттєво збільшує розмірність і без того громіздкої моделі, а подальше спрощення такої моделі при аналізі нівелює врахування додаткових чинників. Крім цього усі без винятку різновиди логіко-ймовірнісних методів не дають змоги адекватно оцінити вплив на ризик експлуатації технічного обслуговування та обмеженого ремонту систем, застосування засобів еонтролю та діагностики систем, простій системи при проведенні ремонту.

4. Оглянуті методи оцінки ризику експлуатації в основному є неформалізованими і відповідно не підходять для багатоваріантного аналізу навігаційно-обчислювальної системи, що є однією з основних вимог системотехнічного проектування, коли потрібно вибрати кращий варіант із конкурентних за обмежений проміжок часу. Крім цього не виявлено засобів автоматизованої побудови дерев відмов,
5. Проведений аналіз методів побудови математичних моделей показав, що для оцінки ризику експлуатації систем радіоуправління безпілотних літальних апаратів доцільно використати метод простору станів з вдосконаленою технологією побудови простору станів на базі структурно автоматних моделей.

Проведений аналіз показав, що для вирішення науково-прикладної задачі зниження ризику експлуатації навігаційно-обчислювальної підсистеми безпілотного літального апарата шляхом реалізації у вигляді відмовостійких конфігурацій найбільш «слабких» з точки зору безпечності підсистем невирішеними завданнями є:

1. Розробка моделей підсистем навігаційно-обчислювальної системи, які є визначальними з точки зору ризику експлуатації. Такими підсистемами, згідно аналізу інформаційних джерел, є обчислювальна підсистема та підсистема навігації. Розроблена модель повинна враховувати всі особливості підсистем, що дозволить правильно оцінити ризик їх експлуатації.
2. Розробка алгоритмів та засобів оцінки показників ризику експлуатації, які дозволять зробити процес побудови моделі формалізованим, що дасть змогу мінімізувати ймовірність внесення помилки у модель. Разом з цим розроблені засоби забезпечать можливість багатоваріантного аналізу досліджуваних підсистем.
3. Розробка засобів візуалізації розвитку аварійних ситуацій у вигляді дерев відмов. Розробка таки засобів пояснюється неохідністю побудови дерев відмов для сертифікації, згідно міжнародних стандартів, проектованих систем радіоуправління з точки зору безпечності.
4. Розробка методики отримання мінімальних січень на основі формування комбінацій непрацездатних станів, які призводять до аварійних ситуацій.
5. Розробка методики дослідження рівня ризику експлуатації систем радіоуправління безпілотними апаратами, яка дозволить проводити багатоваріантний аналіз системи при різноманітних варіантах відмовостійких конфігурацій.

РОЗДІЛ 2. РОЗРОБКА МОДЕЛІ ОБЧИСЛЮВАЛЬНОЇ ПІДСИСТЕМИ З ВИКОРИСТАННЯМ МАЖОРИТАРНОЇ СТРУКТУРИ

Однією з основних умов успішного виконання БпЛА польотного завдання є надійне функціонування обчислювальної підсистеми (ОП). Така підсистема є складовою навігаційно-обчислювальної підсистеми БпЛА і забезпечує: керування іншими підсистемами; розрахунок курсових параметрів, навігаційну точність; автоматизацію процесу управління і звільняє операторів БпЛА від монотонного і повторюваного виконання завдань “ручного” управління.

Аналіз аварійних ситуацій БпЛА, пов’язаних з експлуатацією літальних апаратів, свідчить про те, що вони, в основному, виникають через помилки операторів, втрату концентрації уваги в умовах значних психофізіологічних навантажень [152] та через збої та відмови обчислювальної та навігаційної підсистем [23]. Тому підвищення безпеки польотів БпЛА безпосередньо залежить від рівня автоматизації функцій керування безпілотником, а це може бути реалізовано шляхом удосконалення ОП та забезпечення заданого рівня її надійності.

Для зменшення можливості виникнення аварії окремі підсистеми, що входять до складу навігаційно-обчислювальної підсистеми на БпЛА реалізують як відмовостійкі конфігурації. Для ОП характерним є застосування мажоритарних структур [86-88], оскільки вони забезпечують захист від збоїв на апаратному рівні. Крім цього застосовують функціональне резервування для підсистем, наприклад, навігаційної та супутникової навігаційної, які надають вхідні дані для ОП .

2.1 Узагальнена структура обчислювальної підсистеми

До складу обчислюваної підсистеми, структурна схема якої представлена на рис. 2.1, входить: три обчислювальних мікропроцесори (МКП); детектор несправностей (ДН) для виявлення несправних МКП; фільтр Калмана (ФК); та підсистема електроживлення (ПЕЖ). Також важливими ситемами БпЛА, які мають визначальний вплив на якість роботи ОП є система автопілотування,

котра має зворотній зв'язок з обчислювальною підсистемою та оператором та навігаційна підсистема.

Рис. 2.1 Структурна схема обчислювальної підсистеми БпЛА

При побудові моделі необхідно врахувати наступні її особливості які покликані зменшити ризик експлуатації БпЛА при виникненні несправностей в елементах ОП :

- *Локалізація несправного мікропроцесора ОП.* Контроль працездатності МКП обчислюваної підсистеми системи радіуправління БпЛА виконується за допомогою детектора несправностей (ДН). Детектор несправностей здійснює порівняння сигналів з виходів $МКП_1$, $МКП_2$, $МКП_3$ з вхідним сигналом Калманіського фільтру. При їх неспівпадінні, ДН видає сигнал про втрату працездатності відповідного МКП, яка наступила внаслідок відмови одного з МКП ($МКП_1$, $МКП_2$, $МКП_3$). Також у МКП може

відбутись збій у програмному забезпеченні, оскільки інтенсивність збоїв є більшою за інтенсивність відмов МКП. При виявленні збою запускається процедура тестування МКП. Якщо процедура тестування виявляє факт збою, здійснюється перезавантаження відповідного програмного забезпечення МКП і якщо процедура перезавантаження успішно закінчена то МКП продовжує виконання обробки інформації. В разі неуспішного перезавантаження детектор несправностей вимикає МКП.

- *Локалізація несправного автопілота*. Контроль непрацездатності автопілота БпЛА відбувається за допомогою процедури порівняння наявних сигналів зворотнього зв'язку до МКП. Автопілот може бути непрацездатним внаслідок відмови двох МКП або відмови самого автопілоту.
- *Локалізація несправного калманівського фільтра*. Детектування несправності калманівського фільтра відбувається за допомогою виявлення наявних сигналів на його виході при подачі на його вхід сигналів з мікропроцесорів.

Для формалізації вищезазначених особливостей ОП з метою відображення їх в математичній моделі необхідно сформувати їх у вигляді наступних процедур:

Процедура 1. *Виявлення несправності МКП в системі*. Дана процедура запускається за умови, що відмовив один з МКП. Обчислювальна система підсистеми системи радіуправління БпЛА вважається працездатною за умови, що два з трьох МКП будуть працездатними. За умови використання правила мажоритарної структури два з трьох, в разі виходу з ладу наступного МКП система не зможе приймати правильних рішень для продовження польоту, що однозначно призведе до втрати можливості подальшого польоту БпЛА.

Процедура 2. *Перезавантаження МКП.* У разі збою програмного забезпечення відбувається процедура перезавантаження МКП. Під час

перезавантаження відповідний МКП може або відмовити або успішно перезавантажитись.

Процедура 3. *Виявлення несправності калманівського фільтра*. Процедура виявлення калманівського фільтра (КФ) запускаєтсья за умови, що відмовило два або більше МКП чи відмовило дві або більше НП або відмовив калманівський фільтр.

Процедура 4. *Виявлення несправності автопілоту*. Процедура запускаєтсья за умови, що відмовило два або більше МКП чи відмовило дві або більше НП або в разі відмови самого автопілота.

Процедура 5. *Виявлення несправності системи електроживлення*. Процедура запускаєтсья за умови, що відмовила ПЕЖ.

Для уникнення однотипної відмови МКП для кожного з них розробляється різне програмне забезпечення. Також для виключення однотипних збоїв та відмов у системі використовуються МКП різних виробників. В даній системі використано МКП наступних виробників Atmel, Motorolla та Toshiba.

За умови виявлення несправності МКП у системі запускається процедура тестування відповідного мікпропроцесора на збій, після виконання якої визначається чи відмовив даний МКП або чи відбувся збій його програмного забезпечення. В разі виявлення збою системи з заданою ймовірністю запускається процедура перезавантаження відповідного МКП.

2.3 Удосконалення методу вибору непрацездатних станів з графу станів і переходів для побудови моделей оцінки ризику

Як показав аналіз інформаційних джерел, оцінка ризику експлуатації системи радіуправління БпЛА базується на отриманні та подальшому аналізі комбінацій подій, що потенційно можуть призвести до аварійної ситуацій. Ці події називаються мінімальними січенями. Мінімальні січення (МС) - сукупність відмов елементів системи чи підсистеми, що призводять до відмови системи в цілому. Вважається, що якщо з такої комбінації подій вилучити хоча б одну, то унеможливлюється виникнення аварійної ситуації системи.

На сьогодні МС отримуються на основі дерева відмов (ДВ). Однак, в результаті аналізу МС на базі ДВ, через неврахування особливостей навігаційно-обчислювальної підсистеми БпЛА розробники, за рахунок спрощень в моделі можуть завищувати або занижувати рівень ризику, оскільки складність сучасних БпЛА призводить до необхідності побудови ДВ великої розмірності, що при ручній побудові супроводжується великими затратами часу, внесенням помилок, які важко виявити та неможливістю врахування залежних подій. Окрім недоліків пов'язаних з ручною розробкою, ДВ не дозволяють врахувати вплив надійнісної поведінки БпЛА на ймовірність появи аварійних ситуацій, що є важливим для складних систем.

В повній мірі відобразити особливості ОП (надлишковість, можливість реконфігурації, перезавантаження ПЗ, роботу засобів контролю та діагностики, технічне обслуговування та ремонт тощо) та її надійнісну поведінку дає змогу граф станів та переходів (ГСП). Однак, у відомих методиках отримання ГСП усі непрацездатні стани (аварійні ситуації) об'єднуються в один поглинаючий стан. Спроби розщепити цей стан при використанні навіть автоматизованих методик, призводить неоднозначної ідентифікації непрацездатних станів через їх об’єднання на етапі побудови ГСП та високу ймовірність неправильного розщеплення і відповідно до зменшення достовірності отриманих результатів.

Для можливості отримання МС з графу станів та переходів необхідно скоректувати методику автоматизованої побудови ГСП таким чином, щоби було можна отримувати розщеплений поглинаючий стан аварійних ситуацій. Розщеплений поглинаючий стан представлятиме собою масив непрацездатних станів, на основі яких, стає можливим аналіз відмов чи аварій окремих елементів та підсистем. Окрім цього, необхідно розробити спосіб поєднання непрацездатних станів в окремі аварійні ситуації з врахуванням того, що окремі непрацездатні стани можуть входити в різні аварійні ситуації.

Для реалізації усього вищевказаного, при побудові структурно – автоматної моделі, необхідно вибирати структуру вектора станів таким чином, щоб кожен елемент об’єкту дослідження міг перебувати тільки у двох станах –

працездатному та непрацездатному. Тобто вектор стану набуває бінарного вигляду і сама САМ стає бінарною.

На основі бінарної САМ формується граф станів та переходів, в якому необхідно виділити непрацездатні стани. Оскільки станів може бути порядку $10^2...10^3$ то сортування вимагає використання складних алгоритмів обробки.

Процедуру сортування можна реалізувати наступним чином: розробити модель об'єкту дослідження і згенерувати ГСП з умовою відмови. Таким чином отримується масив усіх можливих працездатних станів. Наступним кроком необхідно розробити модель об'єкту дослідження і згенерувати ГСП без умови відмови - у цьому випадку отримується масив усіх можливих станів, включаючи як працездатні стани, так стани відмови. Приклад ГСП з представленим розщепленим станом відмови представлено на рис. 2.1.

Сукупність станів відмови, які призводять до аварії системи будемо в подальшому називати - аварійними ситуаціями (АС).

Оскільки розщеплений стан відмови може містити декілька аварійних

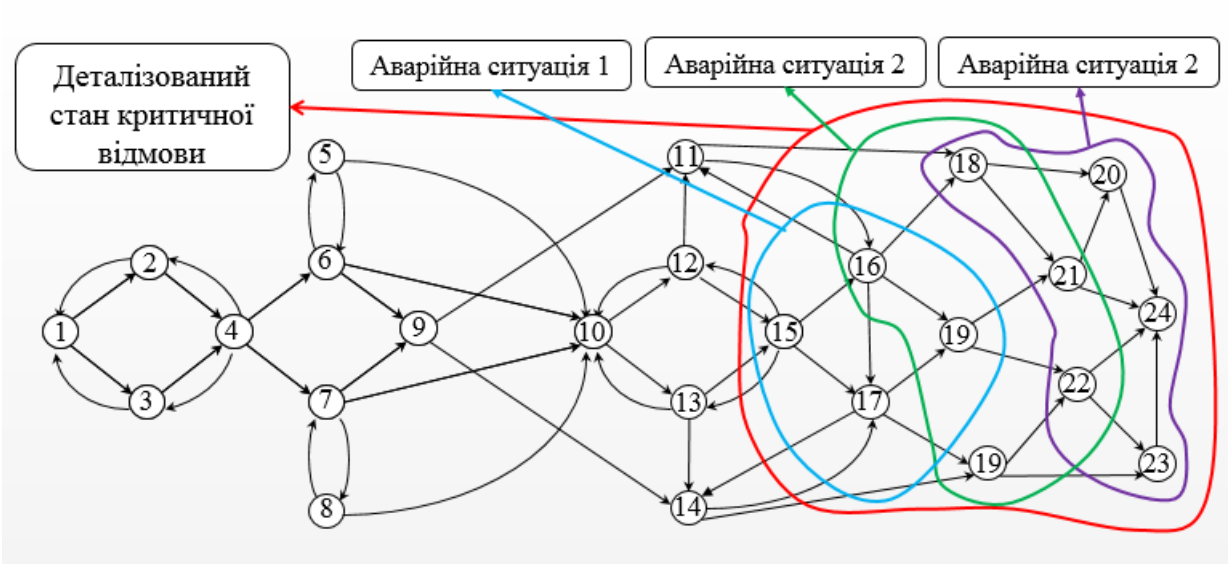

Рис. 2.2 Приклад графа станів та переходів з представленням трьох аварійних ситуацій

ситуацій РСВП, то таким чином він містить в собі декілька дерев відмов. Таким чином, з графа станів та переходів можна отримати МС - комбінації подій котрі призводять до відмови системи чи аварійної ситуації. За допомогою отриманих МС можна знайти ступінь кореляції окремих аварійних ситуацій між собою. В

усіх відомих методиках при побудові МС вважається, що події базового рівня (відмови елементів підсистеми). які входять в одну аварійну ситуацію не залежать від подій базового рівня іншої аварійної ситуації.

Отримавши МС можна виконати зворотну задачу - побудувати ДВ. Побудоване графічне представлення дерева дає змогу розробнику відслідковувати сценарії виникнення аварійних ситуацій. Окрім цього побудова ДВ і МС є одним з етапів оцінки ризику за допомогою FMEA – аналізу, а в подальшому і сертифікації БпЛА.

2.3 Отримання мінімальних січень обчислювальної підсистеми безпілотного літального апарата на основі графу станів та переходів

Автоматизація побудови дерева відмов РСВП базується на тому, що метод визначення МС здійснюється безпосередньо з графа станів та переходів об'єкта дослідження [74]. Отримати МС та побудувати ДВ дозволила удосконалена технологія побудови математичних моделей дискретно-неперервних стохастичних систем [100]. Суть цієї технології полягає в автоматизації процесу побудови математичних моделей поведінки системи на основі структурно-автоматної моделі (САМ) об'єкту дослідження.

Структурно-автоматна модель навігаційно-обчислювальної підсистеми БпЛА є формалізованим представленням її структури та поведінки і включає в себе: параметри об'єкту дослідження, які мають бути відображені в моделі; вектор станів (ВС) об'єкту дослідження; дерево правил модифікації компонент вектора стану.

За допомогою програмного модуля ASNA [101, 116], для якого САМ є вхідними даними про об'єкт дослідження, проектант автоматизовано отримує граф станів і переходів з необхідним для побудови ДВ рівнем деталізації. На основі графа станів і переходів формується аналітична модель системи у вигляді системи лінійних диференціальних рівнянь (СЛДФ) Колмогорова - Чепмена. Розв’язок системи диференціальних рівнянь дає розподіл ймовірностей перебування системи у всіх можливих станах як працездатних так

і непрацездатних. Використанням певних процедур обробки непрацездатних станів стане можливо сформувати масив МС.

Підхід отримання МС та побудови ДВ на основі ГСП з розщепленим станом відмови представлений на рис. 2.3. Слід відзначити, що етапи даного підходу - формування моделі об'єкту у вигляді графа станів та переходів, формування системи диференціальних рівнянь Колмогорова - Чепмена та розв'язання системи диференціальних рівнянь Колмогорова - Чепмена є автоматизованими за допомогою програмного модуля ASNA. А для процедур

Рис. 2.3 Побудови мінімальних січень та дерева відмов на базі ГСП

знаходження МС та побудови ДВ відповідні алгоритми та засоби автоматизації будуть представлені в розділі 4.

2.3.1 Розробка бінарної структурно-автоматної моделі

Згідно підходу, представленого на рис. 2.3, першим етапом є побудова бінарної САМ, в якій кожен елемент системи представляється окремим

компонентом ВС, за яким можна чітко ідентифікувати його стан як у множині працездатних станів так і у розщепленому непрацездатному стані.

Бінарна САМ - це формалізований опис об'єкта дослідження, в якому усі елементи структури системи відображаються окремими компонентами ВС і можуть приймати два значення - нуль за мови настання відмови та одиниця за умови працездатності чи іншого ідентифікатора стану, котрий представляє собою стан відмінний від стану відмови. Бінарна САМ, на відміну від звичайної САМ [94, 102] дає змогу описати структуру і поведінку системи без об'єднання як працездатних так і непрацездатних станів.

Згідно технології [101, 116], при розробці бінарної САМ, необхідно вирішити наступні задачі: сформувати вектори станів (ВС); визначити множину формальних параметрів (МФП) моделі; описати поведінку системи у вигляді базових подій, які відбуваються у системі, а також умов і обставин при яких відбуваються ці події; сформувати формули розрахунку інтенсивностей переходів (ФРІП) із стану в стан; сформувати формули розрахунку альтернативних ймовірностей переходів (ФРАЙП); встановити правила модифікації компонент ВС і визначити умову відмову (УВ) системи.

Множину формальних параметрів моделі складають константи, які визначаються для конкретного об’єкту дослідження. Вектор станів складається із компонент, які однозначно визначають стан елементів системи в кожен момент часу. Для побудови дерева правил модифікації (ДПМ) компонент вектора станів необхідно: здійснити формалізований опис ситуацій в яких відбуваються базові події через представлення умов та обставин; провести формування формул розрахунку інтенсивностей базових подій та правил модифікації компонент ВС.

На основі розробленої САМ та програмного модуля ASNA здійснюється автоматизована розробка графа станів та переходів і відбувається формування математичної моделі у вигляді системи диференційних рівнянь Колмогорова – Чепмена, розв'язок якої, дасть можливість отримати кількісні значення МС.

2.3.2 Отримання мінімальних січень обчислювальної підсистеми безпілотного літального апарата

Для знаходження мінімальних січень, необхідно знайти всі комбінації, при яких відбудеться аварійна ситуація системи за найменшої кількості елементів системи, які вийшли з ладу. У деяких випадках, комбінація може містити лише один елемент. Це означатиме, що даний елемент є найбільш критичною частиною системи і при його виході з ладу настає аварійна ситуація. В переважній більшості випадків комбінація містить два і більше елементи. Вважається, що чим довше січення (більша комбінація елементів), тим менш вразливою є система, з точки зору аварійних ситуацій, до відмов окремих елементів.

Для розрахунку мінімальних січень на основі САМ розроблено методику, яка містить наступні етапи:

1. Розробка бінарної САМ, що включає в себе МФП, ВС, ДПМ, ФРІП, ФРАЙП та УВ.
2. На основі розробленої бінарної САМ за допомогою програмного модуля ASNA у автоматизованому режимі генерується граф станів і переходів та на його основі формується СДР Колмогорова – Чепмена.
3. В результаті розв’язку СЛДР отримується розподіл ймовірностей перебування у працездатних та непрацездатних станах.
4. З врахуванням умови відмови ймовірність безвідмовної роботи об’єкту дослідження дорівнюватиме сумі усіх отриманих працездатних станів в конкретний момент часу. Ймовірність відмови, відповідно буде дорівнювати сумі усіх непрацездатних станів. Сума ймовірностей перебування у працездатних та непрацездатних станах дорівнює одиниці.
5. На основі логічного аналізу непрацездатних станів об’єкту дослідження формуються мінімальні січення.
6. Для визначення значення одного з мінімальних січень необхідно повторити п. 2-4, замінивши умову відмови на одне із січень. В матриці

переходів з'явиться один додатковий стан, котрий матиме значення ймовірності виникнення даного мінімального січення.

7. Повторити п.6, доки не переберуться всі мінімальні січення, вибрані з п.5.

Сума всіх комбінацій відмов в результаті дасть розробнику загальне значення аварійної ситуації об’єкту дослідження – $Q_{заг}$. Відповідно до цього, необхідно визначити процентне відношення усіх комбінацій до загальної відмови та сформувати зведену таблицю мінімальних січень.

Використанням запропонованої процедури фільтрації непрацездатних станів формується масив мінімальних січень. Кількісні показники МС отримуються шляхом сумування ймовірностей перебування системи у відповідних станах та формується таблиця МС.

2.4 Розробка бінарної структурно-автоматних моделі обчислюваної підсистеми безпілотного літального апарата

2.4.1 Визначення базових подій для бінарних структурно-автоматних моделей обчислюваної підсистеми безпілотного літального апарата

Із поведінки системи складається перелік подій, які можуть відбуватись у системі. Події необхідно представляти парами, фіксуючи початок і закінчення відповідного часового інтервалу, який відповідає певному стану системи. Події, обумовлені поведінкою системи, що відбуваються у ній представлено в табл. 2.1. Провівши аналіз подій представлених в таблиці, визначаються базові події.

Таблиця 2.1

Представлення пар подій, які фіксують початок і закінчення часового інтервалу перебування системи в певному стані

Пор. № пари подій	**Подія, яка фіксує початок події**	**Подія, яка фіксує закінчення**
1	«Початок роботи системи»	«Відмова мікропроцесора 1»
2	«Початок роботи системи»	«Відмова мікропроцесора 2»

Пор. № пари подій	Подія, яка фіксує початок події	Подія, яка фіксує закінчення
3	«Початок роботи системи»	«Відмова мікропроцесора 3»
4	«Початок роботи системи»	«Збій МКП1»
5	«Початок роботи системи»	«Збій МКП2»
6	«Початок роботи системи»	«Збій МКП3»
7	«Початок роботи системи»	«Відмова фільтра Калмана»
8	«Початок роботи системи»	«Відмова підсистеми електроживлення»
9	«Початок роботи системи»	«Відмова автопілота»
10	«Початок роботи системи»	«Відмова детектора неспарностей»
11	«Збій МКП1»	«Перезавантаження МКП1»
12	«Збій МКП2»	«Перезавантаження МКП2»
13	«Збій МКП3»	«Перезавантаження МКП3»
14	«Збій МКП1»	«Відмова мікропроцесора 1»
15	«Збій МКП2»	«Відмова мікропроцесора 2»
16	«Збій МКП3»	«Відмова мікропроцесора 3»

Незалежними базовими подіями у системі є:«Відмова мікропроцесора 1», «Відмова мікропроцесора 2», «Відмова мікропроцесора 3», «Перезавантаження МКП1», «Перезавантаження МКП2», «Перезавантаження МКП3», «Відмова підсистеми електроживлення» та «Відмова фільтра Калмана» .

Згідно [132] для даної системи вибрано наступні базові події:

- **Базова подія 1**«Відмова МКП1».
- **Базова подія 2**«Відмова МКП2».
- **Базова подія 3** «Відмова МКП3».
- **Базова подія 4** «Перезавантаження МКП1»
- **Базова подія 5**«Перезавантаження МКП2»
- **Базова подія 6** «Перезавантаження МКП3»
- **Базова подія 7** «Відмова фільтра Калмана»

- **Базова подія 8** «Відмова ПЕЖ»

Відмова автопілота фіксується відсутністю сигналу на його виході при наявності сигналів на його вході.

2.4.2 Допущення прийняті при розробці моделей обчислюваної підсистеми безпілотного літального апарата

При розробці моделей було прийнято декілька допущень:

- Надійність детектора несправностей (ДН), автопілоту та калманівського фільтра є на декілька порядків вищою від інших складових системи, а їх тривалість безвідмовної роботи є більшою ніж тривалість експлуатації обчислювальної системи. Тому, прийнято рішення, що в розроблених автопілот та ДН є безвідмовними.
- Інтенсивність збоїв програмного забезпечення МКП в моделях враховується - ймовірністю $P_{зб}$. Усунення наслідків збою здійснюється шляхом перезавантаження програмного забезпечення з ймовірністю $P_{пер}$. У разі неуспішного перезавантаження відповідний МКП відключається від системи за допомогою ДН.
- Середній інтревал часу перезагрузки МКП для кожного з трьох є одининаковим.
- Тривалість всіх процесів, які відбуваються в системі розподілені згідно експоненційного закону. Інтенсивності подій є сталими в часі величинами.
- Дві батареї підсистеми електроживлення знаходять в гарячому резерві і їх інтенсивності відмов є однаковими.

2.4.3 Параметри обчислювальної пісистеми безпілотного літального апарата, які відображені в моделі

При формуванні моделі необслуговуваної обчислювальної підсистеми БпЛА її склад і окремі складові необхідно представити відповідними параметрами, а саме:

- λ_{me1} – інтенсивність відмов МКП1;
- λ_{me2} – інтенсивність відмов МКП2;
- λ_{me3} – інтенсивність відмов МКП3;
- $P_{зб1}$ – ймовірність виникнення збою в МКП1;
- $P_{зб2}$ – ймовірність виникнення збою в МКП2;
- $P_{зб3}$ – ймовірність виникнення збою в МКП3;
- $P_{перез1}$ – ймовірність успішного перезавантаження МКП1;
- $P_{перез2}$– ймовірність успішного перезавантаження МКП2;
- $P_{перез3}$ – ймовірність успішного перезавантаження МКП3;
- $\lambda_{ПЕЖ}$ – інтенсивність відмов підсистеми електроживлення;
- $\lambda_{ПЕЖ}$ – інтенсивність відмов фільтра Калмана;
- $T_{перез}$ - середнє значення інтервалу перезавантаження МКП.

Інтенсивності відмов МКП взято з технічної документації виробника.

2.4.4 Структура вектора обчислювальної підсистеми безпілотного літального апарата

Вектор стану обчислювальної системи з використанням мажоритарної структури представлений наступними компонентами:

V1 – відображає поточний стан МКП1 (початкове значення компоненти V1 дорівнює два N_1=2, якщо у МКП1 відбудеться збій то стан даного вектора буде рівним одиниці N_1=1, якщо МКП1 відмовить то стан даного вектора буде рівним нулю N_1=0);

V2 – відображає поточний стан МКП2 (початкове значення компоненти V6 дорівнює два N_2=2, якщо у МКП2 відбудеться збій то стан даного вектора буде рівним одиниці N_2=1, якщо МКП2 відмовить то стан даного вектора буде рівним нулю N_2=0);

V3 – відображає поточний стан МКП3 (початкове значення компоненти V3 дорівнює два N_3=2, якщо у МКП3 відбудеться збій то стан даного вектора буде рівним одиниці N_3=1, якщо МКП3 відмовить то стан даного вектора буде рівним нулю N_3=0);

V4 – відображає поточний стан системи електроживлення (початкове значення компоненти V4 дорівнює два N_4=2, якщо одна з ПЕЖ відмовить, то стан даного вектора буде зменшеним на одинцю, за умови відмови двох ПЕЖ стан даного вектора буде рівним нулю N_4=0);

V5 – відображає поточний стан фільтра Калмана (початкове значення компоненти V5 дорівнює одиниці N_5=1, якщо фільтра Калмана відмовить, то стан даного вектора рівним нулю - N_5=0);

Результати розробки, тобто структурно-автоматні моделі, представлені в таблицях 2.2 та 2.3:

Таблиця 2.2

Структурно-автоматна модель обчислюваної підсистеми БпЛА з використанням мажоритарної структури, яка працює за правилом "2 з 3".

Умови та обставини	**ФРІБП**	**ФРЙАП**	**ПМКВС**
1. Базова подія «Відмова МКП №1»			
(V1=2)	$\lambda_{МКП1}$	1 - $P_{зб1}$	V1:= 0
(V1=2)		$P_{зб1}$	V1:= 1
2. Базова подія «Відмова МКП №2»			
(V2=2)	$\lambda_{МКП2}$	1 - $P_{зб2}$	V2:= 0
(V2=2)		$P_{зб2}$	V2:= 1
3. **Базова подія «Відмова МКП №3»**			
(V3=2)	$\lambda_{МКП3}$	1 - $P_{зб3}$	V3:= 0
(V3=2)		$P_{зб3}$	V3:= 1
4. «Перезавантаження МКП1»			
(V1=1)	1/ Тпз	$P_{перез1}$	V1:= 2
(V1=1)		1-$P_{перез2}$	V1:= 0
5. **«Перезавантаження МКП2»**			
(V2=1)	1/ Тпз	$P_{перез2}$	V2:= 2
(V2=1)		1- $P_{перез2}$	V2:= 0
6. **«Перезавантаження МКП3»**			
(V3=1)	1/ Тпз	$P_{перез3}$	V3:= 2
(V3=1)		1- $P_{перез3}$	V3:= 0
7. **«Відмова системи електроживлення»**			
(V4>0)	$\lambda_{ПЕЖ}$	1	V4:= V4-1

Умови та обставини	ФРІБП	ФРЙАП	ПМКВС
8. **«Відмова фільтра Калмана»**			
(V5>0)	$\lambda_{ФК}$	1	V5:= V5-1
Умова критичної відмови:			
(((V1=0) AND (V2=0)) OR ((V2=0) AND (V3=0)) OR ((V1=0) AND (V3=0)) OR (V4=0) OR (V5=0))			

Таблиця 2.3

Структурно-автоматна модель обчислюваної підсистеми з двохкратним резервування МКП.

Умови та обставини	ФРІБП	ФРЙАП	ПМКВС
1. Базова подія «Відмова МКП №1»			
(V1=2)	$\lambda_{МКП1}$	1 - $P_{зб1}$	V1:= 0
(V1=2)		$P_{зб1}$	V1:= 1
2. Базова подія «Відмова МКП №2»			
(V2=2)	$\lambda_{МКП2}$	1 - $P_{зб2}$	V2:= 0
(V2=2)		$P_{зб2}$	V2:= 1
3. **Базова подія «Відмова МКП №3»**			
(V3=2)	$\lambda_{МКП3}$	1 - $P_{зб3}$	V3:= 0
(V3=2)		$P_{зб3}$	V3:= 1
4. «Перезавантаження МКП1»			
(V1=2)	1/ Тперез	$P_{перез1}$	V1:= 1
(V1=2)		1-$P_{зб2}$	V1:= 0
5. **«Перезавантаження МКП2»**			
(V2=2)	1/ Тперез	$P_{перез2}$	V2:= 1
(V2=2)		1- $P_{перез2}$	V2:= 0
6. **«Перезавантаження МКП3»**			
(V3=2)	1/ Тперез	$P_{перез3}$	V3:= 1
(V3=2)		1- $P_{перез3}$	V3:= 0
7. **«Відмова системи електроживлення»**			
(V4=2)	$\lambda_{ПЕЖ}$	1	V4:= V5-1
8. **«Відмова фільтра Калмана»**			
(V5>0)	$\lambda_{ФК}$	1	V5:= V5-1
Умова критичної відмови:			

Умови та обставини	ФРІБП	ФРЙАП	ПМКВС
(((V1=0) AND (V2=0) AND (V3=0)) OR (V4=0))			

Модель обчислювальної системи навігаційно-обчислювальної підсистеми БпЛА у вигляді системи лінійних диференціальних рівнянь (1):

$$\left\{\begin{array}{l}
\frac{dP_1(t)}{dt} = -\left(\lambda_{мкп1}\cdot(1-P_{зб1})+\ldots+\lambda_{мкп2}\cdot P_{зб2}+\lambda_{мкп3}\cdot P_{зб3}+\lambda_{пеж}+\lambda_{ФК}\right)\cdot P_1(t)+\frac{P_3+P_7+P_{10}}{T_{ПЕРЕЗ}} \\
\frac{dP_2(t)}{dt} = -\left(\lambda_{мкп2}\cdot(1-P_{зб2})+\ldots+\lambda_{пеж}+\lambda_{ФК}\right)\cdot P_2(t)+\lambda_{мкп1}\cdot(1-P_{зб1})\cdot \mathrm{P}_1(t)+\frac{(1-P_{ПЕРЕЗ2})}{T_{ПЕРЕЗ}}\cdot \mathrm{P}_3(t)+\frac{P_{ПЕРЕЗ2}}{T_{ПЕРЕЗ}}\cdot \mathrm{P}_8(t)+\frac{P_{ПЕРЕЗ3}}{T_{ПЕРЕЗ}}\cdot \mathrm{P}_{11}(t) \\
\vdots \\
\frac{dP_{82}(t)}{dt} = -\left(\frac{P_{ПЕРЕЗ2}}{T_{ПЕРЕЗ}}+\frac{(1-P_{ПЕРЕЗ2})}{T_{ПЕРЕЗ}}+\lambda_{пеж}+\lambda_{мкп3}\cdot(1-P_{зб3})+\lambda_{мкп3}\cdot P_{зб3}\right)\cdot P_{42}(t)+\ldots+\lambda_{пеж}\cdot \mathrm{P}_{30}(t)+\lambda_{ФК}\cdot \mathrm{P}_{42}(t) \\
\vdots \\
\frac{dP_{161}(t)}{dt} = -\left(\frac{P_{ПЕРЕЗ2}}{T_{ПЕРЕЗ}}+\frac{(1-P_{ПЕРЕЗ2})}{T_{ПЕРЕЗ}}+\frac{P_{ПЕРЕЗ1}}{T_{ПЕРЕЗ}}+\frac{(1-P_{ПЕРЕЗ1})}{T_{ПЕРЕЗ}}+\lambda_{пеж}\right)\cdot P_{80}(t)+\ldots+\frac{(1-P_{ПЕРЕЗ3})}{T_{ПЕРЕЗ}}\cdot \mathrm{P}_{62}(t) \\
\frac{dP_{162}(t)}{dt} = -\left(\frac{P_{ПЕРЕЗ2}}{T_{ПЕРЕЗ}}+\frac{(1-P_{ПЕРЕЗ2})}{T_{ПЕРЕЗ}}+\frac{P_{ПЕРЕЗ1}}{T_{ПЕРЕЗ}}+\frac{(1-P_{ПЕРЕЗ1})}{T_{ПЕРЕЗ}}\right)\cdot P_{81}(t)+\ldots+\lambda_{мкп3}\cdot P_{зб3}\cdot \mathrm{P}_{77}(t)
\end{array}\right. \quad (1)$$

2.5 Отримання ймовірностей виникнення мінімальних січень обчислювальної підсистеми безпілотного літального апарата

Згідно пункту 4 запропонованої методики (п.2.3.2), знаходження мінімальних січень обчислюваної підсистеми БпЛА з графу відбувається шляхом порівняння кожного стану ГСП з умовою катастрофічної відмови, в результаті чого виділяються стани, в котрих настала відмова системи.

Отримавши МС необхідно знайти ймовірності їх виникнення. Ймовірності виникнення кожного з мінімальних січень отримуються шляхом формування виразів, які містять ймовірності перебування в станах, які входять до МС.

Наступним кроком є знаходження сумарної $Q_{сум}$ та загальної $Q_{заг}$ ймовірностей виникнення аварійної ситуації. Сумарна ймовірність виникнення аварійної ситуації визначається, як сума усіх МС, а загальна ймовірність виникнення аварійної ситуації рівна сумі ймовірностей перебування в станах, в котрих виникла аварійної ситуації.

Результати аналізу МС доцільно представляти у вигляді таблиці. В даній таблиці повинно бути: значення ймовірності МС; процентне відношення відповідного МС до сумарної ймовірності катастрофічної відмови $Q_{сум}$; непрацездатні елементи відповідного МС; кількість непрацездатних елементів у МС.

В результаті аналізу моделі обчислюваної підсистеми БпЛА з використанням мажоритарної структури, яка втрачає працездатність після критичної двох МКП було визначено, що ймовірність першого МС рівна q_1- $2{,}51 \cdot 10^{-6}$; другого q_2 - $1{,}48 \cdot 10^{-6}$ та третього q_3 - $1{,}72 \cdot 10^{-6}$; четвертого q_4 - $1{,}22 \cdot 10^{-6}$ та п'ятого q_5 - $2{,}79 \cdot 10^{-7}$ відповідно. Значення загальної ймовірності катастрофічної відмови $Q_{заг}$ - $5{,}52 \cdot 10^{-6}$. Середній час польоту становить $T_{сер}$ = 100 год. Результати аналізу представлені у вигляді табл.2.4

Таблиця 2.4

Мінімальні січення для ОП з використанням
мажоритарної структури котра працює за правилом “2 з 3”

Номер МС	Ймовірність виникнення МС	%	Кількість	Елемент
1	$2{,}51 \cdot 10^{-6}$	44,04	2	1, 2
2	$1{,}48 \cdot 10^{-6}$	25,96	2	1, 3
3	$1{,}72 \cdot 10^{-6}$	30,35	2	2, 3
4	$1{,}22 \cdot 10^{-6}$	21,40	1	4
5	$2{,}79 \cdot 10^{-7}$	4,89	1	5

Як видно з знайдених МС отримано комбінації відмов котрі в більшості випадків складаються з відмов двох елементів. Такі комбінації відмов показують, що підсистема є достатньо вразливою до відмов саме цих елементів. Тому, для зменшення ризику експлуатації БпЛА необхідно ввести резерування для цих елементів та створити у підсистемі можливість до реконфігурації.

Аналіз моделі обчислюваної підсистеми з дублюванням МКП показує, що ОП втрачає працездатність після відмови останього МКП. Для цих випадків визначено два МС. Ймовірність першого МС рівна q_1- $2{,}22 \cdot 10^{-6}$, другого q_2 - $1{,}22 \cdot 10^{-6}$, третього q_3 - $2{,}79 \cdot 10^{-7}$. Значення загальної ймовірності аварійної ситуації $Q_{заг}$ - $5{,}21 \cdot 10^{-6}$. Середній час напрацювання на відмову становить $T_{сер}$ = 100 год. Результати аналізу представлені у вигляді табл.2.5:

Таблиця 2.5

Мінімальні січення для ОП з використанням двохкратного резервування

Номер МС	Ймовірність виникнення МС	%	Кількість	Елементи
1	$3{,}72 \cdot 10^{-6}$	39,02	3	1, 2, 3
2	$1{,}22 \cdot 10^{-6}$	21,40	1	4
5	$2{,}79 \cdot 10^{-7}$	4,89	1	5

Слід відзначити, що модель системи з використання мажоритарної структури має менший ризик виникнення аварійної ситуації, оскільки отримані мінімальні січення мають в своєму складі більшу кількість елементів котрі повинні вийти з ладу для виникнення аварійної ситуації. Також слід відмітити, що система з використанням мажоритарної структури буде отримувати більш достовірну інформацію для можливості польоту, оскільки вона нечутлива до одиночних збоїв як апаратних так і програмних засобів.

В обох моделях найбільш вразливими є система електроживлення. Рекомендовано замінити підсистему електроживлення на таку, в якої інтенсивністю відмов є меншою у два рази ніж підсистема електроживлення, котра використовується на даний момент. Необхідно звернути увагу на високі вимоги щодо найдійності фільтра Калмана адже вихід з ладу даного модулю призводить до відмови усієї ОП. Кількісна оцінка введених рекомендацій в систему представлені в розділі 5.

2.6 Можливості розроблених моделей

В результаті моделювання ОП з використанням розробленої методики, було знайдено МС, які дозволяють не лише оцінити ризик експлуатації, але й модернізувати обчислювальну підсистему, в наслідок чого можна зменшити виникнення аварійних ситуацій шляхом введення додаткової надлишковості. Також слід відмітити, що використання технології [98] дозволяє швидко вводити зміни моделі пов'язані з введенням надлишковості в структуру даної відмовостійкої системи. Це дає можливість швидко проводити переоцінку значень мінімальних січень при модифікаціїї системи при багатоваріантному аналізі.

Ілюстрація вказаних можливостей моделі здійснена на прикладі отриманняя залежностей МС від часу, представлених на рис. 2.4 та 2.5.

При розробці моделі ОП навігаційно-обчислювальної системи БпЛА було використано наступні вхідні дані:

- $\lambda_{me1} = 7{,}46 \cdot 10^{-5}$ год$^{-1}$ – інтенсивність відмов МКП1;
- $\lambda_{me2} = 8{,}64 \cdot 10^{-5}$ год$^{-1}$ – інтенсивність відмов МКП2;
- $\lambda_{me3} = 5{,}05 \cdot 10^{-5}$ год$^{-1}$ – інтенсивність відмов МКП3;
- $P_{зб1} = 0{,}0151$ – ймовірність виникнення збою в МКП1;
- $P_{зб2} = 0{,}0132$ – ймовірність виникнення збою в МКП2;
- $P_{зб3} = 0{,}012$ – ймовірність виникнення збою в МКП3;
- $P_{пер1} = 0{,}995$ – ймовірність успішного перезавантаження МКП1;
- $P_{пер2} = 0{,}995$ – ймовірність успішного перезавантаження МКП2;
- $P_{пер3} = 0{,}984$ – ймовірність успішного перезавантаження МКП3;
- $\lambda_{ПЕЖ} = 7{,}6 \cdot 10^{-4}$– інтенсивність відмов підсистеми електроживлення;
- Тпз = 0,01 год - середнє значення інтервалу перезавантаження МКП.

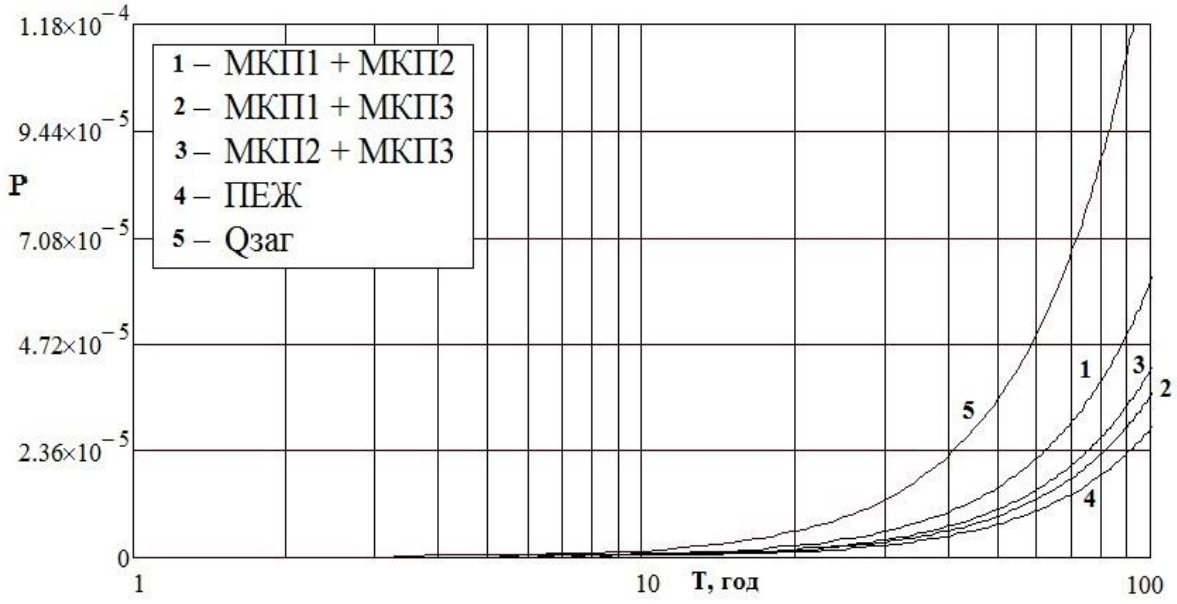

Рис. 2.4. Залежності ймовірності виникнення мінімальних січень для ОП з використанням мажоритарної структури, яка працює за правилом "2 з 3" в залежності від тривалості польоту

На рисунку 2.4 показано залежність ймовірності виникнення МС обчислювальної підсистеми, в які входять відмови: першого та другого мікропроцесорів (лінія 1); першого та третього мікропроцесорів (лінія 2); відмова другого та третього мікропроцесорів (лінія 3); відмова ПЕЖ (лінія 4), відмова ОП (лінія 5). Наведені залежності дозволяють визначати ймовірності виникнення мінімальних січень на заданому інтервалі експлуатації для подальшої оцінки ризику експлуатації за необхідності зміни тривалості

експлуатації.

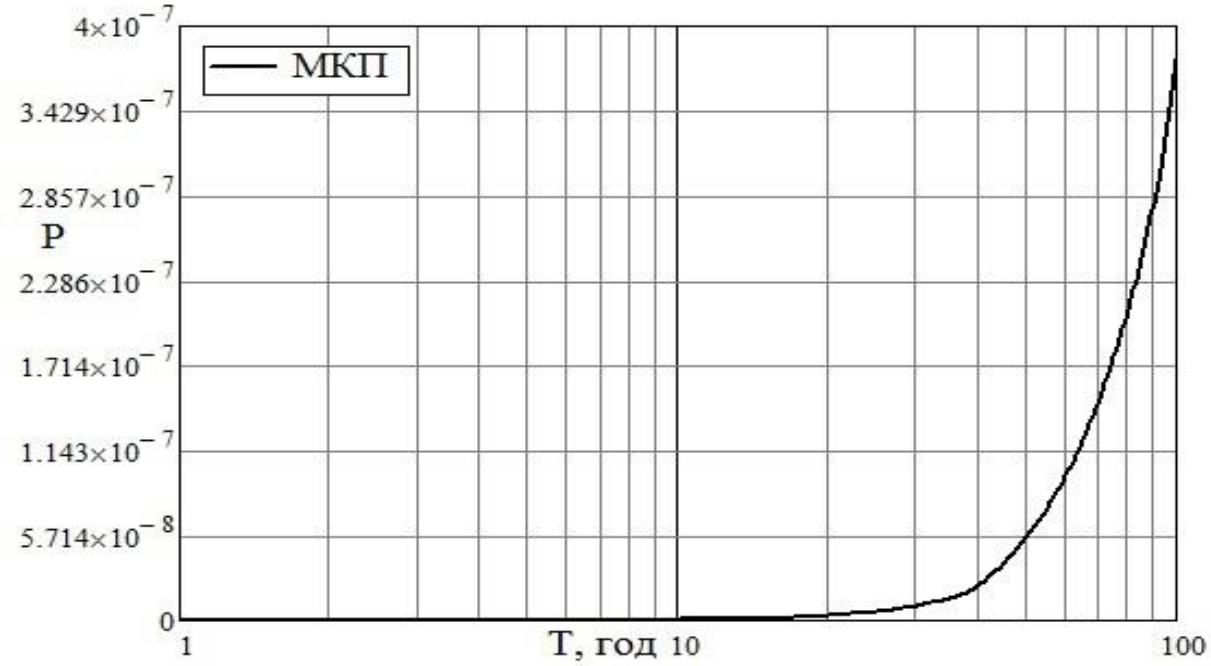

Рис. 2.5. Залежності ймовірності виникнення мінімальних січень для ОП з дублюванням МКП в залежності від тривалості польоту

2.7 Висновки

1. В результаті проведення досліджень встановлено, що для однозначної ідентифікації станів відмови необхідно модифікувати формалізоване представлення об’єкту дослідження у вигляді структурно-автоматної моделі. Таким чином подальший розвиток метод формалізованого представлення об’єкта дослідження у вигляді бінарної структурно-автоматної моделі. Така модель дає змогу отримати граф станів для оцінки ризику експлуатації навігаційно-обчислювальної підсистеми безпілотним літальним апаратом. Цей граф відображає усі можливі аварійні ситуації і дозволяє визначити мінімальні січення без побудови дерева відмов. Отримані мінімальні січення, сформовані із станів цього графа, на відміну від мінімальних січень, отриманих за допомогою дерева відмов, можуть входити в різні аварійні ситуації, що відповідає реальній статистичній картині експлуатації об'єкта дослідження і підвищує достовірність оцінки показника ризику експлуатації.

2. За допомогою модифікованого методу представлення об’єкту дослідження розроблено моделі обчислюваної підсистеми безпілотного літального апарата з використанням мажоритарної структури, яка працює за правилом "2 з 3" та з дублюванням мікпропроцесорів у вигляді бінарної структурно-автоматної моделі. В моделях відображено: мажоритарну структуру та відмови її мікропроцесорів; збої програмних засобів; можливість автоматичного перезавантаження мікропроцесорів після виявлення збою програмних засобів; ненадійність підсистеми електроживлення.

3. Для зменшення рівня ризику експлуатації навігаційно-обчислювальної системи безпілотним літальним апаратом в обчислювальній системі введений фільтр Калмана. Однак оскільки даний модуль увімкнений послідовно до трьох обчислювальних мікропроцесорів, то до даний модуль має мати інтенсивність відмови на два порядки меншу аніж мікропроцесори.

4. Особливістю розроблених моделей є те, що вони, на відміну від існуючих, дають змогу врахувати при оцінці ризику експлуатації базпілотного літального апарата вплив надійності апаратного забезпечення, перезавантаження програмного забезпечення у випадку виникнення збоїв мікропроцесорів та вплив підсистеми електроживлення. Врахування цих чинників дозволило визначити слабкі місця обчислювальної підсистеми.

5. Отримано мінімальні січення обчислюваної підсистеми з використанням мажоритарної структури, яка працює за правилом "2 з 3" та з дублюванням мікпропроцесорів. Отримані мінімальні січення, сформовані із станів цього графа, на відміну від мінімальних січень отриманих за допомогою дерева відмов, можуть входити в різні аварійні ситуації, що відповідає реальній статистичній картині експлуатації об’єкту дослідження і підвищує достовірність оцінки показника ризику експлуатації.

6. Побудовано залежності ймовірності виникнення мінімальних січень для обчислюваної підсистеми з використанням мажоритарної структури, яка працює за правилом "2 з 3" та з подвійним резервуванням мікпропроцесорів в залежності від тривалості експлуатації. В результаті дослідження залежностей

отриманих ймовірностей виникнення мінімальних січень підсистеми від часу показали, що найбільш вразливим місцем у двох варіантах реалізації обчислювальної підсистеми є система електроживлення. Також встановлено, що ризик виникнення аварійної ситуації експлуатації БпЛА при переході від нерезервованої обчислювальної підсистеми до мажоритарної структури зменшується на 33%.

7. Запропонована методика визначення кількісного показника ризику обчислювальної та навігаційної підсистем БпЛА, а саме ймовірності виникнення мінімального січення, без побудови дерева відмов. Методика дозволяє вирішувати задачі зменшення рівня ризику експлуатації навігаційно-обчислювальної підсистеми БпЛА на етапі системотехнічного проектування обчислювальної та навігаційної підсистем навігаційно-обчислювальної підсистеми безпілотним літальним апаратом. Це досягається шляхом оцінки ризику експлуатації багатьох варіантів побудови навігаційно-обчислювальної підсистеми БпЛА з врахуванням вартості їх реалізації. Розв’язання задачі зменшення оцінки ризику експлуатації здійснюється з меншими затратами часу, ніж вимагає методика оцінки ризику експлуатації з використанням дерева відмов, що важливо на етапі системотехнічного проектування.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ НАВІГАЦІЙНОЇ ПІДСИСТЕМИ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Як вже було сказано в розділі 1, крім обчислювальної підсистеми критичноною підсистемою навігаційно-обчислювальної системи БпЛА, з точки зору ризику експлуатації, є навігаційна підсистема. Призначення навігаційної підсистеми – функціональне резервування приймача сигналів від супутникової навігаційної системи. Вихід з ладу цієї підсистеми суттєво підвищує ризик експлуатації БпЛА, оскільки, навіть при відмові приймача супутникової навігаційної системи, БпЛА втрачає орієнтацію в просторі, що може призвести як до зіткнення з іншим літальним апаратом так і до некерованого польоту з подальшим падінням.

Тому на етапі системотехнічного проектування навігаційно-обчислювальної підсистеми БпЛА необхідно максимально зменшити ризик експлуатації навігаційної підсистеми після виходу з ладу її елементів шляхом вибору необхідного рівня надлишковості. Вирішення такої задачі потребує проведення багаторазової оцінки показників ризику в залежності від структури навігаційної підсистеми, кількості резерву, особливостей функціональної поведінки тощо. Таким чином необхідним є розробка моделі навігаційної підсистеми, яка з одного боку врахувує особливості підсистеми, а з іншого боку має високий рівнь формалізації з можливістю автоматизації процедур багатоваріантного аналізу.

3.1 Розробка математичної моделі навігаційної підсистеми безпілотного літального апарата

3.1.1 Перелік процедур, які визначають поведінку навігаційної підсистеми після відмов її складових.

На основі аналізу наслідків відмов елементів НП, проведеному в попередньому пункті, нижче сформовано перелік процедур, які будуть основою сукупності подій для побудови бінарної САМ .

Процедура 1. *Виявлення несправного функціонування акселерометрів*. Процедура виявлення несправних акселерометрів НП запускається за умови, якщо відмовив хоча б один акселерометрів.

Процедура 2. *Виявлення несправного функціонування гіроскопів*. Процедура виявлення несправних акселерометрів НП запускається за умови, якщо відмовив хоча б один акселерометрів.

Процедура 3. *Відновлення функціонування акселерометра*. Процедура відновлення несправного акселерометра НП запускається за умови, якщо виявлено його відмову та в наявності є резервний модуль відповідного акселерометра. Процедура відновлення окремого акселерометра може відбутись лише один за політ.

Процедура 4. *Відновлення функціонування гіроскопа*. Процедура відновлення несправного гіроскопа НП запускається за умови, якщо виявлено його відмову та в наявності є резерррвний модуль відповідного гіроскопа. Процедура відновлення окремого гіроскопа може відбутись лише один за політ.

Процедура 5. *Виявлення несправного функціонування системи повітряних сигналів*. Процедура виявлення несправності ВВШП відбувається за умови, якщо відмовив хоча б один датчиків.

Процедура 6. *Виявлення несправного магнітометра.* Дана процедура відбувається за умови, якщо відмовив магнітометр.

Процедура 7. *Виявлення несправного приймача СНС.* Дана процедура відбувається за умови, якщо відмовив сам приймач СНС.

Процедура 8. *Виявлення несправного приймача СЗО.* Дана процедура відбувається за умови, якщо відмовив сам приймач СЗО.

3.1.2 Розробка бінарної структурно-автоматної моделі навігаційної підсистеми безпілотного літального апарата.

На основі сформованого в п.3.1.1 переліку процедур складено перелік подій, котрі можуть відбуватись у навігаційні підсистемі. Події представлено парами, фіксуючи початок і закінчення відповідного часового інтервалу, який відповідає певному стану системи. Події обумовлені поведінкою системи, що відбуваються у ній представлено в табл. 3.1.1 Провівши аналіз подій представлених в таблиці, визначаються базові події.

Таблиця 3.1.1

Представлення пар подій, які фіксують початок і закінчення часового інтервалу перебування НП в певному стані

Пор. № пари подій	**Подія, яка фіксує початок події**	**Подія, яка фіксує закінчення**
1	«Початок роботи»	«Відмова акселерометра 1»
2	«Початок роботи»	«Відмова акселерометра 2»
3	«Початок роботи»	«Відмова акселерометра 3»
4	«Початок роботи»	«Відмова гіроскопа 1»
5	«Початок роботи»	«Відмова гіроскопа 2»
6	«Початок роботи»	«Відмова гіроскопа 3»
7	«Початок роботи»	«Відмова ВВШП»
8	«Початок роботи»	«Відмова магнітометра»
9	«Початок роботи»	«Відмова СНС»
10	«Початок роботи»	«Відмова СЗО»
11	«Відмова акселерометра 1»	«Перемикання на резервний модуль акселерометра 1»
12	«Перемикання на резервний модуль акселерометра 1»	«Відмова акселерометра 1»
13	«Відмова акселерометра 2»	«Перемикання на резервний модуль акселерометра 2»

Пор. № пари подій	Подія, яка фіксує початок події	Подія, яка фіксує закінчення
14	«Перемикання на резервний модуль акселерометра 2»	«Відмова акселерометра 2»
15	«Відмова акселерометра 3»	«Перемикання на резервний модуль акселерометра 3»
16	«Перемикання на резервний модуль акселерометра 3»	«Відмова акселерометра 3»
17	«Відмова гіроскопа 1»	«Перемикання на резервний модуль гіроскопа 1»
18	«Перемикання на резервний модуль гіроскопа 1»	«Відмова гіроскопа 1»
19	«Відмова гіроскопа 2»	«Перемикання на резервний модуль гіроскопа 2»
20	«Перемикання на резервний модуль гіроскопа 2»	«Відмова гіроскопа 2»
21	«Відмова гіроскопа 3»	«Перемикання на резервний модуль гіроскопа 3»
22	«Перемикання на резервний модуль гіроскопа 3»	«Відмова гіроскопа 3»

3.1.3 Визначення базових подій для бінарної структурно-автоматної моделі навігаційної підсистеми безпілотного літального апарата.

Незалежними базовими подіями у системі є: «Відмова акселерометра 1», «Відмова акселерометра 2», «Відмова акселерометра 3», «Відмова гіроскопа 1», «Відмова гіроскопа 2», «Відмова гіроскопа 3», «Відмова ВВШП», «Відмова СНС», «Відмова СЗО» та «Відмова магнітометра».

Згідно [100] для даної системи вибрано наступні базові події:

- **Базова подія 1** «Відмова акселерометра 1»;
- **Базова подія 2** «Відмова акселерометра 2»;
- **Базова подія 3** «Відмова акселерометра 3»;
- **Базова подія 4** «Відмова гіроскопа 1»;
- **Базова подія 5** «Відмова гіроскопа 2»;
- **Базова подія 6** «Відмова гіроскопа 3»;

- **Базова подія 7** «Відмова ВВШП»;
- **Базова подія 8** «Відмова магнітометра»;
- **Базова подія 9** «Відмова приймача сигналів від СНС»;
- **Базова подія 10** «Відмова приймача сигналів від СЗО»;

3.1.4 Допущення прийняті при розробці бінарної структурно-автоматної моделі навігаційнрї підсистеми безпілотного літального апарата

При розробці моделі було прийнято наступні допущення:

- Кожен окремий гіроскоп та акселерометр зарезервовані лише один раз такими ж відповідними гіроскопами та акселерометрами у ковзному резерві. Відновлення окремого гіроскопа або акселерометра може відбутись та лише один раз за політ БпЛА.
- Відновлення гіроскопа чи акселерометра після відмови основного модуля відбувається автоматично.
- Інтенсивність відмов резервних гіроскопів та акселерометрів є рівною інтесивностям основних гіроскопів та акселерометрів.
- Тривалість всіх процесів, які відбуваються в системі розподілені згідно експоненційного закону. Інтенсивності подій є сталими в часі величинами.
- Система повітряних сигналів вважається такою, що відмовила за умови, якщо відмови хоча б одного з давачів. Інтенсивність відмови ВВШП буде визначатись як сума інтенсивностей усіх чотирьох дававачів, оскільки вважається, що в аспекті надійності дані давачі увімкнені послідовно.
- В системі НП не передбачено автоматичного управління польотом, тому відсутність сигналу від навігаційно-обчислювальної підсистеми призводить до авіаційної події.
- Сигнал від СНС та від СЗО на борт БпЛА отримується постійно.

3.1.5 Параметри навігаційної підсистеми безпілотного літального апарата, які відображені в моделі

При формуванні моделі системи радіуправління НП її склад і окремі складові необхідно представити відповідними параметрами, а саме:

- $\lambda_а$ – інтенсивність відмов акселерометра;
- $\lambda_г$ – інтенсивність відмов гіроскопа;
- $\lambda_{ВВШП}$ – інтенсивність відмов системи вимірювачів висото-швидкісних параметрів;
- $\lambda_{мм}$ – інтенсивність відмов магнітометра;
- $\lambda_{СНС}$ – інтенсивність відмов приймача сигналів від супутникої навігаційної системи;
- $\lambda_{СЗО}$ – інтенсивність відмов приймача сигналів від системи зв'язку з оператором;

Інтенсивності відмов давачів усіх складових взято з технічної документації від повідного виробника. В разі неможливості отримання інформації було прийнято рішення використати інформацію згідно стандартів MILS - 217 [74].

3.1.6 Структура вектора стану навігаційної підсистеми безпілотного літального апарата.

Вектор стану навігаційно-обчислювальної підсистеми БпЛА представлений наступними компонентами:

V1 – відображає поточний стан гіроскопа 1 (початкове значення компоненти V1 дорівнює два N_1=2):

V1 = 2 - гіроскоп 1 працездатний, наявне відновлення;

V1 = 1 - гіроскоп 1 працездатний, відновлення відсутнє;

V1 = 0 - гіроскоп 1 відмовив, відновлення відсутнє.

V2 – відображає поточний стан гіроскопа 2 (початкове значення компоненти V2 дорівнює два N_2=2):

V2 = 2 - гіроскоп 2 працездатний, наявне відновлення;

V2 = 1 - гіроскоп 2 працездатний, відновлення відсутнє;

V2 = 0 - гіроскоп 2 відмовив, відновлення відсутнє.

V3 – відображає поточний стан гіроскопа 3 (початкове значення компоненти V3 дорівнює два $N_3 = 2$):

V3 = 2 - гіроскоп 1 працездатний, наявне відновлення;

V3 = 1 - гіроскоп 1 працездатний, відновлення відсутнє;

V3 = 0 - гіроскоп 1 відмовив, відновлення відсутнє.

V4 – відображає поточний стан акселерометра 1 (початкове значення компоненти V4 дорівнює два $N_4=2$):

V4 = 2 - акселерометр 1 працездатний, наявне відновлення;

V4 = 1 - акселерометр 1 працездатний, відновлення відсутнє;

V1 = 0 - акселерометр 1 відмовив, відновлення відсутнє.

V5 – відображає поточний стан акселерометра 2 (початкове значення компоненти V5 дорівнює два $N_5=2$):

V5 = 2 - акселерометр 1 працездатний, наявне відновлення;

V5 = 1 - акселерометр 1 працездатний, відновлення відсутнє;

V5 = 0 - акселерометр 1 відмовив, відновлення відсутнє.

V6 – відображає поточний стан акселерометра 3 (початкове значення компоненти V6 дорівнює два $N_6 = 2$):

V6 = 2 - акселерометр 1 працездатний, наявне відновлення;

V6 = 1 - акселерометр 1 працездатний, відновлення відсутнє;

V6 = 0 - акселерометр 1 відмовив, відновлення відсутнє.

V7 – відображає поточний стан ВВШП (початкове значення компоненти V7 дорівнює один $N_7 = 1$, якщо ВВШП відмовить то стан даного вектора стане рівним нулю $N_7= 0$);

V8 – відображає поточний стан магнітометра (початкове значення компоненти V8 дорівнює один $N_8 = 1$, якщо магнітометр відмовить то стан даного вектора стане рівним нулю $N_8= 0$);

V9 – відображає поточний стан СНС (початкове значення компоненти V9 дорівнює один $N_9 = 2$, якщо приймач сигналів від СНС відмовить то стан даного вектора стане рівним нулю $N_9= 0$);

V10 – відображає поточний стан СЗО (початкове значення компоненти V10 дорівнює один N_{10} = 1, якщо приймач сигналів від СЗО відмовить то стан даного вектора стане рівним нулю N_{10}= 0);

Розроблена бінарна структурно-автоматна модель навігаційних систем представлена в таблиці 3.1.6:

Таблиця 3.1.6

Структурно-автоматна модель навігаційної підсистеми БпЛА.

Умови та обставини	**ФРІБП**	**ФРЙАП**	**ПМКВС**
1. **Базова подія «Відмова гіроскопа 1 »**			
(V1>0)	$\lambda_г$	1	V1:= V1-1
2. **Базова подія «Відмова гіроскопа 2 »**			
(V2>0)	$\lambda_г$	1	V2:= V1-1
3. **Базова подія «Відмова гіроскопа 3 »**			
(V3>0)	$\lambda_г$	1	V3:= V1-1
4. **Базова подія «Відмова акселерометра 1 »**			
(V4>0)	$\lambda_а$	1	V4:= V1-1
5. **Базова подія «Відмова акселерометра 2 »**			
(V5>0)	$\lambda_а$	1	V5:= V1-1
6. **Базова подія «Відмова акселерометра 3 »**			
(V6>0)	$\lambda_а$	1	V6:= V1-1
7. **Базова подія «Відмова ВВШП»**			
(V7 = 1)	$\lambda_{НП}$	1	V7:= 0
8. **Базова подія «Відмова магнітометра»**			
(V8 = 1)	$\lambda_{ММ}$	1	V8:= 0
9. **Базова подія «Відсутній сигнал від СНС»**			
(V9 = 1)	$P_{СНС}$	1	V9:= 0
10.**Базова подія «Відсутній сигнал від СЗО»**			
(V10 = 1)	$P_{СЗО}$	1	V10:= 0
Умова критичної відмови:			
((((V1=0) OR (V2=0) OR (V3=0) AND ((V4=0) OR (V5=0) OR (V6=0)) AND (V7=0) AND (V8=0)) OR (V9=0) OR (V10=0))			

На основі розробленої бінарної структурно-автоматної моделі та програмного модуля ASNA здійснюється автоматизована побудова графа станів та переходів та відбувається формування математичної моделі у вигляді

системи диференційних рівнянь Колмогорова – Чепмена. На основі бінарної САМ та програмного модуля ASNA здійснено розробку математичної моделі у вигляді систем диференційних рівнянь (2), яка містить 998 рівнянь.

$$
\left\{
\begin{aligned}
&\frac{dP_1(t)}{dt} = -\left(\lambda_{г1}+\lambda_{г2}+\lambda_{г3}+\lambda_{a1}+\lambda_{a2}+\lambda_{a3}+\lambda_{вип}+\lambda_{мм}+\lambda_{снс}+\lambda_{сзо}\right)\cdot P_1(t)\\
&\frac{dP_2(t)}{dt} = -\left(\lambda_{г2}+\lambda_{г3}+\lambda_{a1}+\lambda_{a2}+\lambda_{a3}+\lambda_{вип}+\lambda_{мм}+\lambda_{снс}+\lambda_{сзо}\right)\cdot P_2(t)+\lambda_{г1}\cdot P_1(t)\\
&\frac{dP_3(t)}{dt} = -\left(\lambda_{г1}+\lambda_{г3}+\lambda_{a1}+\lambda_{a2}+\lambda_{a3}+\lambda_{вип}+\lambda_{мм}+\lambda_{снс}+\lambda_{сзо}\right)\cdot P_3(t)+\lambda_{г2}\cdot P_1(t)\\
&\vdots\\
&\frac{dP_{452}(t)}{dt} = -\left(\lambda_{г1}+\lambda_{г2}+\lambda_{снс}+\lambda_{сзо}\right)\cdot P_{452}(t)+\lambda_{г2}\cdot P_{358}(t)+\lambda_{a1}\cdot P_{459}(t)+\lambda_{a2}\cdot P_{432}(t)+\lambda_{a3}\cdot P_{421}(t)+\lambda_{вип}\cdot P_{516}(t)\\
&\frac{dP_{453}(t)}{dt} = -\left(\lambda_{г2}+\lambda_{г3}+\lambda_{вип}+\lambda_{сзо}\right)\cdot P_{453}(t)+\lambda_{г1}\cdot P_{397}(t)+\lambda_{a1}\cdot P_{299}(t)+\lambda_{a2}\cdot P_{489}(t)+\lambda_{a3}\cdot P_{498}(t)+\lambda_{сзо}\cdot P_{613}(t)\\
&\frac{dP_{454}(t)}{dt} = -\left(\lambda_{a2}+\lambda_{г3}+\lambda_{снс}+\lambda_{вип}\right)\cdot P_{454}(t)+\lambda_{a1}\cdot P_{412}(t)+\lambda_{г2}\cdot P_{458}(t)+\lambda_{г1}\cdot P_{327}(t)+\lambda_{a3}\cdot P_{457}(t)+\lambda_{сзо}\cdot P_{589}(t)\\
&\vdots\\
&\frac{dP_{996}(t)}{dt} = -\lambda_{снс}\cdot P_{996}(t)+\lambda_{г1}\cdot P_{799}(t)+\lambda_{г2}\cdot P_{853}(t)+\lambda_{г3}\cdot P_{794}(t)+\lambda_{a1}\cdot P_{885}(t)+\lambda_{a2}\cdot P_{869}(t)+\lambda_{a3}\cdot P_{957}(t)+\lambda_{вип}\cdot P_{984}(t)+\lambda_{мм}\cdot P_{994}(t)\\
&\frac{dP_{997}(t)}{dt} = \lambda_{г1}\cdot P_{899}(t)+\lambda_{г2}\cdot P_{751}(t)+\lambda_{г3}\cdot P_{897}(t)+\lambda_{a1}\cdot P_{755}(t)+\lambda_{a2}\cdot P_{851}(t)+\lambda_{a3}\cdot P_{921}(t)+\lambda_{вип}\cdot P_{954}(t)+\lambda_{мм}\cdot P_{756}(t)+\lambda_{снс}\cdot P_{691}(t)-\lambda_{сзо}\cdot P_{997}(t)\\
&\frac{dP_{998}(t)}{dt} = \lambda_{г1}\cdot P_{899}(t)+\lambda_{г2}\cdot P_{751}(t)+\lambda_{г3}\cdot P_{897}(t)+\lambda_{a1}\cdot P_{755}(t)+\lambda_{a2}\cdot P_{851}(t)+\lambda_{a3}\cdot P_{921}(t)+\lambda_{вип}\cdot P_{954}(t)+\lambda_{мм}\cdot P_{756}(t)+\lambda_{снс}\cdot P_{996}(t)+\lambda_{сзо}\cdot P_{997}(t)
\end{aligned}
\right\} \quad (2)
$$

3.1.7 Знаходження мінімальних січень моделі навігаційної підсистеми безпілотного літального апарата

Шляхом порівняння кожного стану ГСП з умовою катастрофічної відмови, згідно пункту 4 запропонованої методики (п.2.3.2), знаходження мінімальних січень навігаційної підсистем БпЛА з графу відбувається. В результаті чого виділяються стани, в котрих настала відмова системи.

Отримавши МС необхідно знайти ймовірності їх виникнення. Ймовірнісні виникнення кожного з мінімальних січень отримуються шляхом формування виразів, які містять ймовірності перебування в станах, які входять до МС.

Наступним кроком є знаходження сумарної $Q_{сум}$ та загальної $Q_{заг}$ ймовірностей аварійної ситуації. Сумарна ймовірність аварійної ситуації визначається, як сума усіх МС, а загальна ймовірність аварійної ситуації рівна сумі ймовірностей перебування в станах, в котрих настала аварійної ситуації.

В результаті аналізу моделі навігаційних підсистем системи радіуправління БпЛА, було отримано одинадцять МС. Значення загальної

ймовірності аварійної ситуації $Q_{заг}$ - 0,0302. Середній час польоту становить Т = 100 год.

Результати аналізу у вигляді табл.3.1.7:

Таблиця 3.1.7

Мінімальні січення навігаційної підсистеми БпЛА.

Номер МС	Ймовірність виникнення МС	%	Кількість	Елемент
1	$8{,}56\cdot10^{-3}$	28,3	4	1, 4, 7, 8
2	$8{,}56\cdot10^{-3}$	28,3	4	1, 5, 7, 8
3	$8{,}56\cdot10^{-3}$	28,3	4	1, 6, 7, 8
4	$8{,}56\cdot10^{-3}$	28,3	4	2, 4, 7, 8
5	$8{,}56\cdot10^{-3}$	28,3	4	2, 5, 7, 8
6	$8{,}56\cdot10^{-3}$	28,3	4	2, 6, 7, 8
7	$8{,}56\cdot10^{-3}$	28,3	4	3, 4, 7, 8
8	$8{,}56\cdot10^{-3}$	28,3	4	3, 5, 7, 8
9	$8{,}56\cdot10^{-3}$	28,3	4	3, 6, 7, 8
10	0,03	99,3	1	9
11	$8{,}98\cdot10^{-4}$	29,7	1	10

3.2 Побудова ймовірнісних значень мінімальних січень навігаційної підсистеми безпілотного літального апарата

При розробці моделі НП навігаційно-обчислювальної підсистеми БпЛА було використано наступні вхідні дані:

- $\lambda_а = 7{,}64\cdot10^{-5}$ год$^{-1}$ – інтенсивність відмов акселерометра;
- $\lambda_г = 2{,}34\cdot10^{-5}$год$^{-1}$ – інтенсивність відмов гіроскопа;
- $\lambda_{ВВШП} = 2{,}48\cdot10^{-2}$ год$^{-1}$ – інтенсивність відмов датчика повітряного тиску;
- $\lambda_{мм} = 1{,}38\cdot10^{-5}$год$^{-1}$ – інтенсивність відмов магнітометра;
- $\lambda_{СНС} = 3{,}63\cdot10^{-5}$ год$^{-1}$ інтенсивність відмов приймача супутнико-навігаційної системи;
- $\lambda_{СЗО} = 7{,}95\cdot10^{-6}$ год$^{-1}$ інтенсивність відмов приймача навігаційно-обчислювальної системи;;

Отримані МС навігаційних підсистем системи радіуправління БпЛА представлено на рисунку 3.5:

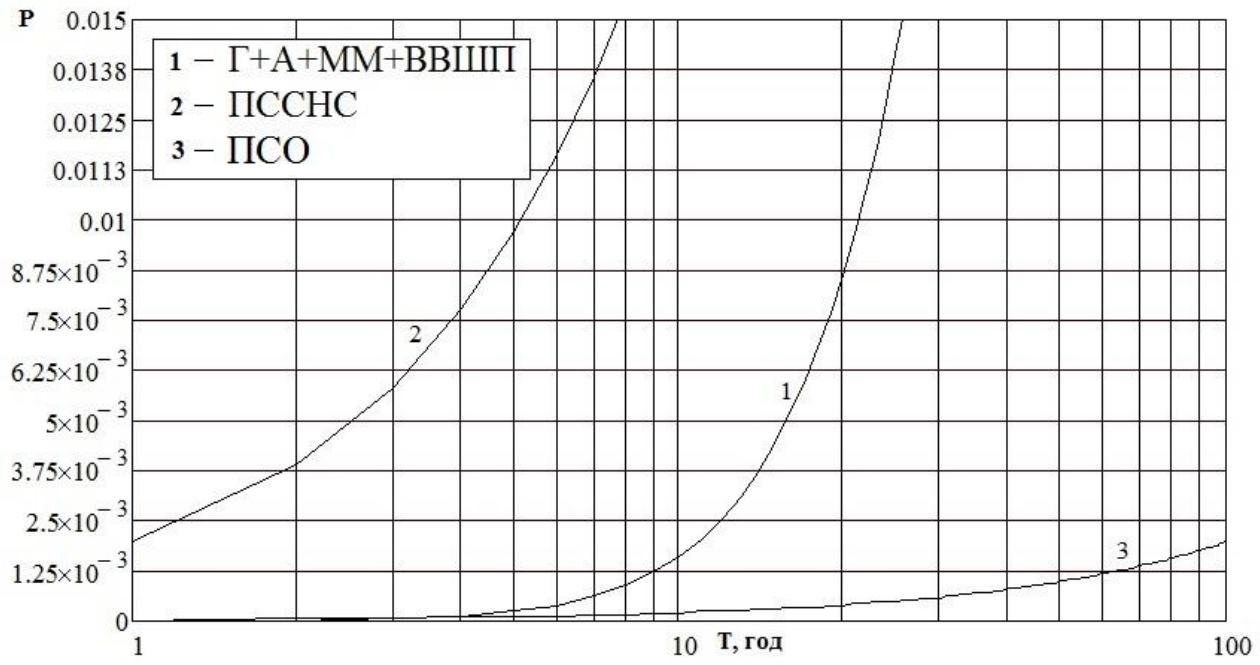

Рис. 3.2 Залежності ймовірності виникнення мінімальних січень для НП в залежності від тривалості польоту

На рисунку 3.2 показано показано залежність ймовірності виникнення МС навігаційної підсистеми, в які входять відмови: акселерометрів, гіроскопів, магнітометра та вимірювачів висотно-швидкісних параметрів (ВВШП) (лінія 1); відмова приймача сигналу від СНС (ПССНС) (лінія 2); відмова ПСО (лінія 3). Наведені залежності дозволяють визначати ймовірності виникнення мінімальних січень на заданому інтервалі експлуатації для подальшої оцінки ризику експлуатації за необхідності зміни тривалості експлуатації.

3.3 Висновки до розділу 3

В даному розіділі роботи розроблено математичну модель навігаційної підсистеми, яка складається з трьох акселерометрів, трьох гіроскопів, магнітометра та вимірювачів висотно-швидкісних параметрів. У моделі відображено: показники надійності дубльованих акселерометрів та гіроскопів; показники надійності магнітометра та вимірювачів висотно-швидкісних параметрів; ненадійність приймача сигналів від супутникової навігаційної системи та ненадійність приймача системи зв’язку безпілотного літального

апарата з оператором. Крім цього, враховано функціональне резервування супутникової навігаційної системи навігаційною підсистемою безпілотного літального апарата. Це забезпечило підвищення достовірності оцінки ризику експлуатації навігаційно-обчислювальної підсистеми безпілотним літальним апаратом, а саме виникнення аварійної ситуації через: ненадійність приймача сигналів від супутникової навігаційної системи; ненадійність приймача зв'язку з оператором.

Отримано мінімальні січення навігаційної підсистеми безпілотного літального апарата.

Побудовано залежності ймовірності виникнення мінімальних січень для навігаційної підсистеми в залежності від тривалості експлуатації. Отримані ймовірності виникнення мінімальні січення системи показали, що найбільш вразливим місцем у системі є приймач супутникової навігаційної системи.

В результаті отримання мінімальних січень обчислювальної системи та навігаційної підсистеми безпілотного літального апарата постала можливість проведення оцінки ризику експуатації навігаційно-обчислювальної підсистеми безпілотного літального апарата. Шляхом композиційного представлення сукупності мінімальних січень обидвох моделей, обчислювальної та навігаційної підсистем, стає можливим не лише проведення оцінки ризику експлуатації але й швидкого параметричного перебору варіантів реалізації двох підсистеми для можливості забезпечення заданого рівня ризику.

РОЗДІЛ 4. АВТОМАТИЗАЦІЯ ПРОЦЕДУР ОТРИМАННЯ ОЦІНКИ РИЗИКУ ЕКПЛУАТАЦІЇ НАВІГАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ ПІДСИСТЕМИ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

4.1 Алгоритм автоматизованого отримання мінімальних січень на основі структурно-автоматної моделі

Розроблена у другому розділі роботи, методика отримання МС передбачає ручну обробку ГСП. Якщо фазовий простір перевищує 20-30 стан, то дана методика втрачає ефективність через значні часові затрати на виконані запропонованих процедур. Тому, необхідно її формалізувати для подальшої автоматизації процедур оцінки ризику.

Для цього в даному розділі здійснено розробку алгоритму автоматизованого отримання МС. Вхідними даними для алгоритму є сукупність непрацездатних станів (січення системи), які отримуються за допомогою бінарної САМ. Для отримання масиву непрацездатних станів була розроблена спеціальна процедура, яка полягає в наступному: після генерації ГСП з використанням умови відмови необхідно повторити генерацію ГСП але вже без умови відмови. У першому випадку отримується масив усіх працездатних станів а після другої генерації - протір усіх можливих станів, які включають як працездатні так і непрацездатні стани об’єкта дослідження. Маючи масив усіх можливих станів та масив працездатних станів можна виділити масив непрацездатних станів, який і є розщепленим станом відмови. Розділити працездатні та непрацездатні стани можна за значенням відповідного компоненту ВС. Якщо елемент працездатний, то значення цього компонента ВС є більше нуля. Якщо елемент відмовив або призвів до аварійної ситуації, то відповідний компонент ВС буде рівним нулю.

При розробці алгоритму автоматизованого визначення МС прийнято наступні припущення:

- в системі існує хоча б одне мінімальне січення;

- січення системи (СС) - стан, в якому система перебуває в катастрофічній відмові.

- мінімальне січення системи - стан, в якому система перебуває в катастрофічній відмові, забравши хоча б одну з елементів котрі відмовили в даному січенні унеможливиться катастрофічна відмова системи в цілому.

Отримання МС відбувається у два етапи:

I етап - знаходження МС;

II етап - визначення ймовірнісних значень МС.

Кожен з етапівє сукупністю ряду процедур, які описано нижче.

Етап I. Знаходження МС відбувається з використанням наступних процедур:

- Сортування січень системи;

- Визначення МС.

Етап II. Отримання ймовірностей МС відбувається з використанням наступних процедур:

- Визначення МС у СС;

- Сумування ймовірностей МС;

- Формування масиву МС та їх ймовірнісних значень.

Для опису розробленого алгоритму прийнято наступні скорочення:

n - вказівник порядкового номера $МС_n$.

i, j - вказівники порядкового номера компонента ВС.

ЛСС - лічильник січень системи.

ЛЗЦ - лічильник зовнішнього циклу.

ЛВЦ - лічильник внутрішнього циклу.

ПКВС - постійна кількості компонентів вектора стану.

ЛКС - лічильник кількості січень системи.

ЛНСn - лічильник нулів січення; даний лічильник фіксує для МС з порядковим номером n кількість компонентів ВС, значення яких рівне нулю.

ЛМС - лічильник мінімальних січень.

МСС - масив січень системи.

ММС - масив мінімальних січень.

ОР - ознака рівності.

ОМС - ознака мінімального січення.

$ВС_n$[i] - значення ***i*** -го вектора стану січення системи з порядковим номером **n.**

4.1.1 Етап знаходження мінімальних січень

Першим етапом є етап знаходження МС. Для цього необхідно просортувати отриманий масив непрацездатних станів системи за ознакою наймешої кількості подій котрі призвели до аварійної ситуації системи. На основі просортованого масиву непрацездатних станів системи знаходять МС. В результаті отримується масив МС.

Першим кроком даного етапу є створення матриці, яка складатиметься з трьох стовбців - у першому стовбці вписується порядковий номер січення - N, в другий - записується через кому компонент ВС та його значення, у третій - значення лічильника нулів у січенні системи - тобто кількість нулів у відповідному січенні (**ЛНС**).

Процедура сортування МС

Процедура сортування виконується у два замкнутих між собою цикли - зовнішній та внутрішній, шляхом порівняння двох сусідніх січень системи, та передбачає виконання наступних кроків:

Початкові дані:

ЛЗЦ - лічильник зовнішнього циклу, якому присвоюється значення кількості січень системи.

ЛВЦ = (ЛЦЗ - 1).

n - вказівник порядкового номера січення системи.

(n+1) - вказівник наступнийого порядковим номера січення системи.

Крок 1. Вказівнику порядкового номера січення системи присвоюється **n = 1**; Вказівник наступного порядковим номера отримує значення **(n+1) = 2**, від лічильника зовнішнього циклу **ЛЗЦ** віднімається одиниця - **ЛЗЦ = ЛЦЗ -1**; Далі необхідно перевіряємо умову чи **ЛЗЦ** рівний нулю:

Якщо **ЛЗЦ = 0,** то процедура сортування СС вважається **закінченою**. В результаті даної процедури отримується матриця СС в якій є просортовані СС за кількітю компонент ВС значення яких рівне нулю. Тобто на початку будуть представлені стани з найменшою кількікісю наявних в собі компонент ВС значення яких рівне нулю.

Якщо **ЛЦЗ > 0,** то процедура сортування СС продовжується тому необхідно перейти до кроку 2.

Крок 2. В даному кроці відбувається порівняння відповідного лічильника січення системи $\mathbf{ЛНС_n}$ під номером **n** та лічильника $\mathbf{ЛНС_{(n+1)}}$ січення системи під номером **(n + 1).**

Якщо значення лічильника $\mathbf{ЛНС_n}$ січення системи під порядковим номером **n** *більше* значення лічильника $\mathbf{ЛНС_{(n+1)}}$ січення системи під порядковим номером **(n+1)** то ці СС необхідно поміняти місцями; Далі необхідно зменшити лічильник внутрішнього циклу **ЛВЦ = ЛВЦ -1** та перейти до кроку 3;

Примітка. У матриці січень системи порядкових номерів заміняти не потрібно, а лише замінити **СС** та їхні відповідні **ЛНС**.

Якщо значення лічильника $\mathbf{ЛНС_n}$ січення системи під порядковим номером **n** *менше чи рівне* значенню лічильника $\mathbf{ЛНС_{(n+1)}}$ січення системи під порядковим номером **(n+1)** то ці **СС** не міняються місцями; Далі необхідно зменшити лічильник внутрішнього циклу **ЛВЦ = ЛВЦ -1** та перейти до кроку 3;

Крок 3. В даному кроці необхідно збільшити на одинцю вказівник порядкового номера січення системи **n = n + 1** та наступний вказівник порядкового номера січення системи **(n+1) = (n+1) + 1.** Також потрібно перевірити чи значення лічильника внутрішніх циклів не стало рівним нулю:

Якщо **ЛВЦ > 0,** то це означає, що не усі сусідні СС були порівняні між собою, тому необхідно перейти до кроку 2;

Якщо **ЛВЧ = 0,** то це означає, що усі сусідні СС були порівняні між собою, тому необхідно перейти до кроку 1.

В результаті переміщення СС у матриці отримується просортована матриця січень системи. Сортування відбувалось по значенню кількостей нулів у січеннях. У першому рядку отриманої матриці буде січення системи з найменшою кількістю нулів.

Слід відзначити, що дана процедура є реалізованою як окрема функція, у програмному модулі CutSetDefiner.

Процедура визначення мінімальних січень.

Процедура визначення МС використовує наступні процедури: знаходження МС та порівняння СС. Процес знаходження МС відбувається у декілька залежних між собою циклів - загальний цикл знаходження МС та внутрішніх циклів процедури порівняння СС.

Вхідні дані:

ЛКС - присвоюється значення кількості січень системи;

ЛМС - лічильник МС присвоюється нулю **ЛМС = 0**;

j - вказівники порядкового компонента ВС;

n - вказівник порядкового номера $СС_n$;

ОР - ознака рівності;

ОМС - лічильник ознаки мінімального січення;

Крок 1. Вказівник порядкового номера СС отримує значення кількості січень системи мінус одиниця - **n = ПКВС** та необхідно перейти до кроку 2.

Крок 2. Вказівник порядкового компонента ВС отримує перше значення а лічильник ознаки мінімального січення отримує значення вказівника порядкового номера СС - **j** = 1; **ОМС** = **n.** Необхідно перейти до кроку 3.

Крок 3. На даному кроці необхідно використати процедуру порівняння СС (ППСС). Вхідними даними для якої будуть **n** - вказівник порядкового номера СС та **j** - вказівник порядкового компонента ВС**.** Після проведення ППСС необхідно перевірити ознаку рівності ОР:

Якщо після ППСС ознака рівності буде рівною нулю **ОР = 0,** то лічильник ознаки мінімального січення необхідно зменшити на одинцю **ОМС = ОМС - 1,** та перейти до кроку 4.

Якщо після ППСС ознака рівності буде не рівною нулю **ОР = 0,** то необхідно перейти до кроку 4.

Крок 4. Збільшивши вказівник порядкового компонента ВС вибирається наступний комопнет ВС **- j** = **j** +1; Але необхідно перевірити чи існує такий компонент ВС, для цього перевіряється умова:

Якщо **j** > **n** то необхідно перейти до кроку 5.

Якщо **j** ≤ n то необхідно перейти до кроку 3.

Крок 5. Даним кроком відбувається перевірка чи СС з порядковим номером **n** є мінімальним січенням. Це відбуваєтья перевіркою лічильника ознаки МС на рівність нулю.

Якщо **ОМС** = 0 то січення з порядковим номером **n** є мінімальним січенням системи. Січення з порядковим номером **n** потрібно записати в масив мінімальних січень **ММС**, та збільшити лічильник МС на одиницю **ЛМС** = **ЛМС** +1; далі потрібно перейти до кроку 6.

Якщо **ОМС** > 0 то необхідно перейти до кроку 6.

Крок 6. **n = n - 1;**

Якщо **n > 0** то потрібно перейти до кроку 2.

Якщо **n = 0** це значить, що усі січення первірені та було пройдено повністю процедури знаходження МС і усі мінімальні стани були знайдені. Процедура знаходження МС завершена.

Слід відзначити, що дана процедура є реалізованою як окрема функція, у програмному модулі CutSetDefiner.

Процедура порівняння станів системи

Вхідні дані:

ПКВС - присвоюється значення кількості векторів стану в системі.

ЛНС$_n$ - присвоюється кількості нулів компонент ВС у стані з порядковим номером **n.**

ВС$_n$[i] - значення і -го вектора стану січення системи з порядковим номером **n.**

$ВС_j$[i] - значення і -го вектора стану січення системи з порядковим номером **j.**

i = 1; Також вхідними даними є дані з процедури знаходження МС а саме **n** та **j.**

Крок 1. В даному кроці відбувається порівняння відповідних ВС двох січень системи.

Якщо **$ВС_n$[i]** рівний нулю **($ВС_n$[i] = 0)** та **$ВС_j$[i]** також рівний нулю **($ВС_j$[i] = 0)** то **$ЛНС_n$= $ЛНС_n$**-1; **i = i + 1;** далі необхідно перейти до кроку 2.

Якщо будь - яка з вищевказаних умов не виконуються то **i = i + 1;** далі необхідно перейти до кроку 2.

Крок 2. В даному кроці відбувається перевірка чи поточний номер ВС не став більшим за загальну кількість ВС у січенні.

Якщо i ≤ **ЛВС** то необхідно повернутись до кроку 1.

Якщо i > **ЛВС** то необхідно перейти до кроку 3.

Крок 3. В даному кроці відбувається присвоєння ознаці порівняння **ОР** певного значення.

Якщо **$ЛНС_n$** = 0 то **ОР** присвоюється 1.

Якщо **$ЛНС_n$** > 0 то **ОР** присвоюється 0.

На цьому кроці процедура порівняння СС закінчується.

Результатом даної процедури є повернення значення ознаки рівності **ОР** до процедури з якої її викликали.

На основі представленого алгоритму розроблено засоби, які реалізовані окремими функціями, що представляють предствалені процедури, у прототипі програмного модуля CutSetDefiner, програмний код якого приведено у Додатку А.

4.1.2. Знаходження ймовірнісних значень мінімальних січень системи.

Знаходження кількісних значень МС складається з двох етапів - перший це пошук станів в яких є МС, другий - сумування відповідних ймовірностей визначених станів системи.

Етап І. Процедура знаходження станів в яких знаходяться МС.

Згідно даного етапу необхідно створити матрицю, яка складається з чотирьох стовбців - у першому стовбці буде вписуватись порядковий номер МС - N, в другому - записується компонент ВС та його значення, у третю - будуть записуватись номери станів, в яких будуть присутні відповідні МС. У четвертому стовбці будуть записані отримані, в результаті виконання даної процедури, ймовірності МС. Також на даному етапі буде використовуватись процедура порівняння станів системи.

Вхідні дані:

Масив мінімальних січень.

Масив усіх станів системи, згенерований без умови відмови.

ЛМС - лічильник кількості мінімальних січень, які записані в масиві **ММС**.

ПКВС - постійна кількості кількість станів системи згенерованих без умови відмови.

Крок 1. Вказівнику порядкового номера МС - **j** присвоюється одиниця. Тобто вибирається перше МС з масиву мінімальних січень - **j = 1.**

Крок 2. Вказівнику порядкового номера СС - **n** присвоюється одиниця. Тобто вибирається перше МС з масиву усіх станів системи - **n = 1.**

*Крок 3.*Далі необхідно використати процедуру порівняння СС (ППСС). Вхідними даними для якої будуть **n** та **j.**

Якщо після ППСС ознака рівності буде рівною одиниці **ОР = 1,** то у ММС в третю колонку необхідно записати номер стану - **n** та перейти до кроку 4.

Якщо після ППСС ознака рівності буде рівною нулю - **ОР = 0,** то потрібно перейти до кроку 4.

Крок 4. Вказівник порядкового номера СС - **n** збільшується на одиницю - **n = n + 1;** Також необхідно первірити чи не зайшов даний вказівник за масив станів системи. Перевірка проводиться наступною умовою:

Якщо **n < ПКВС,** то даний вказівник не зайшов за масив станів системи, тому необхідно перейти до кроку 3.

Якщо **n ≥ ПКВС** тоді необхідно перейти до кроку 5.

Крок 5. Вказівник порядкового номера МС - **j** збільшується на одиницю **j = j + 1;** Також необхідно первірити чи не зайшов даний вказівник за масив МС. Перевірка проводиться наступною умовою:

Якщо **j** ≤ ЛМС, то даний вказівник не зайшов за масив станів системи, тому необхідно перейти до кроку 2.

Якщо **j** > ЛМС то процедура знаходження станів в яких є відповідні МС закінчена.

В результаті даної процедури заповнюється третій стовбчик ММС.

Етап ІІ. Отримання ймовірнісних значень МС

Процедура отримання ймовірнісних значень МС полягає сумуванні значень ймовірностей перебування у відповідних станах, номери яких були знайдені у попередній процедурі, тобто, у станах, котрі записані у третьому стовбці відповідного мінімального січення у матриці масиву МС. В результаті заповнюється четвертий стовбець відповідних МС значеннями їх ймовірностей відповідних МС.

4.2 Алгоритм автоматизованої побудови моделі БпЛА у вигляді дерева відмов на основі мінімальних січень

При оцінці ризику експлуатації РСВП для візуалізації аварійної ситуації є необхідним побудова дерева відмов. Це, з одного боку дозволить наглядно показати розгортання подій від аварійної ситуації і до причин її виникнення. З іншого боку, наявність дерева відмов дає змогу експертам верифікувати події, які призводять до аварійної ситуації. Крім цього дерево відмов є обов’язковим елементом при сертифікації РСВП.

Вхідними даними для побудови ДВ є масив МС. Згідно розробленого алгоритму розробник отримує логічну функцію, за допомогою якої відбувається побудова графічного представлення ДВ.

Автоматизована побудова ДВ виконується у два етапи. На першому етапі отримується логічна функція ДВ, шляхом послідовного перебору масиву МС.

На другому етапі, на основі отриманої логічної функції, відбувається побудова графічного представлення ДВ.

Слід відзначити, що побудоване графічне представлення ДВ є статичним, але ймовірнісні показники МС враховують динамічні процеси, котрі відбуваються в ТС.

За представленою методикою розроблено алгоритм, який будує логічну функцію ДВ і реалізований у пілотному програмному засобі.

4.2 .1 Алгоритм отримання логічної функції дерева відмов

В представленому алгоритмі реалізації першого етапу відбувається послідовний запис логічної функції дерева відмов.

Скорочення, які використовуються в описі алгоритму автоматизованої побудови ДВ:

n - вказівник порядкового номера МС.

i - вказівник порядкового номера компонента ВС.

j - лічильник компонентів ВС, значення яких рівна нулю.

ПКВС - постійна кількості компонентів вектора стану.

ЛНСn - лічильник нулів січення; даний лічильник фіксує для МС з порядковим номером n кількість компонентів ВС, значення яких рівне нулю.

ПКМС - постійна кількості МС.

ВСn[i] - значення i-го компонента вектора стану МС з порядковим номером n.

ФЛФ - форма логічної функції.

Крок 1. Беремо перше мінімальне січення. В (n) записується 1, а лічильник нулів січення (ЛНС1) першого МС фіксує кількість компонентів ВС, значення яких рівне нулю. Лічильник компонентів ВС (j) отримує значення кількості компонентів ВС, значення, які рівні нулю - j = ЛНС1.

Крок 2. Беремо перший компонент вектора стану першого МС системи - i = 1. У ФЛФ записується символ "(".

Крок 3. На цьому кроці потрібно визначити значення i-ого компонента

вектора стану МС з порядковим номером n (При першій ітерації - першого компонента ВС першого МС). При чому можливі два варіанти:

Якщо значення і-ого компонента вектора стану МС рівне нулю (ВСn[i] = 0), то в форму логічної функції (ФЛФ) записується значення вказівника поточного компонента ВС - V "i". Далі потрібно зменшити на одиницю стан лічильника компонентів ВС, значення яких рівне нулю - j = j-1 та перевірити чи j < 0;

Якщо j > 0, то це означає що в даному МС ще є наявні компоненти ВС, значення яких рівне нулю, тому в ФЛФ записуємо знак множення "·" та переходимо до кроку 4. Якщо j = 0, то це означає, що у даному МС більше немає компонентів ВС, значення яких рівне нулю, тому потрібно перейти до кроку 4.

Якщо значення і-ого компонента вектора стану МС більше нуля (ВСn[i] > 0), то потрібно перейти до кроку 4.

Крок 4. Збільшуємо вказівник компонента ВС (i) поточного МС з порядковим номером n на одиницю - i = i +1 та перевіряємо чи вказівник не зайшов за останнє значення компонентів ВС. Перевірка відбувається шляхом порівняння вказівника компонента ВС з значенням постійної компонентів вектора стану (ПКВС):

Якщо i ≤ ПКВС, то необхідно перейти до кроку 3.

Якщо i > ПКВС, то переходимо до кроку 5.

Крок 5. Збільшуємо вказівник МС n на одиницю - n = n+1. Тепер необхідно перевірити чи не перевищило поточне значення вказівника порядкового номера МС кількість МС. Перевірка проводиться шляхом порівняння поточного інкрементованого вказівника МС з постійною кількості МС (БПЛАМС):

Якщо n ≤ ПКВС, то в ФЛФ записується символ ")" та знак додавання "+" і необхідно перейти до кроку 2.

Якщо n > ПКВС, то в ФЛФ записуємо символи ");". На цьому кроці процедура запису логічної функції ДВ закінчена.

4.2.2 Алгоритм побудови графічного представлення дерева відмов

Крок 1. Першим кроком є побудова нижнього рівня ДВ. Для отримання графічного представлення ДВ, усі елементи, які є в дужках і між якими є знак множення "·", необхідно об'єднати логічними елементами AND так, щоб з кожної групи елементів між якими були знаки "·" мали по одному виходу. В результаті отримуємо нижній рівень ДВ. Після побудови нижнього рівня необхідно перейти до кроку 2.

Крок 2. Даним кроком формуються наступні рівні ДВ та вершинна подія. Для цього необхідно об'єднати усі виходи нижнього рівня ДВ, логічними елементами OR згідно з правилом об'єднання елементів. Таким чином отримується ДВ з однією подією найвищого рівня.

Правило об'єднання елементів: одним логічним елементом AND чи OR можна об'єднати лише два виходи з елементів нижнього рівня дерева.

Розроблений алгоритм, який автоматизовано будує логічну функцію ДВ є реалізованим у пілотному програмному засобі CutSetDefiner.

4.3 Врахування особливостей навігаційно-обчислювальної підсистеми безпілотним літальним апаратом в структурно-автоматної моделі

При побудові бінарної САМ необхідно враховувати наступні особливості навігаційно-обчислювальної підсистеми БпЛА: обмежений ремонт як окремих елементів так і підсистем, функціональну та надійнісну поведінку системи, простій системи та визначення подій котрі водять в різні аварійні ситуації подій.

Врахування *функціональної та надійнісної поведінки* об'єкту дослідження реалізується введенням компоненти ВС або окремо визначених значень компонента ВС, в яких однозначно визначено режим роботи елементу чи підсистеми та його працездатність.

Врахування *обмеженого ремонту* окремих елементів чи підсистем реалізується, шляхом введення у бінарну САМ компонента ВС - лічильника, який буде показувати кількість ремонтів окремого елементу чи підсистеми.

Тобто, коли елемент чи підсистема вийшла з ладу а значення лічильника ремонтів більше одиниці, то за таких умов з заданою ймовірністю відбувається ремонт елементу. При чому після ремонту значення даного лічильника зменшується на одиницю. За умови, що значення лічильника ремонтів буде рівне одиниці то це означатиме, що кількість обмежених ремонтів закінчилась.

Простій системи враховується станами, в яких елемент чи підсистема відмовила але для даного елементу чи підсистеми є наявні ремонти чи відповідний резерв що може виконуватись як під час польоту (реконфігурація мажоритарних підсистем систем) так і під час ремнотних робіт.

Можливість визначення подій котрі водять в різні аварійні ситуації в системі представлена простором усіх можливих варіантів перебування системи у різних станах.

4.4 Методика визначення кількісних показників ризику обчислювальної та навігаційної підсистем безпілотного літального апарата у вигляді мінімальних січень

Перший етап розробленої методики полягає у побудові бінарної САМ на основі інформації проведеного аналізу об’єкту дослідження. Розроблена САМ є вхідними даними для програмного засобу ASNA. Програмний засіб ASNA в автоматизованому режимі будує граф станів та переходів, формує та розв’язує систему диференційних рівнянь Колмогорова – Чепмена. В результаті розв’язку системи диференціальних рівнянь отримується масив усіх можливих станів перебування системи у працездатних і непраздатних станах. На основі отриманого масиву отримуються необхідні показники надійності.

Наступним етапом оцінки ризику є отримання мінімальних січень. Етап отримання отримання МС виконується в автоматизованому режимі за допомогою прототипу програмного модуля (ПМ) – CutSetDefiner, програмний код якого приведено у додатку Б.

Вхідними даними для даного ПМ є експортовані файли з програмного засобу ASNA – матриця вектору непрацездатних станів (*.vs) та матриця

інтенсивностей перебування системи в усіх станах (*.ds). В результаті роботи даного ПМ розробник отримує файл, в якому представлені усі мінімальні січення, їх ймовірності значення, процентні відношення МС відносно основної події в визначених моментах часу.

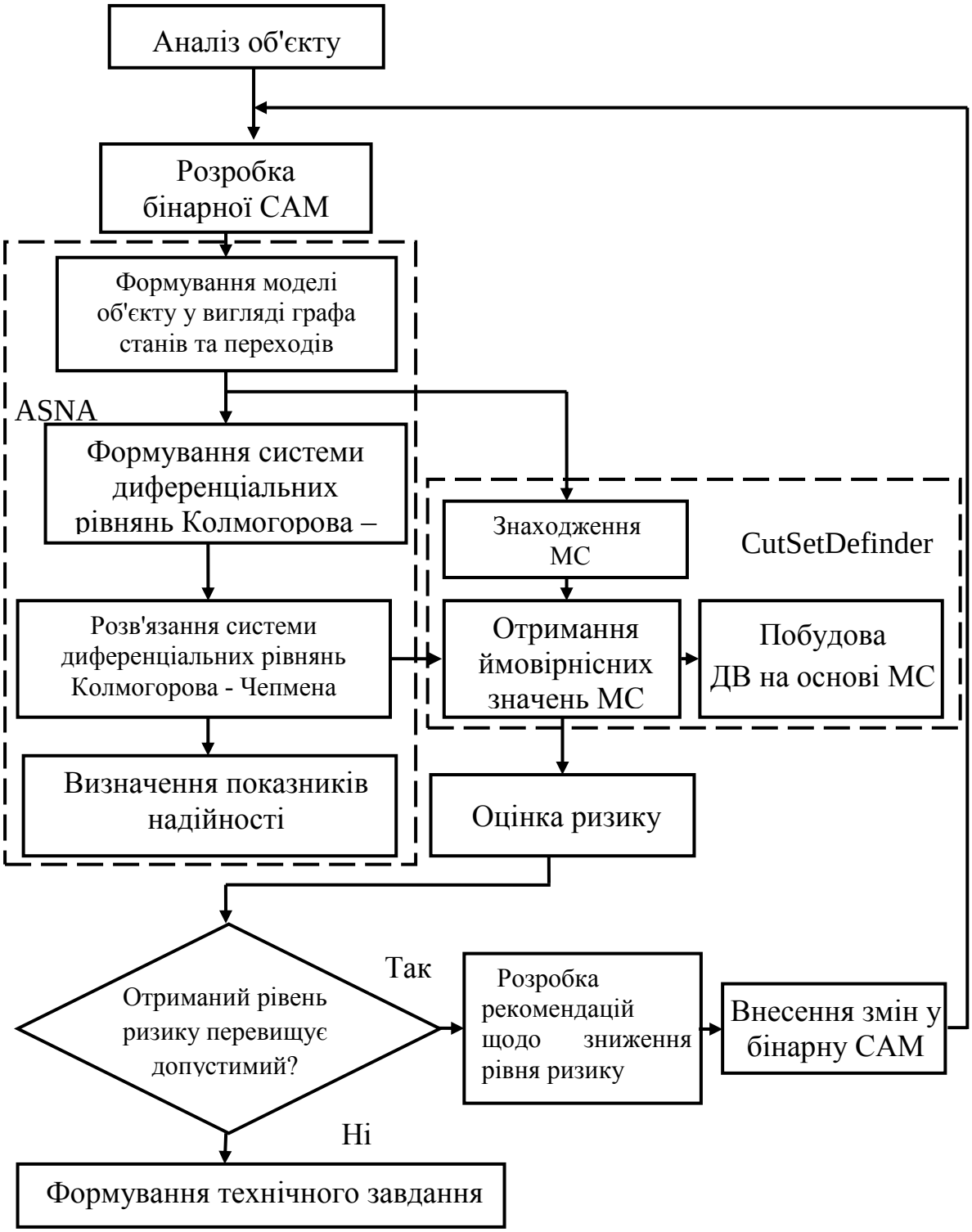

Рис. 4.1 Методика проведення оцінки ризику експлуатації системи радіоуправління БпЛА

Згідно стандартів для звітності по проведеному аналізі оцінки ризику

експлуатації [74] необхідно преставити дерево відмов об'єкту дослідження. Тому для цього, на основі отриманих МС за допомогою представленого алгоритму, який є реалізованим у прогрманому засобі CutSetDefiner, в автоматизованому режимі отримується логічне представлення дерева відмов. Логічне представлення відноситься до статичних ДВ.

За допомогою даних коефіцієнтів згідно таблиць представлених в додатку Б отримується рівень ризику. В данній таблиці рівень ризику має наступні рівні: низький, допустимий, високий та неприпустимий.

Проведення оцінки ризику відбувається згідно міжнародних стандартів [20, 74 - 77, 130] за допомогою технології аналізу видів відмов та їх наслідків (FMEA). Згідно даної технології для отиманих комбінацій відмов необхідно визначити який вплив дані комбінації відмов мають на функціонування об’єкту дослідження та до яких наслідків дані відмови можуть призвести.

Усі визначені на попередніх етапах відмови класифікуються за рівнем наслідків. Дана класифікація полягає у присвоєнню кожній відмові значення рівня наслідків, які можуть статись після настання відповідної відмови (значення від 1 - якщо наслідки є незначними і до 10 - за умови, що наслідки несуть за собою втрати серед населення та екологічні катастрофи). Таким чином отримується коефіцієнт значущості – Severity (S).

Після проведення класифікації по значущості наслідків, потрібно провести класифікацію ймовірностей виникнення отриманих відмов, що відбуваються у системі таким чином - якщо ймовірність виникнення є дуже високою то показнику виявлення присвоюється значення 10, у випадку якщо відмова виникає з низькою ймовірністю то даний коефіцієнт отримує значення 1. Таким чином отримується коефіцієнт ймовірності виникнення відмови – Occurence (O).

Після визначення рівня ризику необхідно визначити показник рівня ризику RPN (Risk Priority Number), для цього необхідно, окрім коефіцієнтів (O) та (S), визначити коефіцієнт ймовірності виявлення відмов – Detection (D). Даний коефіцієнт визначається наступним чином - якщо ймовірність виявлення є дуже

високою то показнику виявлення присвоюється значення 1, у випадку якщо відмову не можливо виявити то даний показник отримує значення 10.

На основі класифікованих факторів ризику розрахувати значення пріоритету ризику (RPN), яке визначається як добуток ймовірності винекнення, ймовірності виявлення відмови та серйозність (значущість) наслідків відмов.

За умови, якщо отриманий рівень ризику або значення пріоритету ризику перевищують допустимий рівень розробники створюють список рекомендацій, щодо його зниження. Однак, згідно традиційного стандарту [74 - 77], дані заходи підвищення безпечності не передбачають внесення змін у структуру та функціональну поведінку системи, і є заключенням експертів, що вносить суттєвий ступінь суб'єктивізму в оцінку рівня ризику. Такий підхід використовують через значні часові затрати при повторному виконанні FMEA/FMECA-аналізу. Тому, в значення пріоритету ризику, отримане таким чином, буде відрізняється від реального значення ризику, оскільки запропоновані експертами рішення не вносяться в модель системи і не перераховубться значення МС.

Запропонований підхід проведення оцінки ризику дозволяє швидко внести запропоновані зміни у структуру та поведінку системи та достатньо швидко перерахувати рівень ризику. Згідно даного підходу, після внесення змін у бінарну САМ, потрібно повторно знайти МС за допомогою програмного засобу CutSetDefinder та повторити процедуру оцінки ризику. За умови, якщо отриманий рівень ризику не буде перевищувати заданий то потрібно формувати технічне завдання для подвльшого етапу розробки об'єкту дослідження інакше потрібно робити зміни у бінарній САМ з врахуванням дій, щодо зменшення рівня ризику.

Для зниження ймовірності виникнення відмов компонентів системи потрібно ввести додаткову надлишковість, замінити компонент більш надійними або змінити режим роботи критичних компонентів для зменшення навантаження на них. Для зменшення наслідків відмов в систему вводяться інформаційно-керуючі системи, що виконують функцію відключення або

блокування об'єкту, у випадку загрози переходу його в аварійний стан або після настання аварійної ситуації. Усі дані заходи можливо реалізувати шляхом зміни вхідних даних бінарної САМ.

Для можливості проведення валідації отриманих комбінацій відмов системи можна побудувати дерево відмов та порівняти з побудованими ДВ отриманими з адопомогою інших відомих програмних засобів.

4. 5. Валідація підходу отримання мінімальних січень

Валідація підходу отримання МС проводилась на тестовому прикладі відмовостійкої відновлювальної системи, котра складається з п'яти модулів. Перший, другий та четвертий модулі виконують задану цільову функцію, а два інших модулі (третій та пятий) є резервними. Інтенсивність відмов усіх модулів є однаковою та рівною $\lambda = 0.05$ год$^{-1}$, інтенсивність відновлення $\mu = 0.1$ год$^{-1}$ а період дослідження становить 30 годин. Структурна схема надійності досліджуваної системи представлена на рисунку 4.2.

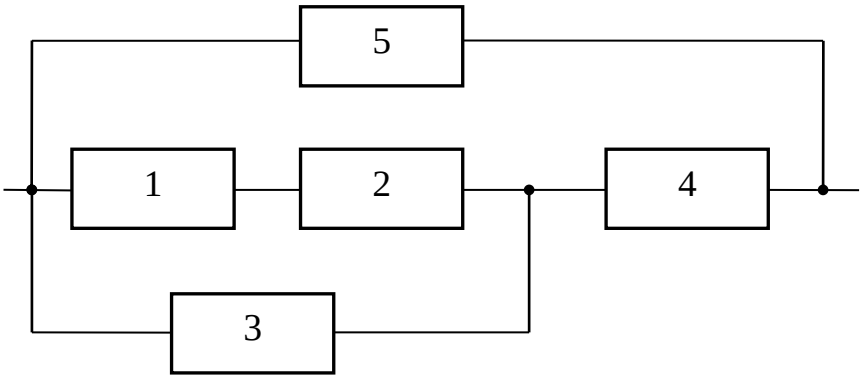

Рис.4.2. Структурна схема надійності досліджуваної системи

На основі структурної схеми надійності досліджуваної системи, за допомогою програмного засобу RAMCommander (A.L.D.), було побудовано дерево відмов, представлене на рисунку 4.3:

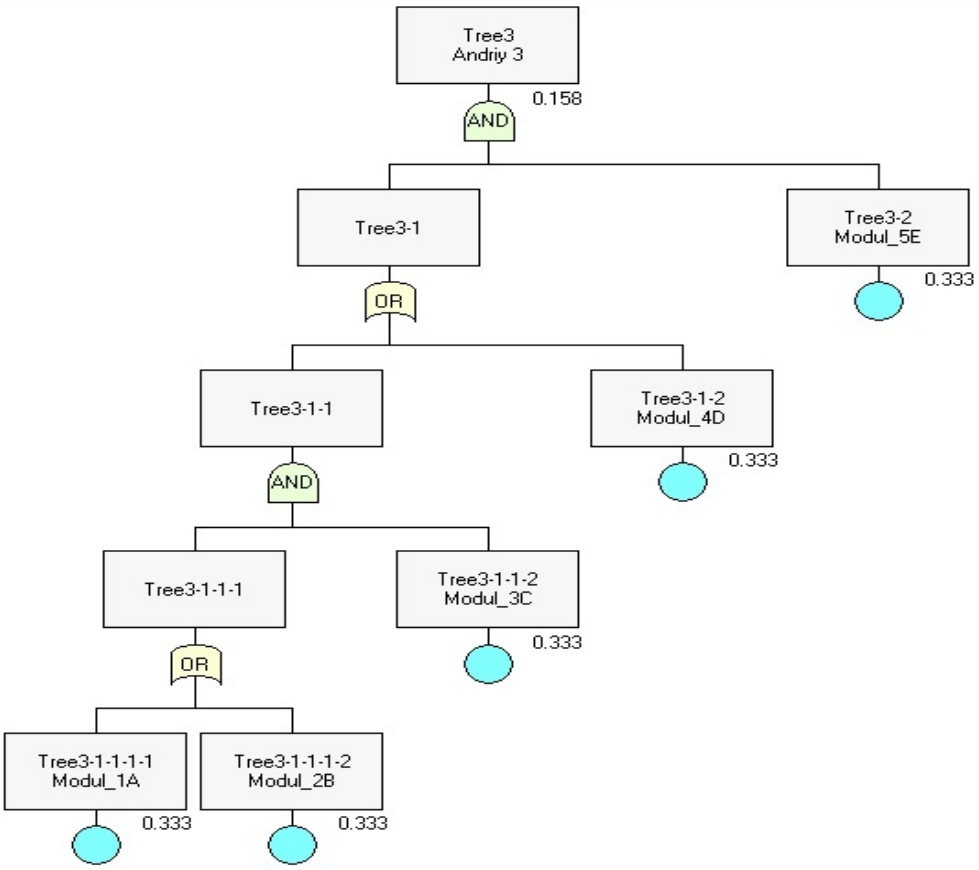

Рис.4.3. Дерево відмов отримане на основі досліджуваної системи за допомогою RAM Commander

На основі побудоваго ДВ отримано мінімальні січення системи. Для системи з безмежним ремонтом було отримано МС представлені в табл. 4.1. Загальна ймовірність відмови досліджуваної системи становить Qmean=0,158:

Таблиця 4.1

Мінімальні січення тестової відмовостійкої відновлюваної системи:

N	Q mean	%	Order	Event 1	Event 2	Event 3
1	0.111	60.0	2	Tree3-1-2	Tree3-2	
2	0.037	20.0	3	Tree3-1-1-1-2	Tree3-1-1-2	Tree3-2
3	0.037	20.0	3	Tree3-1-1-1-1	Tree3-1-1-2	Tree3-2

Для системи без відновлення було отримано МС представлені в табл. 4.2. Загальна ймовірність відмови досліджуваної системи становить Qmean=0,222993:

Таблиця 4.2

Мінімальні січення для тестової відмовостійкої системи без відновлення:

N	Ймов. МС	%	Order	Event 1	Event 2	Event 3
1	0.155	55.961629	2	Tree2-1-2	Tree2-2	
2	0.0609	22.019185	3	Tree2-1-1-1-2	Tree2-1-1-2	Tree2-2
3	0.0609	22.019185	3	Tree2-1-1-1-1	Tree2-1-1-2	Tree2-2

На основі цих самих вхідних даних було розроблено бінарну САМ тестової відмовостійкої системи, яка приведена в Додатку Б. За допомогою програмного забезпечення ASNA було отримано розподіл ймовірностей перебування системи у всіх можливих станах. За допомогою розробленого автором програмного засібу CSD, в автоматизованому режимі, було отримано мінімальні січення системи для тестової відмовостійкої системи з відновленням та без відновлення. Загальна ймовірність відмови тестової відмовостійкої системи без відновлення становить Qmean=0,502 а для системи з відновленням - Qmean=0,22 .

Порівняння отриманих результатів, отриманих стандартизованим методом за допомогою програмного засобу RAM Commander та розробленим підходом за допомогою програмного забезпечення CSD представлено в таблиці 4.3.

Таблиця 4.3

Порівняння отриманих МС за допомогою різних підходів

	RAM Commander		CSD		RAM Commander		CSD	
	Без ремонту				Безмежний ремонт			
N	Ймов. МС.	%	Ймов. МС.	%	Ймов. МС.	%	Ймов. МС.	%
1	0.36	45.45	0.357	45.86	0.102	60.0	0.109	61.0
2	0.216	27.27	0.218	27.12	0.033	20.0	0.032	19.5
3	0.216	27.27	0.218	27.12	0.033	20.0	0.32	19.5

Як видно з табл. 4.3, отримані значення МС збігаються, а отже валідація розробленого підходу пройшла успішно.

Однак, слід відмітити, що запропонований підхід дозволяє отримувати МС для систем з обмеженим відновленням в той час коли стандартизовані підходи працюють коректно лище у випадку необмеженого відновлення системи. Для ілюстрації цієї можливості були побудовані моделі тестової відмовостійкої системи з обмежним відновленням - два, шість та тридцять разів. Граф станів та переходів складався для цих трьох випадків з: 96-ти, 224-х та 992-х станів. У даних графах станів та переходів відповідно 33, 78 та 371 непрацездатний стан. Отримані значення МС для трьох варіантів системи представлено в табл. 4.4:

Таблиця 4.4

Мінімальні січення системи з обмеженим відновленням

		2 відновлення		6 відновлень		30 відновлень	
N	Елем.	Ймовірність	%	Ймовірність	%	Ймовірність	%
1	4,5	0,221	50,36	0,104	59,28	0,103	60,9
2	1,3,5	0,109	24,81	0,038	21,62	0,033	19,54
3	2,3,5	0,109	24,81	0,038	21,62	0,033	19,54

З табл. 4.4 та 4.3 видно, що при малій кількості відновлень (<10) значення як самих МС так і їх відсотковий вклад у аварійну ситуацію суттєво відрізняється від результатів, отриманих для випадку необмеженого відновлення. При рості кількості відновлень, в даному випадку до 30-ти, значення МС наближаються до значень, отриманих при необмеженоній кількості відновлень. Таким чином розроблений підхід у випадку обмеженої кількості відновлень працює правильно.

4.5 Висновки до розділу 4

1. В даному розділі представлена методика визначення кількісного показника ризику обчислювальної та навігаційної підсистем БпЛА, а саме ймовірності виникнення мінімального січення, без побудови дерева відмов.

Методика дозволяє вирішувати задачі зменшення рівня ризику експлуатації навігаційно-обчислювальної підсистеми БпЛА на етапі системотехнічного проектування обчислювальної та навігаційної підсистем. Це досягається шляхом оцінки ризику експлуатації багатьох варіантів побудови навігаційно-обчислювальної підсистеми БпЛА з врахуванням вартості їх реалізації. Розв’язання задачі зменшення рівня ризику експлуатації здійснюється з меншими затратами часу, ніж вимагає методика оцінки ризику експлуатації з використанням дерева відмов, що важливо на етапі системотехнічного проектування.

2. Розроблено алгоритм та прототип програмного засобу, в основу якого покладено запропоновану методику. Програмний засіб автоматизує процес отримання кількісного показника ризику, в якому враховуються: відмовостійкі конфігурації підсистем; відмови апаратних засобів; збої програмних засобів; належність певної частини відмов до двох і більше мінімальних січень; вплив ненадійності приймача сигналу від супутникової навігаційної системи; вплив ненадійності приймача зв’язку з оператором.

3. Розроблена методика розв'язання зворотної задачі, а саме побудова дерева відмов на основі мінімальних січень. Ступінь формалізації методики дав змогу розробити прототип програмного засобу для автоматизованої побудови дерева відмов. Практична необхідність отримання дерева відмов, після того як сформовані мінімальні січення в тому, що воно візуалізує шляхи потрапляння навігаційно-обчислювальної підсистеми у аварійні стани. Необхідно зауважити, що дерево відмов є обов'язковим атрибутом при здійсненні сертифікації на безпечність експлуатації безпілотного літального апарата.

4. Обидва розроблені алгоритми отримання мінімальних січень та побудови ДВ виконуються в автоматизованому режимі за допомогою програмного модуля – CutSetDefiner. Вхідними даними для даного прогрманого модулю є експортовані файли з програмного засобу ASNA – матриця вектору непрацездатних станів (*.vs) та матриця інтенсивностей перебування системи в усіх станах (*.ds). В результаті роботи даного прогрманого модулю розробник

отримує файл, в якому представлені усі мінімальні січення, їх ймовірності значення, процентні відношення мінімальних січень відносно основної події в визначених моментах часу та логічна функція дерева відмов.

5. Здійснено процедуру валідації запропонованого підходу автоматизованого отримання мінімальних січень. В якості об’єкта, на якому перевірялась методика, використана відмовостійка система з структурним резервуванням. Мінімальні січення, отримані за запропонованою методикою, порівнювались з мінімальними січеннями отриманими відомим способом з дерева відмов, яке було побудоване за допомогою програмного засобу RAM Commander. Визначені для відмовостійкої системи ймовірності виникнення мінімальних січень співпали, що підтверджує придатність методики до проведення дослідження ризику експлуатації радіоелектронних систем відповідального призначення. Але слід відзначити, що в порівнянні з відомою методикою отримання мінімальних січень за допомогою дерева відмов, запропонована методика дає можливість отримувати мінімальні січення для систем з обмеженою кількістю відновлень та систем з станом простою. Стан простою системи обумовлений проведенням технічного обслуговування та ремонту. Автоматизація двох процедур методики оцінки ризику експлуатації навігаційно-обчислювальної підсистеми БпЛА створила можливість кількісної перевірки рівня ризику з виявленням критичних елементів системи.

РОЗДІЛ 5. ОБГРУНТУВАННЯ ВИМОГ ДО НАДІЙНОСТІ СКЛАДОВИХ НАВІГАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ ПІДСИСТЕМИ ДЛЯ ЗМЕНШЕННЯ РИЗИКУ ЇЇ ЕКСПЛУАТАЦІЇ

В даному розділі проведена оцінка ризику експлуатації навігаційно-обчислювальної підсистеми БпЛА Futaba T14SG за допомогою розроблених моделей та засобів та продемонстровано можливості багатоваріантного аналізу у випадках зміни параметрів підсистем або часткової зміни стурктури цих підсистем.

Структурна схеми системи приведена на рис.5.1. Дана система складається з

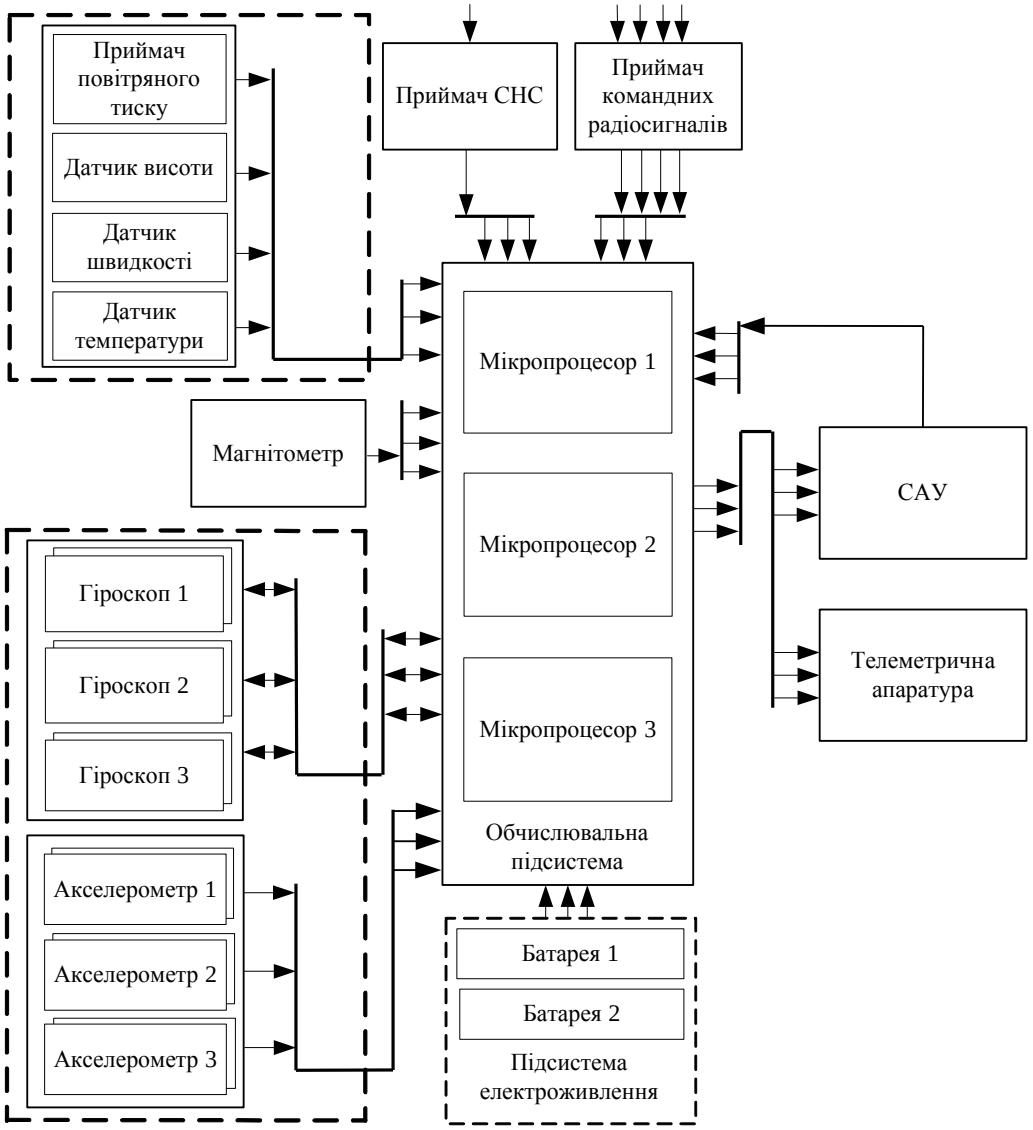

Рис.5.1 Структурна схеми підсистеми радіоуправління БпЛА

навігаційної підсистеми (НП), котра в свою чергу складається з трьох резервованих гіроскопів та трьох резервованих акселерометрів; приймача повітряного тиску; датчиків: висоти, температури, швидкості, котрі складають модуль вимірювачів висотно-швидкісних параметрів; магнітометра.

На вхід обчислювальної підсистеми (ОП) надходять керуючі сигнали від системи зв'язку з оператором та сигналі від супутникової навігаційної системи. До складу навігаційно-обчислювальної системи також відноситься підсистема електроживлення (ПЕЖ) котра складається з дубльованої батареї. Аналіз показав що НП, ВВШП та магнітометр в сукупності резервують приймач СНС.

Навігаційно-обчислювальна система досліджувалась на основі розроблених моделей обчислювальної підсистеми, модель представлена в розділі 2, та моделі навігаційної підсистеми котра представлена в розділі 3 за допомогою розробленого підходу отримання МС.

5.1 Аналіз відмов та можливих наслідків складових навігаційно-обчислювальної системи безпілотного літального апарата

Відмова *приймача повітряного тиску* (ППТ), який входить до складу ВВШП, може виникнути від механічного пошкодження трубки ППТ, попадання в отвори ППТ сторонніх предметів, накопичення в ППТ вологи (води) та її замерзання. В наслідок відмови ППТ система повітряних сигналів не буде визначати взагалі або визначати зі значними похибками дійсну повітряну швидкість і барометричну висоту.

В залежності від того, які камери ППТ несправні, можуть бути різні наслідки:

1) якщо камери статичного тиску несправні, то ВВШП (а саме, датчик барометричної висоти) не визначає взагалі або визначає зі значними похибками барометричну висоту БпЛА, тоді тільки за даними СНС коректно визначається цей параметр. У такому випадку БпЛА може продовжувати виконання завдання.

2) якщо камери динамічного тиску несправні, то ВВШП не визначає взагалі або визначає зі значними похибками дійсну повітряну швидкість БпЛА, тоді тільки за даними СНС коректно визначаються ці параметри і корекція НП здійснюється від СНС та магнітометра. У такому випадку БпЛА може продовжувати виконання завдання.

При умові справних СНС та надійному прийомі сигналів навігації відмова ППТ не буде впливати на успішність виконання завдання.

При відмові *датчика барометричної висоти* ВВШП не визначає взагалі або визначає зі значними похибками барометричну висоту БпЛА. За таких умов барометрична висота визначається лише за даними СНС. Безпілотний літальний апарат може продовжувати виконання завдання. Як правило, точність СНС щодо визначення барометричної висоти є кращою ніж ВВШП, тому відмова ДБВ не буде впливати на успішність виконання завдання, при умові справності СНС та надійного прийому сигналів навігації.

За умови відмови *датчика швидкості* ВВШП не визначає взагалі або визначає зі значними похибками дійсну повітряну швидкість БпЛА, тоді тільки за даними СНС визначаються ці параметри і корекція НП здійснюється від СНС та магнітометра. У такому випадку БпЛА може продовжувати виконання завдання.

Відмова датчика температури буде впливати на точність визначення навігаційних параметрів (висоти та швидкості) за допомогою ВВШП. Окрім інформативного призначення (для індикації температури середовища, у якому знаходиться БпЛА) даний датчик подає сигнал для обчислення похибок заміру параметрів ВВШП в обчислювальну систему з подальшим корегуванням цих параметрів.

Відмова одного з давачів ДШ, ДБВ, ДПТ, ДТ з точки надійності призведе до відмови ВВШП. Якщо відмовить *система повітряних сигналів* (ВВШП), то унеможливиться визначення або буде визначатись зі значними похибками дійсна повітряна швидкості та барометрична висота. Зазвичай дана система є менш точною від СНС. Вихід з ладу ВВШП, за умови справності СНС чи НП а

також справного магнітометра не буде впливати на успішність виконання польоту.

В НП присутні три гіроскопи. Кожен окремий гіроскоп зарезервований. За допомогою гіроскопа визначається кутове відхилення БпЛА щодо однієї з трьох опорних систем координат. Інформація з гіроскопа надходить у бортову цифрову обчислювальну систему, де інтегруються кінематичні рівняння параметрів орієнтації. Таким чином, відповідно, визначається кут або крену або тангажу або курсу. Відмова одного з гіроскопів, за умови що відмовить і його відповідний резервний модуль, призведе до відмови (некоректної роботи) всієї НП. В іншому випадку, це призведе до відмови відповідно одного із трьох каналів (крен або тангаж чи курс) НП.

При умові справності приймача СНС і надійного прийому сигналів навігації, а також справності ВВШП та магнітометра відмова НП не буде впливати на успішність виконання успішність виконання польоту.

Відмова усіх трьох підсистем гіроскопів призведе до відмови НП. за умови, що немає сигналу від супутника і несправна ВВШП безпілотний літальний апарат не може виконувати подальший політ.

Відсутність сигналу від відповідного *акселерометра* та його резервного модуля чи його значні невідповідності значень лінійного прискорення, вздовж однієї з трьох осей БпЛА, призведе до некоректного визначення швидкості БпЛА. Відмова одного з акселерометрів не буде впливати на успішність виконання завдання за умови справних приймача СНС, магнітометра та ВВШП. За умови відмови усіх трьох акселерометрів призведе то відмови НП або її некоректної роботи.

Відмова *магнітометра* призведе до відсутності магнітного курсу та відсутності індикації магнітного курсу БпЛА.

Ненадійний прийом сигналів супутників навігації або відмова приймача СНС призведе до відсутності корекції НП за сигналами СНС, збільшення (на порядок) похибок визначення навігаційних параметрів, таких як координати місцеположення, швидкості та кутів орієнтації БпЛА. Похибки визначення

навігаційних параметрів з часом будуть поступово наростати в основному через дрейф гіроскопів. До прикладу похибка визначення координат для НП виробництва російської компанії «ТеКнол» збільшується з 2 м (при справній СНС та надійному прийомі сигналу від супутника навігації) до 500 м за умови несправного приймача СНС або ненадійному прийомі сигналу від супутника навігації). Відмова СНС найімовірніше призведе до невиконання завдання через значні похибки у розв'язанні навігаційної задачі. Можливе продовження виконання завдання при умові реалізації ручого управління БпЛА.

Відмова *приймача сигналу від системи звязку з оператором* призведе до несправності ручного та напівавтоматичного каналів управління БпЛА.

Варіанти відмов одного або декількох мікропроцесорів обчислювальної системи БпЛА, в залежності від використання або невикористання мажоритарної структури, розглянуті в розділі 2. В залежності від структури, відмови *мікропроцесорів* можуть знижувати достовірність обробленої інформації або призводити до відмови *обчислювальної підсистеми*. Відмова ОП призводить до відмови БпЛА, що веде до авіаційної події.

Відмова однієї з *підсистем електроживлення* призведе до зменшення тривалості польота БпЛА. Відмова системи електроживлення призведе до відмови БпЛА та аварійної події БпЛА.

Аналіз показав що НП, ВВШП та магнітометр в сукупності резервують приймач сигналів від СНС.

Необхідно зауважити, що при необхідності проведення повтрої оцінки ризику експлуатації затрати часу в цьому випадку є суттєво меншими в порівнянні з затрами часу отримання МС за традиційною методикою, яка передбачає побудову дерева відмов. Згідно отриманих МС (див. табл. 2.4 для ОП та табл. 3.1.6 для НП) для оцінки ризику експлуатації навігаційно-обчислювальної системи БпЛА визначено наступні аварійні ситуації, які представлені в таблиці 5.1:

Таблиця 5.1.

Ймовірності виникнення аварійних ситуацій навігаційно-обчислювальної системи БпЛА

Аварійна ситуація	Ймовірність виникнення
Відмова МКП1 та МКП2	$2{,}51 \cdot 10^{-6}$
Відмова МКП1 та МКП3	$1{,}48 \cdot 10^{-6}$
Відмова МКП2 та МКП3	$1{,}72 \cdot 10^{-6}$
Відмова ПЕЖ	$2{,}79 \cdot 10^{-7}$
Відмова ММ, ВВШП, акслерометрів та гіроскопів	$8{,}56 \cdot 10^{-3}$
Відмова приймача сигналів від СНС	$3{,}03 \cdot 10^{-2}$
Відмова приймача сигналів від СЗО	$8{,}98 \cdot 10^{-4}$

Згідно процедури оцінки ризику експлуатації наступним етапом є визначення рівня ризику та значення пріоритету ризику для вищевказаних аварійних ситуацій.

5.2 Визначення рівня ризику експлуатації навігаційно-обчислювальної підсистеми безпілотного літального апарата

Згідно процедури [20] та [74] проведення оцінки ризику експлуатації виконується аналіз видів критичних відмов та їх наслідків. Для навігаційно-обчислювальної системи проаналізовано відмови окремих модулів та класифіковано наслідки їх відмов у п'ятирівневій градації.

Якщо наслідки відмови є значними (високий рівень значущості), то окремому виду відмови призначається перший рівень значущості і навпаки - якщо наслідки відмови є незначні, то такій відмові присвоюють п'ятий рівень значущості. Далі проводиться класифікація визначених відмов в залежності від ймовірності їх виникення. Якщо ймовірність є незначною то їй присвоюється рівень Е і якщо ймовірність є великою (більше 0,3) то такій ймовірності призначають рівень виникнення ймовірності А. Згідно даних ранжувань по таблиці 5.2.1 призначається рівень ризику для відповідного виду відмови.

Таблиця 5.2.1

Матриця критичності складових навігаційно-обчислювальної системи безпілотним літальним апаратом

Значущість події / Діапазон ймовірністей	I	II	III	IV	V
A	Допустимий	Високий	Неприйнятний	Неприйнятний	Неприйнятний
B	Допустимий	Високий	Високий	Неприйнятний	Неприйнятний
C	Низький	Допустимий	Високий	Високий	Неприйнятний
D	Низький	Допустимий	Допустимий	Високий	Високий
E	Низький	Низький	Допустимий	Допустимий	Високий

Рівні наслідків, згідно [74], проранжовано наступним чином:

Дуже незначний (I) - відмова не призводить до помітних наслідків.

Незначний (II) - відмова призводить до незначних наслідки, котрі помітні у системі але не мають впливу на функціонування системи.

Граничний (III) - відмова призводить до незначних змін у системі; система практично може виконувати цільову функцію.

Критичний (IV) - значні наслідки відмови призводять до втрати системою можливості виконання цільової функції але загрози безпеки для людей відмова не представляє.

Катастрофічний (V) - значні наслідки відмови призводять до втрати системою можливості виконання цільової функції та існує загроза небезпеки як навколишньому середовищу так і людям.

Згідно таблиці 5.1 усі знайдені аварійні ситуації мають категорію наслідків Критичний (IV) оскільки такі АС призводять до втрати системою можливості виконання цільової функції і призводять до падіння БпЛА. Категорія ймовірності АС визначалась у відповідності до отриманих значень ймовірності виникнення відповідної АС.

Таким чином для отриманих видів відмов обчислювальної підсистеми та навігаційної підсистем, було визначено наступні відповідні рівні ризику, котрі представлені в таблиці 5.2.2:

Таблиця 5.2.2

Рівень ризику для навігаційно-обчислювальної підсистеми БпЛА

	Вид відмови	Ймовірність виникення	Категорія виникення відмови	Категорія значущості відмови	Отриманий рівень ризику
1	Відмова МКП1 та МКП2	$2{,}51\cdot10^{-6}$	E	IV	Допустимий
2	Відмова МКП1 та МКП3	$1{,}48\cdot10^{-6}$	E	IV	Допустимий
3	Відмова МКП2 та МКП3	$1{,}72\cdot10^{-6}$	E	IV	Допустимий
4	Відмова ПЕЖ	$2{,}79\cdot10^{-7}$	E	IV	Допустимий
5	Відмова ММ, ВВШП, акслерометрів та гіроскопів	$8{,}56\cdot10^{-3}$	D	IV	Високий
6	Відмова приймача сигналів від СНС	$3{,}03\cdot10^{-2}$	B	IV	Неприйнятний
7	Відмова приймача сигналів від СЗО	$8{,}98\cdot10^{-4}$	E	IV	Допустимий

Як видно з табл. 5.2.2 рівень ризику відмови магнітометра, ВВШП, акслерометрів та гіроскопів є “високий” а відмова приймача сигналів від СНС є “неприйнятний”. Усі інші АС мають рівень ризику допустимий. Тому, необхідно напрацювати ряд проектних рішень для зменшення отриманого рівня ризику для АС - відмови ММ, ВВШП, акслерометрів та гіроскопів та відмова приймача сигналів від СНС.

Для зменшення рівня ризику магнітометра, ВВШП, акслерометрів та гіроскопів було рекомендовано замінити магнітометр та ВВШП з меншою на порядок інтенсивністю відмови - $\lambda_{мм} = 1{,}38\cdot10^{-4}$ год, $\lambda_{ВВШП} = 2{,}48\cdot10^{-3}$ год$^{-1}$ відповідно.

Також слід зменшити рівень ризику експлуатації для приймача СНС. Рекомендовано замінити модуль приймача СНС з інтенсивностю відмов $\lambda_{СНС} = 3{,}63\cdot10^{-5}$ год$^{-1}$ на модуль з інтенсивностю відмов на порядок нижче - $\lambda_{СНС} = 3{,}63\cdot10^{-6}$ год$^{-1}$.

Згідно експертної оцінки такі рекомендації знизять рівень ризику до допустимого. Для таких умов отриманий рівень ризику буде відповідати нормам експлуатації.

5.3 Визначення значення пріоритету рівня ризику навігаційно-обчислювальної системи безпілотного літального апарата.

Визначення рівня ризику експлуатації проводиться за допомогою аналізу видів відмов, наслідків та причин їх виникнення згідно [20, 72 - 75, 122]. Визначення видів відмов виконується наступним методом: для кожного компоненту чи підсистеми, який аналізується, створюється таблиця усіх можливих відмов. Для компонентів існують списки видів відмов, які є стандартизованими і представленими в базах даних. В базах цих даних представлено усі можливі види відмов для конкретних елементів а також процентне співвідношення усіх видів відмов.

За допомогою даного аналізу визначено значення пріоритету ризику кожного виду відмови. Визначення значення пріоритету ризику полягало у присвоєнні кожному виду відмови значення факторів ризику, в залежності від наслідків, які можуть статись після відмови. Згідно стандарту присвоюється значення пріоритету від 1 до 10: нижня межа 1, якщо наслідки є незначними; верхня межа 10 за умови, що наслідки несуть за собою втрати серед населення та екологічні катастрофи. Проведено класифікацію можливості виявлення відмов, що відбуваються у системі, і присвоєно значення показника виявлення. Якщо ймовірність виявлення є дуже високою, то показнику виявлення присвоюється значення 1 (нижня межа). У випадку якщо відмову не можливо виявити, то даний показник отримує значення 10 (верхня межа). Наступним кроком було класифіковано усі представлені відмови по значенню ймовірності їх виникнення на (1 – малоймовірні відмови та 10 відмови з дуже великою ймовірністю виникнення). Ймовірності виникнення АС класифікуються згідно діапазонів котрі представлені в Додатку Б.

На основі класифікованих факторів ризику розраховано значення пріоритету ризику, яке визначається як добуток ймовірності виникнення відмови, ймовірності виявлення відмови та серйозність (значущість) наслідків відмови. Умовою перевищення допустимого значення пріоритету ризику є значення 60. Після визначення видів відмов необхідно класифікувати усі представлені відмови по значенню ймовірності їх виникнення або по частоті виникнення та записати усі необхідні дані у результуючу таблицю.

Запропонована в дисертаційній роботі методика проведення оцінки ризику дозволяє в автоматизованому режимі отримати МС після врахування запропонованих рекомендацій щодо зниження рівня ризику. Після чого FMEA - аналіз проводиться ще один раз шляхом введення відповідних змін у бінарну САМ. Далі була проведена повторна процедура оцінки ризику з врахованими змінами у системі для кількісного обгрунтування та перевірки чи дійсно дані заходи зможуть знизити рівень ризику.

Для зниження ймовірності виникнення відмов компонентів системи потрібно ввести додаткову надлишковість, замінити компонент більш надійними або змінити режим роботи критичних компонентів для зменшення навантаження на них. Для зменшення наслідків відмов в систему вводяться інформаційно-керуючі системи, що виконують функцію відключення або блокування об'єкту, у випадку загрози переходу його в аварійний стан або після настання аварійної ситуації. Усі дані заходи можливо реалізувати шляхом зміни вхідних даних бінарної САМ.

За допомогою аналізу згідно стандарту [74] було отримано таблицю, в якій предствлено проранговані можливі відмови модулів та підсистем навігаційно-обчислювальної системи БпЛА.

Таблиця 5.3

Таблиця визначення значення пріоритету ризику навігаційно-обчислювальної системи БпЛА

Назва системи	Потенційна відмова	SEV	Потенційні наслідки	OCC	Система виявлення	DEC	RPN
А та Г	Відмова одного з гіросокпів	3	Відмова одного із каналів НП (крен, тангаж чи курс)	3	МКП	3	27
	Відмова усіх трьох гіросокпів	4	Відмова А та Г	2	МКП	2	16
	Відмова одного з акселерометрів	3	Значні невідповідності значень лінійного прискорення, вздовж однієї з трьох осей БпЛА	3	МКП	3	27
	Відмова усіх трьох акселерометрів	4	Відмова Н А та Г	2	МКП	2	16
ВВШП	Відмова ДТ	2	ВВШП не індикує температури середовища, у якому знаходиться БпЛА	4	МКП	3	24
	Відмова ДПТ	2	ВВШП не визначає взагалі або визначає зі значними похибками барометричну висоту БпЛА	4	МКП	3	24
	Відмова ДБВ	2	ВВШП не визначає взагалі або визначає зі значними похибками барометричну висоту БпЛА	4	МКП	3	24
	Відмова ДШ	2	ВВШП не визначає взагалі або визначає зі значними похибками дійсну повітряну швидкість БпЛА	4	МКП	3	24

ПССНС	Відмова приймача сигналів СНС	9	Відсутность корекції НП за сигналами СНС, одноразового збільшення (у декілька разів) похибок визначення навігаційних параметрів (координат місцеположення, швидкості та кутів орієнтації БпЛА).	4	МКП	2	72
ПССЗО	Відмова приймача сигналів від СЗО	8	Несправність ручного та напівавтоматичного каналів управління БпЛА	2	МКП	1	16
МКП	Відмова одного МПК	6	Погіршення достовірності отримання інформації	3	Детектор несправності МКП	2	36
	Відмова двох МКП	9	Відмова ОП	2	Детектор несправності МКП	2	36
	Відмова трьох МКП	9	Відмова ОП	2	Детектор несправності МКП	2	36
	Відмова ФК	9	Аварійна ситуація	2		2	36
ПЕЖ	Відмова однієї батареї	5	Зменшення тривалості польоту БпЛА	2	МКП	2	20
	Відмова двох батарей	9	Відмова ПЕЖ	3	МКП	3	81

Згідно процедур [74-77] АС значення пріоритету ризику якого є більші за 60 пунктів вважаються критичними. Тому необхідно напрацювати рекомендації щодо зниження показника рівня ризику для даної підсистеми.

Слід зменшити рівень ризику експлуатації для приймача СНС. Рекомендовано замінити модуль приймача СНС з інтенсивностю відмов $\lambda_{СНС}$ = 3,63 $\cdot 10^{-5}$ год$^{-1}$ на модуль з інтенсивностю відмов на порядок нижче - $\lambda_{СНС}$ = 3,63 $\cdot 10^{-6}$ год$^{-1}$. Однак даний приймач повинен не перевищувати масо габаритні параметри попередньо використовуваного приймача. Таким чином значення пріоритету ризику відмови приймача знижено з 9·4·2 = 72 пунктів до 9·3·2 = 54 пунктів.

Згідно рекомендацій експертів, а саме заміна модулів підсистеми електроживлення на такі інтенсивність відмови яких, є в два рази меншою від використовуваних та введення резервної батареї. Необхідно ввести резервні модулі з наступною умовою - резервна батарея ПЕЖ буде легшою та менш габаритною ніж основні батареї підсистеми. Таким чином значення пріоритету ризику буде знижено з 9·3·3 = 81 пунктів до 9·1·3 = 27 пунктів.

5.4 Проведення повторної оцінки ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата для кількісного підтвердження рекомендацій із зменшення рівня ризику

До моделі ОП, у вигляді САМ, необхідно ввести окремий вектор стану котрий буде відповідати за резервний модуль системи електроживлення. Значення даного ВС рівне одиниці. Таким чином у вербальній моделі з'явиться нова базова подія "відмова резервної батареї підсистеми електроживлення". Також необхідно замінити інтенсивність відмов підсистем електроживлення на менші значення, відповідними значеннями більш надійніших. Змінена бінарна САМ, представлена в табл. 5.4.1:

Таблиця 5.4.1

Структурно-автоматна модель обчислюваної системи БпЛА з внесенням змін.

Умови та обставини	ФРІБП	ФРЙАП	ПМКВС
1. **Базова подія «Відмова МКП №1»**			
(V1=2)	$\lambda_{МКП1}$	1 - $P_{зб1}$	V1:= 0
(V1=2)		$P_{зб1}$	V1:= 1
2. **Базова подія «Відмова МКП №2»**			
(V2=2)	$\lambda_{МКП2}$	1 - $P_{зб2}$	V2:= 0
(V2=2)		$P_{зб2}$	V2:= 1
3. **Базова подія «Відмова МКП №3»**			
(V3=2)	$\lambda_{МКП3}$	1 - $P_{зб3}$	V3:= 0
(V3=2)		$P_{зб3}$	V3:= 1
4. **«Перезавантаження МКП1»**			
(V1=1)	1/ Тпз	$P_{пер1}$	V1:= 1
(V1=1)		1-$P_{зб2}$	V1:= 0
5. **«Перезавантаження МКП2»**			
(V2=1)	1/ Тпз	$P_{пер2}$	V2:= 1
(V2=1)		1- $P_{пер2}$	V2:= 0
6. **«Перезавантаження МКП3»**			
(V3=1)	1/ Тпз	$P_{пер3}$	V3:= 1
(V3=1)		1- $P_{пер3}$	V3:= 0
7. **«Відмова підсистеми електроживлення»**			
(V4>0)	$\lambda_{ПЕЖ}$	1	V4:= V4-1
8. **«Відмова резервної батареї ПЕЖ»**			
(V5=1)	$\lambda_{РПЕЖ}$	1	V5:= 0
9. **«Відмова фільтра Калмана»**			
(V6=1)	$\lambda_{ФК}$	1	V6:= 0
Умова критичної відмови:			
(((V1=0) AND (V2=0)) OR ((V2=0) AND (V3=0)) OR ((V1=0) AND (V3=0)) OR ((V4=0) AND (V5=0)) OR (V6 = 0))			

На основі розробленої бінарної структурно-автоматної моделі та програмного модуля ASNA здійснено повторна побудова графа станів та переходів. Граф містить 251 стан та 402 переходи.

Для внесення рекомендацій щодо зменшення рівня ризику відмови приймача СНС необхідно внести заміну інтенсивності відмови приймача СНС, ММ та ВВШП у бінарну САМ представлену в табл. 3.1.6. Зміни в структурі САМ представленій в табл. 3.1.6. проводити не потрібно.

Далі за домогою програмного засобу CSD в автоматизованому режимі було отримано МС, які приведено в табл.5.5. Дана таблиця містить наступні поля: значення ймовірності МС; процентне відношення відповідного МС до сумарної ймовірності катастрофічної відмови $Q_{сум}$; непрацездатні елементи відповідного МС; кількість непрацездатних елементів у МС.

В результаті аналізу моделі обчислюваної підсистеми БпЛА з використанням мажоритарної структури, яка працює за правилом "2 з 3" було визначено, що ймовірність першого МС рівна q_1- $2{,}51 \cdot 10^{-6}$, другого q_2 - $1{,}48 \cdot 10^{-6}$ та третього q_3 - $1{,}72 \cdot 10^{-6}$, четвертого q_4 - $9{,}82 \cdot 10^{-7}$, пятого - $2{,}79 \cdot 10^{-7}$ відповідно. Значення загальної ймовірності катастрофічної відмови $Q_{заг}$ – $5{,}92 \cdot 10^{-6}$. Середній час напрацювання на відмову становить $T_{сер}$ = 20 год. Результати аналізу представлені у вигляді табл.5.4.2:

Таблиця 5.4.2

Мінімальні січення обчислюваної системи БпЛА з використанням мажоритарної структури яка працює за правилом "2 з 3"

Номер МС	Ймовірність виникнення МС	%	Кількість	Елемент
1	$2{,}51 \cdot 10^{-6}$	44,04	2	1, 2
2	$1{,}48 \cdot 10^{-6}$	25,89	2	1, 3
3	$1{,}72 \cdot 10^{-6}$	30,68	2	2, 3
4	$9{,}82 \cdot 10^{-7}$	7,42	1	4, 5
5	$2{,}79 \cdot 10^{-7}$	4,89	1	6

В результаті аналізу моделі навігаційної підсистеми БпЛА з внесенлю зміною інтенсивністю відмови приймача СНС було визначено, мінімальні січення які представлені в таблиці 5.4.2. Значення загальної ймовірності катастрофічної відмови $Q_{заг}$ – 0,0229. Час польоту становить $T_{сер}$ = 20 год. Результати аналізу представлені у вигляді табл.5.4.2:

Таблиця 5.4.3

Мінімальні січення навігаційної підсистеми БпЛА.

Номер МС	Ймовірність виникнення МС	%	Кількість	Елемент
1	$9{,}98\cdot10^{-4}$	44,8	4	1, 4, 7, 8
2	$9{,}98\cdot10^{-4}$	44,8	4	1, 5, 7, 8
3	$9{,}98\cdot10^{-4}$	44,8	4	1, 6, 7, 8
4	$9{,}98\cdot10^{-4}$	44,8	4	2, 4, 7, 8
5	$9{,}98\cdot10^{-4}$	44,8	4	2, 5, 7, 8
6	$9{,}98\cdot10^{-4}$	44,8	4	2, 6, 7, 8
7	$9{,}98\cdot10^{-4}$	44,8	4	3, 4, 7, 8
8	$9{,}98\cdot10^{-4}$	44,8	4	3, 5, 7, 8
9	$9{,}98\cdot10^{-4}$	44,8	4	3, 6, 7, 8
10	0,0203	91,1	1	9
11	$8{,}98\cdot10^{-4}$	40,3	1	10

5.5 Оцінка ризику експлуатації навігаційно-обчислювальної системи після застосування запропонованих рекомендацій.

Згідно отриманих МС (табл. 5.5) навігаційно-обчислювальної системи, було визначено наступні відповідні АС та їх рівні ризику, котрі представлені в таблиці 5.6:

Таким чином для отриманих видів відмов обчислювальної підсистеми та навігаційної підсистеми, було визначено наступні відповідні рівні ризику, котрі представлені в таблиці 5.2.2:

Таблиця 5.5

Рівень ризику для навігаційно-обчислювальної підсистеми БпЛА

	Вид відмови	Ймовірність виникення	Категорія виникення відмови	Категорія значущості відмови	Отриманий рівень ризику
1	Відмова МКП1 та МКП2	$2{,}51\cdot10^{-6}$	E	IV	Допустимий
2	Відмова МКП1 та МКП3	$1{,}48\cdot10^{-6}$	E	IV	Допустимий
3	Відмова МКП2 та МКП3	$1{,}72\cdot10^{-6}$	E	IV	Допустимий

4	Відмова ПЕЖ	$9{,}82 \cdot 10^{-7}$	E	IV	Допустимий
5	Відмова ММ, ВВШП, акслерометрів та гіроскопів	$9{,}98 \cdot 10^{-4}$	E	IV	Допустимий
6	Відмова приймача сигналів від СНС	$2{,}03 \cdot 10^{-2}$	D	IV	Високий
7	Відмова приймача сигналів від СЗО	$8{,}98 \cdot 10^{-4}$	E	IV	Допустимий

Як видно з табл. 5.5 рівень ризику відмови магнітометра, ВВШП, акселерометрів та гіроскопів з рівня “високий” перемістився на рівень “допустимий” а АС відмова приймача сигналів від СНС отримала рівень “високий”. Для зниження рівня ризику АС відмова приймача сигналів від СНС до рівня “допустимий” необхідно замінити приймач сигналів СНС з інтенсивністю відмов на два порядоки нижче.

5.6. Визначення значення пріоритету рівня ризику навігаційно-обчислювальної системи безпілотного літального апарата

За допомогою стандарту [74-77] було здійснено, аналогічно як і п.п. 5.3, аналіз усіх можливих подій котрі прийзводять до аварійної ситуації. В результаті отримано таблицю в котрій записано АС та їх наслідки та можливості щодо виявлення даних АС. Результати представлені у табл. 5.6:

Таблиця 5.6

Аналіз видів та потенційних наслідків відмов навігаційно-обчислювальної системи з використанням у ОП мажоритарної структури, яка працює за правилом "2 з 3"

Назва системи	Потенційна відмова	SEV	Потенційні наслідки	OCC	Система виявлення	DEC	RPN
А та Г	Відмова одного з гіросокпів	3	Відмова одного із каналів НП (крен, тангаж чи курс)	3	МКП	3	27
	Відмова усіх трьох гіросокпів	4	Відмова А та Г	2	МКП	2	16
	Відмова одного з акселерометрів	3	Значні невідповідності значень лінійного прискорення, вздовж однієї з трьох осей БпЛА	3	МКП	3	27
	Відмова усіх трьох акселерометрів	4	Відмова Н А та Г	2	МКП	2	16
ВВШП	Відмова ДТ	2	ВВШП не індикує температури середовища, у якому знаходиться БпЛА	4	МКП	3	24
	Відмова ДПТ	2	ВВШП не визначає взагалі або визначає зі значними похибками барометричну висоту БпЛА	4	МКП	3	24
	Відмова ДБВ	2	ВВШП не визначає взагалі або визначає зі значними похибками барометричну висоту БпЛА	4	МКП	3	24
	Відмова ДШ	2	ВВШП не визначає взагалі або визначає зі значними похибками дійсну повітряну швидкість БпЛА	4	МКП	3	24

ПССНС	Відмова приймача сигналів СНС	9	Відсутность корекції НП за сигналами СНС, одноразового збільшення (у декілька разів) похибок визначення навігаційних параметрів (координат місцеположення, швидкості та кутів орієнтації БпЛА).	3	МКП	2	54
ПССЗО	Відмова приймача сигналів від СЗО	8	Несправність ручного та напівавтоматичного каналів управління БпЛА	2	МКП	1	16
ОП	Відмова одного МПК	6	Погіршення достовірності отримання інформації	3	Детектор несправності МКП	2	36
	Відмова двох МКП	9	Відмова ОП	2	Детектор несправності МКП	2	36
	Відмова трьох МКП	9	Відмова ОП	2	Детектор несправності МКП	2	36
	Відмова ФК	9	Аварійна ситуація	2		2	36
ПЕЖ	Відмова однієї батареї	5	Зменшення тривалості польоту БпЛА	2	МКП	2	20
	Відмова двох батарей	9	Відмова ПЕЖ	2	МКП	3	54

Як видно з таблиці, для події відмова двох підсистем ПЕЖ отримане значення пріоритету ризику рівне 54 пунктам.

5.7. Візуалізація результатів аналізу ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата.

Для аналізу наслідків відмов прийнято, згідно стандартів [74] візуалізувати дану задачу у вигляді побудови ДВ.

Для побудови ДВ застосовано програмне забезпечення CutSetDefiner. Вхідними даними для цього програмного забезпечення є МС (табл. 2.4 та 3.1.7). В результаті його роботи отримано ДВ навігаційно-обчислювальної підсистеми БпЛА, представлене на рис. 5.3.

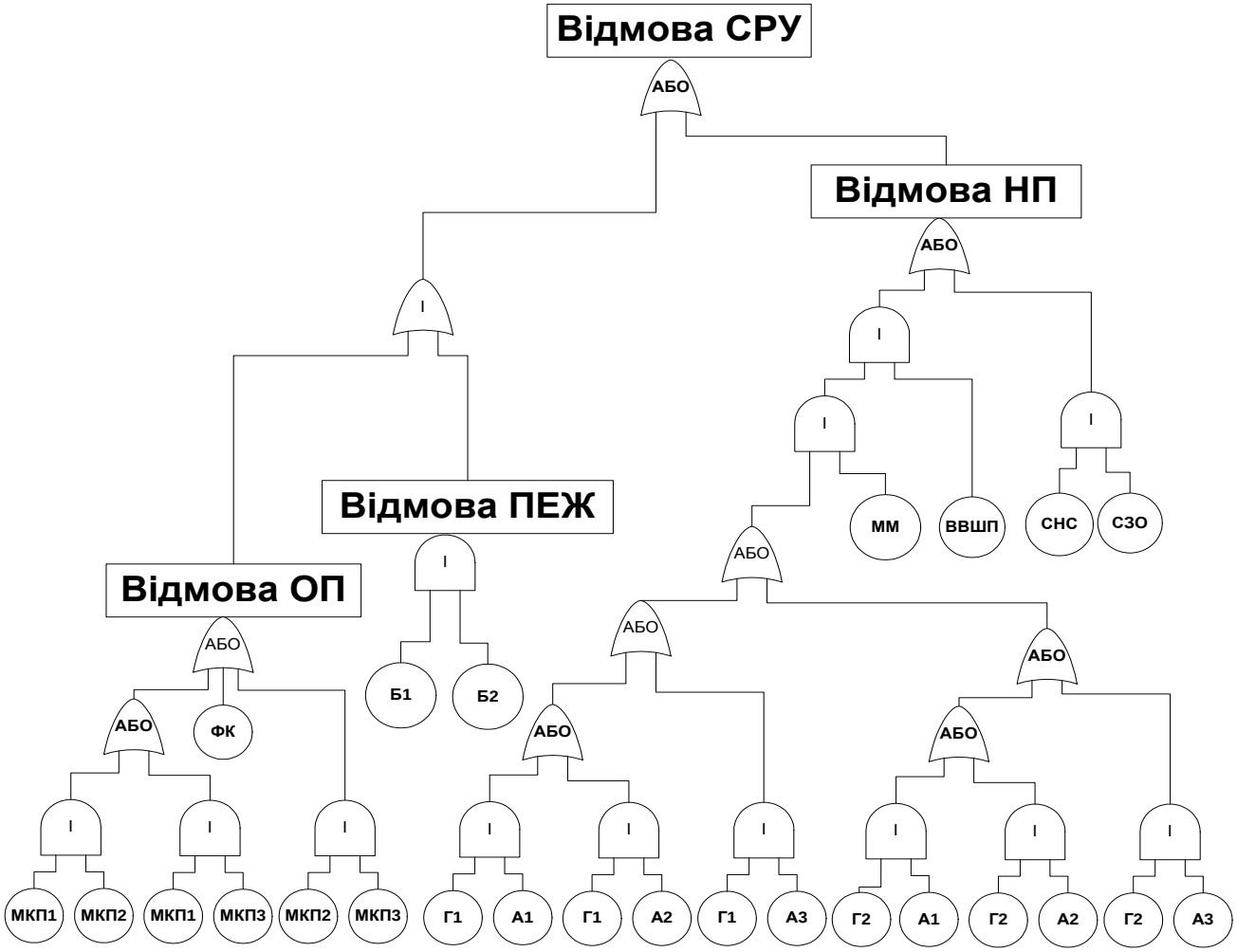

Рис.5.3 Дерево відмов системи навігаційно-обчислювальній системі БпЛА

Побудоване ДВ показало що в навігаційно-обчислювальній системі БпЛА можливі аварійні ситуації представлені в табл.5.2.2. Відмова акселерометрів, гіроскопів, магнітометра та ВВПШ або відмові лише одного з приймачів сигналів від СНС чи СЗО призведуть до відмови навігаційної підсистеми. Дані відмови призводять до втрати орієнтації апарата в просторі. Аналіз представленого ДВ показав, що відмова ПЕЖ або фільтру Калмана є найшвидшим шляхом до відмови навігаційно-обчислювальної системи БпЛА. Тому для зниження рівня ризику експлуатації потрібно провести заходи представлені в п.5.3.

Висновки до розділу 5

1. В даному розділі здійснено оцінку ризику експлуатації навігаційно-обчислювальної системи безпілотним літальним апаратом за допомогою FMEA/FMECA аналізу.

2. За допомогою моделей обчислювальної підсиситеми та навігаційної підсистем в автоматизованому режимі, за допомогою розроблених засобів, проведено оцінку ризику експлуатації. Аналіз отриманих результатів показав, що якісні оцінки значення показника ризику за допомогою FMEA/FMECA аналізу може давати певний розкид результатів. Запропонована методика дозволяє зменшити розкид отриманих показників ризику експлуатації навігаційно-обчислювальної системи безпілотним літальним апаратом шляхом проведння повторної оцінки ризику чи перевірки результатів аналізу отриманих шляхом побудови деревом відмов.

3. Аналіз показав, що рівень ризику відмови магнітометра, вимірювачів висотно-швидкісних параметрів, акселерометрів та гіроскопів є “високий” а відмова приймача сигналів від супутникової навігаційної системи є “неприйнятний”. Для зменшення рівня ризику через відмову магнітометра, вимірювачів висотно-швидкісних параметрів, акселерометрів та гіроскопів необхідно замінити магнітометр та вимірювачів висотно-швидкісних параметрів з меншою на порядок інтенсивністю відмови - $\lambda_{мм} = 1{,}38 \cdot 10^{-4}$ год, $\lambda_{ВВШП} = 2{,}48 \cdot 10^{-3}$ год$^{-1}$ відповідно. Також необхідно замінити приймач супутникової навігаційної приймач з інтенсивностю

відмов на порядок нижче - $\lambda_{СНС} = 3{,}63 \cdot 10^{-6}$ год$^{-1}$. Після внесення змін у моделі та повторного аналізу ризику експлуатації рівень ризику відмови магнітометра, вимірювачів висотно-швидкісних параметрів, акслерометрів та гіроскопів з рівня "високий" перемістився на рівень "допустимий" а відмова приймача сигналів від супутникової навігаційної системи отримала рівень "високий". Для зниження рівня ризику відмова приймача сигналів від супутникової навігаційної системи до рівня "допустимий" необхідно замінити приймач сигналів супутникової навігаційної системи з інтенсивністю відмов на два порядоки нижче.

4. Проведений аналіз показав, що відмова підсистеми електроживлення має неприпустиме значення пріоритету ризику при інтенсивності відмови - $\lambda_{ПЕЖ} = 7{,}6 \cdot 10^{-4}$ год$^{-1}$. Для зменшення рівня ризику від відмови підсистеми електроживлення було рекомендовано замінити підсистему електроживлення на підсистему з меншою у два рази інтенсивністю відмови - $\lambda_{ПЕЖ} = 3{,}8 \cdot 10^{-4}$ год $^{-1}$. Ввівши відповідні зміни у бінарну САМ обчислювальної підсистеми згідно запропонованої методики було отримано МС, на основі яких проведена повторна оцінка ризику експлуатації. Повторний аналіз показав, що значення пріоритету ризику зменшилось на 27 пунктів і стало рівним 54. Також Для зменшення ризику до рівня "допустимий" необхідно зменшити інтенсивність відмов підсистеми електроживлення на два порядки.

5. Розроблені моделі і на їх основі алгоритми та засоби дозволяють швидко перебудовувати модель для зниження ризику. В результаті проведення порівняльних досліджень згідно FMEA аналізу, показано, що у побудованій моделі рекомендовані заходи отримані експертними оцінками дійсно знизили значення пріоритету ризику з 81 до 54.

ВИСНОВКИ

В дисертаційній роботі представлено розв’язання науково-прикладної задачі зменшення рівня ризику експлуатації навігаційно-обчислювальної підсистеми безпілотним літальним апаратом за рахунок обґрунтованого підвищення надійності найбільш критичних з точки зору ризику експлуатації підсистем.

В рамках розв'язання даної задачі отримано наступні результати:

Проведений огляд сучасних джерел, в яких розглядаються моделі, методи, методики та програмні засоби оцінки ризику експлуатації радіосистем відповідального призначення показав, що більшість методів дозволяє отримати лише якісні результати аналізу ризику експлуатації у вигляді експертних оцінок. Частина методів показує лише окремі кількісні параметри, які не враховують можливості відмовостійкостих конфігурацій, технічного обслуговування, приналежність однієї відмови до кількох аварійних ситуацій. Спільним недоліком існуючих методів є “ручна” побудова моделей, і відповідно великі затрати часу при аналізі кількох варіантів реалізації радіосистеми відповідального призначення, що є несумісним з обмеженими часовими рамками етапу системотехнічного проектування.

Дістав подальший розвиток метод формалізованого представлення об’єкта дослідження у вигляді бінарної структурно-автоматної моделі. Така модель дає змогу отримати граф станів для оцінки ризику експлуатації навігаційно-обчислювальної підсистеми безпілотним літальним апаратом. Цей граф відображає усі можливі аварійні ситуації і дозволяє визначити мінімальні січення без побудови дерева відмов. Отримані таким чином мінімальні січення, на відміну від мінімальних січень отриманих за допомогою дерева відмов, можуть входити в різні аварійні ситуації, що відповідає реальній статистичній картині експлуатації об'єкта дослідження і підвищує достовірність оцінки показника ризику експлуатації.

Запропонована методика визначення кількісного показника ризику обчислювальної та навігаційної підсистем безпілотним літальним апаратом, а саме ймовірності виникнення мінімального січення, без побудови дерева відмов. Методика дозволяє вирішувати задачі зменшення рівня ризику експлуатації

навігаційно-обчислювальної підсистеми безпілотним літальним апаратом на етапі системотехнічного проектування обчислювальної та навігаційної підсистем. Це досягається шляхом оцінки ризику експлуатації багатьох варіантів побудови навігаційно-обчислювальної підсистеми безпілотним літальним апаратом з врахуванням вартості їх реалізації. Розв'язання задачі зменшення оцінки ризику експлуатації здійснюється з меншими затратами часу, ніж вимагає методика оцінки ризику експлуатації з використанням дерева відмов, що важливо на етапі системотехнічного проектування.

Для методики оцінки рівня ризику експлуатації навігаційно-обчислювальної підсистеми безпілотним літальним апаратом розроблено надійнісні моделі обчислювальної та навігаційної підсистем з деталізованим представленням стану критичної відмови, які входять до складу навігаційно-обчислювальної підсистеми безпілотним літальним апаратом. Розроблені моделі дали змогу отримати мінімальні січення та їх кількісні показники ризику, за допомогою яких можна визначити критичні модулі підсистем.

Для зменшення рівня ризику експлуатації навігаційно-обчислювальної підсистеми безпілотним літальним апаратом в обчислювальній підсистемі введений фільтр Калмана. Однак оскільки даний модуль увімкнений послідовно до трьох обчислювальних мікропроцесорів, то до даний модуль має мати інтенсивність відмови на два порядки меншу аніж мікропроцесори. Дослідження розроблених моделей дало змогу запропонувати рекомендації щодо зниження рівня ризику експлуатації навігаційно-обчислювальної системи безпілотним літальним апаратом. Зокрема для зменшення рівня ризику через відмови магнітометра, вимірювачів висотно-швидкісних параметрів, акселерометрів та гіроскопів необхідно замінити магнітометр та вимірювачі висотно-швидкісних параметрів з меншою на порядок інтенсивністю відмови - $\lambda_{мм} = 1{,}38 \cdot 10^{-4}$ год, $\lambda_{ВВШП} = 2{,}48 \cdot 10^{-3}$ год$^{-1}$ відповідно. Також необхідно замінити приймач супутникової навігаційної приймач з інтенсивностю відмов на порядок нижче - $\lambda_{СНС} = 3{,}63 \cdot 10^{-6}$ год$^{-1}$. Для зниження рівня ризику відмова приймача сигналів від супутникової навігаційної системи до рівня "допустимий"

необхідно замінити приймач сигналів супутникової навігаційної системи з інтенсивністю відмов на два порядоки нижче. від відмови підсистеми електроживлення рекомендовано замінити підсистему електроживлення на підсистему з меншою у два рази інтесивністю ніж використовувалась попередньо. Дані рекомендації були введені в бінарні структурно-автоматні моделі. В результаті отримано мінімальні січення, на основі яких, проведено повторну оцінку рівня ризику експлуатації. Повторна оцінка підтвердила зниження рівня ризику, згідно FMECA аналізу відмова магнітометра, вимірювачів висотно-швидкісних параметрів, акслерометрів та гіроскопів з рівня “високий” перемістився на рівень “допустимий” а відмова приймача сигналів від супутникової навігаційної системи отримала рівень “високий”.

Розроблено алгоритм та прототип програмного засобу, в основу якого покладено запропоновану методику оцінки рівня ризику експлуатації навігаційно-обчислювальної системи. Програмний засіб автоматизує процес отримання кількісного показника ризику, в якому враховуються: відмовостійкі конфігурації підсистем; відмови апаратних засобів; збої програмних засобів; належність певної частини відмов до двох і більше мінімальних січень; вплив ненадійності приймача сигналу від супутникової навігаційної системи; вплив ненадійності приймача зв’язку з оператором. Також для візуалізації причин та наслідків аварійних ситуацій програмний засіб дозволяє автоматизовано побудувати дерево відмов на основі мінімальних січень.

Список використаної літератури:

1. Babczynski T. Time Coordination Of Distance Protection Using Probabilistic Fault Trees With Time Dependencies / Babczynski T., Lukowicz M., Magott J. // IEEE Transactions on Power Delivery.- 2010 - July (3).- P.1402–1409.
2. Badoniya Rachna System Failure Analysis in Hydro Power Plant / Rachna Badoniya , Rajiv Premi, Praveen Patel// International Journal on Emerging Technologies. - Vol. 5. No.1.- 2014.- p. 54-58.
3. Bauer E. Design for reliability: information and computer-based systems / Eric Bauer // John Wiley & Sons, Inc., Hoboken: New Jersey. - 2010. - 325 p.
4. Baldwin E. Carr Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace / National Center for Policy Analysis. – 2013, - 44 p.
5. Behringer B. Towards Feature-Oriented Fault Tree Analysis / B. Behringer, M. Lehser, S. Rothkugel // Vasteras: IEEE 38th International Computer Software and Applications Conference Workshops (COMPSACW), 2014.- p. 522-527.
6. Blum M. PFH-calculation for complex safety functions by means of generated Markov models / M. Blum, T. Mattes, F. Schiller // Kassel: Seventh International Conference on Networked Sensing Systems (INSS), 2010. - p. 49-52.
7. Bouissou M. Boolean logic Driven Markov Processes as an alternative to Event Trees / Marc Bouissou // EDF R&D, Clamart, France - p. 81-89.
8. Čepin M. A dynamic fault tree / Marko Čepin, Borut Mavko // Reliability Engineering & System Safety. - 2002.- Vol. 75, № 1. - P. 83 - 91.
9. Čepin M. Application of the fault tree analysis for assessment of power system reliability / Andrija Volkanovski, Marko Čepin, Borut Mavko // Reliability Engineering & System Safety. - 2009.- Vol. 94, № 6. - P. 1116- 1127.
10. Chiacchio F. Dynamic Fault Trees Resolution: A Conscious Trade-Off Between Analytical And Simulative Approaches / Chiacchio F., Compagno L., D'Urso D., Manno G., Trapani N. // Reliability Engineering & System Safety. - 2011. - Vol. 96, № 11. - P. 1515 - 1526.

11. Codetta-Raiteri Daniele Integrating Several Formalisms In Order To Increase Fault Trees' Modeling Power / Daniele Codetta-Raiteri // Reliability Engineering & System Safety. - 2011. - Vol.96, № 5. P. - 534 - 544.

12. Contini Sergio Analysis Of Large Fault Trees Based On Functional Decomposition / Sergio Contini, Vaidas Matuzas // Reliability Engineering & System Safety. - 2011. - Vol.96, № 3. - P. - 383 - 390.

13. Danhua Wang An approach of automatically performing Fault Tree Analysis and failure mode and effect techniques to software processes / Wang Danhua, Pan Jingui // Chengdu: 2nd International Conference on Software Engineering and Data Mining (SEDM), 2010. - p.187-191.

14. Danhua Wang An optimization to automatic Fault Tree Analysis and Failure Mode and Effect Analysis approaches for processes / Wang Danhua, Pan Jingui // Qinhuangdao: International Conference on Computer Design and Applications (ICCDA), 2010. - Vol.3.- p. 153-157.

15. DeLong T.A. Dependability metrics to assess safety-critical systems / T.A. DeLong, D.T. Smith, B.W. Johnson // IEEE Transactions on Reliability. - Vol.54, Issue.3. - 2005. - p.498 - 505.

16. Duan Rong-Xing A New Fault Diagnosis Method Based on Fault Tree and Bayesian Networks / Rong-Xing Duan, Hui-lin Zhou // Energy Procedia.- 2012.- No. 17 - p. 1376 – 1382.

17. Elmqvist J. Formal Support for Quantitative Analysis of Residual Risks in Safety-Critical Systems / J. Elmqvist, S. Nadjm-Tehrani, // High Assurance Systems Engineering Symposium, HASE 2008. 11th IEEE. - 3-5 Dec. 2008 - P. - 154 - 164.

18. Ericson Clifton A. Hazard Analysis Techniques for System Safety / Clifton A. Ericson // John Wiley & Sons, Inc., Hoboken: New Jersey. - 2005. - 528 p.

19. Fei-min Sheen Study on Construction and Quantification of Evaluation Index System of Mine Ventilation System/ Sheen Fei-min, Chen Bo-hui, Yang Jain // Procedia Earth and Planatery Science 1. - 2009. - p. 114-122.

20. Fengchan Wang Study of Uncontained Turbine Engine Rotor Failure airworthiness compliance Verification Method / Wang Fengchan, Sun Youchao, Zeng Haijun // Procedia Engineering 17.- 2011.- p. 531-541.

21. Functional safety of electrical /electronic /programmable electronic safety related systems. part 1: General requirements: IEC 61508-1. - 2010.

22. Gleirscher M. Hazard Analysis for Technical Systems Development / M. Gleirscher // Software Quality. Increasing Value in Software and Systems Development. - 2013. - Vol. 133. - P. 104-124.

23. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment: ARP4761.- December 1996.

24. Haitao Guo Automatic creation of Markov models for reliability assessment of safety instrumented systems / Guo Haitao, Yang Xianhui // Reliability Engineering & System Safety. — 2008. — Vol. 93, No 6. — P. 829–837.

25. He Xin A software safety test approach based on FTA and Bayesian networks / Xin He, Tao Xin // Shenzhen: Prognostics and System Health Management Conference (PHM-Shenzhen), 2011.- p.1-5.

26. Henley E. J. Reliability engineering and risk assessment / E. J. Henley, H. Kumamoto // Prentice-Hall. - 1981. - 568 p.

27. Hongliang Pan Software safety analysis of 2-out-of-3 redundant architecture system based on Markov model / Pan Hongliang, Tu Jiliang, Zhang Xingyuan, Dong Decun // Guiyang: 9th International Conference on Reliability, Maintainability and Safety (ICRMS), 2011.- p.493-498.

28. Hongliang Pan The FTA based safety analysis method for urban transit signal system / Pan Hongliang, Tu Jiliang, Zhang Xingyuan, Dong Decun // Guiyang: 9th International Conference on Reliability, Maintainability and Safety (ICRMS), 2011.- p.527-532.

29. Hongyu Sun Integrating Product-Line Fault Tree Analysis into AADL Model / Sun Hongyu, M. Hauptman, R. Lutz // Plano: 10th IEEE High Assurance Systems Engineering Symposium, HASE '07, 2007. - p. 15-22.

30. Hora Cristina Fault-tree analysis used in a thermo- electric power plant / Ortmeier Frank, Adriana Catanase, Horea Hora // International Conference on Hrdraulic Machinery and Hydrodynamics.- 2004.- p. 22 -26.

31. Hosseini S.M. Modeling vehicle safety in vehicular networks using Markov chain model based on cooperative awareness /S.M. Hosseini, S. Yousefi, M.J.F. Ashrafi // Mashhad: 21st Iranian Conference on Electrical Engineering (ICEE), 2013. - p. 1-6.

32. HyeonJeong Kim Bridging the Gap between Fault Trees and UML State Machine Diagrams for Safety Analysis / Kim HyeonJeong, W.E. Wong, V.Debroy, Bae DooHwan // Sydney: 17th Asia Pacific Software Engineering Conference (APSEC), 2010. - p. 195-205.

33. Jacques Janssen Semi-Markov Risk Models for Finance, Insurance and Reliability / Janssen Jacques, Manca Raimondo // Springer: New York. - 2007. - 420 p.

34. Jiang Zhenjian The Design and Implementation of the Computer Aided Fault Tree Analysis System Based on UML and J2EE Technology / Xi'an: Zhenjian Jiang, Yongchun Wu, Na Han // International Conference on Information Management, Innovation Management and Industrial Engineering.- Vol. 2- 2009 . - p.521-524.

35. Jianping Yang Fault tree analysis using evidence theory and evidential networks With imprecise expert knowledge / Yang Jianping, Hong-Zhong Huang, Qiang Liao, Yanfeng Li // Chengdu: International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012. - p. 69-74.

36. Jidong Zeng Fuzzy fault tree analysis of mask stage / Zeng Jidong, Dan Ling, Yu Liu, Song Wang // Chengdu: International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012. - p. 274-277.

37. Jong Chaur-Gong Bayesian Network Based Hydro Power Fault Diagnosis system devepolment by Fault Tree Transformation / Chaur-Gong Jong, Sou- Sen Leu // Journal of Marine Science and Technology .- 2013.- Vol. 21, No.4. - p. 367-379.

38. Joshi A. Behavioral Fault Modeling for Model-based Safety Analysis / A. Joshi, M.P.E. Heimdahl // High Assurance Systems Engineering Symposium, 2007. HASE '07. 10th IEEE - P. 99 - 208.

39. Joshi A. Model-Based Safety Analysis of Simulink Models Using SCADE Design Verifier / A. Joshi, M. Heimdahl // in Proceedings of the 24th International Conference on Computer Safety, Reliability and Security (SAFECOMP).- 2005. - Springer.

40. Kececioglu D. Reliability Engineering Handbook, Volume 2 / D. Kececioglu // Prentice Hall Inc.: New Jersey. - 1991. - 541 p.

41. Kloos J. Risk-Based Testing of Safety-Critical Embedded Systems Driven by Fault Tree Analysis / J. Kloos, T. Hussain, R. Eschbach // Berlin: IEEE Fourth International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2011.- p.26-33.

42. Kramer St. Comparison of Enhanced Markov Models and Discrete Event Simulation: For Evaluation of Probabilistic Faults in Safety-Critical Real-Time Task Sets / Stefan Kramer, Peter Raab, Jurgen Mottok, Stanislav Racek // Verona:17th Euromicro Conference on Digital System Design (DSD), 2014. - p. 591-598.

43. Lanzisero T. Applied safety science and engineering techniques: The ASSET safety management process / T.Lanzisero // Systems, Applications and Technology Conference (LISAT): IEEE Long Island. - 2012.- p.1-6.

44. Liggesmeyer P. Fault Tree analysis, Current Research Issues, Tutorial / Liggesmeyer P. Kaiser B. // SAFECOMP 2004, Potsdam 2004.

45. Lin Zhang Reliability study of disengaging mechanism based on fault tree analysis / Zhang Lin, Haiying Ma, Jianjun Deng // Chengdu: International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012. - p.29-292.

46. Liu Yong A Methodology for Evaluation of Hurricane Impact on Composite Power System Reliability / Yong Liu and Singh C. // Transactions on Power Systems. - 2011.- Vol. 26, №1. - P. 145 - 152.

47. Long A. Variants of Classical Cutsets Characterization / R. Allen // Proceedings of 21th Interantional System Safety Conference. - 2003 - p. 396-406.

48. Lu L. Joint Failure Importance For Noncoherent Fault Trees / Lixuan Lu, Jin Jiang // Reliability, IEEE Trans. on. - 2007. - Vol. 56, № 3. - P. 435 - 443.

49. Lukowicz M. Selection Of Minimal Tripping Times For Distance Protection Using Fault Trees With Time Dependencies / M. Lukowicz, J.Magott, P. Skrobanek // Electric Power Systems Research.- 2011.- 81(July).- P.1556–1571.

50. Maggot J. Timing Analysis Of Safety Properties Using Fault Trees With Time Dependencies And Timed State-Charts / Jan Maggot, Pawel Skrobanek // Reliability Engineering & System Safety. - 2012.- Vol. 97, № 1. - P. 14 - 26.

51. Magott J, Nowakowski T, Skrobanek P, Werbinska S. Analysis Of Possibilities Of Timing Dependencies Modelling - Example Of Logistic Support System / Magott J, Nowakowski T, Skrobanek P, Werbinska S.// Safety, Reliability and Risk Analysis. Theory, methods and applications, ESREL'2008,, - 2008. - vol.2. Leiden: Taylor and Francis.- P.1055–1063.

52. Magott J. Analysis Of Logistic Support System Using Fault Trees With Time Dependencies / Magott J, Nowakowski T, Skrobanek P, Werbinska S. // Archives of Transport .- 2007- Vol. №4.- p.175-182.

53. Magott J. Analysis Of Timing Requirements For Intrusion Detection Systems In: Proceedings of the depend ability of computer systems / Magott J., Skrobanek P., Woda M. // DepCoS’07, Szklarska Poreba, Poland:IEEE Computer Society Press,- 2007.- P.278–285.

54. Mandziy B. Mathematical model for failure cause analysis of electrical systems with load-sharing redundancy of component / B.Mandziy, O. Lozynsky, S. Shcherbovskykh, // Przegląd Elektrotechniczny. - 2013.- Vol. 89, №11. - P. 244-247.

55. May R. Safety standards including IEC 61508 / R. May // Open Control Systems - The Importance of Industrial Standards conference. - 2004.- p. 601-615.

56. Merle G. Improving the Efficiency of Dynamic Fault Tree Analysis by Considering Gates FDEP as Static / G. Merle, J.-M. Roussel, J.-J. Lesage // European Safety and Reliability Conference (ESREL 2010), Rhodes : Greece.- 2010.- P. 1-7.

57. Merle G. Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events / G. Merle, J.-M. Roussel, J.-J. Lesage, A. Bobbio // Reliability, IEEE Trans. on. - 2010. - Vol. 59, № 1. - P. 250 - 261.

58. Mhenni F. Automatic fault tree generation from SysML system models / F. Mhenni, Nga Nguyen, J.-Y. Choley // Besacon: IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM), 2014.- p. 715-720.

59. Myers A. Complex System Reliability. Multichannel Systems with Imperfect Fault Coverage 2nd Edition / A. Myers // Springer-Verlag: London. - 2010. - 238 p.

60. Ortmeier Frank Electronic Notes in Theoretical Computer Science / Frank Ortmeier, Gerhard Schellhorn, - Vol.185.- 2007.- p.139-151.

61. Ph. Hönig A New Modeling Approach for Automated Safety Analysis Based on Information Flows / Philipp Hönig, Rüdiger Lunde // 25th Edition of the International Workshop on Principles of Diagnosis Conference DX'14, Graz: Austria.- September 8-11, 2014. - p. 21-28.

62. Rae Andrew A Behavior-Based Method for Fault tree generation/ Andrew Rae, Peter Lindsay // International System Safety Conference. - 2004.- p. 34-41.

63. Rausand M. System Reliability Theory: Models, Statistical Methods, and Applications / Marvin Rausand, Arnljot Hoylan// Wiley Series in probability and statistics - second edition.- 2004.- p.664.

64. Reece Clothier Determination and Evaluation of UAV Safety Objectives / Reece Clothier, Rodney Walker // In Proceedings 21st International Unmanned Air Vehicle Systems Conference, Bristol, United Kingdom.- 2006, - pages 18.1-18.16

65. Saleh J. H. Spacecraft Reliability and Multi-State Failures: A Statistical Approach, First Edition / Joseph Homer Saleh, Jean-François Castet // John Wiley & Sons, Ltd., Souhtern Gate: Chichester. - 2011. - 216 p.

66. Schweitzer E.O. Reliability Analysis of Transmission Protection Using Fault Tree Methods / E.O. Schweitzer, B. Fleming, J. Tony // International Journal of Chemical Engineering and Applications .- 2011.-Vol. 4, No. 3.- p. 65-71.

67. Singiresu S. Rao Reliability-Based Design / Singiresu S. Rao // Mcgraw-Hill - 1992.- p.569.

68. Skrobanek P. Analysis Of Timing Requirements For Intrusion Detection And Prevention Using Fault Tree With Time Dependencies / Skrobanek P, Woda M. // In: Skrobanek P, editor. Intrusion detection systems. InTech.- 2011.- P. 307–324.

69. Software Considerations in Airborne Systems and Equipment Certification: DO-178B.- December 1, 1992 - 121 p.

70. Souza Rodrigo de Queiroz FMEA and FTA Analysis For Application of The Reliability Centered Maintenance Methodology: Case Study on Hydraulic Turbines / Rodrigo de Queiroz Souza, Alberto José Álvares //, ABCM Symposium Series in Mechatronics - Vol. 3 - P. 803-812.

71. Suiran Yu A comparison of FMEA, AFMEA and FTA / Yu Suiran, Qingyan Yang, Jiwen Liu, Minxian Pan // Guiyang: 9th International Conference on Reliability, Maintainability and Safety (ICRMS), 2011.- p.954-960.

72. Takeichi M. Failure rate calculation with priority FTA method for functional safety of complex automotive subsystems / M. Takeichi, Y.Sato, K.Suyama, T. Kawahara // Xi'an: International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2011.- p.55-58.

73. Telemetry Tutorial. Revision C, 2009. – Andoya Rocket Range – 2009 – 10 p.

74. US Armed Forces Military Procedures document: MIL-P-1629.- 1949 - 678 p.

75. US Department of Defense Standard Practice for System Safety: MIL-STD-882D.- 2000.

76. US Department of Defense Standard Practice for System Safety: MIL-STD-882E.- 2012.- 101p. [2.11]

77. US Department of Defense System Safety Program Requirements: MIL-STD-882C.-1993.

78. Vesely W. Fault Tree Handbook with Aerospace Applications / Vesely William, Michael Stamatelatos, Joanne Dugan, Joseph Fragola, Joseph Minarick III, Jan Railsback // NASA Headquarters: Washington.- 2002. - 205 p.

79. Volochiy B. Estimation of Indexes of Efficiency of Radioelectronic Hardware-Software Systems Based on the Algorithm of Behavior [Текст] / 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.

80. Volochiy B. Minimal Cut Sets Determination for Renewable Systems with Limited Repair [Текст] / B. Volochiy, L. Ozirkovskyy, A. Mashchak, O. Shkiliuk // Матеріали 12-ої Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та комп'ютерної інженерії TCSET-2014», Львів - Славсько, 2014. – С. 216-218.

81. Volochiy B.Yu. Defining Minimal Cut Sets Based On Markov Model [Текст] / B. Volochiy, L. Ozirkovskyy, O. Shkiliuk, A. Mashchak // Матеріали 6-ої Міжнародної конференції молодих вчених «Computer Science & Engineering CSE-2013» в рамках 4-го міжнародного фестивалю науки «LITTERIS ET ARTIBUS», Львів, – 2013. – С. 90-91

82. 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, pp. 183-190.

83. Wang J. A subjective methodology for safety analysis of safety requirements specifications / J. Wang // IEEE Transactions on Fuzzy Systems. - Vol.5. No. 3. - 2006.- p. 418-430.

84. Wang Kai Safety risk analysis of insulators in electric transmission line based on fuzzy fault tree method / Kai Wang, Deng Yu-rong, Zhu Shi-yang, Wang You-yuan // Bali: International Conference on Condition Monitoring and Diagnosis (CMD), 2012.- p. 941-945.

85. Xiangyu Han A combined analysis method of FMEA and FTA for improving the safety analysis quality of safety-critical software / Han Xiangyu, Jun Zhang // Beijing: IEEE International Conference on Granular Computing (GrC).- 2013.- p.353-356.

86. Xiaoqin Su Methodology for visualized fault tree analysis / Su Xiaoqin, Zhaoming Lei // Zhejiang : International Conference on Electronics, Communications and Control (ICECC), 2011.- p. 898-901.

87. Xing L. Efficient Reliability Analysis Of Systems With Functional Dependence Loops / Liudong Xing, Joanne Bechta, Dugan Brock A. Morrissette // Maintenance and Reliability. - 2009. - № 3.- P. 65-69.

88. Xing Liudong Incorporating Common-Cause Failures Into the Modular Hierarchical Systems Analysis / Liudong Xing, A. Shrestha, L. Meshkat, Wendai Wang // Reliability, IEEE Trans. on. - 2009. - Vol. 58, № 1. - P. 10 - 19.

89. Yeh Y.C. Triple-triple redundant 777 primary flight computer / Yeh Y.C. // Aerospace Applications Conference, 1996. Proceedings. – 1996. – P. 293–307.

90. Yeh Y.C. Design Considerations in Boeing 777 Fly-By-Wire Computers / Yeh Y.C. // 3rd IEEE High-Assurance Systems Engineering Symposium (HASE), Washington, D.C., IEEE Computer Society Press. –1998. – P. 64–73.

91. Yeh Y.C. Safety critical avionics for the 777 primary flight controls system. Digital Avionics Systems/ Yeh Y.C. // DASC. 20th Conference. –2001, vol.1. – P. 1C2/1–1C2/11.

92. Yao Cai Improvement of Fault Tree Analysis in Formal Safety Assessment Using Binary Decision Diagram / Cai Yao, Zhengjiang Liu, Zhaolin WuYao Cai // Nanjing: 1st International Conference on Information Science and Engineering (ICISE), 2009.- p. 4330 - 4333.

93. Zhi-Ling Yang Expert System of Fault Diagnosis for Gear Box in Wind Turbine / Yang Zhi-Ling, Wang Bin, Dong Xing-Hui, Liu Hao // Systems Engineering Procedia 4 conf. - 2012.- p 189–195.

94. Zhuang Lin FTA and BN methodologies in the electrostatic safety analysis of vessel's oil system / Lin Zhuang, Jun Li, Zhiqun Guo // Guiyang: 9th International Conference on Reliability, Maintainability and Safety (ICRMS), 2011.- p.516-520.

95. Акимов В. А. Надежность технических систем и техногенный риск. / В. А Акимов, В. Л. Лапин, В. М. Попов, В. А. Пучков, В. И. Томаков, М. И. Фалеев // М.: ЗАО ФИД "Деловой экспресс", 2002. - 368 с.

96. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / Под ред. Харченко В.С. - Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", 2011. - 641 с.

97. Безопасность радиостанций радиоэлектронной аппаратуры с использованием приемопередающей аппаратуры и их составных частей. Общие требования и методы испытаний: ГОСТ Р 50829-95.

98. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК: ГОСТ Р МЭК 61511-2-2011 61511-1.

99. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности: ГОСТ Р МЭК 61511-3-2011.

100. Бобало Ю. Я. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем / 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.

101. Бочков К.А. Методи та засоби доведення функціональної безпеки мікроелектронних систем залізничної автоматики / К.А. Бочков, С.Н. Харлап, Д.Н. Шевченко // Електромагнітна сумісність та безпека на залізничному транспорті: Науково-технічний журнал. - 2011.- №2. - с. 73-81.

102. Викторова В.С. Агрегирование моделей анализа надежности и безопасности технических систем сложной структуры: автореф. дис. на соиск. учен. степ. док. техн. наук: 03.04.09 / В.С. Викторова. - С.Пб.: Ин-т пробл. упр. им. В. А. Трапезникова РАН, 2009. - 43с.

103. Волочій, Б.Ю. Автоматизація побудови дерева відмов для оцінки безпечності експлуатації складних технічних систем [Текст] / Б.Ю. Волочій, Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак // Тези IV Міжнародної науково-практичної конференції «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки PREDT-2014», Чернівці, – 2014. – С. 102-103.

104. Волочій, Б.Ю. Автоматизація побудови дерева відмов для оцінки надійності та безпечності відмовостійких систем з відновленням [Текст] / Б.Ю. Волочій, Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак // Тези доповідей VII Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій», Запоріжжя, – 2014, – С. 268-269.

105. Волочій, Б.Ю. Алгоритм автоматизованої побудови дерева відмов для оцінки безпечності експуатації телекомунікаційних систем [Текст] / Б.Ю. Волочій, Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак // Тези Всеукраїнської науково-практичної конференції «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій СПТЕЛ-2014», Львів, – 2014. – С. 88-91.

106. Волочій, Б.Ю. Отримання мінімальних січень, котрі призводять до втрати працездатності телекомунікаційної системи [Текст] / Б.Ю. Волочій, Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак // Тези Всеукраїнської науково-практичної конференції «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій СПТЕЛ-2013», Львів, – 2013. – С. 263-266.

107. Волочій, Б.Ю. Розрахунок мінімальних січень для відмовостійких систем на основі структурно-автоматної моделі [Текст] / Б.Ю. Волочій, Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак, І.В. Кулик // Матеріали Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи РТПСАС-2013», Київ, – 2013. – С. 160-161.

108. 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.

109. 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. 192-201.

110. 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.

111. Волочій Б.Ю. Методика розрахунку мінімальних січень для відмовостійких систем на основі структурно-автоматної моделі / Волочій Б.Ю., Озірковський

Л.Д.,Мащак А.В., Шкілюк О.П., Кулик І.В. // Вісник НТУУ "КПІ". Серія Радіотехніка. Радіоапаратобудування. – 2013, – №52, с. 38-45.

112. 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.

113. 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.

114. Волочій Б.Ю. Оцінка ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата / Б.Ю. Волочій, Л.Д. Озірковський, Ю.М. Пащук, А.В. Мащак, В.А. Онищенко// Військова техніка та озброєння. – 2015, - №13 – С. 77-87.

115. Волочій Б.Ю. Технологія моделювання алгоритмів поведінки інформаційних систем / Б.Ю. Волочій // Львів: Вид-во Національного університету "Львівська політехніка", 2004. – 220 с.

116. Волошин А.О. Методологічні основи проектування систем безпеки об’єктів водного транспорту/ А.О. Волошин, С.В. Руденко , А.В. Шахов// Проблеми техніки: наук.-вироб. журн. - Вип. 3 - О.:Нац. мор. ун-т., 2011- С.96-Вычужанин В.В. Оценки структурного и функционального рисков сложных технических систем / В.В. Вычужанин, Н.Д. Рудниченко // Східно - Європейський журнал передових технологій. - 2014. - №1 (67). - с. 18 - 22.

117. Гнеденко Б. В. Введение в теорию массового обслуживания / Б. В. Гнеденко, И. Н. Коваленко. – М.: Наука, 1966. – 342 с.

118. Годун Р.Л . Імовірністний аналіз безпеки як інструмент з підвищення рівня безпеки АЕС / Р.Л. Годун, С.В. Кравець // Східно - Європейський журнал передових технологій. - 2011. - №8 (51). - с. 47 - 51.

119. Горопашная А.В. Методы анализа безопасности сложных технических систем: автореф. дис. на соиск. учен. степ. канд. фіз.-мат. наук / А. В. Горопашная . – СПб. : Б.в., 2009 . – 17 с.

120. Грищин Ю.П. Радиотехнические системы / Ю.П. Грищин, В.П. Ипатов, Ю.М. Казаринов и др., под ред. Ю.М. Казаринова – М.: Радио и связь, 1990. – 496 с.

121. Дружинин В.В. Основы военной системотехники / В.В. Дружинин, Д.С. Конторов – М.: ВИРТА, 1983. – 417 с.

122. Дружинин В.В. Проблемы системологии. Проблемы теории сложных систем / В.В. Дружинин, Д.С. Конторов – М.: "Советское радио", 1976. – 296 с.

123. Дружинин В.В. Системотехника / В.В. Дружинин, Д.С. Конторов. – М.:Радио и связь, 1982. – 200 с.

124. Змисний М. М. Засоби аналізу надійності радіоелектронних систем з складними мажоритарними структурами : автореф. дис. на здоб. вчен. зв. канд. техн. наук: 05.12.17 / М. М. Змисний; Нац. ун-т "Львів. політехніка". - Л., 2013. - 21 с. - укр.

125. Костерев В.В. Надежность технических систем и управление риском. - М.: МИФИ, 2008 - 280 с.

126. Кравчук М.В. Разработка системы показателей безопасности АЭС / М.В. Кравчук // Східно - Європейський журнал передових технологій. - 2012. - №8 (56). - с. 4 - 11.

127. Кривошеїн О.О. Моделювання кислотної відмови геосистеми за допомогою графічної моделі у вигляді «дерева відмов»/ О.О. Кривошеїн// - Наук. праці УкрНДГМІ - Вип. 259 - К.: УкрНДГМІ, 2010. - С. 254-262.

128. Кулинич В.С. Методи та моделі оцінювання і забезпечення функціональної безпеки бортових інформаційно-керуючих систем літальних апаратів : автореф. дис.на отрим. вч. зв. канд. техн. наук : 05.13.06 / Кулинич Вікторія Станіславівна ; М-во освіти і науки України, Нац. техн. ун-т "Харк. політехн. ін-т". – Харків, 2013. – 20 с.

129. Кулик І. В. Засоби автоматизованої оцінки показників ефективності стратегій технічного обслуговування і ремонту систем радіоелектронного комплексу :

автореф. дис. на здоб. вчен. зв. канд. техн. наук : 05.12.17 / І. В. Кулик; Нац. ун-т "Львів. політехніка". - Л., 2013. - 21 с. - укр.

130. Маевский Л.С. Методы обеспечения надежности информационно - телекоммуникационных систем на различных этапах жизненного цикла / Л.С. Маевский // СПб.: Издатель Барзилович З.П. - 1999. - 112 с.

131. Менеджмент риска. Анализ дерева неисправностей: ГОСТ Р 51901.13-2005 (МЭК 61025:1990).

132. Менеджмент риска. Метод структурной схемы надежности: ГОСТ Р 51901.14-2005 (МЭК 61078:1991).

133. Менеджмент риска. Применение марковских методов: ГОСТ Р 51901.15-2005.

134. Менеджмент риска. Руководство по применению методов анализа надежности: ГОСТ Р 51901.5-2005.

135. Менеджмент риска. Термины и определения: ГОСТ Р 51897-2002.

136. Методические указания по проведению анализа риска опасных производственных объектов: РД 03-418-01- 2001 .

137. Можаев А.С. Теоретические основы, опыт применения и направления развития общего логико-вероятностного метода и программного комплекса "Арбитр" моделирования надежности, живучести, безопасности и риска систем. Выступление на 17-ом научном семинаре НТЦ "Промышленная безопасность", М. - 23 ноября 2009. - с. 11.

138. Можаев А.С. Методические основы оценки надежности и риска электрических систем и сетей / А.С. Можаев, А.А. Римов // Труды Международной научной школы "Моделирование и анализ безопасности и риска в сложных системах" (МА БР – 2009), СПб: ГУАП, 2009.- с. 445-452.

139. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения: ГОСТ 27.310-95.

140. Новицький А.В. Оцінка надійності системи приготування і роздавання кормів "людина-машина-середовище" методом дерева відмов / А.В. Новицький, С.В. Кропивко // Техніка та енергетика АБПЛА: Науковий вісник НУБіП України - Вип. 166 (2) - К.:Київ. -2011. - С. 331-339.

141. Нозик А.А. Оценка надежности и безопасности структурно - сложных технических систем: автореф. дис. на соиск. учен. степ. канд. техн. наук: 03.04.05 / А. А. Нозикю. - С.Пб.: Ин-т пробл. упр. им. В. А. Трапезникова РАН, 2005. - 19 с.

142. Нозик А.А. Теория и практика автоматизированного моделирования надежности и безопасности структурно-сложных систем / А. А. Нозик, А. С Можаев. // М.: Территория нефтегаз №5. - 2012 - с. 24-25.

143. Озірковський, Л.Д. Розробка методики побудови марковської моделі алгоритму поведінки програмно-апаратної системи [Текст] / Л.Д. Озірковський, О.П. Шкілюк, А.В. Мащак // Матеріали 9-ої науково-технічної конференції науково-педагогічних працівників «Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні», Львів, – 2013. – С. 499-503.

144. Панин О.А. Анализ безопасности интегрированных систем защиты: логико-вероятностный подход // «Специальная техника», №5. - 2004. - с. 1 - 9.

145. Повітряний кодекс України: Відомості Верховної Ради України № 48-49, ст.536 від 16.09.2011 р.:Основні визначення та термінологія - К. : Паливода А. В., 2011. - 108 с.

146. Половко А. М. Основы теории надёжности / Половко А.М., Гуров С.В. // БХВ - Петербург, 2006. – 704 с.

147. Рижков В. Г. Застосування ризик-орієнтованого підходу для аналізу електротравматизму на металургійних підприємствах /В. Г. Рижков, О. В. Новощонова// Металургія - Вип. 23. / ред. В. І. Пожуєв. - З.:Запоріжжя, 2011. - С. 180 - 186.

148. Рябинин И. А. Логико - вероятностный анализ проблем надежности и безопасности / И.А. Рябинин // Saarbrucken , Deutschland , Palmarium Academic Publishing. - 2012. - 263 р.

149. Рябинин И. А. Надежность и безопасность структурно - сложных систем / И.А. Рябинин // СПб: изд - во «Политехника».- 2000.- 248с.

150. Рябинин И. А. Надежность и безопасность структурно - сложных систем (2 - е издание) / И.А. Рябинин // СПБ: Изд - во СПбГУ.- 2007. - 276 с.

151. Салычев О.С. Автопилот БПЛА с Инерциальной Интегрированной Системой - основа безопасной эксплуатации беспилотных комплексов. Перший міжнародний форум “Беспилотные многоцелевые комплексы в интересах ТЭК”, UVS-TECH 2007, Москва – 2007. - 1-9 с.

152. Соколов Ю.Н. Применение компьютерных технологий для оценивания надежности и безопасности программно-технических комплексов / Ю.Н. Соколов, В.С. Харченко, В.М. Илюшко, Ю.Л. Поночевный, М.Ф. Бабаков / Под ред. Ю.Н. Соколова, В.С. Харченко. - Харьков: Нац. аэрокосмический ун-т им. Н.Е. Жуковского "ХАИ", 2013. - 458 с.

153. Сукач Е.И. Компьютерная система вероятносно-алгебраического моделирования сложных систем со многими состояниями / Е.И. Сукач, А.Б. Демуськов , Д.В. Ратобыльская // ІПММС: Математичні машини і системи, 2011, № 3 - с. 33-39.

154. Тараканов К.В. Аналитические методы исследования систем / К.В. Тараканов, Л.А. Овчаров, А.Н. Тырышкин // М.: Сов. радио, 1974. - 240 с.

155. Тарасюк О.М. Пример комплексного использования формальных методов спецификации требований и анализа надежности компьютерных систем управления / Тарасюк О.М., Горбенко А.В., Харченко В.С., Мотора Ю.В. // Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»/ Обробка інформації в складних технічних системах: науковий вісн. - №8 - 2010 - С.83-89.

156. Тоніца О. В. Комп’ютерне моделювання систем аналізу безпеки технологічних об’єктів / О. В. Тоніца, І. В. Єременко //Вісник національного технічного університету "ХПІ" : зб. наук. пр.: темат. вип. 67. - / Харківський політехнічний ін-т, нац. техн. ун-т. - 2010. - С. 45-50.

157. Ткачук П.П. Система автоматизованого управління польотом і корисним навантаженням тактичних безпілотних літальних апаратів / П.П. Ткачук, Ю.П. Сальник, Ю.М. Пащук, І.В. Матала // Військово-технічний збірник. АСВ.- №1 (10). - 2014.- с. 74-78.

158. Федоров А. В. Обзор программных комплексов для оценки надежности систем автоматической противопожарной защиты и безопасности объектов" / А. В.

Федоров, М. И. Лебедева, А. В. Семериков // Материалы двадцатой научно-технической конференции «Системы безопасности−2011». М.: Академия ГПС МЧС России, 2011. - с. 270—274.

159. Фурман И. А. Новая концепция разработки и структурная организация безопасной системы автоматизированного управления движением поездов на метрополитенах [Електронний ресурс] / И. А. Фурман, М. Л. Малиновский // Радіоелектронні і комп'ютерні системи. - 2006. - №5. - с. 97–102.

160. Харченко В.П. Авіоніка безпілотних літальних апаратів / В.П.Харченко, В.І.Чепіженко, А.А.Тунік, С.В.Павлова. – К.: ТОВ «Абрис–принт», 2012. – 464 с.

161. Хом'як Я.І. Розрахунок ризику виникнення аварійного викиду хлору в цеху розливу питної води із застосуванням програми Saphire/ Я.І. Хом'як Р.В. Климась, А.В. Михайлова // - Науковий вісник УкрНДІПБ - № 2 (20) - Л.: ЛДУ БЖД МНС України, 2009. - С.197-203.

162. Черкесов Г.Н. Логико - вероятностные методы расчета надежности структурно - сложных систем / Г.Н. Черкесов, А.С. Можаев // М.: Знание.- 1991. - 64 с.

163. Шевченко Д.Н. Аналіз динамічного дерева відмов / Д.Н. Шевченко // Електромагнітна сумісність та безпека на залізничному транспорті: Науково-технічний журнал. - 2011.- №2. - с. 142-148.

164. Щербовських С.В. Математичні моделі та методи для визначення характеристик надійності багато термінальних систем із урахуванням перерозподілу навантаження / С.В. Щербовських // монографія . – Львів: Вид-во НУ "Львівська політехніка". - 2012. – 296 с.

165. Ядерная критичная безопасность. определение количества делений при постулированной критичной аварии: ISO 16117:2013.

ДОДАТКИ

Додаток А Код програми алгоритму

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>
#define DEC 10
#define N 1000
#define MAX 33
#define MED 21
#define MIN 10

 struct Row {
 float time;
 float value [MAX];
 };
struct row{
 int val [DEC];
 int fl [DEC];
};
void Dota (char * a)
{
while (*a != '\0' && *a != '\n')
 { a++;
 if (*a == ',')
 { *a = '.'; a++; }
 }
}
int Process_Row(char *str, struct row *temp)
{
char *p = str+1;
int i = 0;
 while(*p!='\n')
 {       if ( (*(p-1) == '=') && isdigit(*p))
 { temp -> val[i] = *p - '0';
           temp -> fl[i] = 0;
           i++;   }
           p++; }
 return i;
}
/*Function count how many zeros were founed. Return counted zeros*/
int Process_Zero(struct row temp,int count)
{ int k = 0,i;
 for (i=0; i<count ; i++)
```

```
        if (temp.val[i] == 0)
 k++;
        return k;
}
int Compare_Row (struct row temp1,struct row temp2,int count)
{ int i,k;
 k=Process_Zero(temp2,count);
 for (i=0;i<count;i++)
 { if ((temp1.val[i]==0)&&(temp2.val[i]==0)) k--; }
 if (k==0) return 1;
 else return 0;}
int main (void)
{
        FILE *f;
        int j = 0,i, count, count_row, s, k, count_rows = 0, sum_elem = 0, count_elem = 0;
 int mcs_count;
 char ch, *p, *buff;
 char filename [11] = "Report.doc";
        struct row temp[N],*ptr_temp=temp, rez[N], gen [N];
        char str [127], little_buf [MED];;
        f = fopen ("c:\\6elents.vs","rt");
 printf ("Obtained states are:\n");
        while(fgets(str,127,f))
        {       count= Process_Row(str, ptr_temp);
        for(i=0;i<count;i++)
                printf("%2d",ptr_temp->val[i]);
                 printf("\n");
 ptr_temp++;
 j++;   }
        count_row=j;
 mcs_count = count;
 printf("\n There was found a %d rows", count_row);
 int Fail [count_row];
        puts("\n Last row:");    // Obtained array prints
        for(i=0;i<count;i++)
                printf("%2d",temp[count_row-1].val[i]);
 printf("\n");
                for (i=0;i<count_row-1;i++)   //sorting array
                 for(j=i+1;j<count_row;j++)
                 if (Process_Zero(temp[i],count)> Process_Zero(temp[j],count) )
                 {                       *ptr_temp=temp[i];
                        temp[i]=temp[j];
                        temp[j]=*ptr_temp;                }
                 puts("\nResult after sorting:\n");
```

```
                for(j=0;j<count_row;j++)
                {               for(i=0;i<count;i++)
                        printf("%2d",temp[j].val[i]);
                        printf("\n");          }
                s = 0;
               for (i = count_row-1; i>=0; i--)
               { k = i;
                for(j=0; j<=i; j++)
                if( Compare_Row(temp[i],temp[j],count)==0) k--;
                if (k == 0) rez[s++] = temp[i];          }
               puts("\nFailures are:");
        for(j=0;j<s;j++)
                {
                for(i=0;i<count;i++)
                        printf("%2d",rez[j].val[i]);
                        printf("\n");
                }
 printf("\nthere are %d minimal cuts sets \n Minimal Cut Sets:\n", j);
 for(j=0;j<s;j++)
                {
                for(i=0;i<count;i++)
  if ( rez[j].val[i] == 0 ) printf (" V%d ", i+1);
  if (i == count) printf ("\n");
  else continue;
        }
 /*Opening file wiht all states*/
f = fopen ("c:\\fta_v1.vs","rt");
count_row = 0;
while (fgets(str, 127, f))
{ count_row=count_row+1;}
 printf("\nIn big file a %d row were detected\n", count_row);
 rewind(f);
 struct row tmp_d [count_row], *ptr_tmp_d = tmp_d;
 printf ("In Big file Obtained states are:\n");
        while(fgets(str,127,f))
        {
       count = Process_Row(str, ptr_tmp_d);
        for(i=0;i<count;i++)
                printf("%2d",ptr_tmp_d->val[i]);
                 printf("\n");
 ptr_tmp_d++;
 }
        puts("\n Last row:");    // Obtained array prints
        for(i=0;i<count;i++)
```

```
                printf("%2d",tmp_d[count_row-1].val[i]);
printf("\n");
int hmk = 0, mcs;
int *arr_mcs;
arr_mcs = (int *)malloc(j*count_row); // j - kilkist' MCS, count_row - kilkist' rjadkiv
mcs = j; // mcs - kilkist' minimal cut sets
k = 0;
for (i=0;i<j;i++)
                {
                 for(s=0; s<count_row; s++)
                 if( Compare_Row(tmp_d[s],rez[i],count)== 1)
 {
 arr_mcs [hmk++] = s;
 k++;
 printf("\nThere is MCS in %d state", s );

 }
 arr_mcs [hmk++] = -1;
 printf("\n");
 }
arr_mcs = (int *)realloc(arr_mcs, (k+j)*sizeof(int));
// relocating dyn. memory
for (s = 0; s <= (k+j)-1; s++) // j - kilkist' MCSiv;
{
printf("%d ", arr_mcs[s]);
if (arr_mcs[s] == -1)
printf("\n");
}
count = 0;
f = fopen ("c:\\112.ds","rt");
if (f == NULL)
{
puts("error opening file!");
exit(1);
}
/*Counting row cycle*/
while (1)
{
ch = fgetc(f);
if (feof(f))
{ break; }
if ( ch == '\n')
 count_rows += 1;
}
```

```
printf("\nThis file has a %d rows", count_rows);
rewind(f); // f[0]
/*Counting summ elements cycle*/
if (f == NULL)
{ puts("error opening file!");
exit(1); }
while (1)
{
ch = fgetc(f);
if (feof(f))
{ break; }
if ( ch == '\t')
{ sum_elem += 1; }
}
printf("\nThis file has a %d elements in row and %d sum symblols", sum_elem / count_rows, sum_elem);
rewind(f); //f[0]
if (f == NULL)
{ puts("error opening file!");
exit(1); }
/*Creating array of chars arrays*/
count_elem = (sum_elem / count_rows);
/*Creating tmp string to gets */
buff = (char *)malloc((count_elem )*22*sizeof(char));
p = buff;
char *tmp [count_elem];
for (i = 0; i <= count_elem; i++)
{ tmp[i] = (char *)malloc(22); }
 struct Row mass [count_rows]; // generating array of structs
while (fgets(buff, 25020, f))
{ static int row_counters = 0;
p = buff;
printf("\n and it has a %d symblols", strlen(buff));
/* This cycle replace from string coma to dota*/
Dota(buff);
printf("\nThis file has a %d rows and %d symblols\n", count_rows, count_elem);
 short x = 0, y = 0;
while (*p != '\0' && *p != '\n')
{ tmp[x][y] = *p;
y++;
p++;
 if ( *p == '\t')
{ y = y+1;
tmp[x][y] = '\0';
```

```
   x = x+1;
  y = 0;
  p++; }
}
mass[row_counters].time = atof(tmp[0]);
short t = 0;
printf("\n");
printf("Time is -> %f\n", mass[row_counters].time);
short c;
for (c = 0; c < (count_elem-1); c++)
{ mass[row_counters].value[c] = atof(tmp[c+1]);
if (mass[row_counters].value[c] < 0)
{ mass[row_counters].value[c] = 0; }
printf("%d) Float %f; ", c+1, mass[row_counters].value[c]);
if ((c+1) % 10 == 0)
printf("\n");
}
i = 0;
float sum = 0;
while (i!=count_elem-1)
{
sum = sum + mass[row_counters].value[i];
i++;
}
printf("\nSumm is - %f \n", sum);
row_counters++;
}
float MCS [mcs][count_rows];
float MCSSum [count_rows];
for (s = 0; s < mcs; s++)
{ for (i = 0; i < count_rows; i++)
{ MCS[s][i] = 0; } }
 for (i = 0; i <= count_rows; i++)
{
MCSSum [i] = 0;
}

printf("\n");
printf("\nInitialiazing MCS to zero;\n");
static short ptr;
i = 0, s = 0, k = 0;
short c = mcs, z = 0;
for ( ; k < mcs ;)
{ for ( ; s < count_rows; s++) //moves in mass
```

```
 { i = 0;
 // printf("\nSS%d %d %d", k , s, i);
 while(1) //reading MCS indexes to one MCS value;
 {
 if (arr_mcs[i] == -1)
  break;
 // printf("\nBef%d %d %d %d MCS %f", k , s, i, arr_mcs[i], MCS[k][s]);
  MCS [k] [s] = MCS[k][s] + mass[s].value[arr_mcs[i]];
 //printf("\niteration: %d -> time is - %f; value %f, %f ", s, mass[s].time,
mass[s].value[arr_mcs[i]], MCS[s]);
  if (arr_mcs[i] == -1)
  break;
  i++;
  //printf("\nAFT%d %d %d %d MCS %f", k , s, i, arr_mcs[i], MCS[k][s]);
 }
printf("\n");
printf("\n%d %d %d", k , s, i);
 }
 printf("\n END %d %d %d", k , s, i);
 ptr = ptr + i;
 for ( ; i>=0; i--)
 { arr_mcs++;}
    k++;
    s=0;
}
 ptr = ptr + mcs;
 for(s = 0; s < mcs; s++)
 {
 printf("\nMCS #%d possibilities", s+1);
 for (i = 0; i < count_rows; i++)
 { printf("\n%d) Time %f -> q %f;", i+1, mass[i].time ,MCS[s][i]); }
 printf("\n");
 }
 for ( i = ptr; i >0 ; i--) // moving pointer to first symbol in dynamic array for freeing
 { arr_mcs--; }
 for (i = 0; i < ptr; i++)
 printf("!%d", arr_mcs[i]);
 i = 0; s = 0, k = 0, count = 0;
 j = mcs;
 while(j! = 0)
 { while (arr_mcs[s] != -1)
 { if (Fail[i] = = arr_mcs[s])
    s++;
    Fail[i] = arr_mcs[s];
```

```
   i++;
  s++; }
count = i;
i = 0;
while (count--)
{ if (Fail[i] = = arr_mcs[s])
{ i++;
 continue; }
Fail [count+1] = = arr_mcs[s];
s++;
i = count+1;
break; }
j--;
}
printf("\n");
printf("\n%d %d\n", count_rows , mcs);
for (s = 0; s < mcs ; s++)
{
   for (i = 0 ; i < count_rows; i++)
{ MCSSum [i] = MCSSum[i] + MCS [s] [i]; }
}
 for (i = 0 ; i < count_rows; i++)
{
    printf("\n==> MCS Sum in row is = %f;", MCSSum[i]);
}
printf("\n");
s = ptr - mcs;
int zs = 0;
printf("\nSorting Array of Fails");
for (i = 0; i < s; i++)
{
        for (k =0; k < s-1; k++)
        {
                if (Fail[k] > Fail[k+1])
                {
                        zs = Fail[k] ;
                        Fail[k] = Fail[k+1];
                       Fail[k+1] = zs;
                }
        }
}
k = 0, j = 0;
for (i = 0; i < s; i++)
{
```

```
 Fail[j] = Fail[i];
 j++;
  if (Fail[i] == Fail[i+1])
 { i++; }
 k++;
 }
 Fail[k-1] = -1;
 puts("\nSFails");
 for (i = 0; i < s; i++)
 printf(" -> %d", Fail[i]);
/*Forming Q mean*/
 float Qmean [count_rows];
 for (i = 0; i < count_rows; i++)
 {       Qmean[i] = 0;    }
 i = 0;
 for(k = 0;k < count_rows; k++)
 {
 i=0;
 while (Fail[i] != -1)
 { Qmean[k] = Qmean[k] + mass[k].value[Fail[i]];
 i++; } }
 if ((f = fopen(filename, "w")) == NULL)
    {
        fprintf(stderr, "Error opening file %s", filename);
        exit(1);
     }
 printf("\nFile were created");
 printf("\nPutting data to file...");
 fprintf(f, "\t\t\t\t FTA - Minimum Cut Sets Report\n\n");
 fprintf(f,
"_____________________________________________________________________");
 fprintf(f, "\n\nSystem has a %d Minimal Cut Sets", mcs);
 fprintf(f, "\n\nQmean - Possibility of top Event.");
 fprintf(f, "\nqmean - possibility of MCS.");
 fprintf(f, "\nqsum - possibility of MCS summ.");
 fprintf(f,
"\n_____________________________________________________________________");
 fprintf(f,
"\n_____________________________________________________________________");
 j = 0;
 for(s = 0; s < mcs; s++)
 { fprintf(f,"\n\nMCS #%d:", s+1);
 fprintf(f,"\nVector State:\n");
 for (i=0; i < mcs_count; i++)
```

```
 {   fprintf(f,"V%d = %d ", i+1 ,rez[s].val[i]); }
     fprintf(f, ";");
     fprintf(f,"\n\nVector State which were occured:\n");
 for (i=0; i < mcs_count; i++)
 {
 if (rez[s].val[i] == 0)
    { fprintf(f,"V%d ", i+1);
         j=j+1; }
    }
 fprintf(f, ";");
 fprintf(f, "\n\nThis MCS has a %d occured VS.", j);
 j = 0;
 fprintf(f, "\n\n");
 fprintf(f, "_____________________________________________________________________");
 fprintf(f,"\nMCS #%d possibilities:", s+1);
 fprintf(f,"\nTime \t\t\t qmean \t Qmean \t\t Qmean/qmean \t qm/qsum ", s+1);
 fprintf(f, "\n  \t\t\t [ %% ] [ %% ] ");
 fprintf(f,
"_____________________________________________________________________");
 for (i = 0; i < count_rows; i++)
 { fprintf(f, "\n%.02f \t\t%f; \t%f; \t\t%f; \t\t%f", mass[i].time , MCS[s][i], Qmean[i],
((MCS[s][i]*100)/(Qmean[i])), ((MCS[s][i]*100)/(MCSSum[i])));
 }
 fprintf(f, "\n");
 fprintf(f,
"_____________________________________________________________________");
 fprintf(f, "\n");
 fprintf(f,
"_____________________________________________________________________");
 }
        puts("\nDeleting dynamic arrays");
        for (i = 0; i <= count_elem-1; i++)
        {
                free (tmp[i]);
        }
        free (arr_mcs);
        puts("\nAll dynamic arrays were deleted");
        fclose (f);
        return 0;
}
```

Додаток Б Талиці рангування факторів ризику

Таблиця 1.

Класифікація коефіцієнта значущості Severity (S) наслідків відмов [74-77].

Опис наслідків відмов	Значущість в балах (FMEA)	Значущість в рівнях (FMECA)
Відмова не призводить до помітних наслідків	1	Незначний (V)
Наслідки відмови практично незначні	2	
Наслідки відмови незначні	3	Допустимий (IV)
Наслідки відмови призводять до практично незначних змін у системі.	4	
Наслідки відмови призводять до незначних змін у системі. Система ще може виконувати цільову функцію	5	Граничний (III)
Наслідки відмови призводять до незначних змін у системі. Система практично може виконувати цільову функцію	6	
Наслідки відмови призводять до часткової втрати виконання цільової функції але загрози безпеки відмова не представляє.	7	Критичний (II)
Значні наслідки відмови призводять до втрати виконання цільової функції але загрози безпеки відмова не представляє.	8	
Відмова становить незначну загрозу безпеки людей або навколишньому середовищу	9	Катастрофічний (I)
Відмова становить загрозу безпеки людей або навколишньому середовищу	10	

Таблиця 2.

Класифікація ймовірності відмов та представлення коефіцієнта ймовірності виникнення відмови [74-77].

Ймовірності виникнення відмов за час експлуатації	Ймовірність відмови	Коефіцієнт ймовірнсті у балах (FMEA)	Рівень ймовірності (FMEA)
Відмова практично неймовірна	менше 0,00005	1	Практично неймовірний (E)
Відмова малоймовірна	від 0,00005 до 0,001	2	
Відмова має малу ймовірність, обумовлену тільки точністю розрахунку	від 0,001 до 0,005	3	Малоймовірний (D)
Помірна ймовірність відмови	від 0,005 до 0,001	4	
Відмови можливі, але при випробуваннях або в експлуатації аналогічних виробів не спостерігалися	від 0,001 до 0,003	5	Випадковий (C)
Відмови можливі, можуть спостерігалися при випробуваннях і в експлуатації аналогічних виробів	від 0,003 до 0,005	6	
Відмови цілком ймовірні	від 0,005 до 0,01	7	Ймовірний (B)
Висока ймовірність відмови	від 0,01 до 0,10	8	
Дуже висока ймовірність відмови	від 0,10 до 0,11	9	Частий (A)
Ймовірні повторні відмови	Більше 0,11	10	

Таблиця 3.

Класифікація ймовірностей виявлення відмов у системі [74].

Види відмов по ймовірності виявлення	Ймовірність виявлення відмови, оцінена розрахунковим або експертним методом	Ймовірність виявлення у балах
Дуже висока ймовірність виявлення відмови при контролі.	Більше 0,95	1
Висока ймовірність виявлення відмови при контролі.	Від 0,95 до 0,90	2
Достатня ймовірність виявлення відмови при контролі.	Від 0,90 до 0,85	3
Помірна ймовірність виявлення відмови при контролі.	Від 0,85 до 0,65	4
Середня ймовірність виявлення відмови при контролі.	Від 0,65 до 0,55	5
Ймовірність виявлення відмови при контролі нижче середнього рівня	Від 0,55 до 0,45	6
Низька ймовірність виявлення відмови	Від 0,45 до 0,35	7
Дуже низька ймовірність виявлення відмови	Від 0,35 до 0,3	8
Практично неможливо виявити відмову	Від 0,3 до 0,25	9
Неможливо виявити відмову	Менше 0,25	10

Додаток В

Акти про впровадження результатів дисертаційної роботи

Заступник начальника Національної академії сухопутних військ імені гетьмана Петра Сагайдачного з наукової роботи
кандидат історичних наук, доцент
полковник
А.В. СЛЮСАРЕНКО
"1" 10. 2015 року

АКТ
про використання результатів кандидатської дисертаційної роботи
Мащака Андрія Володимировича,
асистента кафедри теоретичної радіотехніки та радіовимірювань
Національного університету "Львівська політехніка"

Комісія у складі голови – начальника Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, полковника ГРАБЧАКА В.І., членів комісії – ТВО заступника начальника Наукового центру Сухопутних військ з наукової роботи, підполковника ЦИБУЛІ С.А., ТВО начальника НДВ (застосування Сухопутних військ у міжнародних операціях, стабілізаційних та специфічних діях) Наукового центру Сухопутних військ, підполковника ПАШКОВСЬКОГО В.В. та наукового співробітника НДВ (застосування Сухопутних військ у міжнародних операціях, стабілізаційних та специфічних діях) Наукового центру Сухопутних військ, працівника ЗС України ПАЩУКА Ю.М. склала дійсний акт про те, що результати дисертаційної роботи Мащака Андрія Володимировича, поданої на здобуття наукового ступеня кандидата технічних наук, використані у науково-дослідній роботі за шифром "Дрон" інв. № 17-13 НОВ. Зокрема Мащаком А.В. розроблено методику оцінки ризику експлуатації системи радіоуправління безпілотним літальним апаратом, в якій використано оригінальні математичні моделі навігаційної та обчислювальної підсистем. Дана методика дозволяє на основі оцінки ризику експлуатації зазначеної системи здійснити обгрунтований вибір засобів підвищення надійності та безпечності застосування безпілотного літального апарата.

Голова комісії:
Начальник Наукового центру Сухопутних військ
Національної академії сухопутних військ імені гетьмана Петра Сагайдачного
полковник В.І. ГРАБЧАК

Члени комісії:
ТВО заступника начальника Наукового центру
Сухопутних військ з наукової роботи
підполковник С.А. ЦИБУЛЯ

ТВО начальника НДВ (застосування Сухопутних військ
у міжнародних операціях, стабілізаційних та специфічних діях)
Наукового центру Сухопутних військ
підполковник В.В. ПАШКОВСЬКИЙ

Науковий співробітник НДВ (застосування Сухопутних військ
у міжнародних операціях, стабілізаційних та специфічних діях)
Наукового центру Сухопутних військ
працівник ЗС України Ю.М. ПАЩУК

Складений акт розглянуто та схвалено на засіданні науково-технічної ради Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного протокол № 9 від 11.09.15.

«Затверджую»

Проректор з наукової роботи

Національного університету

«Львівська політехніка»

_____ проф. Н.І. Чухрай

«____» _____ 2015 р.

АКТ

про використання результатів кандидатської дисертаційної роботи Мащака Андрія Володимировича на тему "Моделі для оцінки ризику експлуатації бортової навігаційної обчислювальної підсистеми безпілотного літального апарату" поданої на здобуття наукового ступеня кандидата технічних наук.

Комісія у складі начальника науково-дослідної частини, к.т.н. доцента Жук Л.В., завідувача відділу науково-організаційного супроводу наукових досліджень Лазько Г.В., начальника планово-фінансового відділу Чулой Т.М., завідувача кафедри теоретичної радіотехніки та радіовимірювання, д.т.н. професора Бондарєва А.П., наукового керівника НДР ДБ/ПНРЛ та ДБ/ТРИКАФ д.т.н., професора Мандзія Б.А. склала цей акт у тому, що у держбюджетних науково-дослідних роботах «Розроблення моделей, методів та алгоритмів для автоматизованої оцінки показників надійності радіоелектронних та електромеханічних пристроїв та систем» (№ держреєстрації 0110U001098) та НДР ДБ/ТРИКАФ «Розроблення моделей надійності, ризику та безпечності програмно-апаратних технічних систем» (№ держресстрації 0113U001371) використані наступі результати дисертаційної роботи Мащака Андрія Володимировича на тему "Моделі для оцінки ризику експлуатації бортової навігаційної обчислювальної підсистеми безпілотного літального апарату":

- розроблено моделі обчислювальної та навігаційної підсистем з деталізованим представленням стану критичної відмови, які входять до складу системи радіоуправління безпілотним літальним апаратом.
- розроблено програмний засіб який автоматизує процес отримання кількісного показника ризику експлуатації об'єкту дослідження. Також для візуалізації причин та наслідків аварійних ситуацій розроблений програмний засіб дозволяє автоматизовано побудувати дерево відмов на основі мінімальних січень.

Перелічені моделі та програмний засіб дають змогу проводити оцінку ризику експлуатації об'єкту дослідження та зменшувати рівень ризику шляхом підвищення надійності найбільш критичних з точки зоку безпечності підсистем та модулів системи радіоуправління безпілотним літальним апаратом.

Нач. НДЧ, к.т.н., доц. Жук Л.В.

Зав. відділу НОСНД Лазько Г.В.

Нач. ПФВ Чулой Т.М.

Зав. каф ТРР, д.т.н., проф. Бондарєв А.П.

Науковий керівник НДР

ДБ/ТРИКАФ, д.т.н., проф. Мандзій Б.А.

«Затверджую»

Директор

ТОВ «Сілего Технолоджі (Україна)»

Григоренко Т.В.

«24» квітня 2015 р.

АКТ

Про використання результатів кандидатської дисертаційної роботи

Мащака Андрія Володимировича

Результати дисертаційної роботи Мащака Андрія Володимировича, поданої на здобуття наукового ступеня кандидата технічних наук, використані у діяльності Приватного підприємства ТОВ «Сілего Технолоджі (Україна)» в рамках розробки декларації безпечності пристрою моніторингу температури. Зокрема Мащаком А.В. розроблено модель оцінки ризику експлуатації пристрою моніторингу температури. Показники ризику, визначені за такою моделлю, використані під час розробки регламентів безпечності експлуатації пристрою моніторингу температури, що дозволило знизити ймовірність виникнення небезпечних ситуацій при користуванні даним пристроєм з $2{,}5 \cdot 10^{-3}$ до $6{,}4 \cdot 10^{-4}$. Разом з цим розроблена модель дала змогу провести обґрунтовану модернізацію пристрою моніторингу температури, зменшивши час вибору варіанту модернізації на 56%.

Директор Григоренко Т.В.

"СІЛЕГО ТЕХНОЛОДЖІ (УКРАЇНА)" №38905792

Бухгалтер Сильвестер М.В.