БОЙОВЕ ЗАСТОСУВАННЯ ОВТ

УДК 623.746

Б.Ю. Волочій[1,2], Л.Д. Озірковський[1], Ю.М. Пащук[2], А.В. Мащак[1], В.А. Онищенко[2]

[1] *Національний університет "Львівська політехніка", Львів*
[2]*Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів*

ОЦІНКА РИЗИКУ ЕКСПЛУАТАЦІЇ НАВІГАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

У статті представлено розв'язання задачі зменшення рівня ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата (БпЛА) за рахунок обґрунтованого підвищення надійності її критичних складових. Розв'язання поставленої задачі полягало в розробці методики визначення кількісного показника ризику експлуатації навігаційно-обчислювальної системи (НОС), а саме ймовірностей виникнення аварійних ситуацій, без побудови дерева відмов. Методика дозволяє розв'язувати задачі зменшення рівня ризику експлуатації навігаційно-обчислювальної підсистеми БпЛА ще на етапі системотехнічного проектування. Запропонована методика включає в себе нові математичні моделі підсистем НОС з деталізованим представленням стану критичної відмови.

Ключові слова: *безпілотний літальний апарат, навігаційно-обчислювальна система, ризик експлуатації, надійність, мінімальні січення, дерево відмов.*

Постановка проблеми та аналіз останніх досліджень і публікацій

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 (СтП) 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 – унеможливлення чи зменшення частоти виникнення аварій. 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 і отримання недостовірних оцінок ризику, які, в свою чергу, призводять до реалізації неприйнятних проектних рішень.

Оцінку ризику експлуатації РСВП, до яких відносяться системи бортового обладнання безпілотних літальних апаратів (БпЛА) і, зокрема, навігаційно-обчислювальні системи, на сьогоднішній день здійснюють за допомогою таких методів: аналіз видів, наслідків та критичності відмов (Failure Mode, Efects and (Criticality) Analysis (FMEA/FMECA)/Failure Mode and Effect Summary (FMES)); 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 ризику експлуатації РВСП на сьогодні найбільш вживаним є аналіз видів, наслідків та критичності відмов FMEA/FMECA, який регламентований рядом міжнародних стандартів, у т. ч. STANAG 4671 та STANAG 4703. Однак у сучасних методиках реалізації такого аналізу автоматизованими є лише незначна частина процедур, а засобами автоматизації є різновид електронних таблиць, які заповнюються і перевіряються вручну. У цих методиках не передбачено врахування особливостей

технічного обслуговування, зокрема обмеження на кількість ремонтів, вплив використання відмовостійких конфігурацій, засобів контролю, діагностики та самодіагностики на достовірність оцінки ризику експлуатації.

У статтях [1-5] представлено методи та моделі для оцінки ризику експлуатації РСВП на основі аналізу ДВ та FMEA/FMECA аналізу. Однак слід відзначити, що у цих 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 експерти можуть необґрунтовано занизити або завищити показник ризику експлуатації.

У публікаціях [6-11], присвячених розв'язанню задач оцінки ризику експлуатації шляхом побудови ДВ, вказується на необхідність врахування функціональної поведінки системи. Проте 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 таких методик, не враховується функціональна поведінка РСВП, а лише перераховуються чи визначаються відмови елементів системи.

Врахувати взаємозалежність подій у РСВП дозволяють динамічні ДВ у поєднанні з методом імітаційного моделювання Монте-Карло. Можливості динамічних ДВ представлені в статтях [12-15]. Однак варто 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 СтП при розв'язанні задач надійнісного синтезу системи через багатоваріантний аналіз.

Для зменшення затрат часу при побудові та аналізі ДВ у статтях [16-17] 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.

У статті [18] показано метод побудови ДВ, в якому запропонована окрема процедура верифікації ДВ. Однак дана процедура потребує значних затрат часу, що є неприпустимим на етапі СтП, коли необхідно розглянути багато варіантів реалізації РСВП упродовж обмеженого часу.

Отже, для оцінки ризику експлуатації навігаційно-обчислювальної системи БпЛА сучасні методи не дозволяють побудувати моделі з достатнім рівнем адекватності. Вони не враховують належність тих самих відмов до різних аварійних ситуацій, що виключає взаємозв'язок між надійністю та ризиком експлуатації БпЛА. А це, в свою чергу, не дозволяє кількісно оцінити вплив використання відмовостійких конфігурацій на зниження ризику експлуатації, що призводить або до надмірного резервування, і, відповідно, до зростання вартості, або до необґрунтованого ускладнення системи. Також моделі у вигляді ДВ не дають змоги врахувати вплив технічного обслуговування, ремонту та функціональної поведінки на оцінку ризику експлуатації. Крім цього, існуючі моделі не дозволяють враховувати перебування системи у стані простою, який для навігаційно-обчислювальної системи БпЛА аналогічний аварійній ситуації.

Мета статті

Таким чином, актуальною є задача зниження ризику експлуатації навігаційно-обчислювальної системи БпЛА шляхом реалізації у вигляді відмовостійких конфігурацій найбільш "слабких" її підсистем. Для розв'язання 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 аналізу багатьох варіантів реалізації НОС в обмежені терміни етапу СтП.

Виклад основного матеріалу

1. Аналіз методів та моделей для оцінки ризику експлуатації безпілотних літальних апаратів

Узагальнена структурна схема НОС та її взаємозв'язок з іншими бортовими системами показано на рис. 1 [19]. До особливостей НОС слід віднести те, що через необхідність безперервного постачання навігаційної інформації для забезпечення виконання польотного завдання складові такої системи повинні мати відмовостійкі конфігурації. Втім кількість резервних модулів для НОС обмежується допустимими значеннями маси, об'єму, вартості та ін. параметрами, визначеними для БпЛА.

В результаті аналізу інформаційних джерел встановлено, що для окремих підсистем НОС розроблено ряд методик оцінки ризику їх експлуатації. Однак у відомих методиках рівень ризику експлуатації оцінюється переважно на основі експертних оцінок, а заданий рівень ризику експлуатації досягається виконанням ряду рекомендацій. Кількісна оцінка ризику експлуатації НОС доступна лише на спрощених моделях, які, як правило, відображають лише одну з їх особливостей.

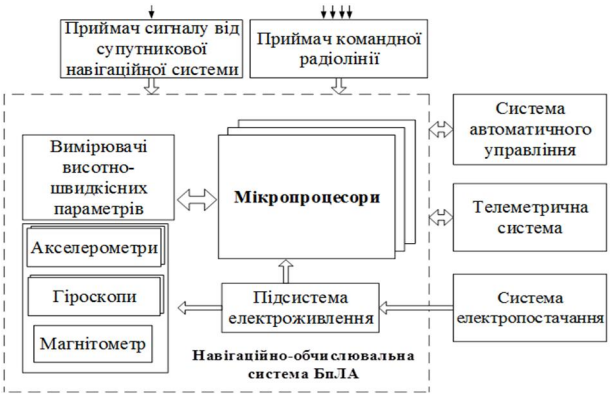

Рис. 1. **Узагальнена структурна схема навігаційно-обчислювальної системи та її взаємозв'язок з бортовими системами БпЛА**

Для побудови математичних моделей НОС з підвищеним ступенем адекватності було проведено аналіз сучасних методів побудови моделей, які дають змогу проводити кількісну оцінку ризику. Метою аналізу був вибір методу і технології моделювання, що дає змогу адекватно відобразити в одній моделі особливості функціонування НОС як з точки зору оцінки ризику, так і з точки зору надійності. Технологія моделювання повинна мати високий ступінь формалізації, щоб забезпечити безпомилкову побудову упродовж короткого часу багатьох варіантів моделі залежно від змін структури і НОС для досягнення заданого рівня ризику експлуатації.

Результати аналізу сучасних технологій побудови моделей для оцінки ризику експлуатації РСВП свідчать про те, що найбільш вживаними для побудови моделей є логіко-ймовірнісний метод та його різновиди (схеми функціональної цілісності, дерева відмов (статичні та динамічні), дерева подій), метод простору станів та імітаційне моделювання.

При використанні різновидів методу логіко-імовірнісного моделювання проектант повинен виконати складну та трудомістку роботу побудови моделі у вигляді логічної функції чи дерева, яка не придатна для багатоваріантного аналізу. Це обумовлено тим, що мінімальні зміни в структурі і алгоритмі поведінки об'єкта проектування спричиняють великі затрати часу на розробку нової моделі. Крім цього, логіко-ймовірнісні методи не дозволяють враховувати технічне обслуговування і ремонт, а також вплив відмовостійких конфігурацій на оцінку ризику експлуатації РСВП.

Найбільш ефективним методом для аналізу ризику експлуатації з урахуванням особливостей НОС є удосконалений метод простору станів з автоматизованою побудовою графа станів і переходів на базі структурно-автоматної моделі [20]. При проведенні досліджень багатьох варіантів реалізації НОС зміни досить просто вносяться в її структурно-автоматну модель (САМ). Але удосконалений метод простору станів потребує модифікації, оскільки він не дозволяє розрізняти аварійні ситуації і орієнтований виключно на отримання показників надійності.

В удосконаленій версії методу простору станів високий рівень формалізації має методика розробки графа станів та переходів, яка дає можливість автоматизувати процес побудови математичних моделей поведінки складних технічних систем у вигляді дискретно-неперервних стохастичних систем. При використанні удосконаленої технології забезпечується автоматизація процесів отримування мінімальних січень об'єкта дослідження та виконання багатоваріантного аналізу. Високий рівень формалізації удосконаленої версії методу простору станів практично унеможливлює внесення помилок при розробці моделі об'єкта дослідження.

На сьогодні не розроблено методик оцінки ризику експлуатації складних систем відповідального призначення, котрі базувалися б на удосконаленій версії методу простору станів. Слід відзначити, що на сьогодні також не розроблено методик, які дозволили б автоматизувати побудову дерева відмов об'єкта дослідження на основі графа станів і переходів, та не створено алгоритму валідації результатів FMEA/FMECA аналізу за допомогою побудованого дерева відмов. Також необхідно розробити математичну модель НОС, в якій були б закладені її особливості, що визначають надійність та рівень ризику експлуатації. Разом з цим модель має враховувати відмовостійкі конфігурації складових БпЛА, а також стратегію його технічного обслуговування та ремонту. Потрібно, щоб розроблена модель дозволяла з прийнятними затратами часу проводити оцінку ризику експлуатації та переоцінку даного рівня ризику при зміні вхідних даних.

2. Розробка математичної моделі обчислювальної підсистеми безпілотного літального апарата

Однією з головних умов успішного виконання безпілотним літальним апаратом завдання є надійне функціонування НОС. Обчислювальна підсистема (ОП) за інформацією, що надходить від навігаційної підсистеми та приймача командної радіолінії (ПКР), формує та передає до системи автоматичного управління сигнали керування. Відмова ОП однозначно призводить до аварійної ситуації. Тому успішність виконання польоту БпЛА залежить від правильного та надійного функціонування даної підсистеми.

Запропонована математична модель ОП забезпечує підвищення достовірності оцінки ризику

експлуатації за рахунок врахування: наявності мажоритарної структури і відмов мікропроцесорів (МКП); збоїв програмного забезпечення; можливості автоматичного перезавантаження МКП після виявлення збою; відмов підсистеми електроживлення (ПЕЖ).

Розробка математичної моделі ОП здійснюється з використанням методу побудови моделей у вигляді графа станів та переходів на основі САМ. У статті [21] запропоновано формалізоване представлення об'єкта дослідження у вигляді бінарної САМ, яка дозволяє деталізувати стан критичної відмови. Особливістю такої САМ є те, що для кожного елемента системи необхідно призначити індивідуальний компонент вектора стану, який може набувати лише два значення: 0 або 1. Представлення стану групи однотипних елементів однією компонентою не допускається.

На основі бінарної САМ за допомогою програмного засобу ASNA [22] формується граф станів і переходів. Отриманий таким чином граф станів та переходів представляє усі можливі аварійні ситуації. Наступним кроком є виділення окремих аварійних ситуацій. Для цього необхідно сформувати логічний вираз, який представляє всі аварійні ситуації для об'єкта дослідження. За допомогою сформованого логічного виразу з графа станів і переходів вибираються стани, які представляють кожну аварійну ситуацію. Таким чином, отримується одна або декілька груп станів, які представляють мінімальні січення [23]. Якщо складові логічного виразу, який описує аварійні ситуації, об'єднані оператором "AND", то для об'єкта дослідження властива одна аварійна ситуація, яка представлена групою станів і, відповідно, одним мінімальним січенням. Якщо складові логічного виразу об'єднані оператором "OR", то для об'єкта дослідження властиві кілька аварійних ситуацій. Визначення мінімальних січень (МС) на підставі розробленої моделі об'єкта дослідження у вигляді графа станів дає змогу враховувати належність певної частини непрацездатних станів до двох і більше мінімальних січень.

Приклад графа станів і переходів з представленням всіх непрацездатних станів (стани 15-25) та трьох аварійних ситуацій показано на рис. 2. Причому, на відміну від існуючих методів оцінки ризику експлуатації, в даному випадку одні аварійні ситуації можуть містити в собі непрацездатні стани від інших аварійних ситуацій. Це дає змогу враховувати належність певної частини відмов до двох і більше мінімальних січень.

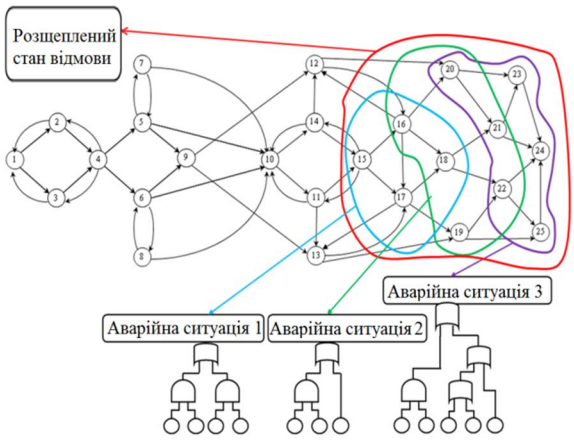

Рис. 2. **Приклад графа станів та переходів з представленням трьох аварійних ситуацій**

Розроблено два варіанти математичної моделі ОП з використанням мажоритарної структури "2 з 3" та з використанням двократного резервування. Для цього згідно з запропонованою методикою було розроблено дві бінарні САМ обчислювальної підсистеми. На основі розроблених бінарних САМ отримано моделі ОП у вигляді графа станів і переходів. Нижче представлена математична модель ОП з використанням мажоритарної структури "2 з 3" у вигляді системи лінійних диференціальних рівнянь (1). У цій моделі враховано такі параметри ОП: інтенсивності відмов мікропроцесорів МКП1 – λмпк1, МКП2 – λмпк2, МКП3 – λмпк3; ймовірності виникнення збою в МКП1 – Рзб1, в МКП2 – Рзб2, в МКП3 – Рзб3; ймовірності успішного перезавантаження МКП1 – Рперез1, МКП2 – Рперез2, МКП3 – Рперез3; інтенсивність відмов підсистеми електроживлення λпеж; середнє значення тривалості перезавантаження МКП Тперез.

За допомогою отриманих математичних моделей двох варіантів реалізації ОП проведено порівняння ризику їх експлуатації за показником "ймовірність виникнення МС", результати якого представлені в табл. 1 та табл. 2. Крім ймовірності виникнення МС, у цих таблицях представлено процентні відношення ймовірності виникнення окремого МС Qмс до загальної ймовірності виникнення аварійних ситуацій Qзаг, кількість несправних елементів ОП в МС, номери елементів, які входять в МС. Елементи ОП мають таке позначення: МКП1 – 1, МКП2 – 2, МКП3 – 3, підсистема електроживлення – 4. Порівняння виконано за таких умов: при реалізації ОП використовуються три типи МКП, щоб уникнути однотипних збоїв; різнотипні МКП мають різну надійність.

$$\frac{d\,P_1(t)}{d\,t} = -(\lambda_{мкп1}(1+P_{зб1})+\ldots+\lambda_{мкп2}P_{зб2}+ \\ +\lambda_{мкп3}P_{зб3}+\lambda_{пеж})P_1(t)+\frac{P_3(t)+P_7(t)+P_{10}(t)}{T_{перез}} \quad (1)$$

$$\frac{d\,P_{162}(t)}{d\,t} = -\left[\frac{P_{перез2}}{T_{перез}}+\frac{(1-P_{перез\,2})}{T_{перез}}\right]P_{162}(t)- \\ -\left[\frac{P_{перез1}}{T_{перез}}+\frac{(1-P_{перез\,1})}{T_{перез}}\right]P_{162}(t)+\ldots \\ +\lambda_{мкп\,3}P_{зб\,3}P_{77}(t).$$

Результати, представлені в табл. 1 і 2, свідчать про те, що використання для ОП двократного резервування зменшує ризик експлуатації в порівнянні з використанням для ОП мажоритарної структури "2 з 3". Але слід зауважити, що у випадку використання двократного резервування для ОП втрачаються позитивні якості мажоритарної структури "2 з 3".

Таблиця 1

Мінімальні січення для ОП з використанням двократного резервування

Номер МС	Ймовірність виникнення МС	Qмс/Qзаг, %	Кількість несправних елементів ОП в МС	Номери елементів, які входять в МС
1	$2{,}22\cdot10^{-6}$	39,02	3	1,2,3
2	$1{,}22\cdot10^{-6}$	21,40	1	4

Таблиця 2

Мінімальні січення для ОП з використанням мажоритарної структури "2 з 3"

Номер МС	Ймовірність виникнення МС	Qмс/Qзаг, %	Кількість несправних елементів ОП в МС	Номери елементів, які входять в МС
1	$2{,}51\cdot10^{-6}$	44,04	2	1,2
2	1,48·10-6	25,96	2	1,3
3	1,72·10-6	30,35	2	2,3
4	1,22·10-6	21,40	1	4

3. Розробка математичної моделі навігаційної підсистеми безпілотного літального апарата

У математичній моделі навігаційної підсистеми (НП), яка складається з блока акселерометрів, блока гіроскопів, магнітометра та вимірювачів висотно-швидкісних параметрів, відображено показники надійності дубльованих акселерометрів та гіроскопів, магнітометра та вимірювачів висотно-швидкісних параметрів, а також приймача сигналу від супутникової навігаційної системи (СНС) та приймача командної радіолінії (ПКР). Крім цього, враховано функціональне резервування СНС інерціальною навігаційною підсистемою БпЛА. В якості показників надійності використано: інтенсивність відмов акселерометра (λаn, де n – порядковий номер акселерометра); інтенсивність відмов гіроскопа (λгn, де n – порядковий номер гіроскопа); інтенсивність відмов вимірювача висотно-швидкісних параметрів (λввшп); інтенсивність відмов магнітометра (λмм); інтенсивність відмов приймача сигналу від СНС (λснс); інтенсивність відмов ПКР (λпкр).

На основі бінарної САМ та з використанням програмного засобу ASNA отримано математичну модель НП у вигляді системи диференційних рівнянь (2), яка налічує 998 рівнянь:

$$\frac{d\,P_1(t)}{d\,t} = -(\lambda_{г1}+\lambda_{г2}+\lambda_{г3}+\lambda_{а1}+\lambda_{а2}+\lambda_{а3}+ \\ +\lambda_{ввшп}+\lambda_{мм}+\lambda_{снн}+\lambda_{пкр})P_1(t) \quad (2)$$

$$\frac{d\,P_{998}(t)}{d\,t} = \lambda_{г1}P_{899}(t)+\lambda_{г2}P_{751}(t)+\ldots+ \\ +\lambda_{ввшп}P_{954}(t)+\lambda_{мм}P_{756}(t)+\lambda_{снс}P_{996}(t)- \\ -\lambda_{пкр}\cdot P_{998}(t).$$

Математичні моделі НП та ОП використовуються в методиці оцінки ризику експлуатації НОС. За наявності цих моделей шляхом композиційного представлення сукупності мінімальних січень стає можливим проведення оцінки ризику експлуатації НОС в цілому.

4. Автоматизація окремих процедур отримання оцінки ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата

Для забезпечення можливості багато-варіантного аналізу ризику експлуатації НОС здійснено розробку алгоритму автоматизації двох трудомістких процедур оцінки ризику: визначення мінімальних січень на основі графа станів та отримання логічної функції ДВ. Структура алгоритму представлена на рис. 3. На основі сформованого алгоритму розроблено програмний засіб CutSetDefiner, вхідними даними для якого є експортовані файли з програмного засобу ASNA – матриця векторів непрацездатних станів (*.vs) та матриця ймовірностей перебування системи в усіх станах графа (*.ds). У результаті використання програмного засобу CutSetDefiner розробник отримує файл, в якому представлені усі мінімальні січення, ймовірності виникнення МС на заданому інтервалі експлуатації, логічну функцію дерева відмов, процентні відношення ймовірності виникнення окремого МС до загальної ймовірності виникнення аварійних ситуацій.

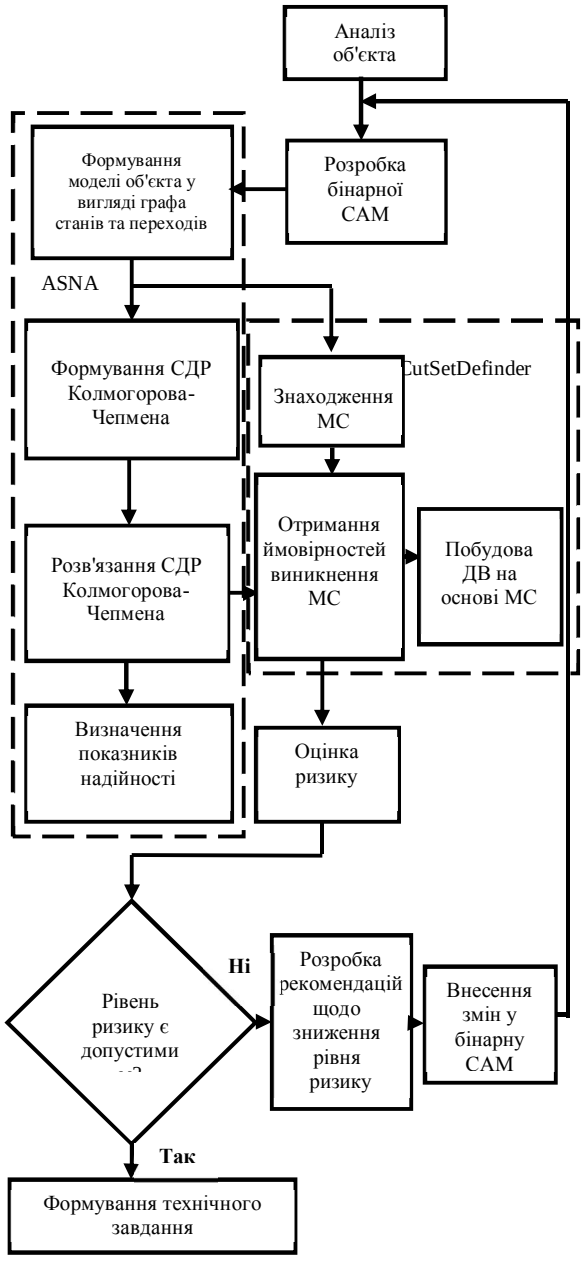

Рис. 3. **Структура алгоритму автоматизації отримання МС**

Виконано валідацію методики автоматизованого отримання мінімальних січень та логічного представлення дерева відмов. Як об'єкт, на якому перевірялась методика, використана відмовостійка система зі 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 зумовлений проведенням технічного обслуговування та ремонту. Автоматизація двох процедур методики оцінки ризику експлуатації НОС створила можливість кількісної перевірки рівня ризику з виявленням її критичних елементів.

5. Обґрунтування вимог до надійності складових навігаційно-обчислювальної системи БпЛА для зменшення ризику її експлуатації

Згідно зі стандартами STANAG 4671, STANAG 4703, MIL-STD-882E та ГОСТ 27.310-95 виконується аналіз видів критичних відмов та їх наслідків. Для НОС проаналізовано відмови окремих модулів та класифіковано наслідки їх відмов у п'ятирівневій градації. Мінімальні січення отримано на основі запропонованих математичних моделей навігаційної та обчислювальної підсистем за допомогою програмного засобу CutSetDefiner. Необхідно зауважити, що затрати часу в цьому випадку є суттєво меншими в порівнянні з затрами часу отримання МС за традиційною методикою, яка передбачає побудову дерева відмов.

Для отримання рівня ризику всі визначені види відмов були ранжирувані згідно з відповідним стандартом: якщо наслідки є значними (високий рівень значущості), то такому виду відмови призначено перший рівень значущості і навпаки – якщо наслідки відмови були незначними, то такій відмові призначено п'ятий рівень значущості (низький рівень значущості). Далі, на основі отриманих ймовірностей виникнення МС, проводилась класифікація відмов залежно від значень ймовірності виникнення МС. Якщо ймовірність виникнення була незначною, то їй призначався "рівень Е", і якщо ймовірність була великою (більше 0,3), то такій ймовірності виникнення призначався "рівень А".

Після проведення ранжирування видів відмов за допомогою таблиці, яка представлена в стандартах, визначено рівень ризику для кожної відмови: відмова ОП – "високий", відмова приймача сигналу від СНС – "допустимий", відмова ПКР – "допустимий", відмова магнітометра та вимірювачів висотно-швидкісних параметрів – "допустимий", відмова акселерометрів, гіроскопів – "допустимий", відмова ПЕЖ – "неприйнятний".

Після цього проведено згідно з вищеназваними стандартами аналіз видів відмов та їх наслідків. На підставі цього аналізу визначено значення пріоритету ризику кожної відмови. Визначення значення

пріоритету ризику полягало у присвоєнні кожному виду відмови значення факторів ризику, залежно від наслідків, які можуть виникнути після відмови. Значення пріоритету лежать у межах від 1 до 10: нижня межа – 1, якщо наслідки незначні; верхня межа – 10 за умови, що наслідки катастрофічні. 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 неможливо виявити, то даний показник отримує значення 10 (верхня межа). Наступний крок полягає у класифікації всіх представлених відмов відповідно до значення ймовірності їх виникнення (1 – малоймовірні відмови та відповідно 10 – відмови з дуже великою ймовірністю виникнення). Значення цих ймовірностей узгоджуються з отриманими ймовірностям виникнення МС.

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. Відповідно до результатів проведеного аналізу відмова ПЕЖ отримала значення пріоритету ризику 81, що є недопустимим.

Проведений аналіз показав, що при значенні інтенсивності відмови λПЕЖ = 1,66·10-5 год-1 рівень ризику ПЕЖ “неприйнятний”. Для зменшення рівня ризику експлуатації БпЛА через відмову ПЕЖ було рекомендовано замінити її ПЕЖ з меншою у два рази інтенсивністю відмови λПЕЖ = 8,3·10-6 год-1. Ввівши відповідні зміни у бінарну САМ обчислювальної підсистеми, за запропонованою методикою було отримано МС, на основі яких проведена повторна оцінка ризику експлуатації. Її результати свідчать про зниження ризику з рівня “неприйнятний” до рівня “високий”, так як значення пріоритету ризику зменшилось на 27 пунктів і стало рівним 54. Для зменшення ризику до рівня “допустимий” необхідно зменшити інтенсивність відмов ПЕЖ на два порядки.

За необхідності пред'явити дерево відмов, наприклад, при сертифікації на безпечність експлуатації безпілотного літального апарата, за запропонованою методикою побудови дерева відмов на основі МС [24-26] здійснена побудова дерева відмов НОС (рис. 4). Ця побудова здійснена за допомогою розробленого програмного засобу CutSetDefiner.

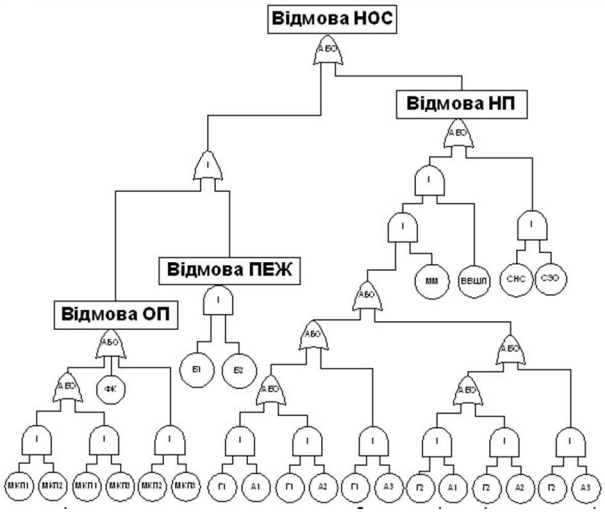

Рис. 4. **Дерево відмов навігаційно-обчислювальної системи БпЛА**

Представлена оцінка ризику експлуатації НОС виконана за умови, що польотний час БпЛА становить 100 годин. При необхідності провести оцінку ризику експлуатації при іншому значенні польотного часу слід скористатися залежностями ймовірності виникнення мінімальних січень для відмов модулів ОП та НП від польотного часу, представленими на рис. 5. На рис. 5а 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). На рис. 5б, розміщеному справа, представлено залежність ймовірності виникнення МС навігаційної підсистеми, в які входять відмови: акселерометрів, гіроскопів, магнітометра та вимірювачів висотно-швидкісних параметрів (ВВШП) (лінія 1);

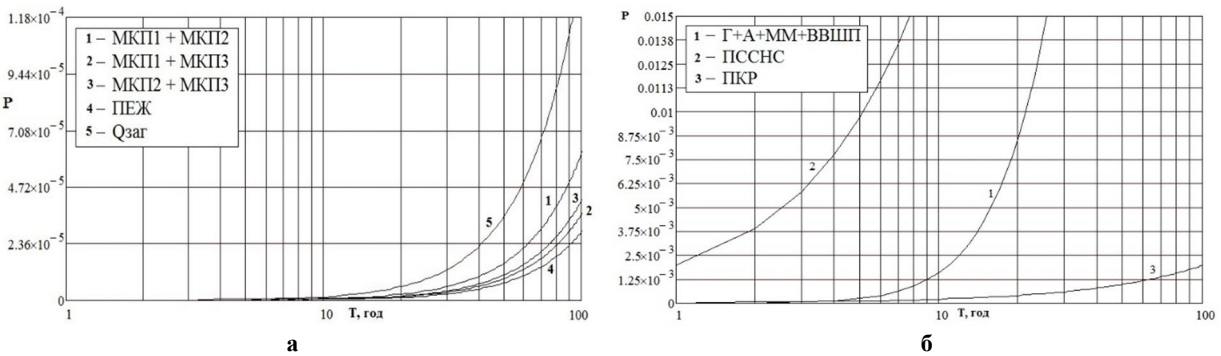

Рис. 5. **Залежності ймовірності виникнення мінімальних січень для ОП (а) та НП (б) від польотного часу**

відмова приймача сигналу від СНС (ПССНС) (лінія 2); відмова ПКР (лінія 3). Наведені залежності дозволяють визначати ймовірності виникнення мінімальних січень на заданому інтервалі експлуатації для подальшої оцінки ризику експлуатації за необхідності зміни тривалості експлуатації.

Висновки

1. Для формалізованого представлення складних технічних систем відповідального призначення запропоновано бінарну структурно-автоматну модель. Така модель дає змогу отримати граф станів для оцінки ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата. Цей граф відображає усі можливі аварійні ситуації і дозволяє визначити мінімальні січення без побудови дерева відмов.

2. Запропоновано методику визначення кількісного показника ризику експлуатації навігаційно-обчислювальної системи безпілотного літального апарата, а саме ймовірності виникнення мінімального січення, без побудови дерева відмов. Така методика дозволяє вирішувати задачу зменшення рівня ризику на етапі системотехнічного проектування. Розв'язання даної задачі за допомогою зазначеної методики здійснюється з суттєво меншими затратами часу, ніж при застосуванні відомої методики з використанням дерева відмов.

3. Для методики оцінки рівня ризику експлуатації навігаційної та обчислювальної підсистем безпілотного літального апарата розроблено їх математичні моделі з деталізованим представленням стану критичної відмови. Дослідження розроблених моделей дало змогу запропонувати рекомендації щодо зниження рівня ризику експлуатації цих підсистем.

4. Розроблено алгоритм та прототип програмного засобу, в основу якого покладено запропоновану методику. Програмний засіб автоматизує процес отримання кількісного показника ризику, а також дозволяє автоматизовано побудувати дерево відмов на основі мінімальних січень.

Список літератури

1.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.

2.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.

3.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.

4.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.

5.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.

6.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.

7.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.

8.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.

9.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.

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

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. Ткачук П.П., Сальник Ю.П., Пащук Ю.М., Матала І.В. Система автоматизованого управління польотом і корисним навантаженням тактичних безпілотних літальних апаратів. – Військово-технічний збірник 1 (10). – 2014, АСВ. – С. 74-78.

20. Бобало Ю. Я. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем: монографія / Ю.Я. Бобало, Б.Ю. Волочій, О.Ю. Лозинський, Б.А. Мандзій, Л.Д. Озірковський, Д.В. Федасюк, С.В. Щербовських, В.С. Яковина. – Львів : Вид. «Львівська політехніка», 2013. – 300 с

21. Волочій Б.Ю. Методика розрахунку 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 // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2013, – №52. – С. 38-45.

22. Volochiy B. Extending the features of software for reliability analysis of fault-tolerant systems / Bohdan Volochiy, Bohdan Mandziy, Leonid Ozirkovskyi // Computational Problems of Electrical Engineering = Обчислювальні проблеми електротехніки: науково-технічний журнал / Lviv Politechnic National University ; editor-in-chief Yuriy Bobalo. – Львів: Видавництво „Львівська політехніка”, 2012. - Volume 2, number 2. - P. 113-121.

23. 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 СІПТЕЛ-2013». – Львів, – 2013. – С. 263-266.

24. 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.

25. 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 СІПТЕЛ-2014». – Львів, 2014. – С. 88-91.

26. Волочій Б.Ю. Методика побудови дерева відмов складної технічної системи на основі графа станів і переходів [Текст] / 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.

Рецензент: д.т.н., проф. Прудиус І.Н., директор Інституту телекомунікацій, радіоелектроніки та електронної техніки, Національний університет “Львівська політехніка”, Львів.

Оценка риска эксплуатации навигационно-вычислительной системы беспилотного летательного аппарата

Б.Ю. Волочий, Л.Д. Озирковский, Ю.М. Пащук, А.В. Мащак, В.А. Онищенко

В статье представлено решение задачи уменьшения уровня риска эксплуатации навигационно-вычислительной системы беспилотного летательного аппарата (БпЛА) за счет обоснованного повышения надежности ее критических составляющих. Решение поставленной задачи заключалось в разработке методики определения количественного показателя риска эксплуатации навигационно-вычислительной системы, а именно: вероятностей возникновения аварийных ситуаций, без построения дерева отказов. Методика позволяет решать задачи уменьшения уровня риска эксплуатации навигационно-вычислительной системы БпЛА еще на этапе системотехнического проектирования. Предложенная методика включает новые математические модели подсистем навигационно-вычислительной системы с детализированным представлением состояния критического отказа.

Ключевые слова: *беспилотный летательный аппарат, навигационно-вычислительная система, риск эксплуатации, надежность, минимальные сечения, дерево отказов.*

Safety risk assessment of navigation and flight control computer system of unmanned aerial vehicle

B. Volochiy, L. Ozirkovskyi, Y. Pashchuk, A. Mashchak, V. Onyshchenko

The article deals with the problem solution of reducing of safety risk level of the navigation and flight control computer system (NAFCCS) of unmanned aerial vehicle (UAV) owing to well-grounded reliability increasing of the NAFCCS critical components. The problem solution lies in development of methods (technique) of calculation of NAFCCS safety risk level, namely probabilities of catastrophic failure occurrence, without Fault Tree Evaluation. The technique allows solving the problems of reducing of safety risk level of the NAFCCS on the systems engineering design stage. The offered technique includes new mathematical models of NAFCCS subsystems with detail presentation of the of critical fault state.

Key words: *unmanned aerial vehicle, navigation and flight control computer system, safety risk, reliability, minimum sections, fault tree.*