УДК 004.03:621.38

В.С. Похил

Військовий інститут телекомунікацій та інформатизації НТУУ «КПІ», Україна

УДОСКОНАЛЕНИЙ МЕТОД АНАЛІЗУ Й ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БОРТОВИХ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ ПОВІТРЯНОГО СУДНА

Наведено аналітичний огляд поняття функціональної безпеки. Відзначено важливість розгляду функціональної безпеки як властивості інформаційно-керуючої системи (ІКС). Запропоновано вдосконалений метод аналізу й оцінювання функціональної безпеки підсистем бортової ІКС повітряного судна. Розглянуто приклад його застосування для оцінювання функціональної безпеки підсистеми автоматичного керування силовою установкою бортової ІКС літака Ан-148.

***Ключові слова**: бортова інформаційно-керуюча система, функціональна безпека, ризик, збиток, метод аналізу й оцінки, сумарна питома критичність елемента.*

Вступ

Інформаційно-керуючі системи (ІКС) на даний час широко застосовуються в різних галузях техніки для забезпечення її безпечного функціонування. Відмова подібного роду систем може привести до виникнення істотних негативних наслідків для людей, техніки, навколишнього середовища. Даний факт привів до виникнення такого поняття як «функціональна безпека систем», що є основним у серії стандартів ГОСТ Р МЭК 61508.

Функціональна безпека (ФБ) є частиною загальної безпеки, що стосується керованого обладнання (КО) і систем керування КО і залежить від правильності функціонування електричних/ електронних/ програмованих електронних (Е/Е/ПЕ) систем, пов'язаних з безпекою, систем забезпечення безпеки, заснованих на інших технологіях і зовнішніх засобах скорочення ризику [1].

За визначенням, безпечний стан – це стан КО, при якому досягається безпека об'єкта керування, тобто стан, у якому відсутній неприпустимий для безпеки даного об'єкта або навколишнього його середовища ризик.

Отже, для визначення меж безпечного функціонування системи необхідно оцінювати величину ризику. Ризик являє собою поєднання імовірності заподіяння збитку й обсягів («ваги») цього збитку [2]. Мета визначення ризику для конкретної небезпечної події, викликаного невиконанням функцій, покладених на КО (відмовою КО), полягає в тому, щоб сформулювати критерії виникнення небезпечної події й визначити ймовірність (частоту) його виникнення, а також збиток при цьому.

Об'єктом аналізу й оцінювання ФБ у даній статті є підсистеми бортової інформаційно-керуючої системи (БІКС). Під бортовою інформаційно-керуючою системою повітряного судна (ПС) розуміється система, що поєднує інформаційні ресурси, математично-лінгвістичне (програмне) забезпечення, обчислювальну й електричну підсистеми, що забезпечують автоматизацію всіх інформаційних і керуючих процесів ПС. БІКС ПС будуються на основі розподіленого бортового обчислювального комплексу з використанням центральної ЕОМ керування, спеціалізованих процесорів (контролерів) і операційної системи (ОС) реального часу.

Аналіз літератури по даному питанню показав, що відсутній підхід до якісного аналізу й кількісної оцінки показника ФБ як ІКС, так і БІКС зокрема. Так, в [3] описані різні методи оцінки ФБ, які дозволяють визначити загрози, причини, наслідки, дії по мінімізації їхньої появи, оцінити надійність та ін. У статті [4] приводиться метод аналізу ФБ, що використовує моделі ризиків, процедури їхньої оптимізації, порівняльний аналіз і дозволяє вибирати набір контрзаходів та інформаційних технологій для зниження ризиків. У книзі [5] розглянуті методики кількісної оцінки впливу порушень функціонування бортового ергатичного комплексу (екіпаж та бортове керуюче обладнання ПС) на рівень безпеки польоту, описані основні методи і засоби забезпечення безпеки функціонування цих комплексів.

Таким чином, можна зробити висновок, що перераховані вище методи, моделі й засоби не дають можливості одержати комплексну кількісну оцінку рівня ФБ БІКС ПС, який би враховував показники критичності використовуваних елементів (або покладених на них функцій), величини ризику невиконання функцій, які безпосередньо є важливими для підтримки заданого рівня ФБ, а також дозволив би провести ранжування підсистем БІКС ПС за ступенем їх критичності й важливості для безпеки.

Незважаючи на різноманіття аспектів проблеми підвищення безпеки польотів ПС, одним з найбільш важливих є **завдання** якісного аналізу й кількісного оцінювання рівня функціональної безпеки їх БІКС з метою підвищення ефективності подальших заходів щодо поліпшення даної властивості.

Метою статті є представлення удосконаленого методу аналізу й оцінювання функціональної безпеки БІКС ПС, що дозволить врахувати структурну надійність їх критичних підсистем.

Метод аналізу критичності окремих елементів і оцінки функціональної безпеки БІКС ПС

У роботі [6] був запропонований метод аналізу й оцінювання функціональної безпеки, в основу якого покладений аналіз видів, наслідків і критичності відмов окремих елементів БІКС, що виконують функції безпеки ($F_Б$). В результаті аналізу властивості функціональної безпеки БІКС із використанням запропонованого методу були отримані оцінки ступеня критичності окремих елементів підсистем, імовірності відмови функції й величина збитку, що може бути викликаний невиконанням даної функції підсистемою БІКС.

У результаті використання зазначеного методу при проведенні подальшого аналізу й оцінки ФБ різних підсистем БІКС ПС було проведено його удосконалення в аспектах проведення аналізу критичності окремих елементів БІКС, визначення показника збитку при відмові функції безпеки й показника надійності (імовірності відмови) $F_Б$. Нижче розглянуті основні етапи, що входять до вдосконаленого методу аналізу й оцінювання ФБ БІКС ПС.

Модель бортової інформаційно-керуючої системи

Структурно-топологічна побудова БІКС задається графом G, вершинам а якого відповідають обчислювально-комунікаційні вузли (бортове кероване, обчислювальне, керуюче обладнання) і шини обміну даними (сигналами) між ними.

Аналіз критичності окремих елементів БІКС з позицій функціональної безпеки

Цей етап заснований на правилах проведення аналізу критичності відмов елементів (AKBE) складних систем, викладених в [7], і містить у своєму складі чотири основних етапи.

У загальному випадку для розглянутих БІКС можливі три основних види відмов елементів (підсистем):

1) відмови, що не впливають на виконання функції безпеки (критичної функції) тієї або іншої підсистеми або БІКС у цілому;

2) відмови, що приводять до погіршення точностних і/або часових характеристик виконання критичної функції підсистемою, але не приводять до небезпечного стану БІКС або до катастрофічних наслідків об'єкт, в якому використовується дана система – відмови, що приводять до частково-працездатного стану БІКС;

3) відмови, що приводять до критичного стану функціональну підсистему БІКС, безпосередньо пов'язану з її функціональною безпекою, що неминуче приводить до катастрофічного збитку для об'єкта керування.

На першому етапі здійснюється аналіз критичності множини функцій {F}, що виконуються системою, з паралельним розкладанням графа БІКС на часткові підграфи G', що містять всі елементи, які беруть участь у реалізації $F_Б$ БІКС, порушення виконання яких може привести до катастрофічних станів системи. Якісні характеристики виконання цих $F_Б$ будуть визначальними для властивості функціональної безпеки системи.

На другому етапі визначається можливість настання катастрофічного стану при невиконання функцій системою, шляхом оцінки величини збитку, що спричиниться відмовлю тієї або іншої $F_Б$.

З метою оцінки нормованого значення показника збитку (U_n) використовуються наступні правила:

- якщо в результаті відмови $F_Б$ підсистеми БІКС ПС наступлять катастрофічні наслідки, пов'язані із загибеллю людей, значення приймається рівним 1;
- якщо в результаті відмови $F_Б$ підсистеми БІКС ПС можливе настання катастрофічних наслідків, але існує компенсуюча $F_Б$, що виконується іншою підсистемою БІКС або поєднанням БІКС і членів екіпажа, то значення приймається рівним 0,75;
- якщо в результаті відмови $F_Б$ підсистеми БІКС ПС можливе настання катастрофічних наслідків, але існує аналогічна $F_Б$, виконувана іншою підсистемою (резервним контуром), то значення дорівнює 0,5;
- якщо в результаті відмови $F_Б$, пов'язаної із проведенням самодіагностики (тестування працездатності), підсистеми БІКС ПС можливе настання катастрофічних наслідків, але існують інші канали (підсистеми), які дозволяють одержати інформацію про порушення працездатного стану розглянутої підсистеми БІКС ПС, то значення показника збитку приймається рівним 0,25;
- якщо в результаті відмови $F_Б$ підсистеми БІКС ПС катастрофічні наслідки не наступають, то значення U_n дорівнює 0.

На третьому етапі кожна з даних $F_Б$, для якої показник збитку не дорівнює 0 (тобто вона є критичною), піддається розкладанню на множину простих задач $\{Z_n\}$ (процесів), виконання яких окремими елементами (блоками, вузлами, пристроями) забезпечує роботу підсистеми, пов'язаної із цією $F_Б$.

Четвертий етап аналізу полягає у визначенні кратності використання окремих елементів підсистем БІКС у вирішенні критичних задач (КЗ), що забезпечують виконання відповідних $F_Б$. При цьому для кожного з і підграфів G'_n формуються матриці критичності M_{KPn} (z_{jn},a_k) елементів a_k, які входять у

їхній склад. Елементи даних матриць m_{jk} на перетинанні рядків, що відповідають певним КЗ z_{jn}, зі стовпцями, що відповідають елементам a_k аналізованого підграфу, заповнюються числовими значеннями відповідно до наступних правил:

1) якщо відмова елемента a_k для даної КЗ z_{jn} відноситься до виду 1 – то значення елемента m_{jk} матриці $M_{KPn}(z_{jn}, a_k)$ дорівнює 1;

2) якщо відмова елемента a_k для даної КЗ z_{jn} відноситься до виду 2 – то значення елемента m_{jk} матриці $M_{KPn}(z_{jn}, a_k)$ дорівнює 0,5;

3) якщо відмова елемента a_k для даної КЗ z_{jn} відноситься до виду 3 – то елемент m_{jk} матриці M_{KPn} (z_{jn},c_k) приймає значення 0;

4) якщо для виконання даної КЗ z_{jn} використовуються d паралельно включених однотипних структурних елементів a_k, що входять в аналізований підграф G_n, то відповідний елемент m_{jk} матриці $M_{KPn}(z_{jn}, a_k)$ прийме значення в d раз менше значення, визначеного за правилами 1 – 3.

П'ятим етапом аналізу є визначення кількісного значення показника кратності критичності – v_k для всіх структурних елементів a_k кожної з і функціональних підсистем БІКС, що проводиться в наступній послідовності:

1) визначення абсолютного значення величини критичності $m_{\Sigma k}$ елемента a_k n-ї підсистеми БІКС шляхом сумування значень всіх елементів m_{jk} k-го стовпця матриці критичності $M_{KPn}(Z_{jn}, a_k)$;

2) обчислення сумарного значення критичності $m_{\Sigma n}$ всіх елементів a_k n-ї підсистеми БІКС шляхом сумування значень $m_{\Sigma k}$ всіх елементів a_k, що утворюють цю підсистему;

3) розрахунок нормованого значення ступеня критичності кожного елемента a_k n-ї підсистеми БІКС – показника кратності критичності v_k відповідно до виразу:

$$v_k = \frac{m_{\Sigma k}}{m_{\Sigma n}}. \qquad (1)$$

Результатом проведення описаного АКВЕ БІКС ПС є і одномірних масивів $V_n(a_k)$, що містять значення показника кратності критичності v_k всіх елементів підсистем БІКС, критичних для ФБ ПС.

Оцінювання функціональної безпеки БІКС ПС

Для проведення оцінювання функціональної безпеки (ОФБ) БІКС у цілому необхідно провести оцінювання даної властивості для всіх функціональних підсистем, кожна з яких представлена набором елементів, відповідальних за виконання відповідної функції безпеки. Оцінювати функціональну безпеку Fs окремої функціональної підсистеми БІКС, що виконує одну з $F_Б$ (f^*_n), пропонується відповідно до виразу:

$$Fs(f^*_n) = 1 - v_{\Sigma n} \cdot R_n, \qquad (2)$$

де $v_{\Sigma n}$ – питома сумарна критичність n-ї підсистеми БІКС, яка виконує $F_Б$, що визначається для повної множини $F_Б$ підсистеми за виразом:

$$v_{\Sigma n} = \frac{\sum_{l=1}^{i} v_{kn_l}}{\sum_{j=1}^{n} v_{kj}}, \qquad (3)$$

де v_{kn} – сумарний показник кратності критичності і елементів, які задіяні при виконанні n-ї $F_Б$;

v_{kj} – сумарний показник кратності критичності по всіх n $F_Б$ j-ї підсистеми БІКС ПС;

R_n – ризик, пов'язаний з відмовою n-ї $F_Б$, що визначається за виразом:

$$R_n = P_{on} \cdot U_n, \qquad (4)$$

де P_{on} – імовірність експлуатаційної відмови n-ї $F_Б$,

U_n – нормований у межах [0, 1] показник збитку, можливого при відмові n-ї $F_Б$.

Імовірність виникнення експлуатаційної відмови виконання функції визначається на підставі причин її виникнення. Як причини розглядаються відмови елементів, агрегатів і підсистем, що належать аналізованій підсистемі. До складу кожної підсистеми входять компоненти, які необхідні для виконання запропонованих функцій, починаючи від обчислювальних вузлів до виконавчих механізмів, а також агрегати, що забезпечують контроль параметрів системи і їхнє відображення екіпажу. В аналізованій підсистемі можуть бути відмови у виконанні функції, які обумовлені відмовами й несправностями в інших системах, але при аналізі окремих функціональних підсистем ці відмови як причини розглянутої відмови функції не враховуються. Подібні відмови розглядаються при аналізі взаємовпливу систем. У якості вихідних даних для визначення ймовірності виникнення відмови функції використаються кількісні характеристики агрегатів, шин передачі даних, обчислювальних пристроїв і пристроїв відображення. Ці дані отримані за матеріалами організацій-постачальників, за результатами обробки статистики про відмови, отриманої в результаті експлуатації й на основі довідкових даних постачальників комплектуючих виробів. Розрахунок імовірності виникнення відмови функції ведеться в припущенні, що всі агрегати перед вильотом справні.

У роботі [3] імовірність експлуатаційної відмови n-ї функції безпеки визначалася за найбільш ненадійним елементом, тобто ймовірність відмови приймалася рівною максимальній ймовірності відмови елементу зі складу елементів, які призначені для виконання даної функції. Подібне визначення ймовірності відмови функції не дає можливості врахувати структурні особливості підсистеми, що виконує розглянуту функцію. В удосконаленому методі аналізу й оцінювання ФБ пропонується використовувати метод визначення ймовірності відмови (невиконання) функції на основі визначення струк-

турної надійності відповідних підсистем методом повного перебору шляхів обміну інформаційно-керуючими сигналами в них [8], що дозволить врахувати всі можливі варіанти структурної організації відповідної підсистеми для задоволення умови виконання основних критичних задач функції, пов'язаної з безпекою. Сутність зазначеного методу оцінки структурної надійності підсистеми БІКС полягає у визначенні середнього значення ймовірності відмови (порушення зв'язності) структурної схеми з'єднання елементів, що відповідають за виконання кожної критичної функції (в найкритичніших проектах створення ІКС доцільно для подальшого визначення показників їх ФБ використовувати найбільше значення ймовірності відмови). Цей метод застосовується за умови, коли події відмови окремих елементів незалежні, елементи підсистеми не є відновлюваними в процесі виконання функції, а порядок появи відмов в підсистемі не має значення.

Оцінювання ФБ з використанням удосконаленого методу на прикладі системи автоматичного керування силовою установкою БІКС літака Ан-148

Розглянемо приклад застосування запропонованого удосконаленого методу оцінювання ФБ й відповідних йому показників при проведенні аналізу ФБ системи автоматичного керування силовою установкою (САКСУ), як однієї з основних підсистем БІКС літака Ан-148 [9].

З використанням запропонованого методу проводимо аналіз критичності множини функцій, що виконуються даною підсистемою. Для САКСУ БІКС Ан-148 виділяють 11 функцій безпеки ($F_Б$):

f^*_1 – запуск обох двигунів;

f^*_2 – ручне керування режимом роботи кожного двигуна положенням важелів керуванням двигуном (РУД) на всіх етапах польоту;

f^*_3 – автоматичне керування режимом роботи кожного двигуна за сигналами приросту, що одержуються від системи автоматичного керування САУ-148;

f^*_4 – перехід на спрощене гідромеханічне регулювання режимами кожного двигуна при відмові електронних регуляторів, а також за командою екіпажу (резервне керування);

f^*_5 – керування реверсом тяги кожного двигуна;

f^*_6 – сигналізація про відмову кожного двигуна і його автоматична зупинка;

f^*_8 – зупинка кожного двигуна за командою екіпажу;

f^*_7 – включення надзвичайного режиму роботи двигуна при відмові сусіднього двигуна на етапі зльоту й відходу на друге коло;

f^*_9 – безперервний контроль ланцюгів датчиків і виконавчих механізмів, установлених на кожному двигуні;

f^*_{10} – тестовий контроль електронних блоків системи керування силовою установкою, а також виконавчих механізмів як на непрацюючому, так і на працюючому двигуні;

f^*_{11} – передачу виміряних значень параметрів кожного двигуна, а також інформації про технічний стан кожного двигуна й системи керування в системи літака.

До складу розглянутої підсистеми входять наступні елементи, що беруть участь у забезпеченні зазначених $F_Б$: агрегат керування реверсивним пристроєм АУР-22, блок комутації й запуску БКЗ-148, блок комутації й керування реверсом тяги БКР-436, блок системи контролю й вібрації БСКВ-436; блок контролю й керування БУК-148, синусно-косинусний трансформатор ДБСКТ-250-1Ш, індикатор параметрів силової установки ИПСУ-148, модуль установки двигуна МДУ-1,2, механізм кінцевих вимикачів МКВ-48КС, механізм для автоматичного переміщення важелів керування МРД-27, два важелі керування двигуном РУД 1 та РУД 2, система вимірювання тиску СИД-3, двоканальний електронний блок керування ЭСУ-436. Розглянута підсистема взаємодіє з наступними підсистемами БІКС: комплексна система електронної індикації й сигналізації КСЭИС-148, обчислювальна система літаководіння ВСС-100, метеонавігаційна радіолокаційна станція МНРЛС «Буран», система керування загальнолітаковим обладнанням СУОСО-148, інформаційний комплекс висотно-швидкісних параметрів ИКВСП-148, система автоматичного керування польотом САУ-148, бортовий пристрій реєстрації БУР-92А, бортова система технічного обслуговування БСТО. Узагальнений вид структурної схеми взаємозв'язку даної апаратури представлений на рис. 1.

На рис. 2 представлена частина структурної схеми, яка відповідає за виконання $F_Б\, f^*_5$.

На другому етапі виконується визначення нормованого показника збитку для всіх функції розглянутої підсистеми (табл. 3), що може наступити в результаті відмови $F_Б$.

Після цього необхідно провести аналіз критичності задач для виконання $F_Б$, показник збитку для яких не дорівнює 0. Для спрощення процедури проведення даного етапу АКВЕ доцільним представляється виділення ряду підграфів $F_Б$ із загального графа розглянутої підсистеми БІКС Ан-148.

Наприклад, розглянемо критичну функцію f^*_5, для якої підграф буде мати вигляд, що представлений на рис. 3.

В результаті розкладання $F_Б\, f^*_5$ на множину простих критичних задач (КЗ) одержали наступний перелік (масив $M_{КЗ\,5}$):

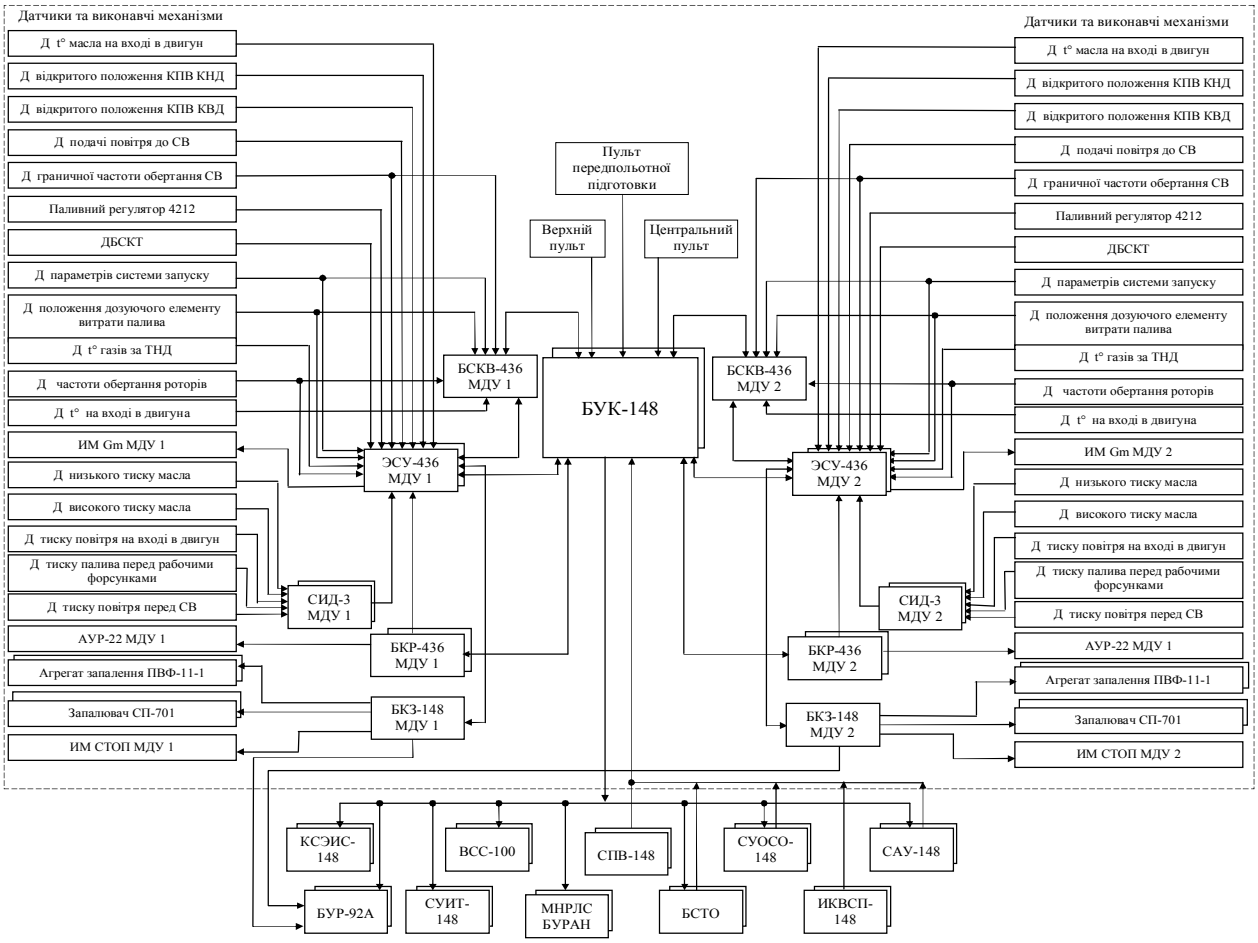

Рис. 1. Структурна схема взаємозв'язку обладнання САКСУ літака Ан-148

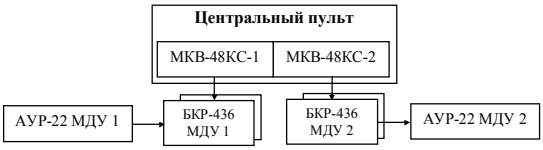

Рис. 2. Частина структурної схеми САКСУ БІКС Ан-148, що відповідає за виконання функції f^*_5

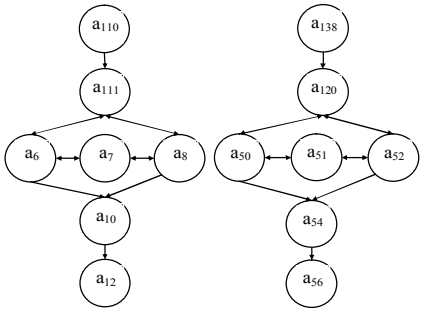

Рис. 3. Підграф $G'_5(a')$ для $F_Б$ f^*_5 підсистеми САКСУ БІКС Ан-148, що оцінюється

Z1 – встановлення реверсивного режиму за допомогою важелю реверса РЕВ1 і РЕВ2 і передача інформації про встановлений режим із МКВ-48 у БКР-436 МДУ 1(2);

Z2 – обробка керуючої команди в БКР-436 МДУ 1(2);

Z3 – видача керуючого сигналу із БКР-436 на АУР-22 відповідного МДУ.

Безпосереднє оцінювання питомої критичності всіх елементів, що входять у відповідні підграфи КЗ певної $F_Б$ відповідно до запропонованого методу оцінки проводиться у три етапи. Для САКСУ матриця критичності елементів $M_{КР\,5}$ підграфу $G'_5(a')$, що виконує $F_Б$ f^*_5, для КЗ із масиву $M_{КЗ\,5}$ і абсолютні значення критичності $m_{\Sigma k}$ елементів підграфа $G'_5(a')$ для виконання $F_Б$ f^*_5 представлені в табл. 1.

При цьому сумарне значення абсолютної критичності всіх елементів ділянки САКСУ БІКС для виконання $F_Б$ f^*_5 становить $m_{\Sigma k5} = 20$. Відповідно до виразу (1) розраховуються нормовані значення ступеня критичності кожного з елементів даної підсистеми БІКС для всіх n $F_Б$, представлені значеннями ν_{kn}. Для даної $F_Б$ f^*_5 одномірний масив ν_{k5} нормованих значень ступеня критичності кожного з елементів розглянутої ділянки САКСУ БІКС Ан-148 представлений в останньому рядку табл. 1.

Аналогічно для всіх $F_Б$ визначаються нормовані значення ступеня критичності кожного з елементів САКСУ БІКС, а також сумарні значення їхньої критичності для підсистеми, що дозволяє визначити перелік компонентів, що вимагають особливої уваги до забезпечення їхньої безвідмовності в процесі проектування й експлуатації.

У табл. 2 наведені значення ймовірностей відмови даних елементів.

Таблиця 1

Матриця критичності M_{KP5} елементів підграфа $G'_5(a')$ для КЗ із масиву M_{K35} ($F_Б$ f^*_5)

	a_6	a_7	a_8	a_{10}	a_{12}	a_{50}	a_{51}	a_{52}	a_{54}	a_{56}	a_{110}	a_{111}	a_{120}	a_{138}
Z1	0,5	1	0,5			0,5	1	0,5			1	1	1	1
Z2	0,5	1	0,5			0,5	1	0,5						
Z3	0,5	1	0,5	1	1	0,5	1	0,5	1	1				
$m_{\Sigma k5}$	1,5	3	1,5	1	1	1,5	3	1,5	1	1	1	1	1	1
ν_{k5}	0,075	0,15	0,075	0,05	0,05	0,075	0,15	0,075	0,05	0,05	0,05	0,05	0,05	0,05

Таблиця 2

Показники надійності елементів, що виконують f^*_5

	a_6	a_7	a_8	a_{10}	a_{12}	a_{50}	a_{51}	a_{52}	a_{54}	a_{56}	a_{110}	a_{111}	a_{120}	a_{138}
$P_{відм.max}$	0,11750	0,01135	0,11750	0,01135	0,10516	0,11750	0,01135	0,11750	0,01135	0,10516	0,07996	0,01135	0,01135	0,07996

Останнім етапом при проведенні аналізу критичності й оцінюванні функціональної безпеки розглянутої частини САКСУ БІКС Ан-148 є оцінка ризику й функціональної безпеки функцій безпеки.

Як було зазначено вище, однією із складових, що входить у поняття ризик, є ймовірність відмови $F_Б$, що визначається за допомогою методу оцінки структурної надійності використовуючи дані, наведені в табл. 3. У табл. 3 наведені результати оцінювання ФБ САКСУ БІКС Ан-148 для всіх $F_Б$ відповідно до запропонованого методу.

Таблиця 3

Результати оцінювання ФБ САКСУ БІКС Ан-148

	U_n	$\nu_{\Sigma n}$	P_{on}	R_n	$Fs(f^*_n)$
f^*_1	1	0,173	0,294	0,294	0,949
f^*_2	1	0,087	0,664	0,664	0,942
f^*_3	1	0,096	0,696	0,696	0,933
f^*_5	1	0,034	0,079	0,080	0,997
f^*_6	1	0,139	0,791	0,791	0,890
f^*_7	0,75	0,069	0,692	0,519	0,964
f^*_8	1	0,041	0,513	0,513	0,979
f^*_9	0,25	0,176	0,588	0,147	0,974
f^*_{10}	1	0,154	0,250	0,250	0,961
f^*_{11}	1	0,031	0,344	0,344	0,989

За результатами оцінки ФБ для всіх $F_Б$ БІКС АН-148 можна зробити висновок, що при великій кількості елементів, які входять у структурну схему виконання певної $F_Б$, результуючий показник питомої сумарної критичності має велике кількісне значення, а показник максимальної питомої критичності елемента може мати мале. В такому випадку показник ФБ для $F_Б$ визначений за окремим критичним елементом буде мати більше значення ніж показник, що визначений на основі питомої сумарної критичності всіх елементів, які виконують $F_Б$, який, до того ж, може бути і меншим за показники ФБ інших $F_Б$ даної підсистеми.

Висновки

У статті запропонований удосконалений метод аналізу й оцінювання функціональної безпеки, що дає можливість врахувати не тільки критичність відмов окремих елементів БІКС, що виконують функції безпеки, а й структурну надійність розглянутих підсистем. Для даного методу удосконалені правила визначення нормованого показника збитку при відмові тих або інших функцій, пов'язаних з безпекою БІКС ПС.

У результаті аналізу критичності окремих елементів БІКС для властивості функціональної безпеки з використанням запропонованого методу визначаються об'єктивні оцінки, що відображають важливість того або іншого елемента в процесі виконання (забезпечення) функції безпеки. Це дозволяє робити обґрунтований вибір елементів, забезпеченню безвідмовності яких необхідно приділяти найбільшу увагу на всіх етапах життєвого циклу подібного роду систем.

Результатом оцінювання функціональної безпеки БІКС є значення таких показників окремих функціональних підсистем, пов'язаних з безпекою ПС, як ризик і комплексний показник функціональної безпеки, який враховує сумарну питому критичність функцій безпеки у структурі підсистеми.

За фізичним змістом запропонований нормований комплексний показник ФБ дозволяє спрогнозувати зміни рівня функціональної безпеки БІКС при відмові тієї або іншої функції безпеки, а також провести ранжування критичних підсистем БІКС за ступенем їхнього впливу на ФБ ПС й порівняти різні за архітектурно-структурною побудовою варіанти

реалізації підсистем, що призначені для виконання однакових функцій.

Подальшу роботу необхідно спрямувати на вдосконалення методу забезпечення ФБ БІКС ПС на етапі їхнього проектування з урахуванням отриманих показників надійності й ФБ, що дозволить забезпечити необхідний рівень показників цих властивостей для систем, що проектуються. Крім того, необхідно розробити метод та відповідну інформаційну технологію забезпечення ФБ ІКС даного класу на етапі їх експлуатації (в польоті), що базуватиметься на проведенні архітектурно-структурної реконфігурації БІКС ПС по результатах оперативного контролю та оцінювання реального рівня ФБ їх окремих підсистем з метою досягнення необхідного або максимально-можливого рівня зазначеної властивості, а відповідно й безпеки польоту ПС.

Список літератури

1. ГОСТ Р МЭК 61508-4-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения: [введен 2008-06-01] – М.: ФГУП «СТАНДАРТИНФОРМ»,, 2008. – 28 с. [Национальный стандарт Российской Федерации].

2. ГОСТ Р 51901.1-2002 (МЭК 60300-3-9:1995). Менеджмент риска. Анализ риска технологических систем: [введен 2003-09-01] – М.: ИПК Издательство стандартов, 2006. – 32 с. [Национальный стандарт Российской Федерации].

3. ГОСТ Р МЭК 61508-7-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства: [введен 2008-09-01] – М.: ФГУП «СТАНДАРТИНФОРМ», 2008. – 74 с. [Национальный стандарт Российской Федерации].

4. Скляр В.В. Элементы методологии анализа функциональной безопасности информационно-управляющих систем / В.В. Скляр // Радіоелектронні і комп'ютерні системи. – 2009. – № 6. – С. 75-79.

5. Макаров Н.Н. Системы обеспечения безопасности функционирования бортового эргатического комплекса: теория, проектирование, применение / под ред. В.М. Солдаткина. – М.: Машиностроение – Полет, 2009. – 760 с.

6. Похил В.С. Метод анализа и оценивания функциональной безопасности авиационных бортовых информационно-управляющих систем / В.С. Похил, А.В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2009. – № 5(39). – С. 70-76.

7. ГОСТ 27.310-95. Анализ видов, последствий и критичности отказов. Основные положения: [чинний від 1997-01-01] – М.: ИПК Издательство стандартов, 1996. – 20 с. [Міждержавний стандарт].

8. Надежность и живучесть систем связи / Б.Я. Дудник, В.Ф. Овчаренко, В.К. Орлов и др.; под ред. Б.Я. Дудника. – М.: Радио и связь, 1984. – 216 с.

9. Самолет Ан-148-100. Стандартная спецификация. – К.: АНТК им. Антонова, 2004. – 490 с.

10. Новожилов Г.В. Безопасность полета самолета. Концепция и технология / Г.В. Новожилов, М.С. Неймарк, Л.Г. Цесарский. – М.: Машиностроение, 2003. – 144 с.

11. Похил В.С. Методы оценивания и обеспечения функциональной безопасности бортовых информационно-управляющих систем летательных аппаратов / В.С. Похил, А.В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2010. – № 8. – С. 104-109.

12. Похил В.С. Аналіз підходів до контролю й забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації / В.С. Похил // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2010. – Вип. 3(15). – С. 115-121.

Надійшла до редколегії 29.06.2010

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М. Є. Жуковського „ХАІ", Харків.

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД АНАЛИЗА И ОЦЕНИВАНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ БОРТОВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ ВОЗДУШНОГО СУДНА

В.С. Похил

Приведен аналитический обзор понятия функциональной безопасности. Отмечена важность рассмотрения функциональной безопасности как свойства информационно-управляющей системы (ИУС). Предложен усовершенствованный метод анализа и оценивания функциональной безопасности подсистем бортовой ИУС воздушного судна. Рассмотрен пример его применения для оценивания функциональной безопасности системы автоматического управления силовой установкой Ан-148.

Ключевые слова: *бортовая информационно-управляющая система, функциональная безопасность, риск, ущерб, метод анализа и оценки, суммарная удельная критичность элемента.*

THE ENHANCED METHOD OF THE FUNCTIONAL SAFETY OF THE AIRCRAFT ONBOARD INFORMATION-CONTROL SYSTEMS ANALYSIS AND ESTIMATION

V.S. Pohyl

A analytical survey of the concept of functional safety is brought. Importance of consideration of functional safety as properties of the information-control systems (ICS) is marked. The enhanced method of the functional safety of the aircrafts onboard ICS analysis and estimation is offered. The example of its application is considered for the estimation of the functional safety for the Antonov-148 aircraft turbojet engines automatic control system.

Keywords: *onboard information-control system, functional safety, risk, harm, analysis and estimation method, summary specific criticism of the ICS elements.*