

УДК 004.03:621.38

В.С. Похил

Військовий інститут телекомунікацій і інформатизації НТУУ «КПІ», Україна

УДОСКОНАЛЕНИЙ МЕТОД ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БОРТОВИХ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ АВІАЦІЇ НА ЕТАПІ ПРОЕКТУВАННЯ

Наведено підхід до забезпечення функціональної безпеки (ФБ) бортової інформаційно-керуючої системи повітряного судна (БІКС ПС), який заснований на застосуванні уніфікованого інформаційно-обчислювального ядра, що у випадку відмов в процесі функціонування може бути реконфігуроване. Запропоновано вдосконалений метод забезпечення ФБ БІКС ПС на етапі проектування, який дозволить врахувати ступінь критичності окремих елементів системи. Розглянуто інформаційну технологію забезпечення заданого рівня ФБ БІУС ПС на етапі її проектування.

Ключові слова: бортова інформаційно-керуюча система, функціональна безпека, метод забезпечення, модель функціонування, обчислювальне ядро, реконфігурація, інформаційна технологія.

Вступ

Результати аналізу даних про авіаподії за останні 6 років свідчать про значне погіршення стану безпеки польотів, а аналіз причин виникнення подій і інцидентів у цивільній авіації за останні 10 років свідчить про те, що приблизно 80% з них відбулися з вини екіпажів і диспетчерів керуючих повітряним рухом повітряних суден (ПС). На сьогоднішній день розробники ПС намагаються автоматизувати все більше число функцій по керуванню літаком на різних етапах польоту, поклавши їх на бортові інформаційно-керуючі системи (БІКС) ПС. Це, у свою чергу, призводить до підвищення їхньої відповідальності за функціональну безпеку (ФБ) ПС, ускладненню а отже, й підвищенню вимог до надійності й ФБ даних систем.

Аналіз досвіду експлуатації вітчизняних і закордонних ПС (розбір ситуацій, що загрожують безпеці польоту, виявлення причин створення особливих і ситуацій, що приводять до катастроф, на літаках, оцінка досягнутого рівня надійності й безпеки польоту) є одним з напрямків забезпечення необхідних характеристик надійності й безпеки польоту ПС. Запобігання в нових проектах БІКС ПС раніше виявлених недоліків є одним з методів підвищення рівня надійності й безпеки польотів, так званий метод експертних знань, що широко застосовується при створенні нових ПС [1]. Іншим напрямком, що дозволяє на ранніх етапах проектування забезпечувати необхідний рівень надійності й функціональної безпеки (ФБ) (як частини загальної безпеки) БІКС, є розрахунково-аналітичний підхід до прогнозування всіх можливих потенційних відмов, оцінювання ступеня їхньої критичності, імовірності їхньої появи й визначення можливих катастрофічних наслідків. У випадку неузгодженості результатів аналізу з необ-

хідним рівнем надійності й ФБ здійснюються конструктивні зміни БІКС ПС, спрямовані на виконання заданих вимог.

Аналіз літератури. В [1] розглядається процес забезпечення вимог надійності й безпеки польоту ПС на етапі проектування. У книзі [2] описані результати розробки систем забезпечення безпеки функціонування бортових ергатичних комплексів (екіпаж – бортове обладнання – повітряне судно), які представлені у вигляді автономних ІКС. У статті [3] наведений аналіз існуючих підходів до забезпечення ФБ систем, пов'язаних з безпекою. Результат аналізу зазначених джерел показав, що вони не дають можливості комплексно забезпечити ФБ, з огляду на такі поняття, як ступінь критичності окремих елементів, ризик, збиток і ймовірність відмови функцій БІКС ПС. В [4] запропонований удосконалений метод аналізу й оцінки ФБ БІКС ПС, показники надійності й ФБ якого повинні враховуватися в перспективних методах забезпечення необхідного (заданого) рівня ФБ БІКС ПС на етапі проектування системи.

Незважаючи на різноманіття аспектів проблеми підвищення безпеки польотів ПС, одним з найбільш важливих є **завдання** забезпечення необхідного (заданого) або максимально можливого рівня надійності й ФБ БІКС ПС на етапах їх проектування, створення, випробувань та піддослідної експлуатації.

Метою статті є описання підходу до забезпечення ФБ БІКС ПС, що заснований на застосуванні у її складі уніфікованого обчислювального ядра, що здатне реконфігуруватися, а також удосконаленого методу забезпечення функціональної безпеки бортових інформаційно-керуючих систем ПС на етапі їхнього проектування, що дозволить врахувати ступінь критичності окремих елементів їхньої структурно-функціональної схеми.

Підхід до забезпечення ФБ БІКС ПС на основі застосування уніфікованого обчислювального ядра

Для підвищення рівня ФБ функціональної БІКС, її обчислювальне ядро (ОЯ) повинне піддаватися реконфігурації у випадку відмови тих або інших обчислювальних блоків (ОБ). Реконфігурація у випадку відмов в ОЯ полягає у виключенні з роботи елементів ОЯ, що відмовили, й зміні його архітектури, тобто повинен відбутися перерозподіл ресурсів і обчислювальних завдань між працездатними елементами системи з метою продовження обчислень. При цьому необхідно врахувати наявність реальних обмежень можливості введення надлишковості до складу ОЯ БІКС, обумовлених обмеженими масогабаритними, енергетичними й часовими (оперативності) показниками для бортових систем ПС. Нижче представлений підхід до моделювання процесу функціонування обчислювального ядра БІКС ПС на основі групи уніфікованих ОБ, що його складають.

Архітектура бортових ІКС, до складу яких входить ОЯ, представляється у вигляді композиції множини обчислювальних блоків (ОБ) ядра, пристроїв комутації (ПК) пакетів даних і мереж обміну інформацією між ними та периферійним обладнанням (датчиками, індикаторами та виконуючими механізмами/автоматами) бортової авіоники. У таких системах всі основні ресурси (не тільки арифметико-логічні й комутуючі пристрої, а також пам'ять і засоби керування) є логічно, і технічно розподіленими.

Обчислювальне ядро БІКС компонується з однорідних ОБ і реконфігуратора. Будемо вважати, що БІКС перебуває в стані $k \in E_0^N = \{0, 1, \dots, N\}$, якщо в ній є k працездатних ОБ.

Для спрощення будемо розглядати лише ОБ, розуміючи, що всі міркування й вирази можуть бути застосовані й для сучасних ПК.

Сучасні обчислювальні системи (ОС) в більшості практичних випадках збоїв в роботі є відновлюваними. Будемо вважати, що відновлювальні роботи у ОЯ БІКС здійснюються деякою системою відновлення, що складається з m пристроїв відновлення (ПВ), $1 \leq m \leq N$. Кожен ПВ в будь-який момент може робити перезапуск після збою тільки одного ОБ.

Для формування в системі віртуальних конфігурацій є спеціальні (апаратно-програмні) засоби, що утворюють реконфігуратор. Він призначений для виконання наступних функцій:

- виключення з ОЯ розглянутої БІКС ОБ, які відмовили, і включення їх в нього після відновлення;
- формування ОЯ БІКС із ОБ, які залишилися працездатними і знову відновилися;
- перетворення паралельної програми, що адаптується, (потоків інформації) з метою досягнення

відповідності між числом її гілок (шляхів) і числом ОБ обчислювального ядра;

- впровадження перетвореної програми (напрямок перерозподіленого інформаційного потоку) у ядро з новою структурою й організації її (його) проходження.

Обчислювальні системи із програмованою структурою мають гнучкі структурні можливості [5] для такої віртуалізації.

Континуальна модель функціонування ОЯ БІКС ВС. Математичне сподівання $N(i, t)$ числа працездатних ОБ визначає в момент часу $t \geq 0$ продуктивність ОЯ і ємність його розподіленої пам'яті; i початковий стан ОЯ, очевидно, що $N(i, 0) = i$, $i = E_0^N$. Саме $N(i, t)$ ОБ становлять у середньому в момент часу $t \geq 0$ обчислювальне ядро БІКС.

Продуктивність ОЯ БІКС у будь-який момент часу $t \geq 0$ визначають $N(i, t)$ машин обчислювального ядра, тобто ті працездатні ОБ, які безпосередньо використовуються для реалізації паралельної програми, що адаптується. У випадку відмови ОБ "залишає" обчислювальне ядро й береться на облік реконфігуратором ОЯ з інтенсивністю відмов ОБ λ . Нехай $L'(i, t)$ – середнє число ОБ, що відмовили, які враховуються реконфігуратором ОЯ в момент $t \geq 0$, $i = E_0^N$. Реконфігуратор виключає з обчислювального ядра ОБ, що відмовили, і утворює із решти працездатних ОБ зв'язну підсистему, скорочує число паралельних гілок виконання програмного забезпечення (ПЗ) і організовує його обробку в обчислювальному ядрі з новою структурою (топологією) і архітектурою (рис. 1).

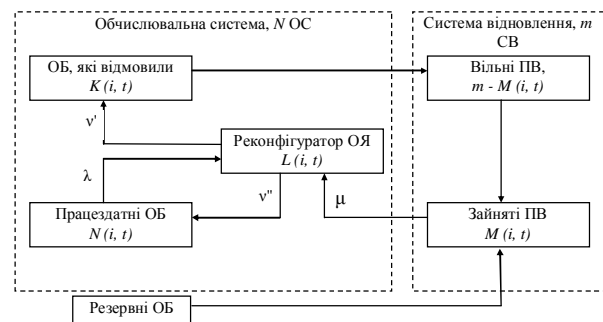


Рис. 1. Узагальнена модель функціонування обчислювального ядра БІКС ПС

У результаті виконання таких функцій реконфігуратор з інтенсивністю v' "перемікає" ОБ, які відмовили, із ОЯ в групу обчислювальних блоків, що підлягають відновленню. Нехай $K(i, t)$ – математичне сподівання числа ОБ, які відмовили, і враховуються системою відновлення.

Припустимо, $M(i, t)$ – середнє число пристроїв, зайнятих відновленням ОБ, які відмовили; μ – інтенсивність відновлення ОБ, які відмовили, одним ПВ. Після відновлення обчислювальні блоки беруться на

облік реконфігуратором ОЯ БІКС. Нехай $L(i, t)$ – середнє число відновлених ОБ, взятих на облік реконфігуратором обчислювального ядра. Включення відновлених ОБ до складу ядра здійснюється з інтенсивністю v ". Середній час $1/v$ " такого включення залежить від часу утворення зв'язної підмножини блоків з існуючого ядра й відновлених ОБ, часу перенастроювання паралельного ПЗ на більше число гілок і часу запуску цього ПЗ на заново створеному ядрі.

При створенні ОЯ БІКС, у загальному випадку використовуються віртуальні відновлюючі пристрої і "ремонт" виявлених ОБ, які відмовили, зводиться до їхньої заміни на ОБ із резерву. У таких випадках інтенсивність μ сприймається як середнє число ОБ резерву, які включаються в одиницю часу одним віртуальним ПВ до складу обчислювального ядра БІКС.

Дійсною є наступна рівність:

$$L(i, t) + K(i, t) + N(i, t) = N,$$

де $L(i, t) = L'(i, t) + L''(i, t)$ – середнє число ОБ, з якими працює реконфігуратор ОЯ БІКС ПС.

Метод забезпечення ФБ БІКС ПС на етапі її проектування

Керування проектуванням є важливим процесом менеджменту надійності, створюваних ІКС, що дозволяє забезпечувати їхню розробку відповідно до цілей надійності. Дії по керуванню проектуванням містять у собі встановлення правил і рекомендацій, спрямованих на забезпечення безпечної експлуатації, виділення фізичних і функціональних блоків, забезпечення модульності, проведення оперативного й гарантованого обслуговування ІКС. Ці дії дозволяють забезпечити відповідність продукції обов'язковим вимогам [6].

Сутність пропонованого методу забезпечення ФБ БІКС ПС зводиться до досягнення максимальної ефективності проведення наступних груп заходів, спрямованих на підвищення ФБ БІКС ПС:

1. Підвищення надійності й стійкості інформаційно-обчислювальних процесів у відповідних підсистемах БІКС, що виконує функції безпеки, шляхом внесення програмно-алгоритмічної, інформаційної, технічної, часової або якоїсь іншої надлишковості.

2. Застосування нових технологічних рішень для елементів, які мають максимальні значення кратності критичності за результатами аналізу ФБ даної критичної підсистеми для збільшення надійності виконання ними покладених на них завдань і функцій.

3. Зміна структурно-архітектурної або алгоритмічної організації найбільш критичних інформаційно-обчислювальних процесів у БІКС ПС з метою зменшення значень кратності критичності елементів, що входять у критичні підсистеми БІКС. При цьому необхідно намагатися досягти максимального

зменшення значень кратності критичності для елементів, що мають найменші кількісні значення показників надійності й/або максимальні значення кратності критичності в підсистемах.

По результатам застосування указаних заходів по підвищенню ФБ окремих підсистем і БІУС ПС в цілому проводиться оцінка їх ФБ і визначається різниця в отриманих значеннях відповідних показників ризику та ФБ для кожної із критичних функцій, після чого проводиться аналіз ефективності прийнятих заходів.

Забезпечення надійності підсистем БІКС ПС на етапі її проектування повинне здійснюватись за наступними основними напрямками:

- забезпечення надійності апаратної частини системи;
- забезпечення надійності програмного забезпечення;
- забезпечення надійного функціонування програмно-апаратного комплексу з урахуванням помилок при взаємодії.

Апаратна надійність припускає здатність технічних засобів БІКС зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції безпеки в заданих режимах і умовах застосування, технічного обслуговування й ремонту.

Для забезпечення надійності БІКС ПС необхідно насамперед використати високонадійні елементи системи, способи й шляхи досягнення заданого ступеня надійності стосовно до апаратної частини, а також висококваліфіковані збирання й обслуговування.

У результаті проведеного аналізу ФБ БІКС ПС в [4] отримані показники ступеня критичності її окремих елементів, які дозволяють визначити найбільш „навантажені” елементи у підсистемах БІКС, і на етапі проектування вжити заходів для підвищення їх характеристик надійності. Це здійснюється шляхом вибору елементів з більшим напрацюванням на відмову, введенням у систему додаткових елементів понад мінімально необхідну кількість або спеціальних конструктивних рішень для виконання функції по призначенню. Для підвищення надійності можуть використовуватись введення наступних видів надлишковості:

- внутрішньоелементна надлишковість (використання елементів з більшою ймовірністю безвідмовної роботи);
- структурна надлишковість (застосування додаткових (надлишкових) шляхів передачі сигналів та даних в системі);
- часова надлишковість (полягає в наявності додаткового часу, що дозволяє реалізувати ті ресурси по підвищенню відмовостійкості, які є в даній системі (реконфігурація, повторення обчислень),

оскільки для цього потрібний додатковий час);

– інформаційна надлишковість (виражається наявністю в системі додаткової інформації, що дозволяє при відмові елемента системи зберегти або відновити цілісність оброблюваної інформації й підтримати в утвореній ситуації правильне виконання покладених на систему функцій).

На практиці можливості застосування надлишковості обмежуються допустимими значеннями маси, об'єму, енергоспоживання, вартості або інших параметрів пристроїв резервування. Тому доводиться в процесі експлуатації вирішувати завдання оптимального введення надлишковості, що має два аспекти: забезпечення максимального значення показників надійності при заданому значенні обмежуючого фактора й забезпечення заданих значень показників надійності при мінімальному значенні обмежуючого фактора.

Раціональне розміщення елементів підсистем також дає можливість нормально функціонувати в різних екстремальних режимах роботи (рознесення в просторі найбільш важливих елементів БІКС, вибір найбільш захищеного місця їх розташування і з урахуванням вібрацій).

Надійність програмного забезпечення припускає його здатність протягом необхідного часу правильно виконувати задані функції під впливом зовнішніх впливів у реальних умовах експлуатації. Інформація, що використовується програмним забезпеченням, може піддаватися спотворенню на різних етапах:

- збору інформації, яка поступає від різноманітних датчиків, оператора, підсистем і служб об'єкта, зовнішніх служб;
- обробки й аналізу інформації;
- видачі інформації операторові та на виконавчі механізми.

На всіх цих етапах інформація піддається всіляким деструктивним впливам, що спотворюють її, і в остаточному підсумку це відбивається на роботі програмного забезпечення БІКС. Підвищення надійності програм забезпечується за рахунок включення в систему засобів виявлення й усунення їхніх відмов, застосування засобів виявлення й усунення помилок і відмов елементів програмного середовища.

Ці методи дозволяють за допомогою різних видів надлишковості підвищити стійкість програмного забезпечення до різного виду впливів. Питання забезпечення функціональної безпеки й керування ризиком програмного забезпечення інформаційно-керуючих систем розглянуті в [7 – 11].

У якості нових технологічних рішень для підвищення надійності функціонування обчислювальних блоків підсистем БІКС можуть використовуватися ПЛІС-системи (програмовані логічні інтегральні схеми), які завдяки своїй гнучкій структурі до-

зволяють не тільки реалізовувати складні проекти на одному кристалі й проводити багаторівневу верифікацію на всіх етапах розробки, але й дозволяють здійснювати оперативну реконфігурацію внутрішньої архітектури в процесі їхнього функціонування. ПЛІС-системи знаходять широке застосування в авіаційних системах, розроблених в Україні й інших країнах. Компанія Boeing має досвід застосування мікросхем Xilinx у літаках Boeing 737, 777 у системі обробки зображення. Одне із провідних національних підприємств-розробників систем керування для авіаційних проектів – Науково-технічне спеціалізоване конструкторське бюро "Полісвіт" об'єднання "Комунар" (м. Харків) більше 6 років використовує для розробок бортових цифрових систем ПЛІС виробництва фірм Altera, Xilinx. До теперішнього часу накопичений багаторічний досвід їхнього застосування в різних модифікаціях бортових систем керування й контролю в літаках Ан-70, Ан-140, Ан-148, Ту-204, Ту-214, Ту-334.

Інформаційна технологія забезпечення ФБ БІКС ПС на етапі проектування

Ядром інформаційної технології забезпечення заданого рівня функціональної безпеки (ІТЗФБ) БІКС ПС є інформаційна технологія аналізу й оцінювання ФБ БІКС ПС. Архітектура прикладного ПЗ, що реалізує ІТ оцінювання й забезпечення ФБ БІКС ПС, наведена на рис. 2 і представлена наступними системами:

- система керування базою вихідних даних (СКБВД), що забезпечує відбір початкових даних (наприклад, значень параметрів використовуваних елементів, вихід з ладу яких може негативно вплинути на загальний стан системи, вимоги до їхньої надійності й т.д.) з деякої БД для їхньої наступної обробки;
- система керування базою моделей і методів (СКБММ), що забезпечує вибір необхідних методів оцінювання й забезпечення ФБ для обробки даних, отриманих від СКБВД;
- система керування інтерфейсом, що забезпечує відображення вихідної інформації в зрозумілій для користувача формі, а також дозволяє користувачеві коректувати роботу СКБВД і СКБММ.

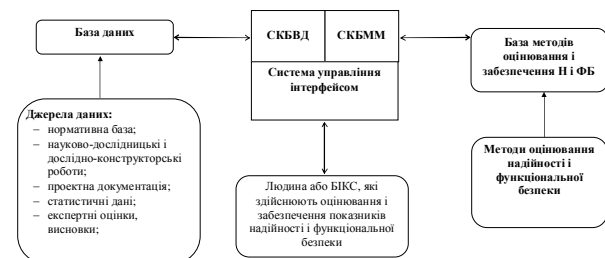


Рис. 2. Архітектура прикладного програмного забезпечення, яке реалізує інформаційну технологію оцінювання і забезпечення ФБ БІКС ПС

Запропонована в цьому випадку ІТ оцінювання й забезпечення призначена для використання на етапах розробки та модернізації БІКС ПС. Тому ключовими складовими є конкретні інформаційні потоки і їхнє перетворення (тобто процес перетворення інформації), а також математичний апарат і відповідні програмні засоби. Ці складові мають безпосереднє відношення до визначення оцінювання й

забезпечення функціональної безпеки складових БІКС.

На рис. 3 представлена схема взаємодії інформаційних потоків, процесів та відповідних інструментальних засобів (ІЗ) ІТ оцінювання надійності й ФБ БІКС відповідно до розроблених моделей і методу оцінювання ФБ, а також визначення найбільш «вразливих» елементів і підсистем.

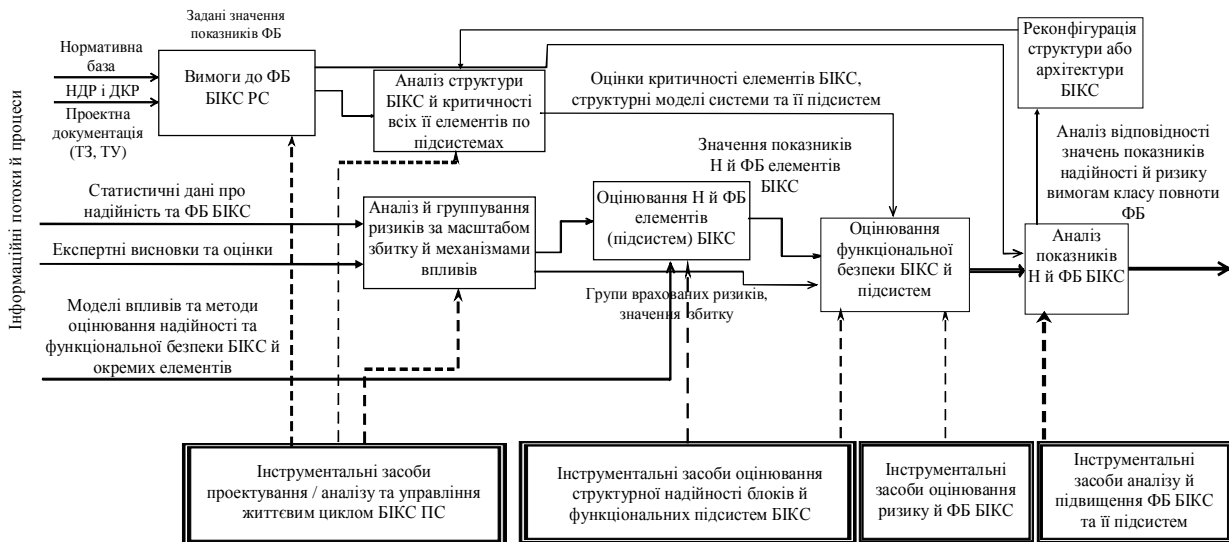


Рис. 3. Концептуальна модель ІТ забезпечення функціональної безпеки БІКС ПС при її проектуванні

Вихідними даними для оцінювання й забезпечення ФБ БІКС є: нормативна база, вимоги проектно-ї документації (технічного завдання – ТЗ, технічних умов – ТУ), науково-дослідні й дослідно-конструкторські роботи, статистичні дані за результатами експлуатації в подібних умовах.

Вимоги до функціональної безпеки БІКС визначаються вимогами ТЗ і нормативних документів і задаються на основі аналізу призначення й функцій, а також структури побудови БІКС, з урахуванням накопиченого досвіду попередніх розробок.

Результатом виконання першого етапу й вихідними даними для оцінки надійності й функціональної безпеки елементів підсистем БІКС є: оцінки критичності елементів системи для виконання найбільш важливих функцій системи, групи ризиків по масштабу збитку й механізмам впливу в групи. Результатом цього етапу є одержання оцінок критичності елементів БІКС, структурні моделі системи і її підсистем.

На другому етапі виконання ІТЗФБ проводиться оцінювання надійності й функціональної безпеки підсистем БІКС, у результаті чого одержують набір показників надійності елементів і функціональної безпеки підсистем БІКС ПС, необхідних для проведення третього етапу оцінювання БІКС ПС.

Наступний етап безпосередньо реалізується на основі розробленого методу оцінки функціональної безпеки БІКС у цілому з урахуванням критичності,

ризиків і збитку можливого у випадку невиконання функції окремими підсистемами БІКС ПС, шляхом аналізу отриманих оцінок показника функціональної безпеки відповідних підсистем БІКС ПС.

Четвертим етапом роботи запропонованої ІТЗФБ є аналіз отриманих показників надійності й функціональної безпеки, шляхом порівняння їх із заданими вимогами.

Результатом даного етапу, крім цього, є визначення переліку найбільш критичних елементів БІКС, які роблять найбільший внесок у безпеку системи в цілому.

П'ятий і заключний етап пов'язаний з реконфігурацією і наступною ітераційною процедурою аналізу й оцінювання ФБ для досягнення оптимального варіанта архітектурно-структурної технологічної побудови БІКС із урахуванням прийнятих обмежень.

Висновки

У статті описаний підхід до забезпечення функціональної безпеки БІКС ПС, що заснований на застосуванні уніфікованого, здатного до реконфігурації, інформаційно-обчислювального обчислювального ядра використовуваного в БІКС ПС, а також представлений удосконалений метод забезпечення необхідного рівня ФБ БІКС ПС на етапі їхнього проектування, що дозволяє врахувати ступінь критичності окремих елементів їх структурно-функціональної схеми.

Також у статті наведена ІТ забезпечення заданого рівня ФБ БІКС ПС, що призначена для використання на етапі проектування. Результати роботи ІТЗФБ БІКС надалі повинні використовуватися в ІТ підтримки прийняття рішень для екіпажа по забезпеченню або підвищенню рівня функціональної безпеки подібного класу систем на етапі експлуатації (в процесі польоту).

Подальші дослідження необхідно направити на розробку методу забезпечення функціональної безпеки БІКС ПС на етапі їхньої експлуатації (під час передпольотної підготовки та в польоті), що буде базуватися на проведенні ре конфігурації архітектурно-топологічної схеми інформаційно-обчислювальних та інформаційно-керуючих процесів в уніфікованому обчислювальному ядрі та в основних функціональних підсистемах БІКС ПС по результатах оперативного контролю в режимі жорсткого реального часу реального рівня ФБ їх окремих функціонально-інформаційних схем і потоків.

Список літератури

1. Новожилів Г.В. *Безопасность полета самолета. Концепция и технология* / Г.В. Новожилів, М.С. Неймарк, Л.Г. Цесарский. – М.: Машиностроение, 2003. – 144 с.
2. Макаров Н.Н. *Системы обеспечения безопасности функционирования бортового эргатического комплекса: теория, проектирование, применение* / Н.Н. Макаров; под ред. В.М. Солдаткина. – М.: Машиностроение – Полет, 2009. – 760 с.
3. 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: зб. наук. праць ЦНДІ НіУ. – К.: ЦНДІУ, 2010. – Вип. 3 (15). – С. 115-121..
4. Похил В.С. *Удосконалений метод аналізу й оцінювання функціональної безпеки бортових інформаційно-*

керуючих систем повітряного судна / В.С. Похил // Системи озброєння і військова техніка. – 2010. – № 2(22). – С. 136-142.

5. Хорошевский В.Г. *Модели функционирования большихмасштабных распределенных вычислительных систем* / В.Г. Хорошевский // Электросвязь. – 2004. – № 10. – С. 30-34.

6. ГОСТ Р 51901.3-2007 (МЭК 60300-2:2004). *Менеджмент риска. Руководство по менеджменту надежности*: [чинний від 2007-27-12] – М.: ИПК Издательство стандартов, 2007. – 45 с. [Національний стандарт Російської Федерації].

7. ГОСТ Р ИСО/МЭК 16085-2007. *Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения*: [чинний від 2008-09-01] – М.: ФГУП «СТАНДАРТИНФОРМ», 2008. – 32 с. [Національний стандарт Російської Федерації].

8. ГОСТ Р МЭК 61508-3-2007. *Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению*: [введен 2007-27-12] – М.: ИПК Издательство стандартов, 2008. – 38 с. [Національний стандарт Російської Федерації].

9. Липаев В.В. *Функциональная безопасность программных средств* / В.В. Липаев. – М.: Синтез, 2004. – 348 с.

10. Липаев В.В. *Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств* / В.В. Липаев // Информационный бюллетень „Jet Info”. – 2003. – № 3 (130). – 27 с.

11. Липаев В.В. *Функциональная безопасность программных средств* / В.В. Липаев // Информационный бюллетень „Jet Info”. – 2004. – № 8 (135). – 28 с.

Надійшла до редколегії 30.07.2010

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

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД И ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ БОРТОВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ АВИАЦИИ НА ЭТАПЕ ПРОЕКТИРОВАНИЯ

В.С. Похил

Приведен подход к обеспечению функциональной безопасности (ФБ) бортовых информационно-управляющих систем воздушных судов (БИУС ВС), который основан на применении унифицированного информационно-управляющего ядра, который в случае отказа может быть реконфигурирован в процессе функционирования. Предложен усовершенствованный метод обеспечения ФБ БИУС ВС на этапе проектирования, который позволит учесть степень критичности отдельных элементов системы. Рассмотрена информационная технология обеспечения заданного уровня ФБ БИУС ВС на этапе проектирования.

Ключевые слова: бортовая информационно-управляющая система, функциональная безопасность, метод обеспечения, модель функционирования, реконфигурируемое вычислительное ядро, информационная технология.

ENHANCED METHOD AND INFORMATION TECHNOLOGY OF SUPPORT THE FUNCTIONAL SAFETY OF THE AIRCRAFT ONBOARD INFORMATION-CONTROL SYSTEMS AT DESIGN PHASE

V.S. Pohyl

The approach to support the functional safety (FS) of the aircraft onboard information-control system (OICS) which is based on using application of the unified information-operating kernel which can be reconfigured during functioning in default is offered. The enhanced method of support the FS of the aircraft OICS, which will allow including degree of criticality of separate elements of system, at design phase is offered. The information technology of support the set level FS of the aircraft OICS at design phase is considered.

Keywords: onboard information-control system, functional safety, method of support, functioning model, reconfigured computing kernel, information technology.