УДК 629.7.05 + 004.05

В.С. ХАРЧЕНКО[1], М.В. ЗАМИРЕЦЬ[2], С.О. ЗАСУХА[3], Ю.Л. ПОНОЧОВНИЙ[4]

[1]*Національный аерокосмічний університет ім. Н.Є. Жуковського "ХАІ", Україна*
[2]*Науково-дослідний технологічний інститут приладобудування, Харків, Україна,*
[3]*Державне космічне агентство України, Київ*
[4]*Військовий інститут телекомунікацій й інформатизації НТУ України „КПІ“, Київ*

ЕЛЕМЕНТИ МЕТОДОЛОГІЇ ОПЕРАТИВНОЇ КОРИГУВАЛЬНОЇ ВЕРИФІКАЦІЇ ПРОГРАМНИХ ЗАСОБІВ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ КОСМІЧНИХ АПАРАТІВ

Проведений аналіз програмного забезпечення (ПЗ) інформаційно-управляючих систем (ІУС) космічних систем (КС) як об'єкта верифікації, нормативної бази й існуючих методів верифікації ПЗ КС. Уведене поняття оперативної коригувальної верифікації (ОКВ), яка може проводитися за різними сценаріями для функцій різного рівня критичності. Визначені етапи й операції верифікації ПЗ ІУС КС на різних етапах. Даний детальний опис операцій етапу розробки ПЗ ІУС КС. Даний формальний опис цілей верифікації ПЗ ІУС КС. Уточнені цілі оперативної коригувальної верифікації ПЗ в польоті, і запропонований теоретико-множинний опис функцій з урахуванням їх критичності й цілей ОКВ. Описані сценарії й показники для оцінки готовності ІУС КС при реалізації ОКВ. Даний короткий опис моделей готовності. Визначені поняття стратегії ОКВ та особливості її формування. Проведено розробку та дослідження моделі готовності однієї з систем з ОКВ.

Ключові слова: *ІУС космічних систем, програмне забезпечення, оперативна коригувальна верифікація, моделі готовності.*

1. Вступ. Проблема верифікації програмного забезпечення ІУС космічних систем при розробці та застосуванні

1.1. Безпека космічних систем і надійність програмних засобів

Функціональні можливості й безпека космічних апаратів і ракетно-космічних комплексів (далі космічних систем – КС) суттєво залежать від якості й надійності їхніх комп'ютерних наземних і бортових інформаційно-управляючих систем (ІУС). У свою чергу, програмні засоби визначають ступінь досконалості й суттєво впливають на технічні характеристики ІУС КС на всіх етапах застосування.

З іншого боку, як ІУС, так і їхні програмні засоби можуть створювати й створюють додаткові дефіцити безпеки в різних критичних додатках, у тому числі космічних. Про це говорять результати досліджень, наведені в [1]. В 90-ті роки минулого сторіччя близько 20% аварій ракетно-космічної техніки було пов'язане з відмовами ІУС, а більше 80% цих відмов обумовлене дефектами ПЗс. За перше десятиліття 21-го століття статистика ще більш переконлива: 27% відмов космічних апаратів, які стали фатальними або обмежили можливості їхнього застосування, були пов'язані з відмовами апаратних (6%) і програмних (21%) засобів. Для відмов ракетоносіїв – схожі дані: 26% відмов викликані відмовами ІУС, у тому числі 6% апаратними й 20% програмними засобами.

Таким чином, кожні шоста й п'ята відмова в передостаннє й останнє десятиліття відповідно були викликані дефектами програмних засобів. Напрошується висновок, що в умовах збільшення складності ІУС КС надійність їхніх програмних засобів, підтримувана стандартними рішеннями, досягала деякого гранично досяжного значення, й потрібне прийняття додаткових принципово інших заходів щодо вдосконалювання процесів створення й супроводу програмного забезпечення (ПЗ).

Одним з важливих напрямків у цьому зв'язку є підвищення якості й гнучкості процедур верифікації програмного забезпечення з урахуванням специфіки розробки й застосування ІУС КС. ПЗ, як відомо, включає програмні засоби (ПЗс) і комплект документації, тому, коли говориться про надійність і функціональну безпеку як про властивості, їх слід відносити до ПЗс (як продукту й компоненту ІУС), а коли мова йде про процеси розробки й верифікації, вони адресуються до ПЗ, оскільки документування є їхньою обов'язковою складовою [2].

1.2. Аналіз нормативної бази верифікації ПЗ ІУС КС

Верифікація – це процес визначення того, чи задовольняють програмні продукти, які є результатом деяких дій, вимогам і умовам, накладеним на них попередніми діями [2, 3]. З метою досягнення найбі-

льшої ефективності (з погляду рівня невиявлених дефектів або підтвердження припустимого ризику їхньої наявності на одиницю витрат) верифікація проводиться з використанням широкого арсеналу методів і засобів. Верифікація може включати аналіз, огляд, тестування та інші методи, описані в міжнародних і національних нормативних документах, що створюють нормативну базу для ПЗ ІУС КС та інших критичних додатків. Вона проаналізована, зокрема, в [4].

Визначальними є стандарти, розроблені Європейською кооперацією з космічної стандартизації (European Cooperation for Space Standardization – ECSS) серій E-10, E-40, Q-80, а саме:

- ECSS- E- 40A "Розробка космічних систем. Програмне забезпечення" і його модифікація ECSS-E-40-1B "Розробка космічних систем. Програмне забезпечення – Частина 1: Принципи й вимоги";

- ECSS- E-10-02A "Розробка космічних систем – Верифікація";

- ECSS- Q- 80B "Гарантія космічних виробів – Гарантія програмного забезпечення".

Стандарти ECSS-E-40A, ECSS-E-40-1B засновані на положеннях ISO/IEC 12207:1995 і описують процеси життєвого циклу програмного забезпечення стосовно до космічних систем.

У рамках Державного космічного агентства України формується галузева нормативна база, гармонізована зі стандартами ECSS, що враховує стандарти, введені IEC і IAEA для ПЗ ІКС, важливих для безпеки АЕС [5-8]. У цю базу входять нормативні документи, що визначають:

- регулюючі вимоги до ПЗ ІУС КС, включаючи вимоги до функціональної безпеки;

- процеси життєвого циклу програмно-технічних комплексів (ПТК) КС;

- основні положення, що відносяться до гарантоздатності ПТК КС;

- методи оцінки якості ПЗ ІУС КС.

У стадії експертизи знаходиться документ, що визначає цілі, процеси й методи верифікації ПЗ ІУС КС [9]. Таким чином, можна говорити про необхідність реалізації положень створюваної нормативної бази.

1.3. Особливості верифікації ПЗ ІУС КС

Аналіз досвіду застосування ІУС КС [4,10,11] дозволяє відзначити низку особливостей, що відносяться до верифікації ПЗ ІУС КС:

1) для деяких систем повну верифікацію функцій неможливо зробити в повному обсязі в наземних умовах внаслідок їхньої специфіки, пов'язаної з:

а) неможливістю в повному обсязі імітувати умови польоту й забезпечити перевірку завдань, виконуваних на борту при старті, орбітальному польоті й посадці;

б) наявністю фактора невизначеності, що відноситься як до умов польоту, так і до розв'язуваних задач, набір яких може змінюватися в його процесі;

в) великою складністю задач тестування (об'ємами вхідних даних, на яких повинні бути проведені перевірки);

2) при верифікації функцій, що відносяться до критичних, повинна бути забезпечена необхідна достовірність перевірки, тобто гарантоване неперевищення припустимих ризиків помилок, які можуть привести до аварійних ситуацій; у протилежному випадку повинне ухвалюватися рішення про:

а) корекцію проекту в частині обсягу виконуваних завдань;

б) продовження процесу верифікації й внесення змін до досягнення прийнятних ризиків;

в) можливості й процедури проведення додаткової верифікації в умовах польоту для підвищення (або забезпечення) потрібної достовірності;

3) для комерційних космічних проектів можлива ситуація (стосовна до функцій, що не є найбільш критичними), коли верифікація на борту, в умовах польоту, може бути економічно більш вигідною й не вимагати:

а) великих часових витрат на проведення верифікації;

б) необхідності розробки або придбання дорогого встаткування;

в) залучення висококваліфікованих фахівців в унікальних галузях;

4) виходячи з міркувань безпеки й/або необхідності виконання хоча б деякої базової сукупності функцій, життєво важливих для ІУС і КС у цілому, за результатами верифікації й внаслідок дефектів ПЗс може бути ухвалене рішення про:

а) самоліквідацію системи;

б) блокування виконання певних функцій через відмову, що відбулася, що викликана фізичними дефектами апаратних засобів, дефектами проектування ПЗс або дефектами взаємодії [12,13], що й зробили неможливим повне коректне й/або безпечне їхнє виконання;

в) перерозподіл ресурсів ІУС і проведення повторної верифікації.

Ситуації, описувані в пп. 4б), 4в), фактично передбачають необхідність верифікації ПЗ в режимах керованої деградації ІУС КС.

1.4. Аналіз методів верифікації ПЗ ІУС

Огляд методів і технологій верифікації ПЗ для критичних застосувань даний у роботах [4,14,15]. Їхній аналіз дозволяє зробити наступні висновки.

1. Для ПЗ ІУС КС існують наступні методи верифікації, описані в [9]: метод випробувань, метод аналізу, метод статичного аналізу, метод тестування, метод

експертизи документації, метод проведення огляду, метод інспекції. Ці методи в цілому враховують специфіку космічних систем, у тому числі й можливість продовження верифікації в польоті, однак, їхній опис носить вербальний характер і не містить формалізованих процедур для розробки й застосування.

2. Формальні методи верифікації [15,16], засновані на представленні й перевірці специфікацій систем з використанням спеціальних нотацій, аналізі виконуваних функцій із застосуванням різних видів темпоральних логік, формулюванні й доказі теорем для підтвердження коректності програм, мають низку практичних обмежень. По-перше, вони суттєво обмежені в застосуванні розмірністю розв'язуваних завдань, яка часто є непорівнянною по складності з реальними задачами, покладеними на ПЗ ІУС КС. По-друге, ці методи не враховують аспект можливої корекції й верифікації ПЗс у польоті.

3. Методи верифікації, засновані на model-checking підході [17] і його модифікаціях, зокрема, інваріанто-орієнтованої технології [15], меншою мірою піддані обмеженням, пов'язаним з розмірністю, однак, також вимагають доробки з урахуванням специфіки ПЗ ІУС КС.

Таким чином, необхідно вдосконалювати існуючі та розробляти нові методи верифікації ПЗ ІУС у процесі застосування КС за призначенням. Будемо далі називати таку верифікацію оперативною верифікацією (ОВ) програмного забезпечення. Якщо за результатами верифікації здійснюється корекція ПЗ, будемо її називати оперативною коригувальною верифікацією (ОКВ).

1.5. Мета і структура статті

Мета даної роботи – теоретико-множинний опис цілей, етапів, операцій верифікації й моделей для оцінки готовності ІУС із урахуванням дефектів програмних засобів, що виявляються при ОКВ у процесі застосування.

Стаття структурована таким чином: у другому розділі дається класифікація й опис програмно виконуваних функцій ІУС КС за рівнем критичності. Моделі етапів і операційний базис процесів верифікації представлені в третьому розділі. Тут же дається приклад операційного базису верифікації при розробці ПЗ ІУС КС. Четвертий розділ присвячений опису цілей верифікації (ОКВ) з урахуванням можливості часткового її продовження в польоті КС. Виходячи із цього дано теоретико-множинний опис функцій різної критичності. У п'ятому розділі пропонуються різні сценарії усунення дефектів за результатами ОКВ і описані відповідні моделі готовності. У шостому розділі надано приклад розробки та дослідження моделі готовності системи космічного апарату (КА) з дубльованою структурою та ОКВ. В останньому розділі зроблені висновки й намічені напрямки подальших досліджень.

2. Класифікація функцій ІУС КС за рівнем критичності

Множина функцій ІУС космічних систем різняться за рівнем критичності відповідно до міжнародної й національної нормативної бази [4,9]. Критичність визначається в остаточному підсумку збитком, який може мати місце в результаті виникнення відповідної події (критичної ситуації). Вони отримали позначення по мірі зниження критичності A, B, C, U.

З урахуванням цього ІУС КС виконує набір функцій MF, які по критичності діляться на чотири множини

$$MF = FA \cup FB \cup FC \cup FU.$$

Кожна з множин описується набором функцій:

$$FA = \{f_{Ai}, i = 1,\ldots, b_A\},$$

$$FB = \{f_{Bj}, j = 1,\ldots, b_B\},$$

$$FC = \{f_{Ck}, k = 1,\ldots, b_C\},$$

$$FU = \{f_{Ul}, l = 1,\ldots, b_U\},$$

причому $\forall N,M \in \{A,B,C,U\}$, $N \neq M$: $FN \cap FM = \varnothing$,

$\text{Card } MF = b_A + b_B + b_C + b_U$.

Кожна з функцій f_z множини MF характеризується рівнем критичності (парируваних ситуацій) u_{cr}, цільовим призначенням a_{cr}, способом m_{cr} і складністю w_{cr} реалізації

$$f_z \sim \{u_{cr,z}, a_{crz}, m_{crz}, w_{crz}\}.$$

Атрибути критичності для функцій $f_z \in MF$ представлено в табл. 1.

Таблиця 1

Характеристика функцій ІУС КС за критичністю

Критичність	Атрибути функцій F			
	Рівень критичності, u_{cr}	Цільове призначення, a_{cr}	Спосіб реалізації, m_{cr}	Складність реалізації, w_{cr}
1	2	3	4	5
FA	Основні функції забезпечення безпеки	1. Попередити критичні ситуації 2. Пом'якшити критичні ситуації	Автоматичний/ ручний у виняткових випадках	Максимально проста реалізація
FB	Додаткові функції забезпечення безпеки	1. Уникнути ініціалізації елементів функції FA 2. Додати категорію FA	Переважно автоматичний	Більш складні засоби, ніж для реалізації функцій FA

Закінчення табл. 1

1	2	3	4	5
FC	Допоміжні або побічні функції	1. Реалізувати частку загального реагування на ситуації, що парирувані через виконання функцій FA, FB (ситуації A,B) 2. Безпосередньо не брати участь у запобіганні й парируванні ситуацій A, B	Автоматичний/ ручний	Засоби різної складності
FU	Некритичні (що не впливають на безпеку)	Не брати участь у запобіганні й парируванні ситуацій A, B, C	Автоматичний/ ручний	Засоби різної складності

3. Етапи й операції верифікації програмних засобів

3.1. Етапи створення й застосування ІУС КС

ІКС КС передбачає виконання верифікації на множині наступних етапів

$$ME = \{ED, EK, EA, ES, EO, EP\},$$

де ED – етап розробки, що характеризується набором операцій

$$V_{ED} = \{v_{EDe}, e = 1,\ldots, c_{ED}\};$$

EK – етап кваліфікації, що характеризується набором операцій

$$V_{EK} = \{v_{EKi}, i = 1,\ldots, c_{EK}\};$$

EA – етап приймання, що характеризується набором операцій

$$V_{EA} = \{v_{EAi}, i = 1,\ldots, c_{EA}\};$$

ES – етап передпольотної підготовки, що характеризується набором операцій

$$V_{ES} = \{v_{ESi}, i = 1,\ldots, c_{ES}\};$$

EO – етап польоту, що характеризується набором операцій

$$V_{EO} = \{v_{EOi}, i = 1,\ldots, c_{EO}\};$$

EG – післяпосадковий етап, що характеризується набором операцій

$$V_{EG} = \{v_{EGi}, i = 1,\ldots, c_{EG}\}.$$

Дана множина етапів є укрупненою. Кожний з етапів може бути представлений множинами підетапів. Зокрема, етап польоту EO включає наступні підетапи: передорбітальний (EOB), орбітальний (EOO), посадковий (EOP):

$$EO = \{EOB, EOO, EOP\}.$$

Крім того, перелічені етапи повторюються для наступних (повторних) польотів, коли верифікація виконується в повному обсязі або частково залежно від зміни функцій системи. З урахуванням цього вираз для опису ME буде виглядати в такий спосіб:

$$ME = \{ME_j, j = 1,\ldots, r; EF\} = \{\{E_1D, E_1K, E_1A, E_1S, E_1O, E_1G\}, \{E_2D, E_2K, E_2A, E_2S, E_2O, E_2G\}, \ldots, \{E_rD, E_rK, E_rA, E_rS, E_rO, E_rG\}, EF\},$$

де r – число пусків;

EF – етап завершення застосування системи.

3.2. Множина операцій верифікації

Множина операцій верифікації описується як об'єднання множин операцій по етапах:

$$MV = V_{ED} \cup V_{EK} \cup V_{EA} \cup V_{ES} \cup V_{EO} \cup V_{EG}.$$

Операції, виконувані при верифікації на різних етапах при повторних пусках, можуть повторюватися, тому

$$\text{Card } MV \le \text{Card } V_{ED} + \text{Card } V_{EK} + \text{Card } V_{EA} + \text{Card } V_{ES} + \text{Card } V_{EO} + \text{Card } V_{EG}.$$

Якщо функції системи від пуску до пуску не змінюються, то кількість і об'єм (для складних функцій) верифікаційних операцій можуть зменшуватися:

$$\forall N \in \{D,K,A,S,O,G\}, \forall i \in \{2,\ldots,r\}: V_{EiN} \subseteq V_{Ei\text{-}1N},$$
$$\text{Card } V_{EiN} \le \text{Card } V_{Ei\text{-}1N}.$$

Дана умова не виконується у випадку, якщо при чергових пусках були виявлені позаштатні ситуації, які викликали введення нових операцій по верифікації.

У випадку зміни множини виконуваних функцій MF або засобів їхньої реалізації, верифікація проводиться на відповідних етапах для тієї частини функцій системи та їх засобів, які змінилися (MF*), і конфігураційних засобів, що забезпечують їхнє вбудовування в модифіковану систему (MF_{conf}). Для таких ситуацій справедливо:

$$\forall f_s \in MF^*, \forall i \in \{2,\ldots,r\}: V_{EiN(s)} = V_{Ei\text{-}1N(s)} \cup V_{EiN(s)conf},$$

де $V_{EiN(s)conf}$ – множина додаткових операцій верифікації конфігураційних засобів.

Слід зазначити, що кожна з множин V_{EiN} складається з підмножин операцій для різних підетапів; ті, у свою чергу, можуть бути розділені на ще більш дрібні операції.

3.3. Операції верифікації етапу розробки

Найбільш відповідальним і трудомістким є етап розробки ПЗс ІУС. Аналіз діючого в Україні галузевого нормативного документа, гармонізованого зі стандартом ECSS [9], дозволяє представити операційний базис для цього етапу. Він включає множину наступних операцій $V_{ED} = \{v_{EDe}, e = 1,\ldots,7\}$:

- *верифікація контракту*, множина $v_{ED1} = \{v_{ED1i}, i = 1,\ldots,5\}$, яка, у свою чергу, складається з окремих операцій (мікроопераций):

1) перевірка того, що постачальник має можливість задовольнити вимоги контракту, v_{ED11};

2) перевірка того, що вимоги є несуперечливими й покривають потреби користувачів, v_{ED12};

3) перевірка того, що існує окрема домовленість щодо адекватних процедур для обробки змін у вимоги й зняття проблем, v_{ED13};

4) перевірка того, що існує окрема домовленість щодо процедур і межи їхнього застосування для здійснення взаємозв'язку й співробітництва між учасниками, включаючи питання прав власності, гарантійних прав, авторських прав і конфіденційності, v_{ED14};

5) перевірка того, що існує окрема домовленість щодо процедур і критеріїв приймання, v_{ED15};

- *верифікація процесу*, множина $v_{ED2} = \{v_{ED2i}, i = 1,\ldots,5\}$, яка складається з окремих операцій (мікрооперацій):

1) перевірка того, що вимоги щодо планування проекту є адекватними й своєчасними, v_{ED21};

2) перевірка того, що обрані для проекту процеси є адекватними й реалізовуваними, виконуються відповідно до плану й відповідають контракту, v_{ED22};

3) перевірка того, що стандарти, процедури й середовище проекту є адекватним, ved_{23};

4) перевірка того, що проект забезпечений персоналом, і персонал проходить навчання відповідно до контракту, v_{ED24};

- *верифікація вимог,* множина $v_{ED3} = \{v_{ED3i}, i = 1,\ldots,4\}$, яка складається з окремих операцій (мікрооперацій):

1) перевірка того, що системні вимоги несуперечливі, реалізовувані й перевіряються, v_{ED31};

2) перевірка того, що системні вимоги відповідним чином розподілені між елементами апаратних і програмних засобів і ручними операціями відповідно до проектних критеріїв, v_{ED32};

3) перевірка того, що вимоги до ПЗ несуперечливі, реалізовувані, перевіряються й точно відображають системні вимоги, v_{ED33};

4) перевірка того, що вимоги до програмних засобів, пов'язані з безпекою, захистом і критичністю, є коректними, що демонструється за допомогою відповідних методів, v_{ED34};

- *верифікація проекту,* множина $v_{ED4} = \{v_{ED4i}, i = 1,\ldots,5\}$, яка складається з окремих операцій (мікрооперацій):

1) перевірка того, що проект коректний, несуперечливий, й що прослідковується відносно вимог, v_{ED41};

2) перевірка того, що проект реалізує правильну послідовність подій, входів, виходів, логіку функціонування, розподіл часових і об'ємних ресурсів, v_{ED42};

3) перевірка того, що проект забезпечує визначення, локалізацію й відновлення системи після помилок, v_{ED43};

4) перевірка того, що проект може бути отриманий виходячи зі сформульованих вимог, v_{ED44};

5) перевірка того, що проект коректно реалізує вимоги з безпеки, захисту та інші критичні вимоги, що демонструється за допомогою відповідних методів, v_{ED45};

- *верифікація коду,* множина $v_{ED5} = \{v_{ED5i}, i = 1,\ldots,6\}$, яка складається з окремих операцій (мікрооперацій):

1) перевірка того, що код є таким, що прослідковується відносно проекта й вимог, тестопридатним, коректним, v_{ED51};

2) перевірка того, що код відповідає вимогам і стандартам кодування, v_{ED52};

3) перевірка того, що код реалізує правильну послідовність подій, несуперечливі інтерфейси, коректні потоки даних і управління, повноту, відповідний розподіл часових і об'ємних ресурсів, v_{ED53};

4) перевірка того, що код забезпечує визначення, локалізацію й відновлення системи після помилок, v_{ED54};

5) перевірка того, що отриманий код може бути виведений із проекту або вимог, v_{ED55};

6) перевірка того, що код коректно реалізує вимоги з безпеки, захисту та інші критичні вимоги, це демонструється за допомогою відповідних точних методів, v_{ED56};

- *верифікація інтеграції,* множина $v_{ED6} = \{v_{E6i}, i = 1,\ldots,3\}$, яка складається з окремих операцій (мікрооперацій):

1) перевірка того, що програмні компоненти й модулі повністю й коректно інтегровані для кожного елемента ПЗс, v_{ED61};

2) перевірка того, що елементи апаратних і програмних засобів і ручні операції повністю й коректно інтегровані в систему, v_{ED62};

3) перевірка того, що завдання інтеграції виконані відповідно до плану інтеграції, v_{ED63};

- *верифікація документації,* множина $v_{ED7} = \{v_{E7i}, i=1,\ldots,3\}$, яка складається з окремих операцій (мікрооперацій):

1) перевірка того, що документація є адекватною, повною й несуперечливою, v_{E71};

2) перевірка того, що документація підготовлена вчасно, v_{E72};

3) перевірка того, що конфігураційне керування документацією відповідає встановленим процедурам, v_{E73}.

Кожна з операцій v_{EDei} множини $V_{ED} = \{\{v_{EDei}, i = 1,\ldots,b_{ei}\}, e = 1,\ldots,7\}$ представляється набором мікроопераций $\{\mu_j v_{EDei}, j = 1,\ldots, d_{EDei}\}$, об'єднаних у мікропрограму верифікації πv_{EDei}. Ця мікропрограма може бути представлена стандартною алгоритмічною моделлю.

4. Цілі та сценарії верифікації

4.1. Загальна множина цілей верифікації

Основна ціль верифікації це підтвердження відповідності результатів розробки на відповідному етапі вимогам, сформульованим на його початку або раніше. Враховуючи багатоетапність життєвого циклу ІУС КС, повторюваність етапів при пусках, загальна ціль верифікації розділяється на множину підцілей.

Множина цілей верифікації, таким чином, може бути представлена у вигляді виразу:

$$МЦ = \{МЦD, МЦK, МЦA, МЦS, МЦO, МЦР\},$$

у якім кожна з множин цілей може бути декомпозована на підмножини відповідно до двох ознак:

- рівня критичності функцій, що верифікуються, u_{cr} (A,B,C,U);
- задачі верифікації, розв'язуваної на даному етапі, виходячи із цільового призначення, a_{cr}, та ін.

4.2. Множина цілей верифікації в польоті

Нормативна база, можливості реалізації й міркування економічної ефективності для комерційних пусків (за умови повного й строгого виконання вимог з безпеки) допускають, що частину функцій системи можливо бути верифікувати у польоті. З урахуванням цього проведемо декомпозицію цілей верифікації ІУС КС для етапу польоту:

$$МЦО = \{ЦА1, ЦВ1, ЦВ2, ЦВ3, ЦС2, ЦС3\},$$

де ЦА1 – підвищення (підтвердження) достовірності верифікації функцій А для зниження рівня прийнятного ризику (подальше підвищення стандартів безпеки),

ЦВ1 – підвищення (підтвердження) достовірності верифікації функцій В для зниження рівня прийнятного ризику (подальше підвищення стандартів безпеки),

ЦВ2 – проведення верифікації функцій В, які неможливо перевірити в наземних умовах або неможливо забезпечити необхідний рівень достовірності оцінки,

ЦВ3 – проведення верифікації функцій В у випадку, якщо це припустимо з міркувань безпеки й вимагає менших витрат, ніж в наземних умовах,

ЦС2 – проведення верифікації функцій С, які неможливо перевірити в наземних умовах або неможливо забезпечити необхідний рівень достовірності оцінки,

ЦС3 – проведення верифікації функцій С у випадку, якщо це припустимо з міркувань безпеки й вимагає менших витрат, ніж в наземних умовах.

Виходячи із цього, маємо:

$$МЦ = \{\Delta МЦ_Д, \Delta МЦ_Н, \Delta МЦ_З\},$$

де $\Delta МЦ_Д = \{ЦА1, ЦВ1\}$ – множина цілей, пов'язаних з підвищенням (підтвердженням) достовірності верифікації функцій А, В для зниження рівня прийнятного ризику (подальше підвищення стандартів безпеки);

$\Delta МЦ_Н = \{ЦВ2, ЦС2\}$ – множина цілей, пов'язаних з проведенням верифікації функцій В, С, які неможливо перевірити в наземних умовах або неможливо забезпечити необхідний рівень достовірності оцінки;

$\Delta МЦ_З = \{ЦВ3, ЦС3\}$ - множина цілей, пов'язаних з проведенням верифікації функцій В, С у випадку, якщо це припустимо з міркувань безпеки й вимагає менших витрат, ніж в наземних умовах.

Відповідність цілей верифікації функцій у польоті й критичності відображається таблицею 2.

У табл. 2 індекси при функціях відповідають цілям і умовам верифікації (підвищення або підтвердження достовірності верифікації – індекс "д", в протилежному випадку "$\overline{д}$"; проведення верифікації функцій, які неможливо перевірити в наземних умовах або неможливо забезпечити необхідний рівень достовірності оцінки – індекс "н", в протилежному випадку – індекс "$\overline{н}$"; проведенням верифікації функцій у польоті у випадку, якщо це припустимо з міркувань безпеки й вимагає менших витрат, ніж в наземних умовах – індекс "з", в протилежному випадку "$\overline{з}$").

Таблиця 2

Відповідність цілей верифікації функцій у польоті та їхні критичності

Критичність	$\Delta МЦ_Д/F$		$\Delta МЦ_Н/F$		$\Delta МЦ_З/F$	
A	ЦА1	$FA_Д$ $FA_{\overline{Д}}$				
B	ЦВ1	$FB_Д$ $FB_{\overline{Д}}$	ЦВ2	$FB_Н$ $FB_{\overline{Н}}$	ЦВ3	$FB_З$ $FB_{\overline{З}}$
C			ЦС2	$FC_Н$ $FC_{\overline{Н}}$	ЦС3	$FC_З$ $FC_{\overline{З}}$
U						

4.3. Теоретико-множинний опис функцій з урахуванням цілей верифікації

З урахуванням декомпозиції цілей верифікації функцій ІУС КС у польоті їхня графічна інтерпретація для різних рівнів критичності представлена на рис. 1. На цьому рисунку лінії різного типу розділяють функції FA (а), FB (б), FC (в), FU (г) відповідно до можливих цілей верифікації.

З урахуванням цілей верифікації для функцій з різною критичністю справедливі наступні вирази:

а) для функцій FA:

$$FA = \{FA_Д, FA_{\overline{Д}}\}, \quad FA_Д \cap FA_{\overline{Д}} = \varnothing;$$

б) для функцій FB:

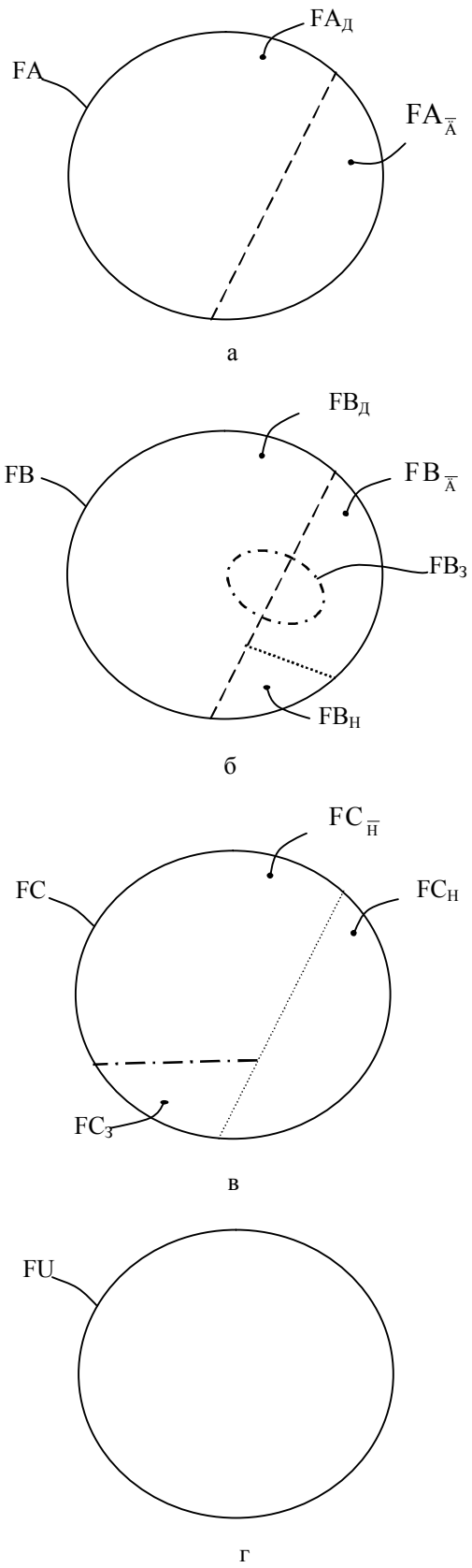

Рис. 1. Графічна інтерпретація функцій ІУС КС різної критичності з урахуванням цілей верифікації (для функцій FA(а), FB(б), FC(в), FU(г))

$FB = \{FB_Д, FB_Н, FB_З, FA_{\bar{Д}}, FB_{\bar{Н}}, FB_{\bar{З}}\}$

$FB = FB_Д \cup FB_{\bar{Д}} = FB_Н \cup FB_{\bar{Н}} = FB_З \cup FB_{\bar{З}}$;

$FB_Д \cap FB_{\bar{Д}} = FB_Н \cap FB_{\bar{Н}} = FB_З \cap FB_{\bar{З}} = \varnothing$;

$FB_Н \subset FB_{\bar{Д}}$, $FB_З \cap FB_Н = \varnothing$ $(FB_З \subset FB \setminus FB_Н)$;

$FB_З = FB_{ДЗ} \cup FB_{\bar{Д}З}$, $FB_{ДЗ} \cap FB_{\bar{Д}З} = \varnothing$;

$FB_{ДЗ} = FB_Д \cap FB_З$, $FB_{\bar{Д}З} = FB_{\bar{Д}} \cap FB_З$

в) для функцій FC;

$FC = \{FC_Н, FC_{\bar{Н}}, FC_З, FC_{\bar{З}}\}$;

$FC = FC_Н \cup FC_{\bar{Н}} = FC_З \cup FC_{\bar{З}}$;

$FC_Н \cap FC_{\bar{Н}} = FC_З \cap FC_{\bar{З}} = \varnothing 4$;

$FC_З \subset FC_{\bar{Н}}$, $FC_З \cap FC_Н = \varnothing$;

$FC_{\bar{Н}} = FC_{\bar{Н}З} \cup FC_{\bar{Н}\bar{З}}$, $FC_{\bar{Н}З} \cap FC_{\bar{Н}\bar{З}} = \varnothing$;

$FC_{\bar{Н}З} = FC_{\bar{Н}} \cap FC_З$, $FC_{\bar{Н}\bar{З}} = FC_{\bar{Н}} \cap FC_{\bar{З}}$.

4.4. Сценарії верифікації й роботи при виявленні дефекту

З урахуванням проведеного аналізу й опису процесів верифікації необхідно розробити можливі сценарії реакції на виявлені в польоті дефекти. Множина сценаріїв може декомпозуватися залежно від множини $H = \{h_i, i = 1,\ldots,4\}$ наступних ознак:

- можливість проведення ОВ для функцій, повна верифікація яких у наземних умовах нездійсненна, h_1 (h_{11} – без можливості корекції при виявленні дефектів, h_{12} – з можливістю корекції дефектів за результатами ОВ при збереженні повної функціональності – випадок ОКВ; корекція може бути виконана шляхом ковзної заміни дефектної ділянки, модуля новим (часткова заміна) або введення нової версії (повна заміна));

- можливість проведення ОВ для функцій з обмеженою критичністю, верифікація яких у наземних умовах більш витратна, h_2 (h_{21} – без можливості корекції, h_{22} – з можливістю корекції – випадок ОКВ);

- можливість проведення відновлення ПЗс у польоті, h_3 (h_{31} – профілактичного, пов'язаного з усуненням дефектів, h_{32} – функціонального, пов'язаного зі зміною набору функцій);

- можливість парирування виявлених дефектів шляхом блокування функцій і втрати якості, h_4 (керована деградація).

Ознаки h_i (а також підознаки h_{ij}) є булєвими змінними й приймають значення 0 або 1 залежно від можливості (1) або неможливості (0) проведення відповідного виду ОВ або ОКВ.

Виходячи зі значень ознак $h_i \in H$ формується множина сценаріїв $MSC = \{SC_q, q = 1,\ldots,w\}$, описувані вектором значень $SC_q \sim < h_{iq} >$. Далі описуються деякі з можливих сценаріїв:

SC1 – усі можливі (для наземних умов) види верифікації виконуються; ОВ і корекція дефектів у польоті неможлива; цьому сценарію відповідає набір ознак $H_{SC1} = \{\forall\ i = 1,\ldots,4: h_i = 0\}$;

SC2 – усі можливі (для наземних умов) види верифікації виконуються; ОВ у польоті не проводиться; можлива корекція (частини) дефектів, що виявилися в польоті; корекція проводиться тільки при виявленні/прояві дефекту; цьому сценарію відповідає набір ознак $H_{SC1} = \{h_1 = h_2 = = h_4 = 0, h_{31} = 1\}$;

SC3 – усі можливі для наземних умов види верифікації виконуються; у польоті проводиться верифікація всіх функцій, верифікація яких неможлива в наземних умовах і за її результатами проводиться корекція виявлених дефектів (випадок ОКВ); цьому сценарію відповідає набір ознак $H_{SC1} = \{h_{12} = 1, h_2 = h_3 = h_4 = 0\}$;

SC4 – усі можливі для наземних умов види верифікації виконуються; у польоті проводиться верифікація всіх функцій, верифікація яких неможлива в наземних умовах і за її результатами проводиться корекція виявлених дефектів (випадок ОКВ); при цьому можливо блокування частини функцій і деградація системи при виявленні дефектів; цьому сценарію відповідає набір ознак $H_{SC1} = \{h_{12} = h_4 = 1, h_2 = h_3 = 0\}$ та ін.

5. Оцінка готовності ІУС КС з оперативною коригувальною верифікацією програмних засобів

5.1. Показники готовності та витрат

Для оцінки ІУС КС із урахуванням можливостей проведення ОКВ пропонується використовувати наступні показники:

1. Показники готовності, а саме:

- функція готовності $К_г(t)$,

- функція оперативної готовності $К_{ог}(t)$ та її стаціонарні значення (для систем з режимом, що встановився);

2. Показники для оцінки ризику аварії $R=[1 - К_г(t)] \cdot У$, де У – збиток;

3. Показники деградації:

- число рівнів d і величина припустимої деградації ΔП;

- коефіцієнт виконання функцій k_F, обумовлений часткою числа виконуваних функцій з урахуванням їхньої критичності, яка може бути оцінена ваговим коефіцієнтом);

4. Показники витрат на верифікацію $З_В$ і корекцію $З_К$.

5.2. Основні типи моделей готовності

Для оцінки готовності й інших показників систем залежно від множини сценаріїв MCS необхідно розробити моделі. Вони можуть базуватися на одно- або багатофрагментних марковських моделях [18, 19]. Приведемо в загальному вигляді приклади таких моделей.

Модель 1 (сценарій SC1). Граф станів для цієї моделі показаний на рис. 2, а. Він характеризується деякою множиною станів і переходів, обумовлених потоками відмов апаратних засобів і відновлень із урахуванням архітектури системи і можливостей виявлення відмов і відновлення працездатності. Один з визначальних параметрів – інтенсивність відмов апаратних засобів, λ_{HW}; З інтенсивністю $\lambda_{деф}$ система переходить у стан відмови.

Модель 2 (сценарій SC2, рис. 2, б). Відмінність полягає в тому, що можливе виявлення й часткове усунення або парирування дефектів програмних засобів. Зменшення їхньої інтенсивності враховується за допомогою коефіцієнта α, $\alpha<1$. Крім того, у модель вводиться коефіцієнт δ ($\delta>1$), що враховує ускладнення апаратних засобів для забезпечення оперативної корекції в польоті.

Модель 3 (сценарій SC3, SC4, рис.2, в). Для даної моделі характерна деревоподібна структура графа переходів, у якому є розбіжні гілки залежно від того, яка подія наступає: виявлення дефекту або початок процесу верифікації. Відмінність моделі для різних сценаріїв обумовлюється тільки значенням параметрів. Для сценарію SC4 інтенсивність переходу в стан верифікації (як і прояву дефектів) може бути вище.

Модель 4 (сценарій SC1). Виконуються всі види верифікації функцій у наземних умовах, за винятком тих функцій, перевірка яких можлива в польоті, і є більш дешевою.

Стратегія верифікації характеризується набором керуючих параметрів і сценарієм верифікації. Стратегія верифікація вибирається виходячи з вимог до системи й наявних обмежень. Формування стратегії верифікації включає:

- визначення параметрів доверифікації тих функцій, верифікація яких неможлива в наземних умовах;

- визначення доцільності й параметрів доверифікації тих функцій, які можуть бути перевірені й у наземних умовах і в польоті.

6. Розробка та дослідження моделі готовності ІУС космічного апарата з оперативною коригувальною верифікацією програмних засобів

6.1. Основні допущення

Для побудови моделі готовності ІУС КА (космічного апарата) прийняті наступні допущення:

– у даному розділі розглядається типова архітектура ІУС КА, яка включає два резервовані апаратних канала, у кожному з яких функціонує однакова версія ПЗ; систему контролю працездатності будемо вважати абсолютно надійною;

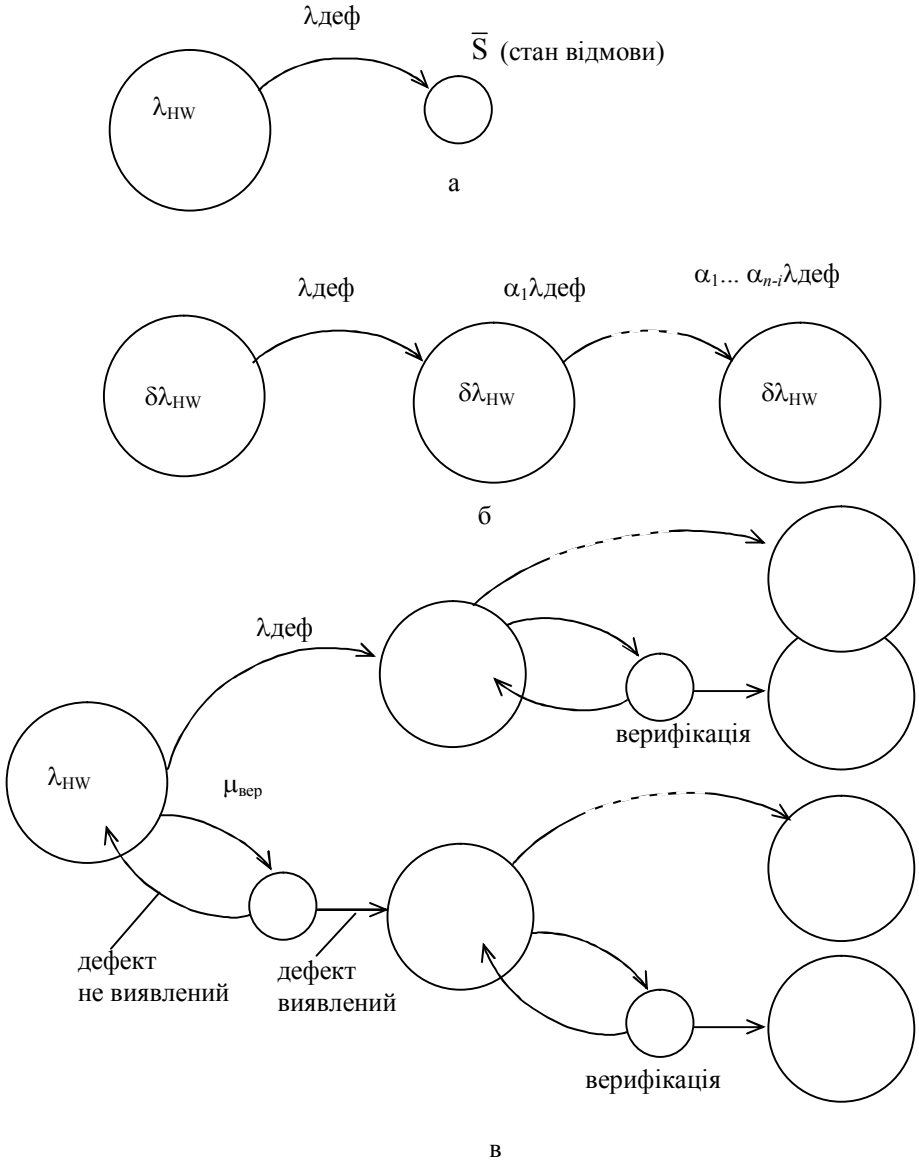

Рис. 2. Моделі готовності ІУС з ОВ (а – модель 1; б – модель 2; в – модель 3)

– ІУС у будь-який момент часу може перебувати або в працездатному, або в непрацездатному стані, а потоки подій, що переводять систему з одного функціонального стану в інший, – найпростіші;

– відновлення ІУС після відмови, викликаної програмним дефектом, проводиться за допомогою перезапуску ПЗ;

– у процесі функціонування ІУС виконується верифікація програмних функцій у спеціальні проміжки часу (стан неготовності);

– усунення програмних дефектів виконується після їхнього прояву як системних відмов, або ж після їхнього виявлення в процесі оперативної верифікації з імовірністю виявлення D;

– у ході виправлення програмних дефектів, нові дефекти не вносяться;

– допускається повне усунення всіх невиявлених дефектів.

6.2. Обгрунтування вхідних параметрів моделі

У ході проведення досліджень із метою виявлення характеру зміни поведінки функції готовності, частина вхідних параметрів моделі мали фіксовані значення, інші параметри змінювалися в межах заданих інтервалів значень. Фіксовані значення мають наступні параметри:

– інтенсивність відмов одного апаратного каналу $\lambda_{HW} = 3*10^{-4}$ (1/год);

– інтенсивність відновлення одного апаратного каналу $\mu_{HW} = 1$ (1/год);

– початкова інтенсивність відмов ПЗ $\lambda_{SW\,0} = 4*10^{-3}$ (1/год);

– інтенсивність відновлення системи після прояву програмного дефекту (шляхом перезапуску ПЗ) $\mu_{SW} = 2$ (1/год);

– інтенсивність відмов ПЗ після усунення всіх дефектів дорівнює нулю $\lambda_{SW\,k} = 0$ (1/год).

Для дослідження готовності системи були прийняті змінювані значення вхідних параметрів, наведені у табл.. 3.

Таблиця 3

Змінні значення вхідних параметрів моделі

Параметр моделі	Змінні значення параметрів		
$\Delta\lambda_{SW}$ (1/год)	$1\cdot10^{-3}$	$5\cdot10^{-4}$	$1\cdot10^{-4}$
D	0,8	0,9	1
λ_{ver} (1/год)	$1{,}39\cdot10^{-3}$	$4{,}63\cdot10^{-4}$	$2{,}31\cdot10^{-4}$
μ_{ver} (1/год)	1	1,5	2

Також при моделюванні можна виділити "базисні" значення змінюваних вхідних параметрів:

– крок зміни інтенсивності відмов ПЗ $\Delta\lambda_{SW} = 5*10^{-4}$ (1/год);

– імовірність виявлення програмного дефекту при верифікації ПЗ D = 0,8;

– інтенсивність проведення верифікації ПЗ $\lambda_{ver} = 4{,}63*10^{-4}$ (1/год);

– інтенсивність відновлення працездатного стану системи після проведення верифікації ПЗ μ_{ver} = 2 (1/год).

6.3. Розробка моделі готовності

З урахуванням прийнятих допущень, у якості методу дослідження приймається марковський аналіз, а урахування зміни інтенсивності відмов λ_{SW} здійснюється за допомогою апарата регулярних багатофрагментних марковських моделей (РБФМ) [18]. Тому в якості базової моделі обрана РБФМ, граф якої зображений на рис. 3.

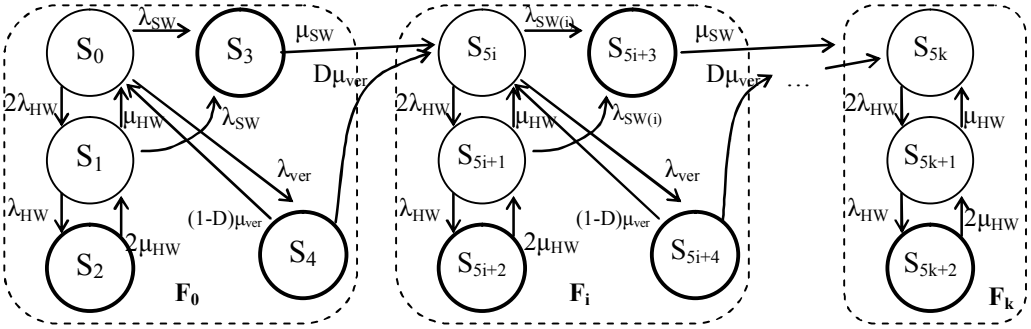

Рис. 3. Розмічений граф функціонування ІУС, що обслуговується КА при проведенні оперативної коригувальної верифікації програмних функцій

Процес функціонування ІУС відбувається в такий спосіб. У початковий момент система реалізує всі приписані функції й перебуває в стані S_0. У процесі функціонування проявляються апаратні дефекти, внаслідок чого система послідовно переходить у стани S_1 (відмова одного з апаратних каналів, система працездатна), S_2 (відмова відразу двох апаратних каналів, система непрацездатна) і відновлюються (система вертається в стани S_0 і S_1).

Через певний часовий інтервал відбувається відмова системи, викликана програмним дефектом, і вона переходить у стан S_3. Після прояву дефекту ПЗ, він, природно, виявляється, і усувається, внаслідок чого система після відновлення переходить у наступний фрагмент РБФМ (стан S_{5i}), який характеризується новим параметром $\lambda_{SW\,i}$. Також через певний часовий інтервал виконується оперативна коригувальна верифікація частини програмних функцій, система переходить у стан S_4. У ході проведення процедур верифікації з імовірністю D можливе виявлення й усунення програмних дефектів, внаслідок чого система також переходить у новий фрагмент РБФМ.

В останньому фрагменті моделі всі програмні дефекти усунуті, і в системі відбуваються тільки відмови апаратних засобів. Система диференціальних рівнянь Колмогорова для моделі надійності, граф якої зображений на рис. 3 буде складатися з наступних регулярних блоків:

– для початкового фрагмента F_0:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -(2\lambda_{HW} + \lambda_{SW} + \lambda_{VER})P_0(t) + \\ \qquad + \mu_{HW}P_1(t) + (1-D)\mu_{VER}P_4(t), \\ \dfrac{dP_1(t)}{dt} = -(\lambda_{HW} + \lambda_{SW} + \mu_{HW})P_1(t) + \\ \qquad + 2\lambda_{HW}P_0(t) + 2\mu_{HW}P_2(t), \end{cases}$$

$$\begin{cases} \dfrac{dP_2(t)}{dt} = -2\mu_{HW}P_2(t) + \lambda_{HW}P_1(t), \\ \dfrac{dP_3(t)}{dt} = -\mu_{SW}P_3(t) + \lambda_{SW}P_0(t) + \lambda_{SW}P_1(t), \\ \dfrac{dP_4(t)}{dt} = -\mu_{VER}P_4(t) + \lambda_{VER}P_0(t); \end{cases}$$

– для внутрішніх фрагментів Fi:

$$\begin{cases} \dfrac{dP_{5\cdot i}(t)}{dt} = -(2\lambda_{HW} + \lambda_{SW(i)} + \lambda_{VER})P_{5\cdot i}(t) + \\ \qquad + \mu_{HW}P_{5\cdot i+1}(t) + D\mu_{VER}P_{5\cdot i-1}(t) + \\ \qquad + \mu_{SW}P_{5\cdot i-2}(t) + (1-D)\mu_{VER}P_{5\cdot i+4}(t), \\ \dfrac{dP_{5\cdot i+1}(t)}{dt} = -(\lambda_{HW} + \lambda_{SW(i)} + \mu_{HW})P_{5\cdot i+1}(t) + \\ \qquad + 2\lambda_{HW}P_{5\cdot i}(t) + 2\mu_{HW}P_{5\cdot i+2}(t), \end{cases}$$

$$\begin{cases} \dfrac{dP_{5\cdot i+2}(t)}{dt} = -2\mu_{HW}P_{5\cdot i+2}(t) + \lambda_{HW}P_{5\cdot i+1}(t), \\ \dfrac{dP_{5\cdot i+3}(t)}{dt} = -\mu_{SW}P_{5\cdot i+3}(t) + \lambda_{SW(i)}P_{5\cdot i}(t) + \\ \qquad + \lambda_{SW(i)}P_{5\cdot i+1}(t), \\ \dfrac{dP_{5\cdot i+4}(t)}{dt} = -\mu_{VER}P_{5\cdot i+4}(t) + \lambda_{VER}P_{5\cdot i}(t). \end{cases}$$

– для останнього фрагмента Fk:

$$\begin{cases} \dfrac{dP_{5\cdot k}(t)}{dt} = -2\lambda_{HW}P_{5\cdot k}(t) + \mu_{HW}P_{5\cdot k+1}(t) + \\ \qquad + D\mu_{VER}P_{5\cdot k-1}(t) + \mu_{SW}P_{5\cdot k-2}(t), \\ \dfrac{dP_{5\cdot k+1}(t)}{dt} = -(\lambda_{HW} + \mu_{HW})P_{5\cdot k+1}(t) + \\ \qquad + 2\lambda_{HW}P_{5\cdot k}(t) + 2\mu_{HW}P_{5\cdot k+2}(t), \\ \dfrac{dP_{5\cdot k+2}(t)}{dt} = -2\mu_{HW}P_{5\cdot k+2}(t) + \lambda_{HW}P_{5\cdot k+1}(t). \end{cases}$$

Тут i – номери внутрішніх фрагментів; k – номер останнього фрагмента,

Значення функції готовності визначається з виразу:

$$A(t) = \sum_{i=0}^{k}\left[P_{5\cdot i}(t) + P_{5\cdot i+1}(t)\right].$$

При дослідженні моделі особливий інтерес представляє початковий етап функціонування системи, тому при розрахунках розглядався часовий інтервал T = 15000 годин (приблизно 1,5 року) з кількістю ділянок інтегрування – 100. Вихідні результати отримані за допомогою модифікованого експонентного методу чисельного вирішення жорстких систем диференціальних рівнянь [8].

6.4. Результати дослідження

Результати обчислень представлені у вигляді графічної залежності функції готовності від часу функціонування систем на рис. 4 – 8. Результуючі функції порівнюються зі стаціонарним коефіцієнтом готовності дубльованої одноверсійної ІУС, отриманим при незмінних початкових параметрах λ_{HW}, μ_{HW}, $\lambda_{SW\,0}$, μ_{SW} за допомогою однофрагментного моделювання.

Аналіз графіків на рис. 4 показав, що значення параметра $\Delta\lambda_{sw}$ у більшій мері впливає на швидкість усунення дефектів (чим більше $\Delta\lambda_{sw}$, тим швидше функція готовності багатофрагментної моделі переходить у стаціонарний стан). Крім того, значення $\Delta\lambda_{sw}$ побічно впливає на величину мінімуму функції готовності на початковому етапі експлуатації системи.

З рис. 5 показне, що з підвищенням імовірності виявлення дефектів при оперативній верифікації ПЗ, готовність системи несуттєво збільшується на часовому інтервалі 1000…7000 годин. Для більш наочного представлення даного виграшу на рис. 6 показані графіки різниці між готовністю системи при різних значеннях параметра D. Настільки малий виграш у готовності пояснюється тим, що в прийнятих значеннях вхідних даних інтенсивності проведення верифікації й прояву дефектів ПЗ мають один порядок.

Це значить, що якщо програмний дефект не буде виявлений при верифікації, він незабаром однаково виявиться у вигляді відмови.

Крім того, значення параметра D ніяк не впливає на величину мінімуму функції готовності, а також на швидкість переходу цієї функції в стаціонарний режим.

Аналіз графіків на рис. 7 показав, що значення параметра λ_{ver} одночасно впливає на величину мінімуму функції готовності й на швидкість переходу функції в стаціонарний режим. При цьому характер впливу не такий, як у параметра $\Delta\lambda_{sw}$: із прискоренням переходу функції готовності в стаціонарний режим при більш частому проведенні процедур оперативної коригувальної верифікації, мінімум функції готовності приймає менші значення на початковому етапі експлуатації системи.

З рис. 8 видно, що значення параметра μ_{ver} у більшій мері впливає на величину мінімуму функції готовності багатофрагментної моделі, і практично не впливає на швидкість переходу цієї функції в стаціонарний режим.

6.5. Аналіз результатів

Аналіз отриманих результатів моделювання готовності ІУС обслуговуваного космічного апарата при проведенні оперативної коригувальної верифікації програмних функцій дозволяє сформулювати наступні висновки.

1. Для прискорення переходу функції готовності в стаціонарний стан необхідно підвищувати значення параметрів $\Delta\lambda_{sw}$ і λ_{ver}, тобто більш часто проводити процедури верифікації й намагатися усунути більшу кількість програмних дефектів за одну перевірку.

2. У початковий період експлуатації готовність систем із плановим проведенням процедур оперативної верифікації нижче, ніж у систем без усунення дефектів ПЗ.

3. Підвищити готовність систем на початковому періоді експлуатації можна збільшуючи значення параметра μ_{ver}, тобто прискоривши відновлення працездатного стану системи.

Планується включити розроблену модель і отримані результати в комплексну методику вибору й обґрунтування параметрів стратегії проведення верифікації ІУС КА.

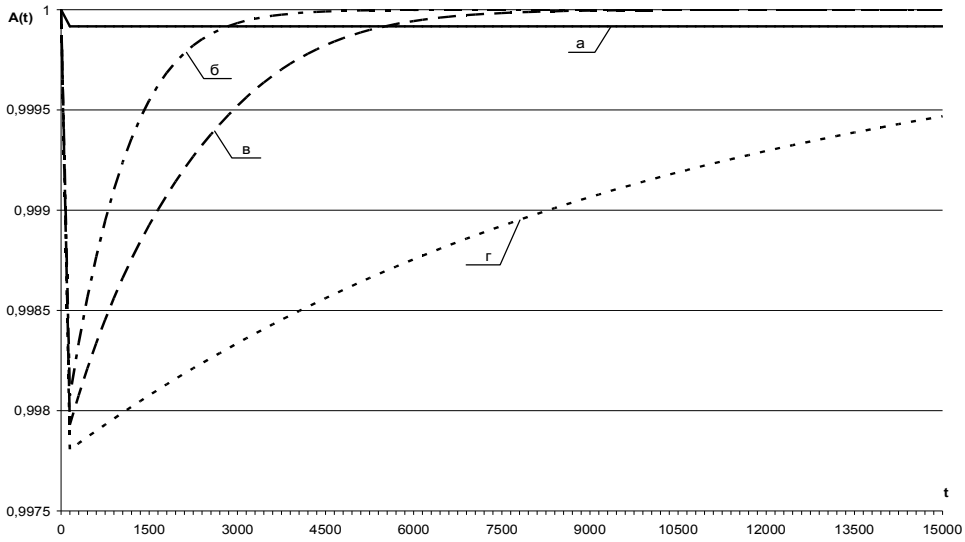

Рис. 4. Графічні залежності зміни функції готовності ІУС від часу експлуатації системи для однофрагментної моделі (а) і при різних значеннях $\Delta\lambda_{sw}$: б) $\Delta\lambda_{sw}=10^{-3}$; в) $\Delta\lambda_{sw}=5*10^{-4}$; г) $\Delta\lambda_{sw}=10^{-4}$

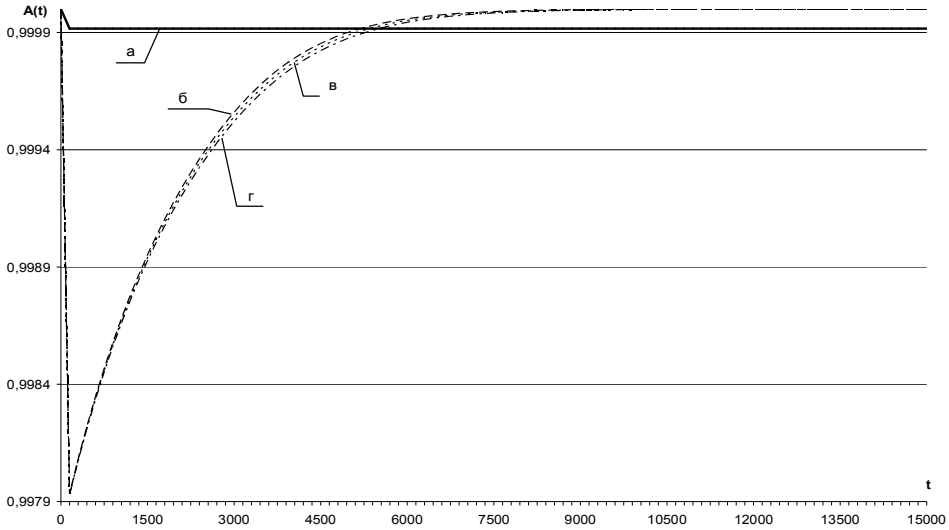

Рис. 5. Графічні залежності зміни функції готовності ІУС від часу експлуатації системи для однофрагментної моделі (а) і при різних значеннях D: б) D = 1; в) D = 0,9; г) D = 0,8

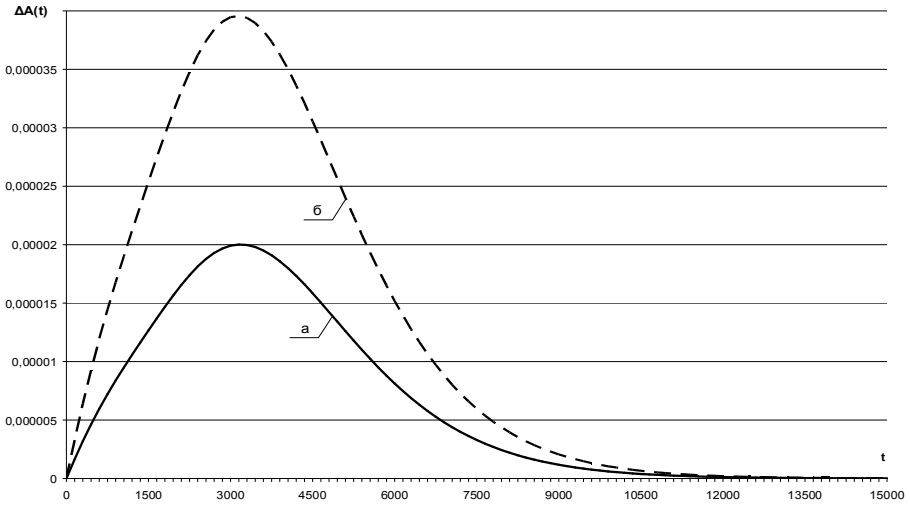

Рис. 6. Деталізація рис. 5 у вигляді графічної залежності різниці між значеннями функції готовності: а) при D = 0,8 і D = 0,9; б) при D = 0,8 і D = 1

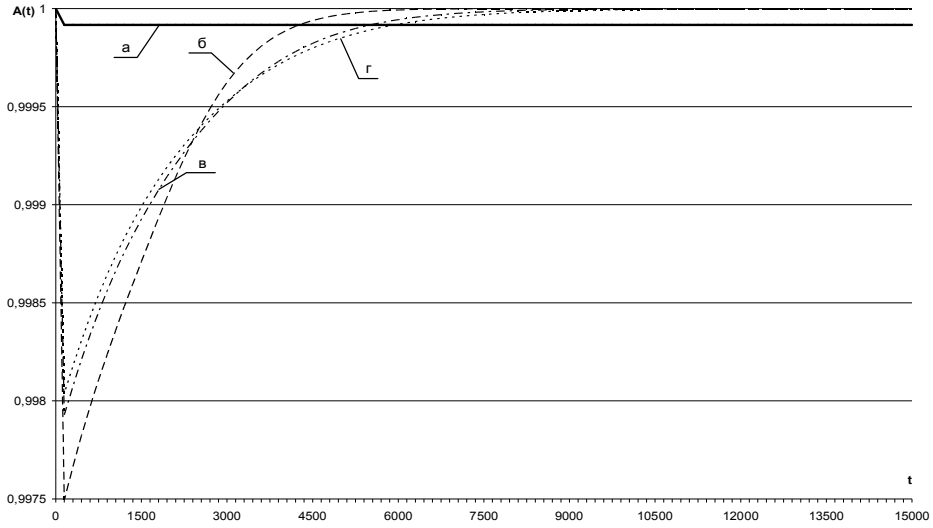

Рис. 7. Графічні залежності зміни функції готовності ІУС від часу експлуатації системи для однофрагментної моделі (а) і при різних значеннях λ_{ver}: б) λ_{ver} = 1,39*10–3; в) λ_{ver} = 4,63*10–4; г) λ_{ver} = 2,31*10–4

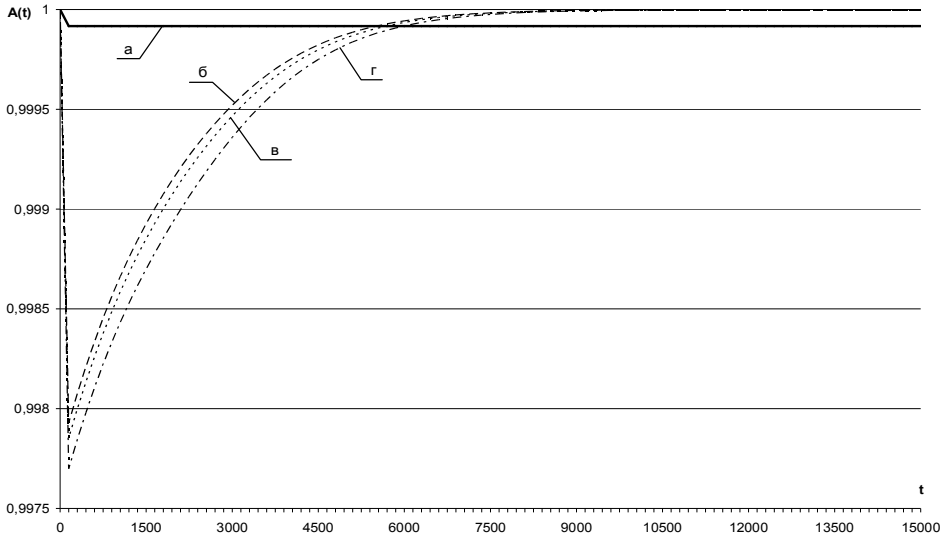

Рис. 8. Графічні залежності зміни функції готовності ІУС від часу експлуатації системи для однофрагментної моделі (а) і при різних значеннях μ_{ver}: б) μ_{ver} = 2; в) μ_{ver} = 1,5; г) μ_{ver} = 1

Висновки. Напрямки подальших досліджень

У статті проведений аналіз ПЗ ІУС КС як об'єкта верифікації, нормативної бази в даній галузі й відповідності існуючих методів верифікації програмного забезпечення специфіці космічних систем. Відомі методи не враховують повною мірою можливість, а за певних умов необхідність і доцільність проведення верифікації ПЗ ІУС КС в умовах польоту і його корекції за результатами верифікації. Уведене поняття оперативної коригувальної верифікації, яка може проводитися за різними сценаріями для функцій різного рівня критичності. Це поняття, на наш погляд, важливо в методологічному плані і є складовою процесів відновлення систем, що частково обслуговуються, які, у свою чергу, відносяться до систем реального часу, що еволюціонують [20]. Представлений теоретико-множинний опис функцій за рівнями критичності, цілей і операцій ОКВ, множини сценаріїв, показників і моделей є базою для створення процедур оперативної верифікації ПЗ й оцінних моделей готовності ІУС КС.

З практичної точки зору це може бути важливо для розробки більш детальних вимог і методик проведення верифікації й корекції ПЗ ІУС КС та інших систем для критичних додатків, що допускають оперативне відновлення.

Подальші дослідження доцільно спрямовувати на розробку процедур вибору стратегій верифікації, а також архітектування систем з оперативною коригувальною верифікацією.

У статті даний теоретико-множинний опис функцій за рівнями критичності, цілей і операцій ОКВ,

запропонована множина сценаріїв, показників і математичних моделей для систем з програмним забезпеченням, що коригується. Ці елементи разом із описом критичності функцій і операцій верифікації формують методологічну базу ОКВ.

Із практичної точки зору слід використовувати її для розробки більш детальних вимог, методик і програмно-апаратних засобів для проведення верифікації й корекції ПЗ ІУС КС, що допускають оперативне відновлення. У теоретичному плані доцільно розробити й досліджувати моделі готовності для різних сценаріїв, а також процедур вибору стратегій верифікації, мінімізуючих ресурси при заданому рівні безпеки.

Література

1. *Безопасность критических инфраструктур: математические и инженерные методы оценки и обеспечения / Под ред. В.С. Харченко. – Х.: Нац. аэрокосм. ун-т «ХАИ». – 2011. – 603 с.*

2. *Липаев, В.В. Функциональная безопасность программных средств [Текст] / В.В. Липаев. – М.: Синтег. – 2004. – 348 с.*

3. *Липаев, В.В. Обеспечение качества программных средств. Методы и стандарты [Текст] / В.В. Липаев. – М.: Синтег. – 2001. – 380 с.*

4. *Оценка и обеспечение качества программных средств космических систем [Текст]/ под ред. В.С. Харченко, Б.М. Конорева. – Харьков: Нац. аэрокосм. ун-т «ХАИ». – 2007. – 244с.*

5. *Галузева система управління якістю. Гарантоздатність програмно-технічних комплексів критичного призначення. Настанова Національного космічного агентства України СОУ-Н НКАУ 0060:2010 [Текст] / Харченко В.С. (наук. керівник розробки). – 2011. – 60 с.*

6. *Галузева система управління якістю. Вимоги до функціональної безпеки програмного забезпечення програмно-технічних комплексів критичного призначення. Настанова Національного космічного агентства України СОУ-Н НКАУ 0058:2009 [Текст] / Харченко В.С. (наук. керівник розробки). – 2009. – 57 с.*

7. *Галузева система управління якістю. Методи оцінки показників якості програмного забезпечення програмно-технічних комплексів критичного призначення. Настанова Національного космічного агентства України СОУ-Н НКАУ 0031:2007 [Текст] / Конорев Б.М. (наук. керівник розробки). – 2007. – 127 с.*

8. *Галузева система управління якістю. Процеси життєвого циклу програмного забезпечення програмно-технічних комплексів критичного призначення. Настанова Національного космічного агентства України СОУ-Н НКАУ 0061:2011 [Текст] / Харченко В.С. (наук керівник розробки). – 2011. – 123 с.*

9. *Галузева система управління якістю. Верифікація програмного забезпечення програмно-технічних комплексів критичного призначення. Настанова Державного космічного агентства України СОУ-Н ДКАУ (проект) [Текст] / Харченко В.С. (наук. керівник розробки). – 2011. – 80 с.*

10. *Александровская, Л.Н. Теоретические основы испытаний и экспериментальная отработка сложных технических систем [Текст] / Л.Н. Александровская, В.И. Круглов, А.Г. Кузнецов. – М.: Логос. – 2003. – 347 с.*

11. *Кульба, В.В. Проектирование информационно-управляющих систем орбитальных станций [Текст] / В.В. Кульба, Е.А. Микрин, Б.В. Павлов. – М.: Наука, 2002. – 343 с.*

12. *Avizienis, A. Basic concepts and taxonomy of dependable and secure computing [Text]/ A. Avizienis , J.-C. Laprie, B. Randell, C. Landwehr // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.*

13. *Харченко, В.С. Гарантоспособность и гарантоспособные системы: элементы методологии [Текст]/ В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. – № 5(17). – С. 7–19.*

14. *Bender, Marc. Positioning Verification in the Context of Software/System Certification [Text]/ Marc Bender, Tom Maibaum, Mark Lawford, Alan Wassyng // Proceedings of the 11th International Workshop on Automated Verification of Critical Systems (AVoCS 2011). – Necastle-upon-Tyne. - 2011. – 15 p.*

15. *Инвариантo-ориентированная оценка качества программных средств космических систем [Текст] / Под ред. Б.М. Конорева, В.С. Харченко. – Х.: Нац. аэрокосм. ун-т «ХАИ». – 2009. – 223 с.*

16. *Formal Methods for Industrial Applications. LNCS 1165. [Text] / J.-R. Abrial (ed.). - Springer . - 1996. – 523 p.*

17. *Clarke, E. Model Checking [Text]/ E. Clarke, O. Grumberg, D. Peled. – The MIT-Press, – 2000. – 330 p.*

18. *Харченко, В.С. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов [Текст]/ В.С. Харченко, О.Н. Одарущенко, Е.Б. Одарущенко // Радіоелектронні і комп'ютерні системи. – 2006. – № 5(17). – С. 62-70.*

19. *Одарущенко, О.Н. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем [Текст] / О.Н. Одарущенко, Е.Б. Одарущенко, Ю.Л. Поночовный // Авиационно-космическая техника и технология. – Х.: Национальный аэрокосмический университет „ХАИ", 2002. – Вып. 35. – С. 187-191.*

20. *Kharchenko, V.S. Dependable Systems and Multi-Version Computing: Aspects of Evolution [Text] / V.S. Kharchenko // Radio Electronic and Computer Systems. – 2009. – № 7 (41). – P. 46-60.*

Надійшла до редакції 7.11.2011

Рецензент: д-р техн. наук, проф., зав. каф. виробництва радіоелектронних систем літальних апаратів В.М. Ілюшко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ЭЛЕМЕНТЫ МЕТОДОЛОГИИ ОПЕРАТИВНОЙ КОРРЕКТИРУЮЩЕЙ ВЕРИФИКАЦИИ ПРОГРАММНЫХ СРЕДСТВ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ КОСМИЧЕСКИХ АППАРАТОВ

В.С. Харченко, Н.В. Замирец, С.А. Засуха, Ю.Л. Поночовный

Проведен анализ программного обеспечения (ПО) информационно-управляющих систем (ИУС) космических систем (КС) как объекта верификации, нормативной базы и существующих методов верификации ПО КС. Введено понятие оперативной корректирующей верификации (ОКВ), которая может проводиться по разным сценариям для функций разного уровня критичности. Определены этапы и операции по верификации ПО ИУС КС на разных этапах. Дано детальное описание операций этапа разработки ПО ИУС КС. Дано формальное описание целей верификации ПО ИУС КС. Уточнены цели оперативной ОКВ ПО в полете, и предложено теоретико-множественное описание функций с учетом их критичности и целей ОКВ. Описаны сценарии и показатели для оценки готовности ИУС КС при реализации ОКВ. Дано краткое описание моделей готовности для разных сценариев ОКВ. Определены понятие стратегии ОКВ и особенности ее формирования. Разработана и исследована модель готовности одной из систем с ОКВ.

Ключевые слова: ИУС космических систем, программное обеспечение, оперативная корректирующая верификация, модели готовности

ELEMENTS Of METHODOLOGY Of OPERATIVE CORRECTING SOFTWARE VERIFICATION OF SPACECRAFT INSTRUMENTATION&CONTROL SYSTEMS

V.S. Kharchenko, N.V. Zamirets, S.A. Zasukha, Yu.L. Ponochevniy

Software (SW) for the Space Instrumentation and Control systems (SICS) as object of verification, normative base and existed verification methods of SICS SW are analyzed. The concept of on-line correcting verification (OCV) which can be performed under different scenarios for functions of different criticality is entered. OCV is carried on in flight when required trustworthiness of checking cannot be provided on the ground or when checking of functions on the ground is impossible or more expensive at guaranteeing of safety requirements. Stages and operations of SICS SW verification at different stages of lifecycle are discussed. The detailed description of operations for SICS SW development phase is given. The formal description of the Space SICS SW) verification purposes is given. The purposes of operative correcting verification SW in flight are specified, and the theoretical-set description of functions in view of their criticality and OCV purposes is offered. Scenarios and indicators for an estimation of SICS availability are proposed taking into account OCV features. The brief description of SICS availability models for different OCV scenarios is given. Concept of OCV strategy and features of its formation are defined. The availability model for one of the SICSs with OKV is developed and researched.

Keywords: space instrumentation and control system, software, on-line correcting verification, availability model.

Харченко В'ячеслав Сергійович – д-р техн. наук, проф., зав. каф. комп'ютерних систем і мереж, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАЇ», Харків, Україна, e-mail: V.Kharchenko@khai.edu.

Замірець Микола Васильович – д-р техн. наук, проф., директор Науково-дослідного технологічного інституту приладобудування, Харків, Україна, e-mail: zamyrets@nitip.nkau.ua.

Засуха Сергій Олексійович – заступник голови Державного космічного агентства України з питань створення ракетно-космічної техніки, Київ, Україна, e-mail: yd@nkau.gov.ua.

Поночовний Юрій Леонідович – канд. техн. наук, старший науковий співробітник, старший викладач кафедри комплексів військового зв'язку, Військовий інститут телекомунікацій і інформатизації Національного технічного університету України «Київський політехнічний інститут» e-mail: pnch1@rambler.ru.