УДК 004.519.217

С.А. Засуха[1], Ю.Л. Поночовный[2]

[1]*Национальное космическое агентство Украины, Киев*
[2]*Военный институт телекоммуникаций и информатизации Национального технического университета Украины „КПИ“, Полтава*

МОДЕЛЬ ГОТОВНОСТИ ДВУХКАНАЛЬНОЙ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ КОСМИЧЕСКОГО АППАРАТА С ОПЕРАТИВНОЙ ВЕРИФИКАЦИЕЙ ПРОГРАММНЫХ СРЕДСТВ

В статье рассмотрена многофрагментная модель информационно-управляющей системы обслуживаемого космического аппарата. При построении модели учтены проведение оперативной верификации отдельных функций программных средств в процессе эксплуатации системы, а также устранение выявленных программных дефектов. По результатам моделирования сделаны выводы о способах определения оптимальных временных параметров проведения верификации.

Ключевые слова: *многофрагментное моделирование, оперативная корректирующая верификация, модификация программных средств.*

Введение

Постановка проблемы. Ракетно-космическая отрасль является одним из важнейших секторов мировой экономики. Возможности ракетно-космической техники, ее надежность и безопасность существенно зависят от характеристик информационно-управляющих систем (ИУС), качества их аппаратных средств и программного обеспечения. Как известно, космические аппараты (КА) могут быть пилотируемыми и беспилотными. В данной работе рассмотрены пилотируемые КА, в которых предусмотрено восстановление работоспособного состояния аппаратных средств ИУС. Обеспечение качества и надежности программных средств (ПС) является одной из ключевых задач, решаемых разработчиками, испытателями, экспертами в этой области.

Оценку качества критических ПС необходимо проводить с учетом ряда присущих ему особенностей, в частности учитывая частые модификации и реинжиниринг ПО в процессе эксплуатации космического комплекса.

При стандартном подходе разработка критических ПС является дорогостоящим процессом, причем большую часть затрат занимает не создание программного кода, а его квалификационные испытания. Термин «квалификационные испытания» в стандартах ECSS [1] используется для обозначения «общего множества действий по верификации и валидации критического программного обеспечения».

Квалификационные испытания предназначены для подтверждения путем предоставления объективных доказательств того, что адекватные спецификации требований и входы (исходные данные, входные данные) существуют для любой деятельности, а выходы деятельности корректны и совместимы со спецификациями и входами. В более широком контексте на системном уровне нормативными документами Национального космического агентства Украины этот термин используется для обозначения оценки «готовности к серийному производству» и, соответственно, к использованию по назначению оборудования элемента космического комплекса, включающего, в общем случае, аппаратные и программные компоненты [2].

Высокая стоимость испытаний связана с необходимостью моделирования в земных условиях внешних условий окружающего открытого космического пространства. Применение на КА программных средств с возможностью их модификации позволяет более гибко распределять этапы верификации. Так, ряд некритических программных функций можно оперативно верифицировать после запуска космического аппарата в ходе его эксплуатации. Однако, учитывая высокую критичность ПС, выбор такой стратегии верификации необходимо предварительно обосновать с помощью математических моделей.

Анализ литературных источников. Известны несколько подходов к моделированию систем с изменяемыми параметрами, основанных на натурном эксперименте [3], методе Монте-Карло [4], аналитических методах исследования Байесовских моделей [5] и аппарате марковских и полумарковских процессов [6]. Использование аппарата марковских (полумарковских) процессов является, предпочтительным подходом, поскольку позволяет систематизировать сам процесс моделирования (определение множества состояний, переходов между ними, интенсивностей переходов). В [7] развит системный поход к построению многофрагментных моделей, однако в

нем не предусмотрено проведение дополнительных процедур верификации ПС.

Целью данного исследования является разработка и анализ модели готовности ИУС пилотируемых КА при проведении оперативной корректирующей верификации программных функций. Предложена методика построения модели на основе определения множеств состояний и механизмов взаимодействия. Для оценки функции готовности выполнены расчет и исследования марковской модели для различных наборов входных данных.

Основной материал

1. Основные допущения моделирования. Для построения модели готовности ИУС КА приняты следующие допущения:

– в данной работе рассматривается наиболее распространенная архитектура ИУС КА, которая включает два взаиморезервированных аппаратных канала, в каждом из которых функционирует одинаковая версия ПС, систему контроля за работоспособностью АС будем считать абсолютно надежной;

– ИУС в любой момент времени может находиться либо в работоспособном, либо в неработоспособном состоянии, а потоки событий, переводящих систему из одного функционального состояния в другое – простейшие;

– восстановление ИУС после отказа, вызванного программным дефектом производится с помощью перезапуска ПС;

– в процессе функционирования ИУС выполняется верификация программных функций, состояние верификации является неработоспособным;

– устранение программных дефектов выполняется после их проявления как системных отказов, либо же после их обнаружения в процессе оперативной верификации с вероятностью обнаружения D;

– в ходе исправления программных дефектов, новые дефекты не вносятся;

– допускается полное устранение всех невыявленных дефектов.

2. Обоснование входных параметров модели. В ходе проведения исследований с целью выявления характера изменения поведения функции готовности, часть входных параметров модели имели фиксированные значения, остальные параметры изменялись в пределах заданных интервалов значений. Фиксированные значения имеют следующие параметры:

– интенсивность отказов одного аппаратного канала $\lambda_{HW} = 3*10^{-4}$ (1/час);

– интенсивность восстановления одного аппаратного канала $\mu_{HW} = 1$ (1/час);

– начальная интенсивность отказов ПС $\lambda_{SW\ 0} = 4*10^{-3}$ (1/час);

– интенсивность восстановления системы после проявления программного дефекта (путем перезапуска ПС) $\mu_{SW} = 2$ (1/час);

– интенсивность отказов ПС после устранения всех дефектов равна нулю $\lambda_{SW\ k} = 0$ (1/час).

Для исследования готовности системы были приняты следующие изменяемые значения входных параметров:

Таблица 1

Переменные значения входных параметров модели

Параметр модели	Переменные значения параметров		
$\Delta\lambda_{SW}$ (1/час)	$1\cdot10^{-3}$	$5\cdot10^{-4}$	$1\cdot10^{-4}$
D	0,8	0,9	1
λ_{ver} (1/час)	$1{,}39\cdot10^{-3}$	$4{,}63\cdot10^{-4}$	$2{,}31\cdot10^{-4}$
μ_{ver} (1/час)	1	1,5	2

Также при моделировании можно выделить «базисные» значения изменяемых входных параметров:

– шаг изменения интенсивности отказов ПС $\Delta\lambda_{SW} = 5*10^{-4}$ (1/час);

– вероятность обнаружения программного дефекта при верификации ПС D = 0,8;

– интенсивность проведения верификации ПС $\lambda_{ver} = 4{,}63*10^{-4}$ (1/час);

– интенсивность восстановления работоспособного состояния системы после проведения верификации ПС $\mu_{ver} = 2$ (1/час).

3. Разработка и исследование модели готовности ИУС КА. С учетом принятых допущений, в качестве метода исследования принимается марковский анализ, а учет изменения интенсивности отказов λ_{SW} осуществляется с помощью аппарата регулярных многофрагментных марковских моделей (РМФМ) [7]. Поэтому в качестве базовой модели выбрана РМФМ, граф которой изображен на рис. 1.

Процесс функционирования ИУС происходит следующим образом. В начальный момент система реализует все предписанные функции и находится в состоянии S_0. В процессе функционирования проявляются аппаратные дефекты, вследствие чего система последовательно переходит в состояния S_1 (отказ одного из аппаратных каналов, система работоспособна), S_2 (отказ сразу двух аппаратных каналов, система неработоспособна) и восстанавливаются (система возвращается в состояния S_0 и S_1. Через определенный временной интервал происходит отказ системы, вызванный программным дефектом, и она переходит в состояние S_3. После проявления дефекта ПС, он, естественно, обнаруживается, и устраняется, вследствие чего система после восстановления переходит в следующий фрагмент РМФМ (состояние S_{5i}), который характеризуется новым параметром $\lambda_{SW\,i}$. Также через определенный временной интервал выполняется оперативная корректирующая верификация части программных функций, система переходит в состояние S_4. В ходе про-

ведения процедур верификации с вероятностью D возможно обнаружение и устранение программных дефектов, вследствие чего система также переходит в новый фрагмент РМФМ.

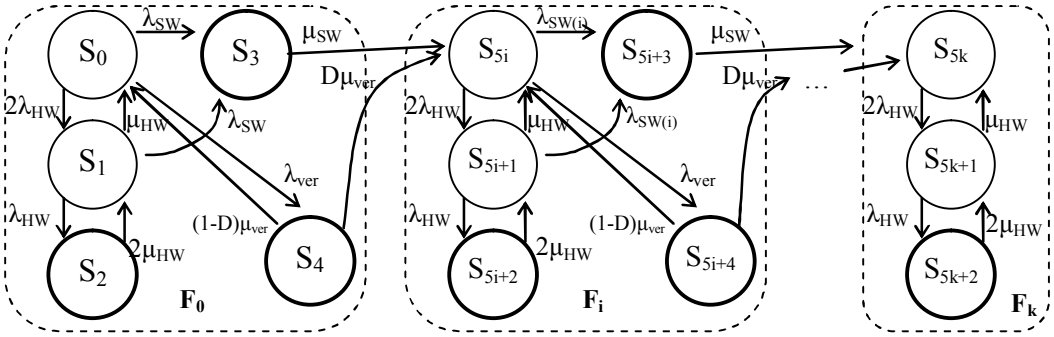

Рис. 1. Размеченный граф функционирования ИУС обслуживаемого КА при проведении оперативной корректирующей верификации программных функций

В последнем фрагменте модели все программные дефекты устранены, и в системе происходят только отказы аппаратных средств. Система дифференциальных уравнений Колмогорова для модели надежности, граф которой изображен на рис. 1 будет состоять из следующих регулярных блоков:

Для начального 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 внутренних фрагментов F_i:

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

Для последнего фрагмента F_k:

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

Здесь i – номера внутренних фрагментов; k – номер последнего фрагмента,

Значение функции готовности определяется из выражения:

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

При исследовании модели особый интерес представляет начальный этап функционирования системы, поэтому при расчетах рассматривался временной интервал T = 15000 часов (примерно 1,5 года) с количеством участков интегрирования – 100. Выходные результаты получены с помощью модифицированного экспоненциального метода численного решения жестких систем дифференциальных уравнений [8].

Результаты вычислений представлены в виде графической зависимости функции готовности от времени функционирования систем на рис. 2 – рис. 6. Результирующие функции сравниваются со стационарным коэффициентом готовности дублированной одноверсионной ИУС, полученным при неизменных начальных параметрах λ_{HW}, μ_{HW}, $\lambda_{SW\,0}$, μ_{SW} с помощью однофрагментного моделирования.

Анализ графиков на рис. 2 показал, что значение параметра $\Delta\lambda_{sw}$ в большей мере влияет на скорость устранения дефектов (чем больше $\Delta\lambda_{sw}$, тем быстрее функция готовности многофрагмент-

ной модели переходит в стационарное состояние). Кроме того, значение $\Delta\lambda_{sw}$ косвенно влияет на величину минимума функции готовности на начальном этапе эксплуатации системы.

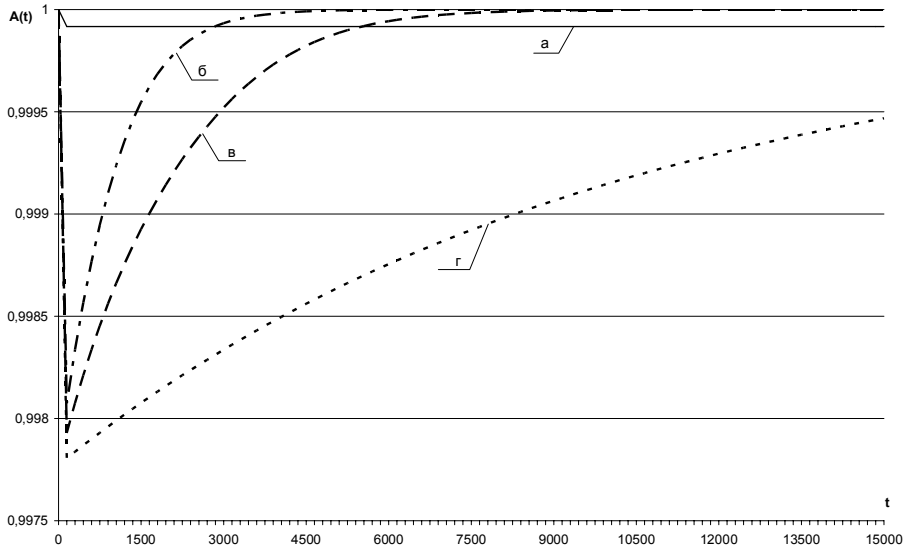

Рис. 2. Графические зависимости изменения функции готовности ИУС от времени эксплуатации системы для однофрагментной модели (а) и при различных значениях $\Delta\lambda_{sw}$: б – $\Delta\lambda_{sw}=10^{-3}$; в – $\Delta\lambda_{sw}=5*10^{-4}$; г – $\Delta\lambda_{sw}=10^{-4}$

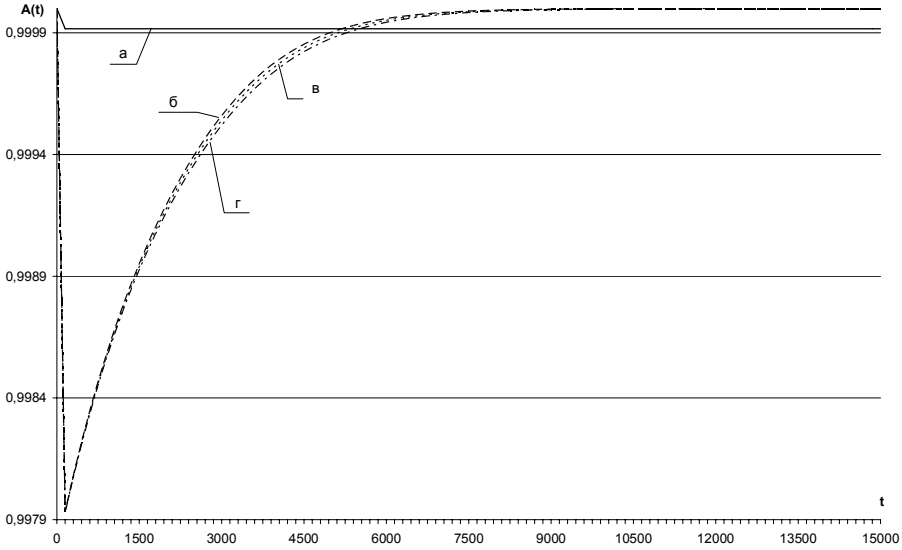

Рис. 3. Графические зависимости изменения функции готовности ИУС от времени эксплуатации системы для однофрагментной модели (а) и при различных значениях D: б – D = 1; в – D = 0,9; г – D = 0,8

Из рис. 3 видно, что с повышением вероятности выявления дефектов при оперативной верификации ПС, готовность системы несущественно увеличивается на временном интервале 1000…7000 часов. Для более наглядного представления данного выигрыша на рис. 4 показаны графики разности между готовностью системы при различных значениях параметра D. Столь малый выигрыш в готовности объясняется тем, что в принятых значениях входных данных интенсивности проведения верификации и проявления дефектов ПС имеют один порядок. Это значит, что если программный дефект не будет выявлен при верификации, он в скором времени все равно проявится в виде отказа.

Кроме того, значение параметра D никак не влияет на величину минимума функции готовности, а также на скорость перехода этой функции в стационарный режим.

Анализ графиков на рис. 5 показал, что значение параметра λ_{ver} одновременно влияет на величину минимума функции готовности и на скорость перехода функции в стационарный режим. При этом характер влияния не такой, как у параметра $\Delta\lambda_{sw}$: с ускорением перехода функции готовности в стационарный режим при более частом проведении процедур оперативной корректирующей верификации, минимум функции готовности принимает меньшие значения на начальном этапе эксплуатации системы.

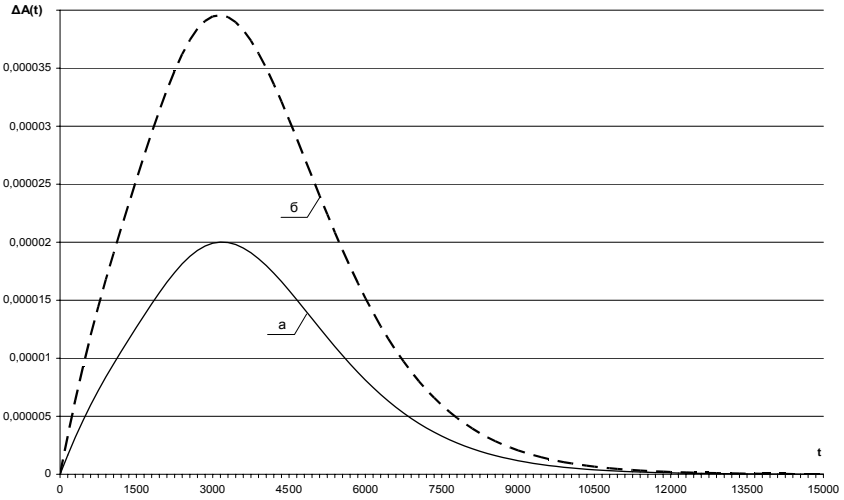

Рис. 4. Детализация рис. 3 в виде графической зависимости разности между значениями функции готовности: а – при D = 0,8 и D = 0,9; б – при D = 0,8 и D = 1

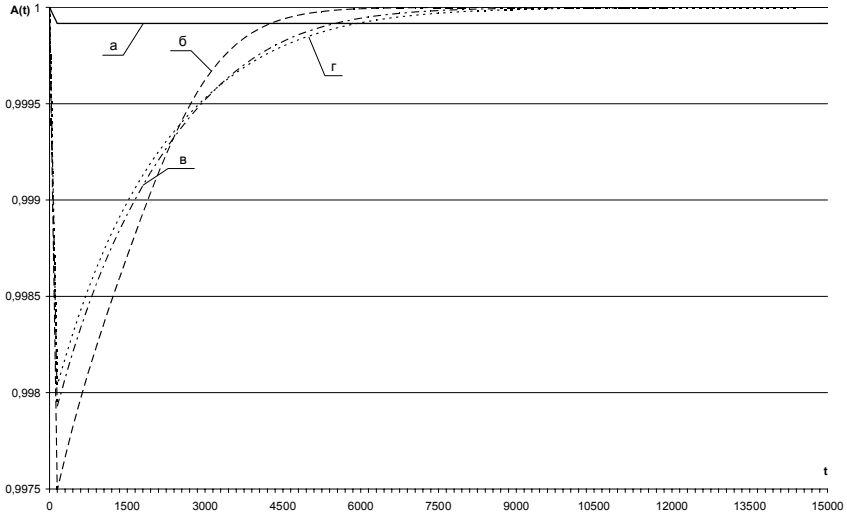

Рис. 5. Графические зависимости изменения функции готовности ИУС от времени эксплуатации системы для однофрагментной модели (а) и при различных значениях λ_{ver}: б – $\lambda_{ver} = 1{,}39*10^{-3}$; в – $\lambda_{ver} = 4{,}63*10^{-4}$; г – $\lambda_{ver} = 2{,}31*10^{-4}$

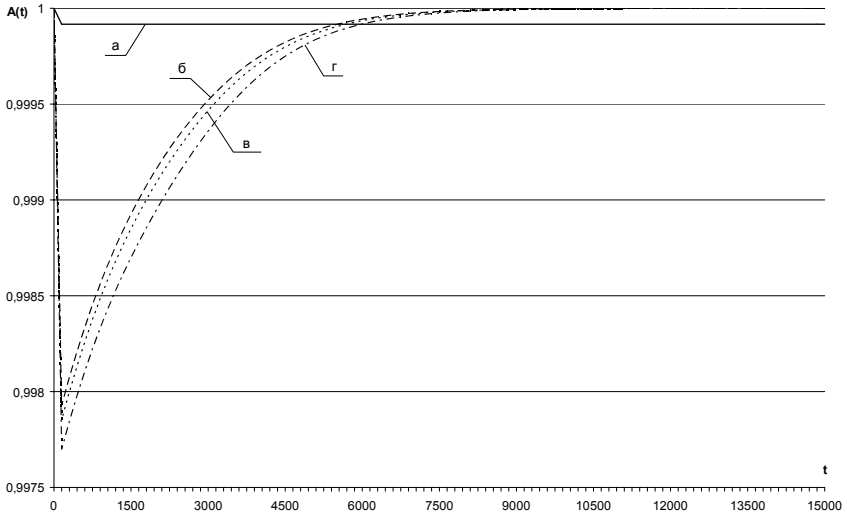

Рис. 6. Графические зависимости изменения функции готовности ИУС от времени эксплуатации системы для однофрагментной модели (а) и при различных значениях μ_{ver}: б – $\mu_{ver} = 2$; в – $\mu_{ver} = 1{,}5$; г – $\mu_{ver} = 1$

Из рис. 6 видно, что значение параметра μ_{ver} в большей мере влияет на величину минимума функции готовности многофрагментной модели, и практически не влияет на скорость перехода этой функции в стационарный режим.

Выводы

Анализ полученных результатов моделирования готовности ИУС обслуживаемого космического аппарата при проведении оперативной корректирующей верификации программных функций позволяет сформулировать следующие выводы.

1. Для ускорения перехода функции готовности в стационарное состояние необходимо повышать значения параметров $\Delta\lambda_{sw}$ и λ_{ver}, то есть более часто проводить процедуры верификации и стараться устранить большее количество программных дефектов за одну проверку.

2. В начальный период эксплуатации готовность систем с плановым проведением процедур оперативной верификации ниже, чем у систем без устранения дефектов ПС.

3. Повысить готовность систем на начальном периоде эксплуатации можно увеличивая значение параметра μ_{ver}, то есть ускорив восстановление работоспособного состояния системы.

Планируется включить разработанную модель и полученные результаты в комплексную методику выбора и обоснования параметров стратегии проведения верификации ИУС КА.

Список литературы

1. ECSS-Q-40B-2002 Space product assurance. Safety (Гарантия продукции космического назначения. Безопасность). – Нордвик: Европейская комиссия по космической стандартизации, 2002.- 42 с.

2. Скляр В.В. Анализ безопасности и выбор технологий реализации информационно-управляющих систем АЭС: риск-ориентированный подход / В.В. Скляр, В.С. Харченко, А.А. Ушаков // Екологія і ресурси: Зб. наук праць Інституту проблем національної безпеки. – К.: ІПНБ, 2006. – № 13. – С. 39-64.

3. Experimenting With Exception Handling Mechanisms Of Web Services Implemented Using Different Development Kits / A. Gorbenko, A. Mikhaylichenko, V. Kharchenko, A. Romanovsky // CS-TR 1010, University of Newcastle upon Tyne, 2007. – P. 67-78.

4. Rotaru T. Service-oriented middleware for financial Monte Carlo simulations on the cell broadband engine / T. Rotaru, M. Dalheimer, F.-J. Pfreundt – Concurrency and Computation: Practice and Experience, John Wiley & Sons, Ltd, 2009. – 348 p..

5. Gashi I. Uncertainty Explicit Assessment of Off-The-Shelf Software: A Bayesian Approach / I. Gashi, P. Popov, V. Stankovic // Elsevier Journal of Information and Software Technology. – Elsevier, 2009. – 51(2). – P. 497-511.

6. Chan P. Making Services Fault Tolerant / P. Chan, M. Lyu, M. Malek // ISAS 2006, LNCS 4328. – 2006. – P. 43-61.

7. Харченко В.С. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов / В.С. Харченко, О.Н. Одарущенко, Е.Б. Одарущенко // Радіоелектронні і комп'ютерні системи. – 2006. – Вип. 5(17). – С. 62-70.

8. Одарущенко О.Н. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем / О.Н. Одарущенко, Е.Б. Одарущенко, Ю.Л. Поночовный // Авиационно-космическая техника и технология. – Х.: Изд-во НАКУ „ХАИ", 2002. – Вып. 35. – С. 187-191.

Поступила в редколлегию 2.09.2011

Рецензент: д-р техн. наук проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

МОДЕЛЬ ГОТОВНОСТІ ДВОКАНАЛЬНОЇ ІНФОРМАЦІЙНО-УПРАВЛЮЧОЇ СИСТЕМИ КОСМІЧНОГО АПАРАТУ З ОПЕРАТИВНОЮ ВЕРИФІКАЦІЄЮ ПРОГРАМНИХ ЗАСОБІВ

С.О. Засуха, Ю.Л. Поночовний

У статті розглянута багатофрагментна модель інформаційно-управлючої системи космічного апарату, що обслуговується. При побудові моделі враховані проведення оперативної верифікації окремих функцій програмних засобів в процесі експлуатації системи, а також усунення виявлених програмних дефектів. За результатами моделювання зроблені висновки про способи визначення оптимальних часових параметрів проведення верифікації.

Ключові слова: *багатофрагментне моделювання, оперативна верифікація, що коректує, модифікація програмних засобів.*

DEPENDABILITY MODEL OF THE SPACE VEHICLE TWO-CHANNEL INFORMATIONAL-OPERATING SYSTEM WITH OPERATIVE SOFTWARE VERIFICATION

S.A. Zasuha, Y.L. Ponochovnyi

In article it is observed multifragments model of the served space vehicle informational-management system. At model construction, also elimination of the revealed software defects are considered conducting of operative verification software separate functions while in service. By results of modeling leading-outs are drawn on ways of definition of optimum time parameters of verification conducting.

Keywords: *multifragments design, operative correcting верификация, modification of programmatic facilities.*