

УДК 004.052+004.519.217

Ю.Л. ПОНОЧОВНЫЙ¹, С.А. ЗАСУХА², В.С. ХАРЧЕНКО³¹Военный институт телекоммуникаций и информатизации
Национального технического университета Украины „КПИ“, Украина²Государственное космическое агентство, Украина³Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

ИССЛЕДОВАНИЕ ИМИТАЦИОННЫХ МОДЕЛЕЙ ГОТОВНОСТИ ДВУХКАНАЛЬНОЙ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ КОСМИЧЕСКОГО АППАРАТА

В статье рассмотрены особенности моделей готовности информационно-управляющих систем космических аппаратов. Для двухканальной одноверсионной структуры системы предложены имитационные модели, учитывающие изменение параметров потоков отказов программных средств вследствие проведения оперативной верификации или обновления программных функций. Указаны особенности построения имитационных моделей, проанализирована сходимость их результатов с аналитическими многофрагментными моделями. Сделаны выводы о возможности применения имитационных моделей при определении оптимального варианта проведения верификации и коррекции проектных дефектов и обновления функций системы в процессе ее применения.

Ключевые слова: имитационная модель, информационно-управляющие системы, оперативная верификация, обновление программных функций.

Введение

Развитие ракетно-космической отрасли напрямую связано с улучшением характеристик и повышением надежности информационно-управляющих систем (ИУС) космических аппаратов (КА), качества их аппаратных средств и программного обеспечения. Программные средства (ПС) современных КА относят к классу критических и имеют ряд особенностей, в частности, возможные модификации и реинжиниринг программного обеспечения в процессе длительной эксплуатации космического комплекса. Разработка критических ПС является дорогостоящим процессом, причем большую часть затрат занимает не создание программного кода, а его квалификационные испытания [1]. Применение в ИУС КА программных средств с возможностью их модификации (путем проведения обновлений в процессе их эксплуатации) позволяет более гибко распределять этапы верификации. Однако, учитывая высокую критичность ПС, такой выбор необходимо предварительно обосновать с помощью специальных моделей, учитывающих изменение параметров системы в процессе ее эксплуатации.

В существующих моделях систем с изменяемыми параметрами используют натурный эксперимент [2], методы имитационного моделирования [3], Байесовские методы исследования [4] и аппарат марковских и полумарковских процессов [5]. Систематизация процесса моделирования (определение множест-

ва состояний, переходов между ними, интенсивностей переходов) при использовании аппарата марковских (полумарковских) процессов делает этот подход более предпочтительным. В [6] представлены элементы общей методологии оперативной верификации (ОВ) программного обеспечения космических систем (теоретико-множественное описание целей, этапов, операций верификации и моделей для оценки готовности). В [7, 8] выполнено исследование отдельных многофрагментных моделей ИУС КА. Проведенные исследования показали, что для малых значений шага изменения интенсивности отказов ПС ($\Delta\lambda_{sw} < 3 \cdot 10^{-5}$), размерность многофрагментной модели превышает сто состояний размеченного графа, что, в свою очередь, увеличивает длительность численного решения системы дифференциальных уравнений Колмогорова. В результате возрастает длительность процедур поиска значений входных параметров, при которых обеспечивается требуемый уровень готовности системы.

В случаях, когда построение аналитической модели по определенным причинам усложняется, применяют метод статистических испытаний или метод Монте-Карло, когда вместо описания случайного явления с помощью аналитических выражений, проводится его моделирование процедурой, которая позволяет получить случайный результат. Применение метода статистических испытаний оправдано для сложных систем, которые состоят из большого количества элементов и в которых случайные факторы

определенным образом взаимосвязаны. Кроме того, моделирование случайных явлений методом Монте-Карло проводится с целью проверки достоверности результатов, полученных при применении определенного математического аппарата.

1. Постановка задачи исследования

В данной работе исследуется наиболее распространенная архитектура ИУС КА, которая включает два резервированных аппаратных канала (бортовых цифровых вычислительных комплекса), в каждом из которых функционирует одинаковая версия ПС (рис.1).

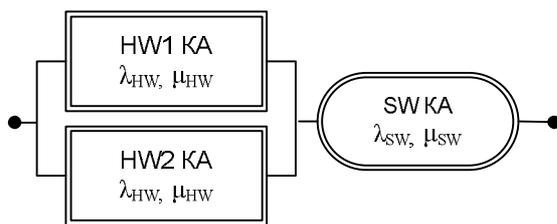


Рис. 1. Структурная схема надежности двухканальной одноверсионной ИУС КА

Условное обозначение такой структуры системы – S_{21} , где 2 – количество аппаратных каналов, 1 – количество версий ПС. При условии использования однотипного оборудования в резервированных аппаратных каналах, такая модель имеет четыре входных параметра:

- интенсивность отказов одного аппаратного канала λ_{HW} (1/час);
- интенсивность восстановления одного аппаратного канала μ_{HW} (1/час);
- интенсивность отказов ПС λ_{SW} (1/час);
- интенсивность восстановления системы после проявления программного дефекта μ_{SW} (1/час).

Другие входные параметры определяются причинами изменения ПС (ОВ либо обновление функций), а также особенностями соответствующей модели готовности системы [6].

В работе [9] представлены основные аспекты построения имитационных моделей систем с изменяемыми параметрами потоков отказов и восстановлений. Эти ключевые моменты положены в основу построения имитационных моделей двухканальной ИУС КА, которые рассмотрены в данной статье. Однако в [9] не учитывается специфика проведения процедур ОВ, а также функционирование системы в условиях проявления скрытых отказов. Эти особенности требуют совершенствования существующих моделей. Кроме того, необходимо рассмотреть во-

просы повышения точности и достоверности статистических испытаний.

Целью данного исследования является описание методики разработки имитационных моделей ИУС КА, изучение свойств этих моделей и возможности их использования совместно с аналитическими (многофрагментными) моделями при определении оптимального варианта проведения верификации, коррекции проектных дефектов и обновления функций ИУС в процессе применения КА. В работе последовательно рассмотрены особенности моделей готовности ИУС КА в соответствии с [6]; особенности разработанных имитационных моделей ИУС КА; результаты сравнения аналитических и имитационных моделей. В заключительной части представлены выводы и направления дальнейших исследований.

2. Модели готовности ИУС КА

Для оценки готовности в зависимости от множества сценариев MCS проведения ОКВ и обновления программных функций ИУС КА разработаны соответствующие модели готовности [6].

Модель 1 (сценарий SC1) характеризуется некоторым множеством состояний и переходов, обусловленных потоками отказов и восстановлений аппаратных средств (АС) и ПС с учетом архитектуры системы и возможностей обнаружения отказов и восстановления работоспособности.

Модель 2 (сценарий SC2) отличается от предыдущей тем, что возможно обнаружение и частичное устранение или парирование дефектов программных средств. Кроме того, в модели учитывается усложнение аппаратных средств для обеспечения оперативной коррекции в полете.

Модель 3 (сценарий SC3). Для данной модели характерна древовидная структура графа переходов, в котором есть расходящиеся ветви в зависимости от того, какое событие наступает: обнаружение дефекта или начало процесса верификации.

Модель 4 (сценарий SC4). Выполняются все виды верификации функций в наземных условиях, за исключением тех функций, проверка которых возможна в полете, и является более дешевой. Для сценария SC4 интенсивность перехода в состояние верификации (как и проявления дефектов) может быть выше.

Признаки описанных моделей можно представить в табулированном виде (табл.1). Таким образом, для дальнейших исследований выделено десять вариантов моделей готовности, уникальность каждой из которых определяется комбинацией набора входных параметров и размеченного графа состояний и переходов.

Таблица 1

Признаки классификации моделей готовности ИУС КА

№ п/п	Номер сценария	Номер модели	Условное обозначение модели	Характеристика изменения параметров	Короткая характеристика модели
1	SC1	М 1	МГ-1.0	все параметры постоянны	Однофрагментная (базовая) модель
2	SC1	М 1	МГ-1.1	увеличение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ max}$	Накопление программных дефектов с ростом интенсивности
3	SC2	М 2	МГ-2.1	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Коррекция ПС не проводится, ограничивается функционал
4	SC2	М 2	МГ-2.2	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Коррекция ПС проводится после обнаружения дефекта
5	SC2	М 2	МГ-2.3	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Коррекция ПС проводится после обновления ПС
6	SC3	М 3	МГ-3.1	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Коррекция ПС не проводится, ограничивается функционал после верификации ПС
7	SC3	М 3	МГ-3.2	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Дефекты ПС устраняются после верификации ПС
8	SC3	М 3	МГ-3.3	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Дефекты ПС устраняются после верификации ПС или после их проявления
9	SC4	М 4	МГ-4.1	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Дефекты ПС устраняются после верификации ПС
10	SC4	М 4	МГ-4.2	уменьшение λ_{sw} на $\Delta\lambda_{sw}$ до $\lambda_{sw\ min}$ (до 0)	Дефекты ПС устраняются после верификации ПС или после их проявления

3. Особенности построения имитационных моделей ИУС КА

В процессе исследования процесса функционирования ИУС КА использовался последовательный метод определения требуемого количества реализаций $n_{тр}$, который состоит из следующих этапов [10].

1. Построение первой реализации A_1 случайной величины A (готовности системы в определенный временной момент).

2. Построение реализации A_n ($n \geq 2$) случайной величины A , не зависящей от предыдущих $A_1 \dots A_{n-1}$ реализаций.

3. Определение оценки дисперсии реализаций величины A_n .

4. Определение точности δ оценки A по формуле $\delta = (t_{\alpha/2, n-1} \cdot S_n) / \sqrt{n}$, где $t_{\alpha/2, n-1}$ – квантиль распределения Стьюдента с $n - 1$ степенями свободы.

5. Проверка условия $\delta \leq \epsilon$, если условие не выполнено, то осуществляется возврат ко второму этапу с заменой n на $n + 1$, в противном случае принимается $n_{тр} = n$.

В работе [9] предложены схожие по построению и характеру имитационные модели, однако детальный анализ позволил выделить и устранить следующие недостатки предыдущих моделей:

1. На каждый канал (АС или ПС) ранее резервировалась четыре динамических массива, в которых хранились данные о временных промежутках – длительности отказов и восстановлений каждого канала и их состояниях (исправен/неисправен). В предложенной модели используется по одному динамическому

массиву на каждый канал, так как отпадает необходимость хранения каждого розыгрыша временного интервала, а состояния каждого канала в любом случае поочередно меняются начиная с исправного.

2. В предложенной модели увеличена размерность массива значений квантиля распределения Стьюдента с [3,100] до [4,1000], что позволило повысить достоверность моделирования до 0,999 и увеличить количество розыгрышей до 1000.

3. Для определения исправности системы в целом используется метод умножения логических состояний аппаратных каналов с последующим сложением с логическим состоянием программного канала, а также состояний обновления либо верификации (в предыдущих моделях использовался метод вложенных логических конструкций if...then):

$$z := \text{ssysw}[0] * \text{ssysw}[1] + \text{ssysw}[2] + \text{ssysw}[3] + \text{ssysw}[4],$$

где z – переменная состояния ИУС в целом, $\text{ssysw}[0]$ – булева переменная состояния первого канала АС, $\text{ssysw}[1]$ – булева переменная состояния второго канала АС, $\text{ssysw}[2]$ булева переменная состояния ПС, $\text{ssysw}[3]$ – булева переменная, соответствующая состоянию проведения обновлений ПС, $\text{ssysw}[4]$ – булева переменная, соответствующая состоянию проведения ОКВ (значения логических переменных соответственно: 0 – исправно, 1 – неисправно; переменной z : 0 – исправно, больше 0 – неисправно).

4. Количество начальных розыгрышей увеличено с 10 до 50, что позволяет уменьшить погрешность расчета выборочного среднего значения, относительного которого определяется результат розыгрыша $A(t_i)$ с заданной точностью ϵ .

4. Результаты вычислительного эксперимента с имитационными моделями и сравнительный анализ с результатами аналитического моделирования

На рис. 2 – 6 представлены графические результаты имитационного моделирования в виде функций готовности двухканальной одноверсионной системы. Для наглядного сравнения на этих графиках представлены также результаты аналогичных аналитических моделей. Из анализа графических зависимостей сделан вывод о высокой сходимости результатов аналитического и имитационного моделирования. При этом максимальное абсолютное расхождение результатов моделирования не превышает 10^{-5} для однофрагментного и 10^{-3} для многофрагментного моделирования, то

есть установочной величины ε – точности моделирования.

Из графиков (рис. 2 и 3) видно, что функция готовности, полученная с помощью имитационных моделей, соответствующих МГ-1.0 и МГ-2.1 располагается ниже результатов аналитического исследования указанных моделей. Это свидетельствует о заниженных в пределах погрешности (точности) ε результатах имитационного моделирования. Также следует отметить, что с помощью имитационной модели сложно исследовать тенденции (поведение) функции готовности, ведь если на рис. 3 интуитивно просматривается увеличение готовности в конце интервала исследования ($T = 15000$ часов), то из рис. 2 сложно судить о переходе функции готовности в стационарный режим по кривой (б).

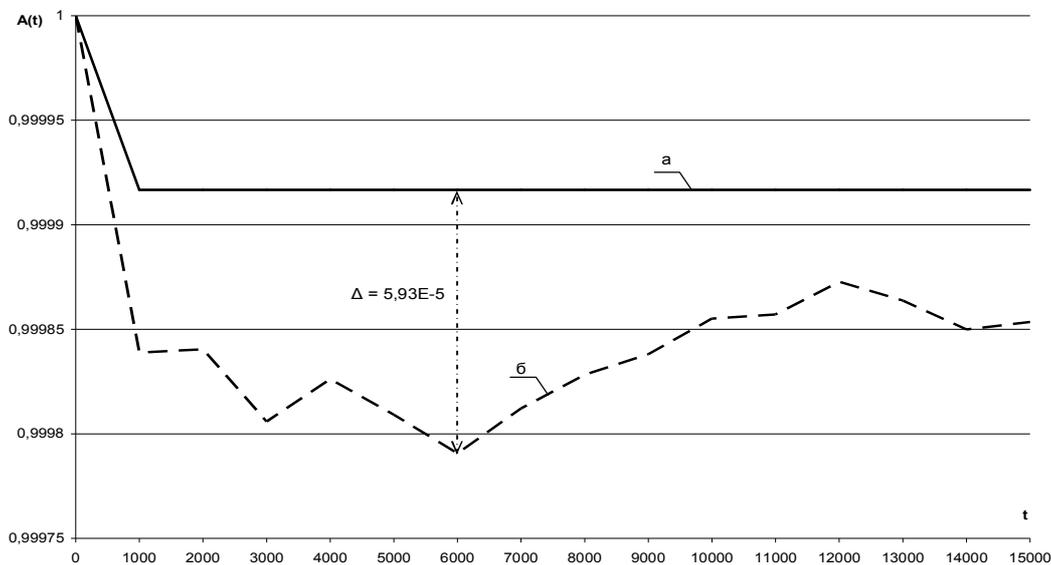


Рис. 2. Сравнение результатов аналитического (а) и имитационного (б) моделирования МГ-1.0

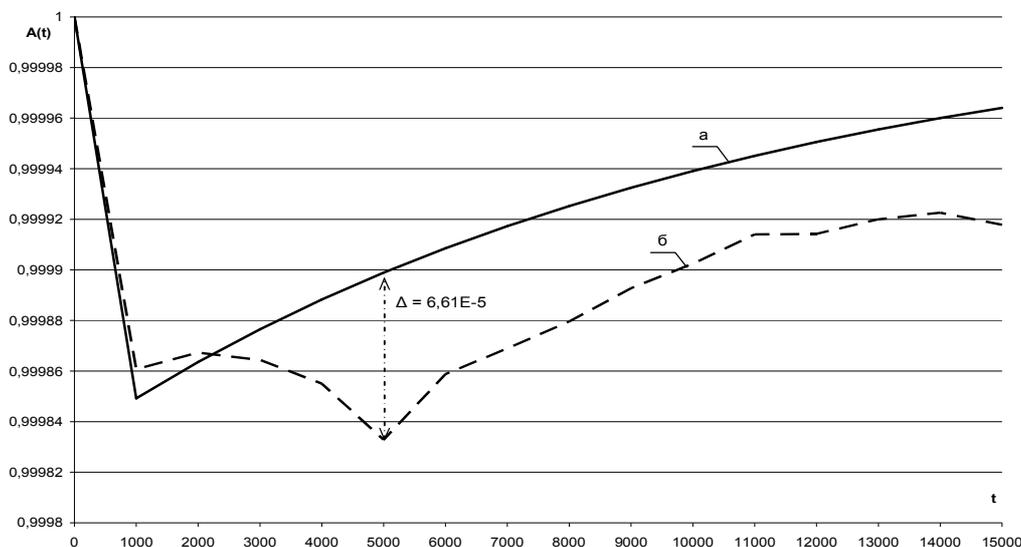


Рис. 3. Сравнение результатов аналитического (а) и имитационного (б) моделирования МГ-2.1

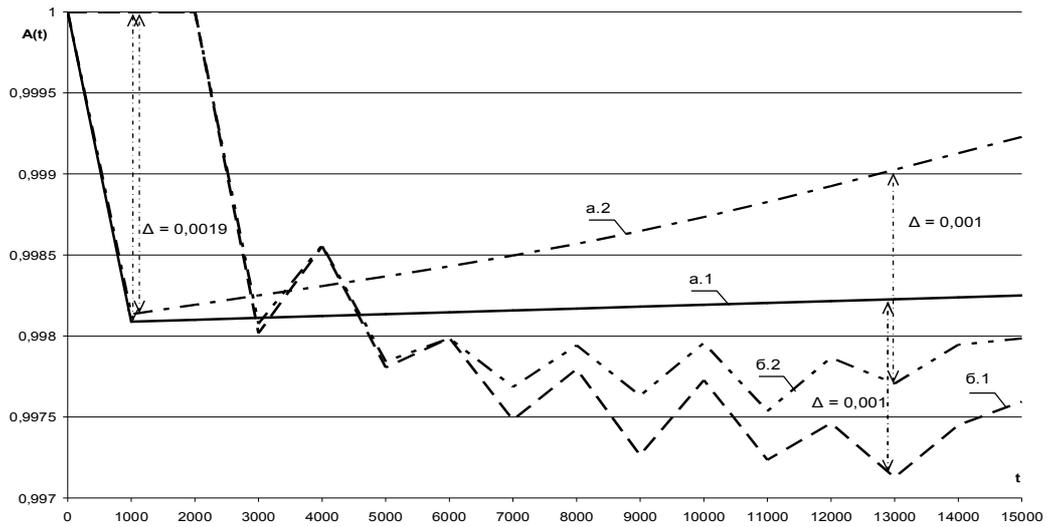


Рис. 4. Сравнение результатов аналитического (а.1 и а.2) и имитационного (б.1 и б.2) моделирования МГ-2.3 для двух наборов входных данных

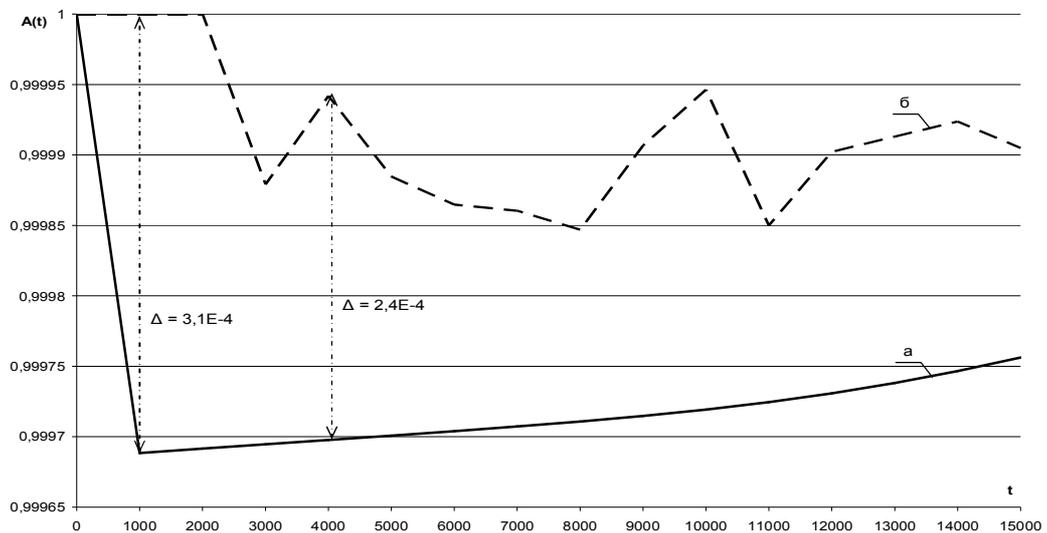


Рис. 5. Сравнение результатов аналитического (а) и имитационного (б) моделирования МГ-3.1

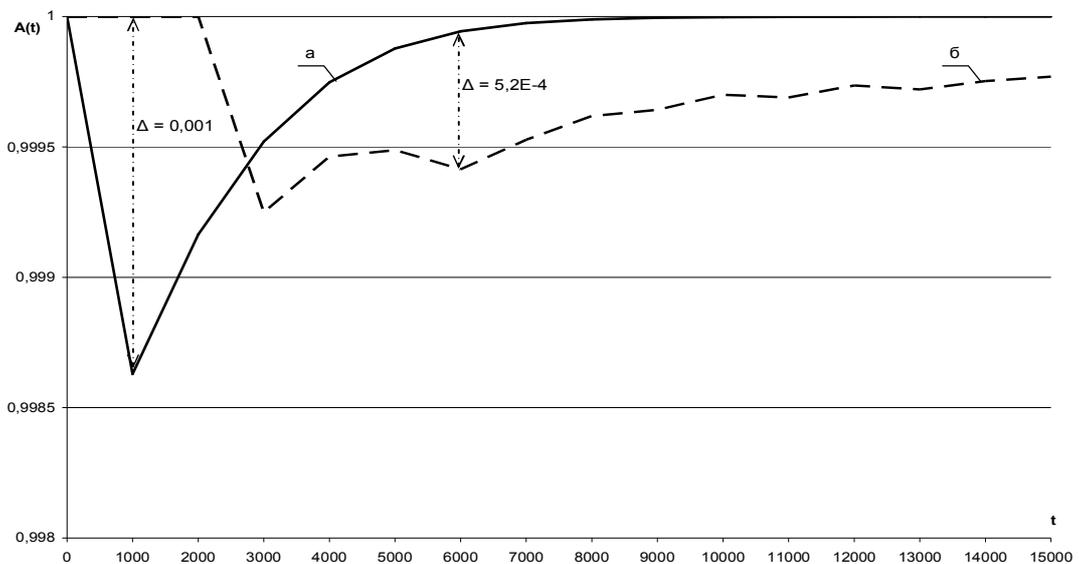


Рис. 6. Сравнение результатов аналитического (а) и имитационного (б) моделирования МГ-3.3

Анализ графиков на рис. 4 позволяет сделать вывод о том, что для модели МГ-2.3, которая учитывает обновление программных функций, имитационное моделирование характерно некоторой «инертностью», запаздыванием, что выражается в начальной погрешности на интервале (100...200 часов) и клинообразном расхождении между графиками имитационного и аналитического моделирования. Несмотря на наличие запаздывания, из рис. 4 видно, что графики (б.1) и (б.2) сохраняют соответствующие тенденции графиков (а.1) и (а.2) соответственно.

Результаты имитационного моделирования МГ-3.1 на фоне исследования других моделей выделяются превышением графика функции готовности над результатами аналитического моделирования. Для данной модели также характерно запаздывание графика имитационной модели, выраженное в повышенной погрешности на временном интервале (100...200 часов).

Для модели готовности МГ-3.3 характерно запаздывание функции готовности имитационной модели и заниженных в пределах погрешности (точности) ϵ результатах имитационного моделирования.

Следует отметить, что при работе с имитационными моделями скорость расчетов функции готовности зависит не только от сложности модели, но и от величины точности моделирования ϵ , а также от достоверности P (один из параметров распределения Стьюдента, в исследуемых моделях принимает дискретные значения [0,9; 0,95; 0,99; 0,999]).

Чем выше точность (меньшее значение ϵ) и чем больше достоверность P , тем больше выполняется розыгрышей и соответственно увеличивается время расчетов.

Кроме того, для «завышенных» комбинаций [ϵ, P] (например [$\epsilon=10^{-4}, P=0,999$] для МГ-2.3) расчеты с помощью имитационной модели невозможны, так как не выполняется условие $\delta \leq \epsilon$ и программа статистических исследований закликивается и требует принудительного завершения.

Выводы

Анализ полученных результатов моделирования надежности ИУС КА методом Монте-Карло позволяет сформулировать следующие выводы.

1. Применение имитационного моделирования, как и в случае применения многофрагментных моделей, позволяет описать процесс функционирования ИУС с учетом изменяющихся параметров ПС.

2. Применение метода Монте-Карло позволяет ускорить в 1,5 раза определение изменяющихся значений коэффициента готовности ИУС при умерен-

ных требованиях к точности моделирования ($\epsilon > 10^{-4}$) и достоверности ($P < 0,99$) по сравнению с применением многофрагментного моделирования.

3. Экспериментально подтверждена достоверность результатов, полученных с помощью аналитических многофрагментных моделей функционирования ИУС КА. Анализ графиков на рис.2 – рис.6 показал, что результаты аналитических и статистических испытаний отличаются не более чем на 4%.

4. Применение имитационных моделей не позволяет в полной мере исследовать поведение функции готовности, а именно точно определить время и значение минимума функции на начальном этапе функционирования системы. Также достаточно сложно выявить тенденцию роста или стационарно-го режима функции готовности.

Несмотря на выявленные недостатки имитационных моделей, допустимо их использование при начальном определении оптимального варианта проведения верификации и коррекции проектных дефектов и обновления функций ИУС в процессе применения КА, так как это позволит сократить время поиска значений входных параметров системы, при которых обеспечивается требуемый уровень готовности.

Планируется включить разработанные имитационные модели в комплексную методику оценки и определения оптимального варианта проведения верификации и обновления функций ИУС.

Литература

1. ECSS - Q - 40B-2002 *Space product assurance. Safety (Гарантия продукции космического назначения. Безопасность)* [Текст]. – Нордвик: Европейская комиссия по космической стандартизации, 2002. – 42 с.
2. *Experimenting With Exception Handling Mechanisms Of Web Services Implemented Using Different Development Kits* [Text] / A. Gorbenko, A. Mikhaylichenko, V. Kharchenko, A. Romanovsky // CS-TR 1010, University of Newcastle upon Tyne, 2007. – P. 67 – 78.
3. Rotaru, T. *Service-oriented middleware for financial Monte Carlo simulations on the cell broadband engine* [Text] / T. Rotaru, M. Dalheimer, F.-J. Pfreundt. – *Concurrency and Computation: Practice and Experience*, John Wiley & Sons, Ltd, 2009. – 348 p.
4. Gashi, I. *Uncertainty Explicit Assessment of Off-The-Shelf Software: A Bayesian Approach* [Text] / I. Gashi, P. Popov, V. Stankovic // *Elsevier Journal of Information and Software Technology*, Elsevier, 2009. № 51(2). – P. 497 – 511.
5. Chan, P. *Making Services Fault Tolerant* [Text] / P. Chan, M. Lyu, M. Malek // *ISAS 2006, LNCS 4328*, 2006. – P. 43–61.
6. *Елементи методології оперативної*

коригувальної верифікації програмних засобів інформаційно-управляючих систем космічних апаратів [Текст] / В.С. Харченко, М.В. Замирець, С.О. Засуха, Ю.Л. Поночовний // *Авиационно-космическая техника и технология*. – 2011. – № 6/83. – С. 117 – 133.

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

8. Засуха, С.А. Модель готовности двухканальной информационно-управляющей системы косми-

ческого аппарата с оперативной верификацией программных средств [Текст] / С.А. Засуха, Ю.Л. Поночовний // *Наука і техніка Повітряних сил Збройних сил України*. – 2011. – № 2(6). – С. 144 – 150.

9. Поночовний, Ю.Л. Имитационное моделирование процесса оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов [Текст] / Ю.Л. Поночовний, Е.Б. Одаруценко // *Радиоелектронні і комп'ютерні системи*. – 2007. – № 7 (26). – С. 68 – 74.

10. Надежность и эффективность в технике: Справочник. В 10т. / под ред. Б. В. Гнеденко. – М.: Машиностроение, 1987. – Т. 2. Математические методы в теории надежности и эффективности. – 296 с.

Поступила в редакцию 23.02.2012

Рецензент: д-р техн. наук, проф., проф. каф. компьютерных систем и сетей Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ДОСЛІДЖЕННЯ ІМІТАЦІЙНИХ МОДЕЛЕЙ ГОТОВНОСТІ ДВОКАНАЛЬНОЇ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧОЇ СИСТЕМИ КОСМІЧНОГО АПАРАТУ

Ю.Л. Поночовний, С.О. Засуха, В.С. Харченко

У статті розглянуті особливості моделей готовності інформаційно-управляючих систем космічних апаратів. Для двоканальної одноверсійної структури системи запропоновані імітаційні моделі, що враховують зміну параметрів потоків відмов програмних засобів внаслідок проведення оперативної верифікації або оновлення програмних функцій. Вказані особливості побудови імітаційних моделей, проаналізована збіжність їх результатів з аналітичними багатофрагментними моделями. Зроблені висновки про можливість застосування імітаційних моделей при визначенні оптимального варіанту проведення верифікації і корекції проектних дефектів і оновлення функцій системи в процесі її застосування

Ключові слова: імітаційна модель, інформаційно-управляючі системи, оперативна верифікація, оновлення програмних функцій.

RESEARCH OF TWCHANNEL INFORMATION-MANAGING SYSTEM AVAILABILITY SIMULATION MODELS OF SPACE VEHICLE

Y.L. Ponochovniy, S.A. Zasucha, V.S. Kharchenko

In the article the features of availability models of the space vehicles information-managing systems are considered. For the twochannel oneversion structure of the system simulation models are offered, taking into account the change of refuses streams parameters of software faults because of operative verification realization or updating of software functions. The features of simulation models construction are indicated, convergence of their results is analysed with analytical multifragmental models. Drawn conclusion about possibility of simulation models application at determination of verification and correction realization optimal variant of project defects and updating of the system functions sn the process of her application

Key words: simulation model, information-managing systems, operative verification, updating of software functions.

Поночовний Юрій Леонидович – канд. техн. наук, с.н.с., старший преподаватель кафедры комплексов военной связи Военного института телекоммуникаций и информатизации Национального технического университета Украины „КПИ“, Полтава, Украина. e-mail: pnchl@rambler.ru.

Засуха Сергей Алексеевич – начальник управления Национального космического агентства Украины, Киев, Украина.

Харченко Вячеслав Сергеевич – заслуженный изобретатель Украины, д-р техн. наук, профессор, заведующий кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина. e-mail: V.Kharchenko@khai.edu.