УДК 681.3(075.8)

В.С. ХАРЧЕНКО[1], В.В. СКЛЯР[2], А.А. СИОРА[3], Ю.А. БЕЛЫЙ[3]

[1] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2] *Государственный НТЦ по ядерной и радиационной безопасности, Украина*
[3] *ЗАО «Радий», Украина*

МОДЕЛИ БЕЗОТКАЗНОСТИ И ГОТОВНОСТИ ВСТРОЕННЫХ МУЛЬТИДИВЕРСНЫХ СИСТЕМ

Проанализировано применение принципа диверсности для встроенных аэрокосмических систем. Определено понятие мультидиверсной системы (МДВС). Разработаны модели надежности (безотказности и готовности) МДВС с учетом возможных переходов между состояниями и интенсивностей проявления различных дефектов программно-аппаратных версий и восстановления отказов систем.

встроенные приложения, мультидиверсные системы, модели безотказности и готовности

1. Использование версионной избыточности в отказоустойчивых аэрокосмических системах. Постановка задачи

Под версионной избыточностью (многоверсионностью) подразумевается метод повышения надежности путем введения двух или более способов (версий) реализации функций системы [1, 2]. Применение многоверсионности позволяет реализовать принцип «защиты в глубину» и снизить вероятность отказов по общей причине (ООП).

Классификация версионной избыточности предложена в [3] и включает шесть типов: программная, аппаратная, субъектная, проектная, функциональная, сигнальная.

Принцип диверсности давно и достаточно широко применялся в аэрокосмических системах – при построении высоконадежных автоматических и человеко-машинных бортовых и наземных компьютерных систем.

Для встроенных отказоустойчивых приложений в аэрокосмической технике применяются программная, аппаратная и сигнальная избыточность продуктов (датчиков и каналов обработки и регистрации информации), субъектная и проектная избыточность процессов их создания [3, 4].

Практически любая система управления самолетом имеет автоматический и ручной каналы управления, автопилот – это вторая (диверсная) подсистема, резервирующая другие части системы управления и навигации.

Одновременно для системы может быть применено несколько видов версионной избыточности, например, аппаратная и программная [5]. Использование многоверсионности технических средств (ТС) и программного обеспечения (ПО) можно назвать «принципом мультидиверсности».

Это создает возможность формирования множества многоверсионных технологий и масштабируемых многоверсионных решений, позволяющих минимизировать риски ООП в зависимости от особенностей разрабатываемых систем и реальных ограничений [6].

Целью статьи является разработка и исследование моделей надежности (безотказности и готовности) мультидиверсных систем.

2. Модель мультидиверсной системы

Определим понятие мультидиверсной системы (МДВС).

Мультидиверсной будем называть такую двухверсионную систему W, в которой версии v_1, v_2 по-

лучены с использованием нескольких видов версионной избыточности, таких что устранение одного из этих видов избыточности не делает версии тождественными (тривиальными [1]), т.е., если существует хотя бы один дефект проектирования, который является относительным для каждого варианта версионной избыточности применительно к версиям v_1, v_2.

Если обозначить версии, в которых используется два и более видов разнообразия как $v_1(r)$, $v_2(r)$, где r – число таких видов, то r-диверсная система будет быть представлена следующим выражением:

$$W = \{X, F, U, V, R, \theta, Z\}, \qquad (1)$$

где X, U – входные и выходные сигналы;

F – множество выполняемых функций;

V – множество (двухместное) версий v_1, v_2 с выходными сигналами U_1, U_2;

Z – функция обработки результатов выполнения версий (отображения U_1, U_2 в U);

R – множество видов используемой версионной избыточности, причем $v_j \in V$ определяются на множестве R с помощью отображения θ.

3. Модели безотказности невосстанавливаемых мультидиверсных систем

При разработке моделей принято дополнительное допущение об экспоненциальном законе распределения времени до отказа [7] и идеальных по достоверности и безотказности средствах контроля. При необходимости вероятности безотказной работы (ВБР) компонентов могут быть вычислены в соответствии с другими законами распределения.

Кроме того, принято допущение о равных интенсивностях отказов версий ТС и ПО (каналов), т.е. $\lambda_1^{ПО} = \lambda_2^{ПО} = \lambda^{ПО}$; $\lambda_1^{ТС} = \lambda_2^{ТС} = \lambda^{ТС}$; $\lambda_{ТС1} = \lambda_{ТС2} = \lambda_{ТС}$. Для определения интенсивности относительных и абсолютных отказов версий ПО и ТС вводится коэффициент абсолютных отказов. Этот коэффициент определяет соотношение между интенсивностями отказов двухверсионной и одноверсионной системы [6].

Интенсивность отказов одной версии складывается из абсолютных и относительных отказов, т.е.: $\lambda^{1В} = \lambda_{12} + \lambda_1$, $\lambda^{2В} = \lambda_{12} + \lambda_2$, $\lambda^{1В} = \lambda^{2В}$. Тогда, коэффициент абсолютных отказов вычисляется как

$$K_{12} = \frac{\lambda_{12}}{\lambda^{1В}} = \frac{\lambda_{12}}{\lambda_{12} + \lambda_1} = \frac{\lambda_{12}}{\lambda_{12} + \lambda_2}. \qquad (2)$$

Для мультивесной системы с версионной избыточностью ТС и ПО ВБР определяется выражением:

$$\begin{aligned} P &= P_{12}^{ТС} \cdot P_{12}^{ПО} \cdot \left[1 - \left(1 - P^{ТС} \cdot P^{ПО} \cdot P_{ТС}\right)^2\right] = \\ &= e^{-K_{12}^{ТС} \cdot \lambda^{1В\,ТС} \cdot t} \cdot e^{-K_{12}^{ПО} \cdot \lambda^{1В\,ПО} \cdot t} \times \\ &\times \left[1 - \left(1 - e^{-(1-K_{12}^{ТС}) \cdot \lambda^{1В\,ТС} \cdot t} \cdot e^{-(1-K_{12}^{ПО}) \cdot \lambda^{1В\,ПО} \cdot t} \cdot e^{-\lambda_{ТС} \cdot t}\right)^2\right]. \end{aligned} \qquad (3)$$

На основании анализа данных об отказах элементной базы и ПО [3, 5] для моделирования были выбраны следующие базовые значения интенсивностей отказов: $\lambda^{1В\,ТС} = 10^{-5}$ 1/час; $\lambda^{1В\,ПО} = 10^{-5}$ 1/час; $\lambda_{ТС} = 10^{-5}$ 1/час.

Результаты моделирования зависимости ВБР от времени представлены на рис. 1, где: 1V – для дублированной одноверсионной системы; 2VSW – для двухверсионной системы с версионной избыточностью ПО; 2VHW – для двухверсионной системы с версионной избыточностью ТС; 2V для МДВС системы с версионной избыточностью ТС и ПО согласно (3).

4. Модели готовности восстанавливаемых мультидиверсных систем

Примем дополнительные допущения, традиционные для такого класса задач [2], о простейшем потоке восстановлений и идеальных средствах контроля и диагностирования. Кроме того, будем рассматривать системы без профилактического ТО, считая, что интенсивности восстановления при идентичных отказах разных версий равны.

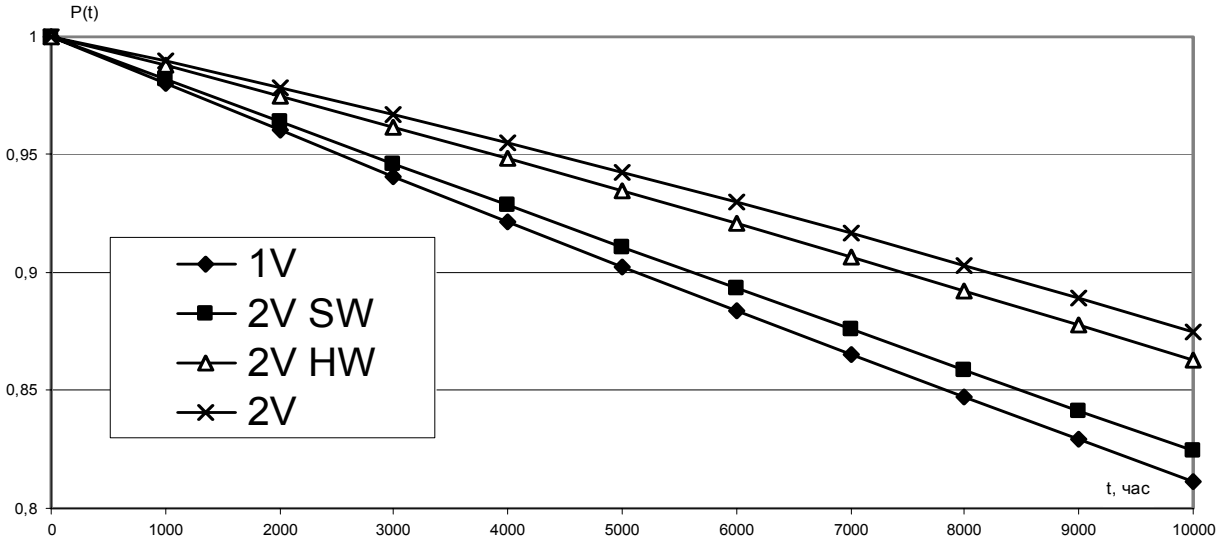

Рис. 1. Графики зависимости ВБР от времени при значениях коэффициентов абсолютных отказов $K_{12}^{TC} = 0{,}2$; $K_{12}^{ПО} = 0{,}8$

В рамках поставленной задачи и с учетом принятого допущения о неизменности интенсивностей проявления дефектов проектирования в процессе работы системы (пессимистический случай), будем считать, что интенсивности восстановления для всех типов отказов также остаются неизменными. Такой подход принимается в большинстве известных работ по исследованию надежности программно-аппаратных комплексов, где используются наиболее популярные, ставшие классическими, модели Джелинского-Моранды, Муссы, Лонгботтома, описанные в [8].

На основании анализа требований нормативных документов и данных о восстановлении работы ИУС при отказах элементной базы и ПО [3, 5] для моделирования были выбраны следующие базовые значения интенсивностей восстановления: интенсивность восстановления в случае отказов ТС из-за физических дефектов $\mu_{TC} = 1$ 1/час; интенсивность восстановления в случае отказов ТС из-за дефектов проектирования $\mu^{TC} = 100$ 1/час; интенсивность восстановления в случае отказов ПО из-за дефектов проектирования $\mu^{ПО} = 100$ 1/час.

В качестве базовых значений интенсивностей отказов применяются значения, выбранные в разделе 3 (10^{-5} 1/час для всех интенсивностей отказов).

Для сокращения объема записей на графах переходов введены следующие обозначения для интенсивностей отказов: интенсивность абсолютных отказов из-за дефектов ТС $\lambda_{12}^{TC} = K_{12}^{TC} \cdot \lambda^{1В\,TC}$; интенсивность абсолютных отказов из-за дефектов ПО $\lambda_{12}^{ПО} = K_{12}^{ПО} \cdot \lambda^{1В\,ПО}$; интенсивность относительных отказов одной версии из-за дефектов ТС $\lambda_{TC} = (1 - K_{12}^{TC}) \cdot \lambda^{1В\,TC}$; интенсивность относительных отказов одной версии из-за дефектов ПО $\lambda_{ПО} = (1 - K_{12}^{ПО}) \cdot \lambda^{1В\,ПО}$.

Исследуем мультидиверсную систему с версионной избыточностью ТС и ПО, имеющую восемнадцать состояний:

S_0 – работоспособное состояние;

S_{12}^{TC} – отказ ТС из-за дефектов проектирования;

$S_{12}^{ПО}$ – отказ ПО из-за дефектов проектирования;

S_{TC1} – отказ одного из каналов ТС;

S_{TC2} – отказ двух каналов ТС;

$S_{TC1,12}^{TC}$ – отказ ТС из-за дефектов проектирования при отказе одного из каналов ТС;

$S_{TC1,12}^{ПО}$ – отказ ПО из-за дефектов проектирования при отказе одного из каналов ТС;

S_1^{TC} – отказ одной из версий ТС;

S_2^{TC} – отказ двух версий ТС;

$S_1^{TC}{}_{12}^{TC}$ – отказ ТС из-за дефектов проектирования при отказе одной из версий ТС;

$S_1^{TC}{}_{12}^{ПО}$ – отказ ПО из-за дефектов проектирова-

ния при отказе одной из версий ТС;

$S_1^{ПО}$ – отказ одной из версий ПО;

$S_2^{ПО}$ – отказ двух версий ПО;

$S_1^{ПО}{}_{12}^{ТС}$ – отказ ТС из-за дефектов проектирования при отказе одной из версий ПО;

$S_1^{ПО}{}_{12}^{ПО}$ – отказ ПО из-за дефектов проектирования при отказе одной из версий ПО;

$S_{ТС1,1}{}^{ТС}$ – отказ одной из версий ТС и одного из каналов ТС;

$S_{ТС1,1}{}^{ПО}$ – отказ одной из версий ПО и одного из каналов ТС;

$S_1{}^{ТС}{}_1{}^{ПО}$ – отказ одной из версий ТС и одной из версий ПО.

Граф переходов мультидиверсной ИУС с учетом интенсивностей переходов представлен на рис. 2. В соответствии с методикой расчета марковских процессов имеем следующую систему дифференциальных уравнений:

$$
\begin{cases}
dP_0(t)/dt = -(\lambda_{12}^{ТС}+\lambda_{12}^{ПО}+2\lambda_{ТС}+2\lambda^{ПО})\cdot P_0(t)+\mu_{12}^{ТС}\cdot P_{12}^{ТС}(t)+\mu_{12}^{ПО}\cdot P_{12}^{ПО}(t)+\mu_{ТС}\cdot P_{ТС1}(t)+\mu^{ТС}\cdot P_1^{ТС}(t)+\\
\quad +\mu^{ПО}\cdot P_1^{ПО}(t)+(\mu_{ТС}+\mu^{ТС})\cdot P_{ТС1,1}{}^{ТС}(t)+(\mu_{ТС}+\mu^{ПО})\cdot P_{ТС1,1}{}^{ПО}(t)+(\mu^{ТС}+\mu^{ПО})\cdot P_1^{ТС}{}_1{}^{ПО}(t);\\
dP_{12}^{ТС}(t)/dt=\lambda_{12}^{ТС}\cdot P_0(t)-\mu_{12}^{ТС}\cdot P_{12}^{ТС}(t);\\
dP_{12}^{ПО}(t)/dt=\lambda_{12}^{ПО}\cdot P_0(t)-\mu_{12}^{ПО}\cdot P_{12}^{ПО}(t);\\
dP_{ТС1}(t)/dt=2\lambda_{ТС}\cdot P_0(t)-(\mu_{ТС}+\lambda_{ТС}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО}+\lambda^{ТС}+\lambda^{ПО})\cdot P_{ТС1}(t)+\\
\quad +2\mu_{ТС}\cdot P_{ТС2}(t)+(\mu_{ТС}+\mu_{12}^{ТС})\cdot P_{ТС1,12}{}^{ТС}(t)+(\mu_{ТС}+\mu_{12}^{ПО})\cdot P_{ТС1,12}{}^{ПО}(t);\\
dP_{ТС2}(t)/dt=\lambda_{ТС}\cdot P_{ТС1}(t)-2\mu_{ТС}\cdot P_{ТС2}(t);\\
dP_{ТС1,12}{}^{ТС}(t)/dt=\lambda_{12}^{ТС}\cdot P_{ТС1}(t)-(\mu_{ТС}+\mu_{12}^{ТС})\cdot P_{ТС1,12}{}^{ТС}(t);\\
dP_{ТС1,12}{}^{ПО}(t)/dt=\lambda_{12}^{ПО}\cdot P_{ТС1}(t)-(\mu_{ТС}+\mu_{12}^{ПО})\cdot P_{ТС12}{}^{ПО}(t);\\
dP_1^{ТС}(t)/dt=2\lambda^{ТС}\cdot P_0(t)-(\mu^{ТС}+\lambda^{ТС}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО}+\lambda_{ТС}+\lambda^{ТС}+\lambda^{ПО})\cdot P_1^{ТС}(t)+\\
\quad +2\mu^{ТС}\cdot P_2^{ТС}(t)+(\mu^{ТС}+\mu_{12}^{ТС})\cdot P_1^{ТС}{}_{12}{}^{ТС}(t)+(\mu^{ТС}+\mu_{12}^{ПО})\cdot P_1^{ТС}{}_{12}{}^{ПО}(t);\\
dP_2^{ТС}(t)/dt=\lambda^{ТС}\cdot P_1^{ТС}(t)-2\mu^{ТС}\cdot P_2^{ТС}(t);\\
dP_1^{ТС}{}_{12}{}^{ТС}(t)/dt=\lambda_{12}^{ТС}\cdot P_1^{ТС}(t)-(\mu^{ТС}+\mu_{12}^{ТС})\cdot P_1^{ТС}{}_{12}{}^{ТС}(t);\\
dP_1^{ТС}{}_{12}{}^{ПО}(t)/dt=\lambda_{12}^{ПО}\cdot P_1^{ТС}(t)-(\mu^{ТС}+\mu_{12}^{ПО})\cdot P_1^{ТС}{}_{12}{}^{ПО}(t);\\
dP_1^{ПО}(t)/dt=2\lambda^{ПО}\cdot P_0(t)-(\mu^{ПО}+\lambda^{ПО}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО}+\lambda_{ТС}+\lambda^{ТС})\cdot P_1^{ПО}(t)+\\
\quad +2\mu^{ПО}\cdot P_2^{ПО}(t)+(\mu^{ПО}+\mu_{12}^{ТС})\cdot P_1^{ПО}{}_{12}{}^{ТС}(t)+(\mu^{ПО}+\mu_{12}^{ПО})\cdot P_1^{ПО}{}_{12}{}^{ПО}(t);\\
dP_2^{ПО}(t)/dt=\lambda^{ПО}\cdot P_1^{ПО}(t)-2\mu^{ПО}\cdot P_2^{ПО}(t);\\
dP_1^{ПО}{}_{12}{}^{ТС}(t)/dt=\lambda_{12}^{ТС}\cdot P_1^{ПО}(t)-(\mu^{ПО}+\mu_{12}^{ТС})\cdot P_1^{ПО}{}_{12}{}^{ТС}(t);\\
dP_1^{ПО}{}_{12}{}^{ПО}(t)/dt=\lambda_{12}^{ПО}\cdot P_1^{ПО}(t)-(\mu^{ПО}+\mu_{12}^{ПО})\cdot P_1^{ПО}{}_{12}{}^{ПО}(t);\\
dP_{ТС1,1}{}^{ТС}(t)/dt=\lambda^{ТС}\cdot P_{ТС1}(t)+\lambda_{ТС}\cdot P_1^{ТС}(t)-(\mu_{ТС}+\mu^{ТС})\cdot P_{ТС1,1}{}^{ТС}(t);\\
dP_{ТС1,1}{}^{ПО}(t)/dt=\lambda^{ПО}\cdot P_{ТС1}(t)+\lambda_{ТС}\cdot P_1^{ПО}(t)-(\mu_{ТС}+\mu^{ПО})\cdot P_{ТС1,1}{}^{ПО}(t);\\
dP_1^{ТС}{}_1{}^{ПО}(t)/dt=\lambda^{ПО}\cdot P_1^{ТС}(t)+\lambda^{ТС}\cdot P_1^{ПО}(t)-(\mu^{ТС}+\mu^{ПО})\cdot P_1^{ТС}{}_1{}^{ПО}(t).
\end{cases}
\tag{4}
$$

Коэффициент готовности системы определяется по формуле (t – текущее время):

$$Кг(t) = P_0(t) + P_{ТС1}(t) + P_1{}^{ТС}(t) + P_1{}^{ПО}(t).$$

Коэффициент оперативной готовности системы для стационарного режима определяется по формуле (далее t – наработка системы):

$$
\begin{aligned}
K_{ОГ}(t) &= P_0\cdot P_{Б0}(t)+P_{ТС1}\cdot P_{БТС1}(t)+P_1^{ТС}\cdot P_{Б1}^{ТС}(t)+\\
&+P_1^{ПО}\cdot P_{Б1}^{ПО}(t)=\\
&=P_0\cdot exp\left[-(2\lambda_{ТС}+2\lambda^{ТС}+2\lambda^{ПО}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО})\cdot t\right]+\\
&+P_{ТС1}\cdot exp\left[-(\lambda_{ТС}+\lambda^{ТС}+\lambda^{ПО}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО})\cdot t\right]+\\
&+P_1^{ТС}\cdot exp\left[-(\lambda_{ТС}+\lambda^{ТС}+\lambda^{ПО}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО})\cdot t\right]+\\
&+P_1^{ПО}\cdot exp\left[-(\lambda_{ТС}+\lambda^{ТС}+\lambda^{ПО}+\lambda_{12}^{ТС}+\lambda_{12}^{ПО})\cdot t\right],
\end{aligned}
\tag{5}
$$

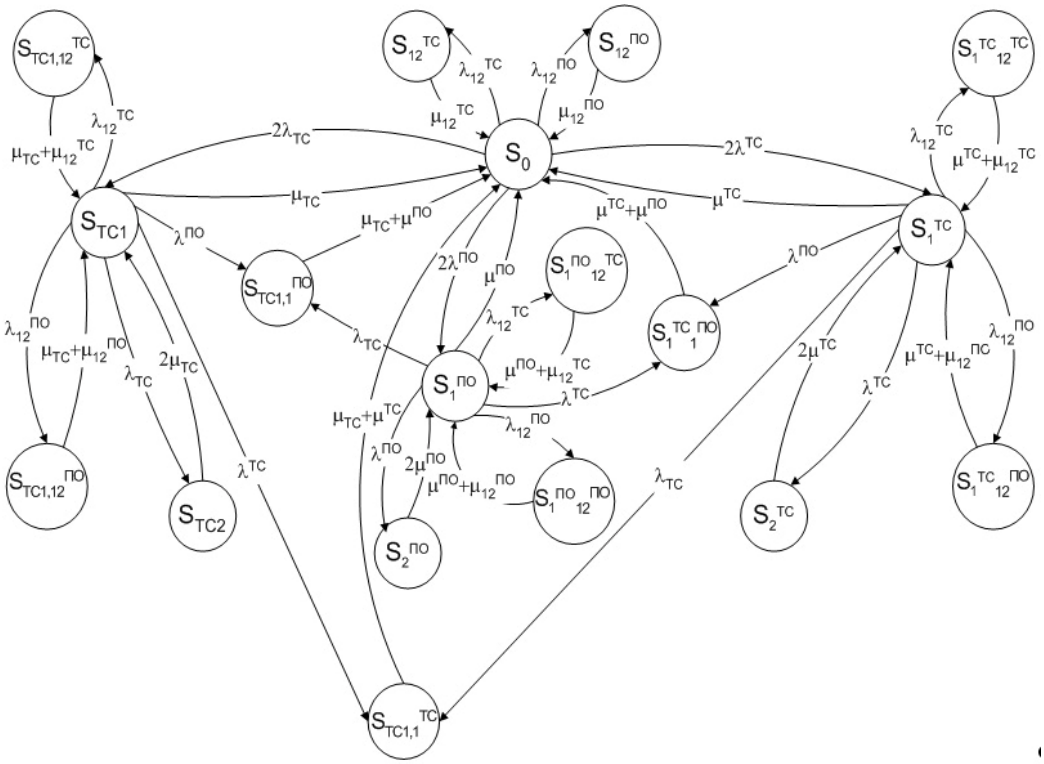

Рис. 2. Граф переходов мультидиверсной системы с версионной избыточностью ТС и ПО

где $P_{Б0}(t)$, $P_{БТС1}(t)$, $P_{Б1}^{ТС}(t)$, $P_{Б1}^{ПО}(t)$ – вероятности безотказной работы системы, находящейся в состояниях S_0, $S_{ТС1}$, $S_1^{ТС}$, $S_1^{ПО}$.

На рис. 3 представлены результаты моделирования коэффициента оперативной готовности в соответствии с формулой (5) при различных значениях коэффициента абсолютных отказов из-за дефектов ПО. При снижении значений $K_{12}^{ТС}$ и $K_{12}^{ПО}$ значение *Ког* также уменьшается из-за уменьшения вероятности нахождения в состоянии S_0.

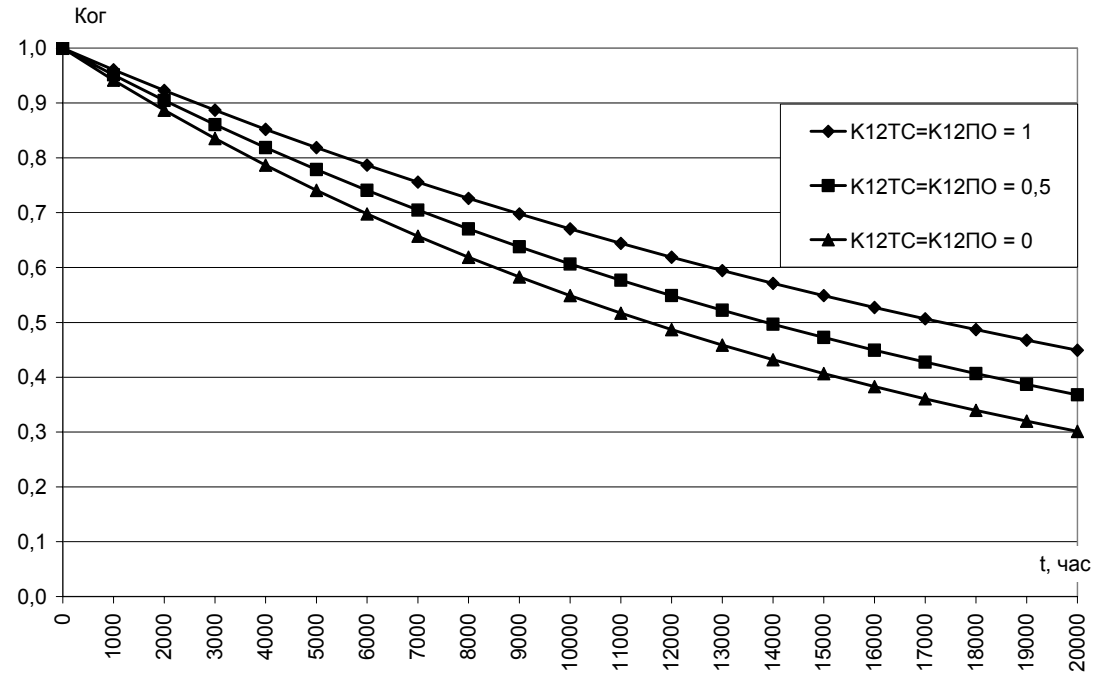

Рис. 3. Графики зависимости коэффициента оперативной готовности от времени при различных значениях коэффициента абсолютных отказов из-за дефектов ТС и ПО для мультидиверсной ИУС с версионной избыточностью ТС и ПО

Выводы

В статье проведен анализ применения принципа диверсности в аэрокосмических системах. Дано понятие и предложена модель мультидиверсной системы и получены модели надежности (безотказности и готовности) МДВС, которые учитывают варианты переходов между состояниями и интенсивности в результате: проявления дефектов программных версий, возникновения аппаратных версий и восстановления систем после их устранения. Разработаны и исследованы модели безотказности систем при использовании многоверсионности ТС и ПО и показано, что:

– ВБР повышается при уменьшении значения коэффициента абсолютных отказов;

– для МДВС с версионной избыточностью и ПО, и ТС выигрыш в ВБР складывается из выигрышей систем с версионной избыточностью ТС и систем с версионной избыточностью ПО;

– максимальный выигрыш в ВБР по сравнению с одноверсионной системой достигается при значениях коэффициентов абсолютных отказов для ТС и ПО $K_{12}{}^{TC} = K_{12}{}^{ПО} = 0$ (см. рис. 3, 4), когда все отказы из-за дефектов проектирования ТС и ПО являются относительными; выигрыш в ВБР для систем с версионной избыточностью ПО и ТС по сравнению с одноверсионной составляет 0,06 через 10 000 часов.

Разработаны и исследованы модели готовности восстанавливаемых МДВС и показано, что:

– марковская модель для описания МДВС требует учета большего количества состояний, чем для обычных многоверсионных систем;

– значения коэффициентов готовности повышаются при уменьшении значения коэффициента абсолютных отказов;

– при снижении значения коэффициента абсолютных отказов значения коэффициентов оперативной готовности могут также уменьшаться из-за уменьшения вероятности нахождения в начальном состоянии S_0.

Анализ влияния принятых допущений на точность оценок надежности МДВС показывает, что компенсирующий эффект при проявлении (возникновении) дефектов и возможность неидентичных реакций версий с разными ТС (ПО) при проявлении идентичного дефекта ПО (ТС) приближает консервативную оценку к точной на единицы процентов.

Литература

1. Avizienis A., Laprie J., Randell B. Fundamental Concepts of Dependability. Research Report n 01145, LAAS-CNRS, 2001. – 25 p.

2. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х.: Изд-во ХВУ, 1996. – 506 с.

3. Preckshot G. Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems. NUREG/CR-6303.– Livermore, USA: Lawrence Livermore National Laboratory, 1994. – 35 p.

4. Материалы фирмы Virginia – [Электронный ресурс]. – Режим доступа: http://www.yesvirginia.org/pdf/guides/VEDP-Areospace_web.pdf (1.02.2008).

5. Sklyar V., Kharchenko V. A Method of Multiversion Technologies Choice on Development of Fault-Tolerant Software Systems // Proceeding of Workshop on Methods, Models and Tools for Fault Tolerance. – Oxford, UK. – 3 July, 2007. – P. 148-157.

6. Скляр В.В. Анализ метрик многоверсионности программного обеспечения // Электронное моделирование. – 2004. – Т. 26, № 4. – С. 95-104.

7. Долманицкий С.М. Построение надежных логических устройств. – М.: Энергия, 1971. – 280 с.

8. Lyu M.R. Handbook of Software Reliability Engineering. – McGraw-Hill Company, 1996. – 805 p.

Поступила в редакцию 17.01.2008

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский государственный технический университет сельского хозяйства, Харьков.