ISSN 1561-8889. Космічна наука і технологія. 1999. Т 5. № 5/6. С. 103—109.

УДК 681.324.001.57

Модель функционирования бортовых вычислительных систем с категорированием задач в условиях сбоев и отказов аппаратных и программных средств

В. С. Харченко, Ю. В. Гридин

Харківський військовий університет

Надійшла до редакції 15.10.99

Досліджена модель відмовостійкої бортової обчислювальної системи з категоріюванням задач в умовах виникнення збоїв і відмов апаратних та прояву дефектів програмних засобів. Сформульовані рекомендації щодо програмно-технічної реалізації такої системи.

ВВЕДЕНИЕ

Важнейшим элементом в составе бортового оборудования современных космических аппаратов (КА) являются цифровые управляющие и вычислительные системы (УВС). В условиях полной автономности функционирования КА на УВС возлагается решение таких ответственных задач, как обработка командно-программной информации, выполнение важных и особо важных разовых команд, выработка управляющих воздействий для различных бортовых систем и др. Очевидно, что любая неисправность, которая приводит к неправильному функционированию УВС, может являться причиной частичной или полной потери работоспособности дорогостоящего оборудования КА. Именно поэтому проблема обеспечения высокой надежности УВС КА стала доминирующей при разработке космических систем и комплексов.

Как известно, условия функционирования бортовых УВС характеризуются, прежде всего высокой интенсивностью сбоев и отказов аппаратных и программных средств (АПС), что сокращает эффективное время работы системы и приводит к ее неработоспособному состоянию. При этом особую опасность представляют отказы и сбои УВС, обусловленные проявлением дефектов программных средств, поскольку для их обнаружения и парирования требуется использование специальных архитектурных решений.

Основным направлением обеспечения работоспособности УВС в условиях сбоев и отказов АПС является синтез архитектур, обладающих свойством отказо- или дефектоустойчивости [5, 13—16]. Сегодня подавляющее большинство современных бортовых УВС строится на принципах распределенных вычислительных систем с программируемой архитектурой. Это, в свою очередь, позволяет обеспечить необходимую отказоустойчивость при помощи версионной избыточности [14], предполагающей наличие резервных каналов, построенных с использованием различных программных или аппаратно-программных средств (различных математических моделей, алгоритмов, языков и субъектов

Таблица 1. Модели решаемых задач

Категория задачи K_j	Приоритет задачи $П_j$	Выделяемые ресурсы (кол-во вычислителей) R_j	Признак многоверсионности программных средств	Обнаруживаемые неисправности при мажоритарной обработке	Возможность исправления ошибок при мажоритарной обработке
1	1—5	1	—	нет	нет
2	1—5	2	—	аппаратные сбои и отказы	нет
3	1—5	2	+	аппаратные сбои и отказы, программные дефекты	нет
4	1—5	3	—	аппаратные сбои и отказы	есть
5	1—5	3	+	аппаратные сбои и отказы, программные дефекты	есть

программирования, аппаратных платформ и т. д.) и имеющих одинаковые вход-выходные характеристики [15].

В [6] предложен метод обеспечения отказоустойчивости, получивший название категорирования. Данный метод заключается в динамическом выделении избыточных вычислительных ресурсов в сочетании с многоприоритетной дисциплиной обслуживания решаемых задач. При этом понятие категории задачи определялось из требований к надежности и достоверности ее реализации в условиях сбоев и отказов АПС.

Целью данной работы является усовершенствование разработанной в [6] математической модели системы с категорированием задач и ее исследование в условиях сбоев и отказов АПС.

МАТЕМАТИЧЕСКИЕ МОДЕЛИ УВС С КАТЕГОРИРОВАНИЕМ ЗАДАЧ В УСЛОВИЯХ СБОЕВ И ОТКАЗОВ АПС

В общем случае модель УВС с категорированием задач (УВСК) состоит из трех составляющих: модели архитектуры, моделей обслуживаемых (решаемых) задач и модели дисциплины обслуживания. Для анализа работы УВСК в условиях сбоев и отказов АПС необходима еще одна составляющая — модель неисправностей.

В качестве модели, описывающей архитектуру и топологию связей, примем ПМЧ-модель [12]. В ней система представляется графом $G(B, E)$ без петель, где B, E — пара конечных множеств. Множество $B = \{B_1, ..., B_n\}$ соответствует вычислителям системы, а множество дуг $E = \{E_1, ..., E_m\}$ — информационным дугам. Введем следующие определения.

Определение 1. УВСК будем называть распределенную многопроцессорную вычислительную систему, состоящую из однородных вычислителей B_i ($i = 1, ..., n_В$), которые при выполнении распределенного вычислительного процесса реализуют принципы многоверсионных вычислений в сочетании с многоприоритетной дисциплиной обслуживания категорированных задач (заявок).

Определение 2. Под вычислителем B_i ($i = 1, ..., n_В$) будем понимать i-й элемент (узел, микропроцессор, вычислительный модуль и т. п.) УВСК, который выполняет распределенный вычислительный процесс.

С учетом многоверсионности вычислений модели задач Z_j ($j = 1, ..., n_З$) представим в виде, показанном в табл. 1.

Рассмотрим теперь модель дисциплины обслуживания задач Z_j. Согласно [7], дисциплина обслуживания — это такое правило приоритета $П_j$, которое определяет относительное расположение задачи Z_j в очереди, т. е. очередность ее решения по отношению к другим.

В системах с фиксированными приоритетами это означает, что задача с приоритетом $П_j$ считается более срочной, чем задача с приоритетом $П_{j-1}$, т. е. $П_j > П_{j-1}$.

Определение 3. Под многоприоритетной дисциплиной обслуживания задач Z_j будем понимать такое правило приоритета $П$, в котором число приоритетов больше двух.

Определение 4. Под категорированием задач Z_j будем понимать такое правило сопоставления K, R и $П$, при котором выполняются следующие условия: $R_j \geq R_{j-1}$, $П_j > П_{j-1}$ или $K_j(R_j, П_j) > K_{j-1}(R_{j-1}, П_{j-1})$.

Назначение категорий K_j задачам Z_j позволяет обеспечить не только необходимую отказоустойчивость выбранных в УВСК конфигураций, но также минимизировать временные задержки при решении задач Z_j путем реализации многоприоритетной дисциплины обслуживания. Условия в определении 4 демонстрируют частный случай, так как в общем случае при категорировании задач распределение их приоритетов может быть задано в произвольном порядке по отношению к категориям.

Принятую выше модель УВСК можно рассматри-

вать как систему массового обслуживания (СМО) [8, 9] при следующих допущениях:

1) в систему поступает экспоненциальный поток задач Z_j ($j = 1, ..., n_З$) категорий K_j ($j = 1, ..., 5$) с интенсивностями $\lambda_j = \lambda$, что соответствует равномерному распределению задач различных категорий в потоке;

2) интенсивности обслуживания задач Z_j равны, т. е. $\mu_j = \mu$;

3) при обслуживании задач реализуется многоприоритетная дисциплина обслуживания с относительными фиксированными приоритетами;

4) обработка потока задач Z_j осуществляется в условиях их информационной независимости;

5) число вычислителей B_j в системе бесконечно, т. е. $n_В \to \infty$.

Как показано в [6], граф состояний такой СМО имеет древовидную структуру. Вероятность нахождения системы в состоянии решения $n_З$ задач различных категорий определяется выражением

$$p(n_З) = \left(\frac{\lambda}{\mu}\right)^{n_З}\left(1 - \frac{5\lambda}{\mu}\right), \quad n_З \geq 0. \tag{1}$$

Рассмотрим тривиальный случай. Согласно [6] нормирующее условие для УВСК имеет вид

$$\sum_{n_З = 0}^{\infty} 5^{n_З} p(n_З) = 1. \tag{2}$$

С учетом (1), (2) можно записать

$$\sum_{n_З = 0}^{\infty} 5^{n_З}\left(\frac{\lambda}{\mu}\right)^{n_З}\left(1 - \frac{5\lambda}{\mu}\right) = 1. \tag{3}$$

Расчеты, проведенные по формуле (3) для $n_З = 0, ..., 4$, сведены в табл. 2. Видно, что при $5\lambda/\mu < 0.4$ состояниями с $n_З > 2$ можно пренебречь, так как вероятность нахождения в них УВСК очень мала (так, например, $p(2) = 0.00384$ при $5\lambda/\mu = 0.4$). Следовательно, имеет место предел

$$\lim_{\frac{5\lambda}{\mu} \to 0} \sum_{n_З = 0}^{\infty} p(n_З) = 0. \tag{4}$$

Как следствие из (4) для любого $n_З \neq 0$ справедливо

$$\lim_{\frac{5\lambda}{\mu} \to 0} p(n_З) = 0. \tag{5}$$

Очевидно, что данный подход позволяет существенно упростить структуру графа состояний УВСК.

В качестве моделей неисправностей АПС рассмотрим логические модели, позволяющие учитывать кратковременные неисправности типа аппаратных сбоев и программных дефектов [13]. Данные модели основываются на проявлении дефекта (физического или логического) в виде неправильных значений сигналов (данных) на выходах вычислителей.

Анализ УВСК в условиях неидеальной надежности АПС будем проводить при следующих условиях:

1) потоки сбоев и отказов АПС имеют пуассоновское распределение;

2) за время решения задачи Z_j категории K_j может возникнуть не более одной неисправности, и только в одном вычислителе;

3) процесс восстановления вычислителей будем описывать величиной $\mu_В$ — интенсивностью восстановления, которая определяется временем перезагрузки задачи в свободный вычислитель и ее решения;

4) в роли восстанавливающего органа будем использовать любой свободный вычислитель. При этом будем считать, что его аппаратная и программная часть, выполняющая функции контроля и восстановления, обладает идеальной надежностью, по крайней мере в течение времени, необходимого для их реализации [10, 11].

Таблица 2. Значения вероятности $5^{n_З}p(n_З)$ для разного числа задач $n_З$

$n_З$	$5\lambda/\mu$				
	0.2	0.4	0.6	0.8	0.999
0	0.8000	0.6000	0.4000	0.2000	0.0010
1	0.1600	0.2400	0.2400	0.1600	0.0010
2	0.0320	0.0960	0.1440	0.1280	0.0010
3	0.0064	0.0384	0.0864	0.1024	0.0010
4	0.0013	0.0154	0.0518	0.0819	0.0010
$\sum_0^1 5^{n_З}p(n_З)$	0.9600	0.8400	0.6400	0.3600	0.0020
$\sum_0^2 5^{n_З}p(n_З)$	0.9920	0.9360	0.7840	0.4880	0.0030

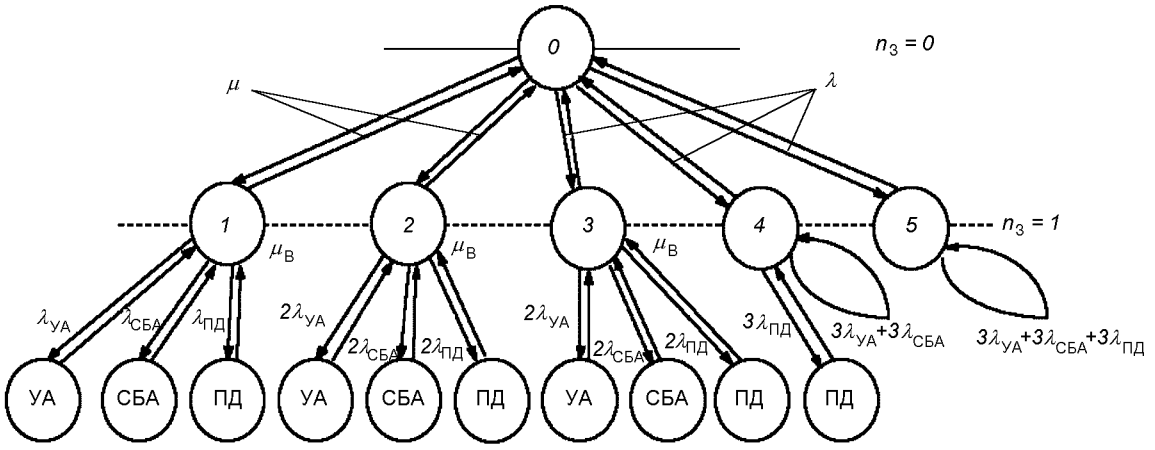

Рис. 1. Граф состояний УВСК; УА и СБА — состояния аппаратного устойчивого отказа и сбоя, ПД — состояние проявления программного дефекта; цифрами 0, 1, ..., 5 обозначены исходное состояние и состояния решения задач пяти категорий

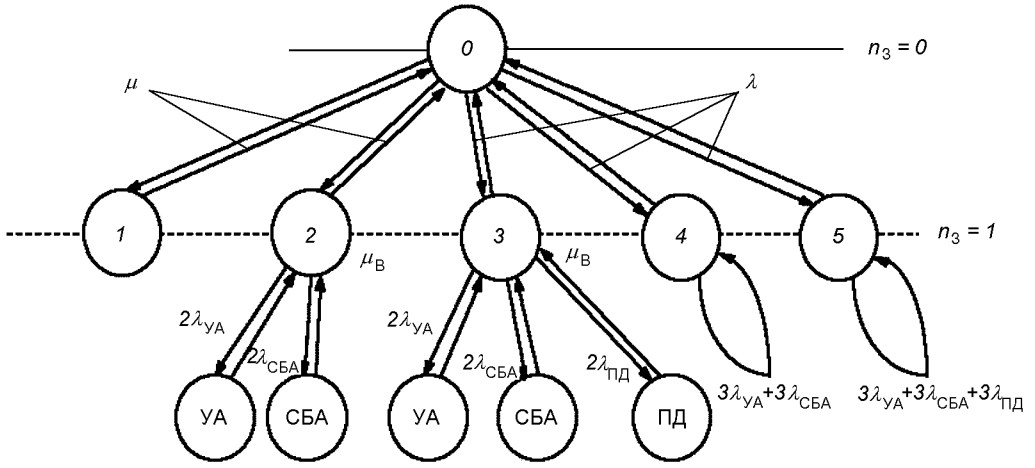

Рис. 2. Упрощенный граф состояний УВСК

Граф состояний УВСК можно представить в виде, показанном на рис. 1.

Сопоставление графа состояний и табл. 1 позволяет сделать вывод, что для получения оптимистической оценки надежности УВСК можно исключить ряд состояний графа, если принять следующие предположения:

1) при решении задач первой категории вероятность появления неисправностей АПС ничтожно мала и ею можно пренебречь;

2) в одноверсионных конфигурациях УВСК используются высоконадежные программные средства.

Принятые предположения позволяют перейти к упрощенному графу состояний УВСК (рис. 2).

АНАЛИЗ МОДЕЛЕЙ УВСК

Анализ матрицы переходов для графа состояний (рис. 2) позволяет получить следующую систему уравнений, описывающих работу УВСК в стационарном режиме (при $t \to \infty$):

$$\begin{cases} p(1) = \left(\dfrac{\lambda}{\mu}\right) p(0), \\ p_{УА}(1) = \left(\dfrac{2\lambda_{УА}}{\mu_В}\right) p(0), \\ p_{СБА}(1) = \left(\dfrac{2\lambda_{СБА}}{\mu_В}\right) p(0), \\ p_{ПД}(1) = \left(\dfrac{2\lambda_{ПД}}{\mu_В}\right) p(0), \\ p(0) + 5p(1) + 2p_{УА}(1) + 2p_{СБА}(1) + 2p_{ПД}(1) = 1, \end{cases} \tag{6}$$

где $p_{УА}(1)$, $p_{СБА}(1)$ и $p_{ПД}(1)$ — вероятности нахождения УВСК в состояниях проявления аппаратного отказа, сбоя и программного дефекта соответственно; $\lambda_{УА}$, $\lambda_{СБА}$ и $\lambda_{ПД}$ — интенсивности потоков аппаратных отказов, сбоев и программных дефектов.

Из уравнений (6) получаем выражение

$$p(0) = \frac{1}{1 + \frac{\lambda}{\mu}\left[5 + 4\frac{\lambda_{УА}}{\mu_В} + 4\frac{\lambda_{СБА}}{\mu_В} + 2\frac{\lambda_{ПД}}{\mu_В}\right]}. \quad (7)$$

Введем множитель

$$\beta_{АПС} = 5 + 4\frac{\lambda_{УА}}{\mu_В} + 4\frac{\lambda_{СБА}}{\mu_В} + 2\frac{\lambda_{ПД}}{\mu_В} \quad (8)$$

и назовем его коэффициентом потерь производительности УВСК. Из (8) видно, что область значений коэффициента $\beta_{АПС}$ лежит от 5 до 15. Случай $\beta_{АПС} = 5$ соответствует УВСК с идеальной надежностью, а случай $\beta_{АПС} = 15$ — критическому режиму. Рассмотрим влияние коэффициента $\beta_{АПС}$ на такой показатель надежности УВСК, как коэффициент готовности. Согласно графа состояний и уравнений (6) коэффициент готовности УВСК можно найти по формуле

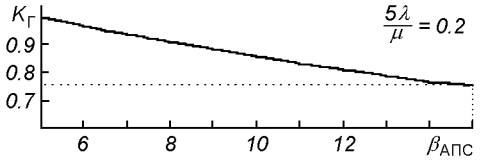

Рис. 3. Зависимость $K_Г$ от коэффициента $\beta_{АПС}$

$$K_Г = p(0) + 5p(1), \quad (9)$$

которая после подстановки выражений для $p(0)$, $p(1)$ и $\beta_{АПС}$ преобразуется к виду

$$K_Г = \frac{1 + 5\lambda/\mu}{1 + \beta_{АПС}\,\lambda/\mu}. \quad (10)$$

Зависимость (10) представлена на рис. 3.

Видно, что величина $\beta_{АПС}$, зависящая от соотношений интенсивностей сбоев и отказов АПС и интенсивности восстановления, может привести к понижению коэффициента готовности УВСК на 25 %.

Необходимо отметить, что рассмотренная выше модель функционирования УВСК также применима

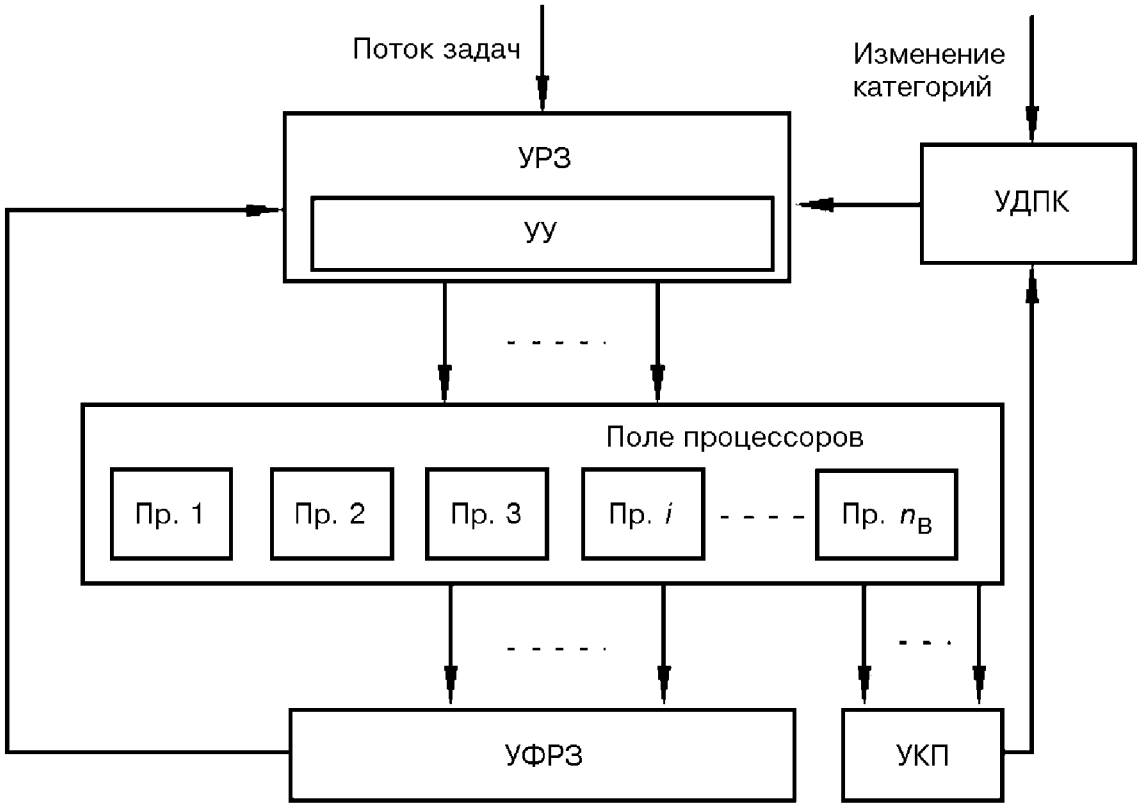

Рис. 4. Структурная схема УВСК

для случаев, когда число вычислителей $n_в$ конечно, при предположении, что аппаратные отказы не приводят к полной потере работоспособности вычислителей. Без этого предположения в УВСК будут иметь место деградационные процессы, приводящие к понижению производительности системы и появлению очередей к вычислительным ресурсам.

Тем не менее, в процессе деградации требуемая надежность и достоверность функционирования УВСК может поддерживаться механизмом динамического переназначения категорий.

ПРИНЦИПЫ ПРОГРАММНО-АППАРАТНОЙ РЕАЛИЗАЦИИ ОТКАЗОУСТОЙЧИВЫХ УВСК

Принципы возможной программно-аппаратной реализации и варианты технических решений отдельных устройств отказоустойчивой УВСК описаны в [1—4].

В общем виде структурная схема УВСК показана на рис. 4. В ее состав входят следующие основные элементы:

— устройство распределения задач УРЗ, включающее в себя централизованное или децентрализованное устройство управления УУ и обеспечивающее распределение категорированных задач с учетом их приоритетов на поле процессоров (вычислителей) с возможностью дообслуживания задач при отказах или сбоях АПС [9];
— поле процессоров, которые под управлением УРЗ объединяются в конфигурации, обеспечивающие требуемую надежность функционирования. Конфигурации строятся с учетом многоверсионности программного обеспечения и поддержания в готовности к подключению резервных процессоров [2, 3];
— устройство формирования результатов выполнения задач УФРВЗ, осуществляющее их анализ путем сравнения наборов выходных данных процессоров в выбранной УРЗ конфигурации с учетом возможной деградации системы по показателю производительности [2, 4];
— устройство контроля процессоров (УКП), которое обеспечивает оперативный контроль их работоспособности;
— устройство динамического переназначения категорий (УДПК), предназначенное для изменения категорий задач по командам извне (при изменении целей или условий функционирования УВСК) либо для их снижения при возрастании числа отказавших процессоров, приводящего к недопустимому увеличению времени выполнения задач.

ЗАКЛЮЧЕНИЕ

Отметим достоинства и недостатки разработанной выше модели функционирования УВСК. К основным достоинствам следует отнести простоту модели и возможность оценки основных показателей УВСК на этапе проектирования с учетом неисправностей АПС. Недостатком является то, что данная модель применима для анализа УВСК только с малыми значениями $5\lambda/\mu$ (что следует из табл. 2), т. е. для УВСК, работающих в режиме реального времени. Это обусловлено тем, что в других случаях необходимо учитывать переходы в состояния с $n_з > 1$, что, в свою очередь, существенно усложняет граф возможных состояний УВСК. Однако этот недостаток не является критичным для систем рассматриваемого класса в течение времени нормальной эксплуатации.

В целом разработанные математические модели и результаты их анализа можно рассматривать как основу для создания методики оценки и выбора параметров отказоустойчивых многопроцессорных систем с категорированием задач в условиях сбоев и отказов аппаратных и программных средств.

Для систем КА с длительным временем активного функционирования, допускающих деградацию (снижение производительности либо снижение требований к надежности и достоверности выполняемых задач), целесообразно использовать предложенную структурную схему адаптивной УВСК и варианты технической реализации ее отдельных устройств. В этом случае необходимо исследовать модели УВСК с динамическим переназначением категорий.

1. А. с. 1524052 СССР, МКИ G06F9/46. Устройство для распределения заданий процессорам / Г. Н. Тимонькин, Д. В. Дмитров, С. Н. Ткаченко, В. С. Харченко. — Опубл. 24.03.88, Бюл. № 43.
2. А. с. 1653448 СССР, МКИ G06F11/18, H05K10/00. Многопроцессорная резервированная система / В. С. Харченко, В. А. Ткаченко, Г. Н. Тимонькин и др. — Опубл. 03.07.89, Бюл. № 11.
3. А. с. 1753476 СССР, МКИ G0F15/16. Резервированная вычислительная система / В. С. Харченко, А. В. Бек, М. А. Чернышов и др. — Опубл. 23.01.90, Бюл. № 29.
4. А. с. 1819116 СССР, МКИ H05K10/00, G06F11/18. Трехканальная резервированная система / В. А. Ткаченко, Г. Н. Тимонькин, В. С. Харченко и др. — Опубл. 18.09.89, Бюл. № 20.
5. Генинсон Б. А., Панкова Л. А., Трахтенгерц Э. А. Отказоустойчивые методы обеспечения взаимной информационной согласованности в распределенных вычислительных системах // Автоматика и телемеханика.—1989.—№ 5.—С. 3—18.
6. Гридин Ю. В., Харченко В. С. Обработка измерительной информации в бортовых отказоустойчивых телеметрических системах с категорированием заявок // Космічна наука и технологія.—1999.—5, № 1.—С. 69—73.

7. Клейнрок Л. Коммуникационные сети (стохастические потоки и задержки сообщений). — М.: Наука, 1970.—256 с.
8. Клейнрок Л. Теория массового обслуживания: Пер. с англ./ Под ред. В. И. Неймана. — М.: Машиностроение, 1979.— 432 с.
9. Клейнрок Л. Вычислительные системы с очередями. — М.: Мир, 1979.—600 с.
10. Лобанов А. В. Взаимное информационное согласование с идентификацией неисправностей на основе глобального синдрома // Автоматика и телемеханика.—1996.—№ 5.— С. 150—159.
11. Лобанов А. В. Метод распределенного мажорирования информации с обнаружением и идентификацией проявлений неисправностей // Зарубежная радиоэлектроника. Успехи зарубежной радиоэлектроники.—1997.—№ 6.
12. Микеландзе М. А. Развитие основных моделей самодиагностирования сложных технических систем // Автоматика и телемеханика.—1995.—№ 4.—С. 3—18.
13. Согомонян Е. С., Слабаков Е. В. Самопроверяемые устройства и отказоустойчивые системы. — М.: Радио и связь, 1989.—208 с.
14. Харченко В. С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. — Харьков: МО Украины, 1996.—502 с.
15. Харченко В. С. Выбор технологии проектирования и базовых архитектур дефектоустойчивых цифровых управляющих и вычислительных систем реального времени // Космічна наука і технологія.—1997.—№ 5/6.—С. 109—119.
16. Харченко В. С., Благодарний М. П. Організація багатоальтернативних асинхронних обчислень у цифрових системах літальних апаратів і комплексів // Наука і оборона.— 1994.—№ 3.—С. 153—161.

THE MODEL OF OPERATION OF SPACECRAFT BOARD COMPUTER SYSTEMS WITH REQUEST CATEGORIZATION TAKING INTO ACCOUNT HARDWARE AND SOFTWARE FAULTS

V. S. Kharchenko and Yu. V. Gridin

The model of fault-tolerant board computer system with request categorization (CSRC) is studied with different kinds of hardware and software faults are researched taken into account. The structure and different variants of technical realization of CSRC elements are proposed.