УДК 78.25.37.29

АЛГОРИТМ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ БОРТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ СО СТРУКТУРНО-ВРЕМЕННОЙ ИЗБЫТОЧНОСТЬЮ

Д. С. Викторов,
канд. техн. наук, старший преподаватель
Военная академия воздушно-космической обороны

Разработан алгоритм обеспечения отказоустойчивости бортовых вычислительных систем с трехканальной архитектурой, который предполагает комплексное применение тестового контроля и восстановления по контрольной точке с различным доминированием в зависимости от количества исправных каналов.

Ключевые слова *— тестовый контроль, контрольная точка, бортовая вычислительная система.*

Введение

Бортовые вычислительные системы (БВС) современных летательных аппаратов решают комплекс задач по навигации, управлению вооружением, обеспечению связи, диагностике, устранению отказов и состоят из большого количества программно-аппаратных компонентов. Элементная база БВС функционирует на предельных тактовых частотах. Это является причиной того, что интенсивность сбоев на порядок выше интенсивности отказов 10^{-9}–10^{-10} 1/с [1].

Отказоустойчивость БВС обеспечивается использованием разных видов избыточности: структурной, временной, функциональной, информационной, версионной [2, 3]. Наиболее распространена в БВС структурная избыточность, которая используется для парирования отказов. Комплексное применение структурной и временной избыточности позволяет распознавать и парировать не только отказы, но и сбои как программных, так и аппаратных компонентов. Это особенно важно для БВС летательных аппаратов, которым наряду с высокими требованиями к надежности и достоверности контроля функционирования присущи довольно жесткие ограничения на массогабаритные и энергетические характеристики.

Классические алгоритмы обеспечения отказоустойчивости, базирующиеся на структурной и временной избыточности, исследованы в работах [3–6] и др., однако их комплексному использованию уделялось недостаточно внимания. Данное обстоятельство обуславливает необходимость разработки алгоритма обеспечения отказоустойчивости БВС на основе комплексного использования структурной и временной избыточности.

Алгоритм обеспечения отказоустойчивости БВС

При разработке алгоритма обеспечения отказоустойчивости БВС приняты следующие допущения:

1) поток отказов всех элементов схемы простейший, последствия сбоев ликвидируются либо мажоритарными органами, либо повторным счетом участка программы обработки информации;

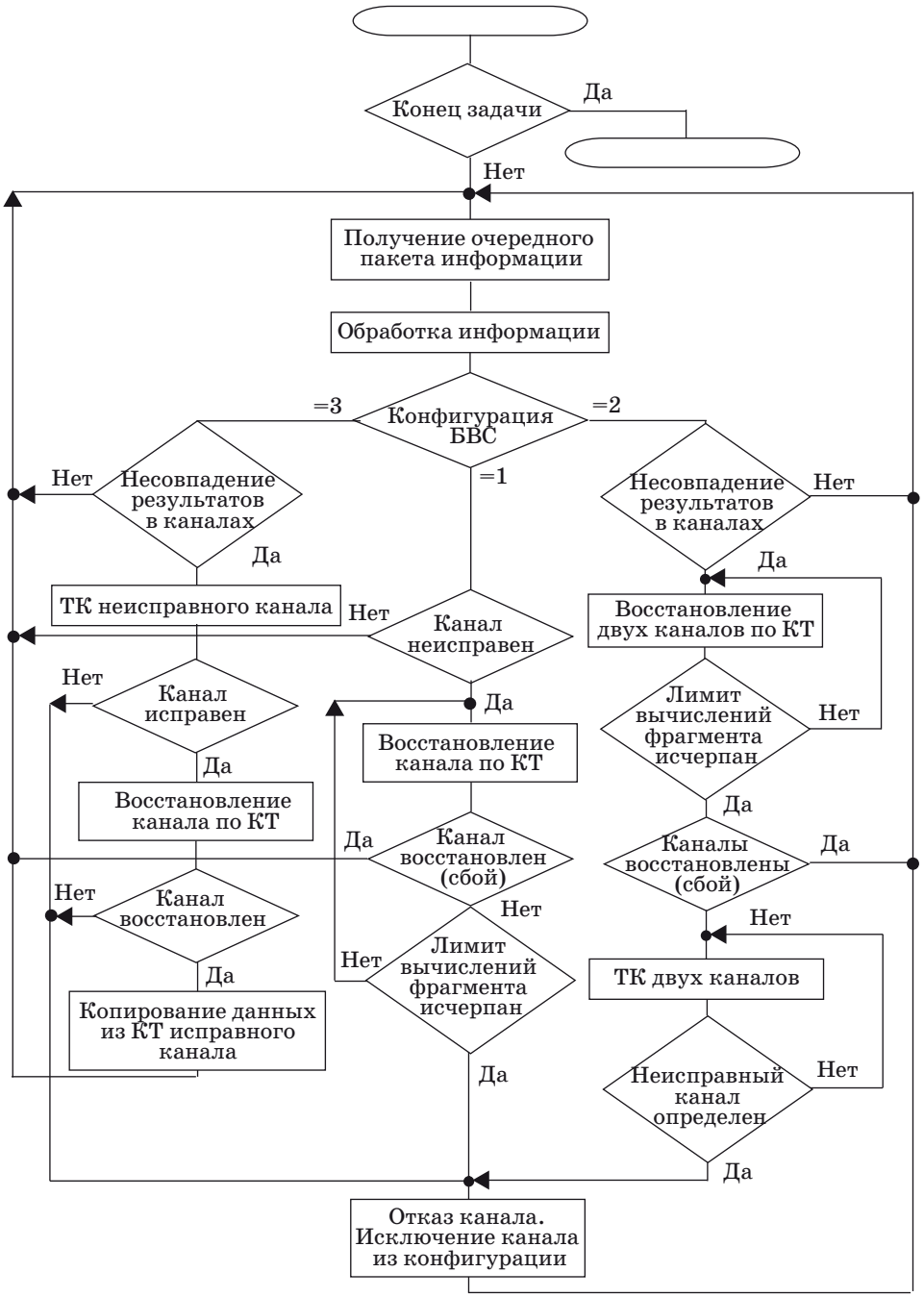
2) отказ любого элемента средств мажоритирования, диагностирования и реконфигурации ведет к отказу БВС;

3) интенсивности восстановления после отказов и сбоев являются неизменными;

4) восстановление сбившегося канала осуществляется путем повтора программы обработки информации с предыдущей контрольной точки (КТ), при этом КТ представляет собой периодически записываемое операционной системой в энергонезависимую память состояние всех полей основной памяти БВС.

Подобный подход применяется в большинстве известных работ по исследованию надежности программно-аппаратных комплексов [1–4].

Предлагаемый алгоритм обеспечения отказоустойчивости представлен на рис. 1. Сущность алгоритма заключаются в применении тестового контроля (ТК) и восстановления по КТ (для за-



■ ***Рис. 1.*** *Алгоритм обеспечения отказоустойчивости БВС*

щиты от сбоев) с различным доминированием в зависимости от количества исправных каналов.

Система начинает работу трехканальной конфигурации, при этом результатом вычислений является тот, который зафиксирован двумя каналами, а третий канал подвергается ТК. Если по результатам ТК канал признан исправным (сбой), то восстановление вычислительного процесса осуществляется по КТ путем повтора последнего фрагмента программы обработки информации. При успешном восстановлении канала данные, характеризующие текущее состояние БВС из любого исправного канала, записываются в КТ восстановленного канала.

В случае идентификации ТК отказа канала БВС реконфигурируется в двухканальную архитектуру.

В двухканальной конфигурации осуществляется периодическое сравнение результатов обработки данных в каналах. При несовпадении ре-

зультатов вычислений оба канала прекращают обработку информации и предпринимается попытка восстановления обоих каналов по КТ путем n-кратного повторения вычислений с предыдущей КТ. Если в результате этой операции удается получить одинаковые результаты вычислений в двух каналах, то БВС продолжает функционировать в двухканальной конфигурации (сбой в канале). В противном случае (отказ канала) оба канала подвергаются ТК в целях выявления отказавшего, который исключается из конфигурации, и БВС переходит на функционирование в одноканальной архитектуре.

Функционирование в одноканальной архитектуре предполагает наличие средств встроенного контроля для выявления неисправности канала. При получении сигнала от средств встроенного контроля о неисправности канала (сбой) осуществляется попытка его восстановления по КТ путем c-кратного повторения фрагмента программы обработки информации. Если средства встроенного контроля обнаружат, что неисправность ликвидирована, то БВС продолжит обработку информации. При исчерпании лимита повторов фрагмента программы БВС признается отказавшей.

Таким образом, комплексное применение ТК и восстановления по КТ с различным преобладанием в зависимости от количества исправных каналов дает возможность классифицировать неисправности как сбой и отказ, что позволяет избежать неоправданного расхода резервных ресурсов и, следовательно, повысить надежность БВС.

Модель надежности БВС при правильном определении вида неисправности

Проведем количественную оценку прироста надежности от применения предложенного выше алгоритма, для чего разработаем модели надежности БВС. При разработке модели примем дополнительное допущение об экспоненциальном законе распределения времени до отказа.

С учетом принятых допущений математическую модель, описывающую поведение БВС для предложенного алгоритма, можно выразить марковской цепью с непрерывным временем и следующими дискретными состояниями:

S_0 — БВС исправно функционирует в трехканальной конфигурации;

S_1 — БВС копирует данные, характеризующие текущее состояние трех исправных каналов в КТ;

S_2 — БВС восстанавливает неисправный канал по КТ;

S_3 — отказ одного канала;

S_4 — БВС исправно функционирует в двухканальной конфигурации;

S_5 — БВС копирует данные, характеризующие текущее состояние двух исправных каналов в КТ;

S_6 — БВС восстанавливает вычислительный процесс двух каналов по КТ;

S_7 — отказ второго канала;

S_8 — БВС исправно функционирует в одноканальной конфигурации;

S_9 — БВС копирует данные, характеризующие текущее состояние исправного канала в КТ;

S_{10} — по сигналу от встроенных средств контроля БВС восстанавливает вычислительный процесс в канале по КТ;

S_{11} — встроенные средства контроля БВС выявили неисправность канала и осуществляется попытка восстановить его функционирование путем c-кратного повторения вычислений с последней КТ;

S_{12} — отказ БВС.

Граф переходов БВС, учитывающий интенсивности переходов, представлен на рис. 2.

В соответствии с методикой расчета марковских процессов имеем следующую систему уравнений:

$$P_0(t)/\mathrm{d}t = -P_0(t)3\lambda_{\text{сб}} - P_0(t)3\lambda_{\text{отк}} - P_0(t)\lambda_{\text{КТ}} + P_1(t)\mu_{\text{КТ}} + P_{12}(t)\mu_{\text{в3}} + P_2(t)\mu_{\text{в1}};$$

$$P_1(t)/\mathrm{d}t = -P_1(t)\mu_{\text{КТ}} + P_0(t)\lambda_{\text{КТ}};$$

$$P_2(t)/\mathrm{d}t = -P_2(t)\mu_{\text{в1}} + P_0(t)3\lambda_{\text{сб}};$$

$$P_3(t)/\mathrm{d}t = -P_3(t)\mu_{\text{ТК}} + P_0(t)3\lambda_{\text{отк}};$$

$$P_4(t)/\mathrm{d}t = -P_4(t)2\lambda_{\text{отк}} - P_4(t)2\lambda_{\text{сб}} - P_4(t)\lambda_{\text{КТ}} + P_3(t)\mu_{\text{ТК}} + P_5(t)\mu_{\text{КТ}} + P_6(t)\mu_{\text{КТ}};$$

$$P_5(t)/\mathrm{d}t = -P_5(t)\mu_{\text{КТ}} + P_4(t)\lambda_{\text{КТ}};$$

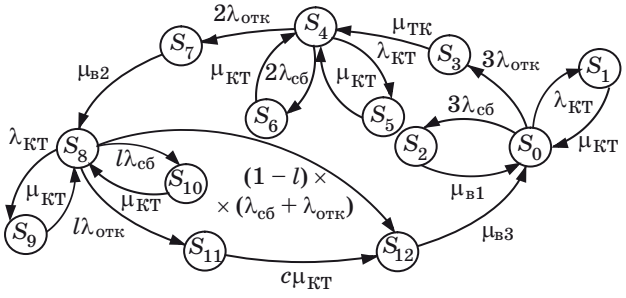
$$P_6(t)/\mathrm{d}t = -P_6(t)\mu_{\text{КТ}} + P_4(t)2\lambda_{\text{сб}};$$

$$P_7(t)/\mathrm{d}t = -P_7(t)\mu_{\text{в2}} + P_4(t)2\lambda_{\text{отк}};$$

$$P_8(t)/\mathrm{d}t = -P_8(t)l\lambda_{\text{сб}} - P_8(t)\lambda_{\text{КТ}} - P_8(t)l\lambda_{\text{отк}} - P_8(t)(1-l)(\lambda_{\text{сб}} + \lambda_{\text{отк}}) + P_9(t)\mu_{\text{КТ}} + P_{10}(t)\mu_{\text{КТ}} + P_7(t)\mu_{\text{в2}};$$

$$P_9(t)/\mathrm{d}t = -P_9(t)\mu_{\text{КТ}} + P_8(t)\lambda_{\text{КТ}};$$

$$P_{10}(t)/\mathrm{d}t = -P_{10}(t)\mu_{\text{КТ}} + P_8(t)l\lambda_{\text{сб}};$$



■ ***Рис. 2.*** *Граф переходов БВС при правильном определении вида неисправности*

$$P_{11}(t)/\mathrm{d}t = -P_{11}(t)c\mu_{КТ} + P_8(t)l\lambda_{отк};$$
$$P_{12}(t)/\mathrm{d}t = -P_{12}(t)\mu_{в3} + P_8(t)(1-l)\times$$
$$\times(\lambda_{сб} + \lambda_{отк}) + P_{11}(t)c\mu_{КТ},$$

где

$$\mu_{в1} = \frac{1}{T_{КТ} + T_{ТК} + \frac{T_{КТ-КТ}}{2}};\ \mu_{в2} = \frac{1}{T_{КТ} + T_{ТК}};\ \mu_{в3} = \frac{1}{T_{ц}}.$$

$\mu_{в1}$ характеризует интенсивность восстановления трехканальной БВС и предполагает проведение ТК неисправного канала в целях определения вида неисправности, повтор фрагмента программы обработки информации с последней КТ и копирование данных, характеризующих состояние системы, из исправного канала в восстановленный.

$\mu_{в2}$ описывает интенсивность восстановления двухканальной БВС и включает повтор фрагмента программы обработки информации с последней КТ и проведение ТК обоих каналов для выявления отказавшего.

$\mu_{в3}$ характеризует интенсивность восстановления БВС после отказа последнего канала и предполагает рестарт системы.

В системе уравнений приняты следующие обозначения:

P_0 — вероятность безотказной работы БВС в трехканальной конфигурации;

P_1 — вероятность нахождения БВС в состоянии формирования КТ;

P_2 — вероятность возникновения сбоя в одном канале;

P_3 — вероятность отказа одного канала;

P_4 — вероятность безотказной работы БВС в двухканальной конфигурации;

P_5 — вероятность нахождения БВС в состоянии копирования КТ;

P_6 — вероятность возникновения сбоя в канале при функционировании БВС в двухканальной конфигурации;

P_7 — вероятность отказа канала при функционировании БВС в двухканальной конфигурации;

P_8 — вероятность безотказной работы БВС в одноканальной конфигурации;

P_9 — вероятность нахождения БВС в состоянии копирования КТ;

P_{10} — вероятность возникновения сбоя в канале;

P_{11} — вероятность восстановления функционирования канала путем c-кратного повторения вычислений с КТ;

P_{12} — вероятность отказа БВС;

$T_{КТ}$ — временной интервал, необходимый для формирования КТ;

$T_{ТК}$ — время, затраченное на тестирование канала;

$T_{КТ-КТ}$ — временной интервал между двумя соседними КТ;

$T_{ц}$ — время цикла обработки информации.

Решая систему уравнений, следует учитывать, что модель описывает все возможные состояния БВС, а следовательно: $\sum_{i=1}^{n} P_i = 1$. Из системы уравнений можно вычислить вероятности нахождения БВС в любом возможном состоянии $P_i(t)$. Для БВС летательных аппаратов представляет интерес оценка вероятности безотказной работы за время t, которая вычисляется по формуле

$$P(t) = \sum_{i \in E} P_i(t),$$

где E — множество работоспособных состояний БВС, в которых система осуществляет обработку информации.

Предложенная модель предполагает применение идеальных по достоверности и безотказности средств встроенного контроля, что дает весьма приблизительные результаты при оценке безотказности.

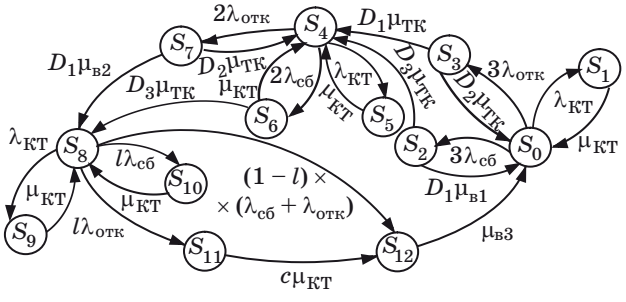
Модель надежности БВС при ошибочном определении вида неисправности

Значительный рост тактовых частот привел к тому, что в ходе тестирования каналов может быть ошибочно классифицирован вид неисправности, т. е. сбой может быть воспринят как отказ и наоборот. Для учета ошибочной классификации вида неисправности в граф (см. рис. 2) добавлены следующие переходы:

$S_3 \to S_0$ и $S_7 \to S_4$, интенсивность которых $D_2\mu_{ТК}$ (характеризуют такое состояние БВС, при котором ТК классифицировал отказ канала как сбой);

$S_2 \to S_4$ и $S_6 \to S_8$, интенсивность которых $D_3\mu_{ТК}$ (означает, что ТК классифицировал сбой канала как отказ).

При этом граф переходов БВС с учетом ошибочной классификации вида неисправности примет вид, показанный на рис. 3. Дискретные состояния в данном графе аналогичны графу, представленному выше.



■ ***Рис. 3.*** *Граф переходов с ошибочным определением ТК вида неисправности*

Принимая во внимание методику расчета марковских процессов, получим следующую систему дифференциальных уравнений:

$$P_0(t)/\mathrm{d}t = -P_0(t)3\lambda_{сб} - P_0(t)3\lambda_{отк} - P_0(t)\lambda_{КТ} + $$
$$+ P_1(t)\mu_{КТ} + P_3(t)D_2\mu_{ТК} + P_{12}(t)\mu_{в3} + P_2(t)\mu_{в1};$$
$$P_1(t)/\mathrm{d}t = -P_1(t)\mu_{КТ} + P_0(t)\lambda_{КТ};$$
$$P_2(t)/\mathrm{d}t = -P_2(t)D_1\mu_{в1} - P_2(t)D_3\mu_{ТК} + P_0(t)3\lambda_{сб};$$
$$P_3(t)/\mathrm{d}t = -P_3(t)\mu_{ТК} + P_0(t)3\lambda_{отк};$$
$$P_4(t)/\mathrm{d}t = -P_4(t)2\lambda_{отк} - P_4(t)2\lambda_{сб} - P_4(t)\lambda_{КТ} + $$
$$+ P_3(t)D_1\mu_{ТК} + P_2(t)D_3\mu_{ТК} + P_5(t)\mu_{КТ} + $$
$$+ P_6(t)\mu_{КТ} + P_7(t)D_2\mu_{ТК};$$
$$P_5(t)/\mathrm{d}t = -P_5(t)\mu_{КТ} + P_4(t)\lambda_{КТ};$$
$$P_6(t)/\mathrm{d}t = -P_6(t)\mu_{КТ} - P_6(t)D_3\mu_{ТК} + P_4(t)2\lambda_{сб};$$
$$P_7(t)/\mathrm{d}t = -P_7(t)D_1\mu_{в2} - P_7(t)D_2\mu_{ТК} + P_4(t)2\lambda_{отк};$$
$$P_8(t)/\mathrm{d}t = -P_8(t)l\lambda_{сб} - P_8(t)\lambda_{КТ} - P_8(t)l\lambda_{отк} -$$
$$- P_8(t)(1-l)(\lambda_{сб} + \lambda_{отк}) + P_7(t)D_1\mu_{в2} + P_6(t)D_3\mu_{ТК} +$$
$$+ P_9(t)\mu_{КТ} + P_{10}(t)\mu_{КТ};$$
$$P_9(t)/\mathrm{d}t = -P_9(t)\mu_{КТ} + P_8(t)\lambda_{КТ};$$
$$P_{10}(t)/\mathrm{d}t = -P_{10}(t)\mu_{КТ} + P_8(t)l\lambda_{сб};$$
$$P_{11}(t)/\mathrm{d}t = -P_{11}(t)c\mu_{КТ} + P_8(t)l\lambda_{отк};$$
$$P_{12}(t)/\mathrm{d}t = -P_{12}(t)\mu_{в3} + P_8(t)(1-l)\times$$
$$\times(\lambda_{сб} + \lambda_{отк}) + P_{11}(t)c\mu_{КТ},$$

где D_1 — вероятность правильной классификации неисправности ТК; D_2 — вероятность того, что ТК классифицировал отказ как сбой; D_3 — вероятность того, что ТК классифицировал сбой как отказ.

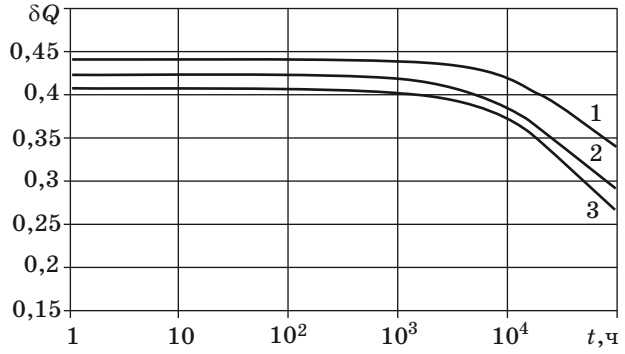
При моделировании значения переменных означают достоверность тестового контроля — D_1, D_2, D_3 могут принимать значения 0 или 1.

В системе уравнений вероятности P_0, P_4, P_8 характеризуют безотказную работу БВС в трехканальной, двухканальной и одноканальной конфигурациии соответственно.

Анализ системы уравнений позволяет предположить, что при увеличении $\lambda_{КТ}$ увеличиваются значения вероятностей P_0, P_4, P_8 и БВС сохраняет работоспособность при любом количестве сбоев.

Результаты моделирования

Учитывая, что в работе рассматриваются БВС летательных аппаратов, безотказность которых лежит в диапазоне 0,9 ÷ 0,999, в качестве показателя для оценки эффективности разработанного алгоритма целесообразно применять показатель — относительный выигрыш δQ в снижении вероятности отказа:



■ ***Рис. 4.*** *Зависимость относительного выигрыша в снижении вероятности отказа при: 1 — $D_1 = 1, D_2 = 0, D_3 = 0$; 2 — $D_1 = 0, D_2 = 1, D_3 = 0$; 3 — $D_1 = 0, D_2 = 0, D_3 = 1$*

$$\delta Q = (Q_0 - Q)/Q_0,$$

где Q — вероятность отказа БВС, реализующей предложенный метод структурно-временного резервирования; Q_0 — вероятность отказа БВС, относительно которой определяется выигрыш в снижении вероятности отказа δQ.

Следует учитывать, что БВС летательных аппаратов рассматриваются как невосстанавливаемые системы, поэтому, согласно работам [2, 3], относительный выигрыш в снижении вероятности отказа целесообразно рассчитывать как

$$\delta Q = (Q_0 - (1 - [P_0 + P_4 + P_8]))/Q_0.$$

В свою очередь, за Q_0 примем вероятность отказа трехканальной БВС без ТК и восстановления по КТ, численные значения которых получены в работе [5].

На основании анализа данных об отказах и сбоях в БВС [1, 3] для моделирования были выбраны следующие базовые значения: $\lambda_{отк} = 10^{-8}$ 1/ч; $\lambda_{сб} = 10^{-9}$ 1/ч; $\lambda_{КТ} = 10^3$ 1/ч; $\mu_{ТК} = 10^4$ 1/ч; $\mu_{КТ} = 5 \cdot 10^{-5}$ 1/ч, $T_{КТ} = 10^{-4}$ ч, $T_{КТ-КТ} = 10^{-3}$ ч, $T_{ТК} = 10^{-4}$ ч, $T_ц = 5 \cdot 10^{-3}$ ч. Результаты моделирования зависимости относительного выигрыша в снижении вероятности отказа от времени эксплуатации при различной достоверности контроля представлены на рис. 4.

Результаты моделирования показали, что применение предложенного алгоритма повышения отказоустойчивости позволяет повысить (до 45 % по показателю δQ) надежность трехканальных БВС со структурно-временной избыточностью.

Заключение

Предлагаемый алгоритм повышения отказоустойчивости ориентирован на идентификацию и парирование сбоев и отказов. Алгоритм может применяться в любых БВС с межканальными

связями. Для его реализации необходимо обеспечить синхронную работу каналов БВС. Все вышеперечисленное позволяет осуществить эффективную практическую реализацию предложенного алгоритма при жестких ограничениях на массогабаритные и энергетические характеристики.

Литература

1. **Kafka P.** How Safe Is Safe Enough? // Proc. of 10th European Conf. on Safety and Reliability, Munich, Germany, 13–17 Sept. 1999. Vol. 1. P. 385–390.
2. **Харченко В. С.** Модели и свойства многоальтернативных отказоустойчивых систем // Автоматика и телемеханика. 1992. № 12. С. 140–147.
3. **Харченко В. С., Литвиненко В. Г., Терещенков С. В., Мельников В. А.** Обеспечение устойчивости управляющих вычислительных систем к физическим дефектам и дефектам программирования программно-аппаратных средств // Зарубежная радиоэлектроника. 1992. № 6. С. 18–35.
4. **Доманицкий С. М.** Построение надежных логических устройств. — М.: Энергия, 1971. — 212 с.
5. **Викторов Д. С.** Восстановление информации в системах сбора и обработки данных // Сб. материалов XXXV военно-научной конф. ВА ВКО. Секция № 8. 2006. С. 32–41.
6. **Черкесов Г. Н.** Надежность программно-аппаратных комплексов. — СПб.: Питер, 2004. — 472 с.