Оригинальная статья
DOI: 10.21683/1729-2646-2017-17-1-46-52

Оценка параметров безопасности и безотказности систем контроля и управления

Олег Л. Маковеев, *ОАО «Радиоавионика», Санкт-Петербург, Россия, e-mail: makoveev38@mail.ru*
Сергей Ю. Костюнин, *ОАО «Радиоавионика», Санкт-Петербургский государственный университет, Санкт-Петербург, Россия, e-mail:kostyunin.sergey@gmail.com*

Олег Л. Маковеев

Сергей Ю. Костюнин

Резюме. Цель *данной работы – получение аналитических оценок показателей безопасности и безотказности систем контроля и управления ответственными объектами. К таким показателям относятся: вероятность безотказной работы, общая интенсивность отказов, интенсивность опасных и защитных (безопасных) отказов, средний срок службы. В работе рассматриваются системы с различной избыточностью («2 из 2», «2 из 3», «2 по 2»), допускающие возможность восстановления отказавшей аппаратуры (каналов) без прекращения функционирования, учитываются такие механизмы обеспечения безопасности и безотказности, как межканальное сравнение данных и защита от негативных проявлений отказов путём взаимной блокировки каналов.* **Методы.** *Для достижения поставленной цели в работе предложена математическая модель функционирования на основе поглощающих однородных цепей Маркова с непрерывным временем. Состояния данной цепи отражают число исправных каналов системы, а интенсивности переходов между состояниями определяются на основе интенсивностей отказов аппаратуры каждого канала и интенсивности восстановления (с учетом работы механизмов межканального сравнения данных и блокировки функционирования неисправного канала). Отсутствие защиты может быть связано с такими событиями, как: необнаружение отказа средствами контроля, неработоспособность механизма блокировки, задержка срабатывания защиты. В этом случае выход из строя канала (каналов) приводит к отказу всей системы и переводит цепь Маркова в поглощающее состояние. Вероятности перехода в поглощающее состояние разделяются на вероятности перехода в состояние защитного отказа и состояние опасного отказа. Поскольку появление отказа при отсутствии гарантированной защиты от возможных негативных последствий при продолжении функционирования может привести к неправомерным воздействиям на исполнительные органы системы, то, основываясь на пессимистическом подходе, считаем такой отказ опасным. Используемые методы позволяют найти вероятности каждого состояния цепи путём решения системы дифференциальных уравнений Колмогорова-Чепмена. На основе данных вероятностей определяется общая интенсивность отказов и средний срок службы, а также интенсивности защитного и опасного отказов. Для обеспечения удобства применения представленных методов приведены приближенные формулы интенсивностей отказов и погрешности приближений.* **Результаты.** *Построена математическая модель функционирования многоканальных микропроцессорных систем. Получены формулы расчета вероятностей состояний систем, среднего срока службы, интенсивностей опасных и защитных отказов, позволяющие оценить безопасность и отказоустойчивость различных систем с горячим резервированием и возможностью восстановления работоспособности в процессе функционирования. Приведённые формулы для расчёта вероятностей состояний систем позволяют расширить число показателей безопасности и безотказности, при необходимости. Представлена возможность упрощённого вычисления интенсивностей отказов.* **Выводы.** *Приведённые в работе формулы могут быть использованы для оценки показателей безотказности, безопасности и долговечности микропроцессорных систем контроля и управления ответственными объектами (судовыми техническими средствами, напольным оборудованием на железнодорожных станциях и перегонах, стационарными энергетическими установками и др.). В процессе разработки они позволяют найти рациональную организацию системы путём сравнительной оценки показателей структур с различной избыточностью. При адаптации системы для использования на различных объектах и при её модернизации данные формулы позволяют провести аналитический расчёт указанных выше показателей.*

Ключевые слова: *функциональная безопасность, безотказность, контроль, диагностика, опасный отказ, защитный отказ, интенсивность отказов.*

Формат цитирования: *Маковеев О.Л., Костюнин С.Ю. Оценка параметров безопасности и безотказности систем контроля и управления // Надежность. 2017. Т.17, №1. С. 46-52. DOI: 10.21683/1729-2646-2017-17-1-46-52*

К системам контроля и управления ответственными объектами предъявляются требования по безотказности и функциональной безопасности [1]. Обеспечение высокого уровня безотказности и функциональной безопасности осуществляется на основе многоканальной организации микропроцессорных систем, их контроля и диагностики.

Для количественной оценки таких систем предлагается к рассмотрению следующие показатели [2, 3, 4]:

– по безотказности – вероятность безотказной работы и интенсивность отказов (общая интенсивность отказов);

– по долговечности – средний срок службы;

– по безопасности – интенсивность опасных и безопасных отказов.

В стандарте по функциональной безопасности оборудования [4] представлено соотношение, являющеюся основой для вывода интенсивностей опасных и безопасных отказов:

$$\Lambda = \Lambda_S + \Lambda_D, \quad (1)$$

где Λ – общая интенсивность отказов;

Λ_S– интенсивность безопасных отказов;

Λ_D –интенсивность опасных отказов.

Это же соотношение показывает связь надёжности с безопасностью. По-видимому, чтобы подчеркнуть актуальность организации защиты рассматриваемых систем от негативных последствий отказов в железнодорожной автоматике безопасный отказ принято называть защитным отказом.

Известны зарубежные и отечественные микропроцессорные системы, обеспечение функциональной безопасности и безотказности [4, 5] которых, осуществляется на базе аппаратно-программной избыточности и автоматических средств технического контроля и диагностики. Организация таких систем при одинаковых требованиях по безопасности и безотказности существенно зависит от условий эксплуатации. Так, в системах, условия эксплуатации которых не допускают замену отказавшей аппаратуры в процессе функционирования, требуемые характеристики безопасности и безотказности достигаются значительным объёмом избыточных аппаратно-программных средств [5].

Существенно меньший объём избыточных аппаратно-программных средств требуется в системах, условия эксплуатации которых допускают замену отказавшей аппаратуры в процессе функционирования. В этом случае наиболее часто применяется 3-канальное «2 из 3» и 4-канальное 2 «2 из 2» горячее резервирование с восстановлением, а так же используются комбинации представленных выше вариантов (для разных устройств одной системы – различный уровень резервирования). Следует отметить, что в ряде случаев применяются и 2-канальные устройства «2 из 2», в которых каждый канал безопасен.

В этих системах на основе оперативного контроля и тестового диагностирования осуществляется локализация неисправностей с дальнейшей заменой отказавших модулей или резервных каналов без прекращения функционирования («безударной» заменой). Оперативный контроль производится на основе межканального сравнения и проверок по ограниченному числу параметров в течение цикла работы системы. Тестовое диагностирование осуществляется периодически в фоновом режиме с целью исключения накопления отказов. При этом проверяются все когда-либо используемые аппаратные средства независимо от реализуемой в данный момент программы управления объектом.

Характерной особенностью таких систем является продолжение нормального функционирования при одном отказе и переход в предельное состояние при появлении второго отказа. Возможны два вида предельного состояния, соответствующих двум типам последствий от отказов [2], а именно:

– состояние после опасного отказа, в результате которого возникает угроза безопасности людей и (или) значительный материальный и (или) моральный ущерб;

– состояние после безопасного отказа, не приводящего к опасным ситуациям.

При отказах с целью исключения опасной ситуации в максимально возможной степени на основе результатов контроля и диагностики осуществляется автоматический перевод системы в состояние безопасного отказа, т.е. производится защита от возможных негативных последствий опасного отказа.

К составным частям системы, обеспечивающим защиту от возможных негативных последствий опасного отказа, следует отнести средства контроля и диагностики состояния системы, а так же механизм блокировки функционирования неисправной части изделия или изделия в целом. При создании безопасных и безотказных систем всех видов избыточности стоит задача в максимально возможной степени исключить опасные отказы при сохранении необходимого уровня работоспособности. Для этого требуется обеспечить высокую достоверность контроля и диагностики при надёжном и быстродействующем механизме блокировки.

С целью восстановления изделия в процессе функционирования сигнализация неисправности осуществляется с точностью до сменного модуля, а замена неисправной аппаратуры – при включённом электропитании.

Поскольку появление отказа при отсутствии защиты от его возможных негативных последствий при продолжении функционирования может привести к неправомерным воздействиям на исполнительные органы системы, основываясь на пессимистическом подходе, считаем такой отказ опасным (ОпОт).

Отсутствие защиты может быть связано с такими независимыми событиями, как: средства контроля не обнаружили отказ, неработоспособен механизм блокировки или время между отказами меньше задержки срабатывания защиты. В связи с этим вероятность отсутствия защиты (q_1, q_2)можно определить следующим образом:

1) при первом отказе:

$$q_1 = q_{1K} + q_{1b}, \quad (2)$$

где: q_{1K} – вероятность того, что средства контроля не обнаружили отказ системы,

q_{1b} – вероятность отказа механизма блокировки.

2) при втором отказе:

$$q_2 = (1 - q_{2\tau})(q_{2K} + q_{2b}) + q_{2\tau}, \quad (3)$$

где: q_{2K} – вероятность того, что средства контроля не обнаружили отказ системы;

q_{2b} – вероятность отказа механизма блокировки;

$q_{2\tau}$ – вероятность того, что время между отказами меньше задержки срабатывания защиты (принимаем, что механизмы защиты гарантированно срабатывают за время τ).

С целью обнаружения неисправностей оперативный контроль в течение каждого цикла работы осуществляет проверки данных при выполнении основных процедур (ввод данных, вычисления, контроль, вывод данных, диагностика и т.п.).

Перечень таких процедур определяется спецификой конкретных систем и для них он постоянен.

В 3 и 4-канальных системах оперативный контроль осуществляется на основе межканального сравнения, и в них до второго отказа имеется возможность двукратной проверки. В 2-канальных системах до блокировки по первому отказу проверка производится так же путём межканального сравнения и, кроме того, производятся проверки целостности принимаемых/передаваемых информационных пакетов абонентами (внешними системами) за счёт избыточного кодирования. Достоверность контроля при двукратных проверках весьма высока, она снижается в случае выполнения межканального сравнения посредством свёрток или сигнатур [6, 7].

После второго отказа в 3 и 4-канальных системах производится однократное сравнение. Для этого случая наиболее характерные ограничения по достоверности контроля связаны с отказами, имеющими одинаковые последствия в различных каналах (не выявляемые при межканальном сравнении). Скорее всего, идентичные последствия отказов могут иметь место при практически одновременном появлении (в течение одного цикла работы системы) однотипных отказах элементов с одинаковыми позиционными обозначениями в двух каналах.

В 2-канальных системах после блокировки по первому отказу продолжение функционирования возможно при наличии средств обеспечения безопасности в составе каждого канала [8] или за счёт проверки внешними устройствами. Это весьма ограничивает применение таких систем.

С учётом отмеченного выше рассмотрим функционирование системы в условиях появления отказов.

При начальном пуске система находится в работоспособном полностью исправном исходном состоянии. После первого отказа (события От1) система переходит в состояние, при котором ведётся поиск неисправности. В случае, если неисправность обнаружена и сработала защита (с вероятностью $1 - q_1$), а так же при отсутствии второго отказа в период его восстановления, без потери работоспособности исключается из функционирования неисправный канал. После восстановления от последствий отказа происходит переход к исходному состоянию.

В случае отсутствия защиты (с вероятностью q_1) уже первый отказ считаем опасным.

Если за время восстановления отказавшего канала появился второй отказ (событие От2), то происходит переход в состояние, связанное с отказом всей системы, при следующих обстоятельствах:

1) второй отказ произошёл через некоторое время после защиты от последствий первого отказа и за этого время осуществлена защита (с вероятностью $1 - q_2$). Однако, из-за исчерпания резерва (количества работоспособных каналов) восстановление осуществляется с потерей работоспособности. Иными словами: после события От1 произошло событие «защита устройства с остановкой функционирования» или, так называемый, защитный отказ (ЗащОт);

2) второй отказ произошёл при отсутствии защиты (с вероятностью q_2), но функционирование продолжается, что позволяет считать такой отказ опасным.

На рисунке 1 представлена блок-схема изменения состояния системы при отказах и восстановлении работоспособности по результатам контроля технического состояния.

На рисунке 1 некоторые состояния обозначены числом исправных каналов на данный момент времени в соответствии с таблицей 1, где:

– начальное состояние – «*i*-канальный режим» (все каналы в работе);

– состояние после первого отказа (по событию От1) – «*j*-канальный режим»;

– состояния после второго отказа (по событию От2) – «(*j*-1)-канальный режим».

Таблица 1

***i*-канальная система (*i*, *j*)**	**Число исправных каналов**		
	в исходном состоянии, *j*	**после первого отказа, *j***	**после второго отказа, *j*-1 (защитный или опасный отказ)**
2-канальная система – (2,1)	2	1	0
3-канальная система – (3,2)	3	2	1
4-канальная система – (4,2)	4	2	1

Каждый тип, рассматриваемых систем (тип резервирования), характеризуется двумя параметрами – *i* и *j*, отличными от других типов, что позволяет исполь-

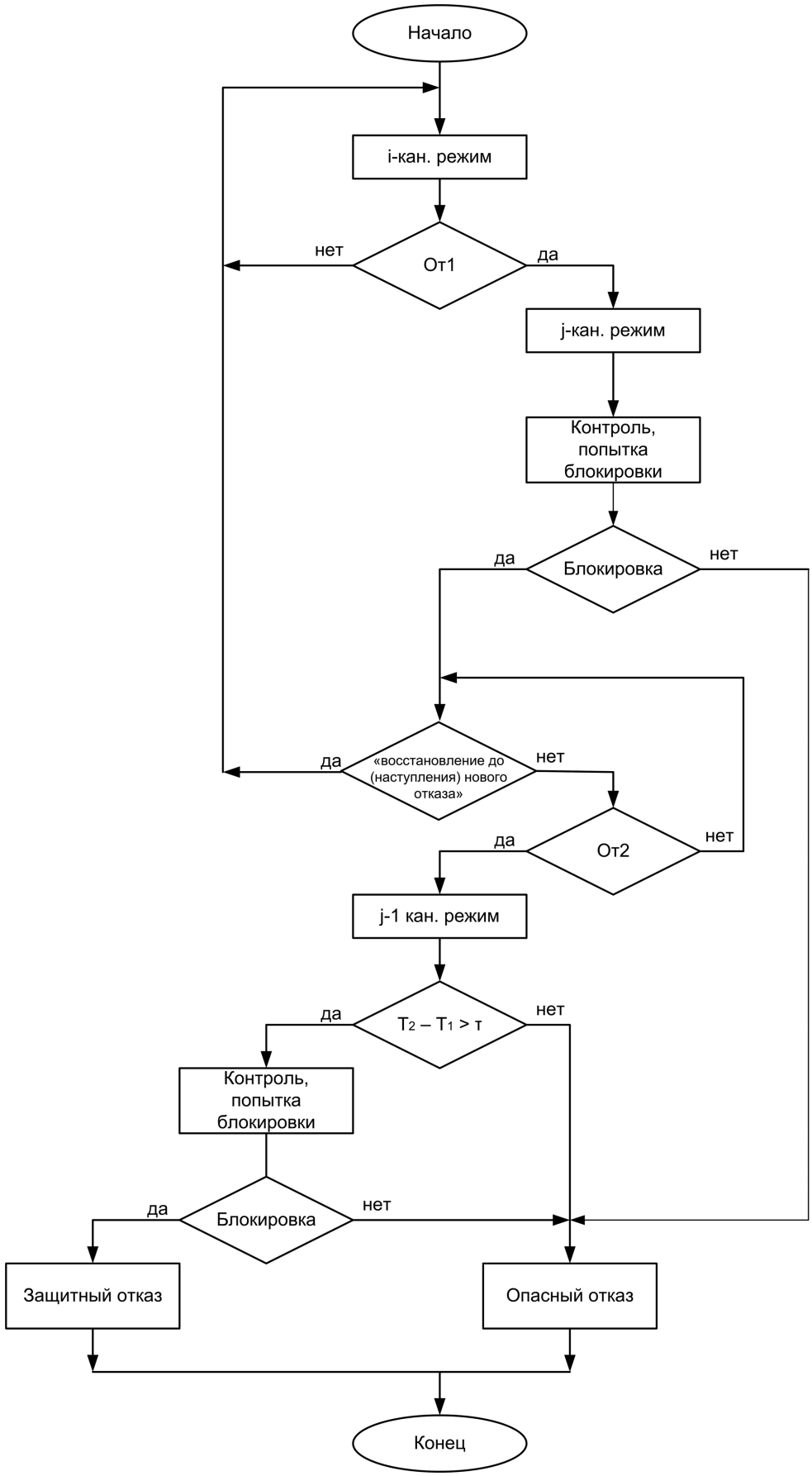

Рисунок 1 – Блок-схема изменения состояния системы

зовать «*i*,*j*» в качестве обозначения принадлежности к конкретному типу.

Переходы из состояния в состояние происходят в следующих случаях:

– при восстановлении отказавшего канала – возврат в начальное состояние;

– при $T_2 - T_1 > \tau$ (время между отказами больше задержки срабатывания защиты) – переход к контролю и при обнаружении неисправности – блокировка отказавшего канала;

– при отказах (От1 и От2) и при срабатывании и несрабатывании средств защиты переходы в (*j*-1)-канальном режиме в состояние «защитный отказ» или «опасный отказ».

Для оценки безопасных отказоустойчивых систем контроля и управления рассмотрим марковский процесс с дискретным множеством состояний и непрерывным временем, представленный в виде графа переходов из одного состояния модели в другое.

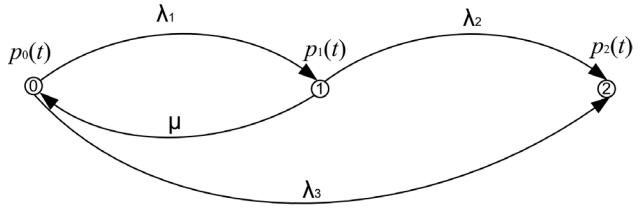

Рисунок 2 – Граф переходов

Состояния модели отражают изменения, связанные с отказами и восстановлением работоспособности изделия, а переходы определяются интенсивностями отказов и восстановлений.

Модель имеет следующие особенности:

1) поток отказов отдельных резервируемых каналов – простейший с интенсивностью $i\,\lambda$ или $j\,\lambda$.

Здесь параметры *i* и *j* представлены как сомножители λ, а в таблице 1 – в качестве обозначения принадлежности к конкретному типу системы, что не противоречит друг другу.

2) поток восстановлений принимаем как простейший, интенсивность которого $\mu = 1/T_в$, где $T_в$ – время восстановления;

3) вероятности состояний:

– $p_0(t)$– вероятность начального состояния (после начального пуска или восстановления работоспособности, когда все *i* каналов исправны);

– $p_1(t)$– вероятность состояния, при котором с интенсивностью $i\lambda$ отказал один канал (следствие события От1), а *j* каналов исправны;

– $p_2(t)$ – вероятность поглощающего состояния, при котором с интенсивностью $j\lambda$ отказал второй канал (следствие события От2) и всё устройство попадает в положение защитного отказа (исключено функционирование) или в положение опасного отказа, когда продолжается работа при неисправности.

От0, От1 и От2 представляют собой полную группу событий, поэтому:

$$p_0(t) + p_1(t) + p_2(t) = 1. \quad (4)$$

На основе графа переходов при известных λ и μ составляется система дифференциальных уравнений (уравнений Колмогорова):

$$\begin{cases} \dfrac{dp_0(t)}{dt} = -(\lambda_1 + \lambda_3)\,p_0(t) + \mu\,p_1(t) \\ \dfrac{dp_1(t)}{dt} = -(\mu + \lambda_2)\,p_1(t) + \lambda_1\,p_0(t) \\ \dfrac{dp_2(t)}{dt} = \lambda_3\,p_0(t) + \lambda_2\,p_1(t) \end{cases} \quad (5)$$

Решение системы позволяет найти вероятности состояний модели, интенсивности защитных и опасных отказов, а так же среднее время безотказного функционирования.

При этом используются следующие соотношения:

1) $\Lambda(t) = f(t)/(1 - F(t))$ – интенсивность отказов системы в целом,

где: $f(t)$– плотность распределения времени безотказной работы;

$F(t)$ – функция распределения.

В связи с тем, что кроме интенсивности отказов системы в целом необходимо определить интенсивность опасных и защитных отказов, с учётом типа системы, введём обозначения:

$\Lambda(t)$ – общая интенсивность отказов системы;

$\Lambda(t)_{\text{ОпОт}}$ – интенсивность опасных отказов;

$\Lambda(t)_{\text{ЗащОт}}$ – интенсивность защитных отказов.

При введённых обозначениях:

$$\Lambda(t) = \frac{\dfrac{dp_2(t)}{dt}}{1 - p_2(t)}, \quad (6)$$

2) интенсивности переходов из одного состояния в другое при отказах происходит в зависимости параметров *i* и *j*, а так же от наличия или отсутствия защиты:

$$\lambda_1 = i(1 - q_1)\lambda,\ \lambda_2 = j(1 - q_2)\lambda + j\,q_2\,\lambda = j\,\lambda,\ \lambda_3 = i\,q_1\,\lambda;$$

3) для рассматриваемых систем наработка на отказ имеет следующий вид

$$T_{ср} = \int_0^\infty t\,p_2'(t)dt \approx \frac{\mu}{ij\,\lambda^2}. \quad (7)$$

4) событие «время между отказами меньше задержки срабатывания защиты» эквивалентно событию «появление второго отказа за время не превосходящее τ». Вероятность последнего события определяется следующим образом:

$$q_{2\tau} = 1 - e^{-\lambda_2 \tau} \approx j\,\lambda\tau. \quad (8)$$

Формулы для определения вероятностей пребывания в различных состояниях системы, полученные при решении дифференциальных уравнений, а также другие параметры представлены в таблице 2.

Таблица 2

Параметры	Формулы
$P_0(t)$	$\frac{1}{k_1-k_2}\left[(\mu+j\lambda+k_1)e^{k_1 t}-(\mu+j\lambda+k_2)e^{k_2 t}\right]$
$P_1(t)$	$\frac{\lambda_1}{k_1-k_2}\left(e^{k_1 t}-e^{k_2 t}\right)$
$P_2(t)$	$\frac{1}{k_1-k_2}\left[(iq_1\lambda+k_2)e^{k_1 t}-(iq_1\lambda+k_1)e^{k_2 t}\right]+1$
T_{cp}	$\frac{1}{k_1k_2(k_1-k_2)}\left[(k_2-k_1)\lambda_3+k_2k_1-k_1k_1\right]\approx\frac{\mu}{ij\lambda^2}$

Здесь k_1 и k_2 – корни характеристического уравнения для системы дифференциальных уравнений (5):

$$k_1=\frac{-(\mu+(i+j)\lambda)+\sqrt{(\mu+(i+j)\lambda)^2-4(ij\lambda^2+iq_1\lambda\mu)}}{2}\approx$$
$$\approx-\lambda\left(\frac{ij\lambda}{\mu}+iq_1\right). \quad (9)$$

$$k_2=\frac{-(\mu+(i+j)\lambda)-\sqrt{(\mu+(i+j)\lambda)^2-4(ij\lambda^2+iq_1\lambda\mu)}}{2}\approx-\mu. \quad (10)$$

При этом абсолютная погрешность приближения k_1 и k_2 находится по формуле:

$$\Delta=\frac{i\lambda(j\lambda+q_1\mu)}{\mu^2}. \quad (11)$$

В соответствии с (6) общая интенсивность отказов равна:

$$\Lambda(t)=\frac{k_1(iq_1\lambda+k_2)-k_2(iq_1\lambda+k_1)e^{(k_2-k_1)t}}{(iq_1\lambda+k_1)e^{(k_2-k_1)t}-(iq_1\lambda+k_2)}. \quad (12)$$

Так как $|k_2|>>|k_1|$ и $|k_2|>>iq_1\lambda$, имеем

$$\Lambda(t)\approx(\lambda_3+k_1)e^{(k_2-k_1)t}-k_1. \quad (13)$$

Если $\Lambda(t)$ определять при назначенном сроке службы $T_н$, где, например, $T_н\approx10^5$ ч, то

$$\Lambda(t)\approx\frac{ij\lambda^2}{\mu}+iq_1\lambda. \quad (14)$$

Определим интенсивности опасного и защитного отказов.

При обозначениях, принятых в настоящей статье выражение (1) имеет следующий вид:

$$\Lambda(t)=\Lambda(t)_{\text{ЗащОт}}+\Lambda(t)_{\text{ОпОт}}. \quad (15)$$

Следствием этого являются выражения:

$$\Lambda(t)=\Lambda(t)p(t)_{\text{ЗащОт}}+\Lambda(t)p(t)_{\text{ОпОт}}. \quad (16)$$

$$p(t)_{\text{ЗащОт}}+p(t)_{\text{ОпОт}}=1, \quad (17)$$

где $p(t)_{\text{ЗащОт}}$, $p(t)_{\text{ОпОт}}$ – вероятности защитного и опасного состояний.

Для определения $p(t)_{\text{ЗащОт}}$ и $p(t)_{\text{ОпОт}}$ целесообразно обратить внимание на вывод формулы вероятности поглощающего состояния $p_2(t)$. Он осуществляется интегрированием уравнения $\frac{dp_2(t)}{dt}=\lambda_3 p_0(t)+\lambda_2 p_1(t)$ (из системы дифференциальных уравнений (5)). Здесь $\lambda_3=iq_1\lambda$ – интенсивность перехода от начального состояния к поглощающему состоянию при отсутствии защиты (с вероятностью q_1), т.е. перехода к опасному отказу, $\lambda_2=j(1-q_2)\lambda+jq_2\lambda$ – интенсивность перехода от состояния после первого отказа к поглощающему состоянию при наличии защиты (с вероятностью $1-q_2$) и при отсутствии защиты (с вероятностью q_2) т.е. переходов к защитному и опасному отказам соответственно.

Таким образом, вероятности переходов к опасному отказу и к защитному отказу разделимы, то есть :

$$p_2(t)=p_{2,\text{оп}}(t)+p_{2,\text{защ}}(t), \quad (18)$$

из чего следует

$$p(t)_{\text{ЗащОт}}=\frac{p_{2,\text{защ}}(t)}{p_2(t)},\ p(t)_{\text{ОпОт}}=\frac{p_{2,\text{оп}}(t)}{p_2(t)}. \quad (19)$$

Если $p_2(t)$ представить в следующем виде

$$p_2(t)=\frac{\lambda_3}{k_1-k_2}\left[\frac{1}{k_1}(\mu+\lambda_2+k_1)e^{k_1t}-\frac{1}{k_2}(\mu+\lambda_2+k_2)e^{k_2t}\right]+$$
$$+\frac{\lambda_3(\mu+\lambda_2)}{k_1k_2}+\frac{\lambda_1\lambda_2}{k_1-k_2}\left(\frac{1}{k_1}e^{k_1t}-\frac{1}{k_2}e^{k_2t}\right)+\frac{\lambda_1\lambda_2}{k_1k_2},$$

то после подстановки значений для интенсивностей переходов получаем разделенную формулу

$$p_2(t)=\frac{iq_1\lambda}{k_1-k_2}\left[\frac{1}{k_1}(\mu+j\lambda+k_1)e^{k_1t}-\frac{1}{k_2}(\mu+j\lambda+k_2)e^{k_2t}\right]+$$
$$+\frac{i(1-q_1)\lambda jq_2\lambda}{k_1-k_2}\left(\frac{1}{k_1}e^{k_1t}-\frac{1}{k_2}e^{k_2t}\right)+$$
$$+\frac{i\lambda(\mu q_1+jq_1\lambda+jq_2\lambda-jq_1q_2\lambda)}{k_1k_2}+$$
$$+\frac{i(1-q_1)\lambda j(1-q_2)\lambda}{k_1k_2(k_1-k_2)}(k_2e^{k_1t}-k_1e^{k_2t}+k_1-k_2),$$

Где

$$p_{2,on}(t)=\frac{iq_1\lambda}{k_1-k_2}\left[\frac{1}{k_1}\left(\mu+j\lambda+k_1\right)e^{k_1t}-\frac{1}{k_2}\left(\mu+j\lambda+k_2\right)e^{k_2t}\right]+$$
$$\frac{i\left(1-q_1\right)\lambda jq_2\lambda}{k_1-k_2}\left(\frac{1}{k_1}e^{k_1t}-\frac{1}{k_2}e^{k_2t}\right)+$$
$$+\frac{i\lambda\left(\mu q_1+jq_1\lambda+jq_2\lambda-jq_1q_2\lambda\right)}{k_1k_2}, \quad (20)$$

$$p_{2,\text{защ}}(t)=\frac{i\left(1-q_1\right)\lambda j\left(1-q_2\right)\lambda}{k_1k_2\left(k_1-k_2\right)}\left(k_2e^{k_1t}-k_1e^{k_2t}+k_1-k_2\right). \quad (21)$$

С целью упрощения выражений для $p(t)_{\text{ЗащОт}}$ и $p(t)_{\text{ОпОт}}$, воспользовавшись примерными значениями k_1 и k_2 (9), (10) и тем, что μ>>λ получим:

$$p(t)_{\text{ЗащОт}}=\frac{p_{2,\text{защ}}(t)}{p_2(t)}\approx\left(1-q_1\right)\left(1-q_2\right), \quad (22)$$

$$p(t)_{\text{ОпОт}}=\frac{p_{2,\text{оп}}(t)}{p_2(t)}\approx 1-\left(1-q_1\right)\left(1-q_2\right). \quad (23)$$

С учётом выражения для интенсивности Λ(*t*) (15) имеем:

$$\Lambda(t)_{\text{ЗащОт}}\approx\lambda\left(\frac{ij\lambda}{\mu}+iq_1\right)\left(1-q_1\right)\left(1-q_2\right), \quad (24)$$

$$\Lambda(t)_{\text{ОпОт}}\approx\lambda\left(\frac{ij\lambda}{\mu}+iq_1\right)\left[1-\left(1-q_1\right)\left(1-q_2\right)\right]. \quad (25)$$

Заключение

В работе представлены формулы, позволяющие оценить безопасность и отказоустойчивость различных систем с горячим резервированием. Эти системы нормально функционируют до двух отказов в различных каналах и имеют возможность восстановления по результатам контроля без остановки функционирования.

Развитый контроль и диагностика позволяют эксплуатировать представленные системы по техническому состоянию.

Библиографический список

1. Некоторые положения отказобезопасности и киберзащищенности систем управления / В. А. Гапанович, Е. Н. Розенберг, И. Б. Шубинский // Надежность.- 2014. – № 2. – С. 88-100

2. ГОСТ Р 27. 002-89 Надежность в технике. Основные понятия. Термины и определения.

3. ГОСТ Р 51901.5-2005 (МЭК 60300-3-1:2003) Руководство по применению методов анализа надежности.

4. ГОСТ Р МЭК 62061-2013 Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью

5. Системы автоматики и телемеханики на железных дорогах мира, под ред.Г.Теега, С.Власенко. ISBN 978-5-89277-098-9,М.: «Интекст», 2010, 496 с.

6. Авакян А.А. Создание сверхнадёжных электронных систем для аэрокоосмической техники // Контроль. Диагностика. – 2013. – №2. С 67-75.

7. Г. Х. Новик, “О достоверности сигнатурного анализа”, Автомат.и телемех., 1982, № 5, С. 157–159

8. Гольдштейн В. Б. Миронов С. В. Хеш-функции для сокращения диагностической информации. Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика, Выпуск№ 2 / том 7 / 2007

9. Иыуду К.А. Надёжность, контроль и диагностика вычислительных машин и систем. М: Высшая школа,1989. с. 145 – 166.

Сведения об авторах

Олег Л. Маковеев, кандидат технических наук, советник по науке НТК ЖАТ ОАО «Радиоавионика». 190005, Россия, Санкт-Петербург, Троицкий пр., д.4, лит. Б, тел. +7(812) 251-49-38, e-mail: makoveev38@mail.ru

Сергей Ю. Костюнин, кандидат физико-математических наук, начальник отдела ОАО «Радиоавионика». 190005, Россия, Санкт-Петербург, Троицкий пр., д. 4, лит. Б, тел. +7(812) 251-49-38, e-mail: kostyunin.sergey@gmail.com

Поступила 29.09.2016