УДК 621.3.019.3

СТРАТЕГИЯ ОТКАЗОБЕЗОПАСНОСТИ КАК АЛЬТЕРНАТИВА ПОЛНОЙ ОТКАЗОУСТОЙЧИВОСТИ ПРИ ПРОЕКТИРОВАНИИ ГАРАНТОСПОСОБНЫХ КОМПЬЮТЕРНЫХ СИСТЕМ. ЧАСТЬ 2

Федухин А.В., Муха А.А.
Институт проблем математических машин и систем
Национальной академии наук Украины

Статья посвящена вопросам безопасности гарантоспособных компьютерных систем. Сформулирована стратегия отказобезопасности как альтернатива дорогостоящей стратегии полной отказоустойчивости системы, описаны методы обеспечения безопасности, приводятся необходимые понятия и определения.
Ключевые слова: безотказность, отказоустойчивость, безопасность, отказобезопасность компьютерных систем.

Введение. Эксплуатация гарантоспособных систем с высокими требованиями к отказоустойчивости в отраслях с повышенным уровнем безопасности позволяет выделить некоторые основные аспекты. **Одним из таких аспектов является стратегия отказобезопасности, которая может быть успешно применена в условиях соблюдения высокого уровня безопасности процесса при относительно экономных затратах.** В таком случаи полная отказоустойчивость сменяется частичной, акцентированной на критически важных факторах безопасности процесса которые могут быть переведены в защитное безопасное состояние при полном исключении негативных последствий. **Таким образом целью стати является формулирование стратегии отказобезопасности как альтернативы стратегии полной отказоустойчивости системы.**

1. Концепция безопасности компьютерных систем

Под **концепцией безопасности** *(safety concept)* понимается совокупность положений, в соответствии с которыми осуществляется построение безопасной системы. Безопасная система должна удовлетворять заданному уровню безопасности. Уровень безопасности определяется предельными значениями показателей безопасности. Показатели безопасности составляют количественную характеристику свойств безопасности.

Концепция безопасности имеет фундаментальное значение, поскольку на ее основе устанавливаются критерии опасных отказов. Для реализации концепций безопасности используют две стратегии – безотказность *(reliability)* и отказоустойчивость *(fault-tolerance)*. Эти стратегии подразумевают, что система, которая правильно выполняет свой алгоритм функционирования, безопасна. **Стратегия отказобезопасности** *(failure safety strategy)* (безопасное поведение при отказах) используется специально для систем критического применения и заключается в переводе системы в **защитное необратимое состояние** при появлении отказа (рис. 1). При этом обратный переход в работоспособное состояние исключается (маловероятен) и осуществляется искусственно (обычно с участием человека).

При построении современных ГКС стратегия отказобезопасности часто используется совместно со стратегией отказоустойчивости либо самостоятельно, так как является самодостаточной. Если при возникновении отказов система исчерпала свои резервные возможности и в результате деградации и реконфигурации перестала быть отказоустойчивой, то при появлении еще одного отказа она должна необратимо перейти в защитное состояние (например, отключенное от объектов управления).

Стратегия отказобезопасности в этом случае формулируется следующим образом: одиночные

дефекты аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться с заданной вероятностью на рабочих или тестовых воздействиях не позднее, чем в системе возникнет второй дефект [1; 2].

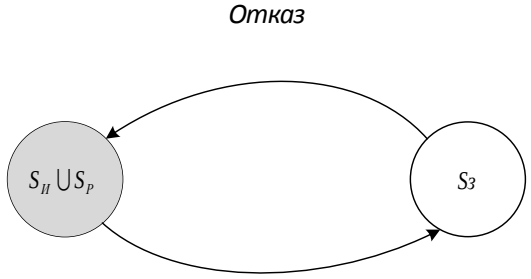

Рис. 1. Граф переходов в отказобезопасной системе

2. Критерии опасных отказов

Критерии опасных отказов устанавливают в нормативно-технической документации для однозначного определения опасных состояний элементов, устройств и систем. Эти критерии используются в дальнейшем при доказательстве безопасности КС на всех стадиях ее жизненного цикла при разработке, испытаниях, эксплуатации и ремонте.

Определяя критерии опасных отказов, следует учитывать вид, назначение и структуру устройств ГКС, требования по безопасности, предъявляемые к ГКС, концепцию безопасности, принятую при разработке, последствия опасных отказов, свойства применяемых материалов [3].

Для аналоговых и части цифровых устройств формальным критерием опасных отказов является выход значений показателей качества функционирования, влияющих на безопасность, за пределы установленных норм. Для цифровых устройств КС формальные критерии опасных отказов связаны с искажениями их алгоритмов функционирования. В общем случае алгоритм работы цифровой системы задается с использованием входных и выходных последовательностей (слов). Если эти последовательности бесконечны, то для их задания применяют различные формализованные языки (регулярные выражения, таблицы переходов, граф-схемы алгоритмов и др.). Тогда алгоритм представляют с помощью некоторой математической конструкции E. Это может быть алгебраическое выражение, граф состояний, цепочки символов специального вида и др. При синтезе безопасной системы опасные искажения ее алгоритма должны быть записаны с использованием специальных конструкций на том же языке. Отсутствие опасных ситуаций в ответственном технологическом процессе гарантируется условием

$$E \cap E_{ОП} = \emptyset \qquad (1)$$

При возникновении внутренних отказов происходит искажение алгоритма работы системы вида $E \rightarrow E'$. Тогда отказ является неопасным, если

$$E' \cap E_{ОП} = \emptyset \qquad (2)$$

Общая математическая постановка задачи синтеза безопасной системы состоит в том, что требуется обеспечить выполнение условий (1) и (2).

Условие (1) удовлетворяется в результате полноты учета (перечисления) всех состояний технологического процесса, связанных с возникновением опасных ситуаций. Принципиально это, очевидно, всегда может быть выполнено. Принципиальная возможность выполнения условия (2) доказана в работе [4]. Процедуры проверки условий (1) и (2) являются содержанием экспериментов, которые проводятся при испытаниях на безопасность ГКС. С помощью компьютерных технологий проверяются на безопасность технологические алгоритмы и работа систем при возникновении отказов. При формулировке критериев опасных отказов для ГКС признаки опасных состояний определяются вследствие нарушения положений концепции безопасности, в соответствии с которой построена система.

3. Анализ методов обеспечения безопасности компьютерных систем

И так, для реализации концепции безопасности используют пять основных стратегий: безотказность; отказоустойчивость; отказобезопасность; безошибочность; помехоустойчивость. Перечислим их.

А. Стратегия безотказности подразумевает, что если в системе нет отказов, то она безопасна. Задачей стратегии безотказности является создание ГКС, у которых интенсивность отказов сравнима с нормируемой интенсивностью опасных отказов. В этом случае любой отказ можно считать опасным, никакой дополнительной защиты от отказов не требуется. Основными путями реализации стратегии безотказности являются: минимизация логических схем; снижение интенсивностей потока отказов элементов.

Классические показатели безотказности систем, такие как вероятность безотказной работы $R(t)$ – вероятность того, что в пределах заданной наработки отказ объекта не возникает, средняя наработка до отказа (на отказ) $T_{ср}$ – математическое ожидание наработки объекта до первого отказа (на отказ), параметр потока отказов $\omega(t)$ – отношение математического ожидания числа отказов восстанавливаемого объекта за достаточно малую его наработку к значению этой наработки не в полном объеме характеризуют безотказность системы, так как не учитывает основное свойство гарантоспособных систем – их отказоустойчивость. В [5] предлагается набор специальных метрик безотказности, учитывающих свойство отказоустойчивости системы, заложенное при проектировании.

Вероятность безотказной работы отказоустойчивой системы ${}^{f}_{c}R^{q}_{s}$**:**

$$ {}^{f}_{c}R^{q}_{s} = c^{s}(1 - {}^{f}F^{q}_{s}), \qquad (3)$$

где ${}^{f}F^{q}_{s}$ – функция вероятности отказа;

s – количество резервов, изначально доступных для подключения;

q – количество модулей одного типа, работающих параллельно (характеристика актуальна для систем, производительность которых зависит от количества одновременно работающих ресурсов);

c – степень компенсации последствий отказа [6] (условная вероятность того, что при возникновении отказа в работающей системе последняя способна восстановить информацию и продолжить ее обработку без долговременной потери данных);

f – способность модуля допускать f одиночных отказов до того, как он станет неработоспособным.

Принимая гипотезу о DN-распределении наработки до отказа элементов, модулей и системы в целом, вероятность отказа будем вычислять следующим образом:

$$ {}^{f}F_{s}^{q} = DN(x; v, f, q, s), \quad (4) $$

где v – коэффициент вариации наработки до отказа;

x – относительная наработка ($x = \frac{t}{T_{ср}}$, t – время работы, $T_{ср}$ – средняя наработка до отказа (на отказ).

Функция вероятности отказа для DN-распределения имеет следующий вид:

$$ DN(x;v) = \Phi\left(\frac{x-1}{v\sqrt{x}}\right) + \exp\left(2v^{-2}\right)\Phi\left(-\frac{x+1}{v\sqrt{x}}\right), \quad (5) $$

где Ф(∗) – функция нормированного нормального распределения.

Если любой из параметров метрики ${}_{c}^{f}R_{s}^{q}$ опускается, то по умолчанию предполагается $q = 1$, $c = 1$, $f = 0$, $s = 0$. Параметры s, c, и f являются параметрами, увеличение которых приводит к увеличению общей безотказности системы.

Число неизбыточных каналов системы $N_{c.}$ – характеристика объема аппаратных затрат, необходимого для достижения данного уровня безотказности системы.

Вероятность безотказной работы неизбыточного канала системы $R_K(t)$ – характеристика уровня надежности элементов и составных частей неизбыточного канала системы.

Установленная наработка системы t_c – наработка системы на момент достижения установленного в спецификации уровня вероятности безотказной работы $R_{спец}(t)$.

$$ R_c(t_c) = R_{спец}, \quad (6) $$

где t_c – время достижения системой установленного в спецификации уровня вероятности безотказной работы.

B. Стратегия отказоустойчивости подразумевает, что если система правильно выполняет свой алгоритм функционирования даже при наличии отказов, то она безопасна. Отказоустойчивые системы нечувствительны к определенному числу отказов. Их еще называют α-безотказными. Это значит, что система работает правильно при наличии в ней α или менее отказов. Число α является показателем отказоустойчивости. Это качество системы резко повышает ее безотказность и безопасность, но требует введения большой избыточности в аппаратные и программные средства. Объем аппаратуры возрастает в таких системах в два, три и более раз. Для ГКС отказоустойчивость становится одним из основных направлений развития. Основные пути реализации стратегии отказоустойчивости: резервирование; диагностирование; реконфигурация; восстановление.

Отказоустойчивость базируется на резервировании. Остальные средства (диагностирование, восстановление и реконфигурация) только повышают ее эффективность.

В реальных ГКС, как правило, используют комплекс мер по обеспечению отказоустойчивости, причем в различных элементах и узлах системы можно использовать различные виды резервирования, отличающиеся степенью избыточности (кратностью резервирования). Используют различные методы и средства контроля, восстановления и реконфигурации.

В качестве дополнительных показателей отказоустойчивости можно применять: полноту резервирования элементов и узлов системы; полноту и достоверность контроля; вероятность восстановления резерва и т.п.

Первые две стратегии подразумевают, что система, которая правильно выполняет свой алгоритм функционирования, безопасна. Номенклатура рекомендуемых показателей гарантоспособности системы в целом приведена в [7].

C. Стратегия отказобезопасности используется специально для систем критического применения и заключается в переводе системы в защитное необратимое состояние при появлении отказа. Обратный переход в работоспособное состояние исключается и производится обычно с участием человека. Основные пути реализации стратегии отказобезопасности: использование самопроверяемых схем; использование элементной базы с несимметричными характеристиками отказов.

При построении безопасных ГКС могут использоваться несколько различных стратегий одновременно. Например, при построении микроэлектронных и микропроцессорных систем стратегия отказобезопасности (безопасного поведения при отказах) применяется совместно со стратегией отказоустойчивости. Если при возникновении отказов система исчерпала резервные возможности и в результате деградации и реконфигурации перестала быть отказоустойчивой, то при появлении еще одного отказа она должна необратимо перейти в защитное состояние.

Безопасность технических средств ГКС в разомкнутых системах управления, регулирования и контроля сильно зависит от человеческого фактора при разработке, изготовлении и эксплуатации системы. Поэтому для создания безопасных технических средств дополнительно используют стратегию безошибочности.

D. Стратегия безошибочности предполагает сведение к минимуму влияния на безопасность функционирования системы человеческого фактора (ошибок человека) при разработке, изготовлении и эксплуатации системы. Основные пути реализации стратегии безошибочности:

· при разработке и проектировании: поэтапное выполнение работ с верификацией результатов каждого этапа; документированность каждого этапа разработки; стандартизация и унификация; контролируемость процесса разработки; автоматизация проектирования;

· организация дружественного интерфейса пользователя; защита от несанкционированного доступа; преемственность по отношению к эксплуатируемым в настоящее время системам; наличие обратной связи от технических средств к пользователю; рациональное распределение функций между пользователем и техническими средствами для обеспечения умеренной загрузки оператора;

· обеспечение контролепригодности системы; простота представления контрольной и диагностической информации; интеллектуаль-

ная поддержка технического обслуживания и ремонта; дублирование информации о работоспособности системы.

Но даже разработанная по всем правилам построения безопасная ГКС может быть неработоспособна из-за ее низкой помехозащищенности.

Е. Стратегия помехоустойчивости на всех этапах разработки микропроцессорных и микроэлектронных ГКС должна обеспечиваться проведением мероприятий по обеспечению заданного уровня помехоустойчивости. **Помехоустойчивость** *(Immunity)* – это свойство аппаратуры, обеспечивающее защищенность ее от воздействия внешних электромагнитных влияний. Поэтому при испытаниях на электромагнитную совместимость (ЭМС) микроэлектронных систем обеспечения безопасности актуальной является проблема анализа последствий сбоев и поиска сбоев, приводящих к нарушению безопасности функционирования систем. Основными путями реализации стратегии помехоустойчивости являются: подавление электромагнитных помех в источнике возникновения; понижение восприимчивости к электромагнитным помехам аппаратуры; воздействие на паразитный канал проникновения помех.

4. Заключение. Стратегия отказобезопасности как альтернатива полной отказоустойчивости в отраслях с критическим уровнем безопасности, может быть применена при возможности перевода системы в **защитное необратимое состояние** для последующего технического обслуживания.

При реализации стратегии отказобезопасности ключевым этапом является определение критериев безопасности и методов их контроля. При формировании критериев безопасности следует использовать стратегии безотказности; отказоустойчивости; отказобезопасности; безошибочности; помехоустойчивости.

Список литературы:

1. ОСТ 32.17-92. Безопасность железнодорожной автоматики и телемеханики. Термины и определения. – СПб.: ПИИТ, 1992. – 33 с.
2. Сапожников В.В., Кравцов Ю.А., Сапожников Вл.В. Дискретные устройства железнодорожной автоматики, телемеханики и связи. – М.: Транспорт, 1988. – 255 с.
3. РД 32 ЦШ 1115842.03-93. Безопасность железнодорожной автоматики телемеханики. Критерии опасных отказов. – СПб.: ПГУПС, 1993. – 19 с.
4. Сапожников В.В., Сапожников Вл.В. О синтезе конечных автоматов с исключением опасных отказов // Автоматика и телемеханика, 1972 № 8. – С. 93-99.
5. Федухин А.В., Пасько В.П. К вопросу о количественных характеристиках безотказности избыточных компьютерных систем // Математичні машини і системи. – 2012. – № 1. – С. 145-156.
6. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.
7. Федухин А.В., Сеспедес Гарсия Н.В. Атрибуты и метрики гарантоспособных компьютерных систем // Математичні машини і системи. – 2013. – № 2. – С. 195-201.

Федухін О.В., Муха А.А.
Інститут математичних машин та систем
Національної академії наук України

СТРАТЕГІЯ ВІДМОВОБЕЗПЕКИ ЯК АЛЬТЕРНАТИВА ПОВНІЙ ВІДМОВОСТІЙКОСТІ ПРИ ПРОЕКТУВАННІ ГАРАНТОЗДАТНИХ КОМПЬЮТЕРНИХ СИСТЕМ. ЧАСТИНА 2

Анотація
Стаття присвячена питанням безпеки гарантоздатних комп'ютерних систем. Сформульована стратегія відмовобезпеки як альтернатива дорогої стратегії повної відмовостійкості системи, описані методи забезпечення безпеки, наводяться необхідні поняття і визначення.

Ключові слова: безвідмовність, відмовостійкість, безпека, відмовобезпека комп'ютерних систем.

Feduhin A.V., Mukha A.A.
Institute of Mathematical Machines and Systems Problems
of the Ukraine National Academy of Science

FAILPASSIVE STRATEGY AS AN ALTERNATIVE DESIGN FULL FAULT TOLERANCE OF DEPENDABLE COMPUTER SYSTEMS. PART 2

Summary
The article is devoted to the issues of security of dependable computer systems. Fail-safe strategy is formulated as an alternative to costly strategy complete fault tolerance system, the methods of security, provides the necessary concepts and definitions.

Keywords: reliability, fault tolerance, security, computer systems failure safety.