УДК 621.3.019.3

СТРАТЕГИЯ ОТКАЗОБЕЗОПАСНОСТИ КАК АЛЬТЕРНАТИВА ПОЛНОЙ ОТКАЗОУСТОЙЧИВОСТИ ПРИ ПРОЕКТИРОВАНИИ ГАРАНТОСПОСОБНЫХ КОМПЬЮТЕРНЫХ СИСТЕМ. ЧАСТЬ 1

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. Наиболее важным свойством гарантоспособных компьютерных систем (ГКС) является свойство отказоустойчивости. Без этого свойства невозможно создать систему с высоким уровнем гарантоспособности. Отказоустойчивость напрямую или косвенно влияет на такие атрибуты, как безотказность, готовность, живучесть и функциональная безопасность. Кроме того отказоустойчивость, основанная, как известно, на структурной избыточности и методах многоверсийного проектирования, определяет уровень гарантоспособности вычислений, выполняемых программными средствами ГКС. **Отказоустойчивость ГКС является дорогостоящим свойством, которое может себе позволить не каждый заказчик.** Например, пилотируемые космические корабли имеют так много избыточных и отказоустойчивых компонент, что их вес сильно увеличивается по сравнению с беспилотными аппаратами, которые не требуют такого уровня отказоустойчивости.

В большинстве случаев критического применения ГКС экономически обоснованным является замена полной отказоустойчивости на частичную отказоустойчивость, названную нами **отказобезопасностью**. Использование подхода, при котором стратегия полной отказоустойчивости заменяется стратегией отказобезопасности позволяет строить экономически эффективные ГКС с меньшими техническими затратами, дополнив их системой предупредительного технического обслуживания для повышения уровня гарантоспособности. Особенностью стратегии отказобезопасности является то, что она допускает наличие отказов системы, но только таких, при которых последняя переходит в защитное безопасное состояние и полностью исключает появление таких отказов, при которых система переходит в опасное состояние, чреватое катастрофическими последствиями. Данная стратегия положена в основу построения электронных и компьютеризованных средств железнодорожной автоматики, связанных с обеспечением безопасности движения поездов. **Целью данной статьи является подробный обзор особенности реализации этих двух подходов в обеспечении безопасности ГКС и формулирование стратегии отказобезопасности как альтернативы стратегии полной отказоустойчивости системы.**

1. Отказоустойчивость как базовая платформа гарантоспособности

Отказоустойчивость *(fault tolerance)* – свойство технической системы сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Отказоустойчивость определяется количеством любых последовательных единичных отказов компонентов, после которых сохраняется работоспособность системы в целом.

Основной способ реализации отказоустойчивости – введение избыточности. **Полная отказоустойчивая инженерия** *(Complete fault-tolerant Engineering)* – это метод проектирования отказоустойчивых систем, которые способны продолжать выполнение запланированных операций (возможно, с понижением эффективности) при отказе их компонентов [1]. Если каждый компонент системы может продолжать работать при отказе одной из его составляющих, то вся система, в свою очередь, также продолжает работать и называется **полностью отказоустойчивой** *(a fully fault-tolerant)*.

Стратегия полной отказоустойчивости основана на введении избыточности в структуру системы. Избыточностью называют функциональность, в которой нет необходимости при безотказной работе системы [2]. Впервые идея включения избыточных частей для увеличения надежности системы была высказана Джоном фон Нейманом в 1950-х годах [3]. Существует два типа избыточности [4]: пространственная и временна́я. Пространственная избыточность реализуется путем введения дополнительных компонентов, функций или данных, которые не нужны при безотказном функционировании. Дополнительные (избыточные) компоненты могут быть аппаратными, программными и информационными. Временная избыточность реализуется путем повторных вычислений или отправки данных, после чего результат сравнивается с сохранённой копией предыдущего результата.

Иногда обеспечение отказоустойчивости ГКС требует, чтобы вышедшие из строя части были извлечены и заменены новыми, в то время как система продолжает работать (горячая замена). Это реализуется с помощью избыточной части, находящейся в резерве и большая часть отказоустойчивых систем строится именно так, при условии, что среднее время между отказами достаточно велико, чтобы операторы могли успеть выполнить ремонт до того, как резервная часть также выйдет из строя.

Наиболее эффективный метод введения избыточности – аппаратная избыточность, которая достигается путем резервирования. Проектирование каждого компонента ГКС как отказоустойчивого привносит в систему некоторые недостатки, такие как увеличение веса, стоимости, энергопотребления, цены и времени, затраченного на проектирование, проверку и испытания, кроме того полностью отказоустойчивые решения имеют и другие, не менее важные недостатки, а именно:

· сложность в обнаружении однокомпонентных неполадок. Возможность неконтролированного накопления неисправностей в компонентах. Проблема может быть решена путем добавления специальной системы для обнаружения неисправностей компонент.

· сложность в обнаружении многокомпонентных неполадок. Отказоустойчивость одного компонента может мешать обнаружению неполадок в другом.

· сложность проверки работоспособности. Для некоторых крайне важных отказоустойчивых систем критического применения нет простого пути, чтобы удостовериться, что дополнительные избыточные компоненты находятся в исправном состоянии.

В качестве показателей, характеризующих отказоустойчивость системы, рекомендуются следующие:

Порог сравнения информации в системе M_c:

$$M_c = \prod_{i=1}^{n} M_{ci}, \quad (1)$$

где M_{ci} порог сравнения i-го последовательно включенного сравнивающего устройства.

Число работоспособных конфигураций системы U_c:

$$U_c = \prod_{i=1}^{n} U_{ci}, \quad (2)$$

где U_{ci} – число работоспособных конфигураций i-ой подсистемы.

Коэффициент отказоустойчивости $K_{ОУ}$ – отношение средних наработок на отказ нерезервированной и отказоустойчивой систем:

$$K_{ОУ} = \frac{T_{НР}}{T_{ОУ}}, \quad (3)$$

где $T_{НР}$ – средняя наработка на отказ нерезервированной системы;

$T_{ОУ}$ – средняя наработка на отказ отказоустойчивой системы.

2. Безопасность компьютерных систем

Требования гарантоспособности предъявляются прежде всего к компьютерным системам критического применения, для которых требование безопасности приобретает наиболее важное значение. **Безопасность** (Security) в обычном понимании этого слова трактуется как сохранность человека, объекта, груза, окружающей среды. Однако в технике этому термину придается и более широкое понятие [5, 6]. Например, под «безопасной компьютерной системой» подразумевается не только наличие ее собственной безопасности как технического объекта, но и наличие безопасности результатов ее работы (расчетов, управляющих команд, информации и т.д.). В зависимости от отрасли применения ГКС понятие безопасности конкретизируется в соответствии с конкретными ее задачами и особенностями. На сегодняшний день трудно найти область человеческой деятельности, где бы ни требовались компьютерные системы высокой надежности и безопасности. В энергетике: системы управления и контроля на атомных, тепловых и гидроэлектростанциях, системы управления котлами высокого давления, системы управления энергоснабжением, системы управления транзитом энергоресурсов и др. На транспорте: системы управления движением транспорта, системы автоматики и автоматизации управления транспортными средствами и др. В промышленности: системы управления и контроля в сфере опасных технологий и инфраструктур и др. В области жизнедеятельности человека: системы охраны, противопожарные системы, системы контроля за состоянием окружающей среды и предупреждения об экологических катастрофах, системы безопасности сооружений с большим скоплением людей, системы обеспечения безопасности от террористических угроз и др. В военно-промышленном комплексе: системы управления войсками, системы управления и навигации объектами военного и смежного назначения, системы безопасности военных арсеналов и др. В медицине: системы обеспечения жизнедеятельности пациентов и др. В области финансов: системы управления финансовыми учреждениями и платежными системами и др.

Безопасность компьютерных систем критического применения можно разделить на внешнюю и внутреннюю. Внешняя безопасность связана с сохранностью компьютерной системы, как технического объекта, и может нарушаться из-за внешних причин (разрушающего влияния окружающей среды или действий человека). Внутренняя безопасность это свойство объекта не являться источником опасности по отношению к внешним объектам (человеку, окружающей среде). Внутренняя безопасность рассматривается как составляющая надежности и безопасности в связи с тем, что отказы элементов КС, которые нарушают безопасность, одновременно приводят к нарушению надежности.

Функциональная безопасность (ФБ) *(functional safety)* – основная часть общей безопасности ГКС, обеспечивающая отсутствие неприемлемого риска как функционированию самой системы, так и здоровью людей, их собственности или окружающей среде. ФБ является очень важным атрибутом для систем критического использования, связанных с безопасностью людей и окружающей среды обитания человека (системы энергетики, химической промышленности, транспорта и т.д.). Целью управления ФБ является минимизация неприемлемого риска нанесения вреда здоровью людей (непосредственно или косвенно – через нанесение ущерба собственности или окружающей среде). Цель обеспечения ФБ считается достигнутой, когда каждая функция обеспечения ФБ системы осуществляется эффективно и обеспечивает выполнение требуемых показателей. В работе [7] безопасность определяется как параметр, показывающий, насколько из-за эксплуатации некоторого технического устройства или из-за выхода из строя частей прибора подвергаются опасности, материальные ценности или человеческие жизни. В работе [8] безопасность рассматривается

как свойство объекта не обусловливать возникновение опасных для производства (движения) ситуаций при наличии определенных внешних воздействий на протяжении определенного времени или при выполнении определенного объема работ. В монографиях [9, 10] безопасность определяется, как способность не допускать ущерба для жизни и здоровья людей, для материальных и духовных ценностей вследствие изменения внутренних свойств объекта, внешних субъективных или объективных дестабилизирующих факторов и воздействий.

3. Показатели безопасности компьютерных систем

В конкретных случаях при разработке реальных ГКС могут использоваться смешанные стратегии безопасности, основная задача которых состоит в том, чтобы обеспечить необходимые предельные значения показателей безопасности (нормы безопасности). Показатели безопасности могут быть количественными или качественными. Количественные показатели характеризуют безопасность непосредственно с помощью некоторых числовых величин. Качественные показатели дают косвенную оценку безопасности.

Количественные показатели безопасности делятся на детерминированные и вероятностные. Детерминированные показатели обычно выражаются физическими величинами или отношением этих величин. Детерминированным показателям присущ ряд недостатков. Они не отражают вероятностную природу процессов эксплуатации и обслуживания систем, имеют обычно ограниченную область применения и носят частный характер. Они не могут быть определены априорными аналитическими методами при разработке систем.

Наиболее адекватно оценивают ФБ вероятностные количественные показатели. Они имеют общий характер (применяются для любых систем, элементов и устройств) и могут определяться экспериментально, быть рассчитанными или смоделированы. Основные показатели безопасности следующие:

Вероятность безопасной работы $R_{ОП}(t)$ – вероятность того, что в пределах заданной наработки опасный отказ системы не наступает.

$$R_{ОП}(t) = 1 - F_{ОП}(t), \quad (4)$$

где $F_{ОП}(t)$ – функция распределения наработки до опасного отказа.

Вероятность опасного отказа $Q_{ОП}(t)$ – вероятность того, что в пределах заданной наработки опасный отказ наступает хотя бы один раз.

$$Q_{ОП}(t) = F_{ОП}(t) = 1 - R_{ОП}(t). \quad (5)$$

Средняя наработка на опасный отказ $T_{ОПср}$ – отношение суммарной наработки восстанавливаемой системы $t_{\Sigma i}$ к математическому ожиданию числа опасных отказов в течение этой наработки $m_{ОП}$.

$$T_{ОПср} = \frac{t_{\Sigma н}}{m_{ОП}}. \quad (6)$$

4. Отказобезопасность как синтез отказоустойчивости и функциональной безопасности

Математический аппарат синтеза и анализа в рамках **стратегии отказобезопасности** принадлежит профессорам Петербургского государственного университета путей сообщения (ПГУПС) братьям Сапожникову В.А. и Сапожникову Вл.А.. Рассмотрение данного направления в проектировании ГКС начнем с введения следующих понятий и определений.

Алгоритм работы ГКС в рамках данной стратегии должен исключать опасные ситуации не только при исправном, но и при неисправном состоянии самой системы. Внутренние отказы системы не должны приводить к опасным искажениям алгоритма ее работы. Сформулируем базовые понятия стратегии отказобезопасности.

Защитное состояние *(Protective State)* – неработоспособное состояние системы, при котором значения всех параметров, характеризующих способность выполнять заданные функции по обеспечению безопасности, соответствуют требованиям нормативно-технической и (или) конструкторской документации (НТД, КД).

Опасное состояние *(Hazardous State)* – неработоспособное состояние системы, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции по обеспечению безопасности, не соответствует требованиям НТД и (или) КД.

Таким образом, ФБ ГКС можно уточнить как свойство системы непрерывно сохранять исправное, работоспособное или защитное состояние в течение некоторого времени или наработки.

Защитный отказ *(Protective Failure)* – событие, заключающееся в нарушении работоспособного состояния системы при сохранении защитного состояния.

Опасный отказ *(Hazardous Failure)* – событие, заключающееся в нарушении работоспособного и защитного состояний системы.

При оценке безопасности в работе [11] исходят из понятия безопасного состояния, которое может принять система или ее компонент. В этом состоянии исключена опасность со стороны системы. В работе [12] безопасность технического устройства рассматривается как его свойство находиться в штатном или нештатном неопасном состоянии. Под штатным понимается состояние, когда технологический процесс развивается в соответствии с заданным алгоритмом, определяющим адекватную реакцию системы управления на внешние факторы.

Рассмотрим схему основных состояний и событий в ГКС (рис. 1), где цифрами обозначены: использование по назначению 1, защитный отказ 2, опасный отказ 3, переход системы в предельное состояние (неустранимое нарушение требований безопасности, снижение эффективности эксплуатации, моральное старение, износ и другие факторы) 4, восстановление 5, ремонт 6.

В документах Международной электротехнической комиссии (МЭК) «Функциональная безопасность программируемых электронных систем: Общие аспекты» (1989 г.) и «Программное обеспечение АСУ ТП, критичных к вопросам безопасности» (1988 г.), даны следующие определения безопасности управляющих систем. **Безопасное состояние** *(Safe state)* – состояние некоторой системы, в котором при определенных допущениях и заданных условиях отсутствует угроза для жизни людей, экономики и окружающей среды. **Безопасность** *(Safety)* – свойство системы, выражающееся в ожидании того, что она при определенных условиях не перейдет в состояние, в ко-

тором угрозе подвергается человеческая жизнь, экономика и окружающая среда.

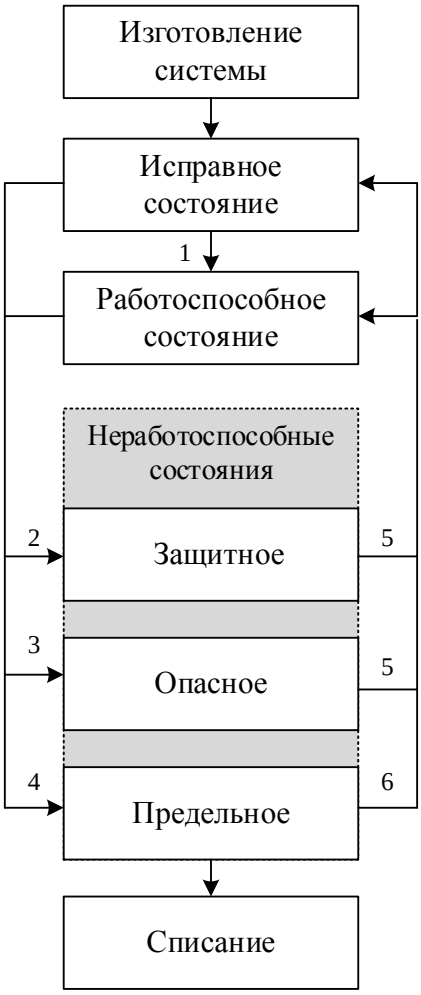

Рис. 1. Схема основных состояний и событий системы

Сравнивая между собой приведенные определения, можно сделать вывод об их эквивалентности, поскольку они основаны на едином подходе – свойство безопасности определяется через состояние системы. Конструктивность этого подхода состоит в том, что он дает способ решения основного вопроса, который возникает при анализе и синтезе безопасных систем. Для этого сформулируем понятие **критерий опасного отказа** *(Hazardous Failure Criterion)* – признак или совокупность признаков опасного состояния системы, установленные в НТД и (или) КД [9].

Итак, **внутренняя безопасность** *(internal security)* – свойство системы сохранять исправное, работоспособное и защитное состояния. В тоже время безотказность – это свойство сохранять исправное и работоспособное состояния. Поэтому в безопасной ГКС внутренняя безопасность выступает как составляющая надежности совместно с безотказностью, долговечностью, ремонтопригодностью и сохраняемостью.

Безотказность характеризуется множеством состояний

$$S_{БОТ} = S_И \cup S_р \qquad (7)$$

где $S_И$ – множество исправных состояний системы;

$S_р$ – множество работоспособных состояний системы,

а безопасность – множеством состояний

$$S_{БОП} = S_И \cup S_р \cup S_З \qquad (8)$$

где $S_З$ – множество защитных состояний.

Из сравнения множеств $S_{БОТ}$ и $S_{БОП}$ (7), (8) следует, что безопасность всегда больше безотказности. В крайнем случае, они равны, если любой отказ в системе является опасным. Таким образом, на основании выше изложенного, сформулируем вводимый нами термин отказобезопасность.

Отказобезопасность *(failure safety)* – свойство технической системы при отказе ее некоторых частей переходить в режим работы, не представляющий опасности для людей, окружающей среды или материальных ценностей.

Отказобезопасность следует отличать от отказоустойчивости – способности системы сохранять способность правильно функционировать после отказа некоторых частей системы. В реальных системах эти два требования могут выступать и совместно.

Заключение. Наиболее важным атрибутом ГКС является свойство отказоустойчивости. Отказоустойчивость является базовой платформой гарантоспособности. Без этого свойства невозможно создать систему с высоким уровнем гарантоспособности. Отказоустойчивость напрямую или косвенно влияет на такие атрибуты, как безотказность, готовность, живучесть и ФБ. Проектирование каждого компонента ГКС как отказоустойчивого привносит в систему недостатки, подробно описанные выше.

Наиболее важным атрибутом компьютерных систем критического применения является ФБ. ФБ является очень важным атрибутом для систем, связанных с безопасностью людей и окружающей среды обитания человека.

Достижение полной отказоустойчивости ГКС является очень затратным мероприятием. В большинстве случаев критического применения ГКС экономически обоснованным является замена полной отказоустойчивости на частичную отказоустойчивость, названную отказобезопасностью. Использование подхода, при котором стратегия полной отказоустойчивости заменяется стратегией отказобезопасности позволяет строить экономически эффективные ГКС с меньшими техническими затратами. Особенностью стратегии отказобезопасности является то, что она допускает наличие отказов системы, при которых ГКС переходит в защитное безопасное состояние, при этом полностью исключаются опасные отказы, при которых система переходит в состояние, чреватое катастрофическими последствиями. Таким образом, отказобезопасность представляет собой синтез отказоустойчивости и функциональной безопасности, обеспечивая при этом свойство технической системы переходить в режим работы, не представляющий опасности для людей, окружающей среды или материальных ценностей при отказе ее некоторых составных частей.

Продолжение следует.

Список литературы:

1. Johnson B. W. «Fault-Tolerant Microprocessor-Based Systems», IEEE Micro (1984), vol. 4, № 6, pp. 6-21.
2. Laprie J. C. (1985). «Dependable Computing and Fault Tolerance: Concepts and Terminology», Proceedings of 15th International Symposium on Fault-Tolerant Computing (FTSC-15), pp. 2-11
3. Von Neumann, J. (1956). «Probabilistic Logics and Synthesis of Reliable Organisms from Unreliable Components», in Automata Studies, eds. C. Shannon and J. McCarthy, Princeton University Press, pp. 43-98.
4. Avizienis A. (1976). «Fault-Tolerant Systems», IEEE Transactions on Computers, vol. 25, № 12, pp. 1304-1312.
5. Ковалев Е. Е., Иванов В. И., Пахомов Б. Я., Иванова А. А. Новая техника и проблема безопасности человека // Вопросы философии, 1981. № 5. – С. 49-59.
6. Пирик К. Система «человек-машина» в управлении транспортными процессами // Железные дороги мира, 1974. № 7. – С. 7-72.
7. Wobig K.-H, Horder A., Strelov H. Prozessrechnersysten mite Fail-Safe-Verhalten // Signal und Draht, 1974. № 11. – P. 211-218.
8. Ape1 W. Grunzuege der Metodik gewaehrlestung von sicherheitsrelevanten schaltungen der eisenbahnsicherangstechnik // Signal und Schience, 1986. Vol. 30 № 1. – P. 20-22.
9. Христов Х. А. Електронизация на осигурителната техника. – София. Техника, 1984. – 355 с.
10. Христов Х. А. Основи на осигурителната техника. – София: Техника, 1990. – 41 с.
11. Graband M., Gunther H. Sichereits philosophie und Prufung // Signal und Draht, 1988. № 9. – P. 199-204.
12. Лисенков В. М. Безопасность ответственных технологических процессов и технических средств на транспорте // Автоматика, телемеханика и связь,1992. № 1. – С. 8-11.

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 1

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 1

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.