УДК 519.711.2:681.326.7

МОДЕЛИ ОТКАЗОБЕЗОПАСНЫХ СТРУКТУР ЦИФРОВЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

д.т.н., проф. В.С. Харченко, к.т.н. В.В. Скляр, В.И. Токарев

Разработан класс моделей систем контроля и управления, которые позволяют учесть особенности многоверсионных отказобезопасных систем. Модели базируются на применении математического аппарата графов переходов и комбинаторных событийных моделей.

Постановка проблемы. Нарастание веса технической составляющей в спектре причин аварий и катастроф должно рассматриваться в контексте увеличения роли цифровых систем контроля и управления (СКУ) как объекта и средства поддержания отказобезопасности, которое объединяет свойства отказоустойчивости и безопасности и является исключительно важным свойством для СКУ комплексов критического применения.

Одно из направлений обеспечения отказобезопасности базируется на применении принципа многоверсионности, под которым подразумевается повышение надежности путем введения избыточности, когда существуют два или более способов выполнения функций системы. Многоверсионность может обеспечиваться путем использования в разных каналах системы для выполнения одной и той же функции технических средств (ТС) от разных производителей, различных алгоритмов, или программного обеспечения (ПО) от разных разработчиков и т.д. При моделировании многоверсионных СКУ следует учитывать как отказы и сбои ПО отдельных версий (относительные), так и отказы, общие для ПО нескольких версий (абсолютные или независимые – от версии). Кроме того, независимые отказы по проявлению могут быть различимыми (ошибочные результаты не совпадают между собой) и неразличимыми (ошибочные результаты совпадают между собой).

Применительно к СКУ остаются нерешенными вопросы формирования их модельной базы, в том числе построения моделей для оценки надежности многоверсионных СКУ. Проведенный анализ существующих моделей показал, что они, во-первых, позволяют учесть только отказы аппаратных и программных компонент системы и не учитывают сбои; во-вторых, существующие модели не учитывают особенностей относительных и независимых отка-

зов (и сбоев) многоверсионного ПО.

Таким образом, **целью статьи** является разработка нового класса моделей для оценки надежности СКУ, позволяющие снять указанные выше ограничения.

Анализ литературы. В монографиях [1 – 3] разработаны методы обеспечения отказоустойчивости и отказобезопасности СКУ, в том числе, и с применением многоверсионного подхода, а также методы оценки надежности таких систем. В работах [4, 5] для оценки надежности многоверсионных СКУ предложена графо-событийная модель (ГрСМ), которая состоит из двух частей: детерминированная часть включает алгоритм адаптации СКУ в случае отказов, а вероятностная часть представляет собой аналитическую модель надежности. В работе [6] построена теоретико-множественная модель дефектов многоверсионной СКУ, а также разработаны метрики диверсности для анализа многоверсионных систем. Предлагаемый в статье новый класс моделей основывается на объединении перечисленных выше ГрСМ [4, 5] и теоретико-множественной модели [6] для описания особенностей многоверсионных СКУ.

Базовая модель СКУ. Согласно ДСТУ 2860-94 «Надійність техніки. Терміни та визначення» сбоем называется самоустраняющий отказ или однократный отказ, устраняемый незначительным вмешательством оператора. Одним из свойств СКУ является циклический характер работы, когда с определенной периодичностью выполняется стандартный набор действий. Исходя из этого, по своей продолжительности сбои системы могут быть классифицированы следующим образом:

– сбои в пределах цикла, не влияющие на готовность системы;

– сбои на протяжении нескольких циклов (влияют на готовность системы);

– сбои, переходящие в отказ.

Данная систематизация позволяет построить первичную описательную модель СКУ с учетом типов сбоев, которая может служить основой для дальнейшей детализации. Модель представляется в виде графа переходов между состояниями системы (рис. 1). В восстанавливаемой системе на графе добавляется одно ребро, соответствующее восстановлению работоспособного состояния системы после отказа (из состояния S3 в S0). На рис. 1 это ребро показано пунктирной линией.

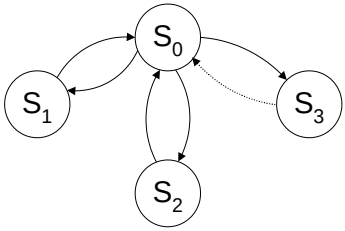
Для учета возможных событий в системе данную модель целесообразно развить в следующих направлениях:

1) учет отказов и сбоев в одноверсионных резервированных системах. Данное сечение характеризуется такими типами систем: нерезерви-

рованная, дублированная и троированная системы;

2) учет отказов и сбоев в многоверсионных системах. Данное сечение детализируется затем для трех вариантов систем: одноверсионная, двухверсионная и трехверсионная системы;

3) учет для многоверсионных систем различимых и неразличимых отказов и сбоев;



S_0 – работоспособное состояние;
S_1 – сбой, не влияющий на готовность системы;
S_2 – сбой, влияющий на готовность системы;
S_3 – сбой, переходящий в отказ.

4) учет отказов аппаратных и программных средств (ПО и ТС).

Рис. 1. Базовая модель СКУ

Авторами были получены модели для всех перечисленных выше комбинаций. В качестве примера в данной статье рассматриваются модели двухверсионной СКУ. Среди многоверсионных СКУ такие системы получили наибольшее распространение. В атомной энергетике наличие диверсности является обязательным требованием для управляющих систем безопасности АЭС (систем аварийной защиты).

Следует отметить, что модели СКУ могут иметь различный вид. Состояния системы и возможные переходы между ними удобно отображать графами переходов, для упрощения которых может быть применен метод укрупнения фазовых состояний. Для учета отказов ТС и ПО в многоверсионных системах применяется ГрСМ. Для многоверсионных систем, кроме того, весьма наглядными являются множественные модели, представленные в виде диаграмм Вейча.

Теоретико-множественная модель двухверсионной СКУ представлена на рис. 2. Для количественных значений мощностей множеств отказов и сбоев данной СКУ справедливы следующие зависимости:

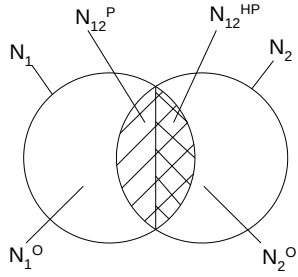
$$N_{12} = N_{12}^{P} + N_{12}^{HP};$$

$$N_1 = N_1^{O} + N_{12} = N_1^{O} + N_{12}^{P} + N_{12}^{HP};$$

$$N_2 = N_2^{O} + N_{12} = N_2^{O} N_{12}^{P} + N_{12}^{HP}.$$

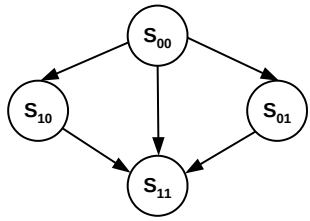
Графовые модели двухверсионной СКУ. Построим граф переходов между состояниями двухверсионной системы без учета различимости и неразличимости отказов (рис. 3). Подчеркнем тот факт, что вероятность

отказов первой P1 и второй P2 версии в общем случае разная. Обозначим состояния версий двухпозиционным кодом, в котором символ «0» обозначает ее исправное состояние, а «1» – отказ.



N_1 – отказы и сбои первой версии ПО;
N_1^{O} – относительные отказы и сбои первой версии ПО;
N_2 – отказы и сбои второй версии ПО;
N_2^{O} – относительные отказы и сбои второй версии ПО;
N_{12} – независимые отказы и сбои двух версий ПО;
N_{12}^{P} – различимые независимые отказы и сбои двух версий ПО;
N_{12}^{HP} – различимые независимые отказы и сбои двух версий ПО.

Рис. 2. Теоретико-множественная модель двухверсионной СКУ



S_{00} – работоспособное состояние обоих версий;
S_{10} – отказ первой версии;
S_{01} – отказ второй версии;
S_{11} – отказ обоих версий (отказ системы).

Рис. 3. Общий вид графа переходов для двухверсионной системы

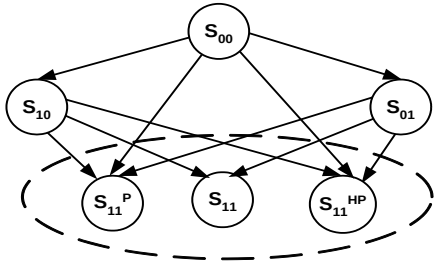
Следует отметить, что состояние S_{11} может наступить как в результате поочередного отказа версий вследствие двух последовательных относительных отказов, так и в результате одного независимого отказа.

Уточним граф переходов с учетом различимых и неразличимых независимых дефектов (рис. 4). В итоге состояние S_{11} (рис. 3) расщепится на три состояния, т.к. отказ двух версий может произойти в случае одного из трех событий: два последовательных относительных отказа, различимый независимый отказ, неразличимый независимый отказ. Если на рис. 4 объединить 3 вершины графа, соответствующие отказу системы, то получим граф, аналогичный графу на рис. 3.

Уточним общий граф переходов двухверсионной системы (рис. 3) с учетом типов сбоев, предложенных в базовой модели (рис. 1). Такая модель будет иметь вид, представленный на рис. 5. Двухпозиционный код для обозначения состояний модифицирован в соответствии с типами событий в системе, как на рис. 5.

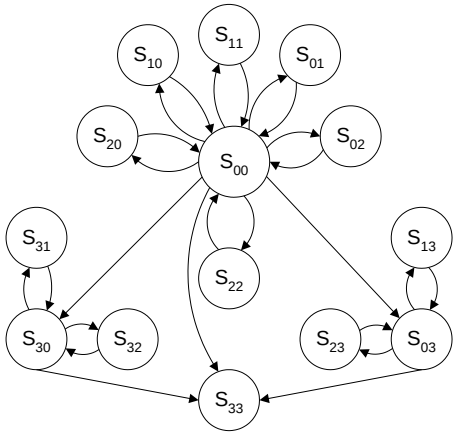
Выводы. В результате исследований получен новый класс графовых

моделей для многоверсионных систем контроля и управления. Данные модели позволяют описывать расширенный класс отказов и сбоев резервированных каналов технических средств, версий многоверсионного ПО



S_{00} – работоспособное состояние обоих версий;
S_{10} – отказ первой версии;
S_{10} – отказ второй версии;
S_{11} – два относительных отказа двух версий (отказ системы);
S_{11}^{P} – различимый независимый отказ двух версий (отказ системы);
S_{11}^{HP} – неразличимый независимый отказ двух версий (отказ системы).

Рис. 4. Граф переходов двухверсионной системы с учетом различимых и неразличимых независимых отказов



S_{00} – работоспособное состояние обоих версий;
S_{10} – относительный сбой первой версии, не влияющий на готовность;
S_{01} – относительный сбой второй версии, не влияющий на готовность;
S_{20} – относительный сбой первой версии, влияющий на готовность;
S_{02} – относительный сбой второй версии, влияющий на готовность;
S_{30} – относительный сбой первой версии, переходящий в отказ;
S_{03} – относительный сбой второй версии, переходящий в отказ;
S_{31} – сбой второй версии, не влияющий на готовность, при отказе первой версии;
S_{32} – сбой второй версии, влияющий на готовность, при отказе первой версии;
S_{13} – сбой первой версии, не влияющий на готовность, при отказе второй версии;
S_{23} – сбой первой версии, влияющий на готовность, при отказе второй версии;
S_{11} – независимый сбой двух версий, не влияющий на готовность;
S_{22} – независимый сбой двух версий, влияющий на готовность;
S_{33} – отказ двух версий (отказ системы).

Рис. 5. Граф переходов двухверсионной системы с учетом типов сбоев

с учетом их различимости; сбои технических средств и программного

обеспечения с учетом их влияния на готовность системы. Эти модели проиллюстрированы для двухверсионных систем. Для учета всех перечисленных факторов графовую часть модели необходимо дополнять событийной схемой, позволяющей дифференцировать состояния, соответствующие вершинам графа переходов. При известных интенсивностях переходов возможно получение аналитических зависимостей для показателей надежности и безопасности систем контроля и управления.

ЛИТЕРАТУРА

1. *Kersken M., Saglietti F. Software fault tolerance. Achievement and assessment strategies. Garchimg: GRS mbH, Research Reports ESPRIT, Project 300, Request, vol. 1, 1992.*
2. *Laprie J.-C. Dependability Handbook. Laboratory for Dependability Engineery, LAAS Report n 98-346, 1998.*
3. *Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х.: ХВУ, 1996. – 506 с.*
4. *Харченко В.С., Скляр В.В. Графово-событийная модель для оценки надежности и последовательность выбора архитектур адаптивных многоверсионных систем // Інформаційно-керуючі системи на залізничному транспорті. – 2000. – № 4. – С. 64 – 67.*
5. *Скляр В.В., Харченко В.С. Отказоустойчивые компьютерные системы управления с версионно-пороговой адаптацией: Способы адаптации, оценка надежности, выбор архитектур // Автоматика и телемеханика. – 2002. – № 6. – С. 131 – 145.*
6. *Харченко В.С., Пискачева И.В., Скляр В.В. Метрики диверсности: Классификация, анализ и применение для оценки надежности и безопасности компьютерных систем управления // Открытые информационные компьютерные интегрирующие технологии. – Х.: НАКУ «ХАИ». – 2001. – Вып. 9. – С. 194 – 214.*

Поступила 10.06.2003

***ХАРЧЕНКО Вячеслав Сергеевич**, доктор техн. наук, профессор, заведующий кафедрой компьютерных систем и сетей НАКУ им. Н.Е. Жуковского "ХАИ". Область научных интересов – надежность, живучесть и безопасность компьютерных систем управления критического применения, технологии их проектирования, моделирования и экспертизы.*

***СКЛЯР Владимир Владимирович**, канд. техн. наук, старший научный сотрудник Государственного научно-технического центра ядерной и радиационной безопасности. В 1992 году окончил ХВВКИУ РВ. Область научных интересов – методы оценки и обеспечения отказоустойчивости аппаратных и программных средств компьютерных систем управления.*

***ТОКАРЕВ Виктор Иванович**, генеральный конструктор по АСУ ТП ЗАО «Радий». В 1979 году окончил Одесский политехнический институт. Область научных интересов – методы, средства оценки и обеспечения надежности и безопасности информационно-управляющих систем АЭС.*