УДК 681.321

ОЦЕНКА НАДЕЖНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ОСНОВЕ ИЕРАРХИЧЕСКИХ FME(C)A-ТАБЛИЦ И МАРКОВСКИХ ЦЕПЕЙ: МОДЕЛИ, МЕТОДИКА И ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

В.С. ХАРЧЕНКО
ИРАДЖ ЭЛЬЯСИ КОМАРИ
А.В.ГОРБЕНКО

Национальный аэрокосмический университет имени Н.Е. Жуковского (ХАИ), Харьков

e-mail: V.Kharchenko@khai.edu

Предложена методика анализа надежности информационно-управляющей системы (ИУС) высокой готовности с использованием аппарата иерархических FME(C)A–таблиц и марковских случайных процессов с дискретными состояниями и непрерывным временем. Проанализированы особенности получения моделей надежности в зависимости от типов отказов, ресурсов и стратегий восстановления с использованием принципа многофрагментности. Приведены примеры моделей готовности ИУС. Разработаны элементы информационной технологии анализа надежности ИУС на основе предложенной методики. Описано инструментальное средство для проведения анализа надежности и снижения критичности элементов ИУС.

Ключевые слова: ИУС высокой готовности, надежность, марковская модель, FME(C)A, многофрагментность.

Проблема оценки надежности информационно-управляющих систем.

Информационно-управляющие системы (ИУС) являются важной, с точки зрения обеспечения надежности и безопасности, частью сложных технических комплексов. В данной работе рассматриваются так называемые ИУС высокой готовности [5,7], используемые для управления объектами с непрерывным и длительным временем функционирования. Кроме того, такие ИУС:

- являются распределенными многокомпонентными системами, для которых сложно сформулировать понятие отказа; они могут быть отнесены к системам с многоуровневой работоспособностью;
- содержат большой набор штатных средств контроля, диагностирования и восстановления работоспособности, которые функционируют автоматически или под управлением администратора;
- подвергаются различным случайным физическим и/или ифнормационным воздействиям, которые могут вызывать кратковременную или длительную потерю работоспособности вследствие отказов (сбоев) программных, аппаратных или сетевых средств.

Ввиду указанных причин весьма сложной является оценка надежности ИУС высокой готовности, в которых значение стационарного коэффициента готовности составляет 0,999-0,9999 [7].

Анализ литературы. Постановка задачи. Для анализа надежности КС используются различные процедуры, в том числе, основанные на FME(C)A (Failure Modes and Effects (Critical) Analysis)-методиках [8,3]. В работе [6] этот метод обобщен на случай web-сервисов, учитывает информационные воздействия на систему и поэтому получил название F(I)MEA-процедур (Failure and Intrusion Modes and Effects Analysis).

Обычно, такие FME(C)A-методики позволяют проанализировать виды и последствия первых (одиночных) отказов. В то же время для критических ИУС, важно оценить их надежность с учетом возможных кратных отказов и последовательностей одиночных и/или кратных отказов. Для этого могут использоваться иерархии FME(C)A-таблиц [3]. Однако, в конечном итоге, необходима модель, которая позволит получить количественные оценки надежности (готовности) системы.

Цель статьи – разработка метода и элементов информационной технологии анализа надежности ИУС, основанного на использовании множества FME(C)A – таблиц, и получении марковской модели готовности. В соответствии с этим в статье решаются следующие задачи:

- предлагается общая последовательность анализа надежности КС с использованием FME(C)A – таблиц, образующих иерархию. Эта иерархия учитывает различные варианты последовательностей одиночных и кратных отказов;
- разрабатывается марковская модель КС, в которой отказы (сбои) компонент группируются с учетом их последствий и возможностей восстановления;
- описываются элементы информационной технологии анализа надежности ИУС.

Последовательность анализа наджности ИУС с использованием FME(C)A–таблиц

1. Формируется модель отказов ИУС, представляющая собой последовательности Пi одиночных или кратных отказов Фif их компонент, МП={Пi}$_{i=1}^{n}$, Пi=<Фij>$^{mi}_{j=1}$.

2. Для отказов компонент Фi1 строится первая FME(C)A-таблица (Fi1- таблица) в соответствии с методикой, приведенной в [2].

3. Множество отказов МФ1, рассмотренных в таблице Fi1, декомпозируется на подмножества $МФ_1^1$, $МФ_1^2$, $МФ_1^3$, исходя из возможностей устранения последствий этих отказов штатными (автоматическими) средствами ($МФ_1^1$), системным администратором автоматизированными средствами ($МФ_1^2$), и путем ремонта с использованием обслуживающего персонала ($МФ_{з_1}$).

Если необходимо оценить надежность ИУС при одиночных отказах, то в соответствии с результатами анализа разрабатывается и исследуется марковская модель готовности, в противном случае (для последовательности одиночных или кратных отказов) – переход к пункту 4.

4. Разрабатывается множество таблиц Fi2, Fi3,...,Fimi для последовательностей отказов, начиная с Фi2 и заканчивая Фimi. Для каждой из таблиц проводится анализ отказов в соответствии с п.3. Таким образом, последовательностям Пi∈МП могут быть поставлены в соответствие иерархии F-таблиц и соответствующих марковских моделей.

Возможность использования аппарата марковских процессов в рассматриваемой ситуации объясняется тем, что принимается допущение о простейших потоках отказов и восстановлений компонент ИУС, которое справедливо для отказов по «естественным» причинам. Если исследуется поведение ИУС в условиях воздействий, приводящих к кратным отказам, использование марковских моделей возможно, если простейшим является поток событий, связанных с отказами заданной кратности. Уменьшение размерности моделей достигается путем применения принципа многофрагментности [5] или за счет группирования отказов с использованием матриц критичности.

Разработка марковской модели ИУС на основе FME(C)A-таблицы

На первом этапе необходимо определить множество состояний, в которых оказывается КС в зависимости от типов отказов (сбоев). Для получения первой группы таких состояний следует воспользоваться результатами анализа FME(C)A-таблицы Fi1 и полученными множествами $МФ_1^1$, $МФ_1^2$, $МФ_1^3$, каждое из которых делится на два подмножества в зависимости от того, каким образом осуществляется восстановление: без использования резервного ресурса или с использованием резерва, автоматически или путем замены отказавшего компонента.

Тогда подмножество состояний, определяющих первую группу событий, включает следующие состояния:

S0 – исходное состояние, когда система полностью работоспособна;

S11, S12 – состояния из множества $МФ_1^1$ без использования резервного ресурса или с использованием резерва соответственно;

S21, S22 – состояния из множества $МФ_1^2$ без использования резервного ресурса или с использованием резерва соответственно;

S31, S32 – состояния из множества $МФ_1^3$ без использования резервного ресурса или с использованием резерва соответственно;

S4 – S6 – состояния, в которые переходит система после использования резерва из состояний S12, S22 , S32 соответственно.

Следует подчеркнуть, что в первой группе могут быть учтены также состояния, связанные с ошибками контроля. Если предположить, что отказы (сбои) из множеств $МФ^{i'}$, j = {1,2,3}, обнаруживаются с вероятностью Dj, то должны быть введены состояния Sj3, в которые осуществляется переходы с вероятностью 1- Dj.

Переходы из состояния S0 в состояния Sjk, i = {1,2}, осуществляются с интенсивностями DjLjk, а в состояния Sj3 – с интенсивностью (1-Dj)Ljk. Далее из состояний Sj2 осуществляются переходы в состояния S4 – S6 с интенсивностями L4 – L6.

Из состояний Sj3 возможны переходы в состояния Sjk, k = {1,2}, с интенсивностями DjLjk. Из состояний Sj1 переход в состояние S0 (восстановление работоспособности) происходит с интенсивностями Mj1.

Размеченный марковский граф, являющийся частью модели для состояний первой группы (назовем его базовым фрагментом и будем обозначать B(S0) в соответствии с начальной вершиной фрагмента), представлен на рис.1. Дальнейшая разработка модели зависит от особенностей построения и стратегий восстановления ИУС. Проиллюстрируем некоторые из возможных вариантов.

Вариант 1. Ресурс (порядок) восстановления по всем типам отказов (переходы с интенсивностями L4 – L6) является общим.

Восстановление ИУС (с остановом функционирования) осуществляется после исчерпания этого ресурса. Тогда граф состояний будет представлять собой цепочку базовых фрагментов с замыканием на начальную вершину следующего фрагмента.

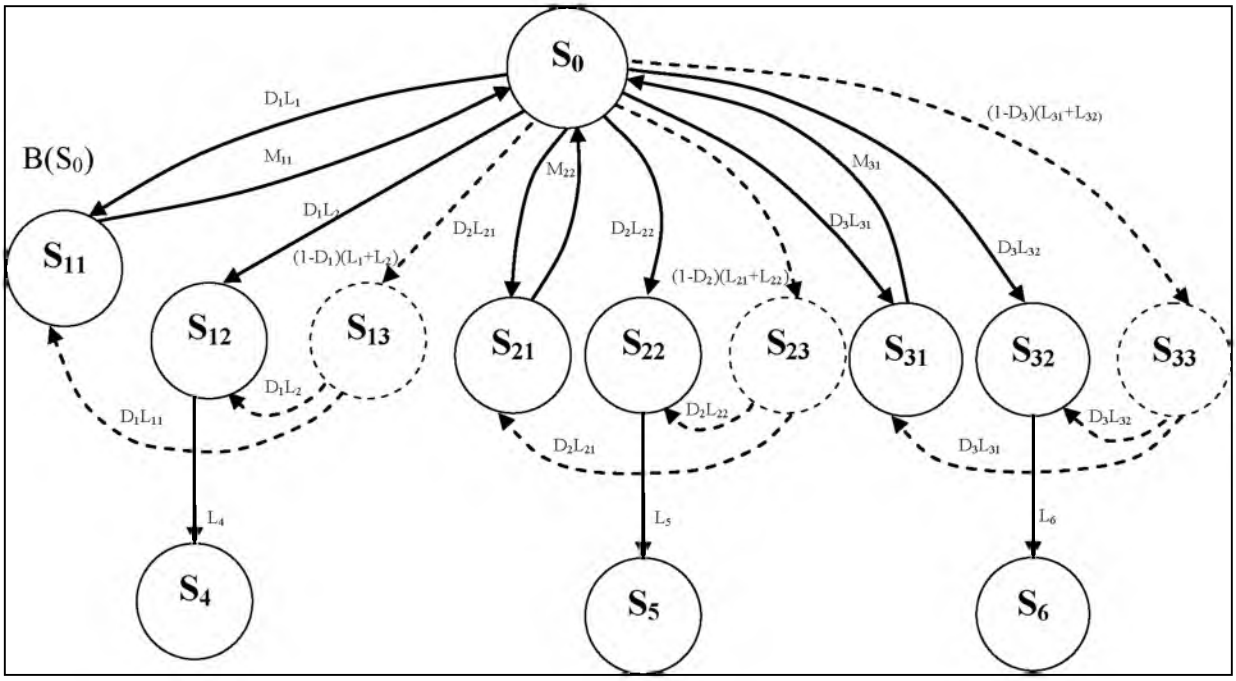


Рис. 1. Базовые фрагменты B (So) марковского графа ИУС

Пример двухфрагментной модели приведен на рис.2, где пунктирами показаны разные варианты восстановления работоспособности (полное и частичное). Состояние,

при котором начинается процесс восстановления (состояние полного отказа), обозначено как Sr. Если принимается стратегия частичного восстановления работоспособности, то тогда, очевидно, должен предусматриваться специальный режим профилактики (состояния Sp1 и Sp2 показаны пунктиром).

Вариант 2. Ресурс (порядок) восстановления по всем типам отказов (переходы с интенсивностями L4 – L6) является раздельным.

Восстановление ИУС (с остановом функционирования) осуществляется после исчерпания ресурса по каждому из множеств $МФ_{v}^{j}$, v = {2,3,...}, в соответствии с последовательностями Пi∈МП. Тогда граф состояний будет представлять собой иерархию базовых фрагментов с разными вариантами восстановления после исчерпания резерва.

Пример марковской модели с двухуровневой иерархией приведен на рис.3, на которой переход в состояние полного отказа Sr осуществляется из фрагментов B(S4 – S6), а восстановление возможно либо поэтапно через эти фрагменты, либо непосредственно в состояние S0. При этом состояния профилактики для стратегии частичного восстановления (как это предусмотрено вариантом 1), для простоты изображения модели, не показаны.

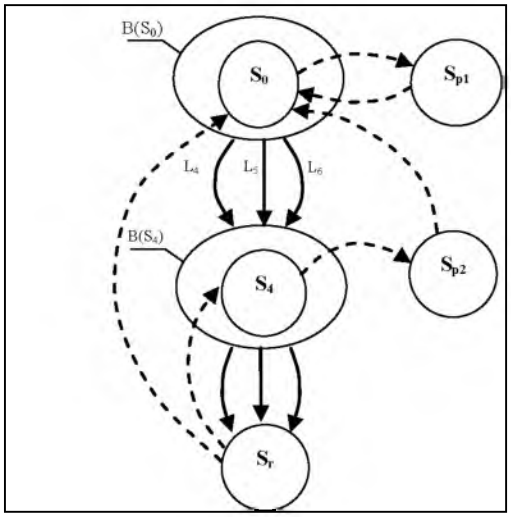


Рис. 2. Многофрагментная марковская модель (вариант 1)

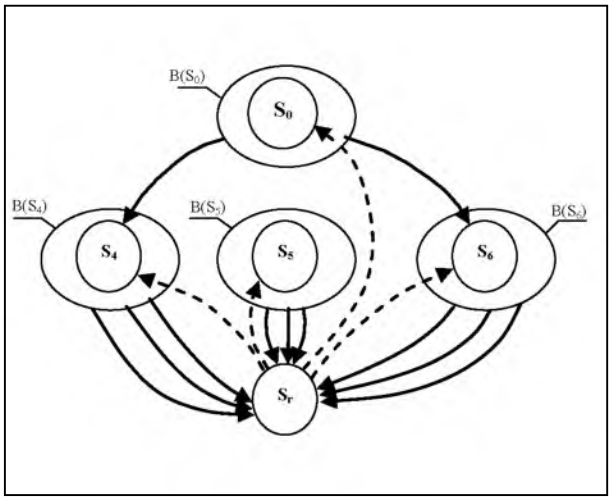


Рис. 3. Многофрагментная марковская модель (вариант 2)

Вариант 3. Данный вариант отличается от предыдущего тем, что после ресурс восстановления группируется по множествам $МФ_{1}^{j}$, j = {1,2,3}, на каждом уровне модели.

Часть графа состояний для этого случая показана на рис. 4. Переходы, описывающие процесс восстановления, здесь не показаны.

Число вариантов моделей может быть весьма велико. Выше были рассмотрены признаки, в соответствии с которыми они могут разрабатываться. Для проведения м оделирования с целью получения показателей готовности и выбора стратегий восстановления КС должно быть отобрано множество конкурентоспособных вариантов.

Определение параметров модели (интенсивностей переходов) проводится с учетом того, что интенсивности L11 (L12), L21 (L22), L31 (L32) могут отличаться на порядок. Тоже можно сказать и об интенсивностях M11, M21, M31.

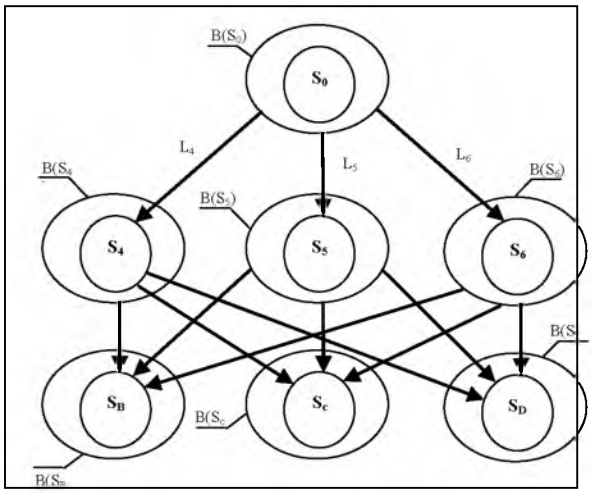


Рис. 4. Фрагмент модели (вариант 3)

Структура информационной технологии оценки ИУС

Полученные модели и методика анализа ИУС позволяют перейти к разработке информационной технологии, под которой понимается совокупность программно-технических средств преобразования информации [1]. Элементы этой технологии структурированы в таблице 1 по схеме:

- операции по преобразованию информации на основе теоретических положений;
- исходные данные и результаты каждого из этапов анализа, оценки и принятия решений;
- используемые инструментальные средства.

Данная технология включает следующие этапы.

1. Проводится анализ технической документации ИУС и выполняется ее представление в виде совокупности иерархий структур, степень детализации которых определяется поставленной задачей.

Исходные данные: архитектура ИУС, аппаратные, программные и сетевые компоненты. Результат: структурные графы GSi на разных уровнях ИУС, i = 1,...n.

2. Формируется множество таблиц видов и последствий отказов (FMECA-таблиц) по уровням ИУС и производится их частичное заполнение с учетом базы данных по блокам (компонентам платформы и/или COTS-компонент).

Исходные данные: структурные графы GSi, типовые FMECA-таблицы компонент FTC j (j = 1,...,z). Результат: иерархия частично заполненных FMECA-таблиц FTЧi.

3. Оценивается тяжесть («сверху-вниз»), вероятность («снизу-вверх»), и длительность устранения («снизу-вверх») отказов компонент на всех уровнях ИУС.

При этом множество анализируемых компонент делится на три группы с точки зрения способов восстановления (автоматический (А), автоматизированный (О), ручной (Р)); затем строятся матрицы критичности.

Исходные данные: Исходные FMECA-таблицы FTH, ТЗ и структурные схемы ИУС, диагональ (сечение) критичности DC. Результат: Заполненные FMECA-таблицы FTЗi, подмножества компонент EA,EO,EP, двух- или трехмерные матрицы критичности MCHi.

4. Определяются возможные средства снижения критичности отказов по каждой из строк таблиц и их характеристики. Уточняется постановка оптимизационной задачи по критериям «критичность-затраты».

Исходные данные: база данных средств обеспечения отказоустойчивости MFi j и их характеристики. Результат: значения затрат и снижения критичности MFi j

5. Решается задача выбора оптимального множества средств обеспечения отказоустойчивости (повышения готовности) по заданному критерию. Выполняется доработка (реинжиниринг) существующей системы или корректируется проект разрабатываемой ИУС.

Исходные данные: результаты решения задачи выбора средств снижения критичности. Результат: итоговый отчет (FMECA-таблицы FTKi, включая преобразованные матрицы критичности MCЗi).

6. При необходимости количественной оценки показателей готовности ИУС осуществляется разработка марковских моделей для разных стратегий восстановления и обслуживания (СВО) и выполняется их исследование.

Исходные данные: структурные графы GSi, FMECA-таблицы FTKi, база данных стратегий SRr. Результат: модели, зависимости готовности от входных параметров.

7. Выбирается СВО по критерию готовности, уточняются параметры компонент системы (потоков отказов и восстановлений, достоверности контроля, периодичности и объема профилактического обслуживания).

Исходные данные: требования к системе, результаты исследования марковских моделей. Результат: стратегия восстановления и обслуживания (параметры и последовательность).

Используемые методы и инструментальные средства даны в таблице 1. IDEFo-диаграмма технологии реализована в инструментальной среде BPWin (рис. 5).

Функции инструментального средства

Для программной поддержки процессов анализа и снижения критичности отказов ИУС разработано клиент-серверное инструментальное средство (ИС) «H-FMECA+», которое реализуют графический интерфейс с пользователем, обеспечивающий ввод исходных данный, параметров для расчета и отображение получаемых результатов. Инструментальное средство «H-FMECA+», базирующееся на предложенной методике, имеет два режима работы: режим оценивания и режим выбора профиля средств.

Функциями ИС «H-FMECA+» в режиме оценивания являются:

1) задание пользователем структуры оцениваемой ИУС, специфицирование подсистем, элементов и компонентов;

2) ввод пользователем иерархии H-FMEA-таблиц в соответствии с проведенным анализом видов, причин и последствий отказов подсистем, элементов и компонентов;

3) задание критичности отказов подсистем, элементов и компонентов:

3.1) задание пользователем количества показателей для интегральной оценки критичности, выбор шкалы оценивания;

3.2) ввод пользователем критичности отказов с использованием качественной шкалы оценивания.

3.3) количественная оценка критичности отказов;

4) построение матрицы (списка) критичности, задания диагонали критичности и выявление дефицитов безопасности.

В режиме выбора профиля средств снижения критичности ИС «H-FMECA+» поддерживает:

1) задание пользователем номенклатуры средств обеспечения отказоустойчивости (снижения вероятности возникновения отказа), восстановления и снижения тяжести последствий отказов;

2) экспертную оценку стоимости и эффективности средств снижения критичности отказов;

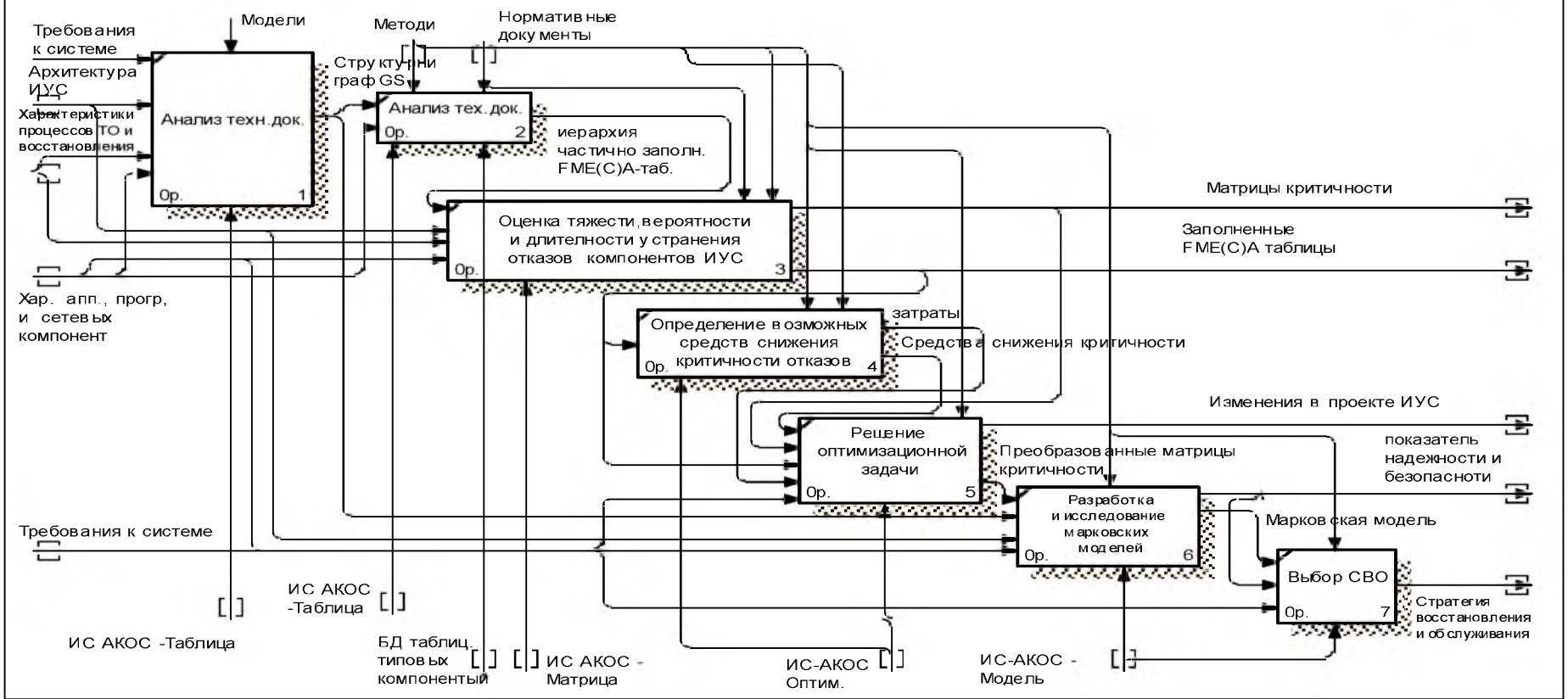
Таблица 1

Последовательность реализации информационной технологии

Операции	Исходные данные	Получаемый результат	Средства ИТ	
			Модели, методы	Инструментальные средства
1. Проводится анализ технической документации ИУС и выполняется е представление в виде совокупности иерархий структур, степень детализации которых определяется поставленной задачей.	Архитектура ИУС, аппаратные, программные и сетевые компоненты	Структурные графы GS_i на разных уровнях иерархии ($i = 1,\ldots n$)	Метод оценки критичности отказов ИУС с использованием FMEA-таблиц (НР №1)	ИС-АКОС-ГРАФ
2. Формируется множество таблиц видов и последствий отказов (FMECA-таблиц) по уровням ИУС и производится их частичное заполнение с учетом базы данных по блокам (компонентам платформы и/или COTS-компонент).	Структурные графы GS_i, типовые FMECA-таблицы компонент $FT_C{}^J$ ($j = 1,\ldots,z$)	Иерархия частично заполненных FMECA-таблиц FT_{Ui}		ИС-АКОС-ТАБЛИЦА (БД)
3. Оценивается тяжесть («сверху-вниз»), вероятность («снизу-вверх»), и длительность устранения («снизу-вверх») отказов компонент на всех уровнях ИУС. Множество анализируемых компонент делится на три группы с точки зрения способов восстановления (автоматический (А), автоматизированный (О), ручной (Р)). Строятся матрицы критичности.	Исходные FMECA-таблицы FT_H, ТЗ и структурные схемы ИУС, диагональ (сечение) критичности DC	Заполненные FMECA - таблицы FT_{3i}, подмножества компонент E_A, E_O, E_P, двух- или трехмерные матрицы критичности MC_{Hi}		ИС-АКОС-МАТРИЦА
4. Определяются возможные средства снижения критичности отказов по каждой из строк таблиц и их характеристики. Уточняется постановка оптимизационной задачи по критериям «критичность-затраты».	База данных средств обеспечения отказоустойчивости $MF_i{}^J$ и их характеристики	Значения характеристики затрат и снижения критичности по средствам $MF_i{}^J$	Метод повышения надежности и безопасности ИУС с использованием многомерных матриц критичности (НР №2)	ИС-АКОС-ОПТИМ
5. Решается задача выбора оптимального множества средств обеспечения отказоустойчивости (повышения готовности) по заданному критерию. Выполняется доработка (реинжиниринг) существующей системы корректируется проект разрабатываемой ИУС.	Результаты решения задачи выбора средств снижения критичности	Итоговый отчет (FMECA-таблицы FT_{Ki}, включая преобразованные матрицы критичности MC_{3i})		ИС-АКОС-ОПТИМ, ИС-АКОС-ПРОЕКТ
6. При необходимости количественной оценки показателей готовности ИУС осуществляется разработка марковских моделей для разных стратегий восстановления и обслуживания (СВО) и их исследование.	Структурные графы GS_i, FMECA-таблицы FT_{Ki}, база данных стратегий SR_r	Марковские модели, зависимости готовности от входных параметров	Многофрагментные марковские модели готовности компьютерных сетей ИУС (НР №3)	ИС-АКОС-МОДЕЛЬ
7. Выбирается СВО по критерию готовности, уточняются параметры компонент системы (потоков отказов и восстановлений, достоверности контроля, периодичности и объема профилактического обслуживания).	Требования к системе, результаты исследования марковских моделей	Стратегия восстановления и обслуживания (параметры и последовательность)		

Серия История. Политология. Экономика. Информатика.
2011. № 19 (114). Выпуск 20/1

USED AT:	AUTHOR: Эльяси	DATE: 15.12.2008	WORKING	READER DATE	CONTEXT:
	PROJECT: информационной технологии	REV: 17.12.2008	DRAFT		
			RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION		A-0



NODE:	TITLE:	NUMBER:
A0	разработка информационной технологии	

3) задание системных ограничений на общую стоимость средств снижения критичности отказов и требуемый уровень критичности;

4) автоматическое решение задачи выбора средств снижения поиск и выбор одного или нескольких профилей разрабатываемой сети минимальной стоимости, отвечающих предъявляемым требованиям.

Архитектура инструментального средства «H-FMECA+» приведена на рис. 6. Инструментальное средство «H-FMECA+» написано с использованием технологии ASP.NET 2.0 и реализует подход к созданию сервис-ориентированных систем Microsoft .NET. Серверная часть, включающая три программных модуля, работает под управлением Microsoft Internet Information Service и взаимодействует с базами данных под управлением СУБД Microsoft SQL Server 2005. Для хранения структуры оцениваемой ИУС, иерархии FMEA-таблиц и методов снижения критичности отказов используется три отдельные базы данных.

Рис. 6. Архитектура серверной части ИС «H-FMECA+»

Заключение

На базе рассмотренного метода анализа разработана система поддержки принятия решений при восстановлении работоспособности ИУС. В ее состав входит база данных фиксированных или динамически обновляемых F–таблиц, программные средства, поддерживающие получение и анализ матриц критичности моделей готовности.

Для оценки количественных значений показателей надежности следует воспользоваться марковскими моделями, методика разработки которых предложена в данной статье. Данная технология апробирована при оценке надежности ИУС для управления нефтегазовыми коммуникациями.

Рецензент: д-р техн. наук, проф. В.А.Краснобаев, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.

Литература

1. Информатика / под ред. Н. В. Макаровой. – М.: Финансы и статистика, 1998. – 768 с.
2. Ирадж Эльяси Комари. Анализ задач разработки и реинжиниринга компьютерных сетей для критических приложений / Ирадж Эльяси Комари, Горбенко А.В. //Радіоелектронні і комп'ютерні системи. 2006.-№ 7(19). – С.32-35.
3. Ирадж Эльяси Комари. Метод анализа надежности компьютерных сетей сервисов с использованием FME(C)A–иерархий / Ирадж Эльяси Комари. Праці МНТК "Інтегровані комп'ютерні технології в машинобудуванні". – Харків: Національний аерокосмічний університет "ХАІ", 2006. – С. 275-276.
4. Мениске Д. Производительность web-служб. Анализ, оценка и планирование / Мениске Д., Алмейда В.. – С.-Пб.: ДиаСофтЮП, 2003.-408с.
5. Харченко В.С. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов / Харченко В.С., Одарущенко О.Н., Одарущенко Е.Б. // Радіоелектронні і комп'ютерні системи. 2006. – № 5(17). – С.62-67.
6. Gorbenko A. F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring / Gorbenko A., Kharchenko V., Tarasyuk O., Furmanov A. LNCS4157. Development of Complex Fault-Tolerant Systems. Butler M., Jones C., Romanovsky A., Trubitsyna E. (eds.). Springer, 2006. -P.153–168.
7. High availability: design, techniques, and processes/Floyd Piedad, Michael Hawkins (eds) Prentice Hall, NJ, USA, 2001. – 205 p.
8. Kharchenko V. FME(C)A Technique of Assessment and Ensuring of a Corporate Computer Network Fault-Tolerance and Safety / Kharchenko V., Gorbenko A. // 6th Probabilistic Safety Assessment and Management Conference, Puerto Rico, 2002.

INSTRUMENTATION AND CONTROL SYSTEMS DEPENDABILITY ASSESSMENT USING HIERARCHICAL FME(C)A-TADLES AND MARKOV'S CHAINS: MODELS, TECHNIQUE AND INFORMATION TECHNOLOGY

V.S. KHARCHENKO
IRAJ ELYASI KOMARI
A..V. GORRENKO

National Aerospace University "KhAI", Kharkiv

e-mail: V.Kharchenko@khai.edu

The dependability analysis technique of high availability instrumentation and control systems (I&Cs) by use hierarchical FME(C)A-tables and Markov's chains with discreet states and continuous transmissions is offered. Features of dependability models development depending on failure modes, resources and strategies of recovery using the multi-fragmentation principle are analysed. The examples of I&Cs availability analysis are described. Elements of information technology for I&C dependability analysis based on the proposed technique are developed. The tool for I&C dependability analysis and decreasing of failures criticality is described.

Key words: high availability I&C systems, dependability, Markov's model, FME(C)A, multi-fragmentation.