УДК 681.3+004.73.052

В.С. Харченко, В.О. Бутенко

*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков*

# ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОЦЕНИВАНИЯ ГОТОВНОСТИ ИФНОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МАРКОВСКИХ МОДЕЛЕЙ НА ОСНОВЕ ВЫБОРА ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ

*В статье представлена структура информационной технологии оценивания надежности информационно-управляющих систем важных для безопасности, описывающая внедрение этапа метрического оценивания марковской модели исследуемой системы в целях выбора эффективного метода ее решения, а также инструментального средства.*

***Ключевые слова:*** *информационная технология, метрическое оценивание, марковская модель, программное средство, информационно-управляющие системы*

## Вступление

Оценка надежности (готовности) информационно-управляющих систем (ИУС) важных для безопасности является обязательным этапом процесса их разработки и сертификации, в связи с повышенными требованиями к показателям надежности функционирования данных систем. Повышение требований связано с областью применения ИУС, так например ИУС использующиеся на АЭС выполняют функции получения, обработки, хранения, передачи, отображения, регистрации данных о состоянии и функционировании систем, элементов конструкций контролируемого объекта, а также такие управленческие функции как инициация срабатывания технологических систем при нарушении заданных проектных

пределов или условий эксплуатации [1]. К надежности ИУС выдвигаются требования, условно представленные в виде так называемых «уровней готовности» (табл. 1) [2].

Таблица 1

Требования к надежности систем, важных для безопасности

| № п/п | Значения $K_г$ | $T_{простоев}$ 1/год | Характеристика |
|---|---|---|---|
| 1 | 0,9999 | 52 мин. 33 с | Устойчивая к отказам (Fault-tolerant) |
| 2 | 0,99999 | 5 мин. 15 с. | С высокой готовность (High-availability) |
| 3 | 0,999999 | 31,54 с | С очень высокой готовностью (Very high-availability) |
| 4 | 0,9999999 | 3,15 с | С ультравысокой готовностью (Ultra-availability) |

Для оценки показателей надежности (готовности) ИУС широко применяются методы математического моделирования, которые могут быть разделены на три категории: аналитические методы, имитационные и гибридные [3]. В свою очередь, аналитические методы делятся на пространственные (Марковские цепи, PTN, SAN [9] и т.д.) и комбинаторные (FTA, RBD [9] и т.д.) Одним из наиболее распространённых подходов аналитического моделирования является аппарат марковского анализа, позволяющий гибко отображать такие свойства моделируемых систем как зависимости отказов и восстановлений, функции горячей замены, общий ресурс восстановления и т.д. [4].

В процессе использования аппарата марковского анализа исследователь может столкнуться с рядом таких вычислительных сложностей как ростом пространства состояний, разреженностью матрицы интенсивностей переходов между состояниями Марковской модели (ММ), жесткостью и разложимостью ММ [5]. Общее множество подходов к исследованию ММ и последующему решению системы дифференциальный уравнений Колмогорова-Чепмена может быть разделено на две группы: прямые (ПР) техники и техники преобразования моделей (НПР) [6, 7]. Однако необходимо отметить, что методы решения ММ, относящиеся к указанным техникам, покрывают каждую из указанных вычислительных сложностей в отдельности, но не всегда рассматривают возможное присутствие двух и больше сложностей одновременно.

За последние 30 лет было разработано множество программных средств (ПС) реализующих каждую из перечисленных техник, которое может быть разделено на три группы: специализированные ПС (λPredict, Möbius, SHARP), коммерческие математические пакеты (Maple, Matlab, Mathematica) и ПС частной разработки (MSMC, ExpMeth, ASNA, MARCA), т.е. утилиты разработанные пользователями для решения ряда узкоспециализированных задач и которые прошли проверку на множестве ранее проведенных исследований [7]. Такое разнообразие ПС является чрезвычайно полезным в процессе моделирования системы, однако может привести к значительным сложностям при выборе наиболее применимого для решения конкретной задачи с точки зрения точности и удобства использования.

Увеличение сложности ИУС приводит к трудностям выбора и применения инструментария (техник, подходов, методов и средств компьютерного моделирования), позволяющего с требуемым уровнем точности вычислять показатели надежности (готовности). Учитывая то, что параметры ИУС (например, интенсивности потока отказов и восстановлений программных средств) могут изменяться, приводит к значительному росту размерности модели исследуемой системы [8]. Таким образом, для достижения требуемой точности, необходимо уделять повышенное внимание как процессу построения модели, так и процессу выбора эффективной техники (метода) решения и ПС. Однако данное утверждение идет вразрез с рекомендациями представленными в одном из базовых стандартов в отрасли функциональной безопасности – IEC 61508 [9], где определяется, что эффективные алгоритмы решения СДР были разработаны достаточно давно, и использование как специализированных так и универсальных программных средств возможно без акцентирования внимания на математических аспектах решения.

Внедрение методики позволяющей на основе анализа таких характеристик ММ как сложность, разреженность, жесткость и фрагментность обоснованно осуществлять направленный выбор метода решения и программного инструментария, позволит повысить результативность (точность) проводимого исследования, а также повысить уровень доверия к выходным результатам.

В данной статье представлена структура и функциональная модель информационной технологии описывающей процесс оценивания готовности ИУС с учетом этапа метрического анализа ММ и последующим выбором инструментального средства. Предложенная информационная технология учитывает процесс пошагового анализа рисков неточных решений на всех этапах, что обеспечивает выполнение условий по точности оценки систем описываемых СДУ Колмогорова-Чепмена.

## 1. Элементы информационной технологии метрико-интервального оценивания готовности ИУС

Элементы информационной технологии структурированы в табл. 2 по следующей схеме:

Таблица 2

Элементы информационной технологии оценивания готовности ИУС

| № п/п | Функция | Входные элементы | Выходные элементы | Элементы механизма | Управляющие элементы |
|---|---|---|---|---|---|
| 1 | Анализ технической документации | Техническое задание, спецификация | Результаты анализа технической документации | ЭЛПР | НТД |
| 2 | Введение и обоснование основных допущений процесса моделирования ИУС | Результаты анализа технической документации, базовые допущения теории МП | Допущения используемые в процессе моделирования ИУС | ЭЛПР | МЭК 61165 |
| 3 | Определение цели моделирования | Результаты анализа технической документации | Исследуемый показатель ИУС (цель) | ЭЛПР | НТД, ИП |
| 4 | Построение ССН ИУС | Результаты анализа п.1, допущения используемые в процессе моделирования ИУС, цель моделирования | ССН ИУС | ЭЛПР, специализированные ПС (SHARP, ITEM и т.д.) | ИП (МЭК 61078) |
| 5 | Построение марковской модели исследуемой ИУС | ССН ИУС, цель моделирования, статистические данные по отказам ИУС, временной интервал исследования, корректировка модели | ММ ИУС | ЭЛПР, специализированные ПС, частные ПС (MSMC) | ИП (МЭК 61165, МЭК 61508), инструкции по применению МФМ и метрико-интервального оценивания |
| 6 | Проведение метрико-интервального оценивания, построение метрико-интервальной модели | ММ ИУС, метрики, альтернативный метод решения | Рекомендация по решению ММ ИУС | ЭЛПР, частные ПС (MSMC) | Инструкции по применению МФМ и метрико-интервального оценивания |
| 7 | Решение ММ ИУС | Рекомендации по решению ММ ИУС, начальные условия, временной интервал исследования, методы | Искомое вероятностное значение | ЭЛПР, специализированные ПС, пакеты математического моделирования, частные ПС (MSMC) | ИП (МЭК 61165) |
| 8 | Верификация результатов решения марковской модели ИУС | Искомое вероятностное значение, методы | Таблица сравнения численных значений, корректировка модели | ЭЛПР, частные ПС, пакеты компьютерной математики, специализированные ПС | ИП |
| 9 | Анализ результатов верификации | Таблица сравнения численных значений | Результаты анализа, альтернативный метод решения | ЭЛПР | ИП |
| 10 | Анализ результатов моделирования | Результаты анализа п. 9 | Результаты моделирования | ЭЛПР | ИП |

- рассматриваемые операции по преобразованию информации (функции) на основе теоретических положений;

- данные или материальные объекты преобразованные рассматриваемыми функциями в выход (входные элементы);

- данные или материальные объекты, произведенные функциями (выходные элементы);

- средства, используемые для выполнения функций (элементы механизма);

- данные использующиеся, для управления процессом выполнения функций (управляющие элементы).

В таблице использованы следующие обозначения:

ЭЛПР – эксперты, лица принимающие решения;

НТД – Нормативно-техническая документация;

ССН – Структурная схема надежности;

ИП – Инструкции предприятия, стандарты национальные и международные;

МФМ – Многофрагментное моделирование.

## 2. Этапы реализации информационной технологии

Функциональная модель ИТ представлена на рис. 1 в виде IDF0 диаграммы. Опишем основные этапы реализации разработанной ИТ.

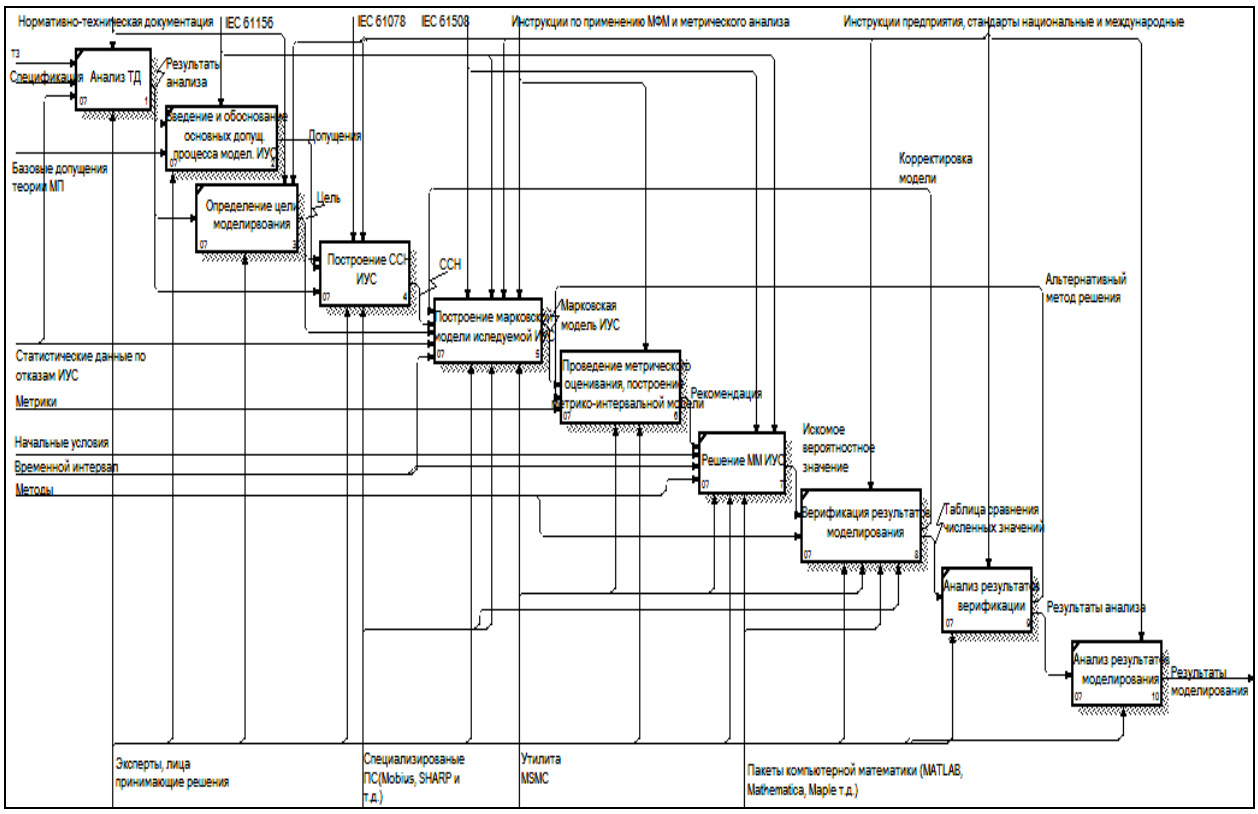


Рис. 1. Функциональная модель информационной технологии оценивания готовности ИУС

*Этап 1.* На данном этапе проводится анализ проектной документации разрабатываемой ИУС, для определения требований к показателям надежности исследуемой системы. Для этого необходимо, во-первых провести анализ технического задания на разработку системы, которое включает всю спецификацию предъявляемых к системе требований. Определяются требования, напрямую влияющие на надежность (готовность) системы (например, требования к архитектуре построения системы).

*Кроме того, результатом* данного анализа является исходная информация о моделируемой системе, т.е. логика ее функционирования, выполняемые функции и т.д., составляется список требований к надежности моделируемой ИУС.

*Этап 2.* Введение и обоснование базовых допущений процесса моделирования ИУС на основе использования исходной информации о системе, полученной на этапе 1, а также проведение анализа основных допущений аппарата марковского моделирования для определения его применимости в рамках проводимого исследования.

*Результатом* этапа является список допущений для разработки математической модели исследуемой системы.

*Этап 3.* Определение цели моделирования, а именно исследуемого и рассчитываемого с помощью марковского анализа, показателя надежности (готовности) как для всей ИУС, так и в случае необходимости – для ее отдельных компонент.

*Результатом* данного этапа являются данные о цели построения модели, а также сопутствующая им информация об уровне детализации этой модели.

*Этап 4.* Построение структурной схемы надежности ИУС в соответствии с определенной целью моделирования, а также установленной глубиной детализации модели. При этом используется информация полученная на этапах 1 – 3.

*Результат* реализации данного этапа – структурная схема надежности ИУС, либо ее компонента.

*Этап 5.* Построение марковской модели исследуемой ИУС на основе использования введенных допущениях (этап 2), цели моделирования (этап 3), опираясь на разработанную структурную схему надежности (этап 4), статистические данные полученные на этапе тестирования ИУС, по отказам и восстановлениям аппаратных и программных компонент моделируемых объектов.

*Результатом* данного этапа является марковская модель исследуемой ИУС.

*Этап 6.* На данном этапе проводится построение метрико-интервальных моделей, на основе метрико-ориентированного оценивания исходных марковских моделей с целью определения наиболее эффективного подхода к их решению. Входной информацией является информация о метриках, а также марковская модель на основе которой проводится расчет данных метрик.

*Результатом* выполнения данного этапа есть рекомендации по применению методов решения

исходной марковской модели, как для основного решения, так и для верификации его результатов.

*Этап 7.* На основе сформулированных на предыдущем этапе рекомендаций по выбору метода решения выполняется решение марковской модели ИУС. Также данный этап учитывает возможность корректировки исходной модели.

*Результатом* данного этапа являются искомые вероятностные значения рассчитываемого показателя надежности ИУС.

*Этап 8.* Проведение верификации полученных результатов, в случае наличия данной рекомендации (этап 6).

*Результатом* является таблица сравнений численных значений результатов, полученных на этапах 7 и 8.

*Этап 9.* Проводится анализ результатов верификации на основе таблицы полученной на этапе 8.

*Результатом* является вывод о точности полученных результатов. В случае не удовлетворения условиям точности, проводится выбор альтернативного метода решения предлагаемого на этапе 6.

*Этап 10*. На данном этапе проводится анализ результатов моделирования, а именно формирование выводов относительно цели моделирования.

*Результатом* выполнения данного этапа является вывод о достижении исследуемой системы предъявляемых требований к ее надежности (готовности) либо составление рекомендаций по корректировке архитектуры ИУС исходя из результатов оценки надежности.

## Выводы

В данной статье представлена информационная технология оценивания готовности важных для безопасности, описывающая внедрение методики метрического оценивания марковской модели исследуемой системы в целях выбора эффективного метода и программного средства для ее решения. Предложенная ИТ учитывает процесс пошагового анализа рисков неточных решений на всех этапах, что обеспечивает выполнение условий по точности оценки систем описываемых СДУ Колмогорова-Чепмена.

## Список литературы

*1. Безопасность атомных станций: системы управления и защиты ядерных реакторов [Текст] / М.А. Ястребенецкий, Ю.В. Розен, С.В. Виноградская, Г. Джонсон, В.В. Елисеев, А. А. Сиора, В.В. Скляр, Л. И. Спектор, В.С. Харченко. − К.: Основа-Принт, 2011. − 768 с.*

*2. Gray J. High-Availability Computer Systems [Text] / J. Gray, D. P. Siewiorek // IEEE Computer. – 1991. – Vol. 9, № 7. – P. 39-48.*

*3. Trivedi, K.S. Achieving and assuring high availability [Text] / K.S. Trivedi, G. Ciardo, B. Dasarathy, M. Grottke, A. Rindos, B. Vashaw // In Proc. 13th IEEE workshop on dependable parallel, 22nd IEEE International parallel & distributed processing sypmosium. – 2008.*

*4. Archana, S. Availability models in practice [Text]/ S. Archana, R. Srinivasan, K. S. Trivedi.// Proc. Int. Workshop on Fault-Tolerant Control and Computing (FTCC-1), Seoul, Korea. – 2000*

*5. Kharchenko, V. Markov's model and tool-based assessment of safety-critical I&C systems: gaps of the IEC 61508 [Text] / V. Kharchenko, O. Odarushchenko, V. Butenko, P. Popov, V. Sklyar, E. Odarushchenko // In Proc. 12th International conference on probabilistic safety assessment and modeling. – pass: http://psam12.org/proceedings/paper/paper_455_1.pdf*

*6. Bobbio, A. A Aggregation Technique for Transient Analysis of Stiff Markov Chains [Text]/ A. Bobbio, K. S. Trivedi// IEEE Trans. on Comp.., 1986. - C-35. - P. 803-814.*

*7. Kharchenko, V. Availability assessment of Computer Systems Described by Stiff Markov Chains: Case Study [Text] / V. Kharchenko, O. Odarushchenko, P. Popov, V. Odarushchenko // Springer. – CCIS(412). – 2013.- P. 112 – 135*

*8. Kharchenko, V. Multi-fragmental availability models of critical infrastructures with variable parameters of system dependability [Text] / V. Kharchenko, O. Odarushchenko, V. Odarushchenko // International Journal Information & Security. – 2011. – 28. – P. 248 – 265.*

*9. IEC 61508 (6 part), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. – 2010*

*Поступила в редколлегию 28.10.2014*

**Рецензент:** д-р техн. наук, проф. А.Л. Ляхов, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава.

### ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ ГОТОВНОСТІ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ З ВИКОРИСТАННЯМ МАРКОВСЬКИХ МОДЕЛЕЙ НА БАЗІ ВИБОРУ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ

В.С. Харченко, В.О. Бутенко

*В статті запропонована функціональна модель інформаційної технології оцінювання готовності інформаційно-керуючих систем важливих для безпеки, що описує впровадження етапу метричного оцінювання марковської моделі досліджуваної системи з метою вибору ефективного методу її розв'язання, а також інструментального засобу.*

***Ключевые слова:*** *інформаційна технологія, метричне оцінювання, марковська модель, інструментальний засіб, інформаційно-керуюча система.*

### INFORMATION TECHNOLOGY FOR AVAILABILITY ASSESSMNET OF I&C SYSTEMS USING MARKOV CHAINS AND SOFTWARE SELECTION

V.S. Kharchenko, V.O. Butenko

*The paper presents functional model of information technology for availability assessment of safety-critical instrumentation and control systems. The information technology shows the process of I&Cs availability assessment using Markov-chains with implementation of metric-based analysis of the system model. The result of such analysis aims to eliminate the non-effective techniques, method and tools for model solution.*

***Key words:*** *information technology, metric-based assessment, Markov chains, tool, instrumentation and control system.*