УДК 681.3(075.8)

**В.В. СКЛЯР[1], В.И. ТОКАРЕВ[2], А.Д. ГЕРАСИМЕНКО[2]**

[1]*Государственный НТЦ по ядерной и радиационной безопасности, Украина*
[2]*ЗАО «Радий», Украина*

# ИЕРАРХИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ НАДЕЖНОСТИ МНОГОКОМПОНЕНТНЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Предложена модель оценки надежности, позволяющая учесть свойства современных много компонентных информационно-управляющих систем (ИУС). Разработанная модель позволяет учесть надежность неидеальной программной составляющей, иерархию структуры ИУС, различное влияние компонентов на надежность ИУС и гибкость структуры ИУС. Кроме того, разработанная модель позволяет реализовать процесс конфигурационного управления оценкой надежности ИУС.

**оценка надежности, многокомпонентные системы, иерархические структуры**

## Постановка задачи и обзор публикаций

К современным информационно-управляющим системам (ИУС) технических комплексов критического использования (ТККИ) для таких отраслей, как энергетика, транспорт, химическая промышленность и др., применяются жесткие требования по надежности [1 – 3]. Требования стандартов Международной электротехнической комиссии (МЭК) к интенсивности отказов ИУС в зависимости от уровня безопасности ТККИ приведены в табл. 1 [4].

Таблица 1

Требования к надежности ИУС ТККИ

| Уровень безопасности ТККИ | Последствия аварии ТККИ | Требуемая интенсивность отказов |
|---|---|---|
| D | Незначительный ущерб без риска для людей | $10^{-6} \div 10^{-5}$ 1/час |
| C | Серьезная угроза здоровью и жизни нескольких человек | $10^{-7} \div 10^{-6}$ 1/час |
| B | Гибель нескольких человек | $10^{-8} \div 10^{-7}$ 1/час |
| A | Гибель большого количества людей | $10^{-9} \div 10^{-8}$ 1/час |

Архитектура современных ИУС ТККИ характеризуются такими свойствами, как иерархичность, распределенность и многокомпонентность. Такой подход к построению систем позволяет локализовать отказы ИУС и обеспечить, таким образом, высокую надежность и безопасность таких систем. При этом возникает задача демонстрации соответствия надежность ИУС ТККИ требований технического задания и нормативных документов. Согласно существующей практике такая задача решается путем проведения анализа надежности ИУС, в ходе которого производится расчет показателей надежности ИУС и их сравнение с заданными [5].

Следует отметить, что существующие методы и модели оценки надежности [6 – 10], как правило, не учитывают в комплексе следующие существенные свойства современных ИУС ТККИ:

– влияние надежности программного обеспечения (ПО) на надежность ИУС;

– иерархичность структуры и различное влияние компонентов на надежность ИУС;

– гибкость структуры ИУС, которая позволяет синтезировать на единой программно-аппаратной платформе различные типы систем; данное свойство повышает важность процесса конфигурационного управления, в том числе, конфигурационного управления оценкой надежности ИУС [11].

**Целью статьи** является разработка модели надежности, позволяющей выполнить оценку многокомпонентных ИУС.

## 1. Принципы оценки надежности многокомпонентных ИУС

Структура многокомпонентной ИУС, а также ее изменения (эволюция) описываются теоретико-множественной моделью, согласно которой ИУС состоит из множества иерархически взаимосвязанных уровней $Level = \{Level_0, ..., Level_X\}$ [11]. На каждом $i$-м уровне формируется множество компонентов $K_i = \{K_{i1}, ..., K_{iY}\}$, реализующих множество функций $\Phi_i = \{\Phi_{i1}, ..., \Phi_{iZ}\}$. Кроме того, для каждого из множеств $K_i$ и $\Phi_i$ в процессе эволюции могут быть выделены по два следующих подмножества:

– подмножества измененных компонентов $\Delta K_i = \{K_{i1}, ..., K_{iY1}\}$ и измененных функций $\Delta\Phi_i = \{\Phi_{i1}, ..., \Phi_{iZ1}\}$;

– подмножества неизмененных компонентов $\delta K_i = \{K_{i1}, ..., K_{iY2}\}$ и неизмененных функций $\delta\Phi_i = \{\Phi_{i1}, ..., \Phi_{iZ2}\}$;

$\Delta K_i \cup \delta K_i = K_i$; $\Delta K_i \cap \delta K_i = \varnothing$; $\Delta\Phi_i \cup \delta\Phi_i = \Phi_i$; $\Delta\Phi_i \cap \delta\Phi_i = \varnothing$.

Эволюционно-компонентная модель ИУС является основой для разработки подхода к конфигурационной оценке надежности компонент и ИУС в целом [11].

Принципы оценки надежности многокомпонентных ИУС включают:

1) использование типовой структуры функциональных подсистем ИУС, включая типовые блоки и типовые функциональные узлы;

2) использование для оценки надежности ИУС иерархической модели структуры программно-аппаратных компонент;

3) конфигурационное управление многокомпонентной моделью надежности ИУС.

## 2. Структура модели надежности многокомпонентных ИУС

Применение модели оценки надежности ИУС осуществляется последовательно от нижнего уровня иерархии к верхнему. При расчете надежности приняты следующие допущения:

– распределение времени до отказа соответствует экспоненциальному закону распределения случайной величины;

– отказы элементов являются взаимонезависимыми;

– для блоков ИУС обеспечивается полное диагностирование.

Структура модели надежности многокомпонентных ИУС приведена в табл. 2.

## 3. Применение модели надежности многокомпонентных ИУС

При разработке моделей надежности элементов ИУС используются математические модели элементов согласно стандарту Министерства обороны США MIL-HDBK-217 «Предсказание надежности электронных компонент».

Для дискретных полупроводниковых элементов, индуктивных элементов и резисторов общая формула для интенсивности отказов имеет вид:

$$\lambda_Э = \lambda_b \cdot \prod \pi_i \,, \qquad (1)$$

где $\lambda_b$ – базовое значение интенсивности отказов элемента; $\pi_i$ – поправочные коэффициенты.

Элементы функциональных узлов, как правило, не резервируются. Поэтому, ССН для расчета надежности функциональных узлов не требуются, а интенсивность отказов функциональных блоков определяется как сумма интенсивности отказов элементов, т.е. $\lambda_{\Phi Y} = \sum \lambda_i$. В случае резервирования элементов на уровне функциональных узлов интенсивности отказов определяются по классическим расчетным формулам [6]:

$$\lambda = n! \lambda_{\Phi Y}^{n} / \mu \,, \qquad (2)$$

где $n$ – кратность резервирования; $\mu$ – интенсивность восстановления.

Таблица 2

Структура иерархической модели оценки надежности многокомпонентных ИУС

| Уровень ИУС | Компоненты ИУС | Изменяемая часть компонентов ИУС | Информация, обрабатываемая в ходе оценки надежности и подлежащая конфигурационному управлению |
|---|---|---|---|
| $Level_0$ (ИУС) | – | – | – состав используемых функциональных подсистем;<br>– структурная схема надежности (ССН) – при необходимости;<br>– перечень состояний, в которых может находиться ИУС;<br>– марковская модель переходов между состояниями;<br>– аналитические модели (формулы) для расчета показателей надежности;<br>– рассчитанные значения показателей надежности (вероятности нахождения системы в различных состояниях, коэффициент готовности, коэффициент оперативной готовности) |
| $Level_1$ | Множество функциональных подсистем $\{КФП_1,...,КФП_L\}$ | Множество измененных функциональных подсистем $\{\Delta КФП\}$ | – количество используемых блоков и для каждого из блоков кратность резервирования;<br>– модель надежности ПО (при необходимости);<br>– ССН, учитывающая надежность ПО;<br>– перечень состояний, в которых может находиться функциональная подсистема;<br>– марковская модель переходов между состояниями;<br>– аналитические модели (формулы) для расчета показателей надежности;<br>– рассчитанные значения показателей надежности (вероятности нахождения системы в различных состояниях, коэффициент готовности, коэффициент оперативной готовности). |
| $Level_2$ | Множество блоков $\{КБ_1,...,КБ_M\}$ | Множество измененных блоков для каждой из функциональных подсистем $\{\Delta КБ^{ФПi}\}$ | – количество используемых функциональных узлов и для каждого из узлов кратность резервирования;<br>– ССН;<br>– аналитические модели (формулы) для расчета показателей надежности;<br>– рассчитанные значения показателей надежности (интенсивность отказов, вероятность безотказной работы, вероятность отказов) |
| $Level_3$ | Множество функциональных узлов $\{КФУ_1,...,КФУ_N\}$ | Множество измененных функциональных узлов для каждого из блоков $\{\Delta КФУ^{Бi}\}$ | – количество используемых элементов и для каждого из элементов кратность резервирования;<br>– ССН (при необходимости);<br>– аналитические модели (формулы) для расчета показателей надежности;<br>– рассчитанные значения показателей надежности (интенсивность отказов, вероятность безотказной работы, вероятность отказов) |
| $Level_4$ | Множество элементов (элементная база) $\{КЭ_1,...,КЭ_P\}$ | Множество измененных элементов для каждого из функциональных узлов $\{\Delta КЭ^{ФУi}\}$ | – базовые значения интенсивностей отказов согласно стандарту MIL-HDBK-217;<br>– номенклатура и значения поправочных коэффициентов, используемых для уточнения базовых значений интенсивностей отказов согласно стандарту MIL-HDBK-217;<br>– рассчитанные значения интенсивностей отказов |
| $Level_5$ | Множество программ процессоров и проектов ПЛИС $\{КПО_1,...,КПО_T\}$ | Надежность ПО учитывается в составе функциональных подсистем | – |
| $Level_6$ | Множество программных модулей $\{КМ_1,...,КМ_Q\}$ | | |
| $Level_7$ | Множество алгоритмов $\{КА_1,...,КА_R\}$ | | |
| $Level_8$ | Множество констант и параметров $\{ККиП_1,...,ККиП_S\}$ | | |

Поскольку внутренняя структура функциональных узлов отличается значительным разнообразием, на данном уровне нецелесообразно проводить обобщения относительно состава элементов. При необходимости для функциональных узлов могут быть получены ССН и аналитические зависимости для показателей надежности.

Исходной информацией для разработки моделей надежности блоков ИУС являются данные о кратности резервирования и количестве для каждого из функциональных узлов, входящих в состав блоков. Для нерезервированных последовательно соединенных однотипных узлов интенсивности отказов суммируются. Для резервированных узлов интенсивности отказов определяется по формуле (2).

Данный уровень иерархической модели оценки надежности ИУС является наиболее важным, поскольку:

– на данном уровне осуществляется пофункциональный расчет надежности; если нет необходимости производить интегральную оценку надежности выполнения всех функций ИУС (а большинство стандартов этого не требуют [4, 5]), то данный уровень является верхним в модели оценки надежности ИУС;

– на данном уровне производится учет надежности ПО;

– на данном уровне производится учет видов резервирования каналов ИУС, а также учет многоверсионности ИУС.

В состав функциональных подсистем может входить один блок или несколько однотипных блоков, обладающих равной интенсивностью отказов. Блоки могут быть резервированы или выполнять часть однотипных функций, то есть быть нерезервированными.

Кроме того, в составе функциональной подсистемы должна быть учтена надежность ПО. Для определения надежности ПО существует ряд соответствующих моделей, позволяющих прогнозировать интенсивность отказов ПО. Для ПО ИУС возможны следующие подходы к определению показателей надежности ПО [12]:

1) использование статистических данных об интенсивности отказов аналогичного по характеристикам ПО в течение эксплуатации;

2) использование данных об интенсивности отказов оцениваемого ПО в течение тестирования в качестве входных данных для вероятностных моделей надежности ПО;

3) использование метрик сложности оцениваемого ПО для определения возможного количества дефектов ПО и для прогнозирования на основе этих данных интенсивности отказов ПО.

В рассматриваемом случае целесообразно использовать первый подход. Согласно статистике для ИУС критического применения интенсивность отказов ПО для одной функциональной подсистемы составляет около $\lambda_{ПО\ блока} = 10^{-7}$ 1/час.

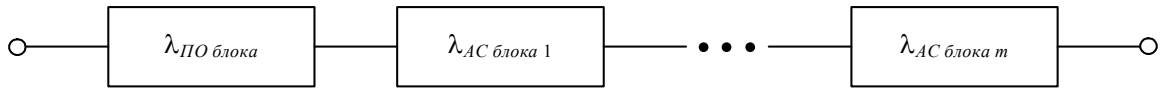
При учете неидеальной надежности ПО в составе функциональной подсистемы используются следующие допущения:

– при наличии в составе функциональной подсистемы нескольких блоков данные блоки являются однотипными и используют в своем составе однотипное ПО;

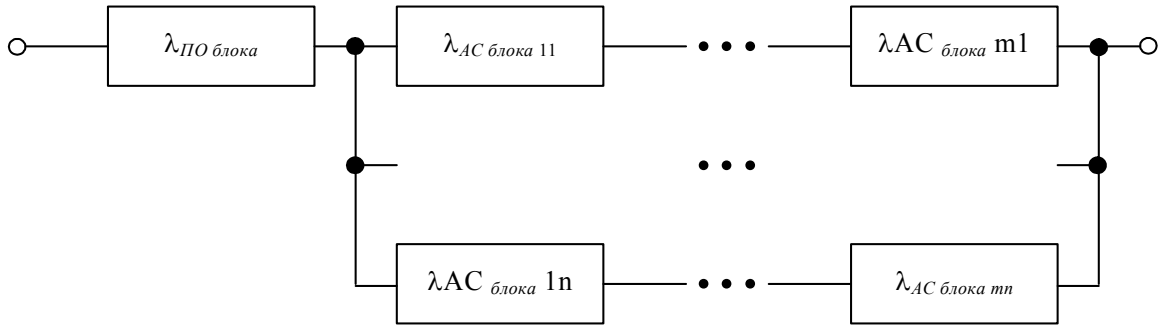
– ПО всех блоков обрабатывает единый массив данных и отказ ПО какого-либо из блоков приводит к общему отказу подсистемы; таким образом, ПО всех блоков имеет общую интенсивность отказов, то есть обозначается на ССН одним элементом;

– при резервировании блоков функциональной подсистемы в них используется одинаковое ПО (за исключением многоверсионных систем), то есть в данном случае ПО всех блоков также имеет общую интенсивность отказов и обозначается на ССН одним элементом.

С учетом рассмотренных допущений ССН для одноверсионных нерезервированных и резервированных функциональных подсистем имеют вид как на рис. 1.




а – нерезервированная функциональная подсистема




б – резервированная функциональная подсистема

Рис. 1. Структурные схемы надежности для нерезервированных (а) и резервированных (б) одноверсионных функциональных подсистем

Интенсивность отказов одного канала функциональной подсистемы (или нерезервированной функциональной подсистемы) составляет

$$\lambda_{ФП} = \lambda_{ПО\,блока} + m \cdot \lambda_{АС\,блока\,i}, \qquad (3)$$

где $m$ – количество блоков в канале функциональной подсистемы.

Интенсивность отказов резервированной функциональной подсистемы в соответствии с формулой (2) составляет

$$\lambda_{ФП} = \lambda_{ПО\,блока} + n!\left(m \cdot \lambda_{АС\,блока\,i}\right)^n / \mu \ . \qquad (4)$$

Согласно принятым допущениям резервирование каналов ИУС и надежность ПО учитывается в составе функциональных подсистем. Поэтому, на верхнем уровне иерархической модели оценки надежности ИУС производится интеграция показателей надежности функциональных подсистем (сложение интенсивностей отказов).

В общем случае для ИУС может быть учтена надежность всех входящих в ее состав функциональных подсистем. После выполнения расчетов значение итогового показателя надежности должно быть сравнено со значением, указанным в требованиях технического задания. Кроме того, может быть проведена интеграция показателей надежности для некоторых функциональных подсистем в том случае, когда они необходимы для выполнения отдельных функций ИУС, указанных в техническом задании.

## Выводы и перспективы дальнейших исследований

Разработанная модель применялась для анализа надежности программно-технических комплексов (ПТК) АЭС разработки ЗАО «Радий» (г. Кировоград) [13]:

– ПТК системы аварийной и предупредительной защиты ядерного реактора;

– ПТК системы автоматического регулирования и ограничения мощности ядерного реактора;

– ПТК управляющей системы безопасности ядерного реактора;

– ПТК системы группового и индивидуального управления органами регулирования ядерного реактора.

Для указанных ПТК применение разработанной модели позволило определить показатели надежности и продемонстрировать их соответствие требова-

ниям по надежности и по безопасности. Поскольку ПТК разработки ЗАО «Радий» базируются на единой программно-аппаратной платформе, для них было реализовано конфигурационное управление оценкой надежности.

В дальнейшем представляется целесообразным разработать модели надежности для уровня функциональных подсистем, которые позволяли бы учитывать конфигурацию программно-аппаратных средств многоверсионных ИУС.

## Литература

1. Laprie J.-C. Dependability Handbook. LAAS Report n 98-346. – Toulouse: Laboratory for Dependability Engineering, 1998. – 365 p.

2. Харченко В.С., Жихарев В.Я., Илюшко В.М., Нечипорук Н.В. Многоверсионные системы, технологии, проекты. – Х.: НАКУ «ХАИ», 2003. – 486 с.

3. Avizienis A., Laprie J., Randell B. Fundamental Concepts of Dependability. Research Report n 01145, LAAS-CNRS, 2001. – 25 p.

4. Смит Д., Симпсон К. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов. – М.: Издательский Дом «Технологии», 2004. – 208 с.

5. Безопасность атомных станций: информационные и управляющие системы / М.А. Ястребенецкий, В.Н. Васильченко, С.В. Виноградская и др. – К.: Техника, 2004. – 472 с.

6. Долманицкий С.М. Построение надежных логических устройств. – М.: Энергия, 1971. – 280 с.

7. Дружинин Г.В. Надежность автоматизированных производственных систем. – М.: Энергоатомиздат, 1986. – 480 с.

8. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. – М.: Радио и связь, 1989. – 208 с.

9. Хетагуров Я.А. Основы построения управляющих вычислительных систем. – М.: Радио и связь, 1991. – 228 с.

10. Чернышев А.А. Основы конструирования и надежности электронных вычислительных средств. – М.: Радио и связь, 1998. – 448 с.

11. Herasimenko O., Sklyar V., Kharchenko V. An Evolutional-Component Model of Process Control System // Proceedings of the 2nd International Conference Advanced Computer Systems and Networks Design and Application “ACSN–2005”. – Lviv (Ukraine). – 21–23 September 2005. – P. 123-126.

12. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. – Х.: НАКУ «ХАИ», 2004. – 159 с.

13. Программно-технические комплексы аварийной и предупредительной защиты ядерных реакторов: обеспечение и оценка безопасности / Е.С. Бахмач, С.В. Виноградская, Ю.В. Розен и др. // Ядерная и радиационная безопасность. – 2005. – Т. 8, № 1. – С. 21-50.

*Поступила в редакцию 28.02.2006*

**Рецензент:** д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.