

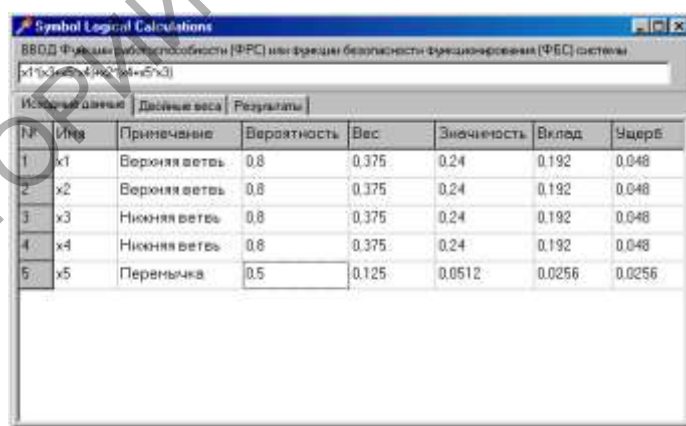
УДК 621.3

## Средства автоматизации анализа надежности систем критического применения

Д. Н. ШЕВЧЕНКО

**Введение.** В настоящее время существует большое количество аналитических и имитационных методов расчета надежности и безопасности функционирования систем. Однако применение сложных моделей надежности, адекватно отражающих свойства современных систем критического применения (СКП, например, систем железнодорожной автоматики, телемеханики и других систем управления ответственными технологическими процессами), ограничивается большой размерностью систем, сложностью связей между компонентами; невыполнением допущений и ограничений методов, связанных с потоками отказов и восстановления системы, отсутствием достоверной информации о характеристиках компонентов СКП. Поэтому для расчета надежности и безопасности функционирования современных СКП на этапах их разработки, сертификации, внедрения и эксплуатации по-прежнему актуально применение таких методов, как логико-вероятностный метод, метод анализа дерева отказов, метод статистического моделирования. Вместе с тем, большая размерность и сложность современных СКП требуют автоматизации расчетов надежности и безопасности функционирования систем.

**Логико-вероятностный метод.** Одним из простейших методов анализа надежности СКП является логико-вероятностный метод (ЛВМ), при котором структура надежности системы описывается средствами математической логики, а количественная оценка ее надежности выполняется теоретико-вероятностными методами. Наряду с вероятностью безотказной (безопасной) работы ЛВМ позволяет определять вес, значимость и вклад компонентов, что важно при разработке и сертификации СКП [1].



№	Имя	Примечание	Вероятность	Вес	Значимость	Вклад	Ущерб
1	x1	Верхняя ветвь	0.8	0.375	0.24	0.192	0.048
2	x2	Верхняя ветвь	0.8	0.375	0.24	0.192	0.048
3	x3	Нижняя ветвь	0.8	0.375	0.24	0.192	0.048
4	x4	Нижняя ветвь	0.8	0.375	0.24	0.192	0.048
5	x5	Перемычка	0.5	0.125	0.0512	0.0256	0.0256

Рисунок 1 – Логико-вероятностный метод. Задание исходных данных

Логико-вероятностный метод реализован автором в программе “Symbol Logical Calculations” (см. рис. 1, 2). Наиболее сложным этапом ЛВМ является построение математической модели надежности методом минимальных путей и сечений, что возможно лишь для структурного уровня представления СКП. Поэтому метод применим лишь на начальных этапах разработки и сертификации СКП. Другие ограничения ЛВМ касаются применения компонентов с тремя состояниями и учетом последовательности отказов компонентов, что актуально при исследовании безопасности функционирования СКП.

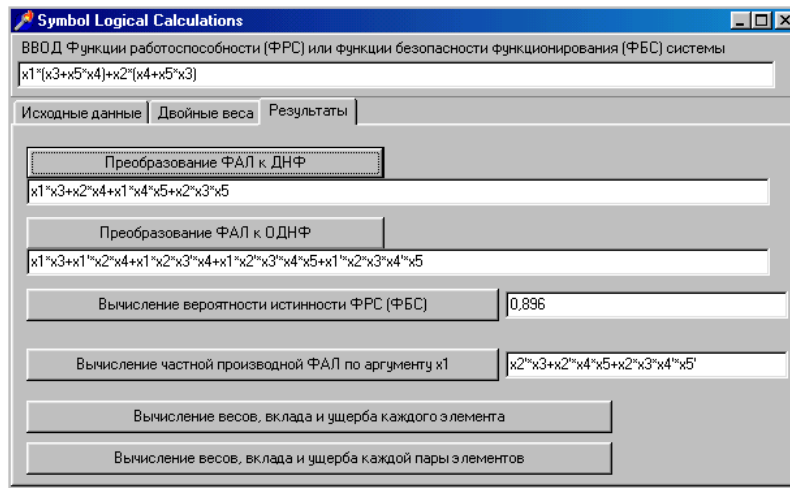


Рисунок 2 – Логико-вероятностный метод. Результаты анализа

**Метод анализа дерева отказов.** Другим эффективным методом расчёта надёжности и безопасности функционирования невосстанавливаемых СКП является метод анализа дерева отказов (FTA – Fault Tree Analysis). Идея метода состоит в разложении событий, связанных с отказами (опасными отказами) системы, на элементарные события, связанные с отказами элементов или подсистем, с учётом причинно-следственных связей между событиями [2]. В дальнейшем, на основе дерева отказов с помощью вероятностных методов определяются основные показатели надёжности СКП.

Вместе с тем, для больших и иерархически сложных (например, структурно резервированных) технических систем причинно-следственные связи между неисправностями компонентов и их последствиями не являются очевидными, что затрудняет построение дерева отказов. Особенно эта проблема актуальна при исследовании безопасности СКП, когда отказы системы подразделяются на опасные, защитные, маскируемые и т.д. По аналогичным причинам затруднен процесс расчета показателей надёжности системы.

Для автоматизации построения дерева отказов (опасных отказов), а также для автоматического расчета основных показателей безотказности и безопасности функционирования СКП, таких, как вероятность безотказной (безопасной) работы, математическое ожидание, дисперсия и другие моменты времени наработки системы на отказ (опасный отказ) с использованием FTA предлагается программа «АВПКО».

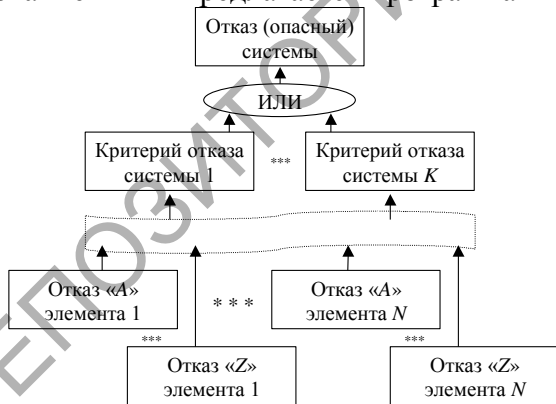


Рисунок 3 – Структура дерева отказов в «АВПКО»



Рисунок 4 – Базовые операции над событиями

Корнем дерева отказов (см. рис.3) являются события, связанные с отказами (опасными отказами) системы. Базовыми являются события связанные с возможными отказами элементов системы. Программа «АВПКО» позволяет строить дерево отказов как сверху вниз, так и снизу вверх. Первый подход может быть применён для анализа надёжности системы на этапе её разработки, когда только определены критерии отказов (опасных отказов) системы и её подсистем. Второй подход рекомендуется на стадии сертификационных и исследовательских

испытаний системы, когда определены все возможные неисправности всех компонентов системы и требуется определить последствия и критичность отказов. Дерево отказов строится в «АВПКО» с помощью стандартного компонента Delphi «TreeView», что позволяет оперативно редактировать ветви и узлы дерева, отображать и масштабировать интересующие ветви дерева отказов.

В качестве базовых операций над событиями в «АВПКО» приняты операции логического сложения, умножения и отрицания (рис. 4). Однако для исследования безопасности функционирования СКП, когда на последствия неисправностей влияет порядок их возникновения, указанный список операций над событиями дополняется операцией логического умножения, учитывающей последовательность наступления событий (приоритетное «И»).

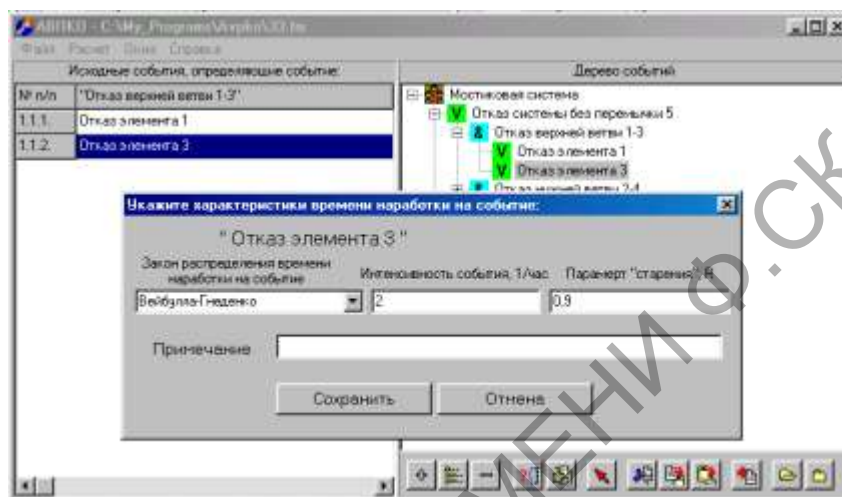


Рисунок 5 – Программа «АВПКО» расчета надежности методом ФТА

Технология построения дерева отказов в «АВПКО» требует выполнения трех основных условий. Во-первых, каждое событие может выражаться через элементарные события только с помощью одной из логических операций сложения «ИЛИ», умножения «И», исключаяющего «ИЛИ» и приоритетного «И». Во-вторых, события, к которым применяется операция логического сложения, должны быть несовместными. В-третьих, события, к которым применяется операция логического умножения, должны быть независимыми. Для обеспечения перечисленных требований дерево отказов может быть дополнено несколькими фиктивными ветвями (связями) и узлами (событиями).

В качестве исходных данных при расчёте надёжности СКП в «АВПКО» используются законы распределения времени до наступления элементарных событий (корней дерева), которые, определяют неисправности компонентов системы (см. рис.5). Знание законов распределения времени до наступления элементарных событий позволяет определять законы распределения до наступления событий, связанных с отказами подсистем, а также вычислять вероятностей наступления событий, определяемых операцией логического умножения с учетом последовательности наступления элементарных событий, что особенно актуально при исследовании безопасности функционирования СКП.

**Статистическое моделирование надежности.** Одним из способов исследования, адекватно отражающим надёжностные свойства СКП, является статистическое моделирование, для которого характерно получение большого числа реализаций имитационной модели СКП на отказ с последующим статистическим анализом полученной выборки [2]. Очевидно, что для статистического моделирования надёжности СКП на основе их имитационных моделей (ИМ) необходимо использование инструментальных средств автоматизации построения ИМ СКП, проведения имитационных экспериментов и анализа результатов. Для этого автором предлагается специализированный программно-технологический комплекс (ПТК) «СМ-ДЭС» и технология использования ПТК для исследования надёжности и безопасности функционирования СКП [3].

## Технология построения имитационных моделей надёжности систем

Дискретные электронные системы			
Исходная схема системы		Уровень детализации модели надёжности	Особенности построения модели надёжности системы
Принципиальная	Функциональная	Логический (вентильный)	Визуальное изображение модели надёжности системы отличается от принципиальной схемы системы наличием фиктивных вентилях, определяющих функционирование монтажных соединений в системе
		Регистровый (функциональный)	Визуальное изображение модели надёжности системы полностью соответствует её функциональной схеме
Структурная		Структурный	Составляется (методом минимальных путей и сечений) логическая структура, соответствующая функции безотказности (безопасности) системы
Аналоговые электронные системы, системы другой физической природы			
Цели исследования		Особенности построения модели надёжности системы	
Качественный анализ безотказности (безопасности)		Используются квазианалоговые компоненты	
Количественный анализ безотказности (безопасности)		Составляется (методом минимальных путей и сечений) логическая структура, соответствующая функции безотказности (безопасности) системы	

Технология построения моделей надёжности и безопасности СКП в ПТК «СМ-ДЭС» зависит от исходной схемы СКП, а также уровня детализации модели надёжности и представлена в таблице 1.

С помощью предлагаемого ПТК «СМ-ДЭС» и технологии его применения могут быть оценены показатели надёжности широкого класса технических систем, в которых события, связанные с отказами и восстановлением компонентов, а также реконfigurацией происходят мгновенно [3]. Использование статистического моделирования при количественной оценке вероятностных показателей надёжности системы снимает ограничения на потоки отказов и восстановления компонентов системы, на независимость и кратность отказов и реконfigurацию системы, которые характерны для аналитических моделей.

Основным ограничением статистического моделирования безопасности функционирования СКП является высокая ресурсоёмкость исследования. Так для подтверждения проектируемого уровня безопасности 0,99999 с доверительной вероятностью 0,995 необходимо провести не менее 529830 экспериментов. Решение данной проблемы состоит в применении методов ускоренного имитационного моделирования: методов уменьшения дисперсии реализаций наработки имитационной модели СКП на опасный отказ и аналитико-статистических методов [2]. На практике применение методов ускоренного моделирования функциональной безопасности ограничивается тем, что не существует универсальных подходов преобразования моделей надёжности систем, определения функционалов показателей безопасности. Для каждой системы особенности применения того или иного метода ускоренного моделирования являются уникальными, поскольку учитывают информацию о структуре системы, распределении вероятностей её возможных состояний и входных воздействий, значения надёжностных характеристик компонентов, критерии опасных отказов. При этом, во многих случаях проблема оптимального преобразования модели безопасности функционирования системы принципиально не имеет аналитического решения; а эффективное преобразование выполняется эмпирическим способом. Кроме того, применение существующих методов ускоренного моделирования для оценки показателей безопасности функционирования СКП затруднено в силу сложности систем, разделения их отказов на защитные и опасные; возможности восстановления и реконfigurации подсистем.

В заключение следует заметить, что ограничение ресурсоёмкости статистического моделирования практически не касается исследования безотказности СКП. В работе [4] представлен пример статистического моделирования безотказности структуры системы диспетчерской централизации «Неман» с помощью ПТК «СМ-ДЭС».

**Abstract.** Automated means of the analysis of reliability of critical application systems and different methods of reliability calculation are considered in the paper.

### Литература

1. Рябинин, И.А. Надёжность и безопасность структурно-сложных систем / И.А. Рябинин. – СПб.: Политехника, 2000. – 248 с.
2. Надёжность и эффективность в технике. Справочник: В 10 т. Т. 2. Математические методы в теории надежности и эффективности / Под ред. Б. В. Гнеденко. – М.: Машиностроение, 1987. – 280 с.
3. Шевченко, Д.Н. Программно-технологический комплекс исследования надежности и безопасности СЖАТ / Д.Н. Шевченко // Испытания систем железнодорожной автоматики и телемеханики на безопасность и электромагнитную совместимость: докл. Междунар. семинара – Гомель, БелГУТ, 2001. – С. 124–130.
4. Харлап, С.Н. Технология исследования безотказности ДЦ «Нёман» с помощью ПТК «СМ-ДЭС» / С.Н. Харлап, Д.Н. Шевченко // Проблемы безопасности на транспорте: тез. докл. Междунар. науч.-практич. конф. – Гомель, БелГУТ, 2002. – С. 187–188.

Белорусский государственный  
университет транспорта

Поступило 8.05.08

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРЫНЫ