АТТЕСТАЦИЯ ПРОГРАММЫ "АРБИТР" АВТОМАТИЗИРОВАННОГО РАСЧЕТА БЕЗОПАСНОСТИ И ТЕХНИЧЕСКОГО РИСКА СИСТЕМ

CERTIFICATION OF THE SOFTWARE FOR AUTOMATED CALCULATIONS OF SYSTEMS' SAFETY AND TECHNICAL RISKS "ARBITER"

Можаев Александр Сергеевич
МА БР 2007

"Специализированная инжиниринговая компания "Севзвпмонтажавтоматика"
E-mail: Alexander_Mozhaev@szma.com

Аннотация. Приведены основные характеристики программы АРБИТР, организация и результаты ее экспертизы в Совете по аттестации программных средств при Ростехнадзоре РФ, опыт практического применения и направления дальнейшего развития.

Abstract: The paper describes the software "ARBITER", organization and results of its expertise by Software Certification Committee of ROSTECHNADZOR of the Russian Federation, its application and further development trends.

Ключевые слова: система, структура, надежность, живучесть, безопасность, риск, общий логико-вероятностный метод, схема функциональной целостности, технология автоматизированного структурно-логического моделирования, ПК АСМ СЗМА.

Разработанное в ОАО "СПИК СЗМА" программное средство (ПС) АРБИТР, "Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА), базовая версия 1.0" [1], успешно прошло экспертизу в Совете по аттестации программных средств Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) РФ, при Научно-техническом Центре по ядерной и радиационной безопасности (НТЦ ЯРБ) [2]. На ПС АРБИТР выдан Паспорт Аттестации №222 от 21 февраля 2007 г. Комплекс АРБИТР аттестован сроком на 10 лет и разрешен к применению на объектах Ростехнадзора РФ.

Теоретической основой ПС АРБИТР является Общий логико-вероятностный метод (ОЛВМ) анализа структурно-сложных системных объектов и процессов различных видов, классов и назначения [3-5]. Уникальность данной разработки заключается в следующем:

- В классических логико-вероятностных методах [6] применяется функционально неполный базис операций **И, ИЛИ**, что позволяет строить только монотонные модели надежности и безопасности систем на основе представления их структур с помощью блок-схем, графов связности, деревьев отказов и деревьев событий. В ОЛВМ впервые используется функционально полный базис логических операций **И**, **ИЛИ**, **НЕ**. На этой основе в комплексе АРБИТР впервые реализованы все возможности основного аппарата моделирования алгебры логики, что позволяет автоматически строить как все прежние виды монотонных моделей, так и принципиально новый класс немонотонных моделей надежности, живучести, безопасности и риска функционирования структурно-сложных системных объектов различного назначения.
- В четырех ранее аттестованных программных средствах аналогичного назначения (две версии Risk Spectrum (Швеция) [7], РИСК [8], CRISS 4.0 [9] (РФ)) реализована только технология "деревьев отказов" (ДО). В ПС «АРБИТР» для структурного описания свойств надежности, безопасности и технического риска систем применяется новое графическое средство ОЛВМ – схемы функциональной целостности (СФЦ) [3-5, 10]. С помощью аппарата СФЦ могут представляться как все типовые монотонные структурные модели (блок-схемы, графы связности, деревья отказов, деревья событий), так и новый класс немонотонных структурных моделей надежности и безопасности систем.

- Все комплексы, реализующие технологию ДО, позволяют пользователю применять только один обратный подход для постановки задач анализа надежности и безопасности систем. Этот подход требует от разработчика точного представления и графического описания условий отказа, неработоспособности или возникновения аварии в исследуемой системе. Если система сложная, например, содержит множественные циклические (мостиковые) связи или множественные состояния элементов, то безошибочное построение соответствующего дерева отказов часто превращается в трудно разрешимую проблему [9]. Используемый в комплексе «АРБИТР» графический аппарат СФЦ предоставляет пользователю на выбор три варианта подходов к постановке задач:
  1. традиционный **обратный подход**, в результате которого пользователь разрабатывает СФЦ дерева отказов исследуемой системы;
  2. **прямой подход**, в результате которого пользователь разрабатывает СФЦ блок-схемы [1] работоспособности (безотказности, невозникновения аварии), причем с возможностью неограниченного представления циклических (мостиковых) связей, существующих в системе;
  3. **комбинированный подход** (смешанный), позволяющий строить немонотонные СФЦ надежности, живучести, безопасности и риска функционирования сложных объектов.

  Независимо от того, какой подход использовался при разработке СФЦ, с помощью комплекса АРБИТР далее могут автоматически определяться и кратчайшие пути успешного функционирования (КПУФ), и минимальные сечения отказов (МСО), а так же различные их немонотонные комбинации. Практика показала, что прямой и комбинированный подходы позволяют пользователю разрабатывать более сложные и высокоразмерные структурные схемы систем, с последующим автоматическим определением МСО (т.е. автоматическим построением ДО высокой сложности и большой размерности).
- Все ранее аттестованные программные средства аналогичного назначения (Risk Spectrum, РИСК, CRISS 4.0) позволяют вычислять только приближенные вероятностные показатели надежности и безопасности исследуемых систем, причем при условии задания вероятностей отказов элементов не более 0.01 [6]. Комплекс АРБИТР изначально разрабатывался как инструмент точного моделирования и расчетов вероятностных показателей. Основой точных вычислений является впервые разработанная в ОЛВМ и реализованная в комплексе АРБИТР процедура автоматического построения правильного многочлена расчетной вероятностной функции [10]. Поэтому корректные расчеты вероятностных характеристик АРБИТР впервые выполняет во всем диапазона возможных значений вероятностных параметров элементов от 0 до 1 включительно.
- В комплексе АРБИТР реализован дополнительный (вспомогательный) режим приближенного моделирования и расчета вероятностных показателей. В этом режиме реализована возможность построения "усеченных" логический функций, из которых исключены маловероятные конъюнкции (пути и/или сечения). Приближенные расчеты выполняются по двум методикам: для независимых отказов элементов (аналог методики, используемой в комплексах Risk Spectrum [7] и Saphire-7, США) и с учетом трех типов отказов элементов – "отказ на требование", "отказ в режиме работы" и "скрытый отказ в режиме ожидания", впервые разработанным и реализованным в аттестованном ПС "CRISS 4.0" [9].

Предназначение ПС АРБИТР:

- автоматизированное моделирование и расчет показателей надежности структурно-сложных систем, включая объекты использования атомной энергии (ОИАЭ) и другие опасные производственные объекты (ОПО);
- автоматизированное моделирование и расчет вероятностей возникновения (невозникновения) аварийных ситуаций и аварий опасных производственных объектов, включая ОИАЭ.

Практическое применение ПС АРБИТР основано на новой информационной технологии автоматизированного структурно-логического моделирования (АСМ) [4, 5], которая включает в себя следующие этапы.

1. Формализованная постановка задачи анализа надежности, живучести, безопасности (технического риска) исследуемой структурно-сложной системы осуществляется на основе ее исходной функциональной схемы и описания процесса функционирования. На этом этапе подготавливается структурная модель исследуемого свойства системы в виде, например, блок-схемы, графа связности, дерева отказов, дерева событий. Подготовленная структурная модель представляется в форме СФЦ. Определяются параметры надежности элементов и задаются исследуемые режимы в виде логических критериев функционирования (ЛКФ).
2. После ввода подготовленных формализованных исходных данных в ПС АРБИТР выполняется автоматическое построение математических моделей и расчеты вероятностных показателей исследуемых свойств надежности, живучести или безопасности исследуемой системы. На этом этапе ПС АРБИТР обеспечивает:

- представление в исходной СФЦ (суперграфе) до 400 элементов (вершин) и до 100 элементов в каждой декомпозированной вершине (подграфе) основного графа исследуемой системы;
- автоматическое построение логических функций, представляющих КПУФ, МСО или их немонотонные комбинации (детерминированные модели исследуемых свойств системы);
- автоматическое построение вероятностных функций, обеспечивающих точный расчет показателей надежности, безопасности и технического риска исследуемых систем;
- расчет вероятности реализации заданных ЛКФ безотказности, отказа и технического риска функционирования системы и/или ее отдельных подсистем;
- расчет вероятности безотказной работы или отказа и средние наработки до отказа невосстанавливаемых систем;
- расчет коэффициента готовности/неготовности, средней наработки на отказ, среднего времени восстановления и вероятности безотказной работы/отказа восстанавливаемой системы;
- расчет вероятности готовности смешанной системы, состоящей из восстанавливаемых и невосстанавливаемых элементов;
- расчет значимостей, положительных и отрицательных вкладов всех элементов системы в вероятность реализации заданного ЛКФ;
- приближенный расчет вероятностных показателей (без построения вероятностной функции) с отсечкой или без отсечки малозначимых путей и сечений;
- расчет вероятности реализации отдельных КПУФ или МСО системы;
- расчет значимости и суммарной значимости сечений отказов по Fussell-Vesely;
- расчет значимости, коэффициентов уменьшения и увеличения риска элементов по Fussell-Vesely;
- приближенный расчет вероятностных характеристик системы с учетом трех типов отказов элементов (отказ на требование, отказ в режиме работы и скрытый отказ в режиме ожидания [9]);
- структурный и автоматический учет отказов групп элементов по общей причине (модели альфа-фактора, бета-фактора и множественных греческих букв);
- учет различных видов зависимостей и множественных состояний элементов, представляемых группами несовместных событий (ГНС);
- учет двухуровневой декомпозиции структурной схемы, дизъюнктивных и конъюнктивных кратностей сложных элементов (подсистем);
- учет неограниченного числа циклических (мостиковых) связей между элементами системы;

– учет различных комбинаторных отношений (К из N) между группами элементов и подсистем.

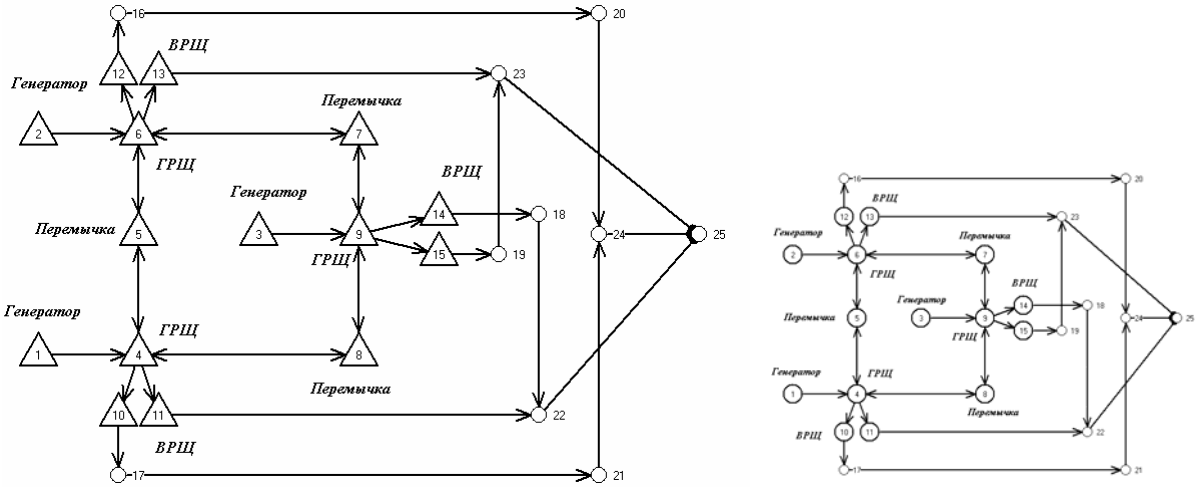
3. На этом завершающем этапе полученные детерминированные (логические) и вероятностные результаты автоматизированного моделирования и расчетов используются для выработки и обоснования управленческих решений в области обеспечения надежности, живучести, безопасности и технического риска исследуемых систем, а также подготовки отчетной документации.

Процедура аттестации ПС АРБИТР

Официальная аттестация проводилась в течение года - с 21 ноября 2005 года по 21 ноября 2006 года. В работе по аттестации приняли участие эксперты из ведущих проектных организаций: СПбАЭП, ВНИИАЭС, АЭП, НТЦ ЯРБ (Москва) и ОКБМ им. И.И.Африкантова (Нижний Новгород). В Отчете о верификации [2], разработанном заявителем, ОАО "СПИК СЗМА", были представлены экспертам 10 расчетно-аналитических Тестов, состоящих из 42 примеров, включающих 184 различные задачи. Тесты представляли следующие классы задач, которые может решать ПС «АРБИТР»:

– вероятностный анализ надежности и возникновения аварийных ситуаций и аварий опасных объектов (Тест №1, 12 задач);
– надежность систем с множественными циклическими (мостиковыми) связями (Тест № 2, Тест №10, 20 задач);
– моделирование и расчет надежности фрагментов ядерных энергетических установок (Тест №3, 9 задач);
– расчет вероятностей вариантов сценария развития аварии (Тест №4, 6 задач);
– вероятностный анализ безопасности систем на основе деревьев отказов (Тест №5, Тест №3, Тест №10, 9 задач);
– типовые и нетиповые модели отказов по общей причине (Тест №6, Тест №7, 68 задач);
– модели надежности комбинаторных подсистем (Тест №8, Тест №4, 14 задач);
– моделирование систем большой размерности (Тест №9, Тест №10, 64 задачи).

В качестве иллюстрации приводятся результаты решения ПС "АРБИТР" следующей тестовой задачи.



а) б)

Рис.1. СФЦ надежности высокоразмерной циклической системы

На рис.1.а изображен суперграф СФЦ известной задачи №35, разработанной основоположником логико-вероятностных методов моделирования академиком Рябининым

И.А. [6]. В данной задаче каждый элемент системы (каждая функциональная вершина 1-15 на рис.1.а) представляет аналогичную по структуре подсистему, подграф СФЦ которой приведен на рис.1.б. Таким образом, вся рассматриваемая система содержит 225 элементов с множественными циклическими связями на разных уровнях декомпозиции. Результаты прямого (безотказность) и обратного (отказ) решения данной тестовой задачи ($p_i = 0.9, i = 1,2,...,225$) приведены в следующей таблице.

ЛКФ системы	Время решения	Оценка полного размера логической ФРС	Надежность системы
Безотказность: y25	1 сек.	КПУФ: 3.49409450070874 E+19	0.886737948063
Отказ: y"25	1 сек.	МСО: 8 621 131	0.113262051937

Несмотря на большие размеры полных логических моделей, вычислить точные значения вероятностных показателей надежности данной системы позволяет реализованный в ПС АРБИТР метод односвязной структурной декомпозиции [3].

Уже в ходе аттестации было выдано задание на решение пяти Контрольных примеров "Моделирования и анализа систем безопасности и ядерной установки при выполнении вероятностного анализа безопасности" (201 стр. исходных данных, 20 задач), ранее решенных с помощью аттестованного комплекса CRISS 4.0 [9]. При выполнении этого задания с помощью ПС АРБИТР были получены и представлены экспертам три вида решений Контрольных примеров:

- приближенные решения всех пяти Контрольных примеров по методике CRISS 4.0 совпали с заданием около 2000 сопоставляемых показателей;
- приближенные решения всех пяти Контрольных примеров по методике Saphire-7 (для независимых отказов элементов) совпали более 2000 сопоставляемых показателей;
- дополнительно, с помощью АРБИТР, впервые были выполнены точные расчеты вероятностей вершинных событий деревьев отказов для трех выданных Контрольных примеров (модели с независимыми отказами элементов).

Контроль правильности решений Тестовых и Контрольных задач, полученных с помощью ПС АРБИТР, осуществлялся экспертами в соответствии с требованиями Положения об аттестации программных средств (РД-03-17-2001) путем сопоставления:

- с аналитическими решениями задач;
- с решениями, приведенными в литературных источниках;
- с решениями, полученными с помощью ранее аттестованных программных средств Risk Spectrum и CRISS 4.0;
- с решениями, полученными с помощью программного комплекса Saphire-7, имеющего лицензию Комиссии ядерного регулирования США;
- с решениями, полученными с помощью программного комплекса RELEX (США), широко используемого во многих странах мира.

В ходе аттестации у экспертов не было ни одного замечания по правильности решений с помощью ПС АРБИТР всех 204 задач расчетно-аналитических Тестов и Контрольных примеров.

Опыт практического использование ПС АРБИТР

Эксплуатация программного комплекса АРБИТР осуществляется рядом организаций, которые имеют лицензии на его применение, в том числе:

- ОАО "СПИК СЗМА", Санкт-Петербург, разработчик ПС АРБИТР; с помощью ПС АРБИТР выполнены проектные расчеты надежности АСУТП опасных производственных объектов: ООО "Киришинефтеоргсинтез", 6 проектов; ООО НПО "МИР", 1 проект; ООО "Мозырский НПЗ", Республика Беларусь, 4 проекта; ОАО "Казаньоргсинтез", Республика Татарстан, 2 проекта.
- "Межотраслевой экспертно-сертификационный, научно-технический и контрольный центр ядерной и радиационной безопасности" (РЭСцентр), Санкт-Петербург, выполнено 13 проектов по расчету показателей надежности, остаточного ресурса и рисков объектов использования атомной энергии ФГУП "ПО Севмаш", г. Северодвинск.
- ЗАО "Компания СЗМА", Санкт-Петербург, выполнен расчет надежности Автоматизированной информационно-измерительной системы коммерческого учета электрической энергии (АИС КУЭ) ФГУП "Петербургский метрополитен".
- ОАО "Гипровостокнефть", г. Самара; выполняются работы по анализу надежности и безопасности систем объектов нефтехимической промышленности.

Стандарты и Руководящие документы, поддерживаемые ПС АРБИТР

1. ГОСТ 24.701-86. Надежность автоматизированных систем управления. Основные положения. М.: ИПК Издательство стандартов, 1986, 17 с.
2. ГОСТ 27.301-95. Надежность в технике. Расчет надежности. Основные положения. М.: ИПК Издательство стандартов, 1996, 15 с.
3. РД 03-418-01. Методические указания по проведению анализа риска опасных производственных объектов. // Нормативные документы межотраслевого применения по вопросам промышленной безопасности и охраны недр. Серия 3. Выпуск 10. М.: Госгортехнадзор России, НТЦ "Промышленная безопасность", 2001, 60 с.
4. ГОСТ Р 51901-2002 (МЭК 60300-3-9:1995). Управление надежностью. Анализ риска технологических систем. М.: ИПК Издательство стандартов, 2002, 22 с.
5. ГОСТ Р 51901.14-2005 (МЭК 61078:1991). Менеджмент риска. Метод структурной схемы надежности. М.: Стандартинформ, 2005, 18 с.
6. ГОСТ Р 51901.13-2005 (МЭК 61025:1990). Менеджмент риска. Анализ дерева неисправностей. М.: Стандартинформ, 2005, 11 с.

Дополнительная информация: http://www.szma.com

В настоящее время ОАО "СПИК СЗМА" и группа компаний приступили к организации совместных работ по развитию и адаптации базовой версии ПС "АРБИТР" к различным специальным предметным областям моделирования и анализа рисков опасных производственных объектов, объектов использования атомной энергии, финансовых рисков и обеспечения учебной и исследовательской деятельности вузов.

Литература

1. АРБИТР, "Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА), базовая версия 1.0". Свидетельство об официальной регистрации № 2003611101. М.: РОСПАТЕНТ РФ, 2003. Аттестационный паспорт №222 от 21 февраля 2006 г., выдан Советом по аттестации программных средств НТЦ ЯРБ Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) РФ.
2. Можаев А.С., Киселев А.В., Струков А.В., Скворцов М.С. Отчет о верификации программного средства "Программный комплекс автоматизированного структурно-

логического моделирования и расчета надежности и безопасности систем" (ПК АСМ СЗМА, базовая версия 1.0, «АРБИТР»). Заключительная редакция. СПб.: ОАО "СПИК СЗМА", 2007. – 498 с.

3. Можаев А.С. Общий логико-вероятностный метод анализа надежности сложных систем. Уч. пос. Л.: ВМА, 1988. - 68с.
4. Можаев А.С. Теория и практика автоматизированного структурно-логического моделирования систем. // Доклады международной конференции по информатике и управлению. (ICI & C') Том 3. СПб.: СПИИРАН, 1997, с.1109-1118. Mozhaev A.S. Theory and practice of automated structural-logical simulation of system. International Conference on Informatics and Control (ICI&C'97). Tom 3. St.Petersburg: SPIIRAS, 1997, p.1109-1118.
5. Можаев А.С. Автоматизированное структурно-логическое моделирование систем. Учебник. СПб: ВМА им Кузнецова Н.Г, 2006. - 590 с.
6. Рябинин И.А. Надежность и безопасность сложных систем. СПб.: Политехника, 2000. -248с.
7. Risk Spectrum PSA Professional 1.20 / Theory Manual. RELCON AB, 1998. - 57p.
8. Код "РИСК" для выполнения стандартных вероятностных расчетов. М.: ОЦРК, http://www.insc.ru/PSA/risk.html.
9. Бахметьев А.М., Былов И.А., Милакова Ю.В. Отчет о научно-исследовательской работе "Верификация и обоснование программы CRISS 4.0 для моделирования и анализа систем безопасности ядерной установки при выполнении вероятностного анализа безопасности". Часть 1 (Заключительная редакция). Нижний Новгород: ФГУП ОКБМ им. И.И.Африкантова, 2005. - 88 с.
10. Можаев А.С., Гладкова И.А. Библиотека программных модулей автоматического построения монотонных и немонотонных логических функций работоспособности систем и многочленов вероятностных функций (ЛОГ&ВФ). Свидетельство об официальной регистрации № 2003611100. М.: РОСПАТЕНТ РФ, 2003.
11. Можаев А.С., Гладкова И.А. Программный комплекс автоматизированного структурно-логического моделирования сложных систем 2001 (ПК АСМ 2001). Свидетельство об официальной регистрации № 2003611099. М.: РОСПАТЕНТ РФ, 2003.
12. Можаев А.С. Универсальный графоаналитический метод, алгоритм и программный модуль построения монотонных и немонотонных логических функций работоспособности систем. // Труды Международной научной школы: "Моделирование и анализ безопасности, риска в сложных системах" (МА БР – 2003). СПб.: СПбГУАП, 2003, с.101-110.
13. Можаев А.С. Программный комплекс автоматизированного структурно-логического моделирования сложных систем (ПК АСМ 2001). // Труды Международной Научной Школы 'Моделирование и анализ безопасности, риска и качества в сложных системах' (МА БРК – 2001). СПб.: Издательство ООО 'НПО 'Омега', 2001, с.56-61.
14. Можаев А.С. Программные средства автоматизированного моделирования и оценки надежности и безопасности АСУТП на стадии проектирования. // Электронный научно-технический журнал "Промышленная безопасность труда", №6, 2003, http://www.alf-center.com/pbt/magazine6/mozhaev.shtml .
15. Можаев А.С. Технология и программный комплекс автоматизированного моделирования и оценки надежности, безопасности и риска опасных производственных объектов. // Пятый тематический семинар: "Об опыте декларирования промышленной безопасности и страхования ответственности. Развитие методов оценки риска аварий на опасных производственных объектах". М.: Федеральная служба по экологическому, технологическому и атомному надзору. НТЦ "Промышленная безопасность", 2004, с.50-58.
16. Можаев А.С. Сравнительный анализ технологий деревьев отказов и автоматизированного структурно-логического моделирования, используемых для выполнения работ по вероятностному анализу безопасности АЭС и АСУТП на стадии проектирования. // Доклад на девятом научном семинаре "Программные средства в области анализа техногенного риска" в Учебно-методическом центре ФГУП НТЦ "Промышленная безопасность" при

Ростехнадзоре РФ. Аннотация опубликована в журнале " Безопасность труда в промышленности", №12, 2005, с.61-63.

17. Ш.В.Камынов, М.И.Рылов, А.С.Можаев, А.А.Нозик. Методика применения программного комплекса АСМ СЗМА для расчета показателей безотказности и безаварийности стенда физических измерений. // Журнал "Управление риском". М.: издательство "АНКИЛ", 2007. – 22с.