УДК 004.51

Б.М. КОНОРЕВ[1], Ю.Г. АЛЕКСЕЕВ[1], В.В. СЕРГИЕНКО[1], В.С. ХАРЧЕНКО[2], Г.Н. ЧЕРТКОВ[1]

[1] *Сертификационный центр АСУ Госцентркачества, Украина*
[2] *Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина*

ЦЕЛЕВАЯ ТЕХНОЛОГИЯ РЕНТАБЕЛЬНОЙ ОЦЕНКИ НАДЕЖНОСТИ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Предложена целевая технология рентабельной оценки надежности и функциональной безопасности критического программного обеспечения (ПО): в процессе независимой верификации и квалификации ПО ИУС критического применения.

гарантоспособность, функциональная безопасность, критическое программное обеспечение

Введение

ИУС являются ключевым фактором обеспечения важнейших характеристик гарантоспособности (надежности, готовности, обслуживаемости) и функциональной безопасности проектов, реализуемых в критических сферах, таких, как атомная энергетика, космическая деятельность.

Уровень критичности ИУС определяется тяжестью последствий аномального функционирования в диапазоне <материальные потери – ущерб окружающей среде – угроза здоровью и жизни людей> с учетом вероятности их наступления. В этих сферах наблюдается устойчивая тенденция роста объемов программно-реализуемых и программно-поддерживаемых критических функций ИУС. В силу этого возрастает зависимость безопасности использования ИУС непосредственно от качества критического ПО. Остаточные (не выявленные на этапах испытаний) дефекты ПО являются факторами риска аномального функционирования ИУС и возникновения аварийных ситуаций. Это обуславливает статус критического ПО, как важного элемента нормативного регулирования, определяющего гарантоспособность и функциональную безопасность ИУС в целом.

Базовой процедурой, реализуемой в контурах нормативного регулирования и разрешительной деятельности, являются квалификационные испытания ИУС [1]. Одна из главных целей квалификации заключается в рентабельной оценке величин рисков аномального функционирования ИУС, связанных с остаточными дефектами критического ПО. Данная статья представляет собой обзор работ [2 – 12], связанных с созданием нормативной и инструментальной баз для критического ПО космических систем, а также других критических приложений, в частности, ИУС АЭС.

Концепция

Подход к решению этой задачи состоит в разработке целевой технологии рентабельной оценки гарантоспособности (безопасности, готовности, обслуживаемости) и функциональной безопасности критического ПО. Достоверность или степень неопределенности оценок указанных характеристик качества критического ПО определяет величины рисков аномального функционирования ИУС, обусловленные вероятностью остаточных дефектов ПО.

Концепцией целевой технологии является независимая верификация критического ПО с использованием усовершенствованной методологии статического анализа исходного ПО ИУС, которая заключается в обеспечении объективных инструментальных измерений семантических, интервально-точностных и логических инвариантов ПО.

Инварианты представляют первичные атрибуты (свойства) ПО, остающиеся неизменными в течение жизненного цикла ПО. Это позволяет решить проблему выбора метрик и критериев оценки результатов измерения инвариантов при тестировании исходного ПО в режиме статического анализа.

На этой основе оцениваются значения и степень неопределенности обобщенных характеристик гарантоспособности (надежности, готовности, обслуживаемости) и функциональной безопасности критического ПО.

Функциональная безопасность ИУС критического применения трактуется как нахождение системы в условиях проектного риска аномального функционирования в течение установленного срока эксплуатации.

Рентабельность оценки характеристик гарантоспособности и функциональной безопасности критического ПО означает достижение приемлемых прогнозируемых уровней рисков, связанных с остаточными дефектами ПО, при допустимых (минимальных) затратах ресурсов.

Актуальность

Большинством международных общепромышленных и отраслевых стандартов в сферах атомной энергетики и космической деятельности рекомендуется использование при проектировании и квалификации ИУС критического применения фундаментальных практик, обеспечивающих в совокупности анализ и оценку критичности возможных дефектов, прогнозирование и управление величиной связанных с ними рисков аномального функционирования и возникновения аварийных ситуаций.

Базовый набор фундаментальных метрик включает: PHA (предварительный анализ рисков), FMECA (анализ видов и критичности отказов), FTA (анализ дерева отказов), HSIA (анализ взаимодействия ПО и оборудования), HAZOP (анализ операционных рисков), CCFA (анализ отказов по общей причине).

Для случая ИУС критического применения с интенсивным использованием ПО соответствующие метрики для анализа и оценок ПО должны быть совместимы и интегрированы в фундаментальные практики системного уровня. При этом следует учитывать, что многие риски аномального функционирования ИУС могут быть вызваны комбинациями дефектов ПО с отказами оборудования или ошибками персонала, которые могут быть обнаружены при квалификационных испытаниях опосредованно через измерение атрибутов критического ПО. Кроме того, для ИУС, начиная с некоторого класса безопасности, строго рекомендуемым требованием является проведение независимой верификации критического ПО. Средством решения этих задач является презентуемая целевая технология рентабельной оценки характеристик гарантоспособности и функциональной безопасности ПО ИУС критического применения, обеспечивающая:

- независимую верификацию на основе усовершенствованной методологии статического анализа исходного ПО, обеспечивающую повышение достоверности оценок характеристик ПО и прогнозирование рисков аномального функционирования из-за остаточных дефектов ПО;
- интегрированную инструментальную поддержку сценария независимой верификации критического ПО на аналитическом, информационном и организационном уровнях;
- рентабельную оценку и прогнозирование рисков, связанных с остаточными дефектами критического ПО.

Именно такая целевая технология определяет реальные возможности организаций-разработчиков и регулирующих органов в проведении рентабельных оценок гарантоспособности и функциональной безопасности критического ПО при независимой верификации, квалификации, сертификации в рамках risk-informed подходов к регулированию безопасности в критических сферах технической деятельности.

Описание

Целевая технология рентабельной оценки гарантоспособности и функциональной безопасности ПО

ИУС критического применения основана на использовании усовершенствованной методологии статического анализа исходного ПО для независимой верификации и квалификации критического ПО. Руководящей идеей усовершенствования является измерение семантических, интервально-точностных и логических инвариантов, представляющих неизменные для всех условий использования атрибуты (физические или абстрактные свойства) ПО [11]. Реализация подхода на процедурном уровне выглядит следующим образом:

- формируется инструментированная версия исходного ПО, в которой определены контрольные точки или зонды, содержащие информацию, обеспечивающую реализацию алгебры контроля семантического, интервально-точностного и логического инвариантов ПО. В общем случае контрольные точки покрывают все переменные ПО. Инструментированная версия исходного ПО представляет оценочную модель;
- измеряются значения инвариантов в конечных и промежуточных контрольных точках для всех реально реализованных в ПО цепочках операторных отображений в режиме рекурсивной (до исчерпания множественности связей переменных на всех уровнях иерархии структуры ПО) интерпретации оценочной модели ПО;
- оцениваются траектории изменения значений семантических, интервально-точностных и логических векторов переменных для реально реализованных в ПО множеств цепочек операторных отображений. Искажение значения инварианта является признаком (критерием) наличия дефекта (ошибки) ПО. Для случая сохранения значения инварианта в общем случае требуется дополнительный анализ чувствительности и полноты тестового покрытия реализованной композиции диверсных методов измерения инвариантов;
- формируется интегральные оценки инвариантов и основанные на них метрики гарантоспособности и функциональной безопасности критического ПО;
- оценивается полнота тестового покрытия исходного ПО при измерении инвариантов, степень неопределенности измерений инвариантов и уровни рисков аномального функционирования ИУС, связанных с остаточным дефектами ПО;
- оценивается рентабельность достижения допустимых величин рисков аномального функционирования ИУС при приемлемых (минимальных) затратах ресурсов.

Нормативная база

Реализация целевой технологии рентабельной оценки характеристик качества ПО ИУС критического применения основана на использовании нормативных профилей, гармонизированных с международными стандартами общепромышленного назначения:

IEC 61508, IEC 60815, IEC 61025, ISO/IEC 12207, ISO/IEC 9126, ISO/IEC 14598, ISO/IEC 15504, ISO/IEC 25 000TR и международными отраслевыми стандартами:

а) для атомной энергетики:

IEC 1226, IEC 60880 1,2; IAEA NS-G 1.1, IAEA TR No 384;

б) для космической отрасли:

ECSS – E40, ECSS-Q-30, 40, 80 –xx; ESA PSS 05-xx.

Сценарий

Полный сценарий рентабельной оценки критического ПО включает три базовых концепт–методики:

- нормализация проекта ПО;
- измерение инвариантов;
- обобщенная рентабельная оценка гарантоспособности и функциональной безопасности.

Функциональная IDEF0 – модель сценария представлена на рис. 1.

В соответствии с IDEF0 – аксиоматикой на модели для каждой концепт-методики, представленной прямоугольником, определены входные и выходные данные (левая и правая грани), механизмы выполнения с использованием компьютеризированных процедур – утилит (нижняя грань), средства управления

выполнением и ограничения (верхняя грань).

Дерево узлов 0-1-2 уровней детализированной IDEF0 модели сценария представлено на рис. 2.

Концепт-методика «Нормализация оцениваемого проекта критического ПО» предусматривает выполнение следующих заданий [4]:

- формирование и верификация нормативного профиля требований для оцениваемого проекта;
- раскрытие спецификаций измеряемых атрибутов проекта ПО и формирование опорной модели (схемы измерений – атрибутов ПО);
- исчерпывающая (прямая и инверсная) трассировка дизъюнктов (элементов) ссылочной модели и технической документации проекта ПО, включающей нормативный профиль проекта ПО, требования к ПО (ТЗ), файлы проектных определений и проектных обоснований;
- верификация опорной модели (схемы измерений атрибутов ПО);
- оценка полноты тестового покрытия проекта ПО при независимой верификации и квалификации.

Формирование нормативного профиля проекта ПО производится на основе таксономии ISO 10 000 TR с использованием процедур скрининга и гармонизации дизъюнктов (clause) ссылочной профилеобразующей базы, включающей актуальные международные стандарты общепромышленного назначения (серии ISO/IEC), международные отраслевые стандарты (серии стандартов IAEA, ECSS) и соответствующие стандарты и нормативы национальных систем стандартизации [1, 2].

Конечными целями концепт-методики «Нормализации проекта ПО» являются:

- формирование и верификация схемы измерений (оценочной модели) проекта ПО, определяющей полную спецификацию измеряемых атрибутов и соответствующих им метрик (методы + шкалы измерений);
- оценка полноты тестового покрытия проекта ПО.

Концепт-методика «Измерение инвариантов в режиме статического анализа исходного кода ПО» предусматривает выполнение следующих заданий [11]:

- инструментирование исходного ПО – формирование оценочной модели (с определением контрольных точек – зондов для измерения инвариантов);
- измерение семантических, интервально-точностных и логических инвариантов в режиме интерпретации инструментированной версии исходного ПО – оценочной модели;
- обработка результатов измерения инвариантов ПО и диагностирование дефектов ПО.

Инварианты ПО представляют атрибуты ПО остающиеся неизменными для всех условий эксплуатации ИУС. Это свойство позволяет радикально решить проблему установления критериев оценки результатов тестирования при статическом анализе ПО.

Результаты измерений инвариантов представлены системами линейных уравнений и неравенств, описывающих траектории инвариантов для фактически реализованных в оцениваемом проекте цепочек операторных отображений на всех уровнях архитектуры проекта.

Обработка результатов статического анализа и диагностика дефектов ПО заключается в решении систем линейных уравнений и неравенств с использованием процедур логического вывода и восстановления пропущенных значений инвариантов.

Концепт-методика «Интегральная оценка ПО» предусматривает выполнение следующих заданий [5, 6, 12]:

- Диверсификация методов измерения различных категорий инвариантов ПО и калибровка их чувствительности и степени разнообразия.
- Оценка степени неопределенности измерения инвариантов и прогнозирование рисков аномального функционирования ИУС, связанных с остаточными дефектами ПО.
- Свертка радиально-метрических диаграмм всех уровней и формирование интегральной оценки характеристик гарантоспособности и функциональной безопасности.

Цель диверсификации методов измерения инвариантов заключается в повышении достоверности оценки характеристик ПО.

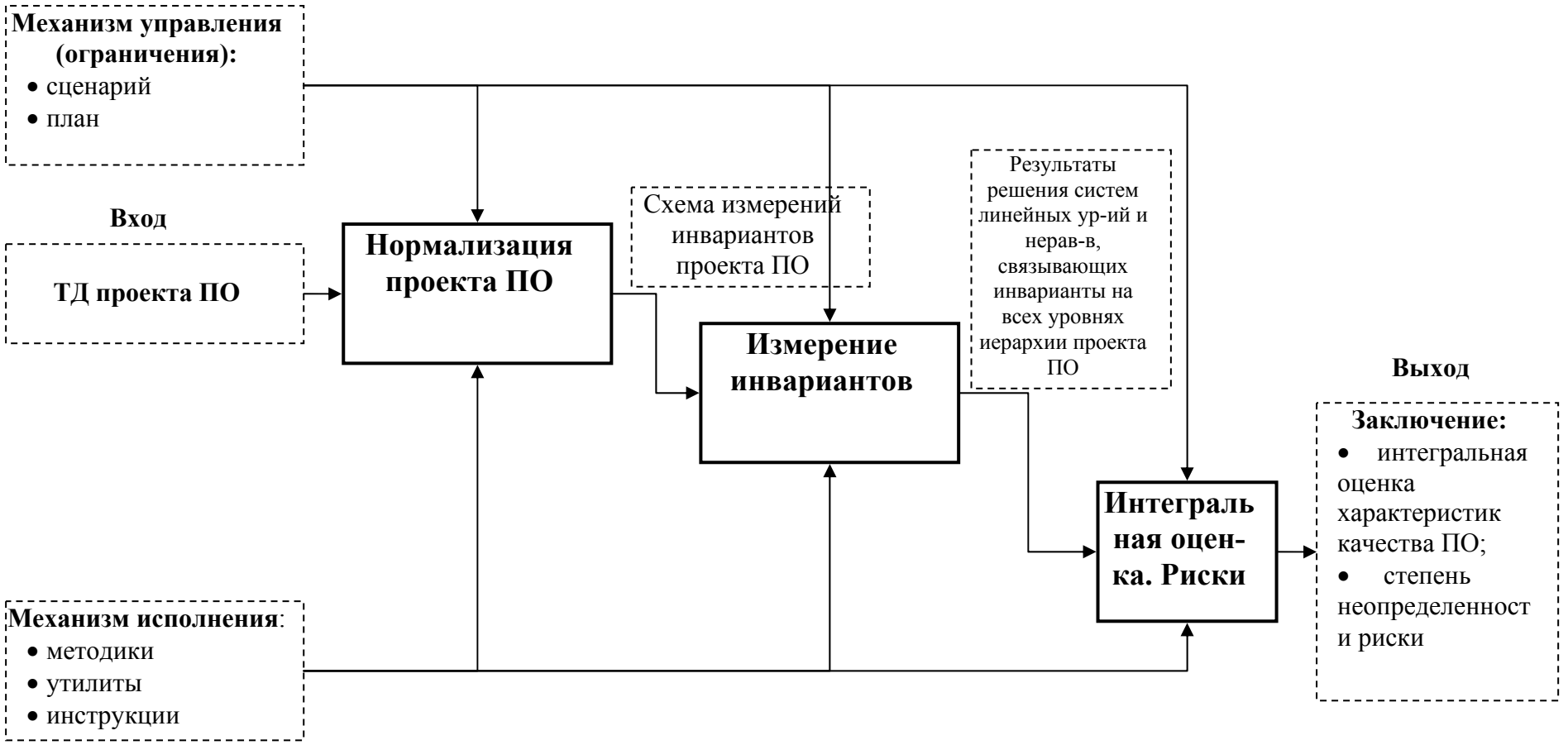

Рис. 1. Функциональная IDEF0 – модель сценария оценки критического ПО при независимой верификации и квалификации

Рис. 2. Декомпозиция функциональной IDEF0 – модели сценария целевой технологии. Дерево узлов 0-1-2 уровней

Калибровка представляет экспериментальное определение методом «посева» дефектов ПО в соответствии с установленным профилем дефектов чувствительности и степени разнообразия диверсных методов измерения инвариантов ПО с учетом специфики конкретного (оцениваемого) проекта ПО [10].

Используется усовершенствованный метод капельной инъекции для «посева» тестовых дефектов ПО в соответствии с устанавливаемыми профилями. Использование метода капельной инъекции позволяет исключить эффекты «интерференции» и «мутации» дефектов в адресном поле ПО в процессе калибровок.

Итоговая оценка степени неопределенности измерений инвариантов производится по индикатору, выражающему уменьшение вероятности остаточных дефектов в оцениваемом проекте в диапазоне 0 – 100%(теоретически в пределе на 100% с учетом типа критического ПО и при выполнении определенных условий) для композиции диверсных методов измерения инвариантов при установленном уровне рентабельности.

Итоговая интегральная оценка характеристик качества критического ПО производится с использованием процедур свертки радиально-метрических диаграмм (Kiviat-diagrams), отражающих реализацию установленной схемы измерений атрибутов и оценки характеристик гарантоспособности и функциональной безопасности оцениваемого проекта ПО [1, 6, 12]. Полная спецификация заданий целевой технологии рентабельности оценивания критического ПО представлена деревом узлов функциональной IDEF0- модели для 0-1-2 уровней иерархии на рис.2.

Подход к реализации комплексов утилит интегрированной инструментальной среды поддержки целевой технологии**:**

1. Использование parser (Gold Parser – Free SW) с механизмом настройки- адаптации на синтаксис актуальных языков программирования (C, C++, C#, Java, VHDL) для статического разбора исходного ПО и формирования инструментированной версии ПО обеспечивающей измерение инвариантов.

2. Построение графического пользовательского GUI интерфейса комплексов утилит интегрированной инструментальной среды с использованием модели однодокументного интерфейса SDI (Single-Document-Intreface).

3. Реализация комплексов утилит в форме программируемых Web – приложений (сервисов) на основе современных стандартов Internet.

4. Визуализация всех стадий оценки с помощью Kiviat диаграмм (иерархия радиальных метрических диаграмм) и процедур свертки РМД.

Базовые решения целевой технологии защищены 2 патентами.

Нововведения и преимущества

В рамках целевой технологии рентабельной оценки гарантоспособности и функциональной безопасности критического ПО реализованы следующие нововведения:

1. Независимая верификация критического ПО на основе усовершенствованной методологии статического анализа исходного ПО. Усовершенствования заключаются в обеспечении объективных инструментальных измерений семантических, интервально-точностных и логических инвариантов первичных атрибутов ПО в режиме статического анализа и оценке на их основе характеристик гарантоспособности и функциональной безопасности ПО.

2. Повышение достоверности оценок характеристик ПО за счет диверсификации методов измерения инвариантов и количественной оценки степени неопределенности оценок для композиции диверсных методов измерения инвариантов, представляющей риски аномального функционирования ИУС критического применения из-за остаточных дефектов.

3. Экспериментальная калибровка чувствительности и степени разнообразия диверсных измерения инвариантов в контексте конкретного проекта ПО методом «посева» дефектов ПО в соответствии с устанавливаемым профилям дефектов.

4. Использование усовершенствованного метода «посева» – капельной инъекции дефектов, исклю-

чающей эффекты «интерференции» и «мутации» тестовых дефектов при посеве в адресном поле ПО.

5. Исчерпывающая (прямая и инверсная) трассировка «Спецификации инвариантов ПО» с дизъюнктами (элементами) «Спецификации требований к ПО (ТЗ)», «Нормативного профиля проекта», «Спецификации проектных определений и обоснований (ТД проекта)» и оценка на этой основе полноты тестового покрытия критического ПО при независимой верификации и квалификационных испытаниях.

6. Для достижения приемлемой рентабельности оценки критического ПО используется:

а) итеративная процедура, управляемая параметрами <тип инварианта ПО> – <профиль дефектов ПО>, основанная на диверсификации и экспериментальной калибровке чувствительности и степени разнообразия диверсных методов измерения инвариантов в контексте оцениваемого проекта;

б) индикатор снижения прогнозируемых рисков аномального функционирования ИУС из-за дефектов ПО для композиции диверсных методов измерения инвариантов и учет затрат ресурсов для реализации сценария оценки;

в) нормирование удельных затрат ресурсов для реализации различных вариантов сценария оценки критического ПО с использованием целевой технологии и оценка рентабельности достижения приемлемых прогнозируемых уровней рисков, связанных с остаточными дефектами критического ПО, при допустимых (минимальных) затратах ресурсов.

Заключение

1. Предложенная целевая технология определяет реальные возможности организаций – разработчиков и регулирующих органов в прогнозировании рисков аномального функционирования ИУС из-за дефектов ПО и проведении рентабельных оценок гарантоспособности и функциональной безопасности критического ПО при независимой верификации, квалификации и сертификации критического ПО в рамках risk-informed подходов к регулированию безопасности в критических сферах технической деятельности (таких как атомная энергетика, космическая техника и т.п.).

2. Проект целевой технологии рентабельной оценки гарантоспособности и функциональной безопасности критического ПО соответствует передовому мировому научно-техническому уровню и общей политике МАГАТЭ и ECSS в сфере рентабельной оценки качества при квалификации критического ПО.

3. Целевая технология создает возможности в рамках risk-informed подходов к регулированию безопасности АЭС и элементов космических комплексов количественно оценивать и управлять индикатором снижения вероятности остаточных дефектов критического ПО ИУС и, соответственно, связанных с ними рисков аномального функционирования ИУС в диапазоне 0 – 100% (в пределе теоретически на 100% при выполнении определенных условий с учетом типа критического ПО) для композиции диверсных технологий верификации при независимой верификации и квалификации критического ПО.

4. Стадия разработки: разработан теоретический базис и доступные для тестирования прототипы комплексов утилит интегрированной инструментальной среды поддержки целевой технологии.

Техническая реализуемость утилит и готовность к полномасштабной разработке подтверждена интеграционными лабораторными тестами с использованием реальных объектов экспертизы – ИУС критического применения АЭС на языке C/C++.

Ключевые решения целевой технологии защищены 2 патентами.

Литература

1. Конорев Б.М., Харченко В.С., Чертков Г.Н. Концепция и принципы реализации интегрированной инструментальной системы для поддержки экспертизы и независимой верификации критического программного обеспечения. – Х.: Государственный комитет ядерного регулирования Украины, Государственный центр регулирования качества поставок и

услуг, Сертификационный центр АСУ, 2003. – 60 с.

2. Конорев Б., д-р техн. наук (керівник розробки), Алексеєв Ю. (відповідальний виконавець), Харченко В., д-р техн. наук, Чертков Г., Сергієнко В. та ін. Вимоги до якості програмного забезпечення програмно-технічних комплексів критичного призначення // СОУ-Н НКАУ 0012:2006. Галузева система управління якістю. Видання офіційне, 2006р., 118 стор.

3. Конорев Б.М., Алексеев Ю.Г., Засуха С.А., Манжос Ю.С., Семенов Л.П., Сергиенко В.В., Харченко В.С., Чертков Г.Н. Модель оценивания качества ПО ИУС критического применения на основе инвариантов // Радіоелектронні і комп'ютерні системи. – 2006. – № 7. – С. 162-170.

4. Конорев Б.М., Сергиенко В.В., Чертков Г.Н. Оценивание качества ПО ИУС критического применения: нормализованное представление объекта экспертизы // Системы контроля и управления технологическими процессами: Сб. научных статей. – Луганск: Світлиця, 2006. – С. 385-390.

5. Конорев Б.М., Засуха С.А., Семенов Л.П., Харченко В.С., Чертков Г.Н. Методология оценки качества и функциональной безопасности критического программного обеспечения элементов космических систем // Сучасні тренажерно-навчальні комплекси та системи: Збірка наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – 2006. – Т. 2. – С. 85-89.

6. Конорев Б.М., Алексеев Ю.Г., Брюханков С.С., Манжос Ю.С., Сергиенко В.В., Харченко В.С., Чертков Г.Н. Теоретический базис и инженерные решения рентабельной оценки качества критического программного обеспечения // Материалы Международной научно-практической конференции по проблемам атомной энергетики «Эффективность, Безопасность, Ресурс АЭС» МНПК ПАЭ-5. Сб. научных трудов СНУЯЕ-иП – Севастополь-Батилиман. – 21-26 сентября 2006. – С. 322-324.

7. Конорев Б.М., Манжос Ю.С., Харченко В.С. и др. Семантический метод независимой верификации программного обеспечения информационно-управляющих систем важных для безопасности АЭС // Межд. симпозиум «Измерения, важные для безопасности в реакторах». – Москва.– 25-27 ноября 2003. – С. 10.

8. Конорев Б.М., Харченко В.С., Чертков Г.Н., Алексеев Ю.Г., Манжос Ю.С. Методология и интегрированная инструментальная среда поддержки экспертизы и независимой верификации программного обеспечения ИУС // Межд. симпозиум «Измерения, важные для безопасности в реакторах». – Москва. – 25-27 ноября 2003. – С. 12.

9. Конорев Б.М., Алексеев Ю.Г., Манжос Ю.С. и др. Риск-ориентированный подход к оценке качества ПО ИУС важных для безопасности АЭС с учетом независимой верификации // Межд. симпозиум «Измерения, важные для безопасности в реакторах». – Москва. – 23-25 ноября 2004. – С. 15-16.

10. Конорев Б.М., Алексеев Ю.Г., Клименко Т.А., Манжос Ю.С., Петрик В.Л., Сергиенко В.В., Харченко В.С., Чертков Г.Н. Калибровка чувствительности методов статического анализа, используемых для оценки качества и безопасности ПО ИУС АЭС // Межд. симпозиум «Измерения, важные для безопасности в реакторах». – Москва. – 23-25 ноября 2004. – С. 35-36.

11. Методики статического анализа сохранности программных инвариантов. – Х.: Государственный комитет ядерного регулирования Украины, Государственный центр регулирования качества поставок и услуг, Сертификационный центр АСУ, 2005. – 32 с.

12. Конорев Б., д-р техн. наук (керівник розробки), Алексеєв Ю. (відповідальний виконавець), Харченко В., д-р техн. наук, Чертков Г. и др. Методи оцінки показників якості програмного забезпечення програмно-технічних комплексів критичного призначення. // Пр. СОУ-Н НКАУ 0031:XXXX. Галузева система управління якістю. Видання офіційне, 2007. – 128 с.

Поступила в редакцию 27.02.2007

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