УДК 004.052.42

Б.М. КОНОРЕВ[1], С.А. ЗАСУХА[2], Ю.С. МАНЖОС[1], Л.П. СЕМЕНОВ[2], В.В. СЕРГИЕНКО[1], В.С. ХАРЧЕНКО[3], Г.Н. ЧЕРТКОВ[1]

[1]*Сертификационный центр АСУ Госцентркачества Государственного комитета ядерного регулирования Украины, Харьков, Украина*
[2]*Национальное космическое агентство Украины, Киев, Украина*
[3] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*

МОДЕЛЬ ОЦЕНИВАНИЯ КАЧЕСТВА ПРОГРАМНОГО ОБЕСПЕЧЕНИЯ ИУС КРИТИЧЕСКОГО ПРИМЕНЕНИЯ НА ОСНОВЕ ИНВАРИАНТОВ

Предложенный подход создает возможности в рамках risk-informed регулирования безопасности АЭС количественно оценивать и управлять величиной снижения вероятности рисков остаточных дефектов программного обеспечения (ПО) ИУС для композиции диверсных технологий верификации на основе экспериментальной калибровки чувствительности и реальной степени разнообразия диверсных методов верификации.

программное обеспечение, оценивание, безопасность, статический анализ

Введение. Проблема оценки качества критического ПО

Актуальность проблемы. ИУС – ключевой фактор обеспечения безопасности АЭС в долгосрочных программах развития атомной энергетики. Наблюдается устойчивая тенденция – рост объемов программно-реализуемых и программно-поддерживаемых критических функций ИУС АЭС, таким образом безопасное использование ИУС непосредственно зависит от качества ПО и остаточные дефекты ПО являются факторами риска аномального поведения ИУС и возникновения аварийных ситуаций. Следовательно, ПО является важным элементом нормативного регулирования качества и безопасности ИУС критического применения [1].

Нормативно-методическое и инструментальное оснащение процессов экспертизы ПО ИУС решающим образом определяет реальные возможности обеспечения необходимого уровня безопасности и качества ИУС в целом, в т.ч. в рамках risk-informed подходов к регулированию безопасности [2].

Развитие этого подхода реализуется [3, 4]:

– в теоретическом плане – в совершенствовании методологии и процедур оценки соответствия ПО предъявляемым требованиям с учетом рисков сохранения невыявленных дефектов ПО;

– в практическом отношении – в разработке и внедрении комплексов утилит, обеспечивающих реальное снижение таких рисков.

В то же время существующая практика экспертизы: значительная степень субъективизма, недостаточная полнота и достоверность, высокая трудоемкость экспертных оценок соответствия ПО ИУС регулирующим требованиям.

Основным направлением повышения достоверности оценок качества ПО ИУС является диверсификация технологий верификации.

Цель и задачи повышения качества экспертизы ПО:

– повышение качества экспертизы соответствия ПО ИУС регулирующим требованиям на основе диверсификации технологий верификации по показателям: достоверность, полнота, трудоемкость;

– уменьшение рисков аварийных ситуаций, связанных с остаточными дефектами ПО ИУС критического применения;

– создание нормативно-методического и

инструментального оснащения испытательных лабораторий, выполняющих экспертизу и независимую верификацию ПО ИУС критического применения;

– профилирование регулирующих нормативных требований к ПО в рамках ЖЦ ИУС критического применения;

– диверсификация технологий верификации; модели и методы оценки качества ПО ИУС для композиции диверсных технологий верификации;

– концепция, технические требования и разработка утилит статического анализа как основы инструментального оснащения испытательных лабораторий и организаций-разработчиков;

– реализация процедур инструментирования исходного ПО, измерения атрибутов (инвариантов), калибровки чувствительности к дефектам ПО различных типов и степени разнообразия методов верификации.

В данной статье приведены результаты решения этих задач для двух основных сфер применения:

– независимая верификация ПО, выполняемая организациями-разработчиками на различных этапах жизненного цикла ПО ИУС критического применения;

– экспертиза, сертификация и лицензирование ПО ИУС критического применения в контурах Государственного регулирования безопасности, качества поставок и услуг.

Нормативное регулирование качества и безопасности ПО ИУС

Высококачественное экспертное заключение о соответствии ПО ИУС критического применения предъявляемым требованиям, на основе адекватных нормативных профилей требований, является ключевым элементом нормативного регулирования качества и безопасности в атомной энергетике и других прикладных областях.

Главные показатели качества экспертного заключения – достоверность, полнота, стоимость – должны в полной мере соответствовать социально допустимому риску.

Качество экспертного заключения о соответствии ПО нормативным профилям решающим образом определяет эффективность (результативность) функционирования контуров Государственного регулирования и разрешительной деятельности в сферах критического применения ИУС.

Необходимым условием достижения высокого качества экспертных заключений является наличие адекватного нормативно-методического обеспечения и широкомасштабное использование инструментальных средств поддержки процессов экспертизы, включающих средства (утилиты) объективного анализа и оценки характеристик качества ПО ИУС. В совокупности это означает наличие развитой (эффективной) системы управления качеством испытательных лабораторий, выполняющих экспертизу и независимую верификацию ПО ИУС критического применения.

Таким образом, процессы нормативного регулирования и собственно экспертизы являются неотъемлемой частью глобального жизненного цикла и независимой верификации ПО.

Профилирование нормативных требований. Структура нормативного профиля ПО ИУС критического применения. Скрининг-технология

Наличие адекватных нормативных профилей требований к ПО является необходимым условием обеспечения безопасной эксплуатации ИУС в целом на объектах атомной энергетики.

Нормативные профили (НП) различных статусов утверждения представляют спецификации регулирующих требований к качеству ПО и прежде всего к функциональной безопасности с учетом сферы применения, фазы жизненного цикла и особенностей конкретного проекта.

НП – это выверенные знания, подтвержденные многолетним опытом мирового сообщества в сферах

разработки и эксплуатации сложных технических систем и технологий критического использования.

Разработка НП, гармонизированных с требованиями международных отраслевых стандартов (IAEA), международных общепромышленных стандартов (ISO/IEC) и национальных стандартов, представляет сложно-протекающий процесс, выполняемый уполномоченными международными или национальными организациями.

Проблемы и противоречия:

– слабоструктурированная и слабоформализованная область деятельности, велико влияние человеческого фактора (субъективизм);

– необходимость обеспечить возможно более полный учет имеющихся на период разработки опыта и знаний в конкретных прикладных областях;

– значительная трудоемкость и продолжительность разработки НП.

Предлагаемая общая схема разработки НП различных статусов утверждения включает (рис. 1):

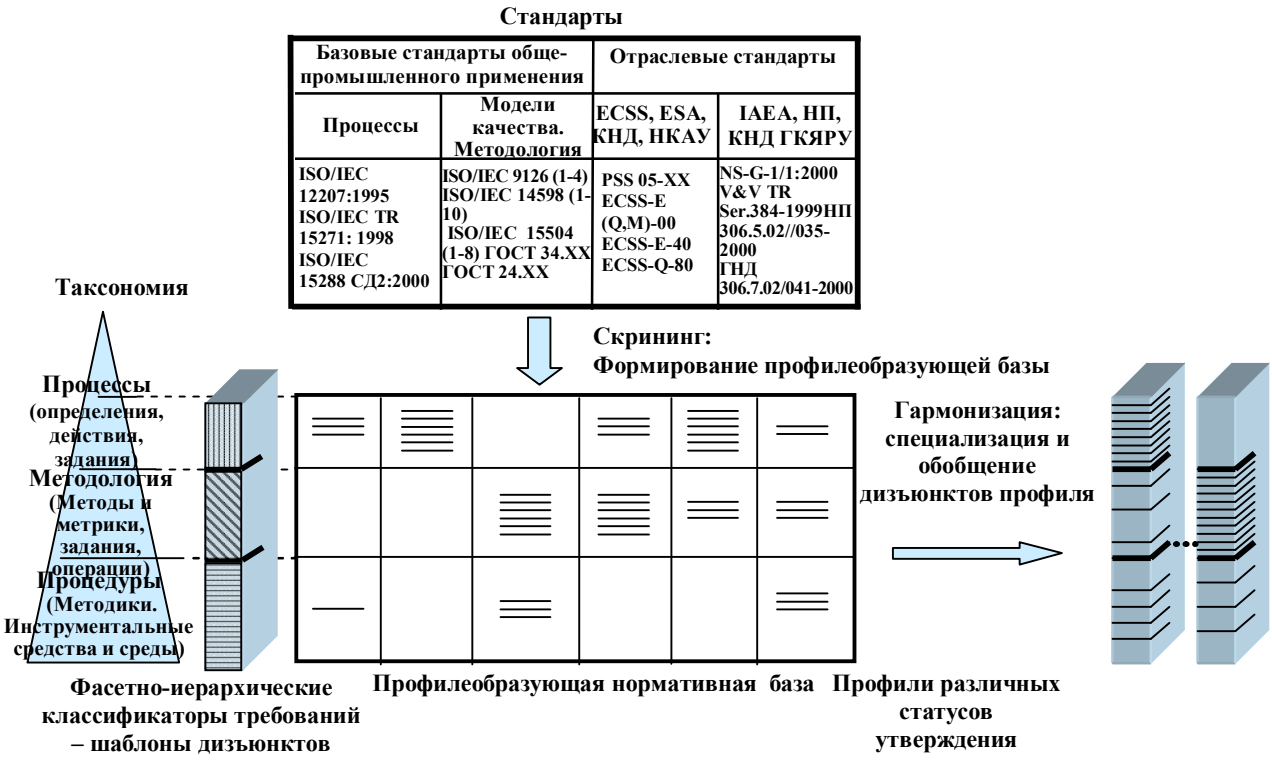


Рис. 1. Профилирование нормативных требований. Скрининг-технология

– формирование профилеобразующей (ссылочной) базы;

– формирование фасетно-иерархических классификаторов требований к конкретному проекту ПО и разработка на их основе шаблонов-дизъюнктов (статей) профилеобразующей базы;

– формирование препарированной профилеобразующей базы с использованием скрининг-технологии (просеивания) в соответствии с таксономией (классификационной схемой) стандартов в области программной инженерии и информационных технологий;

– гармонизацию препарированной профилеобразующей базы с использованием процедур анализа, специализации и обобщения дизъюнктов (статей) требований стандартов и формирование соответствующего НП.

Она реализуется с помощью специальной, относительно автономной утилиты профилирования, включающей базу данных

стандартов – исходных нормативных профилей и специальные средства их профилирования, синтеза и верификации адекватных проекту ПО ИУС.

Оценка качества ПО в течение жизненного цикла ИУС критического применения

ИУС критического применения в атомной энергетике и других прикладных областях представляет специфический комплексный (комбинированный) весьма наукоемкий вид продукции. Комбинация оборудования, программного обеспечения и человеческого фактора (людей) поднимает сложность создаваемых систем до беспрецедентного уровня. Главными критериями оценки качества таких систем являются безопасность применения и интегральная полезность. Социальная значимость несоответствующего (недостаточного) качества определяется рисками в диапазоне «материальные потери – нанесение вреда окружающей среде – угроза здоровью и жизни людей».

ПО, представляющее программно-реализуемые и программно-поддерживаемые функции ИУС, является важным элементом, определяющим функциональную безопасность ИУС в целом. Это обуславливает необходимость измерения и оценивания качества ПО в течение всего жизненного цикла ИУС. Базовыми этапами ЖЦ ИУС критического применения являются:

– разработка и предварительные испытания;

– квалификационные испытания (валидация, сертификация, лицензирование);

– приемка в опытную эксплуатацию и промышленную эксплуатацию;

– сопровождение и модернизация.

Общая схема (номенклатура) испытаний ПО в течение ЖЦ ИУС представляется в виде «расщепленной», эволюционной V-модели, учитывающей испытания и независимую верификацию на базовых этапах ЖЦ ИУС (рис. 2).

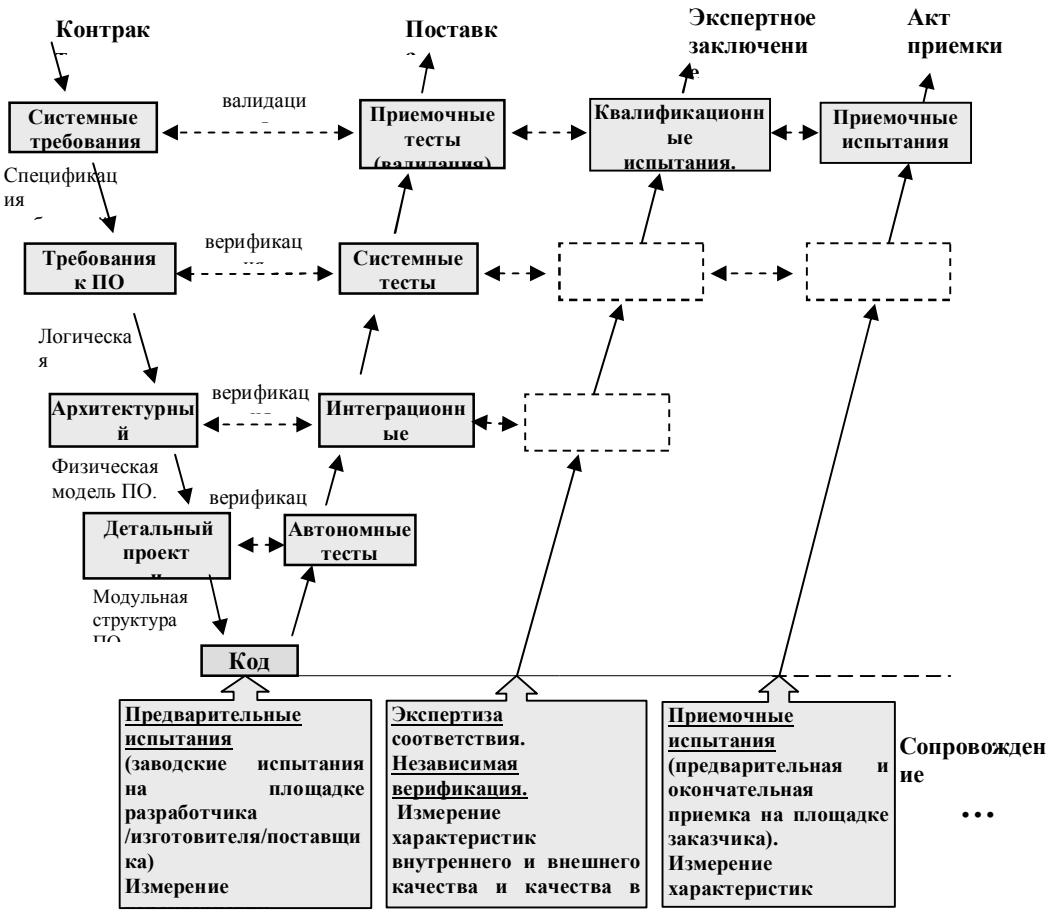


Рис.2. Оценка качества ПО в течение жизненного цикла ИУС критического применения

Номенклатура (варианты) правых ветвей «расщепленной» модели ЖЦ отражает эволюцию и виды испытаний ПО ИУС критического применения в диапазоне «предварительные испытания – квалификационные испытания – сертификация – приемочные испытания – сопровождение в эксплуатации». Каждой правой ветви «расщепленной» V-модели соответствует объем испытаний, адекватный установленному профилю регулирующих требований к качеству и безопасности ПО и обеспечивающий (гарантирующий) социально допустимый уровень риска аномального функционирования ИУС критического применения из-за влияния остаточных дефектов ПО.

Модель и схема измерения качества ПО

Полная модель качества ПО (в соответствии с базовыми стандартами ISO/IEC 9126, 14598) представлена тремя моделями, определяющими (рис. 3): внутреннее качество; внешнее качество; качество в использовании.

Диверсификация моделей качества ПО в соответствии с ISO/IEC 9126 – оценка качества с разных точек зрения на разных фазах жизненного цикла и в разных средах реализации ПО

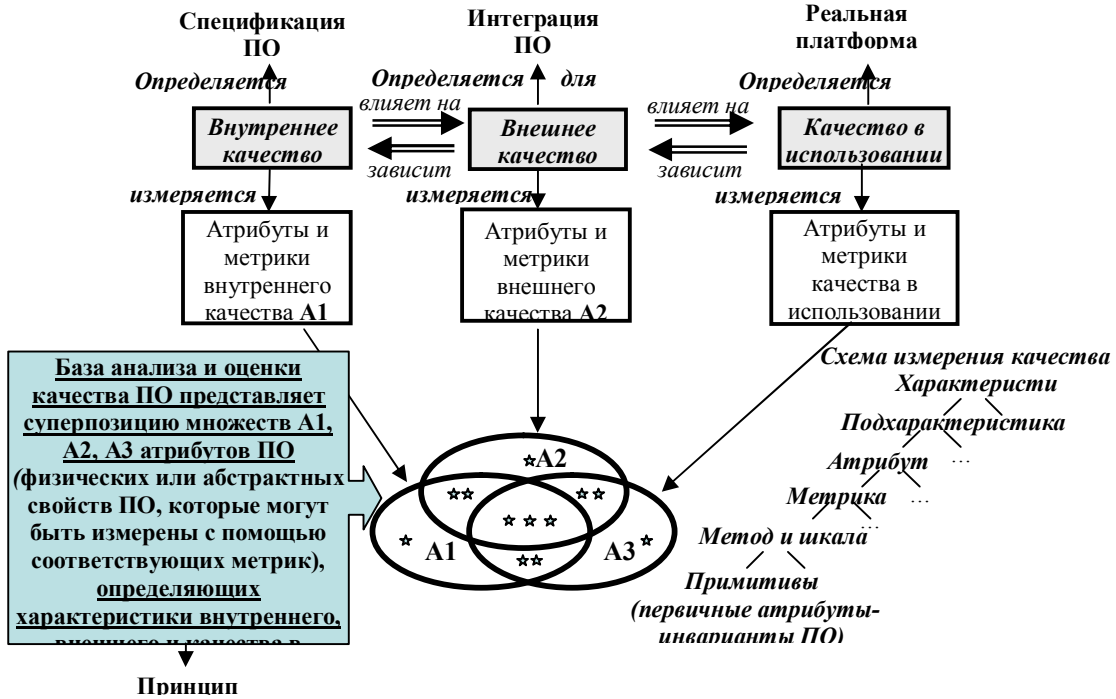


Рис. 3. Модель и схема измерения качества ПО

Такая диверсификация моделей качества предназначена для оценивания качества ПО в разных средах реализации на следующих базовых этапах ЖЦ ИУС: разработка спецификаций ПО; интеграция ПО; реализация на реальной платформе.

Необходимым условием обеспечения качества является возможность измерения атрибутов – физических или абстрактных свойств, которые могут быть измерены с использованием соответствующих метрик.

Метрика, по определению, представляет совокупность метода и шкалы измерения атрибута или характеристики ПО.

Общая схема измерений качества ПО предусматривает формирование иерархии значений «метрика (мера) – атрибут – подхарактериститка – характеристика» для всех составных частей (иерархии) архитектуры и на их основе интегральной оценки качества конкретного проекта ПО.

База анализа и оценки качества проекта ПО представляет суперпозицию множеств атрибутов ПО A1 U A2 U A3, определяющих характеристики внутреннего качества, внешнего качества и качества в использовании.

Элементы методологии диверсификации технологий верификации ПО

Общие принципы. Диверсификация технологий верификации ПО – это принцип, обеспечивающий повышение полноты и достоверности оценок характеристик качества ПО и получения интегральной улучшенной оценки, основанная на реализации принципа разнообразия. Задача каждой из диверсных технологий – измерение метрик различных атрибутов ПО с использованием различных методов.

Понятие дефекта ПО является ключевым при решении проблемы диверсификации технологий верификации. Это понятие рассматривается на двух уровнях:

а) на уровне спецификаций (исходный текст ПО) – некорректное значение (аномалия) атрибута ПО (в терминах языков программирования);

б) на уровне адресного поля ПО – отображение (проекция) аномалии на уровне спецификации ПО в некорректную композицию ячеек адресного поля ПО (в терминах исполняемого кода).

Возможные варианты обнаружения дефектов диверсными методами A1 и A2 представлены в табл. 1.

Таблица 1

Возможные варианты обнаружения дефектов

d1	d2	Результат композиции диверсных методов
+	+	Подтверждение дефекта обоими диверсными методами
+	–	Эффективное разнообразие диверсных методов
–	+	Дополнительный анализ для разрешения противоречия
–	–	Нечувствительность обоих диверсных методов

Эффект диверсификации технологий зависит от:

а) *полноты охвата* контролируемых (оцениваемых) атрибутов для композиции диверсных технологий;

б) *чувствительности* (проверяющей способности) каждой из диверсных технологий при обнаружении программных дефектов различных типов;

в) *реальной (не терминологической) степени разнообразия* технологий по чувствительности к дефектам различных типов в условиях конкретного проекта ПО.

Предлагаемое решение – реализация д***иверсных технологий*** верификации ***на основе инвариантов ПО:***

а) технология на основе ***логико-числового анализа*** (инвариант – численное значение переменных с учетом интервальных ограничений, точности представления и логики вычисления);

б) технология на основе ***семантического анализа*** (инвариант – физическая размерность переменных).

Критерии оценки – сохранение инвариантов (неизменных свойств ПО) в различных условиях эксплуатации ИУС.

Оценка ПО на базе числовых и семантических инвариантов. Концепция оценки базируется на следующих положениях.

1. Исходные (отправные) понятия для диверсификации методов оценки ПО:

. Дефект ПО – отображение на адресное поле ПО аномалий в проектных спецификациях ПО на уровне языка программирования.

. Инвариант ПО – первичный атрибут, не изменяющий значения в различных режимах эксплуатации (реализации) ПО конкретного проекта:

- логико-числовой (интервально-точностной) инвариант переменных ПО;
- семантика переменных ПО;
- операционная смесь (спектр инструкций-команд ПО).

. UA_i – суперпозиция множеств атрибутов ПО и соответствующих им характеристик внутреннего, внешнего качества и качества в использовании – база для диверсификации технологий.

2. Эффективная диверсность методов оценки –

обнаружение дефекта одним из диверсных методов и не обнаружение другим – является результатом реализации общего принципа разнообразия.

3. Проверяющая способность каждой из диверсных технологий (в терминах языка программирования) – выражается множествами D_1 или D_2 обнаруживаемых дефектов различных типов на множествах A1 и A2 инвариантов (первичных атрибутов) соответственно (рис. 4).

4. Проверяющая способность композиции диверсных технологий – определяется отображением множества дефектов обнаруживаемых композицией диверсных технологий $D'_1 \cup D'_2$, на адресное поле ПО.

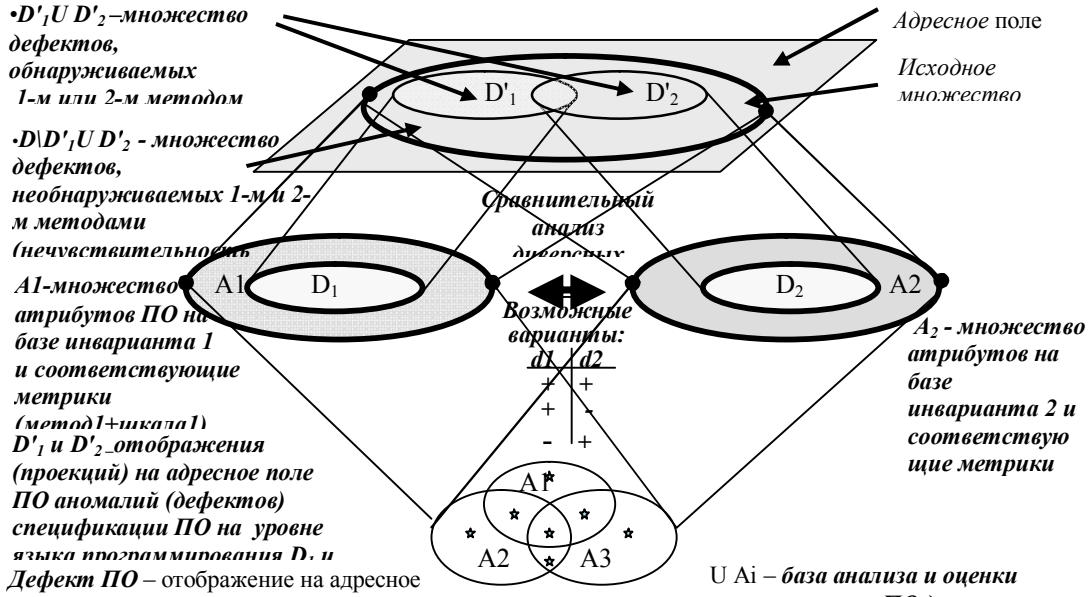


Рис. 4. Диверсификация технологий верификации ПО: оценка ПО на базе числовых и семантических инвариантов. Проверяющая способность композиции диверсных технологий

Неполнота, нечувствительность композиции диверсных методов оценки определяется $D/D'_1 \cup D'_2$.

5. ПО представляет отображение области определения в область значений использования логико-числовых и семантических инвариантов, обеспечивает (при необходимости) измерение базовых характеристик качества ПО: функциональность; надежность; обслуживаемость и др.

Достаточность 2-х инвариантов для повышения достоверности и полноты оценок характеристик ПО, при условии существования реальной степени разнообразия методов измерения с точки зрения чувствительности к дефектам ПО различных типов, подтверждается проведенными исследованиями и анализом реальных проектов.

Теоретико-множественная модель остаточных дефектов ПО для композиции диверсных технологий верификации.

1. Модель остаточных дефектов ПО представляет суперпозицию подмножеств Mi для композиции диверсных методов верификации с различной чувствительностью (проверяющей способностью).

2. Результативность верификации определяется вероятностью остаточных дефектов ПО.

3. Проверяющая способность композиции диверсных технологий определяется множеством

обнаруженных дефектов ПО M\ M1 ∩M2 на адресном поле ПО.

4. Возможные варианты (рис. 5): а) M1 ∩M2 = Ø – наилучший; б) M1 $\subseteq$ M2 – наихудший; в) M1 ∩M2 ≠ Ø – общий случай.

5. Для композиции диверсных технологий модель остаточных дефектов в общем случае представлена пересечением множеств M1 и M2, каждое из которых является суперпозицией парциальных подмножеств остаточных дефектов различных типов, необнаруживаемых при измерении различных атрибутов-инвариантов ПО, определенных используемым профилем дефектов.

Парциальное подмножество дефектов – подмножество остаточных дефектов ПО определенного типа, существующее в результате конечной парциальной чувствительности (нечувствительности) метода измерения инварианта ПО к дефектам определенного типа, задаваемых профилем дефектов.

Оценка эффективности диверсификации технологий верификации. Количественная оценка эффективности диверсификации технологий верификации базируется на множественно вероятностной модели (рис. 6).

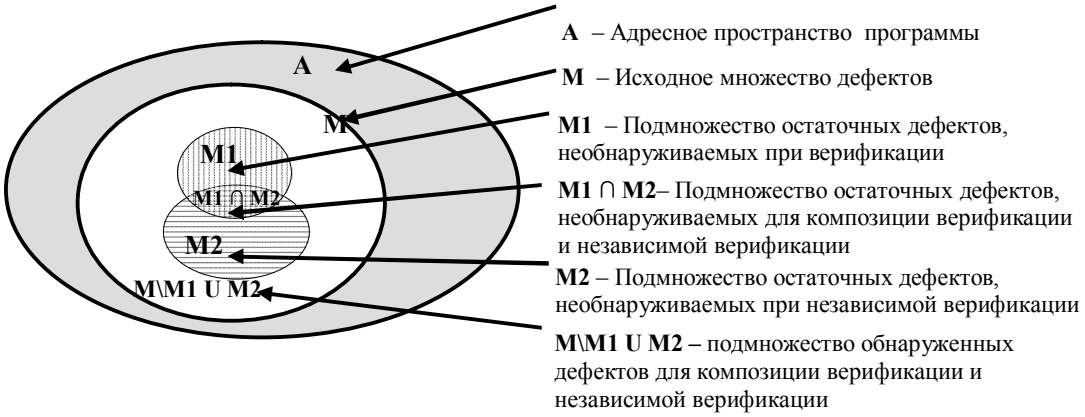
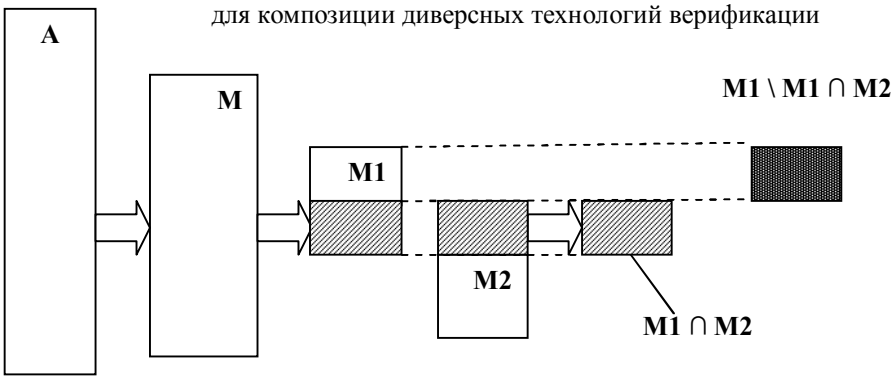


Рис. 5. Теоретико-множественная модель остаточных дефектов ПО для композиции диверсных технологий верификации



A – множество адресов ПО; M – исходное множество дефектов ПО;
M1, M2 – множества остаточных дефектов ПО после реализации диверсных технологий

Рис. 6. Оценка эффективности диверсификации технологий верификации

Предлагаются следующие индикаторы показателей количественной оценки выигрыша для композиции верификации и независимой верификации.

• ***Вероятность отсутствия дефектов ПО:*** после верификации – $P_{бд}$ = 1–P(M1); после независимой верификации – $P_{бд1.2}$= 1–P(M1 ∩ M2).

• ***Максимально возможное значение выигрыша*** от независимой верификации может составить P(M1).

• ***Индикатор снижения рисков остаточных***

дефектов ПО для композиции верификации и независимой верификации $P(M1 \cap M2)$

$$B = P(M1) - P(M1) = P(M1)\,(1 - P(M2 \mid M1)\,P(M1).$$

Снижение вероятности остаточных дефектов ПО после реализации композиции диверсных верификаций в пределе (идеальный случай) может составить 100%, что соответствует состоянию ПО:

$$P_{од} = 0;\ P_{бд} = 1.$$

Заключение

Концепцией нормативно-методического и инструментального оснащения процессов независимой верификации и экспертизы ПО ИУС является использование принципа разнообразия (технологической диверсности) как целевого средства повышения качества экспертных оценок по показателям достоверность, полнота, трудоемкость.

Диверсификация технологий основана на измерении семантических и логико-числовых инвариантов исходного ПО. Платформой для реализации диверсных технологий на основе инвариантов ПО является статический анализ исходных текстов ПО.

Реализация диверсных технологий на основе статического анализа исходного ПО обеспечивает контролируемую степень разнообразия технологий при оценивании базовых характеристик качества ПО ИУС «Функциональность», «Надежность», «Обслуживаемость» и т.д. с использованием метрик «Семантика», «Интервал», «Точность» переменных ПО.

Основой нормативно-методического оснащения испытательных лабораторий являются нормативные профили требований к ПО различных статусов утверждения, включающие регулирующие требования к процессам, методам, метрикам и процедурам оценивания ПО ИУС, включая повторное использование имеющегося или модернизированного ПО. Адекватные нормативные профили требований к ПО являются необходимым условием достижения качества и безопасности использования ИУС критического применения.

Предложенный подход создает возможности в рамках risk-informed регулирования безопасности АЭС количественно оценивать и управлять величиной снижения вероятности рисков остаточных дефектов ПО ИУС для композиции диверсных технологий верификации на основе экспериментальной калибровки чувствительности и реальной степени разнообразия диверсных методов верификации.

Перспектива длительной эксплуатации и развития инструментального оснащения испытательных лабораторий на базе методологии статического анализа исходного ПО ИУС обеспечивается благодаря использованию принципа открытой архитектуры и современных web-технологий (web-сервисы, программируемые web-приложения, коммуникационные протоколы) и соответствующих механизмов настройки комплекса утилит статического анализа на различные языки программирования.

Литература

1. Безопасность атомных станций: информационные и управляющие системы / М.А. Ястребенецкий и др. – К.: Техника, 2004. – 472 с.

2. Носовский А.В. Особенности безопасности ядерной энергетики // Ядерная и радиационная безопасность. – 2003. – Вып. 6, № 2. – С. 29-39.

3. 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. – Государственный комитет ядерного регулирования Украины, Государственный центр регулирования качества поставок и услуг, Сертификационный центр АСУ, Харьков, 2003. – 60 с.

4. Риск-ориентированный подход к оценке ИУС АЭС критического применения с учетом независимой верификации / Б.М. Конорев, Ю.Г. Алексеев, В.В. Сергиенко, В.С. Харченко, Г.Н. Чертков // Материалы Международного Симпозиума “Измерения на АЭС важные для безопасности”. – М., 23-25 ноября, 2004. – С. 37 – 41.

Поступила в редакцию 22.02.2006

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