ISSN 1561-8889. Космічна наука і технологія. 2008. Т 14. № 4. С. 9—26.

**Б. М. Конорев[1, 2], Ю. Г. Алексеев[1], С. А. Засуха[3], Л. П. Семенов[3], В. С. Харченко[2], Г. Н. Чертков[1]**

[1]Сертифікаційний центр АСУ, Харків

[2]Національний аерокосмічний університет ім. М. Є. Жуковського, Харків

[3]Національне космічне агентство України, Київ

# Квалификационные испытания критического программного обеспечения космических систем: целевая технология независимой верификации и прогнозирования скрытых дефектов

*Надійшла до редакції 12.12.07*

Представлено концепцію і методологію доказової незалежної верифікації критичного программного забезпечення (ПО), основаної на кількісних оцінках ступеня різноманітності методів верифікації (вимірювання характеристик ПО). Концепція полягає у використанні методу диверсифікованого вимірювання семантичних, інтервально-точнісних, логічних та інших інваріантів (незмінних властивостей) ПО на платформі статичного аналізу первинних текстів ПО. Враховано вимоги гарантоздатності і безпеки сучасних міжнародних стандартів у сфері космічної діяльності.

## ВВЕДЕНИЕ

***Структура космического комплекса. Критичность программного обеспечения.*** Развитие космической техники связано с непрерывным ростом требований к функциональным возможностям и эффективности элементов космического комплекса. Способность гибкой программной реализации функций высокой сложности обуславливает тенденцию непрерывного роста объемов программно-реализованных и программно-поддерживаемых функций и степени влияния качества критического программного обеспечения (ПО) на гарантоспособность и функциональную безопасность элементов космического комплекса [15].

Критическое программное обеспечение — это программное обеспечение, выполняющее функции, важные для безопасности, отказ которых из-за наличия дефектов и ошибок в ПО или неправильная эксплуатация могут привести к катастрофическим последствиям в диапазоне «материальные потери — ущерб окружающей среде — угроза здоровью и жизни людей». Наиболее часто критические функции связаны непосредственно с функционированием физического оборудования при выполнении необратимых операций в реальном времени. Отказы ПО из-за скрытых дефектов в таких случаях могут явиться причиной возникновения аварийных ситуаций и рисков нарушения безопасности при эксплуатации космического комплекса.

Применительно к ПО гарантоспособность (надежность, готовность, обслуживаемость) и функциональная безопасность представляют два связанных, но не идентичных понятия. Гарантоспособность концентрируется на анализе критичности, прогнозировании вероятности скрытых дефектов и обеспечении безотказности ПО. Функциональная безопасность непосредственно связана с тяжестью последствий отказов, а не просто с наличием дефектов ПО. Программное обеспечение становится критическим для безопасности в случаях программной реализации функций управления потенциально опасными системами или процессами [19, 20].

***Особенности программного обеспечения космических систем.*** Оценки гарантоспособности и функциональной безопасности критического ПО необходимо проводить с учетом следующей специфики:

- высокий уровень критичности программно реализуемых функций элемента космического комплекса и предельно высокие требования к качеству ПО;
- разработка, как правило, оригинального, сложного ПО для создаваемого космического комплекса;
- частые модификации и реинжиниринг ПО в процессе эксплуатации космического комплекса;
- жизненный цикл превышает продолжительность использования обычных компьютерных программ;
- отсутствие достоверных статистических данных по ПО космических систем.

Указанные особенности делают критическое ПО элементов космического копмлекса важным (актуальным) объектом нормативного регулирования, разрешительной деятельности и сертификации при создании и эксплуатации космической техники.

Схема контура нормативного регулирования качества (гарантоспособности и функциональ-

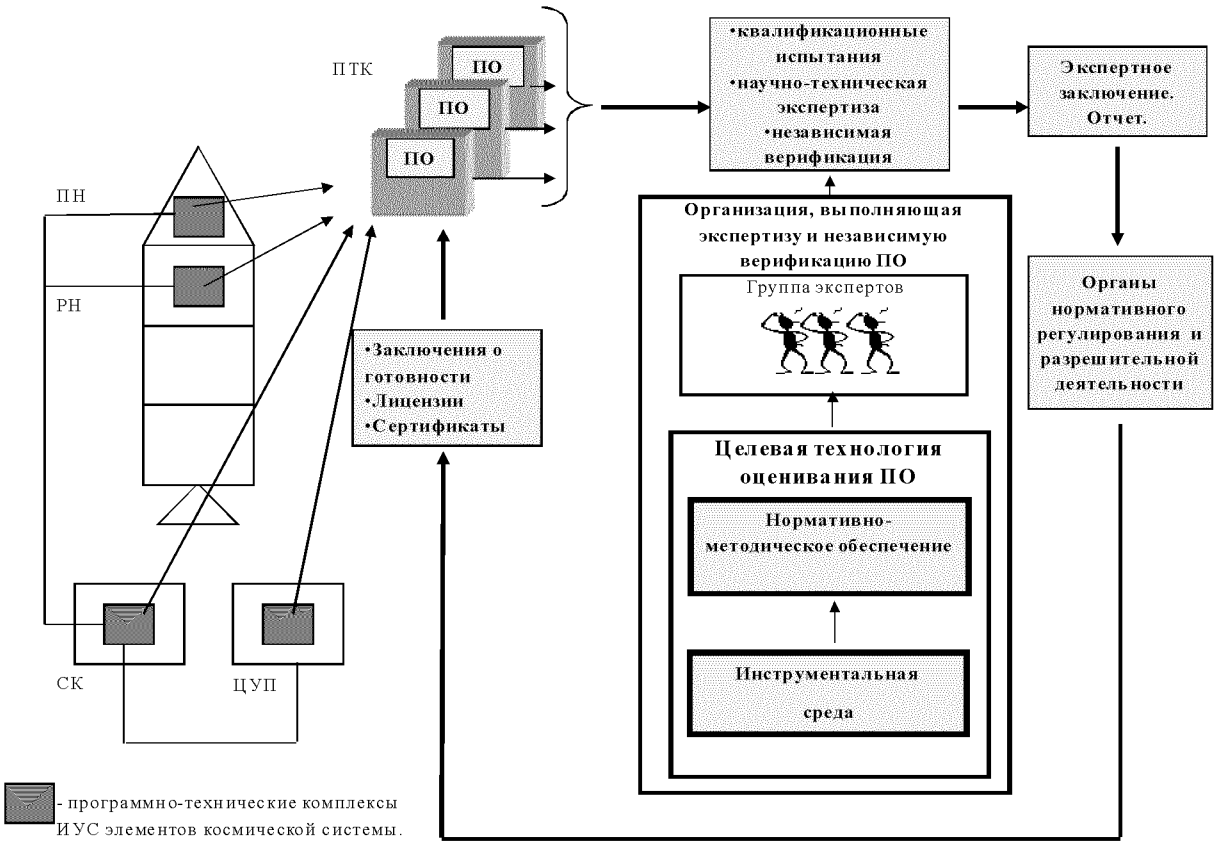


Рис. 1. Контур нормативного регулирования качества программного обеспечения элементов космической системы

ной безопасности) критического ПО представлена на рис. 1. Контур нормативного регулирования определяет общую инфраструктуру и нормативно-методическое обеспечение проведения квалификационных испытаний для всех уровней иерархии космического комплекса.

Применительно к ПО термин «квалификационные испытания» в стандартах ECSS [15] используется для обозначения «общего множества действий по верификации и валидации критического ПО».

В более широком контексте для системного уровня нормативными документами Национального космического агентства Украины этот термин используется для обозначения оценки «готовность к серийному производству» и к использованию по назначению оборудования элемента космического комплекса, включающего в общем случае аппаратные и программные компоненты [10].

Уровень нормативно-методического и инструментального оснащения работ в контурах нормативного регулирования качества критического ПО в значительной мере определяет реальные возможности достижения требуемых показателей гарантоспособности и функциональной безопасности космического комплекса в целом.

***Нормативная база квалификационных испытаний критического программного обеспечения.*** Согласно таксономии международных стандартов в сфере информационных технологий и программной инженерии может быть определена 3-уровневая классификационная схема процессов квалификационных испытаний критического ПО, представленная на рис. 2.


Рис. 2. Таксономия требований к процессам квалификационных испытаний критического программного обеспечения: 1 — процессы (фундаментальные методики квалификационных испытаний), 2 — методология (модели, методы, метрики, целевые технологии), 3 — технологические инструкции

Иерархия структуры классификационной схемы образуется на основе отношений «состоит из» или «входит в состав» элементов архитектуры процессов квалификационных испытаний и обеспечивает представление требований в диапазоне «что-как» («какая работа должна быть выполнена: цели, задачи» — «как выполнить конкретную работу: технологические инструкции»).

На верхнем уровне таксономии определяются требования к «Процессам» квалификационных испытаний, исходя в большей степени из того, какая работа должна быть выполнена или какие результаты должны быть достигнуты, а не из того, как организовать и выполнить конкретную работу. Это позволяет предприятиям и организационным структурам использовать имеющиеся в их распоряжении методы везде, где они эффективны, исключая необходимость в переделке действующих стандартов. Процессы анализа и оценки гарантоспособности и функциональной безопасности критического ПО при квалификационных испытаниях представлены набором стандартных фундаментальных методик.

На уровне таксономии «Методология» определяются требования к моделям, методам, метрикам, представляющим целевые технологии процессов квалификационных испытаний критического ПО.

И наконец, на уровне таксономии «Технологические инструкции» определяются производственные инструкции целевых технологий — стандарты конкретного предприятия, включающие конкретные технологические операции и измерение их результатов с использованием установленных на уровне «Методология» метрик.

Стандартами ECSS определяются требования, методы и методики анализа критичности и оценки характеристик гарантоспособности и функциональной безопасности на системном уровне для космического комплекса в целом и для его элементов [17, 18]. На их базе формируется профиль требований для критического ПО, гармонизированный со стандартами системного уровня [11—13, 19, 20].

Профиль требований регламентирует обязательное использование базового набора фундаментальных методик, включающих:
— независимую верификацию и валидацию критического ПО (IS V &V);
— анализ видов, влияния и критичности отказов критического ПО (SFMEA/SFMECA);
— анализ дерева дефектов ПО (SFTA);
— обнаружение, изоляция и удаление отказов ПО (SFDIR);
— анализ аппаратно-программных взаимодействий (HSIA);
— анализ безопасности и анализ эксплуатационной безопасности для ПО (HAZOP);
— анализ отказа по общей причине (SCCFA);
— историю эксплуатации ПО.

Фундаментальные методики квалификационных испытаний критического ПО полностью интегрированы в соответствующие методики системного уровня. Их проведение на всех этапах жизненного цикла в виде набора итеративных процедур является активным инструментом улучшения характеристик проекта ПО или процессов. Стандартный набор фундаментальных методик представляет спецификацию, семантику и объемы работ по «Программам обеспечения безопасности и гарантии продукта», в которых определяется полный объем квалификационных испытаний проекта критического ПО.

Реализация фундаментальных методик (процессов) квалификационных испытаний критического ПО основана на разработке соответствующих целевых технологий. Общими требованиями к целевым технологиям являются:
• обеспечение необходимой достоверности результатов, выраженной как точность или степень неопределенности оценок при использовании предлагаемых моделей, методов, метрик;
• компьютеризация и использование утилит как путь повышения достоверности результатов и снижения трудоемкости работ;
• рентабельность как комплексная характеристика, выражающая достижение установленной степени неопределенности квалификационных оценок при допустимых (минимальных) затратах ресурсов.

Методология целевых технологий должна быть представлена сбалансированной совокупностью моделей, методов и метрик, обеспечивающей эффективное решение задач квалификационных испытаний критического ПО.

В силу отмеченных ранее особенностей ПО космической техники целевая технология независимой верификации критического ПО является одной из самых информативных и значимых при квалификационных испытаниях. Это определяет ее высокую актуальность как важного механизма достижения требуемых уровней гарантоспособности и функциональной безопасности космического комплекса в целом и его элементов при реализации критических функций.

***Модель переходов состояний проекта критического программного обеспечения.*** Важным механизмом управления разработкой космического комплекса является проведение обзоров (совместных пересмотров — Review). Базовый принцип проведения обзоров состоит в том, что они реализуются с привлечением независимой экспертизы для полной и всесторонней оценки технического состояния проекта на ключевых этапах создания элементов космического комплекса.

Результативная реализация процессов обзоров позволяет квалифицировать состояние проекта критического ПО [15]. Модель переходов состояний проекта ПО приведена на рис. 3. Цели и задачи обзоров варьируются в зависимости от фазы работ. Обязательная спецификация обзоров проекта критического ПО включает:
— обзор требований (SSR);
— предварительный обзор проекта (PDR);
— критический обзор проекта (CDR);
— обзор квалификационных испытаний (QR);
— обзор приемо-сдаточных испытаний (AR).

Обзор квалификационных испытаний должен содержать результаты реализации фундаментальных методик анализа и оценки гарантоспособности и функциональной безопасности критического ПО, представляющих основное содержание «Программ обеспечения качества (гарантии продукта) и безопасности» конкретного проекта ПО.

## ПОСТАНОВКА ЗАДАЧИ

Разработка методологии и нормативно-методического обеспечения целевой технологии доказа-

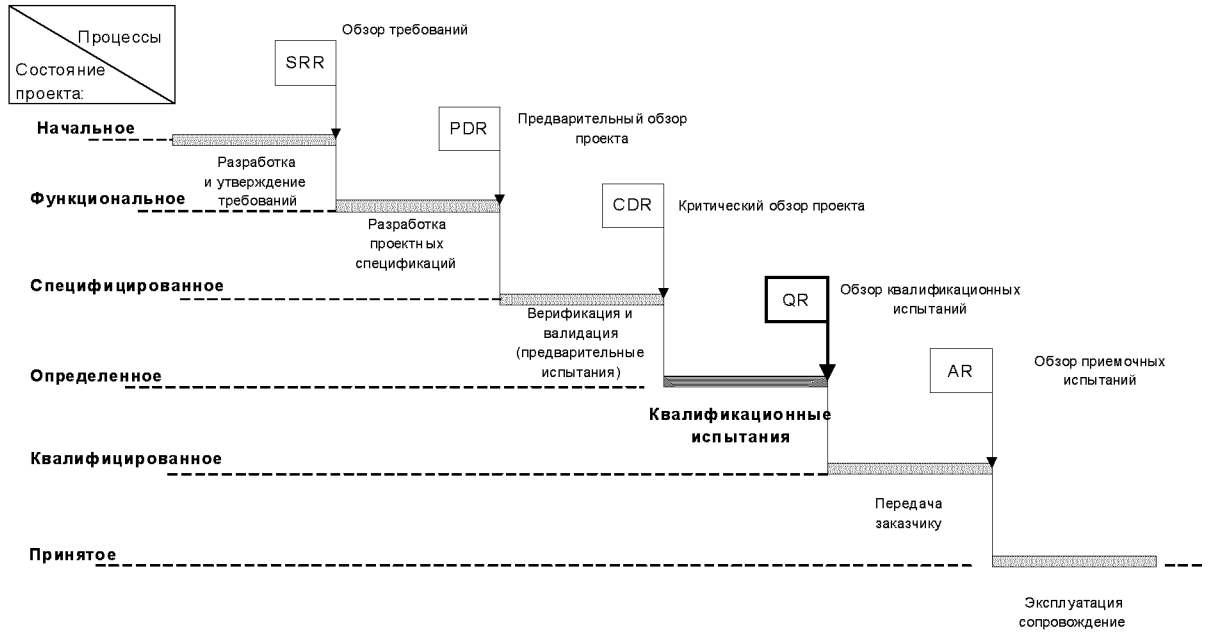


Рис. 3. Модель переходов состояний проекта программного обеспечения космической системы

тельной независимой верификации критического ПО, обеспечивающей:

— повышение достоверности результатов независимой верификации на основе метода диверсифицированного измерения семантических, интервально-точностных, логических и др. инвариантов (неизменных свойств ПО) на платформе статического анализа исходных текстов ПО.
— рентабельное прогнозирование вероятности скрытых дефектов с требуемой степенью неопределенности оценок;
— оценку полноты тестового покрытия при доказательной независимой верификации.

***Связь с «Общегосударственной космической программой Украины на 2008—2012 гг.».*** Разработка целевой технологии доказательной независимой верификации критического ПО представляет базовую междисциплинарную задачу раздела 5 «Космические комплексы», тем 5.5 «Качество», 5.6 «Сертификация», 5.7 «Стандарты» «Общегосударственной космической программы Украины на 2008-2012 гг.» [6].

Предлагаемый подход основан на нормативной базе Национального космического агентства Украины [11—13] и гармонизирован с соответствующими стандартами Европейской кооперации по стандартизации в сфере космической деятельности ECSS [17—20].

***Учет опыта квалификационных испытаний критического программного обеспечения при создании ракетно-космической техники в СССР.*** При разработке целевой технологии независимой верификации критического ПО учтен также и актуальный в настоящее время для космической отрасли Украины 25-летний опыт разработки критического ПО систем управления профилирующих объектов ракетно-космической техники СССР в период 1965—1990 гг. организацией АО «Хартрон» [2]. Перечень профилирующих объектов включает:

- сверхмощную ракету-носитель «Энергия» космического комплекса «Энергия — Буран» [5];
- несколько поколений стратегических межконтинентальных баллистических типов 15А14, 15А18, 15А30, 15А35 и др. [3];
- тяжелые орбитальные модули «Квант», «Кристалл», «Природа» и орбитальные пилотируемые станции «Салют» и «Мир» [1].

В частности, в настоящее время продолжает оставаться весьма актуальной многоверсионная

технология квалификационных испытаний критического ПО с использованием на заключительном этапе «электронного пуска». Многоверсионная технология включает испытания критического ПО в связанных технологических контурах с использованием разомкнутых и замкнутых схем моделирования [2]. Синхронизация и привязка результатов к шкале жесткого регламента времени производится с использованием механизма контрольных точек, которыми оснащается инструментированная версия критического ПО. «Электронный пуск» представляет цикл имитационного моделирования, проводимый на специальных исследовательских стендах [4], включающих инструментальную ЭВМ, реализующую математическую модель объекта управления, реальную БЦВМ, актуальную для конкретного цикла натурных испытаний версию ПО БЦВМ и полетное задание конкретного запуска ракеты (или соответственно суточное, недельное полетное задание проведения динамических операций на орбите космического аппарата).

Вариант многоверсионной технологии квалификационных испытаний критического ПО с проведением «электронного пуска» на стартовой позиции с полетным заданием конкретного запуска реализован при квалификационных испытаниях критического ПО СУ ракеты-носителя «Энергия» [5]. В настоящее время многоверсионная методология с использованием метода «электронного пуска» активно применяется в программах создания ракеты-носителя «Циклон-4», коммерческих запусков ИСЗ с использованием МБР «Днепр», «Стрела», «Рокот».

Эффективность этой методологии квалификационных испытаний критического ПО подтверждена результатами проведенных в 1970—1980 гг. свыше 300 циклов натурных испытаний различных типов профилирующих объектов ракетно-космической техники [2].

## КОНЦЕПЦИЯ

Предлагаемая целевая технология доказательной независимой верификации и прогнозирования скрытых дефектов критического ПО основана на использовании усовершенствованной методологии статического анализа исходных текстов ПО, обеспечивающей:

- повышение достоверности оценок характеристик ПО за счет реализации принципов


Рис. 4. Функциональная IDEF0-модель сценария независимой верификации

технологического разнообразия (диверсности) и независимости на основе метода диверсифицированного измерения семантических, интервально-точностных, логических и других инвариантов ПО (физических или абстрактных свойств ПО, не изменяющихся по определению в течение жизненного цикла);

- прогнозирование вероятности скрытых дефектов ПО на основе экспериментальной калибровки чувствительности и степени разнообразия диверсных методов измерения инвариантов в условиях конкретного проекта ПО, методом посева тестовых дефектов;
- управление рентабельностью (путем минимизации расходуемых ресурсов) прогноза вероятности скрытых дефектов с использованием индикатора снижения вероятности остаточных дефектов ПО в процессе реализации композиции диверсных методов измерения инвариантов, при этом функциональная безопасность космической системы трактуется как нахождение системы в условиях проектного риска аномального функционирования в течение установленного срока эксплуатации. В качестве метрики оценки риска в общем случае используется двумерная величина (мера) прогнозируемых уровней рисков $m_{ij} = (B, T)$, связывающая вероятность скрытых дефектов $B$ и тяжесть последствий их проявления на системном уровне $T$.
- оценку полноты тестового покрытия критического ПО при доказательной независимой верификации методом прямой и обратной трассировки множеств дизъюнктов: а) опорной (ссылочной) и оценочной моделей качества ПО; б) технического задания (спецификации требований к ПО); в) проектных определений и обоснований (проектно-конструкторской документации ПО).

***Методология. Основные положения. Модели и методы.*** Методология целевой технологии доказательной независимой верификации критического ПО космических систем базируется на следующих основных положениях.

**1. Процессный подход.** Сценарий целевой технологии независимой верификации представляет сеть взаимодействующих процессов, реализующих три концепт-методики:

— нормализация проекта ПО как объекта экспертизы;
— измерение инвариантов и оценка характеристик качества ПО;
— калибровка чувствительности и степени разнообразия методов измерения инвариантов и прогноз вероятности скрытых дефектов ПО.

Функциональная модель сценария (рис. 4) разрабатывается на основе методологии IDEF0 моделирования [14] и представляет иерархию моделей различных уровней детализации процессов сценария.

Аксиоматикой построения функциональной модели сценария определяются следующие элементы процессного подхода:

- концепт-методики, которые представляют сложно протекающие процессы, определяющие спецификации частично упорядоченных множеств заданий или рабочих пакетов.
- рабочий пакет, который является базовым элементом сценария, определяющим функционально завершенную процедуру, а полная спецификация рабочих пакетов обеспечивает построение и поддержку работ сценария на аналитическом, информационном и организационном уровнях. Рабочий пакет является основной единицей планирования работ сценария.
- процедуры выполнения рабочих пакетов, которые по способу реализации могут быть: не автоматизированными, компьютеризированными (с использованием утилит), комбинированными. Утилиты представляют инструментальные средства решения проблем фиксации, накопления, распространения и повторного использования передового опыта в сфере оценивания соответствия критического ПО нормативным (регулирующим) требованиям.
- механизм управления работами сценария (входы на верхней грани прямоугольника, обозначающего концепт-методику) представлены «Планом сценария», «Нормативным профилем проекта ПО», «Ограничениями».
- механизмы исполнения рабочих пакетов (входы на нижней грани концепт-методик) представлены «Методиками», «Утилитами», «Инструментариями».
- результаты реализации концепт-методик (выходы правых граней) представлены «Схемой измерения инвариантов проекта ПО», «Результатами решения систем линейных уравнений и неравенств, описывающих отображения инвариантов на всех уровнях иерархии проек-


Рис. 5. Дерево узлов функциональной IDEF0-модели сценария

та ПО» и «Оценками: характеристик качества ПО, прогноза вероятности скрытых дефектов, полноты тестового покрытия и рентабельности независимой верификации в целом».

- экспериментальная калибровка чувствительности и степени разнообразия диверсных методов измерения инвариантов для получения количественных оценок и достижения установленной рентабельности сценария независимой верификации критического ПО в целом осуществляется с использованием контура «Калибровка» на основе обратной связи типа «выход-управление».

Полная спецификация рабочих пакетов (заданий) сценария независимой верификации представлена деревом узлов 0-1-2 уровней иерархии функциональной IDEF0-модели на рис. 5.

Критерий завершенности сценария независимой верификации формулируется как достижение установленной степени неопределенности (достоверности) оценок вероятности скрытых дефектов ПО при приемлемом (минимальном) уровне затрат ресурсов. Критерий в целом определяет уровень рентабельности целевой технологии доказательной независимой верификации критического ПО.


Рис. 6. Общая схема измерения характеристик программного обеспечения. Опорная и оценочная модели

В целом же измеренные при независимой верификации инварианты ПО представляют базу первичных атрибутов (примитивов), с использованием которых могут быть оценены (вычислены метрики) базовые характеристики внутреннего и внешнего качеств и качества в использовании критического ПО в соответствии

с международной и национальной нормативной базой [11—13, 21—23].

**2. Нормализация проекта программного обеспечения.** Цель нормализации заключается в построении верифицированных: опорной (ссылочной) модели (ОМ) и совместимой оценочной модели (СОМ), обеспечивающих достоверную оценку соответствия характеристик качества конкретного проекта ПО предъявляемым требованиям при независимой верификации. Качественно совместимость ОМ и СОМ см. на рис. 6.

Для нормализации проекта критического ПО необходимо наличие:

— спецификации требований, содержащихся в техническом задании (ТЗ) или технических условиях;

— файлов проектных определений и обоснований, содержащих полный комплект технической (проектно-конструкторской) документации (ТД) проекта ПО;

— ссылочная нормативная база, содержащая перечень стандартов и нормативных документов, выполнение которых является обязательным или рекомендуемым для конкретного проекта ПО.

Опорная (ссылочная) модель (ОМ) представляет нормативный профиль (НП) проекта ПО, включающий спецификацию гармонизированных дизъюнктов требований общепромышленных и отраслевых стандартов ссылочной нормативной базы проекта ПО.

Формирование НП производится с использованием скрининг-технологии, обеспечивающей отбор (просеивание) и гармонизацию дизъюнктов ссылочной базы проекта.

Общая схема использования скрининг-технологии приведена на рис. 7. Основные этапы скрининг-технологии:

- скрининг 1 — формирование структуры (шаблона) препарированной профилеобразующей базы (ППБ) на основе общей таксономии международных стандартов программной инженерии и информационных технологий.
- скрининг 2 — формирование содержания ППБ на основе отбора дизъюнктов ссылочной профилеобразующей базы (ПБ) проекта в соответствии со структурой ППБ.
- скрининг 3 — гармонизация дизъюнктов на уровнях «Процессы», «Методология», «Про-

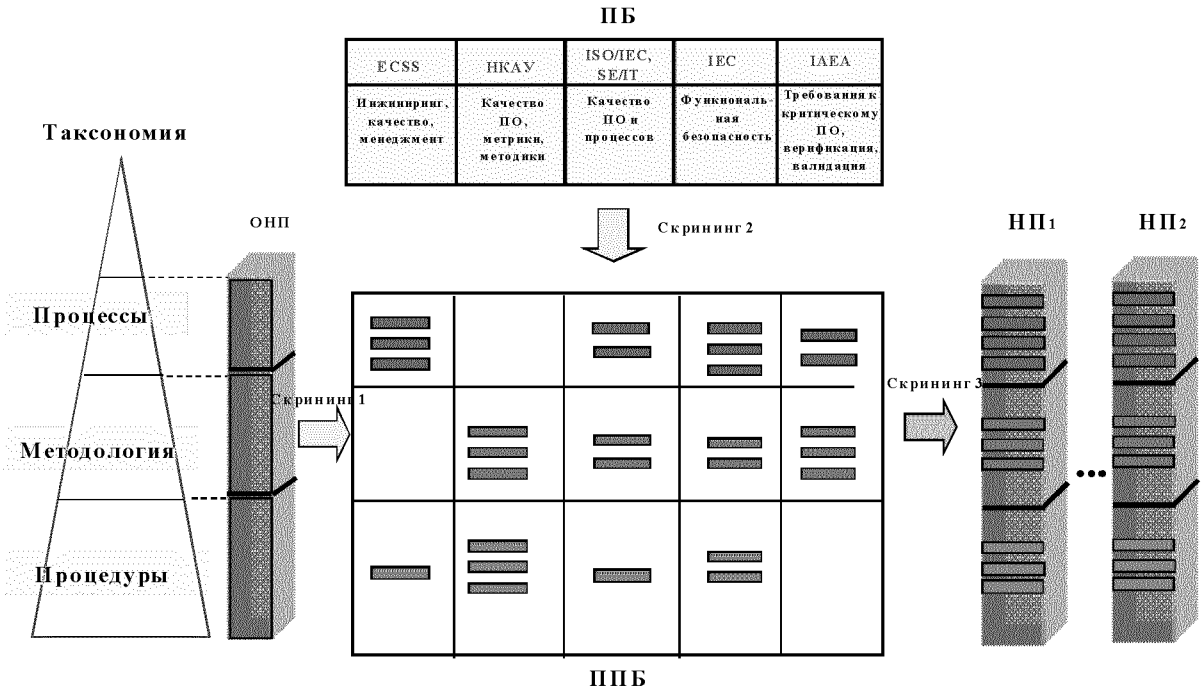


Рис. 7. Профилирование требований. Скрининг-технология формирования опорной (ссылочной) модели

цедуры» ППБ и формирование НП конкретного проекта ПО.

Совместная оценочная модель (СОМ) представляет расширение ОМ, выполняемое с целью определения метрик (методов и шкал) измерения атрибутов ПО конкретного проекта ПО.

Базовой процедурой формирования СОМ является раскрытие спецификаций атрибутов-инвариантов конкретного проекта ПО и определение спецификации (состава) методик их измерения и оценки.

Формально СОМ может быть описана как декартово произведение множеств дизъюнктов

$$\text{СОМ} \subseteq \text{НП} \times \text{ТЗ} \times \text{ТД}.$$

Раскрытие спецификации инвариантов проекта ПО производится на базе модели консолидированной оценки качества ПО. Основные элементы моделей соответствуют стандартам [21—23] и представлены в секторах А, Б, В рис. 8.

В секторе А представлены модели внутреннего качества ПО, внешнего качества ПО и качества ПО в использовании, относящиеся к стадиям (фазам) жизненного цикла «Спецификация ПО», «Интеграция ПО», «Функционирование на реальной платформе» соответственно.

Каждой модели качества ПО поставлены в соответствие множества $A_1$, $A_2$, $A_3$ атрибутов и метрик для их измерения.

В секторе Б представлена модель оценки качества процессов ПО — модель технологической зрелости (Capability Maturity Model — CMM) и общий вид статистических моделей точности прогноза и распределения разбросов (дисперсии) оценок целевых функций для различных (пяти) уровней технологической зрелости процессов организации-разработчика ПО.

В результате консолидированного рассмотрения моделей качества продукта и процессов ПО формируется суперпозиция — объединение множеств атрибутов и метрик $A_1$, $A_2$, $A_3$, определяющих базу анализа и оценки качества ПО (сектор В). Такая база является отправной точкой формирования СОМ при нормализации проекта ПО.

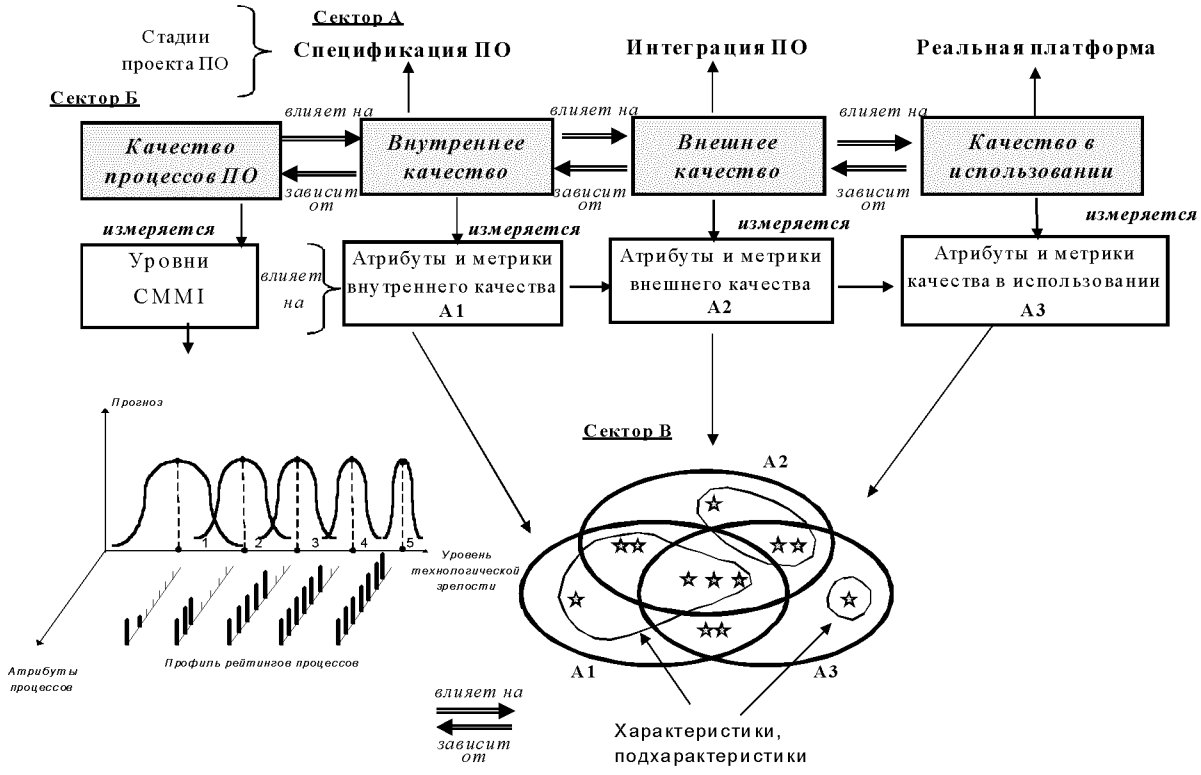


Рис. 8. Консолидированная опорная (ссылочная) модель измерения качества программного обеспечения

Основные задачи СОМ состоят в том, чтобы:
- создать основу (платформу) для объединения состояния проекта ПО в процессе его разработки с ответственностью за обеспечение (гарантии) качества;
- обеспечить раннюю идентификацию и устранение проблемы;
- обеспечить базис для ключевых выборов (проектных решений) как с технической так и с управленческой точек зрения при учете проектных ограничений, таких как стоимость, график, качество и функциональность;
- прослеживать специфические цели проекта;
- защищать и обосновывать проектные решения в течение жизненного цикла.

Верификация СОМ проводится методом исчерпывающей прямой и обратной трассировки взаимного соответствия дизъюнктов множеств НП, ТЗ, ТД. Трассировка — это процедура специфицирования и анализа отношений между дизъюнктами (элементами) множеств.

Главной задачей верификации является представление доказательств истинности отношений следствия и эквивалентности между дизъюнктами на основании выполнения процедур трассировки. Критерием являются значения «истина/ложь» при анализе отношений эквивалентности ($\Leftrightarrow$) или импликации (следствия) ($\rightarrow$) между дизъюнктами (элементами) этих множеств. Исчерпывающая трассировка достигается при последовательной реализации трассировки соответствия дизъюнктов проекций декартова произведения СОМ $\subseteq$ НП × ТЗ × ТД, $П_{р1.2} \subseteq$ НП×ТЗ, $П_{р2.3} \subseteq$ ТЗ×ТД, $П_{р1.3} \subseteq$ НП×ТД.

Верифицированная СОМ является необходимым промежуточным продуктом реализации сценария целевой технологии независимой верификации.

**3. Диверсифицированное измерение инвариантов ПО на платформе статического анализа исходных текстов.** Формальная модель ПО может быть представлена отображением Г: X → Y, где Г — формула или операторное отображение, содержащее упорядоченный перечень математических (компьютерных) операций, таких как сложение, умножение, деление, корень, степень, логарифм, ветвление, логика и т. п. Относительные количества таких операций в проекте ПО образуют операционный спектр (профиль), являющийся также статистическим инвариантом конкретного ПО.

При отображении реализуются заданные для конкретного проекта ПО отношения между элементами области определения X и области значений Y. Свойство неизменности (постоянства) реализованных отношений в течение жизненного цикла определяет возможность рассматривать ПО в целом как инвариант. В общем случае реализованное ПО отображение может быть представлено спецификацией, включающей в первом приближении следующие типы инвариантов:
— физическая размерность переменных (семантика);
— числовая размерность переменных (интервал);
— логическая схема вычислений переменных (алгоритмы решаемой задачи);
— спецификация требований к ПО (функциональные возможности и ограничения);
— требуемые ресурсы вычислительной платформы (объемы ЗУ, производительность).

Для оценки качества ПО в общем случае [16, 19, 23] используются базовые характеристики: функциональность, надежность, эффективность, практичность, переносимость, обслуживаемость (удобство эксплуатации), качество в использовании (включая функциональную безопасность). При выборе метрик для оценки этих характеристик в качестве примитивов — первичных атрибутов в предлагаемом подходе используются инварианты ПО, представляющие неизменные физические или абстрактные свойства ПО [7].

Модель консолидированной оценки качества ПО, представленная на рис. 8, позволяет сформировать базу анализа и оценки качества ПО в виде суперпозиции (объединения) множеств атрибутов $\overset{i}{UA}_i$, $i = \overline{1, 3}$ внутреннего качества ($i$ = = 1), внешнего качества ($i$ = 2) и качества в использовании ($i$ = 3), устанавливаемых в общем случае с учетом статистической связи с моделью технологической зрелости процессов жизненного цикла ПО.

Возможные скрытые дефекты ПО могут быть причиной искажения инвариантов, проявляющегося как потеря свойств неизменности или ошибки ПО. Проявление скрытых дефектов (ошибка ПО) в процессе эксплуатации ПО может приводить к отказам на системном уровне.

Методы измерения различных типов инвариантов характеризуются различной чувствительностью к скрытым дефектам ПО. На этом основана концепция диверсифицированного измерения инвариантов и реализации многоверсионных технологий на платформе статического анализа для повышения достоверности и точности результатов независимой верификации критического ПО. Дефекты ПО могут быть причиной искажения инвариантов. Критерием для оценки измеренного значения атрибута-инварианта ПО является его неизменность.

Методы измерения инвариантов характеризуются в общем случае разной чувствительностью, выражаемой вероятностью обнаружения дефекта ПО. Степень разнообразия каждой пары методов в общем виде представлена вероятность дефектов ПО, не обнаруживаемых обоими методами. Совокупность диверсных методов измерения инвариантов, реализованных на платформе статического анализа исходных текстов ПО, образует многоверсионную технологию диверсифицированного измерения атрибутов-инвариантов ПО. Реальное разнообразие диверсных методов является необходимым условием повышения достоверности (уменьшения неопределенности) при использовании многоверсионной технологии измерения инвариантов ПО [8].

Количественная оценка степени разнообразия представляет базовую характеристику метода диверсифицированного измерения инвариантов ПО при независимой верификации.

Общая схема диверсифицированного измерения инвариантов и теоретико-множественная модель интегральной проверяющей способности (чувствительности) композиции диверсных технологий верификации, основанных на измерении инвариантов ПО, представлена на рис. 9. Иллюстрируется случай измерения двух типов инвариантов, являющихся подмножествами базы консолидированной оценки качества $UA_i$, $i = \overline{1, 3}$. Схема включает две базовые процедуры:

- инструментирование исходного ПО, заключающееся в формировании технологической

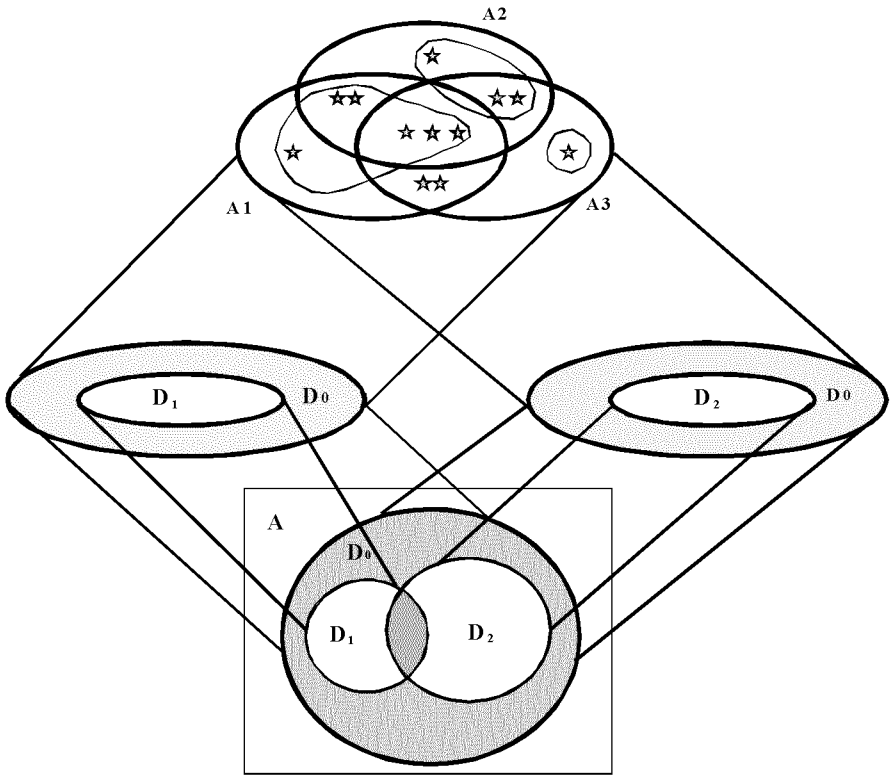


Рис. 9. Диверсифицированное измерение инвариантов программного обеспечения

версии — инструментированной модели исходного ПО, в которой определены контрольные точки — зонды, содержащие исходные данные и алгебру оценки различных инвариантов;

- интерпретация инструментированной версии исходного ПО и измерение в контрольных точках инвариантов для реализованных в ПО операторных отображений и ветвлений и оценка сохранения значений инвариантов.

Результаты измерения представлены с помощью диаграммы Эйлера — Венна, на которой $A$ — адресное пространство ПО, $D_0$ — исходное множество дефектов, $D_1$ и $D_2$ — множества дефектов, обнаруженных при диверсифицированном измерении двух типов инвариантов ПО.

Различная чувствительность к дефектам ПО разных типов диверсных методов измерения инвариантов определяют мощности множеств $|D_1|$ и $|D_2|$. Взаимное положение множеств $D_1$ и $D_2$ определяет степень разнообразия (диверсности) методов измерения инвариантов $|D_1 \cap D_2|/|D_1 \cup D_2|$ и множество остаточных дефектов, не обнаруживаемых обоими методами после последовательной реализации (композиции) двух диверсных методов $D_0 \setminus D_1 \cup D_2$, определяющих интегральную чувствительность композиции реализованных методов измерения инвариантов.

Для прогнозирования вероятности скрытых дефектов критического ПО при независимой верификации используется инверсная теоретико-множественная модель остаточных дефектов композиции диверсных методов измерения инвариантов (см. рис. 10).

Модель представлена диаграммой Эйлера — Венна для суперпозиции виртуальных подмножеств остаточных дефектов $D_1 \ldots D_i \ldots D_n$ композиции диверсных методов измерения инвариантов с различными чувствительностью и степенью диверсности (разнообразия).

Главным параметром модели является $\overset{v}{\cap} D_i$ — множество остаточных дефектов, не обнаруженных ни одним из методов. Модель обеспечивает проведение анализа и оценки возможных вариантов суперпозиции (взаимного расположения) множества скрытых дефектов ПО, не обнаруженных на предыдущих этапах до независимой верификации (позиции 1, 2, 3) и множества дефектов, не обнаруженных ни одним из методов композиции диверсных методов при независимой верификации.

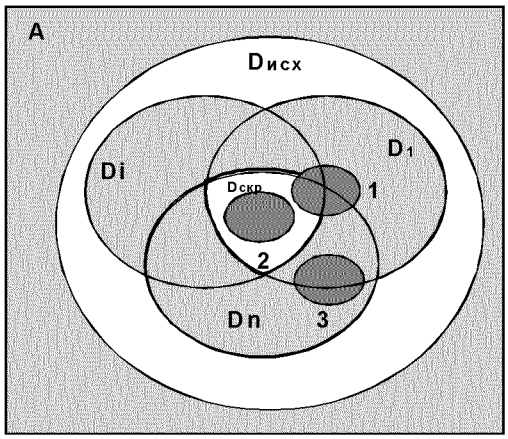


Рис. 10. Инверсная модель о статочных (с крытых) дефектов программного обеспечения для композиции диверсных методов измерения инвариантов

Индикатором оценки достигаемого эффекта является величина (в %), на которую уменьшается вероятность скрытых дефектов $P(D_{скр})$ в процессе последовательной реализации композиции диверсных методов измерения инвариантов при независимой верификации

$$I = P(D_{скр}) - \frac{|\overset{n}{\cap} D_i \setminus D_{скр}|}{|D_{скр}|} \cdot P(D_{скр}).$$

Если при независимой верификации не будут обнаружены $\overset{v}{\cap} D_i$скр, то $I = 0$, и величина отношения $|\cap D_i|/|\cup D_i|$ может служить основой рамочной оценки вероятности скрытых дефектов.

Возможны варианты:

а) теоретически возможный случай уменьшения вероятности скрытых дефектов на 100 % $(\cup D_i) \cap D_{скр} = \varnothing$, $I = 1$ (позиция 3, рис. 10),

б) максимально неблагоприятный вариант $D_{скр} \subset \overset{v}{\cap} D_i$ (позиция 2, рис. 10),

в) общий случай $(\cup D_i) \cap D_{скр} \neq \varnothing$, $I = \overline{0, 1}$ (позиция 1, рис. 10).

Таким образом, целевая технология доказательной независимой верификации обеспечивает оценку снижения вероятности скрытых дефектов на величину в диапазоне 0—100 % (в пределе на 100 %) в зависимости от характеристик конкретного проекта ПО.

**4. Количественная оценка вероятности скрытых дефектов на основе экспериментальной калибровки чувствительности и степени разнообразия диверсных методов измерения инвариантов.** Целью независимой верификации критического ПО является предоставление объективных (достоверных) доказательств соответствия ПО предъявляемым требованиям. Такими доказательствами в предлагаемом подходе служат результаты диверсифицированного измерения инвариантов ПО. Естественным критерием для оценки результатов измерений является подтверждение неизменности (сохранения) инвариантов ПО.

В то же время задача прогнозирования скрытых дефектов критического ПО, наряду с фундаментальными практиками анализа и оценки гарантоспособности и функциональной безопасности ПО космических систем, обуславливает необходимость количественных вероятностных оценок бездефектности критического ПО. Реализация количественных оценок основана на экспериментальной калибровке чувствительности (как вероятности обнаружения дефектов) и степени разнообразия диверсных методов измерения инвариантов в условиях конкретного проекта ПО. Калибровка осуществляется методом «посева» тестовых дефектов в ПО в соответствии с установленным профилем дефектов и последующего обнаружения их с использованием методов измерения инвариантов. Специфика конкретного проекта учитывается путем использования для посева профиля дефектов, отражающего типы и процентный состав операций конкретного проекта ПО.

Реализация калибровки методом «посева» тестовых дефектов производится с помощью модифицированного метода «капельной» (точечной) инъекции единичных тестовых дефектов и итеративного выполнения процедуры «инъекция — обнаружение — устранение». Инъекция единичных тестовых дефектов по определению исключает вредные эффекты интерференции и мутации тестовых дефектов в адресном пространстве ПО. Последовательная реализация такой процедуры при калибровке позволяет определять виртуальные подмножества остаточных дефектов, характеризующие парциальную (по типам дефектов) и полную (по профилю дефектов в целом) чувствительность каждого метода измерения инвариантов.

Использование откалиброванных методов является основой для количественной оценки с необходимой точностью интегральной чувствительности реализованной композиции диверсных методов измерения инвариантов, выражаемой как вероятность остаточных дефектов ПО. Оценка интегральной чувствительности проводится с использованием индикатора уменьшения вероятности остаточных дефектов после реали-

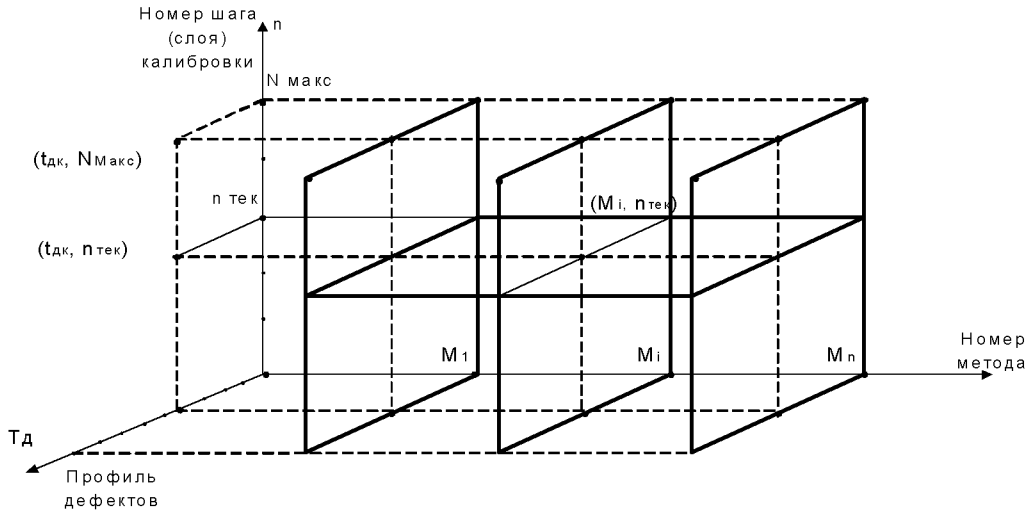


Рис. 11. Пространство результатов реализации процедуры инъекция-обнаружение тестового дефекта при калибровке методом посева дефектов

зации каждого последующего метода измерения инвариантов. Итоговое значение индикатора для композиции методов может лежать в диапазоне 0—100 % (в пределе вероятность скрытых дефектов ПО может быть уменьшена теоретически на 100 %, т. е. до 0 в зависимости от характеристик конткретного проекта).

Экспериментальная калибровка парциальной и полной чувствительности каждого метода и интегральной чувствительности композиции диверсных методов производится в контексте пространства калибровочных испытаний (рис. 11), представляющего декартово произведение

$$\Pi_{\text{КИ}} \subseteq \text{N}\times\text{M}\times\text{T},$$

где $\text{N} = \{n_i\}$ — множество инъекций тестовых дефектов, реализованных при калибровке; $\text{M} = \{m_j\}$ — множество калибруемых методов измерения инвариантов; $\text{T} = \{t_k\}$ — множество типов инъектируемых тестовых дефектов или профиль дефектов. $\Pi_{\text{КИ}}$ — определяет множество (кортеж) исходов — результатов экспериментов при калибровке. Значение элемента $\Pi_{\text{КИ}}$ с координатой $(n_i; m_j; t_k)$ может принимать значение 0, если тестовый дефект не обнаружен, или 1, если тестовый дефект обнаружен.

Инъекция кортежа $\text{T} = t_k$ при калибровке метода $\text{M} = m_j$ представляет шаг или слой калибровки в пространстве $\Pi_{\text{КИ}}$.

На каждом шаге $n_i$ для каждого метода $m_j$ выполняется итеративная параметрически управляемая процедура, включающая последовательность операций:

— определение на основании спектра операций конкретного проекта ПО в адресном пространстве точки (адреса) для инъекции тестового дефекта;
— инъекция тестового дефекта в инструментированную версию исходного ПО;
— цикл интерпретации инструментированной версии исходного ПО, оснащенной контрольными точками — зондами измерения инвариантов, и извлечение тестового дефекта;
— регистрация результатов обнаружения дефекта и формирование множеств обнаруженных и не обнаруженных (остаточных) дефектов;
— формирование для каждой пары калибруемых методов текущих значений элементов матрицы разнообразия $m_{ij} = 1 - (\cap D_i/\cup D_i$, где $D_i$ — множество остаточных дефектов и индикатора $I$ уменьшения вероятности остаточных дефектов ПО;

По результатам обработки полного объема калибровки для условий конкретного проекта ПО определяются:

— гистограмма распределения значений парциальной (по типам дефектов профиля) чувствительности методов измерения инвариантов (см. рис. 12);
— полная (для полного профиля дефектов) чувствительность диверсных методов измерения инвариантов;
— интегральная чувствительность композиции диверсных методов измерения инвариантов с учетом их степени разнообразия на основе модели остаточных дефектов (см. базовый принцип 3).

На гистограмме (рис. 12) значком «минус» обозначены объемы работ, которые могут быть исключены при калибровке для уменьшения затрат ресурсов и повышения рентабельности.

Прекращение инъекций дефектов при формировании гистограммы значений парциальной чувствительности метода производится, исходя из величин среднего значения $\overline{P}$ и дисперсии $\sigma$ вероятности обнаружения дефекта.

Минимальный объем выборки $n_{i\,\min}$ (число шагов калибровки метода по типу дефекта) определяется по схеме [9]:

- устанавливается достоверность оценки $\gamma$;
- определяется аргумент t функции Лапласа $\Phi(t) = \gamma/2$;
- устанавливается точность оценки $\delta = t\sigma/\sqrt{n}$;
- определяется доверительный интервал $\overline{P} \pm \delta$;
- определяется минимальный объем выборки при калибровке парциальной чувствительности метода $n_{i\,\min} = t^2\sigma^2/\delta^2$;
- определяется минимальный объем выборки для всех методов композиции, обеспечивающий достижение установленной точности прогноза вероятности скрытых дефектов критического ПО после независимой верификации, составляет $n_\Sigma = \max(n_{i\,\min})$.

**5. Оценка полноты тестового покрытия и рентабельности целевой технологии независимой верификации.** Полнота тестового покрытия, достигаемая при использовании целевой техно-

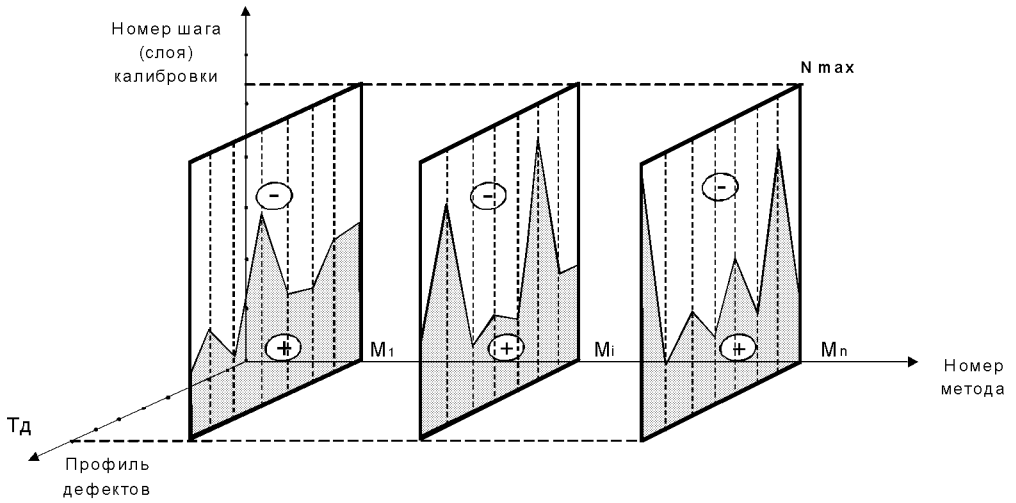


Рис. 12. Гистограмма значений парциальной (к типам дефектов профиля) калибровки чувствительности методов измерения инвариантов программного обеспечения в условиях конкретного проекта

логии независимой верификации, оценивается для двух уровней представления проекта ПО:

1) спецификации требований, проектные определения и проектные обоснования;

2) исходные тексты (коды) ПО.

Для первого уровня в качестве метрики оценки тестового покрытия используется мера полноты оценок отношений эквивалентности и импликативности дизъюнктов множеств НП, ТЗ, ТД при верификации совместимой оценочной модели на этапе нормализации проекта ПО. По результатам измерения инвариантов ПО в соответствии с совместимой оценочной моделью мера полноты тестового покрытия уточняется.

Для второго уровня в качеств метрики и меры используется интегральная чувствительность реализованной при независимой верификации композиции диверсных методов измерения инвариантов ПО. Общей стратегией является достижение максимальных значений обоих показателей полноты тестового покрытия на уровнях спецификации требований и программной реализации, определяющих общую достоверность результатов и прогноза скрытых дефектов ПО.

Рентабельность целевой технологии независимой верификации определяется как достижение установленной степени неопределенности (достоверности) прогноза скрытых дефектов ПО при минимальных затратах ресурсов. В качестве индикатора количественной оценки используется величина изменения вероятности скрытых дефектов ПО. Значение индикатора определяется для каждого шага калибровки композиции диверсных методов измерения инвариантов. Калибровка чувствительности и степени разнообразия диверсных методов в условиях конкретного проекта ПО обеспечивает требуемую точность (достоверность) индикатора.

Ресурсоемкость (затратность) независимой верификации определяется рядом факторов. Эффект рентабельности определяется минимизацией главных из них:

— выбор минимально необходимого числа шагов калибровки методов измерения инвариантов $n_{min}$ для получения статистически достоверных результатов;

— выбор профилей тестовых дефектов для калибровки на основе экспериментально измеренного спектра операций конкретного проекта ПО;

— выбор спецификации диверсных методов измерения инвариантов на основе спектра операций конкретного проекта и статистики по чувствительности методов;

— выбор для анализа областей адресного пространства (модулей) ПО при калибровках,

исходя из предположений (доказательств) стационарности статистических характеристик конкретного проекта ПО.

Наиболее значимым параметром является число шагов калибровки $n_{\min}$. Шаг калибровки представляет итеративно выполняемую процедуру, для кортежа профиля дефектов включающую «инъекцию единичного дефекта — обнаружение — протоколирование — исключение дефекта и обработку результатов». Параметры управления итерациями — «инвариант ПО», «тип дефекта», «число шагов калибровки».

Число шагов $n_{i\,\min}$ калибровки метода $M_i$ определяется по выбранным значениям сводных показателей достоверности, точности и доверительного интервала оценки матожидания вероятности бездефектности (чувствительности) калибруемого метода $M_i$ измерения инвариантов. Определение $n_{\min}$ производится в процессе калибровки и используется как признак останова итеративной процедуры.

В результате для калибровки композиции $M_i$ суммарное число шагов равно $N_{k\,\min} = \max(n_{i\,\min})$.

## ЗАКЛЮЧЕНИЕ

Целевая технология доказательной независимой верификации и прогнозирования вероятности скрытых дефектов критического ПО представляет одну из ключевых методик анализа критичности и оценок гарантоспособности и функциональной безопасности при квалификационных испытаниях космических систем. Эффективность и рентабельность такой технологии в значительной мере определяют реальные возможности достижения необходимых уровней гарантоспособности и функциональной безопасности разрабатываемой космической системы в целом.

Предложенный подход (концепция, методология, модели и методы):

— расширяет реальные возможности организаций — разработчиков и регулирующих органов в части повышения достоверности и точности прогнозирования рисков аномального функционирования космических систем из-за дефектов критического ПО в общем контексте квалификационных испытаний.

— обеспечивает возможность количественно оценивать предельные значения и управлять снижением вероятности скрытых дефектов критического ПО в диапазоне 0—100 % (в пределе на 100 % в зависимости от характеристик проекта ПО и приемлемых уровней рентабельности);

— определяет методологическую основу для решения актуальной междисциплинарной задачи разработки нормативно-методического и инструментального обеспечения оценок гарантоспособности и функциональной безопасности критического ПО космических систем в рамках раздела 5 «Космические комплексы», тем 5.5 «Стандарт», 5.6 «Сертификат», 5.7 «Качество» «Общегосударственной космической программы Украины на 2008—2012 гг.»


1. Айзенберг Я. Е., Бек А. В., Конорев Б. М. и др. Система управления транспортного корабля снабжения и функционально-грузовых орбитальных модулей «Квант», «Кристалл», «Спектр», «Природа». Теоретические принципы построения, управляющие алгоритмы и программы, разработка, отработка, натурные испытания // Цикл работ. — Харьков: Хартрон, 1966—1996.
2. Айзенберг Я. Е., Бек А. В., Конорев Б. М. и др. Динамическая отработка программного обеспечения бортовых цифровых вычислительных машин систем управления объектов ракетно-космической техники // Космічна наука і технологія.—1997.—3, № 1/2.—С. 61—74.
3. Айзенберг Я. Е., Златкин Ю. М., Конорев Б. М. и др. Система управления семейства межконтинентальных баллистических ракет. Теоретические принципы построения, алгоритмы управления и контроля, ПО БЦВМ, разработка, отработка, натурные испытания // Цикл работ. — Харьков: Хартрон, 1964—1991 гг.
4. Айзенберг Я. Е., Конорев Б. М. Организация имитационного моделирования в автоматизированных системах производства программ реального времени // УСиМ.—1982.—№ 4.—С. 83—87.
5. Айзенберг Я. Е., Конорев Б. М., Щербаченко В. Т. и др. Комплекс автономного управления ракеты-носителя «Энергия». Теоретические принципы построения, управляющие алгоритмы и программы, разработка, отработка, натурные испытания // Цикл работ. — Харьков: Хартрон, 1985—1990 гг.
6. Загальнодержавна космічна програма України на 2008—2012 рр. — Київ: НКАУ, 2007. http://www.nkau.gov.ua
7. Конорев Б. М., Алексеев Ю. Г., Засуха С. А. и др. Модель оценивания качества ПО ИУС критического применения на основе инвариантов // Радиоэлектронные и компьютерные системы.—2006.—№ 7.—С. 162—170.
8. Конорев Б. М., Засуха С. А., Семенов Л. П. и др. Методология оценки качества и функциональной безопасности критического программного обеспечения эле-

ментов космических систем // Сучасні тренажерно-навчальні комплекси та системи: Зб. наук. праць Ін-ту проблем моделювання в енергетиці ім. Г. Є. Пухова. — Київ, 2006.—Т. 2.—С. 85—89.
9. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. — М.: Наука, 1970.—720 с.
10. Правила космічної діяльності в Україні. Проведення наукової і науково-технічної експертизи проектів, науково-дослідних і дослідно-конструкторських робіт. Загальні положення і вимоги: Затверджено НКА України УРКТ-10.03. — Київ, 2006.—91 с.
11. СОУ-Н НКАУ 0012:2006. Галузева система управління якістю. Вимоги до якості програмного забезпечення програмно-технічних комплексів критичного призначення / НКАУ. — Запров. 01.09.06. — Київ, 2006.—118 с.
12. СОУ-Н НКАУ 0031:2007. Галузева система управління якістю. Методи оцінки показників якості програмного забезпечення програмно-технічних комплексів критичного призначення / НКАУ. — Запров. 01.01.08. — Київ, 2007.—128 с.
13. СОУ-Н НКАУ 0058:2008. Галузева система управління якістю. Вимога до функціональної безпеки ПЗ програмно-технічних комплексів критичного призначення / НКАУ. — 2008.—60 с.
14. Функциональное моделирование. Методология IDEF0. Стандарт. Русская версия. — М.: Мета Технология, 1993.—108 с.
15. ECSS-E-40 Part 1B—2003. Космічний інжиніринг. Програмне забезпечення. Ч. 1: Принципи та вимоги = Space engineering. Software. Part 1: Principles and requirements.
16. ECSS-E-40 Part 2B—2005. Космічний інжиніринг. Програмне забезпечення. Ч. 2: Визначення вимог до документів = Space engineering. Software. Part 2: Document requirements definitions (DRDs).
17. ECSS-Q-30B-2002. Гарантія продукції космічного призначення. Гарантоздатність = Space product assurance. Dependability.
18. ECSS-Q-40B-2002. Гарантія продукції космічного призначення. Безпека = Space product assurance. Safety.
19. ECSS-Q-80B-2002. Гарантія продукції космічного призначення. Гарантія програмного продукту = Space product assurance. Software product assurance.
20. ECSS-Q-80-2003. Гарантія продукції космічного призначення. Методи та методики оцінки надійності та безпеки програмного забезпечення = Space product assurance. Methods and techniques to support the assessment of software dependability and safety.
21. ISO 25000:2005. Космічний інжиніринг. Вимоги до якості та оцінка програмного забезпечення (SQuaRE) — Настанова з SQuaRE = Software Engineering — Software Product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE.
22. ISO/IEC 14598-1:1999. Інформаційні технології — оцінювання програмного продукту. Ч. 1: Загальний огляд = Information technology — Software product evaluation — Part 1: General.
23. ISO/IEC TR 9126-1-4:2001-2004. Інжиніринг програмного забезпечення — Якість продукту = Software Engineering — Product Quality.

## QUALIFICATION TESTS OF THE CRITICAL SOFTWARE FOR SPACE SYSTEMS: TARGET TECHNOLOGY OF INDEPENDENT VERIFICATION AND LATENT DEFECT PREDICTION

*B. M. Konorev, Yu. G. Alekseev, S. A. Zasukha, L. P. Semenov, V. S. Kharchenko, G. N. Chertkov*

We present a conception and methodology for independent verification and validation of critical software (SW) which are based on the quantitative estimation of measure of verification methods variety (software characteristic measurement). The conception consists in using the diverse measurement method for interval-precision, logical and other software invariants (constant properties) on the basis of static analysis of SW sources. The dependability and safety requirements of existed international standards in space activity area are taken into account.