# ТЕСТУВАННЯ, ВАЛІДАЦІЯ ТА ВЕРИФІКАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 004.052.42

**Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ"**

**Б.М.Конорев, В.В.Сергієнко, І.Б.Туркін**

# ДОКАЗОВА НЕЗАЛЕЖНА ВЕРИФІКАЦІЯ ТА ПРОГНОЗУВАННЯ ПРИХОВАНИХ ДЕФЕКТІВ КРИТИЧНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ ДИВЕРСНОГО ВИМІРЮВАННЯ ІНВАРІАНТІВ

*Надійність та безпека інформаційно-керуючих систем критичного призначення суттєво залежать від якості програмного забезпечення (ПЗ), за допомогою якого виконуються критичні функції. Приховані дефекти (дефекти, що не були виявлені при тестуванні та верифікації) критичного ПЗ являються факторами ризику відмови системи. Незалежна верифікація критичного ПЗ, що підтверджує виконання заявлених функцій та дає оцінку вірогідності наявності прихованих дефектів, є необхідною умовою нормативних вимог для різних галузей (МАГАТЕ, Європейська Космічна Агенція ). З цієї точки зору основними проблемами є: надійність незалежної верифікації, оцінювання вірогідності прихованих дефектів, повнота тестового покриття для критичного ПЗ та, як результат, кількісна оцінка функціональної безпеки.*
*Розглядається розробка та використовування вдосконаленої методології доказової незалежної верифікації на базі статичного аналізу вихідних текстів ПЗ для оцінювання семантичних, інтервально-точностних, логічних та інших інваріантів (властивостей ПЗ, які залишаються незмінними по визначенню протягом життєвого циклу ПЗ) критичного ПЗ, а також формування і подання результатів оцінки відповідності ПЗ вимогам стандартів і специфікацій проекту.*

*Dependability and Safety of instrumentation and control critical systems depend on characteristics of quality of the software, performing critical functions. Latent faults (faults undetected during testing or verification) of the critical software are factors of the risk of system failure. The independent verification of the critical software, which confirms a performance of declared functions and estimates a probability of latent faults existence, is the necessary condition according to the regulative requirements for different areas (IAEA, ESA and so on). From this point of view, the main problems are: the reliability of independent verification; assessment of latent faults probability; completeness of test coverage for the critical software and as result the quantitative assessment of functional safety. Considered is the development and implementation of the advanced methodology of proven independent verification on the base of the software sourcecode static analysis. Methodology is aimed at the assessment of the semantic, interval-precision, logic and others invariants ((software properties invariable during the life cycle)) of critical software and also generation and presentations of results of assessment conformity to requirements of standards and project specifications.*

*Надежность и безопасность информационно-управляющих систем критического использования существенно зависят от качества программного обеспечения (ПО), реализующего критические функции систем. Скрытые дефекты (дефекты, не выявленные при тестировании и верификации) критического ПО являются факторами риска отказа системы. Независимая верификация критического ПО, которая подтверждает выполнение заявленных функций и дает оценку вероятности наличия скрытых дефектов, является необходимым условием нормативных требований для различных отраслей (МАГАТЭ, Европейское космическое агентство). В этом контексте основными проблемами являются: надежность независимой верификации, оценка вероятности скрытых дефектов, полнота тестового покрытия для критического ПО и как результат количественная оценка функциональной безопасности.*
*Рассматривается разработка и использование усовершенствованной методологии доказательной независимой верификации на базе статического анализа исходных текстов ПО для оценки семантических, интервально-точностных, логических и др. инвариантов ПО (свойств ПО, остающихся неизменными по определению в течение жизненного цикла) критического ПО, а также формирование и представление результатов оценки соответствия ПО требованиям стандартов и спецификаций проекта.*

**Ключові слова:** програмне забезпечення, формальні методи верифікації, тестування, незалежна верифікація, інваріант, калібрування, профіль дефектів

 

**Вступ**

Загальна тенденція в атомній енергетиці, космічній та інших галузях, пов'язаних з широким використанням інформаційних технологій, складається у швидкому зростанні обсягів і масштабів застосування інформаційно-керуючих систем (ІКС), які засновані на інтенсивному використанні програмного забезпечення (ПЗ) і збільшення частки критичних функцій ІКС, які програмно реалізуються та програмно підтримуються.

З цим пов'язане збільшення ризиків існування прихованих дефектів, які є джерелами аномалій (можливих відмов) ІКС.

Приховані дефекти ПЗ, які не були виявлені при тестуванні та верифікації, можуть проявитися як аномалії у процесі експлуатації ІКС, призвести до їх відмови та вплинути на безпеку всієї системи у цілому. Рівень критичності ПЗ таких систем визначається «вагою» наслідків відмов (аномального поводження) ІКС через приховані дефекти ПЗ.

Забезпечення функціональної безпеки та надійності ІКС суттєво залежить від якості ПЗ. Внаслідок цього ПЗ має статус важливого об'єкта нормативного регулювання, який значною мірою визначає якість і безпеку ІКС у цілому. Важливою нормативною вимогою для такого класу ІКС є проведення технологічно диверсної незалежної верифікації ПЗ.

Незалежна верифікація та валідація є ключовою методикою кваліфікаційних випробувань критичного ПЗ. Її проведення є обов'язковою нормативною вимогою в сферах критичної діяльності, таких як атомна енергетика ("Software for computer based systems important to safety in nuclear power plants"- Серія стандартів МАГАТЕ з безпеки), космічна галузь (стандарти ECSS-Q-40B, ECSS-Q-80B) та інші.

Незалежна верифікація в обсязі кваліфікаційних випробувань ПЗ ІКС вирішальним чином визначає реальні можливості в забезпеченні необхідного рівня безпеки і якості ІКС критичного застосування в цілому.

Вимога проведення незалежної верифікації та валідації має на увазі доказову, засновану на кількісних оцінках реалізацію принципу технологічного і адміністративного різноманіття.

Доказова вимірювана реалізація принципу технологічної різноманітності є базовою концепцією досягнення необхідної вірогідності результатів і рентабельності (ефективності) незалежної верифікації та валідації.

Доказовість полягає в наданні об'єктивних кількісних оцінок чутливості використовуваних методів верифікації ПЗ та ступеня різноманітності для кожної пари методів. Рішення цієї проблеми є вирішальним фактором, який визначає вірогідність результатів незалежної верифікації та валідації і ступінь невизначеності кількісних оцінок гарантоздатності та безпеки критичного ПЗ. При цьому одним з головних результатів незалежної верифікації повинне бути прогнозування прихованих дефектів ПЗ.

У той же час сучасна практика проведення незалежної верифікації та кваліфікаційних випробувань ПЗ значною мірою заснована на ручному аналізі. Через це має місце значний вплив суб'єктивного фактору на якість оцінок. Як наслідок, після проведення таких випробувань існують проблеми повноти, достовірності і високої трудомісткості оцінок критичного ПЗ та викликані цим ризики існування прихованих дефектів ПЗ.

Необхідними умовами досягнення високого рівня надійності та безпеки критичного ПЗ є наявність адекватного (ефективного) нормативно-методичного забезпечення та широкомасштабне застосування інструментальних засобів підтримки процесів кваліфікаційних випробувань (експертизи), що відображають сучасний динамічний розвиток стандартизації у сфері інформаційних технологій та програмної інженерії. Основним напрямком підвищення достовірності оцінок якості ПЗ ІКС критичного застосування під час кваліфікаційних випробувань є диверсифікація технологій верифікації. Виконання цих умов вирішальним чином визначає реальні можливості гарантування необхідного рівня безпеки та якості ІКС в цілому, в тому числі в межах risk-informed підходів до регулювання безпеки. Оцінка характеристик якості ПЗ ІКС критичного застосування з врахуванням ризиків прихованих дефектів ПЗ є актуальною складовою реалізації risk-informed підходів до регулювання безпеки та кваліфікаційних випробувань ІКС критичного застосування в різноманітних прикладних галузях (АЕС, космос, транспорт та інше).

Метою є розробка методології доказової незалежної верифікації та валідації ПЗ, важливого для безпеки, та інтегрованого інструментального середовища, що включає утиліти підтримки незалежної верифікації на аналітичному, інформаційному та и організаційному рівнях. Методологія базується на диверсифікованому вимірюванні семантичних, інтервально-точностних, логічних та інших інваріантів кри-

 

тичного ПЗ в режимі статичного аналізу вихідних кодів. Інваріанти являють собою властивості ПЗ, які залишаються незмінними по визначенню протягом життєвого циклу ПЗ. Множина контрольованих (вимірюваних) інваріантів ПЗ визначає специфікацію моделей вихідного ПЗ та відповідно, диверсних методів виміру інваріантів [1]. Збереження значень обмірюваних інваріантів є визначальною характеристикою якості ПЗ. Для перевірки кожного з інваріантів будується відповідна модель представленого на експертизу програмного забезпечення. Теоретичне обґрунтування придатності використання підходу орієнтованого на моделях для перевірки ПЗ розроблено Кларком [2]. На відміну від методу верифікації моделей або перевірки на моделях (Model Checking), де вся специфікація представляється як єдиний інваріант, необхідно зосередитися на контролі збереженості окремих формальних властивостей, перевірки яких можуть бути автоматизовані.

Нововведенням пропонованої методології доказової незалежної верифікації є визначення на основі виміру інваріантів у режимі статичного аналізу вихідних текстів кількісних значень характеристик гарантоздатності і безпеки, прогнозу імовірності прихованих дефектів у ПЗ та оцінки тестового покриття.

Кількісні оцінки засновані на експериментальному калібруванні чутливості і ступеню різноманітності методів виміру інваріантів в умовах конкретного проекту ПЗ з урахуванням специфічних спектрів операцій і даних [3].

**Особливості підходу**

В якості базової методології отримання метричної або статистичної інформації про об'єкти ПЗ виявлення відхилень від стандартів, верифікації коректності об'єктів ПЗ пропонується статичний аналіз ПЗ. Використання статичного аналізу програмного коду як процедури оцінки безпеки ІКС АЕС коду є перспективним напрямком реалізації незалежної верифікації та регламентовано стандартами Міжнародної електротехнічної комісії [4,5].

Пропонується розширення методології статичного аналізу для вирішення завдання диверсифікації методів оцінювання характеристик якості ПЗ ІКС критичного застосування (згідно з серією стандартів ISO/IEC 9126, ISO/IEC 14598) на основі вимірювання семантичних, інтервально-точностних та логічних інваріантів ПЗ з використанням метрик „Фізична розмірність", „Інтервальні обмеження", „Точність" змінних, «Логіка виконання» ПЗ та інших.

Розширення включає наступні функції (процедури):

- вхідний контроль (розбір) вихідного коду ПЗ. Побудова синтаксичної моделі ПЗ;

- інструментування вихідного ПЗ. Перетворення синтаксичної моделі ПЗ у множину моделей з механізмами контролю (на підставі розроблених алгебр) семантичних, інтервально-точностних та логічних інваріантів конкретного проекту шляхом лінеаризації структури вихідного ПЗ;

- рекурсивна інтерпретація множини моделей коду ПЗ. В результаті виконання процедур перевірки вимірюються та реєструються значення семантичних, інтервально-точностних та логічних інваріантів для всіх реалізованих в проекті ПЗ ланцюжків операторних відображень;

- оцінювання атрибутів ПЗ. Зареєстровані сукупності значень інваріантних властивостей представляють системи лінійних алгебраїчних рівнянь та нерівностей. Існування єдиного рішення цих систем є критерієм коректності вихідного ПЗ та означає збереження інваріантів для всіх реально реалізованих в ПЗ ланцюжків операторних відображень. Для практично можливих випадків відсутності описів відповідних характеристик передбачається їх відновлення шляхом формування та аналізу відповідних гіпотез;

- калібрування методів вимірювання інваріантів ПЗ. Калібрування дозволяє визначити кількісні значення повноти тестового покриття, чутливість використаних методів виміру інваріантів, індикатор ефективності реалізації композиції діверсних методів і, як результат, обчислити імовірності прихованих дефектів у ПЗ.

Калібрування здійснюються методом «посіву» тестових дефектів відповідно до встановлених профілів дефектів. Використається модифікований метод «краплинної» ін'єкції одиночного тестового дефекту певного типу, що дозволяє виключити ефекти «інтерференції» і «мутації» дефектів при «посіві». Його суть складається у реалізації в обраній крапці адресно-временного простору комплексної процедури «ін'єкція тестового дефекту - виявлення - повернення у вихідний стан». Така процедура визначає тимчасово створювану контрольну крапку або «зонд», за допомогою якого оцінюється парціальна чутливість кожного діверсного методу виміру інваріантів до кожного типу дефектів, установленим нормативним профілем

для калібрування. Кількість контрольних крапок (зондів) вибирається виходячи з досягнення статистично достовірних результатів калібрування при мінімальних витратах ресурсів або інших слів прийнятної рентабельності незалежної верифікації і валідації в цілому.

Калібрування дозволяє статистично оцінити контролюючу здатність або результативність кожного методу виміру інваріантів, визначити реальний ступінь розмаїтості методів виміру інваріантів попарно та результуючу чутливість використаних методів. Пропонованими методами виміру інтервально-числових, семантичних, логічних та інших інваріантів для верифікації забезпечується охоплення (перевірка) всіх входжень інваріантів у вихідні тексти ПЗ. Це забезпечує можливість оцінки статистичної складового показника повноти тестового покриття вихідного ПЗ при незалежній верифікації і валідації.

**Сценарій доказової незалежної верифікації**

Методологія проведення доказової незалежної верифікації представлена у вигляді сценарію, який включає три базових методики:

1. Нормалізація проекту ПЗ;
2. Вимір інваріантів ПЗ в режимі статичного аналізу;
3. Експериментальне калібрування. Інтегральна оцінка.

Функціональна модель сценарію (рис. 1) розробляється на основі методології IDEF0 моделювання та представляє ієрархію моделей різних рівнів деталізації процесів сценарію. Дерево вузлів функціональної IDEF0-моделі сценарію незалежної верифікації з деталізацією до 2-го рівня вкладеності подано на рис.2. Проведення сценарію підтримується на аналітичному, інформаційному та організаційному рівнях.

**Методика «Нормалізація проекту ПЗ»** включає:

- формування профілю інваріантів проекту ПЗ;
- формування і верифікацію нормативного профілю вимог для оцінюваного проекту;
- оцінка плануємої повноти тестового покриття при вимірі інваріантів.

**Методика «Вимір інваріантів у режимі статичного аналізу вихідного ПЗ»** включає:

- інструментування вихідного ПЗ: побудова базової моделі ПЗ. Розкриття специфікації інваріантів проекту ПЗ;
- формування моделей для виміру інваріантів ПЗ;
- вимір і контроль збереження значень інваріантів за допомогою моделей.

**Методика «Експериментальне калібрування методів виміру інваріантів. Інтегральна оцінка характеристик ПЗ»** включає:

- Формування профілю тестових дефектів
- параметричне керування калібруванням чутливості і ступеню різноманітності діверсних методів виміру інваріантів;
- оцінку прогнозованих ризиків аномального функціонування ПЗ через приховані дефекти;
- оцінку повноти тестового покриття;
- інтегровану оцінку характеристик якості проекту ПЗ.

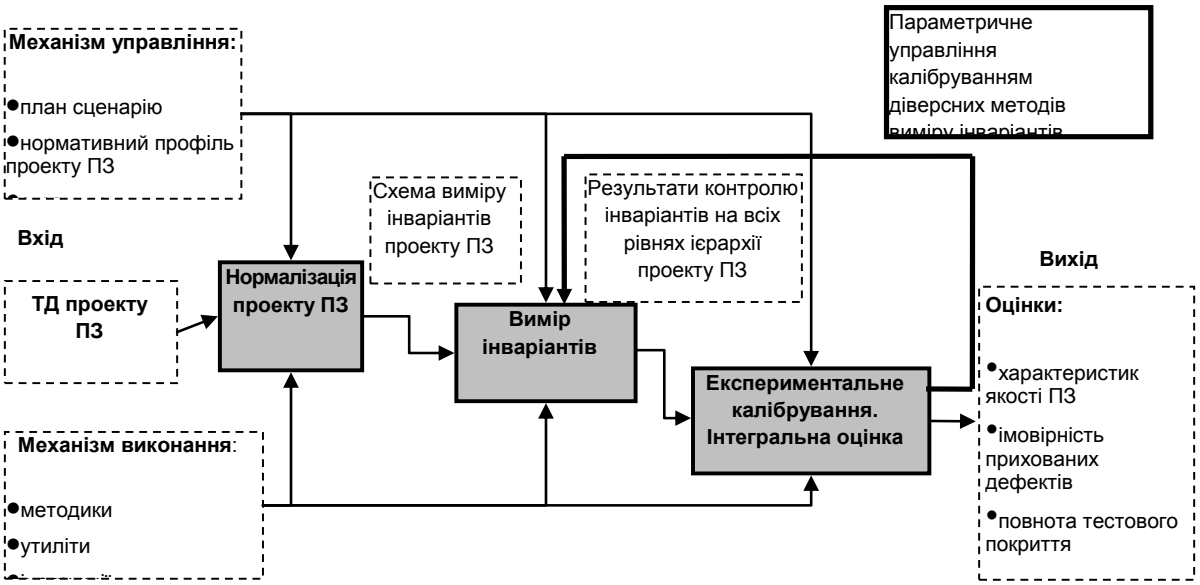


Рис. 1 Модель доказової незалежної верифікації на базі вимірів інваріантів з використанням калібрування (функціональна модель сценарію)

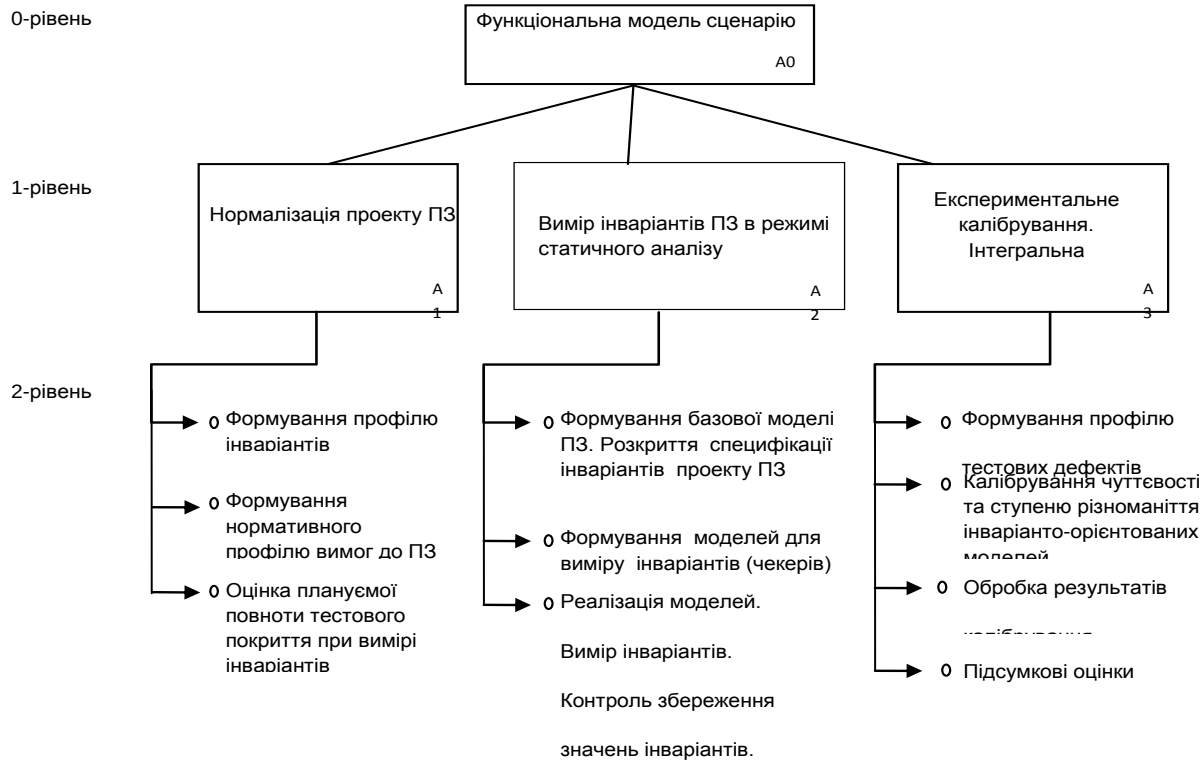


Рис. 2. Дерево вузлів функціональної IDEF0-моделі сценарію

Деталізація методик з описом входів, процесів і результатів (виходів) наведені нижче.

## 1 Методика «Нормалізація проекту ПЗ».

Дана методика, разом з підтримуючими її програмними утилітами, дозволяє виконати:

- вхідний контроль (відповідність нормативним вимогам) представлених для незалежної верифікації матеріалів;

- формування нормативного профілю вимог;
- формування профілю інваріантів проекту ПЗ на основі аналізу програмно реалізованих функцій проекту ПЗ;
- оцінку плануємої повноти тестового покриття при вимірі інваріантів.

IDEF0 модель методики наведена на рис. 3

**Вхідні** дані **для методики:** технічна документація (технічне завдання, проектні рішення, алгоритми та інші матеріали, надані для випробувань), нормативні вимоги, вихідні тексти ПЗ. Надалі використовується узагальнююча назва наданих матеріалів – об'єкт експертизи (ОЕ).

Методика має реалізувати наступні процеси:

*1.1 Формування профілю інваріантів проекту ПЗ (позначення вузла на діаграмі - А1.1)*

**Входи:** об'єкт експертизи (ОЕ).

**Дії процесу:** виконується вхідний контроль документації, що надана на експертизу. В результаті має бути виділене ПЗ, що придатне для автономних перевірок. Далі мають бути ідентифіковані інваріанти і сформовано профіль інваріантів для проекту.

**Виходи:** загальний профіль інваріантів.

*1.2 Формування нормативного профілю вимог (НПВ) до ПЗ ( А1.2)*

**Входи:** об'єкт експертизи.

**Дії процесу:** за допомогою встановлених правил формування НПВ аналізується нормативна база, виділяються вимоги до ОЕ і формується НПВ конкретного проекту.

**Виходи:** нормалізований НПВ.

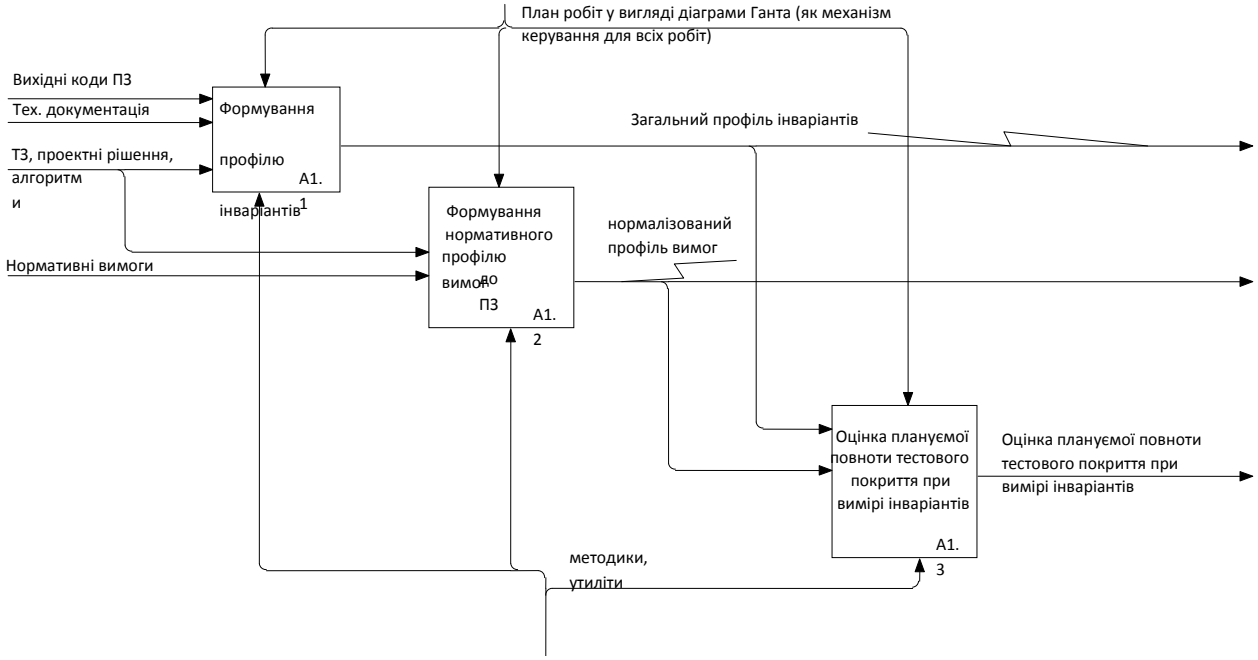


Рис.3 Нормалізація проекту ПЗ

*1.3 Оцінка плануємої повноти тестового покриття при вимірі інваріантів (А1.3)*

**Входи:** загальний профіль інваріантів; НПВ.

**Дії процесу:** виконується трасування елементів отриманих профілю інваріантів та нормативного профілю вимог і оцінка відношень еквівалентності та імплікативності. Аналіз відношень дає можливість виконати оцінку плануємої повноти тестового покриття ПЗ, що перевіряється шляхом виміру і контролю збереження інваріантів.

**Виходи:** оцінка плануємої повноти тестового покриття при вимірі інваріантів.

Результатом методики «**Нормалізація проекту ПЗ**» мають бути: профіль інваріантів; нормативний профіль вимог; оцінка плануємої повноти тестового покриття при вимірі інваріантів.

## 2 Методика «Вимір інваріантів у режимі статичного аналізу вихідного ПЗ»

Дана методика, разом з підтримуючими її програмними утилітами, дозволяє:

- настроїти утиліти на роботу з даним типом проекту;
- сформувати моделі ПЗ для виміру інваріантів відповідно до профілю інваріантів конкретного проекту ПЗ;
- виміряти і проконтролювати збереженість значень інваріантів.

IDEF0 модель методики наведена на рис. 4.

**Вхідні дані для методики:** ТЗ, проектні рішення, алгоритми; загальний профіль інваріантів.

Методика має реалізувати наступні процеси:

*2.1 Формування базової моделі ПЗ. Розкриття специфікації інваріантів проекту ПЗ (А 2.1).*

**Входи:** ТЗ, проектні рішення, алгоритми; загальний профіль інваріантів.

**Дії процесу**: ОЕ за допомогою комплексу утиліт статичного аналізу (СА) повинен бути приведений до проміжного (внутрішнього) коду (представлення об'єкта, що перевіряється, усередині системи, призначене для побудови моделей виміру інваріантів). Щоб таке перетворення виконалося автоматично необхідно одноразово для кожного діалекту мови програмування виконати настроювання на конкретний діалект мови програмування. За допомогою програмної утиліти настроювання формується базова модель ОЕ (ОЕ приводиться до проміжного коду). Аналізуючи базову модель із загального профілю інваріантів, формується профіль інваріантів конкретного проекту ПЗ.

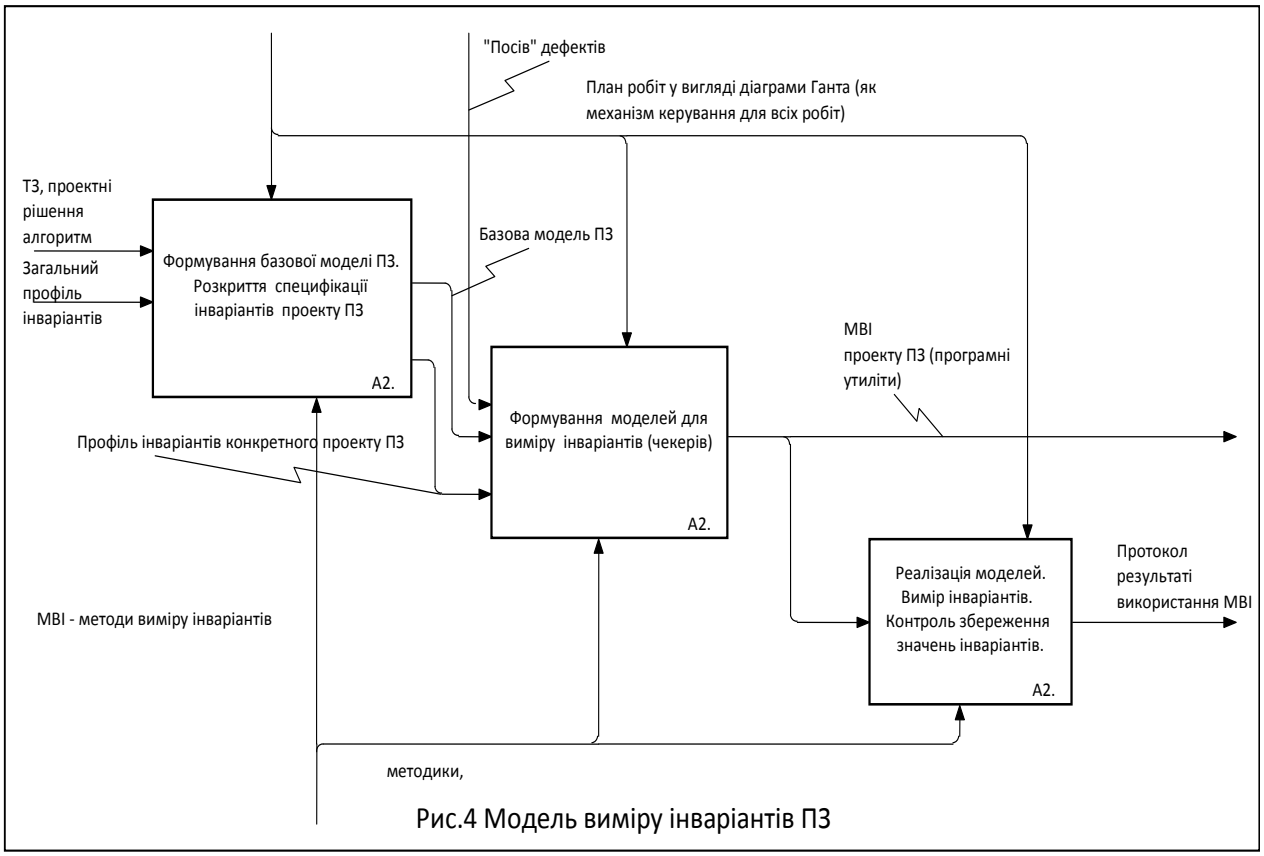


Рис.4 Модель виміру інваріантів ПЗ

**Виходи:** базова модель ПЗ (проект ПЗ у вигляді проміжного коду); профіль інваріантів конкретного проекту ПЗ.

*2.2 Формування моделей для виміру інваріантів (чекерів) (А 2.2).*

**Входи:** базова модель ПЗ, специфікація (профіль) інваріантів конкретного проекту ПЗ.

**Дії процесу:** виконується формування моделей для виміру всіх інваріантів, що присутні в проекті.

**Виходи:** моделі для виміру інваріантів.

*2.3 Реалізація моделей. Вимір інваріантів. Контроль збереження значень інваріантів (А 2.3).*

**Входи:** моделі для виміру інваріантів.

**Дії процесу:** виконується вимір значень інваріантів конкретного проекту. Надалі необхідно інтерпретувати результати виміру інваріантів: установити еталонні значення для інваріантів (або правила їхнього формування) і виконати автоматизовані процедури контролю збереженості інваріантів.

**Виходи:** Протокол результатів виміру та контролю значень інваріантів.

Результатом методики «Вимір інваріантів ПЗ в режимі статичного аналізу» мають бути: моделі для виміру інваріантів; методики контролю збереженості інваріантів; результати контролю значень інваріантів (протокол).

## 3 Методика «Експериментальне калібрування методів виміру інваріантів. Інтегральна оцінка характеристик ПЗ»

Використання даної методики, разом з підтримуючими її програмними утилітами, повинне дозволити:

- оцінити результати застосування моделей для виміру інваріантів та установити ступінь покриття вихідного коду перевірками;
- за результатами калібрування вибрати оптимальний набір методів. Визначити при цьому надлишкові методи (що не перевіряють нові види дефектів);
- сформувати підсумковий протокол робіт, проведених за сценарієм.

IDEF0 модель методики наведена на рис. 5.

Входи: нормалізований ОЕ (ОЕ представлений у вигляді проміжного коду); результати вимірювання і контролю незмінності інваріантів.

Методика має реалізувати наступні процеси:

*3.1 Формування профілю тестових дефектів (А 3.1).*

Під профілем тестових дефектів розуміється перелік типів дефектів, можливих у конкретному проекті ПЗ, які будуть використані для процедури калібрування.

**Входи:** нормалізований ОЕ; використовувані конструкції; можливі перекручування.

**Дії процесу:** повинні бути виконані:

– аналіз використовуваного діалекту мови програмування, у ході якого проводиться аналіз мовних конструкцій, їхня класифікація й аналіз можливих спотворень для встановлених видів конструкцій;

– безпосереднє формування профілю тестових дефектів з урахуванням специфіки конкретного проекту ПЗ. Виконується побудова класифікаційної схеми спотворень у прив'язці до класифікаційної схеми конструкцій - визначається профіль дефектів конкретного проекту. Отриманий профіль дефектів необхідно оцінити на предмет повноти й придатності для використання в конкретних умовах (необхідно визначити принципову можливість внесення визначених типів дефектів в конкретний проект).

Виходи: профіль дефектів;

*3.2 Калібрування чуттєвості та ступеню різноманіття інваріанто-орієнтованих моделей (А3.2).*

**Входи:** моделі для виміру інваріантів; профіль дефектів; результати контролю інваріантів.

**Дії процесу:** проводиться визначення конструкцій, що перевіряють методами виміру інваріантів (МВІ) і типів дефектів, до яких чутливі МВІ, визначається метод калібрування МВІ (механізм внесення тестових дефектів) і фіксується чутливість/нечутливість кожного методу до внесених дефектів.

**Виходи:** методика калібрування, вимоги до утиліт, що реалізують процедуру калібрування (включаючи системний інтерфейс).

*3.3 Обробка результатів калібрування (А3.3).*

**Входи:** результати калібрування.

**Дії процесу:** повинні бути оброблені отримані в результаті калібрування дані для оцінки чутливості і ступеню різноманітності МВІ і оцінки повноти тестового покриття. Необхідно визначити оптимальний набір МВІ за критерієм забезпечення необхідного тестового покриття при мінімальних ресурсовитратах.

**Виходи:** методики оцінки чутливості МВІ, оцінки повноти тестового покриття, визначення ступеню різноманітності МВІ і визначення оптимального набору МВІ.

*3.4 Підсумкові оцінки (А3.4).*

**Входи:** результати виконання процесів 3.1 – 3.3 даної методики.

**Дії процесу:** накопичена під час виконання процесів 3.1 – 3.3 інформація повинна бути збережена в загальну базу даних. Для цього використовується відповідна структура сховища. За допомогою отриманих даних необхідно зробити оцінку якості програмного забезпечення, представленого на експертизу. Використовуються метрики: імовірність прихованих де-

фектів, повнота тестового покриття, що характеризують якість ПЗ.

**Виходи:** метрики характеристик якості ПЗ, результати їх використання.

Результатом методики «Експериментальне калібрування. Інтегральна оцінка» мають бути: профіль дефектів, метод калібрування, метрики характеристик якості ПЗ.

**Переваги підходу**

При використанні розробленої системи створюються умови для реалізації керованої повноти перевірки ПЗ в залежності від специфіки проекту.

Забезпечується:

– можливість досягнення 100%-вих перевірок відповідності проекту ПЗ формалізованим вимогам нормативного профілю;

– виключення надмірності і зменшення обсягів ручних рутинних операцій та, на цій основі, значне скорочення трудомісткості реалізації сценаріїв і підвищенні рентабельності оцінки якості ПЗ;

– можливість використання інтегрованого інструментального середовища при розробці ПЗ ІКС критичного застосування, для яких обов'язковою нормативною вимогою є проведення незалежної верифікації.

Інтегроване інструментальне середовище включає комплекс взаємодіючих, повністю комп'ютеризованих утиліт, що виконують базові функції системи, та відповідних методик, які реалізуються безпосередньо користувачами-експертами за чітко розробленою послідовністю – сценарієм. Частка операцій, зокрема при формуванні профілів проектів, потребує відповідної кваліфікації користувачів.

Універсальність утиліти статичного аналізу обмежується на даному етапі мовами програмування вихідного коду ПЗ, але у проекті будуть надані чіткі рекомендації щодо зняття цього природного обмеження шляхом створення відповідних емуляторів. Інше обмеження, пов'язане з універсальністю профілю дефектів, що повинні відповідати вимогам проектної документації та виявлятися при використанні системи, є не критичними завдяки відкритій архітектурі і можливості нарощування засобів тестування.

Очікуване зниження ймовірності прихованих дефектів ПЗ після доказової незалежної верифікації, може складати до 100% в залежності від реального ступеню різноманітності диверсних методів оцінки характеристик якості в умовах конкретного проекту ПЗ. Експериментальне визначення чутливості та ступеню різноманітності диверсних методів верифікації, з урахуванням специфіки конкретного проекту ПЗ, проводиться за допомогою калібрування методом „посіву" дефектів ПЗ згідно з встановлюваними профілями, що враховують специфіку конкретного проекту ПЗ.

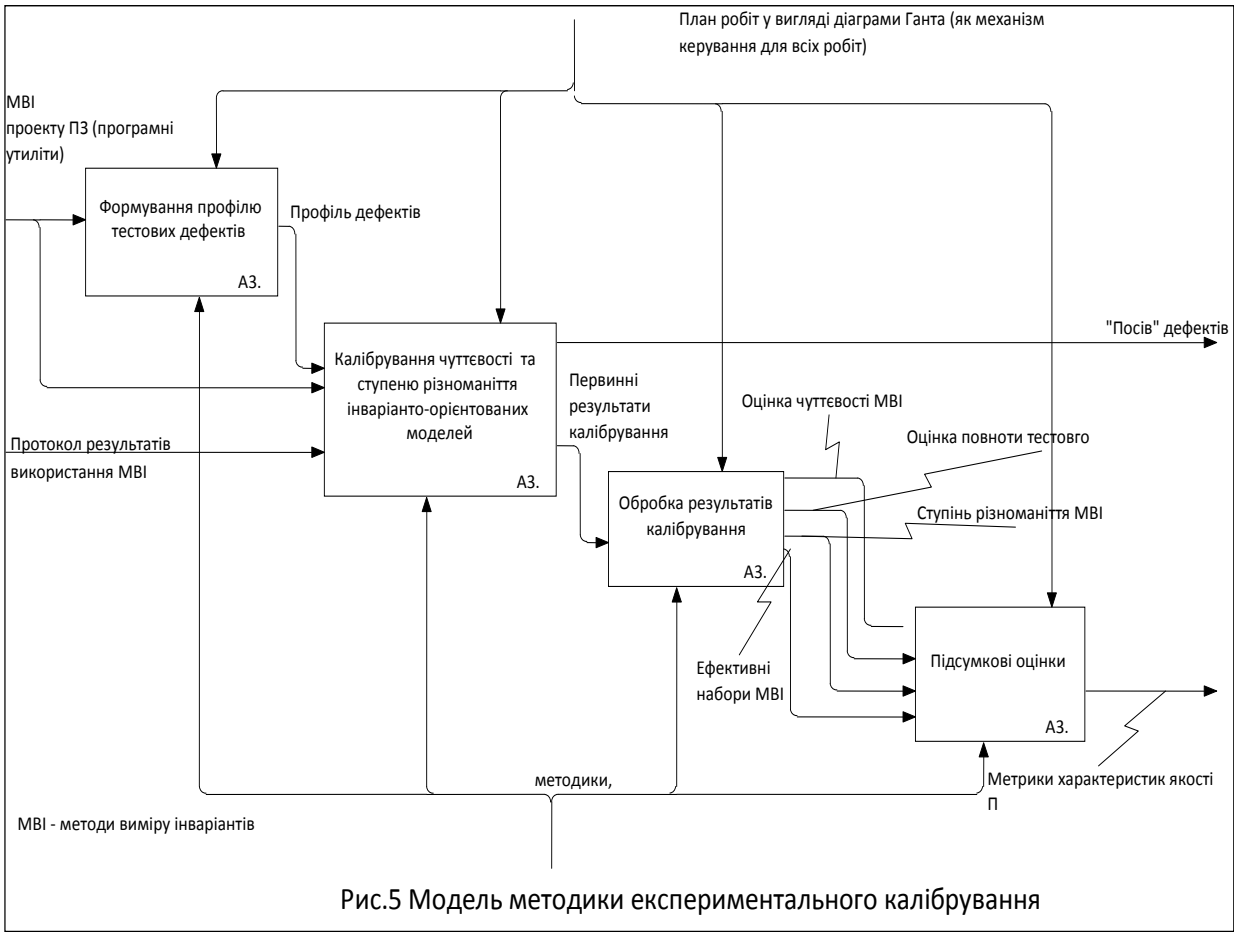


Рис.5 Модель методики експериментального калібрування

**Висновки**

Запропонований підхід забезпечує рішення наступних задач:

- одержання достовірних оцінок характеристик якості ПЗ за рахунок доказової (вимірюваної) реалізації принципів технологічної різноманітності (диверсифікованості) незалежної верифікації на основі виміру семантичних, інтервально-точностних, логічних та ін. інваріантів ПЗ на платформі статичного аналізу вихідного ПЗ;
- прогнозування імовірності прихованих дефектів ПЗ на основі експериментального калібрування чутливості та ступеня різноманітності методів виміру інваріантів в умовах конкретного проекту ПЗ, методом посіву тестових дефектів;
- керування рентабельністю (шляхом мінімізації ресурсів, які витрачають) прогнозування імовірності прихованих дефектів при композиції методів виміру інваріантів, за допомогою статичного аналізу з меншим ступенем консервативності та використанням індикатора зниження імовірності залишкових дефектів ПЗ;
- оцінку повноти тестового покриття критичного ПЗ методом прямої і зворотного трасування для оцінки відносин еквівалентності ті імпликативності множин диз'юнктів: а) опорної (посилальної) і оцінної моделей якості ПЗ; б) специфікації технічних вимог до ПЗ); в) проектних визначень і обґрунтувань (проектно-конструкторської документації ПЗ), а також статичного складового показника повноти тестового покриття при випробуваннях (перевірках, незалежній верифікації) ПЗ
- розробки методів метрико-імовірнісної оцінки надійності та гарантоздатності програмних засобів та ІКС взагалі;
- розробку комплексів утиліт, що забезпечують підтримку сценарію доказової незалежної верифікації на аналітичному, організаційному та інформаційному рівнях, і досягнення необхідних вірогідності та ступеню невизначеності результатів.

**Література**

1. *Конорев Б.М.* Инварианто-ориентированная оценка качества программного обеспечения космических систем/ Конорев Б.М., Харченко В.С., Алексеев Ю.Г., Манжос Ю.С., Сергиенко В.В., Чертков Г.Н. / Монография. Под ред. Конорева Б.М., Харченко В.С. – Харьков: ГП Госцентркачества, Национа-

льный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2009. – 224 с.

2. *Кларк Э.М.* Верификация моделей программ: Model Checking / Э.М. Кларк, О. Грамберг, Д. Пелед Пер. с англ. / Под ред. Р. Смелянского. — М.: МЦНМО, 2002. – 416 с.

3. *Конорев Б.М., Сергиенко В.В., Новы Л., Чертков Г.Н.* Калибровка методов измерения инвариантов критического программного обеспечения: профиль инъектируемых тестовых дефектов// Радіоелектронні і комп'ютерні системи. Науково-технічний журнал №6 (25), Харків, "ХАІ" 2008, с.161-167 (ISSN 1814-4225).

4. IEC 60880 ed2:2006. Nuclear power plants – Instrumentation and Control systems important for safety – Software aspects for computer-based systems performing category A functions.

5. IEC 62138:2004. Nuclear power plants – Instrumentation and Control systems important for safety – Software aspects for computer-based systems performing category B and C functions.

**Відомості про авторів**:

**Конорев Борис Михайлович** – д.т.н., професор кафедри інженерії програмного забезпечення Національного аерокосмічного університету ім. М.Є. Жуковського "ХАІ", Харків, Україна.
e-mail: admin@scasu.com

**Сергієнко Володимир Володимирович** - керівник випробувальної лабораторії інформаційно-обчислювальних систем керування Сертифікаційного центру АСУ ДП Держцентрякості, Харків, Україна.
e-mail: admin@scasu.com

**Туркін Ігор Борисович** – д.т.н., професор, зав каф. інженерії програмного забезпечення Національного аерокосмічного університету ім. М.Є. Жуковського "ХАІ", Харків, Україна.
e-mail: energy@d4.khai.edu.

Стаття надійшла до редакції 16.02.2011 р.

 