**ЛЕТИЧЕВСЬКИЙ**
**Олександр Адольфович –**
академік НАН України,
завідувач відділу теорії цифрових автоматів Інституту кібернетики ім. В.М. Глушкова НАН України

# ВИСОКОНАДІЙНІ СИСТЕМИ МАТЕМАТИЧНОГО ЗАБЕЗПЕЧЕННЯ

## Стенограма наукової доповіді на засіданні Президії НАН України 7 грудня 2016 року

*Доповідь присвячено важливій проблемі створення методів та алгоритмів побудови високонадійних систем математичного забезпечення для програмно-технічних комплексів, які використовуються в критичних з точки зору безпеки галузях, таких як аерокосмічна, медична, телекомунікаційна, в ядерній енергетиці, у виробництві сучасного озброєння тощо. Процес розроблення високонадійних систем оснований на принципі зменшення ризику або повного виключення неспрацьовування засобів безпеки в системі.*

Шановні члени Президії! Шановні колеги!

Нерідко виникає питання: чому українські програмісти так високо цінуються в зарубіжних країнах? Відповідь, на мій погляд, полягає в традиціях виховання спеціалістів у нашій країні. З одного боку, на старших курсах університетів фахові дисципліни викладають зазвичай співробітники академічних інститутів, які ознайомлюють студентів з найбільш загальними сучасними методами й технологіями комп'ютерної науки, що мають *широке поле застосування*. З іншого боку, на молодших курсах університетів студентам забезпечується можливість опанувати *широкий спектр фундаментальних знань*. Тому українським програмістам притаманна *гнучкість мислення* та *готовність до адаптації* у різних спеціальних предметних галузях.

Одній із таких сучасних технологій, яка основана на алгебраїчній теорії інформаційних взаємодій у багатоагентних розподілених середовищах і називається *інсерційним моделюванням*, і присвячено мою сьогоднішню доповідь на засіданні Президії НАН України. Важливим застосуванням інсерційного моделювання є створення високонадійних систем математичного забезпечення.

Надійність програмних систем є зовнішня та внутрішня. Зовнішня забезпечує захист від несанкціонованого втручання, внутрішня — відсутність помилок, надійність та коректність внутрішньої взаємодії програмних компонентів. Інші аспек-

ти надійності комп'ютерних систем пов'язані з надійністю систем технічного забезпечення. В Інституті кібернетики ім. В.М. Глушкова НАН України та в інститутах Кібернетичного центру НАН України проводяться дослідження, які охоплюють усі аспекти проблеми надійності програмних систем. Однак у цій доповіді ми обмежимося лише розглядом внутрішньої надійності.

Вимоги високої надійності насамперед стосуються систем, критичних до безпеки (так званих *safety-critical systems*). До таких систем, зокрема, належать системи, які використовують в аерокосмічній і медичній галузях, в ядерній енергетиці, виробництві сучасної зброї, управлінні залізницями, в автомобільній промисловості, телекомунікаційній і мікропроцесорній індустрії та ін. Відмови в цих системах пов'язані із загрозою життю людей, втратою чи руйнуванням устаткування, забрудненням навколишнього середовища тощо. Процес розроблення високонадійних систем оснований на принципі зменшення ризику або повного виключення неспрацьовування умови безпеки в роботі системи.

Програмна інженерія систем, критичних до безпеки, ґрунтується на включенні в процес розроблення процедур верифікації та валідації. Сучасні методи верифікації потребують застосування формальних методів, побудови математичних моделей та генерації тестових наборів, що забезпечують максимальне покриття програмних кодів.

Проектування та аналіз складних систем на всіх етапах їх розроблення потребує побудови формальних моделей різних рівнів абстракції. Застосування формальних моделей дає змогу виявляти неправильні рішення, помилки та некоректності ще на ранніх етапах, що значно зменшує зусилля та заощаджує кошти порівняно з тим випадком, коли ці помилки виявляються на пізніх етапах розроблення або в готовій продукції.

На рис. 1 наведено (щоправда, дуже спрощено) фрагмент життєвого циклу системи математичного забезпечення та його трансформацію в разі застосування технології інсерційного моделювання. Основною особливістю цієї технології є побудова формальної моделі вимог на етапі дизайну та включення

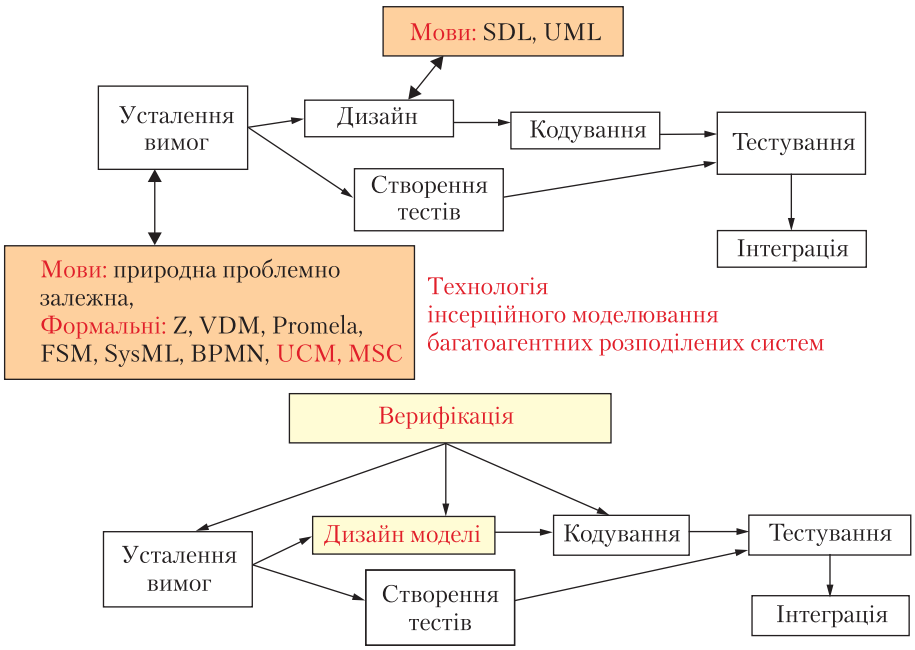


***Рис. 1.*** Фрагмент життєвого циклу системи математичного забезпечення

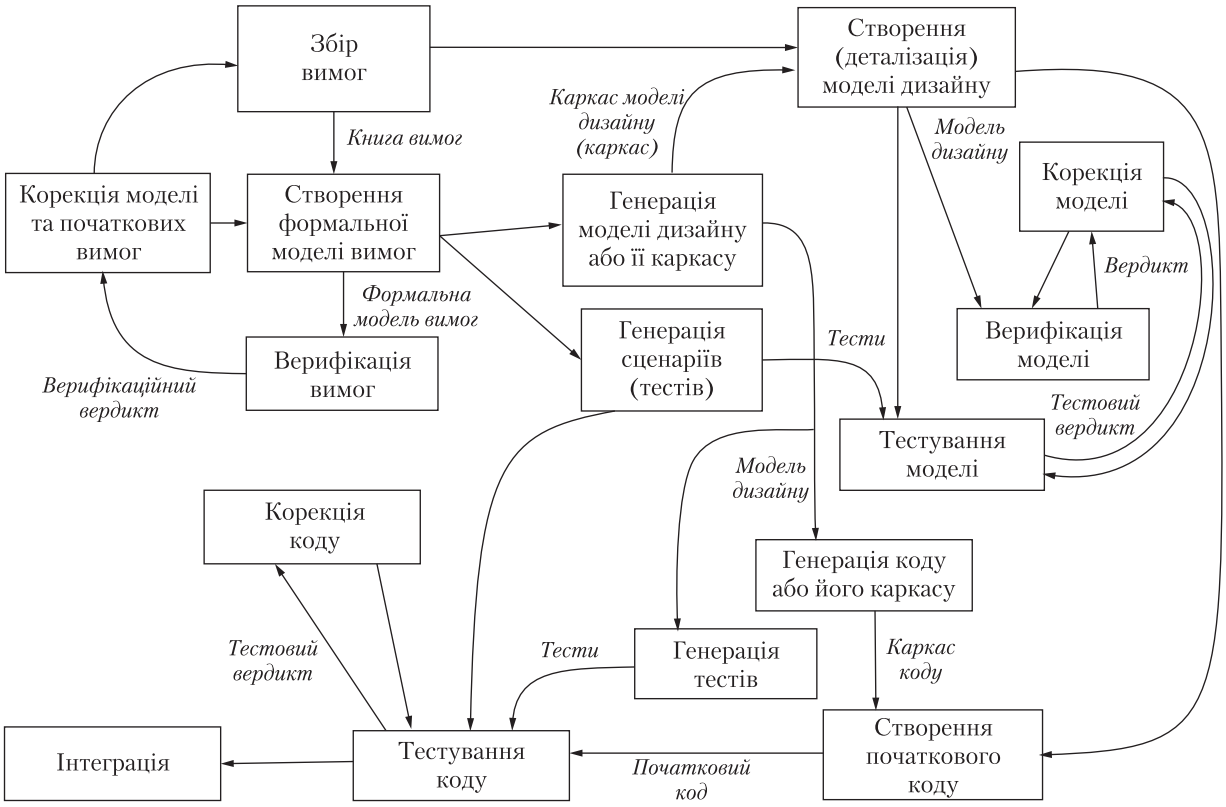


***Рис. 2.*** Загальна схема розроблення високонадійної системи модельним методом (із застосуванням інсерційних моделей)

процедур верифікації. Формальна модель використовується також для генерації тестів, які забезпечують необхідні параметри надійності системи.

На рис. 2 показано більш детальну схему розроблення високонадійних програмних систем. Наведено етапи, на яких створюються та застосовуються формальні моделі системи.

В інсерційних моделях систему представлено у вигляді композиції середовища та агентів, занурених у нього. Середовище та агенти представлено як транзиційні (динамічні) системи, що еволюціонують у часі та мають спостережувану ззовні поведінку.

Основи інсерційного моделювання було закладено наприкінці 90-х років минулого століття в роботах про модель взаємодії агентів та середовищ, а практичне використання інсерційного моделювання відноситься до початку 2000-х років, коли на замовлення фірми Motorola в українській компанії ISS (Information Software Systems) за участю співробітників Інституту кібернетики ім. В.М. Глушкова НАН України було розроблено першу систему автоматичної верифікації вимог до програмних систем VRS (верифікація вимог та специфікацій). В подальшому цю систему придбала американська компанія UniqueSoft, з якою ми й дотепер дуже плідно співпрацюємо. На основі системи верифікації було створено нові засоби проектування та дизайну, зокрема засоби тестування і генерації коду.

Отже, математичною основою інсерційного моделювання є, як я вже говорив, алгебраїчна теорія взаємодії. Інсерційне моделювання узагальнює традиційні підходи до теорії взаємодії інформаційних процесів, основані на алгебрах та численнях процесів (CCS, CSP, ACP, π-числення, мобільні амбієнти та багато інших напрямів у загальній алгебро-логічній теорії

взаємодії). Основні методи, теоретичні та практичні побудови в інсерційному моделюванні продовжують традиції школи В.М. Глушкова в комп'ютерній науці, що ґрунтуються на теорії автоматів, алгебрі алгоритмів, методах автоматичної перевірки суджень, макроконвеєрних обчисленнях та ін.

Базові принципи парадигми інсерційного моделювання, які мотивують його можливі застосування, прості й достатньо зрозумілі. Вони містять у собі такі положення (рис. 3).

1. Система складається з ієрархії середовищ та агентів, занурених у ці середовища. Мова може йти про технічні, програмно-технічні, а також про біологічні, соціальні та економічні системи. При побудові моделей таких систем нас цікавить передусім їх взаємодія в багатоагентному середовищі.

2. Середовища та агенти є об'єктами, що еволюціонують у часі та мають спостережувану поведінку. До таких систем належать як неперервні класичні динамічні системи, так і дискретні системи (автомати, транзиційні системи, моделі програм). Поведінка системи характеризує її зовнішні інваріанти і є основою взаємодії.

3. Занурення нового агента в середовище змінює поведінку цього середовища. Як приклад можна навести комп'ютер, який є середовищем для агентів — програм. Першою програмою, яку на ньому встановлюють, є, звичайно, операційна система, яка перетворює вихідний комп'ютер на юнікс- або віндовз-комп'ютер і, відповідно, змінює середовище, а установка сервісних агентів-програм забезпечує ефективну взаємодію з компонентами комп'ютерного середовища та користувачами.

4. Середовище як агент може бути занурене у середовище вищого рівня. Ця двоїстість (агент як середовище та як простий агент, який, у свою чергу, може бути занурений в інше середовище) дуже важлива для побудови необмеженої рекурсивної динамічної ієрархії компонент складної системи.

5. У багаторівневому середовищі агенти можуть переходити з одного середовища в інше (динамічність структури).

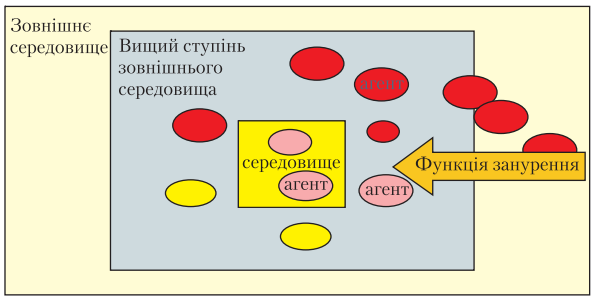


***Рис. 3***. Схема базових принципів парадигми інсерційного моделювання

6. Агенти та середовища можуть моделювати інших агентів та середовища на різних рівнях абстракції. Ця властивість відкриває можливість побудови когнітивних архітектур для моделювання розумової діяльності людини, а також створення інтелектуальних програмних систем (інтелектуальних агентів).

Одним з основних досягнень теорії інсерційного моделювання є побудова нової алгебри поведінок та її застосування при розв'язуванні багатьох важливих задач проектування надійних систем. На відміну від традиційної теорії взаємодії, основаної на звичайних алгебрах та численнях процесів, в інсерційному моделюванні використовується неперервна багатоосновна алгебра. Занурення агента в середовище змінює поведінку середовища за допомогою неперервного оператора занурення, який розглядається як один з операторів алгебри поведінок. Можливість збагачення алгебри поведінок введенням нових неперервних функцій та операторів дозволяє налаштовувати засоби проектування на необхідні проблемні області.

Основним методом дослідження інсерційних моделей є символьне моделювання атрибутних середовищ. Стани таких середовищ у символьному моделюванні є формулами числення предикатів з кванторами, а програмні реалізації символьних моделей використовують системи автоматичної дедукції.

Впровадження технології інсерційного моделювання здійснюється через компанію ISS, яка, як уже зазначалося, була заснована з допомогою партнерів з компанії Motorola на початку 2000-х років. Технологію було успішно

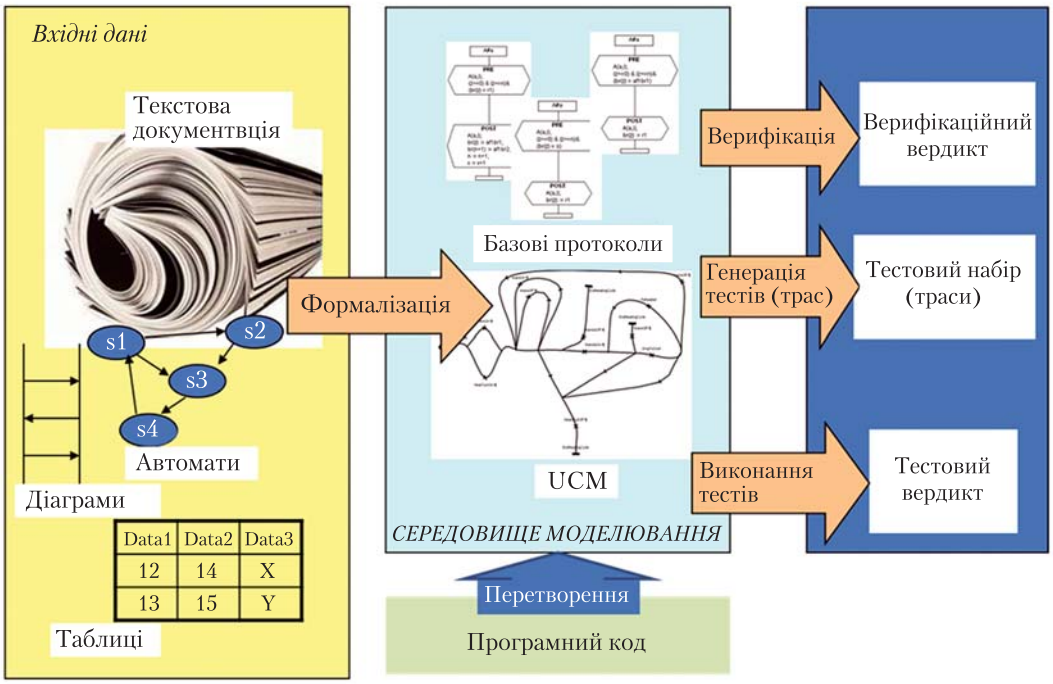


***Рис. 4***. Верифікація та тестування в системі IMS

апробовано в понад 150 проектах, виконаних спільно з фірмою Motorola у галузях мікропроцесорної, автомобільної, мережевої, телекомунікаційної індустрії. Зараз в ISS працює вже понад 100 співробітників і виконуються замовлення зарубіжних компаній. Група, до складу якої входить близько 40 фахівців з Інституту кібернетики ім. В.М. Глушкова НАН України та Національного технічного університету України «КПІ імені Ігоря Сікорського», працює за сумісництвом у дочірній компанії IssSoft за технологією інсерційного моделювання та іншими передовими західними технологіями.

Досвід, накопичений під час роботи із зарубіжними компаніями, було використано для розроблення в Інституті кібернетики ім. В.М. Глушкова власної системи інсерційного моделювання IMS (рис. 4), яка має засоби для створення високонадійних систем математичного забезпечення. У розробленні цієї системи беруть активну участь співробітники Херсонського державного університету. Засоби IMS включають програми символьної верифікації, генерації тестів із майже 100% покриттям коду або вимог, залежно від рівня абстракції моделі, програми генерації інваріантів, засоби оптимізуючих перетворень і рефакторингу програм та їх моделей.

Важливою сферою застосування цієї технології є розпаралелювання обчислювальних процесів на багатопроцесорних обчислювальних машинах та організація ефективних обчислень у мережевих і хмарних системах. Наприклад, результати досліджень з інсерційного моделювання було використано при виконанні спільних проектів з фірмою Intel. Проведено дослідження з верифікації паралельних програм, створених у середовищі бібліотеки MPI, а також анотовано більшість бібліотечних функцій, достатніх для використання в процесі верифікації та експериментів з реальними проектами.

У щойно завершеному проекті УНТЦ «Когнітивна архітектура для розуміння програмного забезпечення» було досліджено можливість

автоматичної формалізації вимог, виражених природною мовою.

Мова формальних моделей системи включає алгебро-логічні засоби опису поведінки систем у поєднанні із графічними мовами MSC та UCM, що належать до стандартів ITU. Формальна семантика цієї мови представлена за допомогою інсерційних моделей. Ця семантика використовується в процесі розроблення системи IMS, що забезпечує високу якість засобів.

До складу системи IMS входять такі групи засобів.

1. **Формалізація вимог**. Засоби побудови інсерційної моделі у вигляді атрибутного середовища та занурених у нього агентів (наприклад, телекомунікаційна система та користувачі).

2. **Статична перевірка вимог**. До цієї групи належать засоби перевірки властивостей системи формалізованих вимог:

• доведення повноти вимог (відсутність тупиків);

• доведення несуперечливості (детермінізм вимог);

• доведення властивостей безпеки.

3. **Динамічна перевірка властивостей** системи, що задовольняє вимогам, генерація конкретних та символьних трас (сценаріїв функціонування системи). Доведення динамічних властивостей виконується за допомогою розгортання системи рівнянь в алгебрі поведінок. Зокрема, цим забезпечується перевірка досяжності властивостей.

4. **Дедуктивна система** забезпечує перевірку властивостей, виражених у мові прикладного багатосортного (типізованого) числення предикатів першого ступеня, налаштованого на предметну галузь, до якої належить система. Дедуктивна система включає спеціалізовані прувери, алгоритми перевірки виконуваності та розв'язування обмежень у змішаних чисельно-логічних теоріях та використовується на всіх етапах проектування із застосуванням методу інсерційного моделювання.

5. **Генерація та виконання тестів**. Генерація тестів виконується на базі моделей вимог. Моделі системи, які з'являються на різних етапах розроблення, мають задовольняти вимогам, які лежать в основі проекту системи. Тому одним з основних критеріїв якості системи тестів є покриття всіх вимог до системи. Інші критерії залежать від рівня абстракції моделі. Для тестування готових кодів використовується, наприклад, критерій покриття всіх рядків коду. Виконання тестів відбувається під керуванням моделі відповідного рівня абстракції.

Досвід використання аналогічних засобів у компанії ISS здобуто в процесі верифікації та розроблення сотень систем із реального життя та різних предметних галузей, у тому числі таких, як телекомунікації, вбудовані системи (зокрема, з автомобільної промисловості), системи реального часу (наприклад, управління залізничною станцією) та ін.

Об'єми інформації, які фігурують у виконуваних проектах, вимірюються такими параметрами:

• десятки тисяч базових протоколів (формалізованих вимог);

• сотні атрибутів;

• сотні помилок, знайдених у документаціях;

• тисячі тестів, що забезпечують повне покриття вимог.

Дослідження з теоретичних основ та методів побудови систем, критичних до безпеки, із застосуванням формальних математичних методів проводяться в найбільших наукових центрах і компаніях Європейського Союзу та Сполучених Штатів Америки. Співпраця із зарубіжними IT-компаніями має великий позитивний вплив на молодих учених, які беруть участь у створенні промислових проектів, а потім застосовують набуті навички для розроблення нових вітчизняних технологій.

Сьогодні в Україні основи інсерційного моделювання викладаються в Київському національному університеті імені Тараса Шевченка, Херсонському державному університеті та інших вищих навчальних закладах країни. До початку воєнних дій на Сході України курс інсерційного моделювання читався також у Донецькому національному університеті імені Василя Стуса. Таким чином в Україні поступово зростає кількість фахівців, які володіють

технологією інсерційного моделювання. За останні роки захищено 4 докторські та більш як 10 кандидатських дисертацій в галузі створення високонадійних програмних систем.

Отже, в Інституті кібернетики ім. В.М. Глушкова НАН України на базі технології інсерційного моделювання та досвіду, накопиченого в процесі співробітництва із зарубіжними компаніями, розроблено вітчизняну технологію створення високонадійних програмних систем, готову для впровадження в промислових організаціях.

Проте широкому впровадженню у промислових організаціях України сучасних методів побудови високонадійних систем заважає відсутність належного фінансування. Ми докладаємо багато зусиль для пошуку міжнародної фінансової підтримки і сподіваємося отримати частину коштів, необхідних для продовження робіт з впровадження технології інсерційного моделювання, через систему міжнародних грантів, зокрема за програмою «Горизонт-2020».

*За матеріалами засідання*
*підготувала О.О. МЕЛЕЖИК*