ВІДГУК

офіційного опонента на дисертаційну роботу
ШКАРУПИЛА Вадима Вікторовича
«Методи і засоби контролю артефактів процесу проєктування програмно-алгоритмічного забезпечення систем критичного призначення»,
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми.

Функційна безпечність інформаційно-керуючих систем критичного призначення (ІКСКП) визначається їх програмно-алгоритмічним забезпеченням (ПАЗ). Його вплив має дві складові: з одного боку, ПАЗ є об'єктом оцінювання і забезпечення функційної безпечності ІКСКП, у випадку, коли безпосередньо виконує функції, важливі для безпеки, або підтримує їх виконання (прикладом є так звані системи нормальної експлуатації для АЕС), з іншого, - ПАЗ використовується як інструментарій для власне захисту і переведення критичних об'єктів в захищений стан (керуючі системи безпеки – системи аварійного захисту реакторів). Від того, наскільки повно ПАЗ було опрацьовано із залученням методів і засобів верифікації та тестування розробника або/та незалежного аудиту, істотним чином залежить рівень довіри до його результатів та вчасне надання відповідних дозвільних документів регулюючими органами.

Важливою вимогою процесів верифікації ПАЗ для таких ІКСКП є незалежність її проведення, яка передбачає, що перевірка здійснюється спеціалістами, організаційно і фінансово незалежними від розробників, а отже з використанням власного верифікаційного інструментарію. Ця обставина була однією з причин, яка прискорила розроблення так званих модель-орієнтованих методів (методів перевірки на моделі - Model Checking), що вийшли на порядок денний як відповідь на зростання складності ПАЗ і виникнення «прокляття» розмірності. Крім того, їх зростаюча поширеність обумовлена порівняно високим ступенем придатності до автоматизованого застосування. Підтвердженням дієвості названих методів і засобів є науково-технічних публікації, на які здобувач посилається у тексті дисертаційної роботи, щоб підкреслити значимість своєчасного виявлення потреби доопрацювання прийнятих проєктних рішень, поданих у формі артефактів.

Автором обґрунтовується, формулюється та вирішується важлива науково-технічна проблема забезпечення повноти і достовірності верифікації ПАЗ шляхом відбору, систематизації та контролю несуперечності артефактів на етапі проєктування та зниження супутніх витрат. Це формулювання дещо відрізняється від авторського, але не звужує, а навпаки розширює рамки проблеми, яку вирішив автор.

Отже, обрана автором тема дисертаційної роботи є цілком актуальною і суттєвою з точки зору безпекових задач для ІКСКП.

Аналіз змісту дисертації.

Дисертаційну роботу викладено на 369 сторінках. Вона складається із анотації, вступу, шести розділів, висновків, списку використаних джерел зі 189 найменувань, а також 9 додатків. Обсяг основної частини – 255 сторінок.

У *першому розділі*, із посиланням на актуальні науково-технічні публікації за тематикою дисертації, здобувачем опрацьовано аспекти і сценарії застосування формальних методів і засобів у процесі розроблення комп'ютерних систем як ядра ІКСКП із наголосом на ПАЗ цих систем. У межах дисертації процес розроблення подано як послідовність етапів аналізу вимог, проєктування, реалізації, валідації. Наголошено на важливості застосування формальних методів і засобів у якості засобів контролю, перш за все на етапі проєктування.

Здобувачем аргументовано значимість проведення контролю не лише функціональних (ФХ), але й нефункціональних характеристик (НФХ). Варто при цьому зауважити, що контроль НФХ типово виконується саме на заключному етапі валідації у складі етапів процесу розроблення. Автором у межах розділу сформульовано засади доцільності сполучення методів і засобів контролю показників ФХ і НФХ при проєктуванні, базуючись на перевірці несуперечності ПАЗ.

Зауваження. Незважаючи на те, що рамки дослідження окреслено доволі широко, на нашу думку, на більшу увагу заслуговувала аргументація стосовно важливості етапу формулювання та перевірки вимог та фактичного зародження формальних методів саме на цьому етапі задля мінімізації помилок на наступних етапах. Можливо, дещо детальніше слід було б проаналізувати систему показників і обмежень.

Другий розділ присвячено розробленню концепції верифікації на підставі застосування у якості методів і засобів контролю артефактів, одержуваних у процесі проєктування ПАЗ. Представлено розроблену модель подання ПАЗ формальними специфікаціями (ФС) та зауважено, що ця модель застосована у якості засобу уніфікації ФС. У свою чергу, безпосередньо ФС було опрацьовано як засоби уможливлення проведення формальної верифікації за показником несуперечності ПАЗ на основі методу перевірки на моделі в автоматизованому режимі. За результатами проведених досліджень моделі здобувачем було узагальнено, що залучення правила композиції Чарльза Гоара дозволило істотно скоротити кількість рядків коду ФС, одержуваних згідно розробленої моделі. Дослідження автором проведено для штучних граничних випадків. При цьому було відзначено, що одержуваний у результаті застосування правила композиції корисний ефект безпосередньо залежить від архітектурної складової ФС.

Зауваження. В цьому розділі ключові наукові положення можна було узагальнити і викласти як певну методологію, оскільки фактично автор формулює концепцію, принципи і обґрунтовує взаємозв'язки відповідних моделей і методів, що у сукупності є ознакою методології як окремого

наукового результату. Було б дуже доречно надати її структуру з вертикальними і горизонтальними зв'язками.

У третьому розділі розроблено метод синтезу ФС на основі запропонованої моделі. Здобувачем слушно зауважено, що цей метод слугуватиме як підґрунтя засобів автоматизації процесу «постачання» ФС як похідних артефактів – від первинних артефактів-подань ПАЗ: блок-схем алгоритмів, UML-діаграм дій. Враховано дуальний характери сприйняття досліджуваних артефактів процесу проєктування розробником: опрацьовано і аналітичну площину, і площину реалізації; першу – розглянуто з позиції сутностей, якими оперує розробник при аналізі артефактів, другу – з точки зору сутностей, форма подання яких уможливлює застосування в автоматизованому режимі формального методу перевірки на моделі TLC. Розроблено також метод контролю відповідності результуючих ФС первинним артефактам-поданням ПАЗ, призначений до застосування на заключному етапі синтезу ФС. Він має на меті надати змогу розробникові поширювати висновки стосовно результатів формальної верифікації ФС також і по відношенню до первинних артефактів-подань ПАЗ, несуперечність яких контролюється при проєктуванні.

Зауваження. Було б доцільно супроводжувати розроблення означених методів більш системним аналізом відповідних показників повноти, достовірності та часу верифікації.

У четвертому розділі здобувачем розвинуто метод формальної верифікації TLC. Автором зауважено, що він налаштований до застосування за умов ітеративного підходу до організації процесу формальної верифікації при проєктуванні ПАЗ. Дослідження удосконаленого методу TLC проведено і для граничних синтетичних випадків, і для випадків предметно-орієнтованих критичних сценаріїв, що охоплюють, зокрема, енергетичну та аерокосмічну галузі. Дослідження здобувачем проведено у частині опрацювання обчислювальних і просторових витрат, супутніх реалізації процесу формальної верифікації на основі базового і розвинутого методу TLC. З урахуванням можливостей сучасних обчислювальних систем досліджено корисний ефект від введення мультипоточності до альтернативних реалізацій методу.

Зауваження. Результати цього розділу підкреслюють важливість оцінювання ефекту від впровадження методів (модифікованого TLC) з системних позицій, включаючи показників достовірності (ризиків залишкових прихованих дефектів).

П'ятий розділ описує розроблену модель як стратифіковану архітектуру. Елементи виокремлених ієрархічних рівнів здобувачем представлено на основі математичного апарату DEVS, з використанням відповідних конструкцій «атомарної» і «складеної» моделей. Стверджується, що розроблена модель призначена уможливити проведення при проєктуванні ПАЗ також і контролю показників НФХ: завдяки поданню їх складових засобами згаданих «атомарної» і «складеної» моделей, і

накопичення результуючого значення шляхом проведення дискретно-подійного імітаційного моделювання.

Зауваження. Було б цікаво порівняти запропоновану модель з традиційними «лінійними» моделями верифікації, що базуються на звичайних чек-листах, які можуть деталізуватися для перевірки на рівні «так-ні». Підрозділ, с. 254, дещо перевантажений поясненнями, які доречно було б перенести у наступний підрозділ або виключити.

У шостому розділі розроблено метод контролю НФХ при проєктуванні ПАЗ на основі представленої у п'ятому розділі моделі як стратифікованої архітектури. Метод засновано на проведенні дискретно-подійного імітаційного моделювання, і накопиченні при цьому значення показника НФХ. Опрацьовано часові витрати, супутні реалізації ФХ згідно ПАЗ. Автором було слушно зауважено, що аналогічним чином можуть бути оцінені супутні матеріальні витрати. Дослідження проведено для випадку реалізації ПАЗ у формі композитного вебсервісу, виконання обчислень на компонентах якого координується централізовано.

Зауваження. Здобувачем доведено, що залучення оціночних значень складових досліджуваного показника, замість фактичних, істотним чином впливає на зниження результуючих часових витрат. Такий підхід, однак, обумовлює питання стосовно достовірності одержуваних результатів при застосуванні розробленого методу. Було б також доцільно, на нашу думку, виокремити підрозділ з аналізом результатів практичних розробок і впроваджень основних наукових положень дисертації з акцентуванням ІКСКП.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій. Достовірність результатів досліджень.

Наукові положення, висновки і рекомендації дисертаційної роботи обґрунтовано завдяки:

- коректному використанню здобувачем засобів математичного апарату теорії множин, теорії алгоритмів, засобів апарату математичної статистики, засобів формалізації;
- опрацюванню як предметно-орієнтованих, так і граничних випадків при проведенні досліджень;
- порівнянню одержуваних експериментальних даних із результатами дослідження вже відомих методів і засобів;
- підтвердженню зроблених припущень експериментальними даними.

Достовірність результатів дисертаційного дослідження забезпечується завдяки співставлення формульованих здобувачем положень і одержуваних експериментальних даних із відповідними здобутками визнаних науковців за окресленою тематикою, серед яких – лауреати премії Тюрінга.

Серед іншого, достовірності також сприяють і додатково запропоновані здобувачем у якості допоміжних засобів оціночні функції просторових витрат, супутніх вирішенню задачі формальної верифікації, значення яких було підтверджено експериментально. Важливим фактором у

даному контексті також є залучення допоміжних авторських програмних реалізацій як засобів автоматизації. Достовірність результатів забезпечується і вичерпним переліком документальних підтверджень значимості результатів від організацій та установ, наведених у додатках.

Окремої уваги у контексті достовірності результатів заслуговує перелік праць автора, серед яких 15 (14 цитованих) праць, індексованих у міжнародних наукометричних базах Scopus та Web of Science.

Наукова новизна отриманих результатів.

Наукова новизна результатів, винесених на захист, полягає у наступному (їх формулювання збігається з авторським за ключовими елементами).

1. Розроблена здобувачем модель подання ПАЗ у формі ФС, де, на відміну від відомих альтернативних рішень, правило композиції Чарльза Гоара було вперше застосовано у якості засобу скорочення кількості рядків коду результуючої ФС. Відносну частку такого скорочення опрацьовано як показник одержуваного корисного ефекту. Водночас автором було зауважено, що названий ефект визначається, у тому числі, кількістю змінних у ФС, архітектурною складовою ФС.

2. Розроблений метод синтезу ФС, заснований на моделі подання ПАЗ, на відміну від відомих, за рахунок виокремлення двох площин опрацювання розробником артефактів – аналітичної і реалізації – надає прозорий механізм співставлення конструкцій у складі артефактів як аналітичних подань із відповідними конструкціями у складі похідних артефактів – ФС.

3. Розроблений метод контролю відповідності одержуваних ФС первинним артефактам, на відміну від відомих, за рахунок опрацювання систем переходів як графів, надає механізм опосередкованого контролю за показниками глибини обходу простору станів і загальної кількості станів систем переходів. Цей процес супроводжується суттєвим скороченням обчислювальних витрат, у порівнянні із такими, що мають місце, наприклад, за вирішення задачі встановлення граф-підграф ізоморфізму.

4. Розроблена модель як стратифікована архітектура, на відміну від відомих, завдяки виокремленню ієрархічних рівнів для складових формалізованих подань і оперування конструкціями «атомарної» і «складеної» моделей DEVS, є засобом, що уможливлює відтворення архітектурної складової ФС, несуперечність якої підтверджено на основі поширеного формального методу перевірки на моделі TLC або розвинутого автором методу.

5. Розроблений метод контролю досліджуваного показника НФХ при проєктуванні ПАЗ, завдяки базуванню на моделі як стратифікованій архітектурі, надає дуальний механізм проведення контролю при проєктуванні шляхом оперування оціночними і фактичними значеннями складових показника; при цьому результуюче значення показника накопичується у процесі дискретно-подійного імітаційного моделювання шляхом залучення механізму обміну повідомленнями між складовими

комп'ютерної моделі, побудованої згідно згаданої вище розробленої здобувачем моделі як стратифікованої архітектури.

6. У розвинутому формальному методі перевірки на моделі TLC вперше було застосовано комбінування методів обходу у ширину і глибину для досягнення комплексного ефекту: метод обходу у ширину було використано у якості засобу встановлення глибини обходу простору станів системи переходів, що будується у процесі формальної верифікації, а метод обходу у глибину – у якості засобу скорочення супутніх даному процесу обчислювальних витрат.

Значущість отриманих результатів для науки і практичного використання.

Значущість отриманих результатів для науки полягає у розвитку теоретичних засад проведення модельно-базованої верифікації шляхом контролю артефактів, одержуваних у процесі розроблення ПАЗ ІКСКП. Здобувачем розроблено комплекс методів і супутніх засобів для їх застосування у якості засобів контролю артефактів, одержуваних у процесі розроблення ПАЗ.

Значущість результатів для практичного використання полягає у залученні розробленого комплексу моделей і методів у якості засобів оцінювання і забезпечення функційної безпечності ПАЗ ІКСКП.

Висновки і рекомендації, сформульовані у докторській дисертації, мають світову новизну.

Практичне значення отриманих результатів.

Згідно копій документів, зведених у додатках до рукопису дисертації, підтвердженням практичного значення представленої роботи є, у тому числі, акт впровадження у робочий процес ТОВ «НВП «ХАРТРОН-ЮКОМ», листи підтримки від Громадської спілки «Міжнародна рада з великих електроенергетичних систем СІГРЕ в Україні», від Державного підприємства «Державний науково-технічний центр з ядерної та радіаційної безпеки», від Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (ДЦКЗ Держспецзв'язку). Окрім зазначеного, у додатках також надано копію листа підтвердження впровадження у навчальний процес Навчально-наукового інституту енергозбереження та енергоменеджменту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», копію листа підтвердження впровадження у навчальний процес кафедри комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Повнота викладення результатів в опублікованих матеріалах.

Основні результати дисертаційної роботи викладено у 68 опублікованих працях: 6 монографій та розділів монографій у вітчизняних і

закордонних виданнях, з яких 1 індексується міжнародною наукометричною базою Scopus; 22 статті у періодичних фахових виданнях, з яких 7 індексуються міжнародними наукометричними базами Scopus та Web of Science Core Collection, 3 опубліковано у періодичних фахових виданнях категорії А; 40 публікацій у формі матеріалів збірників тез доповідей наукових, науково-технічних та науково-практичних конференцій, включно із міжнародними, з яких 7 публікацій індексуються міжнародними наукометричними базами Scopus та Web of Science Core Collection.

У працях, опублікованих у періодичних фахових виданнях, основні наукові положення дисертаційної роботи та отримані результати висвітлено повно і якісно.

Випадків плагіату в наукових статтях та дисертації не виявлено. У монографіях здобувача використано матеріали опублікованих статей, на які є посилання у тексті. На ідеї та наукові результати інших авторів, використані у дисертаційній роботі, є відповідні посилання; вони не використані в наведених наукових результатах, що належать виключно автору. У дисертації опрацьовано достатню кількість літературних джерел для класу систем, що розглядаються. На ці джерела у тексті дисертації наявні посилання.

Особистий внесок здобувача в сумісних публікаціях матеріалами дисертаційної роботи підтверджено у достатній мірі. Рівень та кількість публікацій відповідають вимогам, що висуваються до докторських дисертацій в Україні.

Реферат є ідентичним за змістом стосовно основних положень дисертації, і достатньо повно відображає актуальність, мету, поставлені та вирішені задачі, наукові положення, практичну значимість, результати апробації, зміст дисертації за розділами, висновки. Дисертаційну роботу та реферат оформлено у відповідності до вимог, що висуваються до докторських дисертацій в Україні.

Зауваження та дискусійні питання стосовно положень докторської дисертації.

Частина зауважень надана при аналізі змісту розділів дисертації. Крім того, зазначимо наступне.

1. У першому розділі, с. 94, представлено зведену таблицю методів і засобів, залучених до процесу досліджень. Незрозуміло, однак, чому у якості засобу формальної верифікації не було обрано техніку символьної перевірки на моделі, що характеризується вищим рівнем стійкості до ефекту експоненційного зростання простору станів системи переходів.

2. Стосовно розробленої моделі подання ПАЗ, хотілося б бачити інформацію у частині перевірки адекватності даної моделі на основі загальновідомих статистичних критеріїв. Втім, можна припустити, що дану перевірку проведено опосередковано, шляхом аналізу результатів застосування розробленого методу контролю відповідності, викладеного у наступному, третьому, розділі.

3. Дещо ускладненими є, на наш погляд, термінологія і стиль викладення окремих частин тексту дисертації. Крім того, було б цікаво, отримати оціночні судження автора стосовно аспектів виявлення вразливостей ПАЗ з огляду на кібербезпекові виклики.

Перелічені зауваження не є принциповими і не впливають на позитивний висновок, деякі є дискусійними і належать до можливих напрямів подальших досліджень.

Загальні висновки.

Вважаємо, що дисертаційна робота ШКАРУПИЛА Вадима Вікторовича «Методи і засоби контролю артефактів процесу проєктування програмно-алгоритмічного забезпечення систем критичного призначення» є завершеною науковою працею, у якій отримано нові науково обґрунтовані результати, що забезпечують досягнення поставленої автором мети досліджень та вирішення науково-технічної проблеми забезпечення повноти і достовірності верифікації ПАЗ шляхом відбору, систематизації та контролю несуперечності артефактів на етапі проєктування та зниження супутніх витрат. Вважаю, що представлена дисертація відповідає паспорту спеціальності 05.13.05 - комп'ютерні системи та компоненти, у тому числі за напрямами досліджень, поданими пунктами 2, 5 та 7.

Дисертаційна робота цілком відповідає вимогам «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 року № 1197, а її автор ШКАРУПИЛО Вадим Вікторович заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.05 - комп'ютерні системи та компоненти.

Офіційний опонент – завідувач кафедри
комп'ютерних систем, мереж і кібербезпеки
Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут»,
лауреат Державної премії України в галузі науки і техніки,
заслужений винахідник України
доктор технічних наук, професор Вячеслав ХАРЧЕНКО

« 24 » травня 2024 р.

Підпис професора Харченка Вячеслава Сергійовича засвідчую.
Вчений секретар Вченої ради
Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут»
кандидат технічних наук, доцент Тетяна БОНДАРЄВА