НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ІМ. Г.Є. ПУХОВА

**ШКАРУПИЛО ВАДИМ ВІКТОРОВИЧ**

УДК 004.052.42

# МЕТОДИ І ЗАСОБИ КОНТРОЛЮ АРТЕФАКТІВ ПРОЦЕСУ ПРОЄКТУВАННЯ ПРОГРАМНО-АЛГОРИТМІЧНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

05.13.05 – комп’ютерні системи та компоненти

**РЕФЕРАТ**

дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2024

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми**. Сучасне суспільство у різних сферах своєї діяльності істотним чином покладається на функціонування систем критичного призначення (СКП, Safety-critical System) – систем, до функційної безпечності (ФБ; формулювання згідно ДСТУ EN 61508-3:2019) яких висуваються підвищені вимоги – систем, збої і відмови в роботі яких можуть призвести до значних небажаних наслідків критичного характеру.

Регламентації механізмів забезпечення ФБ зазначених систем присвячено відповідні міжнародні галузеві стандарти, де наголошується на важливості застосування формальних методів та супутніх засобів на кожному із етапів процесу розроблення СКП: IEC 61508 (електронні системи із програмною складовою), ISO 26262:2018 (транспортні засоби), CENELEC – EN 50128 (залізнична галузь), DO-178C (авіаційна галузь) тощо. Формальні методи і засоби розглядаються при цьому як дієві інструменти зниження ролі небажаного впливу людського фактору, у тому числі як інструменти самоконтролю для розробників.

У межах дисертації процес розроблення розглянуто як послідовність наступних етапів: аналіз вимог, проєктування, реалізація, валідація. У свою чергу, згідно положень міжнародного стандарту IEEE 1012-2016, валідація може бути проведена і шляхом імітаційного моделювання, і шляхом тестування.

Питанням розвитку заходів досягнення заданого рівня ФБ присвячено праці багатьох вітчизняних і закордонних наукових діячів. Серед праць вітчизняних діячів доречним вбачається виокремити публікації лауреата Державної премії України в галузі науки і техніки, заслуженого винахідника України, доктора технічних наук, професора Вячеслава Сергійовича Харченка, доктора технічних наук, професора Бориса Михайловича Конорева: значна увага приділяється аспектам забезпечення ФБ на рівні програмно-алгоритмічної складової (ПАС) комп’ютерних систем, шляхом залучення, у тому числі, формальних методів і засобів. Опрацьовано і питання розроблення метрик кількісного оцінювання ризиків виникнення нештатних ситуацій, що загрожують ФБ. У якості показових при цьому фігурують критичні сценарії з енергетики, аерокосмічної галузі.

Окремої уваги заслуговують наукові здобутки доктора технічних наук, професора Межуєва Віталія Івановича, які було успішно застосовано для контролю несуперечності артефактів розроблюваної операційної системи реального часу, призначеної до використання в аерокосмічній галузі.

Значних схвальних відгуків міжнародної науково-дослідницької спільноти, серед якої – і колектив компанії Motorola, здобули праці доктора фізико-математичних наук Олександра Олександровича Летичевського, присвячені дослідженню, розробленню і розвитку методів і засобів символьної формальної верифікації.

Серед численних праць закордонних діячів за окресленою тематикою варто виокремити здобутки Едмунда Кларка (Edmund Melson Clarke, Jr.), Алана Емерсона (Ernest Allen Emerson), Джозефа Сіфакіса (Joseph Sifakis) – лауреатів премії Тюрінга 2007 р. за вагомий внесок у розвинення техніки перевірки на моделі (Model Checking) до рівня ефективної технології формальної верифікації, яка у наш час є

широко застосовуваною у процесі розроблення програмних, апаратних, комп'ютерних систем, у тому числі СКП.

Не менш вагомим є науковий внесок лауреата премії Тюрінга 2013 р., першого лауреата премії Дейкстри – Леслі Лемпорта (Leslie Lamport), чиї праці здобули світове визнання. Відомі формальні методи і засоби: темпоральна логіка дій TLA (Temporal Logic of Actions), відповідний формальний метод перевірки на моделі TLC (TLA Checker), виразні засоби LaTeX, PlusCal, TLA+ тощо.

Статусу фундаментальних набули, у тому числі, і праці Дорона Пеледа (Doron A. Peled), Орни Грумберг (Orna Grumberg).

У межах представленої дисертації метод TLC, а також засоби TLA, TLA+ і PlusCal, залучено у якості інструментів здійснення контролю несуперечності ПАС як досліджуваного показника функціональних характеристик (ФХ) розроблюваної ПАС. При цьому у якості показника нефункціональних характеристик (НФХ) охоплено часові витрати, супутні реалізації ПАС. Такий підхід застосовано до вирішення важливої науково-технічної проблеми забезпечення контролю артефактів процесу проєктування ПАС систем критичного призначення стосовно несуперечності артефактів. Проблему опрацьовано у частині сприяння ФБ розроблюваної ПАС.

Роботу представлено із використанням поняття «артефакт». Згідно визначення компанії IBM, артефактом є результат виконання певного кроку процесу розроблення, поданий у формі файлу, що зберігається у пам'яті обчислювальної системи. Доповненням виступає також визначення професора Мюнхенського технічного університету Манфреда Броя (Manfred Broy): артефакт – сутність, яка характеризується структурою і змістом. Цю інтерпретацію у межах дисертації було розширено: артефакт – сутність, що характеризується архітектурою (структурою та зв'язками) і змістом. При цьому у якості досліджуваних артефактів опрацьовано графічні і формалізовані подання ПАС, що фігурують на етапі проєктування ПАС (рис. 1). Серед них: UML-діаграми дій, станів, формальні специфікації (ФС) і програмні реалізації як засоби автоматизації.

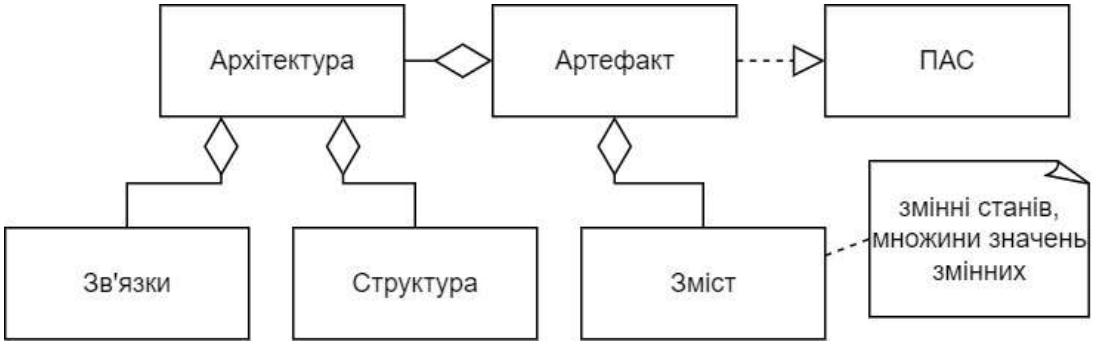


Рисунок 1 – Подання понятійної складової представленої роботи

На рисунку 1 у формі UML-діаграми зведено ключові складові залученого понятійного апарату.

З урахуванням вищезазначеного, обрану тему дисертаційного дослідження можна вважати актуальною.

**Зв'язок роботи з науковими програмами, планами, темами**. Дисертаційні дослідження проведено протягом 2015−2023 рр. Роботу виконано у відповідності до планів і задач наступних науково-дослідних робіт: НДР № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики» (2020−2024 рр.; науковий керівник); НДР № 0121U110615 «Розроблення методів та засобів верифікації артефактів процесу проєктування систем критичного призначення» (2021−2022 рр.; науковий керівник), виконуваних / виконаних в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. При цьому НДР № 0121U110615 було профінансовано у межах гранту НАН України дослідницьким лабораторіям/групам молодих вчених НАН України для проведення досліджень за пріоритетними напрямами розвитку науки і техніки (2021−2022 рр.). Роботу також було узгоджено із вирішенням задач міжнародного проєкту Erasmus+ Internet of Things: Emerging Curriculum for Industry and Human Applications ALIOT Project (reference number: 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP (2016−2019 рр.; виконавець).

**Мета і задачі дослідження**. Метою дисертаційного дослідження є підвищення ефективності контролю артефактів у процесі розроблення програмно-алгоритмічної складової систем критичного призначення на етапі проєктування для забезпечення несуперечності артефактів та зниження супутніх витрат, за рахунок розроблення, дослідження і застосування формальних методів, розвитку методу, моделей, супутніх засобів, у тому числі засобів автоматизації.

Для досягнення сформульованої мети в роботі ставляться і вирішуються наступні задачі:

1. Проведення аналізу аспектів застосування методів і засобів контролю показників ФХ і НФХ розроблюваної ПАС системи критичного призначення, з використанням методів формальної верифікації (ФВ), у тому числі методів перевірки на моделі, моделей, підходів, інструментів, виразних засобів. За результатами проведеного аналізу – розроблення комплексного підходу до застосування формальних методів і супутніх засобів контролю показників ФХ і НФХ розроблюваної ПАС на етапі проєктування.
2. Розроблення моделі подання ПАС у формі формальної специфікації (ФС). Модель призначена слугувати прототипом – засобом уніфікації – ФС, які, у свою чергу, залучаються у якості вихідних конструкцій для застосування по відношенню до них формального методу перевірки на моделі як засобу контролю несуперечності ПАС в автоматизованому режимі.
3. Розроблення методу синтезу ФС для ПАС, що дасть змогу одержувати в автоматизованому режимі відповідні первинним артефактам – графічним поданням – результуючі формалізовані подання. Це уможливить застосування по відношенню до останніх методу перевірки на моделі – засобу автоматизованого контролю досліджуваних артефактів у розрізі несуперечності.
4. Розроблення методу контролю відповідності одержуваних результуючих ФС первинним графічним поданням ПАС, що дозволить поширювати висновки,

сформульовані за результатами проведення формальної верифікації ФС, на відповідні графічні подання ПАС.

5. Дослідження шляхів підвищення ефективності поширеного методу формальної верифікації – TLC – стосовно зниження супутніх його застосуванню обчислювальних витрат при проведенні контролю несуперечності розроблюваної ПАС на основі відповідної ФС.

6. Розроблення моделі, призначеної слугувати засобом регламентування формалізованого подання ПАС, де охоплюватимуться, у тому числі, засоби подання НФХ-складової, що уможливить проведення контролю значень заданих показників зазначеної складової вже на етапі проєктування процесу розроблення ПАС.

7. Розроблення методу автоматизованого контролю значення заданого показника НФХ розроблюваної ПАС на етапі проєктування. Метод має забезпечувати механізм накопичення значення показника шляхом проведення дискретно-подійного імітаційного моделювання.

**Об'єкт дослідження** – процес розроблення програмно-алгоритмічної складової комп'ютерних систем критичного призначення.

**Предмет дослідження** – формальні методи і супутні засоби, у тому числі моделі, засоби автоматизації, призначені до застосування на етапі проєктування програмно-алгоритмічної складової систем критичного призначення.

**Методи дослідження**. Засоби, прийоми теоретико-множинного підходу – для формалізації аналітичної складової. Формальні методи перевірки на моделі – для вирішення задачі формальної верифікації в автоматизованому режимі. Методи теорії графів, а саме – метод обходу вершин графу в ширину (Breadth-first Search, BFS) і метод обходу в глибину (Depth-first Search, DFS) – для дослідження і розвитку поширеного методу перевірки на моделі TLC, у тому числі – для оцінювання обчислювальних і просторових витрат, супутніх вирішенню задачі формальної верифікації. Математичний апарат структури Кріпке – для аналітичного подання системи переходів (СП), що будується при вирішенні задачі формальної верифікації методом перевірки на моделі. Метод імітаційного дискретно-подійного моделювання – для реалізації процесу формальної верифікації в автоматизованому режимі, а також для агрегування значення заданого показника НФХ. Математичний апарат числення послідовних процесів, що взаємодіють Чарльза Гоара (C.A.R. Hoare) – для формалізації послідовностей станів, у яких перебуває СП у процесі формальної верифікації; залучено також трійки і аксіоми Гоара, а саме – правила композиції, виведення і умовного оператора, у тому числі – для зменшення обсягу ФС. Математичний апарат в основі темпоральної логіки дій TLA – для подання ПАС у формі ФС. Математичний апарат модульного ієрархічного формалізму DEVS (Discrete Event System Specification) Бернарда Зейглера (Bernard P. Zeigler) – для формалізованого подання і накопичення результуючого значення досліджуваного показника НФХ. Методи і прийоми математичної статистики – для опрацювання і узагальнення одержуваних експериментальних даних. Методи теорії паралельних обчислень – для дослідження впливу залучення мультипоточності на результуючі часові витрати, супутні застосуванню формального методу перевірки на моделі TLC, а також розробленого розвитку даного методу. Методи теорії

алгоритмів, у тому числі – теорії обчислювальної складності – для подання досліджуваних артефактів процесу проєктування ПАС, оцінювання просторових витрат, граничних випадків одержуваного корисного ефекту від проведеного розвитку методу TLC.

**Наукова новизна отриманих результатів** полягає у розроблених методах, моделях, розвитку вже існуючого методу, застосовуваних згідно запропонованого комплексного підходу до їх залучення при проєктуванні ПАС. Комплексність досягається за рахунок охоплення показників ФХ і НФХ.

Наукові результати, винесені на захист і отримані автором особисто:

1. Розроблено модель подання ПАС системи критичного призначення у формі ФС, де правило композиції Гоара вперше застосовано з позиції стратифікованого підходу до подання ПАС у формі ФС, що, на відміну від альтернативних рішень, дозволяє зменшити кількість рядків коду результуючої ФС. Названа модель призначена слугувати засобом уніфікації ФС як форм подання ПАС – для проведення автоматизованого контролю несуперечності останніх шляхом формальної верифікації методом перевірки на моделі. Модель побудовано шляхом виокремлення двох рівнів опрацювання розробником складових формалізованих подань як артефактів – аналітичного рівня і рівня реалізації. При цьому у якості виразних засобів було залучено, у тому числі, засоби структури Кріпке, числення CSP, алгоритмічну мову PlusCal, а також формалізм TLA+. Перші два перелічені засоби призначені до застосування на рівні аналітичному, останні два засоби – на рівні реалізації.

2. Розроблено метод синтезу ФС на основі графічного подання ПАС, де вперше комплексно охоплено і аналітичний рівень подання ФС, і рівень реалізації. Такий крок, на відміну від альтернативних рішень, забезпечує прозорий механізм подання складових ФС та зв’язків між ними як на аналітичному рівні, так і на рівні програмної реалізації. Для цього було залучено математичний апарат темпоральної логіки дій TLA, відповідний формалізм TLA+ та алгоритмічну мову PlusCal. Застосування виразних засобів PlusCal дозволило одержати прототип результуючої ФС, із наголосом на архітектурній складовій. Його було залучено у якості артефакту, на основі якого формується результуюча ФС, побудована на основі виразних засобів TLA+. Останні, у свою чергу, уможливлюють здійснення процесу формальної верифікації ФС в автоматизованому режимі.

3. Розроблено метод контролю відповідності одержуваної ФС первинному артефакту – графічному поданню ПАС, де вперше запропоновано уніфікований механізм співставлення сутностей аналітичного рівня подання досліджуваного артефакту із відповідними сутностями рівня реалізації – елементами у складі результуючої ФС. Це дозволило узагальнити процес контролю одержуваних похідних артефактів – ФС – на рівні їх архітектурної складової (структури та зав’язків): шляхом співставлення СП для аналітичного рівня і рівня реалізації – за показниками кількостей станів СП і глибин обходу просторів станів СП.

4. Розроблено модель – стратифіковану архітектуру, де ієрархічний підхід вперше запропоновано застосовувати у якості засобу одержання похідних формалізованих подань на основі артефактів, несуперечність яких вже було

підтверджено шляхом залучення формального методу перевірки на моделі. Це дозволило отримувати при проєктуванні ПАС формалізовані подання, що містять також і засоби представлення досліджуваного показника НФХ. Ієрархічний підхід реалізовано на основі засобів математичного апарату DEVS: шляхом оперування конструкціями «атомарної» і «складеної» DEVS-моделей, які включають засоби подання досліджуваного показника НФХ.

5. Розроблено метод контролю значення досліджуваного показника НФХ, де вперше враховано можливість оперування і оціночними, і фактичними значеннями складових названого показника – вже на етапі проєктування ПАС. Метод реалізовано шляхом проведення дискретно-подійного імітаційного моделювання на основі засобів математичного апарату DEVS. Накопичення значення показника у процесі моделювання реалізовано на основі механізму обміну повідомленнями між компонентами результуючої складеної ієрархічної DEVS-моделі, що, у випадку оперування оціночними значеннями, дозволяє скоротити часові витрати, супутні застосуванню методу. У якості досліджуваного показника НФХ опрацьовано часові витрати, супутні реалізації ФХ згідно ПАС.

6. Набув подальшого розвитку поширений метод перевірки на моделі TLC. На відміну від базового методу, проведений розвиток базується на комбінуванні методів обходу в ширину (BFS) і в глибину (DFS) теорії графів при здійсненні обходу простору станів СП за ітеративного підходу до організації процесу формальної верифікації: на початковій ітерації застосовується метод BFS, що дає змогу визначити глибину обходу простору станів СП; на наступних ітераціях застосовується метод DFS, що дозволяє скоротити результуючі часові витрати, супутні ітеративному процесу формальної верифікації, – за рахунок зниження обчислювального навантаження за DFS-обходів для заданої кількості змінних станів. Одержуваний при цьому корисний ефект залежить від кількості змінних станів, архітектурної складової ФС, кількості ітерацій процесу формальної верифікації.

**Практичне значення отриманих результатів**. Розроблені моделі, методи, розвиток методу, сполучені згідно запропонованого підходу, забезпечують механізм здійснення комплексного контролю артефактів процесу розроблення ПАС системи критичного призначення вже на етапі проєктування, у тому числі:

1. Розроблений підхід, викладений у першому розділі, слугує засобом сполучення винесених на захист наукових результатів у формі комплексного рішення, що уможливлює здійснення контролю показників і ФХ, і НФХ вже на етапі проєктування процесу розроблення ПАС системи критичного призначення.

2. Розроблена модель подання ПАС системи критичного призначення у формі ФС є засобом уніфікації ФС, до яких в автоматизованому режимі застосовується формальна верифікація методом перевірки на моделі. Залучення моделі дозволяє зменшити кількість рядків псевдокоду результуючої ФС.

3. Розроблений метод синтезу ФС, що базується на зазначеній вище моделі подання ПАС, є засобом автоматизації процесу постачання вихідних даних для методу формальної верифікації – методу перевірки на моделі TLC, а також розробленого розвитку цього методу. Залучення розробленого методу на етапі

проєктування процесу розроблення ПАС дозволить знизити вплив людського фактору у процесі одержання формалізованих подань досліджуваних артефактів.

4. Розроблений метод контролю відповідності ФС, одержуваних у результаті застосування зазначеного вище розробленого методу синтезу ФС, є засобом контролю архітектурної відповідності результуючих ФС первинним графічним поданням ПАС. Використання названого методу призначене сприяти підвищенню рівня довіри розробників до похідних артефактів – ФС, побудованих на основі виразних засобів формалізму TLA+, які, у свою чергу, є конструкціями, до яких застосовується метод TLC, а також розроблений розвиток зазначеного методу.

5. Розроблений розвиток поширеного методу перевірки на моделі TLC дозволить знизити результуючі часові витрати, супутні процесу ФВ, за ітеративного підходу до організації процесу проєктування ПАС. Одержуваний при цьому корисний ефект залежить, у тому числі, від архітектурної складової ФС, кількості змінних, кількості ітерацій процесу формальної верифікації. Названий ефект, зокрема, зростає із зменшенням кількості умовних переходів у ФС.

6. Розроблена модель як стратифікована архітектура призначена слугувати засобом уніфікації комп’ютерних моделей, одержуваних у відповідності до ФС, несуперечність яких вже було підтверджено формальним методом перевірки на моделі, згідно розробленого підходу. Модель включає, у тому числі, засоби подання НФХ-складової. За рахунок залучення математичного апарату DEVS, модель характеризується властивостями модульності та ієрархічності – чинниками, що сприяють структурованості результуючої програмної реалізації, а також спрощенню процесу внесення доопрацювань.

7. Розроблений метод контролю значення показника НФХ є засобом уможливлення зазначеного контролю вже на етапі проєктування процесу розроблення ПАС – шляхом проведення імітаційного дискретно-подійного моделювання на основі комп’ютерних моделей, побудованих у відповідності до зазначеної вище стратифікованої моделі, із можливістю оперування і оціночними, і фактичними значеннями названого показника. При цьому корисний ефект від залучення саме оціночних значень проявляється у скороченні результуючих часових витрат, супутніх застосуванню методу.

Практичне значення отриманих і винесених на захист результатів проведених досліджень підтверджено документально – актом впровадження, листами підтвердження впровадження, листами підтримки від організацій та установ, серед яких: акт впровадження у робочий процес ТОВ «НВП «ХАРТРОН-ЮКОМ», що співпрацює з КБ «Південне»; лист підтримки від Громадської спілки «Міжнародна рада з великих електроенергетичних систем СІГРЕ в Україні»; лист підтримки від Державного підприємства «Державний науково-технічний центр з ядерної та радіаційної безпеки»; лист підтримки від Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України (ДЦКЗ Держспецзв’язку); лист підтвердження впровадження у навчальний процес Навчально-наукового інституту енергозбереження та енергоменеджменту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»; лист підтвердження впровадження у навчальний процес

кафедри комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України (НУБіП України).

**Особистий внесок здобувача**. Усі представлені та винесені на захист наукові та науково-технічні результати отримано автором самостійно. У працях, опублікованих у співавторстві, здобувачеві належать: [1] – розроблена модель подання ПАС у формі ФС; [2] – розроблений метод синтезу ФС, розроблена модель як стратифікованої архітектура, розроблений метод контролю значення досліджуваного показника НФХ; [3] – результати проведеного аналізу предметної області, розроблена модель подання ПАС у формі ФС, розроблений метод синтезу ФС, включаючи розроблений метод контролю відповідності у якості допоміжного засобу; [4] – результати проведеної класифікації формальних методів і засобів, елементи розробленого підходу у частині контролю досліджуваного показника ФХ, розроблена модель подання ПАС у формі ФС, елементи розробленого методу синтезу ФС, результати експериментальних досліджень базового методу TLC; [5] – розроблена модель як стратифікована архітектура, розроблений метод контролю значення досліджуваного показника НФХ, результати аналізу предметно-орієнтованого сценарію енергетики; [6] – представлення і результати проведеного розвитку базового методу перевірки на моделі TLC; [7] – результати дослідження альтернативних реалізацій базового методу TLC для граничного випадку послідовного сценарію; [8] – результати експериментального дослідження розроблених моделі як стратифікованої архітектури і методу контролю значення досліджуваного показника НФХ; [9] – елементи розробленої моделі подання ПАС у формі ФС, на прикладі розподіленої комп'ютерної системи; [10] – елементи розробленої моделі подання ПАС у формі ФС, на прикладі сценарію контролю відповідності програмних складових компонентів розподілених комп'ютерних систем; [11] – запропонований підхід до контролю адекватності розробленої моделі подання ПАС у формі ФС, розроблений метод контролю відповідності результуючих ФС, предметно-орієнтовані результати досліджень; [12] – опрацювання часових витрат у якості досліджуваного показника НФХ; [13] – результати дослідження розробленого розвитку методу TLC на прикладі предметно-орієнтованого сценарію енергетики; [14] – запропонований підхід до організації процесу проєктування, елементи розробленої моделі як стратифікованої архітектури, результати проведених досліджень; [15] – опрацювання часових витрат як показника доцільності залучення компонентів розподілених систем; [16] – опрацювання часових витрат як показника НФХ стосовно сценаріїв потоків робіт; [17] – результати дослідження базового методу TLC для граничного випадку подання паралелізму згідно моделі чергування; [18] – елементи розробленого методу контролю досліджуваного показника НФХ, опрацювання у якості такого показника часових витрат; [19] – результати проведеного аналізу предметної області, у тому числі обґрунтування доцільності застосування формальних методів і засобів на етапі проєктування; [20] – результати дослідження впливу конфігурації апаратної складової комп'ютерної системи на показники швидкодії обчислень, у тому числі у частині впливу від введення мультипоточності; [21] – елементи і

результати дослідження розробленої моделі подання ПАС у формі ФС, розроблений метод синтезу ФС згідно зазначеної моделі; [22] – результати дослідження базового методу TLC за показниками просторових витрат; [23] – результати дослідження впливу від введення мультипоточності до реалізації методу TLC на часові витрати, супутні процесу формальної верифікації, опрацювання предметно-орієнтованого сценарію аерокосмічної галузі; [24] – дослідження часових витрат як показника НФХ вебсервісів; [25] – опрацювання часових витрат як показника НФХ стосовно UML-подань як артефактів; [26] – розроблений модельно-орієнтований підхід до контролю показників НФХ, елементи розроблених моделі як стратифікованої архітектури, розробленого методу контролю досліджуваного показника НФХ; [27] – розроблена модель як стратифікована архітектура; [28] – обґрунтування важливості проведення контролю показників і ФХ, і НФХ у процесі розроблення; [31] – залучення стратифікації стосовно формалізації архітектурної складової артефактів процесу розроблення програмно-конфігурованих мереж, елементи розробленої моделі подання ПАС у формі ФС; [32] – представлення і результати застосування розробленої моделі подання ПАС у формі ФС стосовно предметно-орієнтованого сценарію; [33] – застосування розроблених моделі подання ПАС, а також відповідного розробленого методу синтезу ФС по відношенню до артефактів як подань протоколів взаємодії компонентів розподілених комп’ютерних систем; [34] – розроблена модель подання ПАС у формі ФС; [35] – розроблений розвиток методу TLC, результати дослідження застосування проведеного розвитку методу для критичного сценарію аерокосмічної галузі; [39] – застосований підхід до подання паралелізму у ФС, результати оцінювання просторових характеристик СП, що конструюються у процесі формальної верифікації; [42] – елементи розробленої моделі як стратифікованої архітектури; [44] – обґрунтування доцільності проведення стратифікації складових ФС; [45] – елементи застосованого підходу в основі розробленого методу контролю досліджуваного показника НФХ; [46] – результати проведеного аналізу методів та засобів формальної верифікації; [47] – обґрунтування важливості опрацювання несуперечності ПАС у якості досліджуваного показника ФХ на прикладі сценаріїв систем Інтернету речей; [48] – обґрунтування важливості застосування методів перевірки на моделі при проєктуванні СКП; [51] – запропонований підхід до застосування методу перевірки на моделі TLC, отримані результати проведених досліджень у частині обчислювальних витрат, супутніх процесу ФВ; [52] – отримані результати оцінювання просторової складності вирішуваної методом перевірки на моделі задачі ФВ; [53] – отримані результати оцінювання впливу від залучення мультипоточності на часові витрати, супутні реалізації процесу ФВ; [54] – обґрунтування важливості застосування методу перевірки на моделі при проєкутванні інформаційно-технологічних систем суб’єктів ринку електроенергії, отримані результати проведених експериментальних досліджень; [55] – модельно-орієнтований підхід до формалізації досліджуваного показника НФХ, покладений в основу розробленого методу контролю значення названого показника при проєктуванні ПАС, елементи розробленого комплексного підходу до контролю показників і ФХ, і НФХ; [56] – дуальний підхід, покладений в основу розроблених моделі подання ПАС у формі

ФС та методу синтезу ФС; [57] – результати дослідження мультипоточної реалізації методу TLC; [58] – узагальнення засобів ФВ у частині відповідних програмних реалізацій; [59] – підхід, покладений в основу розробленого методу контролю показника НФХ; [60] – обґрунтування важливості проведення контролю показників і ФХ, і НФХ на етапі проєктування у складі етапів процесу розроблення; [61] – запропонований модельно-орієнтований підхід як засіб сполучення артефактів виокремлених типів; [62] – узагальнення стосовно шляхів проведення контролю НФХ у контексті поняття ФБ; [63] – складові розробленого методу контролю значення показника НФХ; [64] – узагальнення стосовно аспектів контролю несуперечності ПАС у якості досліджуваного показника ФХ; [65] – висновки, узагальнення за результатами застосування методу TLC при вирішенні задач енергетики; [66] – обґрунтування і узагальнення стосовно вважливості опрацювання при проєктуванні ПАС у якості показників ФХ і НФХ, відповідно, несуперечності ПАС і супутніх реалізації кроків ПАС часових витрат; [67] – висвітлення предметної області енергетики з позиції поняття резилієнтності; [68] – узагальнення стосовно одержуваного корисного ефекту від мультипоточної реалізації методу TLC.

**Апробація результатів дисертації**. Отримані результати проведених дисертаційних досліджень пройшли апробацію на наступних науково-технічних та науково-практичних конференціях і семінарах: Науково-технічний семінар «Критичні комп'ютерні технології та системи» – КриКТехС-2024/1/186 (м. Харків, 2024 р.); П'ята науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України «Безпека енергетики в епоху цифрової трансформації» (м. Київ, 2023 р.); Міжнародна науково-практична конференція «живучість та резильєнтність – 2023» (Survivability & Resilience – 2023), (м. Київ, 2023 р.); III Всеукраїнська науково-практична конференція пам'яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського «Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук» (м. Київ, 2023 р.); XLI Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (м. Київ, 2023 р.); Sixth International Workshop on Computer Modeling and Intelligent Systems, CMIS-2023 (Zaporizhzhia, 2023); Міжнародна науково-практична конференція «Продовольча та екологічна безпека в умовах війни та повоєнної відбудови: виклики для України і світу», присвячена 125-річчю заснування Національного університету біоресурсів і природокористування України (м. Київ, 2023 р.); XLIX Міжнародна науково-практична інтернет-конференція «Проблеми та перспективи розвитку сучасної науки в країнах Європи та Азії» (м. Переяслав, 2022 р.); XL Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (м. Київ, 2022 р.); Науково-практична конференція «Тиждень науки-2022» (м. Запоріжжя, 2022 р.); Третя науково-практична конференція «Безпека енергетики в епоху цифрової трансформації» (м. Київ, 2021 р.); XII Міжнародна науково-практична конференція молодих вчених «Інформаційні технології: економіка, техніка, освіта '2021» (м. Київ, 2021 р.); 2021 IEEE KhPI Week on Advanced Technology (м. Харків, 2021 р.); 2nd International

scientific and practical conference on Topical issues of modern science, society and education – SPC «Sci-conf.com.ua» (м. Харків, 2021 р.); IX Міжнародна науково-практична конференція «European scientific discussions» (м. Рим, Італія, 2021 р.); IX Міжнародна науково-практична Інтернет конференція «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні 2021» (м. Київ, 2021 р.); XXXIX Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, присвячена 40-річчю Інституту, Дню науки в Україні та з нагоди відзначення 30-ї річниці незалежності України (м. Київ, 2021 р.); Друга науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України «Безпека енергетики в епоху цифрової трансформації» (м. Київ, 2020 р.); X Ювілейна міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій», присвячена 120-річчю з дня заснування Національного університету «Запорізька політехніка» (м. Запоріжжя, 2020 р.); VIII Міжнародна науково-практична Інтернет-конференція «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2020» (м. Київ, 2020 р.); 11th International Conference on Dependable Systems, Services and Technologies, DESSERT'2020 (м. Київ, 2020 р.; доповідь відзначено сертифікатом за кращу доповідь); Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (м. Київ, 2020 р.); 2019 International Scientific-Practical Conference on Problems of Infocommunications. Science and Technology, PIC S&T`2019 (м. Київ, 2019 р.); Науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України «Безпека енергетики в епоху цифрової трансформації» (м. Київ, 2019 р.); VII Міжнародна науково-практична конференція «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2019» (м. Київ, 2019 р.); 2018 IEEE International Scientific and Practical Conference on Problems of Infocommunications. Science and Technology, PIC S&T`2018 (м. Харків, 2018 р.); IX Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій» (м. Запоріжжя, 2018 р.); VI Міжнародна наукова конференція «Моделювання-2018», приурочена до 100-річчя від дня утворення Національної академії наук України та річниці з Дня народження академіка НАН України Пухова Георгія Євгеновича (м. Київ, 2018 р.); VI Міжнародна науково-практична інтернет-конференція «Тенденції та вектор розвитку науки в сучасному світі» (м. Дніпро, 2018 р.); Науково-практична конференція «Тиждень науки-2018» (м. Запоріжжя, 2018 р.); 14th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET'2018 (с. Славське, 2018 р.); Int. research and practice conference on Modern methods, innovations, and experience of practical application in the field of technical sciences (Radom, Republic of Poland, 2017); Науково-практична конференція «Тиждень науки 2017» (м. Запоріжжя, 2017 р.); Tenth International Scientific-Practical Conference «Internet-education-science-2016», IES-2016 (м. Вінниця, 2016 р.); VIIIth Int. scientific-practical conf. on Modern problems and achievements of radio engineering

(electronics), telecommunications and information technology (м. Запоріжжя, 2016 р.); 27th Int. Central European Conference on Information and Intelligent Systems, CECIIS 2016 (Varazdin, Croatia, 2016); Науково-практична конференція «Тиждень науки 2016» (м. Запоріжжя, 2016 р.); XIIIth Int. Conf. on Modern Problems of Radio Engineering, Telecommunications, and Computer Science, TCSET'2016 (с. Славське, 2016 р.); Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (м. Київ, 2016 р.); XXXIV науково-технічна конференція «Моделювання» (м. Київ, 2015 р.).

**Публікації**. За темою дисертаційної роботи опубліковано 68 наукових праць, з яких: 4 – колективні монографії, 2 – розділи колективних монографій у закордонних виданнях, у тому числі 1 індексується у міжнародній наукометричній базі Scopus; 22 – статті у періодичних фахових виданнях, з яких 7 – у виданнях, що індексуються у міжнародних наукометричних базах Scopus та Web of Science Core Collection, 3 – у фахових виданнях категорії А; 40 – матеріали доповідей на наукових конференціях, з яких 7 – індексуються у міжнародних наукометричних базах Scopus та Web of Science Core Collection.

**Структура та обсяг роботи**. Дисертаційна робота складається з анотації, вступу, шести розділів, висновків, списку використаних джерел, додатків.

Загальний обсяг дисертаційної роботи становить 369 сторінок, з яких: 255 сторінок основного тексту, список із 189 використаних джерел на 33 сторінках та 9 додатків на 48 сторінках. Робота містить 27 таблиць та 38 рисунків.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

**У вступі** обґрунтовано актуальність обраної теми дослідження, підкреслено зв'язок роботи з виконуваними і завершеними НДР, напрямами досліджень; сформульовано мету, поставлено вирішувані згідно мети задачі дослідження; надано перелік використаних у процесі дослідження методів; наведено наукову новизну і практичне значення отриманих результатів; підкреслено особистий внесок здобувача; подано дані стосовно апробації отриманих результатів, а також дані стосовно їх впровадження.

**У першому розділі** викладено результати проведеного аналізу досліджуваної предметної області, у тому числі – результати порівняльного аналізу формальних методів (включно з методами перевірки на моделі) та супутніх засобів (моделей, виразних засобів, засобів автоматизації), застосовуваних у процесі розроблення ПАС, у тому числі і у складі СКП, – з позиції аспектів їх застосування, а також одержуваного корисного ефекту, супутніх обчислювальних і просторових витрат.

За результатами проведеного аналізу обґрунтовано доцільність залучення формальних методів перевірки на моделі, і супутніх засобів, вже на етапі проєктування у складі етапів процесу розроблення ПАС, опрацьовуючи при цьому досліджувані артефакти за показниками і ФХ, і НФХ. Це дозволить вчасно виявляти потребу доопрацювання артефактів процесу розроблення з позиції їх несуперечності.

Результати проведеної класифікації формальних методів і засобів зведено, у відповідності до положень стандарту IEEE 1012-2016, у формі UML-діаграми (рис. 2), де центральними є поняття верифікації і валідації (V&V).

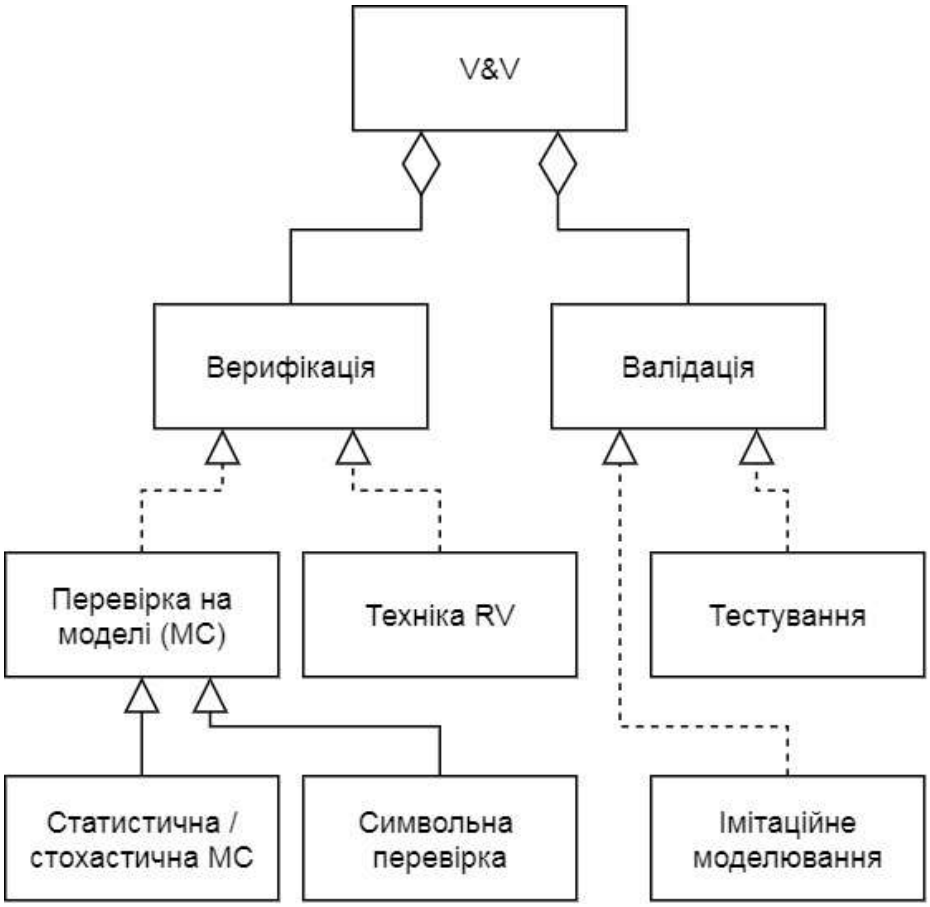


Рисунок 2 – Результати проведеної класифікації формальних методів і засобів

На рисунку 2, у частині змістового навантаження верифікації, вирізняється техніка RV (Runtime Verification), призначена до застосування на етапі реалізації у складі етапів процесу розроблення. Базуючись, у тому числі, на положеннях стандарту IEEE 1012-2016, за результатами проведеного аналізу було сформовано засади стосовно доцільності розроблення і застосування нового підходу до здійснення контролю артефактів процесу розроблення ПАС систем критичного призначення, за якого, згідно концепції багатовимірної верифікації, контроль пропонується здійснювати за показниками і ФХ, і НФХ, вже на етапі проєктування у складі етапів процесу розроблення.

**У другому розділі**, на підставі результатів проведеного аналізу, висвітлено розроблений комплексний підхід до контролю артефактів процесу розроблення ПАС. Підхід реалізовано у відповідності до концепції в основі об’єктно-орієнтованого підходу до проєктування – забезпечення єдності застосовуваних концепцій і нотацій. Цього було досягнуто, у тому числі, шляхом розроблення і застосування відповідних правил виконання перетворень конструкцій у складі досліджуваних артефактів. Дані правила викладено у межах опису розробленого методу синтезу формальних специфікацій, представленого у третьому розділі.

Концептуально, розроблений підхід є засобом регламентування шляхів сполучення результатів вирішення поставлених у роботі задач у формі комплексного рішення, призначеного до застосування при проєктуванні ПАС (рис. 3).

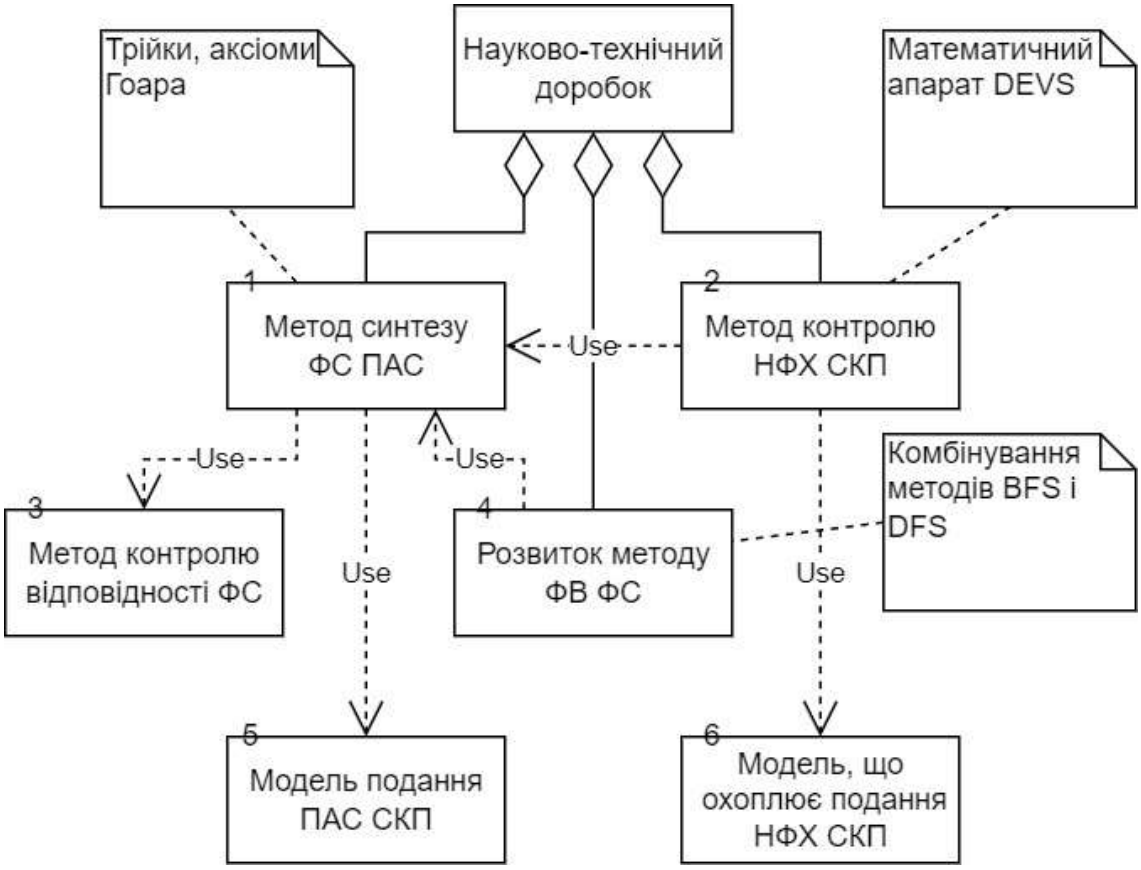


Рисунок 3 – Графічне подання розробленого і застосованого підходу

Комплексність підходу полягає в охопленні при проведенні контролю показників і ФХ, і НФХ, при проєктуванні ПАС.

На рисунку 3 згаданий вище розроблений метод синтезу формальних специфікацій, якому присвячено наступний, третій, розділ, представлено блоком 1. Використання на діаграмі відношення агрегування замість відношення композиції має на меті висвітлення допустимості залучення винесених на захист наукових здобутків, поданих блоками 1, 2 і 4, як безпосередньо, так і у складі альтернативних конструкцій.

Підходом охоплено, у тому числі, застосування наступних виразних засобів: алгоритмічної мови PlusCal – для формалізованого подання архітектурної складової ПАС; засобу TLA+ – для уможливлення проведення ФВ в автоматизованому режимі; засобів математичного апарату DEVS – для оцінювання результуючого значення досліджуваного показника НФХ.

У межах розділу також представлено розроблену модель подання ПАС у формі ФС (рис. 3, блок 5), призначену слугувати засобом уніфікації ФС – для здійснення на основі останніх контролю несуперечності ПАС, як досліджуваного показника ФХ, в автоматизованому режимі – шляхом застосування формального

методу перевірки на моделі TLC, а також розробленого розвитку цього методу, викладеного у четвертому розділі, і представленого блоком 4 на рисунку 3. Уніфікація при цьому розглядається у якості чинника, що уможливлює автоматизацію.

Розроблена модель полягає у виокремленні двох рівнів оперування складовими досліджуваних артефактів – аналітичного рівня і рівня реалізації. Аналітичний рівень – як площина сприйняття і аналізу ПАС розробником; рівень реалізації – площина уможливлення автоматизації процесу ФВ.

На аналітичному рівні залучаються трійки і аксіоми Гоара, у тому числі у якості засобів зниження обсягу коду результуючої ФС за показником кількості рядків коду, яка на рівні реалізації подається виразними засобами PlusCal і TLA+ (рис. 4).

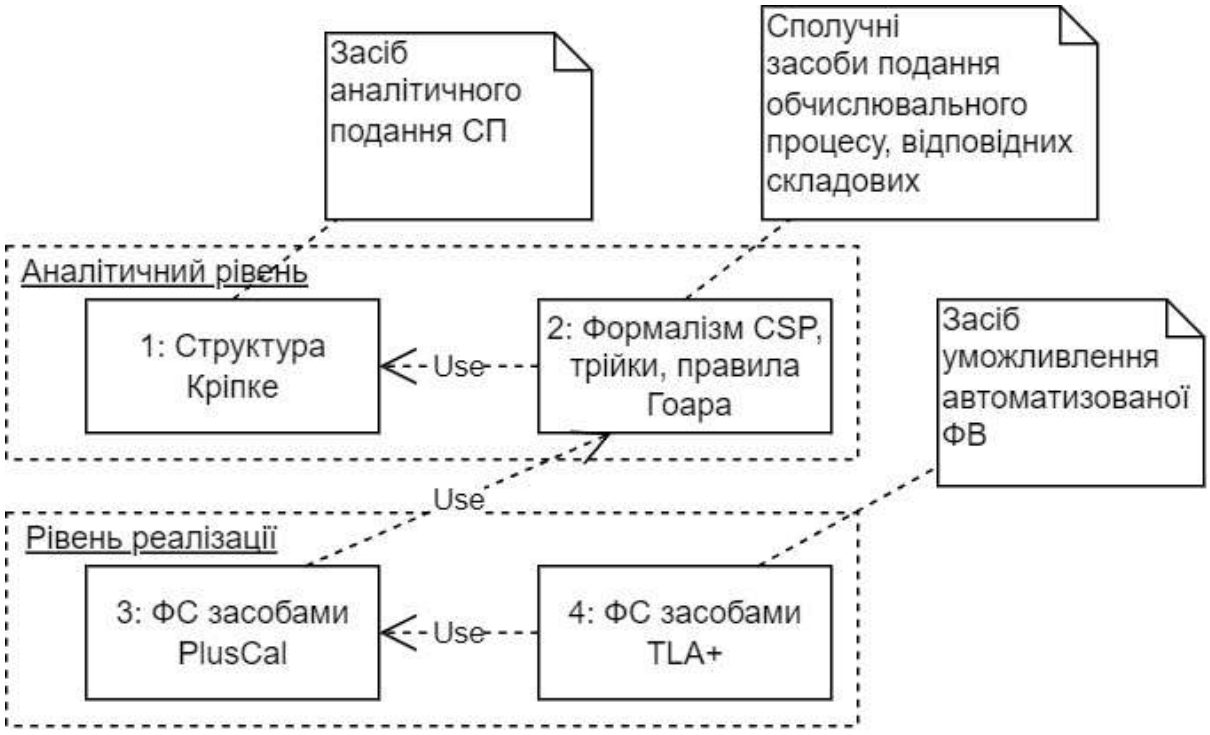


Рисунок 4 – Графічне подання концептуальної складової розробленої моделі

На рисунку 4 озвучені концептуальні рівні окреслено пунктиром. У межах пунктирних областей фігурують виокремлені типи артефактів. Типи визначено у залежності від залученого виразного засобу. Відношення, встановлені між блоками, є поданнями кроків розробленого методу синтезу ФС, викладеного у наступному, третьому, розділі. Нумерація блоків відображає порядок опрацювання артефактів відповідних типів.

Блок 1. Подання артефактів на основі засобів структури Кріпке $M = \langle S, S_0, R, L \rangle$ над кінцевою множиною атомарних висловлювань $AP = V \times D$, де $V$ і $D$ – множини змінних і допустимих значень змінних відповідно; $S$ – кінцева множина станів; $S_0 \subset S$ – непуста множина початкових станів СП; $R \subseteq S^2$ – тотальна множина переходів: $\forall s \in S \; \exists s' \in S : (s, s') \in R$; $L : S \to 2^{AP}$ – функція розмітки

станів СП елементами множини $AP$, що приймають істинні значення у відповідних станах.

Блок 2. Подання артефактів на основі засобів формалізму CSP (Communicating Sequential Processes), включно з «трійками» і правилами Гоара, серед яких правило композиції опрацьовано у якості засобу скорочення кількості рядків результуючої ФС як артефакту на основі засобів TLA+.

Блок 3. Подання артефактів засобами алгоритмічної мови PlusCal для окреслення архітектурної складової результуючої ФС.

Блок 4. Подання артефактів на основі виразних засобів формалізму TLA+, для сприяння автоматизації процесу ФВ, призначеного до виконання на основі методу TLC або розробленого розвитку зазначеного методу, представленого у четвертому розділі.

Розроблену модель, графічно представлену на рисунку 4, формалізовано згідно теоретико-множинного підходу:

$$\langle A, T \rangle, \tag{1}$$

де $A = \{a_i | i = 1,2,...,4\}$ – множина виокремлених типів артефактів: $a_i \in A$ вирізняється з-поміж інших типів залученою формальною системою: $a_1 \in A$ – структурою Кріпке; $a_2 \in A$ – засобами CSP; $a_3 \in A$ – засобами PlusCal; $a_4 \in A$ – засобами TLA+; $T \subset A^2$ – множина відношень над елементами множини $A$: $T = \{(a_1, a_2), (a_2, a_3), (a_3, a_4)\}$, для елементів якої встановлено властивість «спадковості»: $a_2 = T(a_1)$, $a_3 = T(a_2) = T(T(a_1))$, $a_4 = T(a_3) = T(T(a_2)) = T(T(T(a_1)))$; іншими словами: $a_1 \prec a_2 \prec ... \prec a_4$. Елементи множини $T$ – подання кроків розробленого методу синтезу ФС, викладеного у третьому розділі.

Для артефактів типу $a_1 \in A$ ПАС представлено множиною «поведінок» – кінцевих послідовностей станів СП:

$$B = \{b_i\}, i = 1,2,...,m \in N, \tag{2}$$

де $b_i \in B$ – $i$-а поведінка:

$$b_i = s_0, s_1, ..., s_f, ..., s_{l \in N}, \tag{3}$$

де $s_0 \in S_0 \subset S$ – початковий стан СП; $s' = R(s) \in S \setminus S_0$ – наступний стан: $s_1 = R(s_0)$, $s_2 = R(s_1) = R(R(s_0))$ і т. д., $0 \le f \le l = (n \cdot |D|) - 1$, де $n = |V|$ – кількість змінних станів СП, $|D|$ – кількість допустимих значень змінних. При цьому $s_l \in S$ – заключний стан: $R(s_l) = s_l$.

Для артефактів типу $a_2 = T(a_1) \in A$ елементи (3) множини (2) подано у формі відповідних протоколів обчислювального процесу – виразних засобів формалізму CSP:

$$p_i = \langle e_1, e_2, ..., e_f, ..., e_{l \in N} \rangle \in P, \quad (4)$$

де $e_f$ – f-а подія, передумовою виникнення якої є стан $s_{f-1} \in S\ (f = 1,2,..,l)$, пост-умовою – стан $R(s_{f-1}) = s_f \in S$.

Для залучення перед- і пост-умов у якості засобів сполучення подій застосовано «трійки» Гоара:

$$\{\varphi_{f-1}\} e_f \{\varphi_f\}, \quad (5)$$

де $\varphi_{f-1}$ – передумова виникнення події $e_f$ – як кон'юнкція на основі елементів множини $L(s_{f-1}) \subset AP$; $\varphi_f$ – пост-умова, формалізована аналогічним чином – на основі елементів множини $L(R(s_{f-1})) = L(s_f) \subset AP$.

Для сполучення конструкцій (5) згідно виразу (4) залучено правило композиції Гоара:

$$\frac{\{\varphi_0\} e_1 \{\varphi_1\}, \{\varphi_1\} e_2 \{\varphi_2\}, ..., \{\varphi_{l-1}\} e_l \{\varphi_l\}}{\{\varphi_0\} e_1; e_2; ...; e_l \{\varphi_l\}}, \quad (6)$$

де $\varphi_0$ – початкова умова – кон'юнкція над елементами множини $L(s_0)$: як точка відліку для початку процесу ФВ методом перевірки на моделі. У чисельнику – послідовність конструкцій (5) згідно протоколу (4). У знаменнику – результат застосування правила, що проявляється у зменшенні кількості рядків псевдокоду результуючої ФС – за рахунок виключення подань проміжних конструкцій – $\varphi_1, ..., \varphi_{l-1}$.

У **третьому розділі** представлено кількісне оцінювання одержуваного корисного ефекту від застосування правила (6): для двох граничних випадків – за аналогією до оцінок «зверху» і «знизу» теорії алгоритмів.

«Оцінка знизу». Із залученням програмно реалізованих допоміжних засобів автоматизації, згенеровано множину синтетичних ФС послідовного характеру – без умовних переходів: для кількості змінних $n = 2^1, 2^2, ..., 2^8$; $|D| = 3$. Отримані результати зведено у таблицю 1.

Таблиця 1 – Результати оцінювання корисного ефекту для граничного випадку «оцінка знизу»

| № з/п | $n$ | Кількість рядків ФС | | Різниця, $y - y'$ | $\alpha$ |
|---|---|---|---|---|---|
| | | Без застосування правила (6), $y$ | Із застосуванням правила (6), $y'$ | | |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | $2^1$ | 17 | 14 | 3 | 0,1765 |
| 2 | $2^2$ | 29 | 22 | 7 | 0,2414 |
| 3 | $2^3$ | 53 | 38 | 15 | 0,2830 |
| 4 | $2^4$ | 101 | 70 | 31 | 0,3069 |
| 5 | $2^5$ | 197 | 134 | 63 | 0,3198 |
| 6 | $2^6$ | 389 | 262 | 127 | 0,3265 |
| 7 | $2^7$ | 773 | 518 | 255 | 0,3299 |
| 8 | $2^8$ | 1541 | 1030 | 511 | 0,3316 |

У таблиці 1 $n = |V|$ (стовпець 2) – кількість змінних станів СП – варіативна складова: $V \times D = AP$. Із табл. 1 видно, що різниця $(y - y')$ становить $2 \cdot n - 1$ (стовпець 5). У якості показника одержуваного корисного ефекту залучено наступний вираз (стовпець 6):

$$\alpha(y, y') = (y - y') / y . \qquad (7)$$

Згідно таблиці 1, на залученому діапазоні $n = 2^1, 2^2, ..., 2^8$ отримано, відповідно, корисний ефект від близько 18 % – до близько 33 %.

Адекватність розробленої моделі підтверджено опосередковано – шляхом застосування розробленого методу контролю відповідності результуючого артефакту типу $a_4 \in A$ первинному артефакту типу $a_1 \in A$ (1), (рис. 4).

«Оцінка зверху». У ФС паралелізм подано згідно моделі чергування. Прототипом архітектурної складової ФС послугував сценарій функціонування розподіленої Grid-системи, за якого обчислювальна задача розподіляється на складові задачі, які, у свою чергу, надсилаються обчислювальним вузлам. Потім проміжні результати обчислень зберігаються (рис. 5).

На рисунку 5, у якості прикладу, подано архітектурну складову ФС для випадку $n = 2^3$ і $|D| = 2$. Пунктиром окреслено ідеальне бінарне дерево у складі результуючої архітектури. Номер рівня задає порядок зміни значень відповідних елементів. При цьому значеннями $2^0, ..., 2^2$ подано кількості змінних, що залучаються на відповідних рівнях, де верхні індекси 0,…,2 – порядкові номери рівнів. На рівнях 1 і 2 застосовується модель чергування.

Елементи множини $V$ змінюють значення наступним чином: спочатку – $v_1 \in V$, потім, згідно моделі чергування, – $v_2, v_3 \in V$, і. т. д.

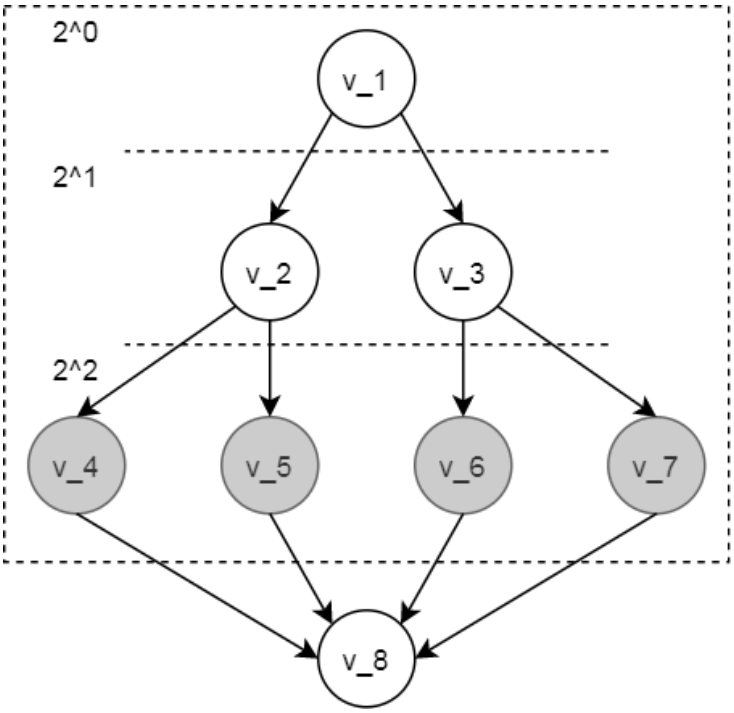


Рисунок 5 – Графічне подання архітектурної складової ФС для випадку $n=2^3$

На рисунку 5 $(n/2)-1$ вершин-елементів підмножини $\{v_1,...,v_3\}\subset V$ – подання вузлів, на яких виконується декомпозиція обчислювальної задачі; $n/2$ вершин-елементів підмножини $\{v_4,...,v_7\}\subset V$ – подання вузлів, на яких безпосередньо виконуються обчислення; $v_8\in V$ – подання вузла, де накопичуються результати проміжних обчислень.

Отримані результати проведеного кількісного оцінювання корисного ефекту від залучення розробленої моделі для даного граничного випадку зведено у табл. 2.

Таблиця 2 – Результати оцінювання корисного ефекту для граничного випадку «оцінка зверху»

| № з/п | $n$ | Кількість рядків ФС | | Різниця, $y-y'$ | $\alpha$ |
|---|---|---|---|---|---|
| | | Без застосування правила (6), $y$ | Із застосуванням правила (6), $y'$ | | |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | $2^2$ | 18 | 14 | 4 | 0,2222 |
| 2 | $2^3$ | 111 | 92 | 19 | 0,1712 |
| 3 | $2^4$ | 1936702 | 1936428 | 274 | $1{,}4148\cdot10^{-4}$ |

У таблиці 2, на відміну від таблиці 1, спостерігається протилежна ситуація – із збільшенням значення $n=2^2,2^3,2^4$ одержуваний корисний ефект знижується – від близько 22 % – до близько 0 %.

У таблиці 2 значення $n$ обмежено на рівні $2^3$ – через експоненційний характер зростання простору станів СП, у залежності від $n$: для випадку $n=2^4$ мала місце нестача доступної обчислювальній системі оперативної пам'яті (8 ГБ). Стрімкість такого зростання опосередковано відображена у стовпцях 3 і 4. Наприклад, для випадку $n=2^3$ розмір файлу-подання ФС склав близько 7 КБ, а для випадку $n=2^4$ – близько 210727 КБ.

Зведений (для обох граничних випадків) графік отриманих результатів проведеного оцінювання корисного ефекту від застосування розробленої моделі подано на рисунку 6.

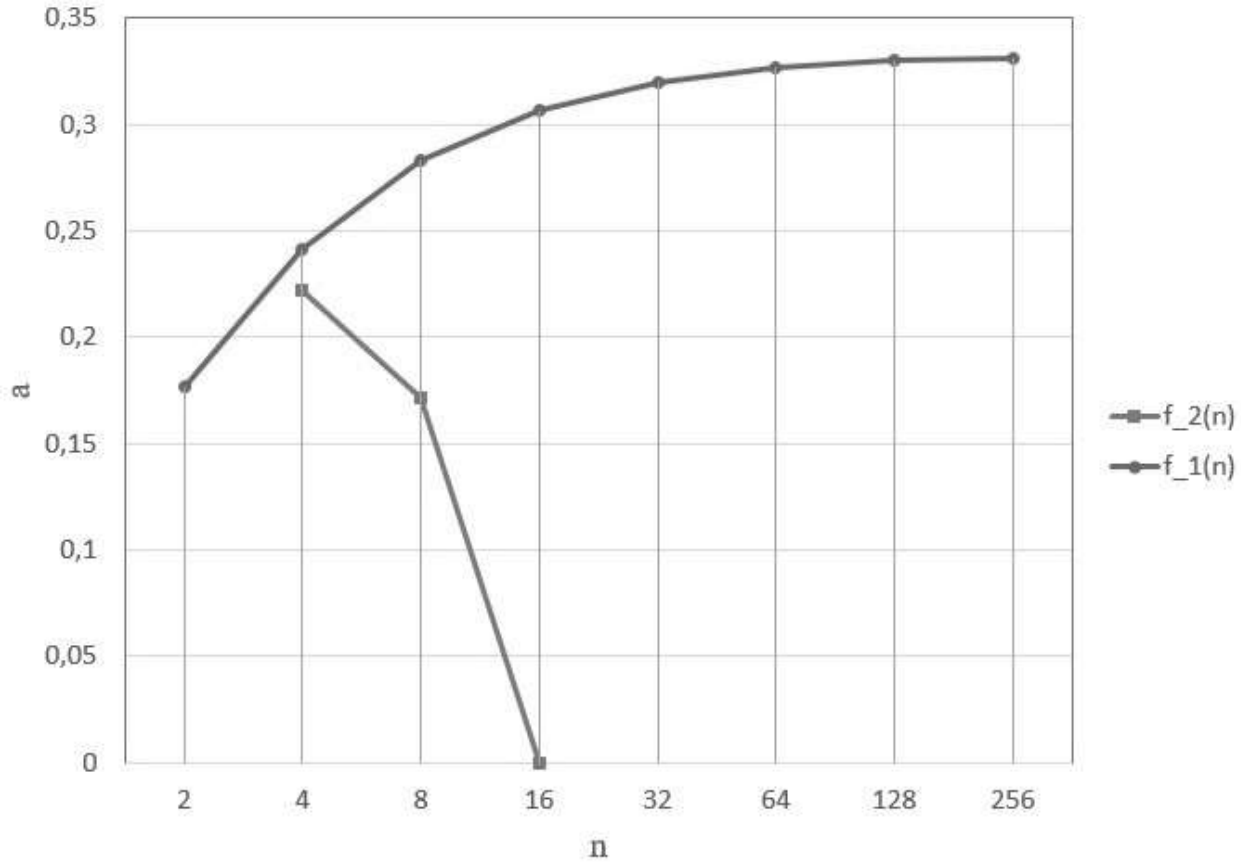


Рисунок 6 – Зведений графік отриманих результатів оцінювання корисного ефекту від застосування правила композиції (6)

На рисунку 6 при побудові графіку застосовано кусково-лінійну інтерполяцію.

Викладено розроблений метод синтезу ФС, із застосуванням виразних засобів CSP, PlusCal і TLA+. Методом передбачено залучення викладеної у другому розділі розробленої моделі подання ФС.

Метод побудовано у відповідності до рисунку 4, де кожен крок подано відповідним відношенням «use» UML-нотації.

Результатом застосування методу є артефакт типу $a_4 \in A$, а формалізованими поданнями кроків методу – елементи множини $T=\{(a_1,a_2),(a_2,a_3),(a_3,a_4)\}$ (1).

Призначення методу – надати прозорий уніфікований механізм одержання артефактів типу $a_4 \in A$ – (1), (рис. 4) – на основі графічних подань ПАС, що фігурують у формі блок-схем алгоритмів, UML-діаграм дій.

При розробленні методу, для оцінювання успішності застосування останнього, було поставлено і вирішено допоміжну задачу – проведення контролю відповідності результуючого артефакту типу $a_4 \in A$ первинному артефакту типу $a_1 \in A$ – щоб мати можливість поширювати висновки за результатами проведення автоматизованої ФВ похідних артефактів типу $a_4 \in A$ на первинні артефакти типу $a_1 \in A$.

Для розв'язання названої допоміжної задачі – задачу ФВ, вирішувану методом TLC, а також із застосуванням розробленого розвитку цього методу, викладеного у четвертому розділі, сформульовано наступним чином:

$$(M, b \models \psi) \vee (M, b \models \neq \psi), \tag{8}$$

де $M$ – структура Кріпке; $b$ – поведінка (3); $\psi$ – темпоральна формула, подана у формі артефакту типу $a_4 \in A$.

Вираз (8) є тавтологією – щоб наголосити на значимості одержуваних результатів проведення ФВ як для випадку підтвердження несуперечності ФС, так і для випадку виявлення суперечностей.

У випадку істинності виразу $(M, b \models \psi)$ у складі конструкції (8) формула $\psi$ прийматиме істинне значення $\forall s \in S$ у складі $b$. При цьому протилежне твердження $(M, b \models \neq \psi)$ буде хибним. У свою чергу, виразом $(M, b \models \neq \psi)$ подається альтернативний сценарій – $\exists s \in S : M, s \models \neq \psi$, що може бути обумовлений як суперечністю первинного артефакту типу $a_1 \in A$, так і спотвореннями, внесеними при здійсненні кроків розробленого методу синтезу ФС – послідовності переходів від артефакту типу $a_1 \in A$ – до результуючого артефакту типу $a_4 \in A$.

Вираз (8) подано як диз'юнкцію, аби поставити наголос на доцільності проведення ФВ методом TLC або на основі розробленого розвитку зазначеного методу, викладеного у четвертому розділі, – для одержання корисного ефекту, який проявляється у кожному з наступних випадків:

– підтвердження несуперечності ПАС для обраного рівня деталізації ФС, свідченням чого є істинність висловлювання $(M, b \models \psi)$. Це, за умови встановлення відповідності результуючого артефакту типу $a_4 \in A$ на основі розробленого методу контролю відповідності, є аргументом на користь або підвищення рівня деталізації ФС і повторного проведення ФВ, або завершення процесу ФВ;

– виявлення суперечності / суперечностей у ФС – результуючому артефакті типу $a_4 \in A$. При цьому, шляхом залучення розробленого методу контролю відповідності, встановлюється першопричина суперечності / суперечностей – безпосередньо первинний артефакт типу $a_1 \in A$ або результуючий похідний від нього артефакт типу $a_4 \in A$.

Запропонований і застосований підхід до використання розробленого методу контролю відповідності подано на рисунку 7.

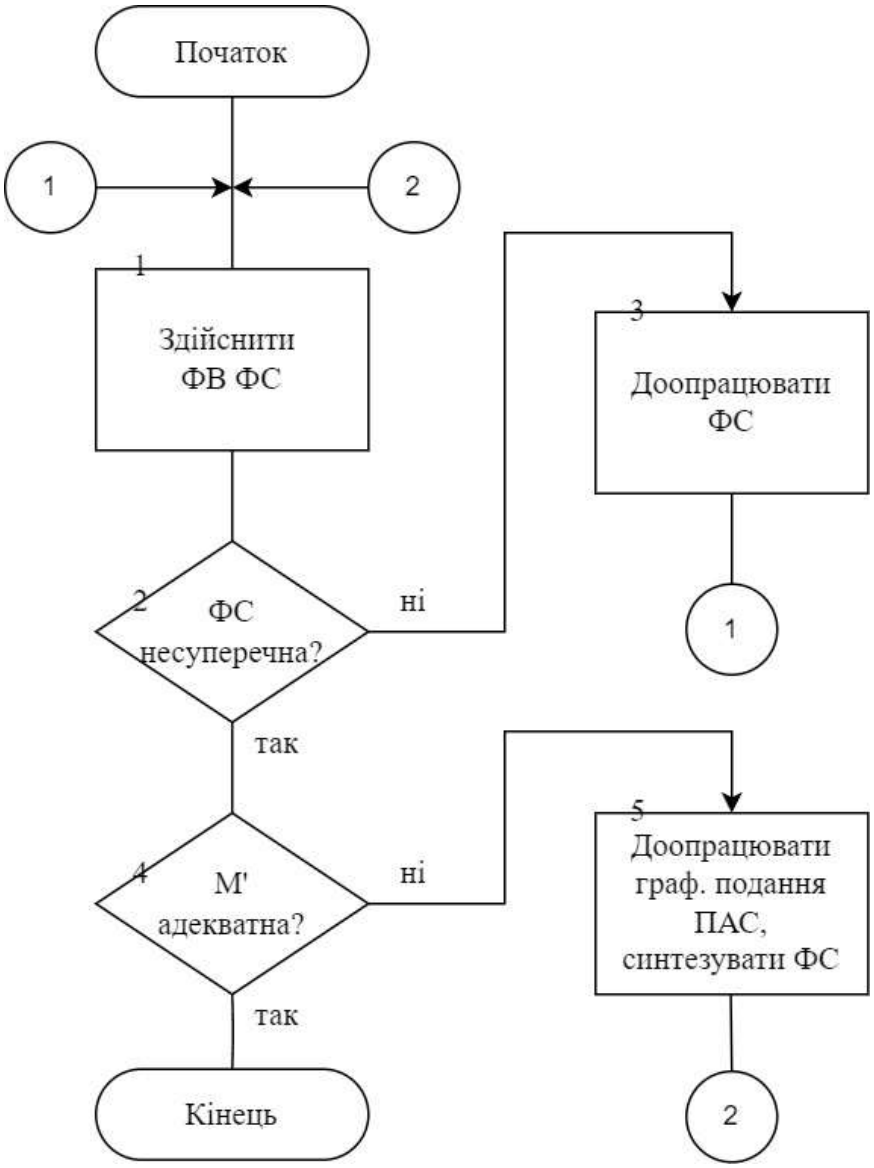


Рисунок 7 – Блок-схема алгоритму залучення розробленого методу контролю відповідності

На рисунку 7 застосування методу контролю відповідності подане блоком 4.

Метод полягає у співставленні наступних характеристик СП для артефактів типу $a_1 \in A$ і $a_4 \in A$: кількість станів СП; глибина обходу простору станів СП.

Для артефакту типу $a_1 \in A$ СП будується аналітично; для випадку $a_4 \in A$ – одержується в автоматизованому режимі – шляхом зчитування даних файлу-лістингу результатів ФВ.

Розроблений метод контролю відповідності подано на рисунку 8.

Для граничного випадку «оцінка зверху» (рис. 5, табл. 2) у якості засобів оцінювання просторових характеристик ФС і відповідних СП запропоновано оціночні функції $g_1(n), g_2(n),...,g_6(n)$, де $n = |V|$.

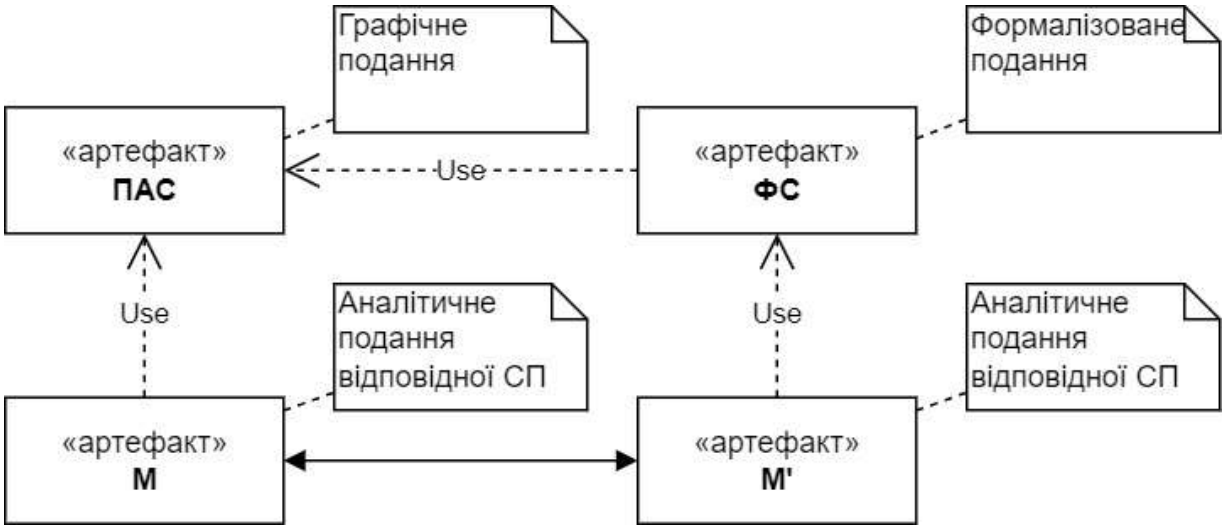


Рисунок 8 – Графічне подання розробленого методу контролю відповідності

Функція оцінювання кількості вузлів підграфу, окресленого прямокутною областю (рис. 5):

$$g_1(n)=\sum_{k=0}^{(\log_2 n)-1} 2^k = |V|-1=n-1, \tag{9}$$

де $k$ – порядковий номер рівня вузлів у складі підграфу.

Функція оцінювання кількості дуг графу-подання архітектурної складової ФС – $G=\langle V,E\rangle$ (рис. 5):

$$g_2(n)=|E|=n+\frac{n}{2}-2=\frac{3\cdot n-4}{2}, \tag{10}$$

де $n=2^2,2^3,..,2^{\lfloor \log_2 n \rfloor}$.

З виразу (10) маємо, що для випадку $n=2^1$ архітектурна складова (рис. 5) вироджується у таку, що відповідає граничному випадку «оцінка знизу». Через цей аспект відлік значень було почато з $n=2^2$.

Для оцінюванні кількості станів СП, що буде синтезовано у процесі ФВ, запропоновано і залучено наступну функцію:

$$g_3(n)=\sum_{k=1}^{(\log_2 n)-1}\left(2^{2^k}-1\right)+\beta=|S|, \tag{11}$$

де $\beta=3=const$ – засіб врахування наступних станів СП: $s_0\in S$, а також передостаннього і заключного станів – $s_{l-1}\in S:\ R(s_{l-1})=s_l\in S:\ R(s_l)=s_l\in S$.

Згідно (11), для випадків $n=2^2,2^3,2^4$ маємо $|S|=6,21,276$ відповідно. Наприклад, для випадку $n=2^2$ відповідну СП подано на рисунку 9.

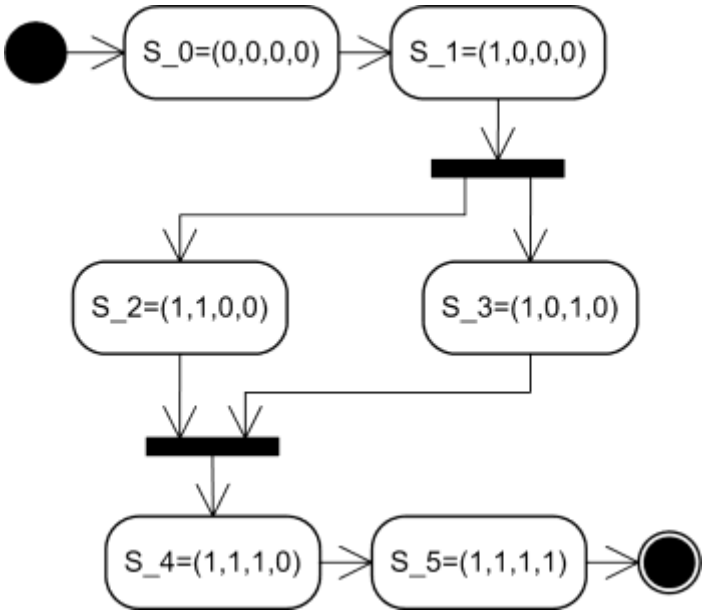


Рисунок 9 – Діаграма станів для випадку $n = 2^2$

З рисунку 9 видно, що згідно моделі чергування залучено стани $s_2, s_3 \in S$, що відрізняються значеннями змінних $v_2, v_3 \in V$: $L(s_2) \Delta L(s_3) = \{(v_2,0),(v_2,1),(v_3,0),(v_3,1)\}$. Результатом цього є дві альтернативні поведінки $b_1, b_2 \in B$ (3), для яких формуються відповідні протоколи обчислювальних процесів $p_1, p_2 \in P$ (4): $p_1 = \langle e_1, e_2, e_3, e_4 \rangle$, $p_2 = \langle e_1, e_3, e_2, e_4 \rangle$.

Функція оцінювання кількості переходів між станами СП:

$$g_4(n) = \sum_{k=1}^{(\log_2 n)-1} \left(2^{2^k+k-1}\right) + \gamma = |R|, \tag{12}$$

де $\gamma = 2 = const$ – засіб урахування початкового і заключного переходів СП: $(s_0, s_1) \in R$ і $(s_{l-1}, s_l) \in R$.

Функція оцінювання глибини обходу простору станів СП:

$$g_5(n) = \sum_{k=0}^{(\log_2 n)-1} \left(2^k\right) + 2 = g_1(n) + 2 = |V| + 1 = n + 1, \tag{13}$$

де $n = 2^1, 2^2, 2^3, \ldots$

Функція оцінювання кількості альтернативних шляхів СП, що буде побудовано у процесі ФВ реалізованої згідно моделі чергування ФС:

$$g_6(n) = \prod_{k=1}^{(\log_2 n)-1} \left(2^k\right)! = |B|. \tag{14}$$

Як узагальнення, вирази (9) і (10) залучено у якості засобів оцінювання просторових характеристик безпосередньо ФС, поданої згідно моделі чергування, а вирази (11) – (14) – у якості засобів оцінювання просторових характеристик СП, що будується у процесів ФВ. Розрахункові значення, підтверджені експериментально, зведено у таблиці 3.

Таблиця 3 – Розрахункові значення функцій (9) – (14)

| № з/п | $n$ | Оціночні функції | | | | | |
|---|---|---|---|---|---|---|---|
| | | $g_1(n)$, (9) | $g_2(n)$, (10) | $g_3(n)$, (11) | $g_4(n)$, (12) | $g_5(n)$, (13) | $g_6(n)$, (14) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | $2^2$ | 3 | 4 | 6 | 6 | 5 | 2 |
| 2 | $2^3$ | 7 | 10 | 21 | 38 | 9 | 48 |
| 3 | $2^4$ | 15 | 22 | 276 | 1062 | 17 | 1935360 |

Отже, у межах розділу викладено два розроблені методи – метод синтезу ФС і метод контролю відповідності результуючих ФС первинним артефактам – блок-схемам алгоритмів, UML-діаграмам дій. Метод синтезу ФС базується на основі розробленої моделі, викладеної у другому розділі, із залученням на завершальному кроці методу контролю відповідності.

Розроблений метод синтезу ФС полягає у виконанні наступних кроків:

1. Сформувати множини $V$ і $D$, на основі яких одержати множину $AP$.

2. Побудувати структуру Кріпке на основі елементів множини $AP$.

3–5. Послідовно реалізувати переходи $(a_1, a_2) \in T$, $(a_2, a_3) \in T$ і $(a_3, a_4) \in T$ (1), результатом чого має бути одержання цільового артефакту типу $a_4 \in A$ – ФС на основі виразних засобів формалізму TLA+.

6. Підтвердити відповідність результуючого артефакту типу $a_4 \in A$ первинному артефакту типу $a_1 \in A$ на основі розробленого методу контролю відповідності.

Для реалізації кроків 3–5 методу розроблено і застосовано відповідні правила перетворення конструкцій у складі артефактів відмінних типів.

**У четвертому розділі** викладено розроблений розвиток поширеного методу перевірки на моделі TLC. Проведений розвиток полягає у сполученні методів обходу вершин графу-подання СП у процесі автоматизованої ФВ – методу BFS і методу DFS теорії графів – за ітеративного підходу до організації процесу ФВ.

Проведений розвиток полягає у виконанні наступних кроків:

1. Здійснення BFS-обходу простору станів СП, що дасть змогу визначити глибину обходу. На наступних кроках цей параметр залучається для проведення DFS-обходів.

2. Проведення серії DFS-обходів, за рахунок чого досягається скорочення супутніх процесу ФВ результуючих часових витрат. Одержуваний при цьому корисний ефект визначається, у тому числі, архітектурною складовою ФС, кількістю змінних станів, кількістю ітерацій проведення DFS-обходу.

Дослідження проведеного розвитку методу TLC здійснено для штучних граничних і предметно орієнтованих сценаріїв, поданих у формі відповідних артефактів – блок-схем алгоритмів, UML-діаграм дій.

Граничні випадки – на основі сценаріїв, опрацьованих при дослідженні розробленої моделі подання ПАС, викладеної у другому розділі.

Предметно орієнтовані випадки охоплюють сценарії галузі енергетики, аерокосмічної галузі (рис. 10).

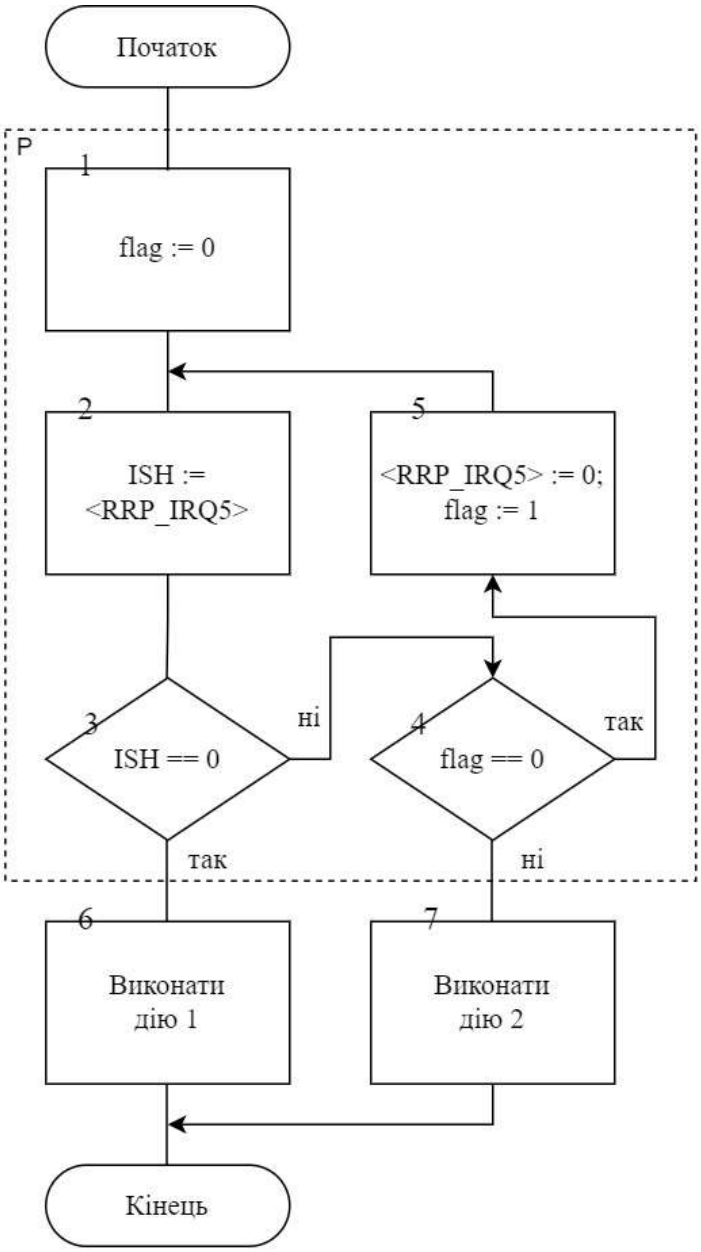


Рисунок 10 – Фрагмент блок-схеми алгоритму контролю вихідного стану регістрів пристрою введення-виведення підсистеми керування орієнтацією космічного апарату

Дослідження проведено у напрямі оцінювання обчислювальних і просторових витрат, супутніх реалізації процесу ФВ – на основі базового методу TLC і на основі розробленого розвитку зазначеного методу. При цьому було опрацьовано обидві

альтернативні реалізації методу TLC – здійснюваних шляхом BFS- і DFS-обходів простору станів СП.

На рисунку 10 пунктирною областю окреслено фрагмент блок-схеми, що поетапно повторюється ще 14 разів, із залученням відмінних змінних. Результуючий артефакт містить 77 блоків, і включає $n = |V| = 18$ змінних.

Отримані результати проведених досліджень у розрізі співставлення значень показників обчислювальних і просторових витрат, супутніх BFS- і DFS-реалізаціям методу TLC, для випадку, поданого на рис. 10, зведено на рисунку 11.

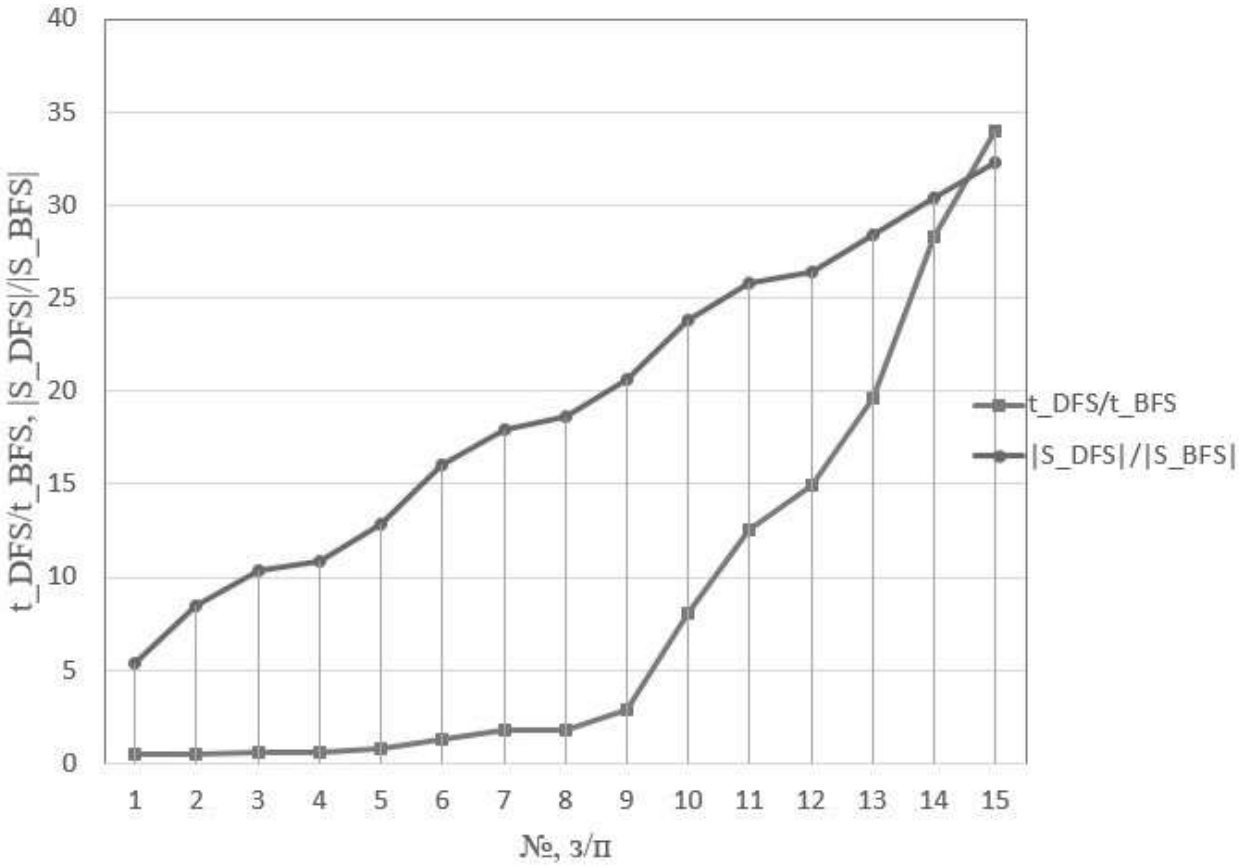


Рисунок 11 – Графік залежності значень показників $\bar{t}_{DFS}/\bar{t}_{BFS}$ і $\left|S^*_{DFS}\right|/\left|S^*_{BFS}\right|$ від архітектурної складової ФС і кількості залучених змінних

На рисунку 11 показники $\bar{t}_{DFS}/\bar{t}_{BFS}$ і $\left|S^*_{DFS}\right|/\left|S^*_{BFS}\right|$ наведено для демонстрації характеру зміни відношень значень обчислювальних і просторових витрат відповідно, де $\bar{t}_{DFS}$ – середнє значення часових витрат на ФВ шляхом DFS-обходу простору станів СП, $\bar{t}_{BFS}$ – шляхом BFS-обходу; $\left|S^*_{DFS}\right|$ – загальна кількість станів СП, сформованих і опрацьованих у процесі ФВ шляхом DFS-обходу, $\left|S^*_{BFS}\right|$ – шляхом BFS-обходу. При цьому по осі Ox подано порядкові номери ітерацій, де за кожен наступний крок (2, 3,…,15) поточна версія блок-схеми, починаючи з такої, поданої на рисунку 10, розширюється фрагментом, окресленим пунктиром, із залученням нових змінних.

З рисунку 11 видно, що за показником просторових витрат $\left|S^*_{DFS}\right| / \left|S^*_{BFS}\right|$ DFS-реалізація поступається альтернативній BFS-реалізації на усьому інтервалі значень осі Ox. У свою чергу, за показником обчислювальних витрат $\bar{t}_{DFS} / \bar{t}_{BFS}$ має місце граничне значення $n$, яке опрацьовано у якості критерію обґрунтування доцільності залучення DFS-реалізації. Для наведеного випадку таким значенням є $n \le 2^3$ (табл. 4).

Таблиця 4 – Результати дослідження обчислювальних витрат, супутніх процесу ФВ для випадку, поданого на рисунку 10

| № з/п | $n$ | $\bar{t}_{BFS}$, с | $\bar{t}_{DFS}$, с | $\bar{t}_{DFS} / \bar{t}_{BFS}$ | $depth$, вершин |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 4 | 0,893 | 0,437 | 0,489 | 10 |
| 2 | 6 | 0,929 | 0,477 | 0,513 | 15 |
| 3 | 7 | 0,957 | 0,554 | 0,579 | 18 |
| 4 | 7 | 0,969 | 0,578 | 0,596 | 19 |
| 5 | 8 | 1,001 | 0,788 | 0,787 | 22 |
| 6 | 10 | 1,140 | 1,505 | 1,320 | 27 |
| 7 | 11 | 1,448 | 2,577 | 1,780 | 30 |
| 8 | 11 | 1,468 | 2,674 | 1,822 | 31 |
| 9 | 12 | 1,682 | 4,818 | 2,864 | 34 |
| 10 | 14 | 2,460 | 19,751 | 8,029 | 39 |
| 11 | 15 | 3,552 | 44,575 | 12,549 | 42 |
| 12 | 15 | 3,560 | 53,226 | 14,951 | 43 |
| 13 | 16 | 5,370 | 105,340 | 19,616 | 46 |
| 14 | 17 | 9,666 | 273,970 | 28,344 | 49 |
| 15 | 18 | 17,127 | 581,860 | 33,973 | 52 |

У таблиці 4 параметр $depth$ – глибина обходу простору станів СП, як кількість станів.

Проведений розвиток методу TLC базується на визначенні граничного значення $n$ і на ітеративному застосуванні DFS-реалізації методу. Для оцінювання одержуваного корисного ефекту від застосування проведеного розвитку методу залучено розроблені для цього оціночні функції, отримані шляхом вирішення задачі апроксимації. Дослідження проведено, у тому числі, за критерієм зниження результуючих часових витрат на здійснення ФВ – одержуваний корисний ефект склав від близько 15 % – до близько 110 %.

З позиції урахування апаратних можливостей актуальних обчислювальних систем, досліджено, у тому числі, одержуваний корисний ефект від введення мультипоточності до складу програмних реалізацій – він склав від близько 26 % – до близько 123 % – у залежності від застосованого методу обходу (BFS або DFS) і кількості залучених програмних потоків.

За результатами проведених досліджень сформульовано рекомендації до застосування розробленого розвитку методу TLC.

**У п’ятому розділі** викладено розроблену стратифіковану модель подання ПАС у формі комп’ютерної моделі, призначену слугувати прототипом останньої – засобом уможливлення охоплення у формалізованому поданні також і НФХ-складової – вже на етапі проєктування процесу розроблення ПАС.

Розроблена модель характеризується властивістю забезпечення спадковості – відтворення архітектурної складової ФС, несуперечність якої вже було підтверджено на основі базового методу TLC або на основі розробленого розвитку зазначеного методу, викладеного у четвертому розділі.

Представлена модель є інструментом, що надає засоби подання як оціночних, так і фактичних значень складових заданого показника НФХ, результуюче значення якого накопичується у процесі імітаційного дискретно-подійного моделювання на основі розробленого методу, викладеного у шостому розділі.

Розроблена модель також характеризується властивостями модульності та ієрархічності, які адресуються у якості чинників, що сприяють структурованості та, як результат, гнучкості реконфігурування результуючої комп’ютерної моделі ПАС, призначеної слугувати засобом уможливлення контролю значення заданого показника НФХ вже на етапі проєктування процесу розроблення ПАС.

Модель базується на оперуванні конструкціями «атомарної» і «складеної» моделей математичного апарату DEVS. При цьому «атомарні» складові залучаються у якості елементів нижнього ієрархічного рівня, а «складені» – у якості елементів наступних рівнів. У межах рівнів відповідні елементи взаємодіють згідно моделі обміну повідомленнями.

**У шостому розділі** викладено розроблений метод контролю значення досліджуваного показника НФХ при проєктуванні ПАС, який фігурує у складі артефактів процесу розроблення.

Метод призначений слугувати засобом уможливлення зазначеного контролю шляхом проведення імітаційного дискретно-подійного моделювання на основі комп’ютерних моделей, побудованих у відповідності до розробленої моделі як стратифікованої архітектури, представленої у п’ятому розділі.

Розроблений метод полягає у виконанні таких кроків:

1. У відповідності до запропонованої моделі як стратифікованої архітектури, викладеної у п’ятому розділі, шляхом оперування конструкціями «атомарної» і «складеної» моделей математичного апарату DEVS, будується результуюча складена комп’ютерна модель, призначена слугувати засобом, на основі якого виконується контроль досліджуваного показника НФХ при проєктуванні ПАС системи критичного призначення.

2. Вибір механізму просування модельного часу, що полягає у використанні у якості відліків оціночних та/або фактичних значень.

3. Проведення імітаційного дискретно-подійного моделювання, у процесі якого результуюче значення досліджуваного показника накопичується на основі механізму обміну повідомленнями між компонентами складеної комп’ютерної

моделі, які, у відповідності до розробленої моделі, представленої у п’ятому розділі, фігурують на спільному ієрархічному рівні.

Зауваження: архітектурна складова результуючої складеної комп’ютерної моделі, що будується на кроці 1 розробленого методу, формується згідно відповідної складової ФС, несуперечність якої вже було підтверджено на основі методу TLC або розробленого розвитку цього методу, викладеного у четвертому розділі.

При дослідженні розробленого методу у якості показника НФХ опрацьовано часові витрати, супутні реалізації ФХ згідно ПАС. Оцінювання корисного ефекту, одержуваного у результаті застосування методу, проведено згідно наступного показника: відношення часових витрат, супутніх роботі методу для випадку оперування оціночними значеннями досліджуваного показника НФХ, до відповідних витрат для випадку залучення фактичних значень складових.

Для проведення досліджень методу, ПАС було реалізовано у формі композитного вебсервісу. Отримані результати оцінювання корисного ефекту охарактеризовано як вагомі. Достовірність одержуваних на основі методу оціночних значень досліджуваного показника НФХ підтверджено.

Наведено інформацію стосовно практичного значення отриманих результатів, відомості щодо впровадження.

**У додатках** до дисертаційної роботи представлено наступне: формальні специфікації, фрагменти формальних специфікацій; програмні реалізації допоміжних засобів автоматизації процесу проведення дисертаційних досліджень; фрагмент UML-діаграми дій як фрагмент дослідженого артефакту; допоміжні результати досліджень; копії документів, що підтверджують практичне значення отриманих результатів, серед яких – акт впровадження, листи підтвердження впровадження, листи підтримки від організацій та установ; перелік публікацій, у яких висвітлено отримані результати проведених досліджень; відомості стосовно апробації отриманих результатів.

## ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну проблему забезпечення контролю артефактів процесу проєктування програмно-алгоритмічної складової систем критичного призначення стосовно несуперечності артефактів. Проблему вирішено за рахунок розроблення, дослідження і застосування формальних методів, моделей, розвитку методу TLC, а також підходу до їх комплексного використання.

Отримано наступні основні результати:

1. На основі аналізу розроблено підхід, де вперше, у формі комплексного рішення, сполучено засоби контролю показників функціональних і нефункціональних характеристик досліджуваних артефактів процесу проєктування ПАС. У якості названих артефактів опрацьовано, у тому числі, блок-схеми алгоритмів, UML-діаграми дій, станів, похідні формалізовані подання на основі виразних засобів числення послідовних процесів, що взаємодіють, Ч. Гоара, алгоритмічної мови PlusCal, формалізму TLA+, математичного апарату DEVS. У

якості допоміжних засобів створено і залучено засоби автоматизації процесів одержання похідних формалізованих подань і опрацювання результатів досліджень.

2. Розроблено модель подання ПАС у вигляді формальної специфікації, де вперше застосовано правило композиції Ч. Гоара у якості засобу скорочення кількості рядків коду специфікації. Названу модель залучено у якості засобу уніфікації формальних специфікацій як форм подання ПАС. Це дозволило автоматизувати процес постачання формальних специфікацій для здійснення на їх основі формальної верифікації методом перевірки на моделі TLC, а також на основі розробленого розвитку цього методу, за показником несуперечності ПАС.

Розроблену модель побудовано із залученням виразних засобів числення послідовних процесів, що взаємодіють, Ч. Гоара, алгоритмічної мови PlusCal і формалізму TLA+ темпоральної логіки дій TLA Л. Лемпорта.

Отримані результати проведених досліджень розробленої моделі дали підстави стверджувати, що застосування правила композиції Ч. Гоара дозволило скоротити кількість рядків коду результуючих формальних специфікацій на частку від близько 18 % – до близько 33 % (для найліпшого випадку – послідовний сценарій: від 2 – до 256 змінних станів); від близько 22 % – до близько 0 % (для найгіршого випадку – із поданням паралелізму згідно моделі чергування: від 4 – до 16 змінних станів). Зазначені випадки опрацьовано як граничні. У якості додаткового показника просторових витрат на подання ПАС у формалізованому вигляді розглянуто також розмір відповідного файлу-артефакту. Для граничного випадку із поданням паралелізму згідно моделі чергування, для 8 змінних станів, він склав близько 7 КБ, а для 16 змінних – вже близько 210 МБ. При цьому для випадку 16 змінних було зафіксовано факт нестачі наявної оперативної пам’яті обчислювальної системи при проведенні формальної верифікації.

3. Розроблено метод синтезу формальних специфікацій на основі графічних подань ПАС, де вперше комплексно охоплено і аналітичний рівень опрацювання результуючих формалізованих подань, і рівень реалізації. Метод побудовано на основі розробленої моделі подання ПАС. Такий крок, на відміну від альтернативних рішень, забезпечує прозорий механізм опрацювання складових результуючої формальної специфікації та зв’язків між ними на рівнях аналітичному і програмної реалізації. Для цього було залучено математичний апарат темпоральної логіки дій TLA, відповідний формалізм TLA+ та алгоритмічну мову PlusCal. Застосування виразних засобів PlusCal опрацьовано як допоміжний крок, що полягає у попередньому формуванні архітектурної складової результуючої формальної специфікації. Останню, у свою чергу, сформовано на основі виразних засобів TLA+, що уможливило проведення формальної верифікації методом перевірки на моделі TLC або на основі розробленого розвитку даного методу в автоматизованому режимі.

4. Вперше розроблено метод контролю відповідності результуючих формальних специфікацій, одержуваних на основі зазначеного вище запропонованого методу синтезу, первинним артефактам – графічним поданням ПАС. Метод є допоміжним засобом, застосовуваним на заключному кроці методу синтезу. Метод контролю базується на співставленні показників архітектурних

складових системи переходів для подань ПАС на рівнях аналітичному і реалізації. Такими показниками є глибина обходу простору станів системи переходів, що будується у процесі формальної верифікації, а також загальна кількість станів системи переходів. Отримані результати застосування розробленого методу контролю підтвердили відповідність результуючих формальних специфікацій первинним артефактам за названими показниками. Окрім зазначеного, розроблений метод є також засобом контролю достовірності результатів формальної верифікації методом перевірки на моделі у частині допустимості поширення зроблених висновків за результатами також і на первинні артефакти.

5. Набув подальшого розвитку поширений метод формальної верифікації TLC. Розвиток проведено у частині підвищення ефективності роботи методу за ітеративного підходу до організації процесу формальної верифікації специфікацій – за показником зниження супутніх результуючих часових витрат: на першій ітерації при обході простору станів системи переходів застосовано метод обходу у ширину теорії графів, що дало змогу визначити глибину обходу; на наступних ітераціях – метод обходу у глибину, що дозволило скоротити результуючі часові витрати, супутні ітеративному процесу формальної верифікації специфікацій.

Експериментальні дослідження базового методу TLC проведено для граничних синтетичних випадків, а також по відношенню до предметно-орієнтованих артефактів процесу проєктування ПАС систем критичного призначення: за напрямами оцінювання обчислювальних і просторових витрат, супутніх залученню альтернативних реалізацій базового методу – на основі методів обходу у ширину і у глибину теорії графів.

Дослідження одержуваного корисного ефекту від проведеного розвитку базового методу TLC здійснено у залежності від кількості виконуваних ітерацій для граничних значень кількості змінних станів стосовно предметно-орієнтованого сценарію аерокосмічної галузі. Зазначений ефект склав від близько 15 % – до близько 110 %.

Також проведено оцінювання одержуваного корисного ефекту від введення мультипоточності до складу програмних реалізацій базового методу TLC. Він склав від близько 26 % – до близько 123 %, у залежності від кількості залучених програмних потоків, кількості змінних станів і застосованого методу обходу простору станів системи переходів.

6. Розроблено модель – стратифіковану архітектуру, де ієрархічний підхід вперше застосовано у якості засобу досягнення архітектурної відповідності результуючої складеної комп’ютерної моделі вихідній формальній специфікації, несуперечність якої вже було підтверджено шляхом формальної верифікації методом перевірки на моделі. Ієрархічний підхід реалізовано на основі засобів математичного апарату DEVS: шляхом оперування конструкціями «атомарної» і «складеної» моделей DEVS. Дослідження розробленої моделі проведено шляхом опрацювання у якості показника нефункціональних характеристик часових витрат, супутніх реалізації кроків ПАС. Адекватність розробленої моделі підтверджено шляхом проведення дискретно-подійного імітаційного моделювання, і

співставлення отриманих результатів, у тому числі – результуючих агрегованих значень показника, із результатами тестування.

7. Розроблено метод контролю значення досліджуваного показника нефункціональних характеристик, де вперше враховано можливість оперувати і оціночними, і фактичними значеннями складових названого показника, – вже на етапі проєктування ПАС. Метод реалізовано у відповідності до зазначеної вище моделі: шляхом проведення дискретно-подійного імітаційного моделювання на основі засобів математичного апарату DEVS. Накопичення значення показника у процесі моделювання реалізовано на основі механізму обміну повідомленнями між компонентами результуючої складеної ієрархічної комп'ютерної моделі. У якості досліджуваного показника нефункціональних характеристик опрацьовано часові витрати, супутні реалізації кроків ПАС. Отримані результуючі накопичені значення показника співставлено із відповідними значеннями, одержуваними шляхом тестування. Встановлено, що оперування оціночними значеннями складових показника, замість фактичних значень, у залежності від специфіки обчислювальних дій, виконуваних згідно ПАС, дозволяє істотно скоротити часові витрати, супутні реалізації процесу контролю значення показника.

8. Практичне значення отриманих результатів проведених дисертаційних досліджень було підтверджено на основі наступних документів: акту впровадження, листів підтвердження впровадження, листів підтримки від організацій та установ.

## СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

***Наукові праці, у яких опубліковано основні наукові результати.***

***Монографії:***

1. Shkarupylo V.V., Timenko A.V. On the interoperability and consistency aspects with respect to the Internet of Things domain. Engineering sciences: development prospects in countries of Europe at the beginning of the third millennium: Collective monograph. Vol. 2. Riga: Izdevnieciba "Baltija Publishing", 2018. P. 466–485. ISBN 978-9934-571-63-3 (**розділ колективної монографії**)

2. Блінов І.В., Парус Є.В., Шкарупило В.В. Структура та моделі інформаційної взаємодії учасників ринку електричної енергії: монографія. Вінниця: ГО «Європейська наукова платформа», 2021. 114 с. ISBN 978-617-8037-31-4. DOI: https://doi.org/10.36074/stmivyree-monograph.2021 (**колективна монографія**)

3. Шкарупило В.В., Блінов І.В. Сценарії, методи та засоби формальної верифікації артефактів процесу проєктування систем критичного призначення: монографія. Вінниця : ГО «Європейська наукова платформа», 2021. 104 с. ISBN 978-617-8037-55-0. DOI: https://doi.org/10.36074/smtzfvappskp-monograph.2021 (**колективна монографія**)

4. Shkarupylo V.V., Blinov I.V., Chemeris A.A., Dusheba V.V., Alsayaydeh J.A.J. On Applicability of Model Checking Technique in Power Systems and Electric Power Industry. In: Zaporozhets A. (Eds.) Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control, 2022, Vol. 399. Springer, Cham. ISBN 978-3-030-87675-3. DOI: https://doi.org/10.1007/978-3-030-87675-3_1 (**Scopus:**

https://www.scopus.com/record/display.uri?eid=2-s2.0-85120868312&origin=resultslist&sort=plf-f ; **розділ колективної монографії**)

5. Борукаєв З.Х., Блінов І.В., Остапченко К.Б., Чемерис О.А., Шкарупило В.В. Моделі та засоби автоматизації систем організаційного управління енергоринком: монографія / за заг. ред. З.Х. Борукаєва. Вінниця: ГО «Європейська наукова платформа», 2022. 122 с. ISBN 978-617-8037-82-6. DOI: https://doi.org/10.36074/mtzasoye-monograph.2022 (**колективна монографія**)

6. Шкарупило В., Блінов І., Кучанський В., Давидюк А., Дімітрієва Д. Методи і засоби контролю артефактів процесу проєктування програмно-алгоритмічної складової систем критичного призначення: монографія / за заг. ред. В.В. Шкарупила. Publishing House «European Scientific Platform», 2023. 120 с. ISBN 978-617-8126-22-3. DOI: https://doi.org/10.36074/mzkapppasskp-monograph.2023 (**колективна монографія**)

***Статті у фахових періодичних виданнях:***

7. Shkarupylo V.V., Tomičić I., Kasian K.M. The investigation of TLC model checker properties. *Journal of Information and Organizational Sciences*, 2016, Vol. 40, No. 1. P. 145–152. ISSN: 1846-9418 (Online), 1846-3312 (Print). DOI: https://doi.org/10.31341/jios.40.1.7 (**Web of Science Core Collection**: https://www.webofscience.com/wos/woscc/full-record/WOS:000409240900008 ; **Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-84975057117&origin=resultslist ; **Q4**)

8. Shkarupylo V., Skrupsky S., Oliinyk A., Kolpakova T. Development of stratified approach to software defined networks simulation. *Eastern-European Journal of Enterprise Technologies*. Information and controlling systems, 2017, Vol. 5, No. 9 (89). P. 67–73. ISSN: 1729-3774 (Print), 1729-4061 (Online). DOI: https://doi.org/10.15587/1729-4061.2017.110142 (**Scopus, Q3**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85031750626&origin=resultslist ; **фахове видання категорії А**)

9. Alsayaydeh J.A.J., Shkarupylo V., Hamid M. S. B., Skrupsky S., Oliinyk A. Stratified model of the Internet of Things infrastructure. *Journal of Engineering and Applied Sciences*, 2018, Vol. 13, No. 20. P. 8634–8638. ISSN: 1816-949x (Print), 1818-7803 (Online). DOI: https://docsdrive.com/pdfs/medwelljournals/jeasci/2018/8634-8638.pdf (**Scopus, Q3**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85056326734&origin=resultslist)

10. Timenko A.V., Shkarupylo V.V., Oliinyk A.O., Hrushko S.S. Formal Model for Checking the Interoperability Between the Components of the IoT system. *Problemele Energeticii Regionale*, 2019. Vol. 40, No. 1-1. P. 69–78. ISSN: 1857-0070. DOI: https://zenodo.org/record/3239196 (**Web of Science Core Collection:** https://www.webofscience.com/wos/woscc/full-record/WOS:000472596400007)

11. Shkarupylo V., Alsayaydeh J.A.J., Tomičić I., Chemeris A., Dusheba V. A technique for checking the adequacy of formal model. *ARPN Journal of Engineering and Applied Sciences*, August 2021, Vol. 16, No. 16. P. 1707–1719. ISSN: 1819-6608. URL: http://www.arpnjournals.org/jeas/research_papers/rp_2021/jeas_0821_8670.pdf (**Scopus,**

**Q3**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85118181893&origin=resultslist)

12. Polska O.V., Kudermetov R.K., Shkarupylo V.V. An approach web service selection by quality criteria based on sensitivity analysis of MCDM methods. *Radio Electronics, Computer Science, Control*, 2021. No. 2. P. 133–143. ISSN: 1607-3274 (Online), 2313-688X (Print). DOI: https://doi.org/10.15588/1607-3274-2021-2-14 (**Web of Science Core Collection:** https://www.webofscience.com/wos/woscc/full-record/WOS:000673377700014**; фахове видання категорії А**)

13. Shkarupylo V., Blinov I., Dusheba V., Alsayaydeh J. A. J. Case Driven TLC Model Checker Analysis in Energy Scenario. *CEUR Workshop Proceedings*, 2023. Vol. 3392. P. 65–75. ISSN: 1613-0073. DOI: https://doi.org/10.32782/cmis/3392-6 (**Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85160296577&origin=resultslist&sort=plf-f)

14. Шкарупило В.В., Кудерметов Р.К., Польська О.В. DEVS-орієнтована методика валідації композитних веб-сервісів. *Радіоелектроніка, інформатика, управління*, 2015, № 4. С. 79–86. ISSN: 1607-3274 (Print), 2313-688X (Online). DOI: 10.15588/1607-3274-2015-4-12 URL: http://ric.zntu.edu.ua/article/view/60404 (**фахове видання категорії А**)

15. Polska O.V., Kudermetov R.K., Shkarupylo.V.V. Discovery and selection of web-services. *Electrotechnic and computer systems*, 2015. No. 19(95). P. 169–173. ISSN: 2221-3937 (Print), 2221-3805 (Online). URL: http://nbuv.gov.ua/UJRN/etks_2015_19_39 (**фахове видання**)

16. Kudermetov R., Polska O., Shkarupylo V., Shcherbak N. Quality of services in scientific workflows. *Electrotechnic and Computer Systems*, 2018. Vol. 28, No. 104. P. 170–177. ISSN: 2221-3805 (Print), 2221-3937 (Online). DOI: 10.15276/eltecs.28.104.2018.20 URL: https://eltecs.op.edu.ua/index.php/journal/article/view/155/42 (**фахове видання**)

17. Shkarupylo V.V., Tomičić I., Kasian K.M., Alsayaydeh J.A.J. An Approach to increase the Effectiveness of TLC Verification with Respect to the Concurrent Structure of TLA+ Specification. *International Journal of Software Engineering and Computer Systems*, 2018. Vol. 4, No. 1. P. 48–60. ISSN: 2289-8522. DOI: https://doi.org/10.15282/ijsecs.4.1.2018.4.0037 (**фахове видання**)

18. Shkarupylo V.V., Kudermetov R.K., Polska O.V. On the approaches to cyber-physical systems simulation. *Advances in Cyber-Physical Systems (ACPS)*, 2018, Vol. 3, No. 1. P. 51–54. ISSN: 2524-0382 (Print), 2707-0069 (Online). DOI: https://doi.org/10.23939/acps2018.01.051 (**фахове видання**)

19. Шкарупило В.В., Євдокимов В.Ф., Душеба В.В. Застосування формальних методів для перевірки систем критичного призначення. *Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки»*, 2019, Том 30 (69), Ч. 1, № 6. С. 188–193. ISSN: 2663-5941 (Print), 2663-595X (Online). DOI https://doi.org/10.32838/2663-5941/2019.6-1/34 (**фахове видання**)

20. Тіменко А.В., Шкарупило В.В., Скрупський С.Ю., Смолій В.В. Дослідження шляхів підвищення пропускної спроможності підсистеми пам’яті сучасної обчислювальної системи. *Вчені записки Таврійського національного*

*університету імені В.І.Вернадського, серія «Технічні науки»*, 2020, Том 31 (70), Ч. 1, № 2. С. 208–212. ISSN: 2663-5941 (Print), 2663-595X (Online). DOI: https://doi.org/10.32838/2663-5941/2020.2-1/32 (**фахове видання**)

21. Шкарупило В.В., Чемерис О.А., Душеба В.В., Кудерметов Р.К., Польська О.В. Метод синтезу формальних специфікацій на основі трійок Хоара. *Наукові праці ДонНТУ, Серія "Інформатика, кібернетика та обчислювальна техніка"*, 2020, № 1(30). С. 49–57. ISSN: 1996-1588. DOI: 10.31474/1996-1588-2020-1-30-49-57 URL: https://iktv.donntu.edu.ua/1-30-2020/ (**фахове видання**)

22. Шкарупило В.В., Чемерис О.А., Душеба В.В. Оцінювання просторової складності задачі формальної верифікації, вирішуваної методом перевірки на моделі. *Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки»*, 2020, Том 31 (70), № 5. С. 147–151. ISSN: 2663-5941 (Print), 2663-595X (Online). DOI: https://doi.org/10.32838/2663-5941/2020.5/24 (**фахове видання**)

23. Шкарупило В.В., Чемерис О.А., Душеба В.В., Кудерметов Р.К. Дослідження мультипоточної реалізації методу перевірки на моделі для темпоральної логіки дій. *Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки»*, 2020, Том 31 (70), № 6, Ч. 1. С. 173–177. ISSN: 2663-5941 (Print), 2663-595X (Online). DOI: https://doi.org/10.32838/TNU-2663-5941/2020.6-1/28 (**фахове видання**)

24. Polska O.V., Kudermetov R.K., Shkarupylo V.V. The approach for QoS based web service selection with user's preferences. *Наукові праці Донецького національного технічного університету, серія: «Проблеми моделювання та автоматизації проектування»*, 2020. №2 (16). С. 19–27. ISSN: 2074-7888. DOI: 10.31474/2074-7888-2020-2-19-27 URL: http://pmap.donntu.edu.ua/sites/upload/articles/pmap_2020_19-27.pdf (**фахове видання**)

25. Polska O.V., Kudermetov R.K., Zolotukhina O.A., Shkarupylo V.V. A UML profile for quality-based web service selection using logic scoring of preference method. *Telecommunication and information technologies*, 2021. No. 1 (2021). P. 65–78. ISSN: 2412-4338. DOI: https://doi.org/10.31673/2412-4338.2021.016578 (**фахове видання**)

26. Шкарупило В.В., Чемерис О.А., Душеба В.В., Кудерметов Р.К., Польська О.В. Модельно-орієнтований підхід до контролю показників нефункціональних характеристик під час проєктування. *Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки»*, 2021, Том 32 (71), Ч. 1, № 1. С. 166–171. ISSN: 2663-5941 (Print), 2663-595X (Online). DOI: https://doi.org/10.32838/2663-5941/2021.1-1/27 (**фахове видання**)

27. Шкарупило В.В., Душеба В.В., Скрупський С.Ю., Блінов І.В. Стратифікована модель подання нефункціональних характеристик системи критичного призначення при проєктуванні. *Електронне моделювання*, 2022. Т. 44, № 2. С. 90–106. ISSN: 0204-3572. DOI: https://doi.org/10.15407/emodel.44.02.090 (**фахове видання**)

28. Куликовська Н.А., Руденко В.В., Тіменко А.В., Шкарупило В.В. Дослідження часу збирання додатків, побудованих на основі сучасних стратегій розроблення. *Вчені записки Таврійського національного університету імені*

*В.І.Вернадського, серія «Технічні науки»*, 2023. Том 34 (73), № 4. С. 65–70. ISSN: 2663-5941 (Print), 2663-595X (Online). DOI: https://doi.org/10.32782/2663-5941/2023.4/11 (**фахове видання**)

***Праці апробаційного характеру:***

29. Shkarupylo V. A Technique of DEVS-Driven Validation. *Proc. XIIIth Int. Conf. on Modern Problems of Radio Engineering, Telecommunications, and Computer Science, TCSET'2016* (Lviv-Slavske, Ukraine, February 23–26, 2016). P. 495–497. DOI: https://doi.org/10.1109/TCSET.2016.7452097 (**Web of Science Core Collection**: https://www.webofscience.com/wos/woscc/full-record/WOS:000381804300127 ; **Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-84969263650&origin=resultslist)

30. Shkarupylo V. A Simulation-driven Approach for Composite Web Services Validation. *Proc. 27th Int. Central European Conference on Information and Intelligent Systems, CECIIS 2016* (Varazdin, Croatia, September 21–23, 2016). P. 227–231. URL: http://archive.ceciis.foi.hr/app/public/conferences/1/ceciis2016/papers/QoS-1.pdf (**Web of Science Core Collection**: https://www.webofscience.com/wos/woscc/full-record/WOS:000595003500030)

31. Shkarupylo V., Polska O. The Approach to SDN Network Topology Verification on a Basis of Temporal Logic of Actions. *Proc. 14th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET'2018* (Lviv-Slavske, Ukraine, February 20–24, 2018). P. 183–186. DOI: https://doi.org/10.1109/TCSET.2018.8336182 (**Web of Science Core Collection**: https://www.webofscience.com/wos/woscc/full-record/WOS:000465121700033 ; **Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85047524592&origin=resultslist)

32. Shkarupylo V., Kudermetov R., Golub T., Polska O., Tiahunova M. Towards Model Checking of the Internet of Things Solutions Interoperability. *Problems of Infocommunications. Science and Technology: proc. 2018 IEEE International Scientific and Practical Conference, PIC S&T-2018* (Kharkiv, Ukraine, October 9–12, 2018). P. 465–468. DOI: https://doi.org/10.1109/INFOCOMMST.2018.8632037 (**Web of Science Core Collection**: https://www.webofscience.com/wos/woscc/full-record/WOS:000458659100087 ; **Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85062879597&origin=resultslist)

33. Shkarupylo V., Kudermetov R., Timenko A., Polska O. On the Aspects of IoT Protocols Specification and Verification. *Problems of Infocommunications. Science and Technology: 2019 International Scientific-Practical Conference, PIC S&T'2019* (Kyiv, Ukraine, October 8–11, 2019). P. 93–96. DOI: https://doi.org/10.1109/PICST47496.2019.9061406 (**Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083637232&origin=resultslist)

34. Shkarupylo V., Chemerys O., Dusheba V., Kudermetov R., Oliinyk A. On Hoare triples applicability to dependable system specification synthesis. *Dependable Systems, Services and Technologies, DESSERT'2020: The 11th International Conference* (Kyiv, Ukraine, May 14–18, 2020). Kyiv, 2020. P. 371–375. DOI: https://doi.org/10.1109/DESSERT50317.2020.9125074 (**Web of Science Core Collection**: https://www.webofscience.com/wos/woscc/full-

record/WOS:000619228000064 ; **Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85087906543&origin=resultslist)

35. Shkarupylo V., Blinov I., Chemeris A., Dusheba V., Alsayaydeh J., Oliinyk A. Iterative Approach to TLC Model Checker Application. *Proc. 2021 IEEE KhPI Week on Advanced Technology* (Kharkiv, Ukraine, September 13–17, 2021). P. 283–287. DOI: https://doi.org/10.1109/KhPIWeek53812.2021.9569981 (**Scopus**: https://www.scopus.com/record/display.uri?eid=2-s2.0-85118943601&origin=resultslist)

36. Шкарупило В.В. Концепція формальної верифікації UML-діаграм методами Model Checking. *Моделювання: XXXIV науково-технічна конференція*, 13–14 січня 2015 р.: тези доп. К.: ІПМЕ ім. Г. Є. Пухова НАН України, 2015. С. 13.

37. Шкарупило В.В. Особливості використання методу формальної верифікації TLC. *Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*: тези доп., м. Київ, 12 січня 2016 р. С. 31. DOI: http://dx.doi.org/10.5281/zenodo.2545399

38. Shkarupylo V.V. An in-depth look at TLC model checker. *Тиждень науки-2016*: зб. тез доп. науково-практ. конф., 18–22 квітня 2016 р. Запоріжжя: ЗНТУ, 2016. С. 523–524. URL: https://zp.edu.ua/uploads/conference/2016/TN2016_T1.pdf (дата звернення: 06.08.2023)

39. Shkarupylo V.V., Tomičić I., Arapin D.V. The concurrency representation in TLA+ specification. *Proc. VIIIth Int. scientific-practical conf. on Modern problems and achievements of radio engineering (electronics), telecommunications and information technology* (Zaporizhzhya, Ukraine, September 21–23, 2016). P. 118–119. URL: http://rtt.zntu.edu.ua/data/Tezy_ZNTU_2016.pdf (дата звернення: 06.08.2023)

40. Shkarupylo V. TLC model checking and the concurrency in specification. *Proc. Tenth International Scientific-Practical Conference "INTERNET-EDUCATION-SCIENCE-2016", IES-2016* (Vinnytsia, Ukraine, October 11–14, 2016). P. 89–91. URL: http://ir.lib.vntu.edu.ua/handle/123456789/13390 (дата звернення: 06.08.2023)

41. Shkarupylo V.V. An Approach to DEVS-driven Simulation of Software-defined Networks. *Тиждень науки-2017*: науково-практ. конф., 18–21 квітня 2017 р.: тези доп. Запоріжжя: ЗНТУ, 2017. С. 652. URL: https://zp.edu.ua/uploads/dept_s&r/2017/conf/1/TN2017.pdf (дата звернення: 06.08.2023)

42. Shkarupylo V.V., Timenko A.V. An approach to the Internet of things simulation on a basis of discrete event system specification. *Proc. Int. research and practice conference on Modern methods, innovations, and experience of practical application in the field of technical sciences* (Radom, Republic of Poland, Dec. 27–28, 2017). P. 32–34.

43. Shkarupylo V.V. On the applicability of model checking techniques in the Internet of Things domain. *Тиждень науки-2018*: науково-практ. конф., 16–20 квітня 2018 р.: тези доп. Запоріжжя: ЗНТУ, 2018. С. 967–968. URL: https://zp.edu.ua/uploads/dept_s&r/2018/conf/1/TN2018.pdf (дата звернення: 06.08.2023)

44. Shkarupylo V.V., Timenko A.V. On the expediency of stratification to foster the reconfigurability of formal specifications. *Тенденції та вектор розвитку науки в*

*сучасному світі*: *VI Міжнародна науково-практична інтернет-конференція*: тези доповідей, Дніпро, 30 квітня 2018 р. Ч. 1. Дніпро: НБК, 2018. С. 46–49. URL: https://ispic.ngo-seb.com/assets/files/6_conf_30.04.18_P.1.pdf (дата звернення: 06.08.2023)

45. Shkarupylo V., Kudermetov R. On the aspects of cyber-physical systems modeling with UPPAAL. *Simulation-2018: 6th Int. conference*, September 12–14, 2018: theses. Kyiv: Pukhov Institute for Modelling in Energy Engineering, 2018. P. 267–269. URL: https://ipme.kiev.ua/en/conference/simulation-2018/ (дата звернення: 06.08.2023)

46. Shkarupylo V., Polska O., Shcherbak N. On the classification of model checking methods for the Internet of Things. *Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: IX Міжнародна науково-практична конференція*, 3–5 жовтня 2018 р.: тези доп. Запоріжжя: ЗНТУ, 2018. С. 77–78.

47. Шкарупило В. В., Кудерметов Р. К., Польська О. В., Тіменко А. В. Щодо доцільності перевірки протоколів взаємодії компонентів систем інтернету речей. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2019*: матеріали VII Міжнародної науково-практичної конференції, 15–16 травня 2019 р. Київ: НУБіП України, 2019. С. 63–65. URL: https://lib.lntu.edu.ua/sites/default/files/2021-03/Київ_Конференція_НУБІП_2019_UA.pdf (дата звернення: 06.08.2023)

48. Шкарупило В.В., Євдокимов В.Ф., Душеба В.В. Аспекти застосування методів перевірки на моделі при проектуванні систем критичного призначення. *Безпека енергетики в епоху цифрової трансформації: науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України* : програма та матеріали, 20 грудня 2019 р. Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2019. С. 94–96. URL: https://ipme.kiev.ua/wp-content/uploads/2019/12/Програма-КБЕЕЦ-2019.pdf (дата звернення: 06.08.2023)

49. Шкарупило В.В. Про застосування правила композиції при синтезі формальних специфікацій. *Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, 15 травня 2020 р. Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2020. С. 21–22. URL: https://zenodo.org/record/3813710 (дата звернення: 06.08.2023)

50. Шкарупило В.В. Дослідження методу перевірки на моделі TLC. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2020 : VIII Міжнародна науково-практична Інтернет-конференція* (м. Київ, Україна, 14–15 травня, 2020). 2020. Київ: НУБіП України. С. 84–86. URL: http://econference.nubip.edu.ua/index.php/grpi/grpi20/paper/view/2306/317 (дата звернення: 06.08.2023)

51. Шкарупило В.В., Скрупський С.Ю. Комбінований підхід до застосування методу перевірки на моделі TLC. *Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: X Ювілейна міжнародна науково-практична конференція, присвячена 120-річчю з дня заснування Національного університету «Запорізька політехніка»* (Запоріжжя,

Україна, 7–9 жовтня, 2020). Запоріжжя: НУ «ЗП». С. 95–97. URL: http://rtt.zntu.edu.ua/data/Tezy_NUZP_2020.pdf (дата звернення: 06.08.2023)

52. Шкарупило В.В., Кудерметов Р.К., Польська О.В. Дослідження просторової складності алгоритмів в основі методу верифікації TLC. *Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: X Ювілейна міжнародна науково-практична конференція, присвячена 120-річчю з дня заснування Національного університету «Запорізька політехніка»* (Запоріжжя, Україна, 7–9 жовтня, 2020). Запоріжжя: НУ «ЗП». С. 93–95. URL: http://rtt.zntu.edu.ua/data/Tezy_NUZP_2020.pdf (дата звернення: 06.08.2023)

53. Шкарупило В.В., Чемерис О.А., Душеба В.В. Дослідження впливу мультипоточності на швидкодію методу перевірки на моделі. *Безпека енергетики в епоху цифрової трансформації*: Друга науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (Київ, Україна, 28–29 грудня, 2020). Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2020. С. 75–77. URL: https://ipme.kiev.ua/wp-content/uploads/2021/01/Програма-та-матеріали-КБЕЕЦ-2020.pdf (дата звернення: 06.08.2023)

54. Шкарупило В.В., Блінов І.В. Щодо застосування методу перевірки на моделі при проєктуванні інформаційно-технологічних систем суб'єктів ринку електроенергії. *XXXIX науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, присвячена 40-річчю Інституту, Дню науки в Україні та з нагоди відзначення 30-ї річниці незалежності України* (м. Київ, Україна, 12 травня, 2021). Київ: ІПМЕ ім. Г.Є. Пухова НАН України. С. 7–9. URL: https://drive.google.com/file/d/1QOydMJU3nHOjXZ92vcLF2zAclu8w1RcG/view?usp=share_link (дата звернення: 06.08.2023)

55. Шкарупило В.В., Блінов І.В. Модельно-орієнтований підхід до формалізації нефункціональних характеристик систем критичного призначення, зокрема у природокористуванні. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні 2021*: IX Міжнародна науково-практична Інтернет-конференція (м. Київ, Україна, 13–14 травня, 2021). Київ: НУБіП України. С. 55–57. URL: https://drive.google.com/file/d/1IPmtWaLu85W3c9CsrYXYqx2_iFYIq4q2/view?usp=sharing (дата звернення: 06.08.2023)

56. Шкарупило В.В., Блінов І.В., Душеба В.В., Тіменко А.В. Дуальний підхід до формалізації функціональних характеристик систем критичного призначення. *European scientific discussions : 9th International scientific and practical conference. Potere della ragione Editore* (м. Рим, Італія, 18–20 липня, 2021 р.). С. 143–149. URL: https://sci-conf.com.ua/wp-content/uploads/2021/07/EUROPEAN-SCIENTIFIC-DISCUSSIONS-18-20.07.2021.pdf (дата звернення: 06.08.2023)

57. Шкарупило В.В., Блінов І.В., Душеба В.В., Кучанський В.В. Щодо мультипоточного застосування формального методу перевірки на моделі TLC. *Topical issues of modern science, society and education. Proceedings of the 2nd International scientific and practical conference. SPC "Sci-conf.com.ua"*. Kharkiv,

Ukraine. 2021. P. 231–236. URL: https://sci-conf.com.ua/wp-content/uploads/2021/09/TOPICAL-ISSUES-OF-MODERN-SCIENCE-SOCIETY-AND-EDUCATION-5-7.09.21.pdf (дата звернення: 06.08.2023)

58. Дімітрієва Д.О., Шкарупило В.В. Огляд інструментів використання формальних методів та засобів при проєктуванні систем критичного призначення. *ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ: ЕКОНОМІКА, ТЕХНІКА, ОСВІТА '2021*: Збірник матеріалів XI Міжнародної науково-практичної конференції молодих вчених, 11–12 листопада 2021 року, НУБіП України, Київ. С. 164–165. URL: https://drive.google.com/file/d/10iRiRUwpXqTY510LzL1j0BeDt-Kpx4Ab/view?usp=sharing (дата звернення: 06.08.2023)

59. Шкарупило В.В., Душеба В.В. Підхід до синтезу формалізованих подань нефункціональних характеристик на етапі проєктування. *Безпека енергетики в епоху цифрової трансформації* : III науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 22 грудня 2021 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2021. С. 128–130. URL: https://ipme.kiev.ua/wp-content/uploads/2021/12/Матеріали-КБЕЕЦ-2021-1.pdf (дата звернення: 06.08.2023)

60. Шкарупило В.В., Душеба В.В. Спадковість артефактів у контексті багатовимірної верифікації. *Тиждень науки-2022*: науково-практ. конф., 18–22 квітня 2022 р.: тези доп. Запоріжжя: НУ "Запорізька політехніка", 2022. С. 789–791. URL: https://zp.edu.ua/uploads/dept_s&r/2022/conf/4.1/TN_2022.pdf (дата звернення: 06.08.2023)

61. Шкарупило В.В., Душеба В.В. Модельно-орієнтований підхід до синтезу формалізованих подань. *XL Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, 11 травня 2022 р.: тези доп. Київ: ІПМЕ ім. Г.Є. Пухова НАН України, 2022. С. 20–22. URL: https://bit.ly/3cPGyFk (дата звернення: 06.08.2023)

62. Дімітрієва Д.О., Шкарупило В.В. Огляд нефункціональних характеристик систем критичного призначення. *XL Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, 11 травня 2022 р.: тези доп. Київ: ІПМЕ ім. Г.Є. Пухова НАН України, 2022. С. 78–79. URL: https://bit.ly/3cPGyFk (дата звернення: 06.08.2023)

63. Шкарупило В.В., Тіменко А.В. Складові методу контролю показників нефункціональних характеристик розроблюваної комп'ютерної системи при проєктуванні. *XLIX Міжнародна науково-практична інтернет-конференція «Проблеми та перспективи розвитку сучасної науки в країнах Європи та Азії»*, 31 серпня 2022 р.: тези доп., Переяслав, 2022. С. 69–71.

64. Шкарупило В.В., Душеба В.В. Щодо аспектів контролю несуперечності програмно-алгоритмічної складової систем критичного призначення. *Продовольча та екологічна безпека в умовах війни та повоєнної відбудови, присвячена 125-річчю заснування Національного університету біоресурсів і природокористування України: виклики для України та світу*: мат. Міжн. наук.-практ. конф., секція 5: Інженерія, енергетика та інформаційні технології в умовах війни та післявоєнній

відбудові країни (м. Київ, 25 трав. 2023 р.): тези доп. Київ: НУБіП України, 2023. С. 170–172. URL: https://nubip.edu.ua/sites/default/files/u381/sekciya_5.pdf (дата звернення: 06.08.2023)

65. Шкарупило В.В., Блінов І.В., Душеба В.В. Дослідження методу верифікації TLC при вирішенні задач енергетики. *XLI Науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* (м. Київ, Україна, 17 травня, 2023 р.). С. 21–22. URL: https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf (дата звернення: 06.08.2023)

66. Шкарупило В.В., Душеба В.В., Тіменко А.В., Казакова Н.О. Аспекти досягнення функційної безпечності при розробленні систем критичного призначення. *Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук*: ІІІ Всеукраїнської науково-практичної конференції пам'яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського (м. Київ, Україна, 21 червня 2023 р.): тези доп. Київ: УДУ ім. Михайла Драгоманова, 2023. С. 394–395. URL: https://drive.google.com/file/d/1nS1d9cf9EUNUZDnY0ZWLkQTaBlb0xoIN/view (дата звернення: 06.08.2023)

67. Шкарупило В.В., Душеба В.В., Тіменко А.В. Огляд рівнів забезпечення резилієнтності у галузі енергетики. *Survivability & Resilience – 2023*: collection of materials of the international scientific and practical conference, Kyiv, October 19, 2023, PIMEE of NAS of Ukraine. 2023. P. 33–34. URL: https://ipme.kiev.ua/konferencii/zhivuchist-ta-rezilyentnist-2023/ (дата звернення: 21.10.2023)

68. Шкарупило В.В., Душеба В.В. Аспекти введення мультипоточності до реалізації методу формальної верифікації TLC. *Безпека енергетики в епоху цифрової трансформації*: П'ята науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна, 22 листопада, 2023 р. Київ : ІПМЕ ім. Г.Є. Пухова НАН України. С. 121–122. URL: https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bevect-2023/ (дата звернення: 23.11.2023)

## АНОТАЦІЯ

**Шкарупило В.В. Методи і засоби контролю артефактів процесу проєктування програмно-алгоритмічного забезпечення систем критичного призначення.** – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, 2024.

Дисертаційну роботу присвячено вирішенню важливої науково-технічної проблеми забезпечення контролю артефактів процесу проєктування програмно-алгоритмічної складової систем критичного призначення стосовно несуперечності артефактів.

Для вирішення зазначеної проблеми за мету ставиться підвищення ефективності контролю артефактів у процесі розроблення програмно-алгоритмічної складової систем критичного призначення на етапі проєктування для забезпечення несуперечності артефактів та зниження супутніх витрат, за рахунок розроблення, дослідження і застосування формальних методів, розвитку методу, моделей, супутніх засобів, у тому числі засобів автоматизації.

Для досягнення сформульованої мети у роботі поставлено і вирішено відповідні задачі. Отримані результати викладено у межах шести розділів.

У першому розділі подано результати проведеного аналізу аспектів застосування формальних методів і засобів, зокрема методів перевірки на моделі, у процесі розроблення систем критичного призначення. За результатами проведеного аналізу обґрунтовано доцільність здійснення контролю показників функціональних і нефункціональних характеристик програмно-алгоритмічної складової названих систем вже на етапі проєктування процесу розроблення, оперуючи одержуваними при проєктуванні артефактами. Викладено сформульовані засади стосовно важливості розроблення комплексного підходу до здійснення зазначеного контролю.

Названий підхід викладено у межах другого розділу, де також представлено розроблену модель подання програмно-алгоритмічної складової комп'ютерної системи критичного призначення у формі формальної специфікації, призначену слугувати засобом уніфікації формалізованих подань для здійснення на основі останніх автоматизованого контролю несуперечності розроблюваної програмно-алгоритмічної складової методом перевірки на моделі. За рахунок залучення аксіом Ч. Гоара, застосування розробленої моделі дозволило скоротити кількість рядків коду результуючих формальних специфікацій. У якості виразних засобів використано, у тому числі, засоби структури Кріпке, числення послідовних процесів, що взаємодіють, алгоритмічну мову PlusCal, засоби TLA+ темпоральної логіки дій TLA Л. Лемпорта (Leslie Lamport).

У третьому розділі висвітлено розроблений метод синтезу формальних специфікацій на основі первинних артефактів-подань програмно-алгоритмічної складової. Викладено правила одержання результуючих артефактів. При цьому охоплено як аналітичний рівень опрацювання артефактів, так і рівень реалізації. Рівень реалізації розглянуто у якості чинника уможливлення автоматизації процесу формальної верифікації специфікацій. У межах розділу у якості допоміжного засобу також представлено розроблений метод контролю відповідності результуючих артефактів, одержуваних на основі розробленого методу синтезу, первинним артефактам. Представлений метод контролю призначений до застосування на заключному кроці методу синтезу.

У четвертому розділі викладено розроблений розвиток широко використовуваного формального методу перевірки на моделі TLC (TLA Checker). Проведений розвиток призначений до застосування за ітераційного підходу до організації процесу формальної верифікації специфікацій розроблюваної програмно-алгоритмічної складової. Розвиток полягає у поєднанні методів обходу у ширину і у глибину теорії графів при здійсненні обходів простору станів системи переходів, що будується і перевіряється у відповідності до формальної специфікації у процесі

формальної верифікації. Представлено отримані результати проведених досліджень базового методу і розробленого розвитку методу. Дослідження здійснено у розрізі оцінювання просторових і обчислювальних витрат, супутніх вирішенню задачі формальної верифікації: і для граничних синтетичних випадків, і для випадків предметно-орієнтованих критичних сценаріїв галузі енергетики, аерокосмічної галузі.

У п’ятому розділі викладено розроблену модель як ієрархічну архітектуру, що включає також і засоби подання нефункціональних характеристик при проєктуванні програмно-алгоритмічної складової систем критичного призначення. Модель опрацьовано і представлено у якості засобу контролю досліджуваного показника нефункціональних характеристик при проєктуванні програмно-алгоритмічної складової. Модель реалізовано на основі засобів математичного апарату DEVS Б. Зейглера (Bernard Phillip Zeigler). У якості досліджуваного показника нефункціональних характеристик опрацьовано часові витрати, супутні реалізації кроків програмно-алгоритмічної складової.

У шостому розділі представлено розроблений метод контролю значення досліджуваного показника нефункціональних характеристик розроблюваної програмно-алгоритмічної складової при проєктуванні. Метод реалізовано на основі висвітленої у п’ятому розділі запропонованої моделі. Метод полягає у проведенні дискретно-подійного імітаційного моделювання, і накопиченні при цьому результуючого значення досліджуваного показника. Метод дозволяє оперувати і оціночними, і фактичними значеннями складових показника.

Винесені на захист результати дисертаційної роботи пройшли відповідну апробацію. Прикладне значення отриманих результатів підтверджено документально – актом впровадження, листами підтвердження впровадження, листами підтримки. Копії зазначених документів, перелік публікацій, досліджені артефакти, фрагменти артефактів, а також допоміжні програмні реалізації як засоби автоматизації зведено у формі додатків.

**Ключові слова**: артефакт, верифікація, перевірка на моделі, програмно-алгоритмічна складова, система критичного призначення, специфікація.

## ABSTRACT

**Shkarupylo V.V. Methods and means for safety-critical systems’ software and algorithmic constituent design process artifacts control.** – As the manuscript.

Thesis for Doctor of Technical Sciences Degree in 05.13.05 specialty – Computer Systems and Components. – G.E. Pukhov Institute for Modelling in Energy Engineering of the National Academy of Sciences of Ukraine, Kyiv, 2024.

Dissertation is devoted to solving the following significant scientific and technical problem: provide the control of the artifacts taking place during the design of software and algorithmic constituent of the safety-critical system – from the viewpoint of artifacts consistency.

To solve specified problem, the goal of work is to increase the effectiveness of artifacts control during the process of safety critical systems’ software and algorithmic constituent engineering at the design stage. It has been done to provide the consistency of

the artifacts, and decrease the related expenses, by the development, study and application of formal methods, further development of method, models, related tools, including the automation tools.

To achieve the specified goal, corresponding tasks have been defined and solved. Obtained results have been described within six sections.

In the first section, the results of the analysis of formal methods and tools, model checking methods in particular, application during the safety critical systems engineering process have been provided. In accordance with obtained results, the expedience of conducting the control of both functional and non-functional properties of software and algorithmic constituent of named systems at the design stage of engineering process by operating with corresponding artifacts has been substantiated. Foundations regarding the significance of developing a comprehensive approach to named control implementation have been introduced.

In the second section, named approach has been described. Proposed model of software and algorithmic constituent of safety-critical system representation in the form of formal specification has also been introduced. Model is intended to be used as an instrument for formal specifications unification to conduct on the basis of the latter the automated consistency control of the software and algorithmic constituent with model checking method. By applying the Hoare rules, the application of the proposed model has made it possible to reduce the number of code lines in the resulting formal specifications. The following means of expression have been utilized: the instruments of Kripke structure, calculus of communicating sequential processes, PlusCal algorithmic language, TLA+ language of the temporal logic of actions TLA (by Leslie Lamport).

In the third section, the proposed method of formal specifications synthesis on the basis of the initial artifacts-representations of the software and algorithmic constituent has been described. The rules for obtaining the resulting artifacts have been outlined. Here, both the analytical and the implementation planes of artifacts processing have been covered. The implementation plane has been considered as a factor enabling the automation of the process of specifications formal verification. Within the section, as an auxiliary instrument, the proposed method for controlling the compliance of the resulting artifacts, obtained on the basis of the introduced specifications synthesis method, with the initial artifacts has also been presented. This method of control is intended to be applied at the final step of specifications synthesis method.

In the fourth section, the proposed further development of the widely applied formal TLC (TLA Checker) model checking method has been described. Named further development of the TLC method is intended to be used under the iterative approach to the implementation of the process of specifications of the software and algorithmic constituent formal verification. Proposed further development of the TLC method is about combining the methods of the breadth- and the depth-first search of the graph theory while traversing the state space of a transition system that is constructed and checked with respect to a formal specification during the process of formal verification. Obtained research results of the main method and of the introduced further development of method have been provided. Research has been carried out in terms of evaluation of spatial and computational expenses related with the formal verification task solving: both for

borderline synthetic cases and for the cases of subject-oriented critical scenarios from energy domain, as well as the scenarios from the aerospace domain.

In the fifth section, a proposed model as hierarchical architecture has been described. Model includes also the means for the non-functional properties representation at the design of the software and algorithmic constituent of the safety-critical systems. The model has been considered and represented as an instrument for checking the specified index of the non-functional properties at the design of software and algorithmic constituent. Model has been implemented on the basis of the means of the DEVS mathematical apparatus of Bernard Phillip Zeigler. As a studied index of the non-functional properties, the time costs, accompanying implementation of the steps of the program and algorithmic constituent, have been considered.

In the sixth section, a method for controlling the value of the studied index of the non-functional properties of the software and algorithmic constituent under development at design has been introduced. Method is implemented on the basis of the proposed model described in the fifth section. Method is grounded on conducting the discrete-event simulation, and accumulating during this process the resulting value of studied index. Method makes it possible to operate with both estimated and actual values of the constituents of studied index.

Obtained results of the dissertation have been proved. Practical value of named results has been proved documentary – with implementation act, letters of implementation confirmation, support letters. Copies of specified documents, as well as the list of publications, studied artifacts, artifact fragments, and auxiliary software implementations as automation facilitating means have been gathered in the form of appendixes.

**Keywords**: artifact, verification, model checking, software and algorithmic constituent, safety-critical system, specification.