ВІДГУК

офіційного опонента, доктора технічних наук,
професора, завідувачки кафедри інформаційних систем
Національного університету «Одеська політехніка»
Арсірій Олени Олександрівни
на дисертаційну роботу Москаленка В'ячеслава Васильовича
«**Методологічні основи та інформаційні технології створення резильєнтних систем інтелектуального аналізу даних**»
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.06 – інформаційні технології

1. Актуальність теми дисертаційного дослідження

Дисертаційна робота Москаленка В.В. присвячена вирішенню важливої та вкрай актуальної науково-прикладної проблеми підвищення *резильєнтності* систем інтелектуального аналізу даних (СІАД), які є складовими інформаційно-керуючих та кіберфізичних систем, що функціонують в агресивному середовищі за наявності жорстких обчислювальних, часових та енергетичних обмежень. Автор виходить за межі класичної відмовостійкості чи кібербезпеки тому що на практиці такі СІАД зазнають вплив широкого спектру деструктивних факторів: апаратні/програмні пошкодження пам'яті, що призводять до бітових інверсій (bit-flip) у параметрах нейромереж; змагальні атаки (adversarial attacks) на дані та моделі; дрейф даних (data drift) і концепцій (concept drift); появу новизни та даних поза навчальним розподілом (Out-Of-Distribution, OOD). Тому для СІАД в таких умовах важливою є не лише точність у штатному режимі, а й здатність протидіяти зазначеним деструктивним впливам, а також відновлювати функціональну ефективність за обмежень часу, пам'яті, енергії й обчислювальних ресурсів. Як зазначено у дисертації, ця проблема розглядається через поняття *резильєнтності* СІАД як комплексної властивості, що охоплює підготовку до збурень, їх поглинання, збереження працездатності, відновлення, адаптацію та, за потреби, керовану деградацію.

Актуальність дисертаційної роботи посилюється доведенням автором наявності низки суперечностей: по-перше, між потребою у комплексному оцінюванні *резильєнтності* СІАД до різнотипних збурень і фрагментарністю наявних методів оцінювання; по-друге, між потребою у комплексному забезпеченні *резильєнтності* СІАД до різнотипних збурень та різноманіттям засобів забезпечення окремих її аспектів з неочевидною сумісністю в єдиній системі; по-третє, між вимогами реального часу й ресурсними обмеженнями та обчислювальною складністю наявних методів підвищення *резильєнтності*.

Спрямування дисертаційної роботи на подолання зазначених суперечностей підкреслює її актуальність та визначає її зміст.

2. Зв'язок роботи з науковими програмами, планами і темами

Дослідження, представлені в дисертації, виконувалися у Національному аерокосмічному університеті «Харківський авіаційний інститут» та Сумському державному університеті в межах науково-дослідних робіт Міністерства освіти і науки України за держбюджетними темами, а саме:

– «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (Національний аерокосмічний університет «Харківський авіаційний інститут», № Д/Р 0122U001065, 2022–2023 рр.) – у частині розроблення концепції, принципів, методів та моделей оцінювання та забезпечення резильєнтності СІАД до різнотипних збурюючих чинників;

– «Розроблення системи керування безпілотним літальним апаратом на основі інтелектуального аналізу оптичного зображення» (Сумський державний університет, № Д/Р 0125U001029, 2025 р.) – у частині розроблення ІТ забезпечення резильєнтності СІАД на борту БПЛА в умовах обмежених обчислювальних ресурсів та впливу різнотипних збурюючих чинників;

– «Виконання завдань перспективного плану розвитку наукового напряму "Технічні науки" Сумського державного університету» (СумДУ, № Д/Р 0121U112684, 2024–2025 рр.) – у частині розроблення нейромережевої моделі СІАД з керованою структурною реконфігурацією та моделі формування збурюючих впливів для оптимізації обчислювальної ефективності та резильєнтності бортової СІАД БПЛА під час аналізу сенсорних даних;

– «Інформаційна технологія забезпечення резильєнтності інтелектуальної бортової системи малогабаритних літальних апаратів» (СумДУ, № Д/Р 0124U000548, 2024–2025 рр.) – у частині розроблення нейромережевих моделей СІАД з паралельною корекцією модулів та швидкою адаптацією до нових реалізацій збурень чи зміни умов;

– «Інформаційна технологія забезпечення резильєнтності систем штучного інтелекту для захисту кіберфізичних систем» (СумДУ, № Д/Р 0122U000782, 2022–2024 рр.) – у частині систематизації типів збурень і засобів захисту СІАД, а також розроблення методів мета-оптимізації резильєнтності СІАД та моделі операцій машинного навчання (MLOps) для забезпечення резильєнтності до різнотипних збурюючих впливів протягом життєвого циклу СІАД.

Зв'язок дисертаційної роботи Москаленка В.В. із наведеною науково-дослідною тематикою підтверджує послідовний характер виконаних досліджень, їх відповідність актуальним напрямам розвитку інформаційних технологій та орієнтацію на практичні завдання створення і експлуатаційної підтримки резильєнтних інтелектуальних систем.

3. Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій

Обґрунтованість наукових положень дисертації забезпечується коректним застосуванням фундаментального апарату системного аналізу, теорії ймовірностей і математичної статистики, методів оптимізації, мета-навчання та нейромережевого моделювання. Автор вибудував чітку і нерозривну логічну ланку: від концептуальних положень і формальних моделей до алгоритмічних методів і практичної реалізації.

Достовірність отриманих результатів підтверджується широкою експериментальною перевіркою, що базується на застосуванні методів стохастичного формування збурень та ін'єкцій апаратних/програмних несправностей, а також використанням різнотипних нейромережевих архітектур, репрезентативних наборів даних і абляційних досліджень. Суттєвою перевагою роботи є оригінальний траєкторний підхід до оцінювання: аналізується не лише миттєва реакція моделі на збурення, а вся динаміка її відновлення й адаптації. Для об'єктивного порівняння конфігурацій використано інтегральний показник резильєнтності у поєднанні зі статистичним узагальненням та ймовірнісною PAC-подібною процедурою перевірки порогових вимог.

Практична реалізованість результатів дослідження переконливо підтверджується створенням завершених програмних засобів і фреймворків для автоматизованої генерації збурень та реалізації параметричної/структурної реконфігурації СІАД, а також успішним впровадженням розроблених інформаційних технологій у галузевих організаціях та в навчальний процес провідних університетів (що підтверджено відповідними актами і довідками про впровадження). Запропоновані рішення готові до безпосередньої інтеграції в сучасні контури MLOps для забезпечення надійного функціонування кіберфізичних систем в умовах деструктивних впливів.

4. Наукова новизна отриманих результатів

Наукова новизна дисертаційної роботи має системний характер і полягає в розвиненні методологічних, модельних та методичних засад створення *резильєнтних СІАД*. До основних науково-нових результатів роботи належать такі:

1) *вперше розроблено методологію* (концепцію, принципи і структуру) створення резильєнтних СІАД, яка, на відміну від відомих, базується на розвитку концепції ресурсообмежених резильєнтних систем, що функціонують в агресивному кіберфізичному середовищі, та принципах всебічного врахування синергетичності впливу збурюючих чинників, мета-оптимізації резильєнтності та зміни реконфігураційних надбудов, що надає можливість обґрунтувати загальну структуру та вибір засобів забезпечення резильєнтності на різних етапах створення СІАД;

2) *вперше розроблено метод оцінювання* резильєнтності СІАД, який, на відміну від відомих, ґрунтується на обчисленні інтегрального показника

резильєнтності на траєкторіях адаптації до збурень за умови заданого ресурсного забезпечення та його статистичному узагальненні за серією стохастично сформованих випробувань, що надає змогу обґрунтувати вибір архітектурних рішень та значень параметрів резильєнтних систем;

3) *набула подальшого розвитку модель* формування синтетичних збурюючих впливів, яка відповідно до принципу всебічного врахування їх синергетичності базується на уніфікованій стратегії пошуку, яка не потребує доступу до градієнтів чи внутрішньої структури моделі СІАД, що дозволяє застосовувати єдиний алгоритмічний підхід для генерації широкого спектра різнотипних граничних станів задля комплексного оцінювання резильєнтності системи;

4) *вперше розроблено метод мета-оптимізації* резильєнтності СІАД, який, на відміну від існуючих, використовує інтегральний показник резильєнтності як мета-ціль та реалізує мета-навчання за результатами (траєкторіями) адаптації в умовах збурюючих впливів різної природи, що забезпечує узгоджене налаштування механізмів толерування впливів і динаміки адаптації з урахуванням ресурсних обмежень;

5) *вперше розроблено метод багатоетапного навчання* СІАД з керованою структурною реконфігурацією для узгодження вимог резильєнтності та обчислювальної ефективності, який, на відміну від відомих, включає етапи навчання модулів СІАД з реконфігураційними надбудовами в незбуреному режимі та мета-навчання в режимі збурення різнотипними впливами і регламентує етап адаптації релевантних модулів на нових даних, що дозволяє сформувати здатність до адаптивного перерозподілу обчислювальних ресурсів під час парирування атак та збоїв;

6) *удосконалено модель операцій машинного навчання* (MLOps) СІАД завдяки введенню операцій постфактум мета-оптимізації резильєнтності і постфактум калібрування невизначеності та адаптації під час тестування, які слугують основою для реалізації етапів підготовки та поглинання збурень, швидкого відновлення та/або керованої деградації системи;

7) *удосконалено нейромережну модель* СІАД з параметричною реконфігурацією завдяки реалізації паралельної корекції модулів у вигляді каскадної адаптерної надбудови з розділенням параметрів за режимами мета-оптимізації та оперативної адаптації, що забезпечує ресурсоефективне підвищення резильєнтності в умовах дії різнотипних збурюючих впливів;

8) *набула подальшого розвитку нейромережева моде*ль СІАД з керованою структурною реконфігурацією шляхом введення диференційовних надбудов умовної активації модулів основної моделі, узгоджених із форматами проміжних представлень моделі, та модифікованої функції активації з насиченням і витоком, які у сукупності сприяють обмеженню поширення збурень у глибині моделі та покращенню результатів мета-оптимізації резильєнтності.

Сукупність наведених наукових результатів є логічно взаємопов’язаною: методологія визначає принципи побудови резильєнтних СІАД, метод оцінювання

формує кількісну основу для порівняння рішень, модель збурень забезпечує інструментарій випробувань, реконфігураційні моделі реалізують механізми адаптації, методи мета-оптимізації та багатоетапного навчання здійснюють їх цілеспрямоване налаштування, а вдосконалена модель MLOps інтегрує ці засоби у процеси життєвого циклу. Отримані результати є новим теоретичним розв'язанням важливої науково-прикладної проблеми створення резильєнтних систем інтелектуального аналізу даних для кіберфізичних середовищ, що має вагоме прикладне значення для галузі.

5. Зв’язок матеріалів кандидатської дисертації з докторською дисертацією

Наукові положення, результати, висновки, рекомендації та інші матеріали наукових досліджень, представлені та захищені здобувачем у кандидатській дисертації, не стали предметом розгляду та не були використані в дослідженнях, представлених у поданій до захисту докторській дисертації Москаленко В’ячеслава Васильовича.

6. Практичне значення отриманих результатів

Практична цінність одержаних результатів полягає в доведенні теоретичних положень, моделей і методів до рівня прикладних інформаційних технологій оцінювання та забезпечення резильєнтності СІАД, придатних для безпосередньої інтеграції в індустріальні контури.

У роботі сформовано дві взаємопов’язані прикладні інформаційні технології:

– *Інформаційна технологія оцінювання резильєнтності*, яка регламентує повний цикл стрес-тестування: автоматизоване формування сценаріїв збурень, проведення контрольованих випробувань, побудову траєкторій зміни функціональної ефективності, статистичне узагальнення результатів та імовірнісну PAC-верифікацію виконання порогових вимог;

– *Інформаційна технологія забезпечення резильєнтності*, яка інтегрує механізми параметричної та структурної реконфігурації, мета-оптимізації, багатоетапного навчання, калібрування невизначеності, тестової адаптації (Test-Time Adaptation, *TTA*) і регламентовані MLOps-процедури для експлуатаційної підтримки систем.

Важливою перевагою розроблених технологій є їхня формалізація у вигляді IDEF0-діаграм із чітко визначеними входами, виходами, керуваннями та механізмами, а також доведеність до рівня готових програмних модулів і комп'ютерних програм, що підтверджено наведеними 3 *свідоцтвами про реєстрацію авторського права.*

Достовірність та високий індустріальний потенціал розробок підтверджено серією з 7 *офіційних актів про впровадження*. Результати досліджень та створені програмно-методичні комплекси успішно інтегровано в науково-дослідну роботу та навчальний процес провідних закладів вищої освіти України (Національного

аерокосмічного університету «Харківський авіаційний інститут» та Сумського державного університету), а також у практичні проєкти високотехнологічних галузевих підприємств (зокрема у сфері розробки та модернізації безпілотних систем, бортових комплексів, систем моніторингу місцевості та інфраструктурних об'єктів). Це переконливо доводить універсальність, адаптивність та готовність запропонованих технологій до практичного застосування у різноманітних критично важливих інформаційних та кіберфізичних системах.

7. Повнота викладення результатів дослідження в наукових публікаціях та апробація

Основні результати дисертаційної роботи відображено у 27 наукових публікаціях. Серед них є статті у виданнях, що індексуються у Scopus та Web of Science, у тому числі у виданнях першого і другого квартилів, розділи у зарубіжних монографіях, одноосібна монографія, матеріали міжнародних конференцій, в тому числі індексованих у Scopus, а також 3-х свідоцтв про реєстрацію авторського права на комп'ютерні програми. Тематика публікацій охоплює всі заявлені в науковій новизні методологічні, модельні та методичні засади створення *резильєнтних СІАД*.

8. Оцінка змісту, структури дисертаційної роботи та відповідності встановленим вимогам

Дисертаційна робота має чітку логічну структуру і складається зі вступу, шести розділів, висновків, списку використаних джерел і додатків.

У *першому розділі* виконано ґрунтовний аналіз поняття резильєнтності, систематизовано класи деструктивних збурень, охарактеризовано сфери застосування СІАД і критично проаналізовано відомі підходи до забезпечення робастності, відмовостійкості та адаптації, що дозволило обґрунтувати актуальність проблеми й сформувати задачі дослідження.

У *другому розділі* сформовано теоретико-методологічне ядро роботи: концепцію, базові принципи, модель формування синтетичних збурюючих впливів, метод оцінювання резильєнтності та модель операцій машинного навчання (MLOps).

У *третьому та четвертому розділах* розроблено комплекс архітектурно-модельних рішень, що охоплює нейромережні моделі СІАД із параметричною реконфігурацією (на основі адаптерних надбудов) та з керованою структурною реконфігурацією (на основі проміжних відгалужень і вентильних модулів).

У *п'ятому розділі* запропоновано методи мета-оптимізації та багатоетапного навчання резильєнтних СІАД із керованою реконфігурацією, а також наведено результати їхнього комплексного експериментального дослідження.

У *шостому розділі* теоретичні та практичні результати інтегровано в прикладні інформаційні технології оцінювання й забезпечення резильєнтності, формалізовані у вигляді IDEF0-моделей процесів та інструментальних засобів.

Зміст розділів тісно взаємопов’язаний, висновки логічно випливають з отриманих результатів, а комплекс додатків (від А до Ж) органічно доповнює основний текст та містить вичерпні доказові матеріали, а саме: відомості про програмну реалізацію інформаційних технологій, повний систематизований перелік публікацій здобувача за темою дисертації, офіційні акти впровадження результатів у виробництво та навчальний процес, розгорнуті оглядові та аналітичні таблиці до розділів, а також наочні графічні IDEF0-діаграми процесів забезпечення, оцінювання та верифікації резильєнтності СІАД.

За своєю суттю, науковою спрямованістю та практичним рівнем розроблених інформаційних технологій дисертаційна робота повністю відповідає вимогам спеціальності 05.13.06 – інформаційні технології.

9. Дотримання принципів академічної доброчесності

Аналіз змісту дисертації та поданих відомостей не дає підстав вважати, що робота містить ознаки академічного плагіату, фабрикації чи фальсифікації. Використані положення інших авторів супроводжуються посиланнями, а власні результати здобувача систематизовано у формулюваннях наукової новизни, особистого внеску та висновках.

10. Зауваження та дискусійні питання стосовно положень дисертації

Попри високий науково-теоретичний рівень та практичну цінність дисертаційної роботи Москаленка В. В., доцільно висловити окремі дискусійні міркування та зауваження:

1) експериментальна база дисертації переважно зосереджена на задачах систем комп'ютерного зору (Computer Vision Systems), а саме детектування та класифікації зображень, в той час поняття СІАД у роботі сформульоване набагато ширше. З огляду на те, що реальні кіберфізичні системи часто оперують гетерогенними даними (часовими рядами, телеметричними сенсорними потоками, структурованими записами), доцільно було б чіткіше окреслити, які компоненти запропонованої методології є інваріантними до типу вхідних даних, а які вимагають окремої предметної валідації;

2) для більш однозначного трактування експериментального протоколу варто було б детальніше розмежувати призначення адаптаційних, валідаційних і контрольних вибірок у неперервному потоці даних після розгортання СІАД, особливо за умов відкладеної або не повної розмітки;

3) інтегральний показник резильєнтності є зручним інструментом узагальнення динаміки функціональної ефективності. Водночас близькі значення цього показника можуть відповідати суттєво різним за наслідками сценаріям (наприклад, короткочасному критичному просіданню або тривалій помірній деградації). Доцільно уточнити порядок спільного використання інтегрального показника з мінімально допустимим рівнем ефективності та часом відновлення;

4) запропонована в роботі процедура ймовірнісної PAC-подібної верифікації (яка є складовою розробленого методу оцінювання резильєнтності СІАД у Розділі 2) гарантує статистичні гарантії стійкості для заданого класу збурень. Однак під час тривалого життєвого циклу СІАД конфігурація моделі та розподіл інформаційних потоків змінюються через дрейф даних і концепцій або неперервну експлуатаційну адаптацію. У зв'язку з цим доцільно чіткіше визначити критерії, за яких попередній результат верифікації втрачає чинність і вимагає повторного переоцінювання перед запровадженням оновленої версії СІАД у контурі операцій машинного навчання, (MLOps, Розділ 6);

5) у рамках дослідження нейромережевих моделей СІАД із параметричною реконфігурацією (здобувачем удосконалено модель із каскадними адаптерними надбудовами, Розділ 3) та керованою структурною реконфігурацією (набула подальшого розвитку модель із надбудовами умовної активації та вентильними модулями, Розділ 4) доцільно було б додатково проаналізувати стійкість самих реконфігураційних елементів за умов безпосереднього деструктивного впливу на них, наприклад, апаратних пошкоджень типу bit-flip або змагальних атак (adversarial attacks);

6) у низці експериментів покращення показників функціональної ефективності та резильєнтності мають відносно невелику абсолютну величину. Для глибшого розуміння практичної цінності результатів варто детальніше прокоментувати баланс між таким приростом, складністю синтезованих збурень та додатковими ресурсними витратами (FLOPS, пам'ять), пов'язаними із задіянням реконфігураційних надбудов;

7) хоча в роботі теоретично класифіковано різні типи дрейфу даних і концепцій, в експериментальній частині основну увагу приділено переважно різким змінам. Доцільно було б розширити дослідження щодо поведінки розроблених методів за умов поступового, інкрементного та тривалого дрейфу концепцій, коли деградація накопичується непомітно для стандартних детекторів;

8) з огляду на загальну дослідницьку логіку роботи (від теоретичних засад і методології оцінювання до розроблення нейромережевих моделей та методів їх навчання), здобувачеві можна запропонувати перенести наукове положення про модель формування синтетичних збурюючих впливів (яке в авторефераті наведено 7-м) на 3-тє місце в загальному переліку наукової новизни (після концепції та методу оцінювання резильєнтності). Така передислокація дозволить розташувати всі пункти наукової новизни строго послідовно за розділами дисертації та забезпечить наскрізну логічну цілісність викладу дослідницьких результатів.

Наведені зауваження мають переважно дискусійний і рекомендаційний характер, не ставлять під сумнів достовірність основних наукових положень та не знижують загальної позитивної оцінки дисертаційної роботи.

11. Загальний висновок

Дисертаційна робота Москаленка В'ячеслава Васильовича «Методологічні основи та інформаційні технології створення резильєнтних систем інтелектуального аналізу даних» є завершеною самостійною науковою працею, в якій розв'язано актуальну науково-прикладну проблему створення резильєнтних СІАД, що функціонують за різнотипних збурюючих впливів та ресурсних обмежень.

За актуальністю, науковою новизною, теоретичною і практичною значущістю, ступенем обґрунтованості та достовірності результатів, повнотою їх оприлюднення, структурою та рівнем виконання дисертаційна робота відповідає вимогам чинного Порядку присудження та позбавлення наукового ступеня доктора наук і вимогам до дисертацій на здобуття наукового ступеня доктора технічних наук, а її автор, Москаленко В'ячеслав Васильович, заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Офіційний опонент,
завідувачка кафедри інформаційний систем
Національного університету «Одеська політехніка»
доктор технічних наук, професор Олена АРСІРІЙ

Особистий підпис д-ра техн. наук, проф. Арсірій О. О. засвідчую

Вчений секретар Вченої ради
Національного університету
«Одеська політехніка» Лада ПРОКОПОВИЧ