ВІДГУК

офіційного опонента, доктора технічних наук, професора,
заступника директора з наукової роботи Національного центру
«Мала академія наук України» МОН України і НАН України
Стрижака Олександра Євгенійовича
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

АКТУАЛЬНІСТЬ ТЕМИ

Сучасні системи інтелектуального аналізу даних дедалі частіше є складовими розподілених інформаційних платформ, у яких поєднуються різнорідні потоки даних, навчувані моделі, засоби формування рішень, моніторингу та післярозгортальної адаптації. За таких умов якість системи визначається не лише точністю окремої моделі в штатному режимі, а й здатністю зберігати функціональну та інформаційну цілісність під дією несправностей, змагальних впливів, дрейфу даних, зміни задачі та обмежень ресурсів.

У дисертаційній роботі ця проблема розглядається через концепцію резильєнтності СІАД як динамічної властивості, що охоплює підготовку до збурень, їх поглинання, відновлення функціональної ефективності, адаптацію та, за потреби, керовану деградацію. Важливим є системне поєднання таксономічного й онтологічного опису предметної області, моделі формування збурень, траєкторного оцінювання, мета-оптимізації, реконфігураційних механізмів та MLOps-процедур. Така постановка відповідає сучасним тенденціям розвитку інтелектуальних інформаційних технологій, для яких критичними стають не лише продуктивність, а й контроль ризику, відтворюваність і здатність працювати в умовах змін.

Дослідження, представлені у дисертаційній роботі, виконувалися в межах низки науково-дослідних робіт Міністерства освіти і науки України, тематика яких безпосередньо пов'язана з розробленням методів, моделей та інформаційних технологій забезпечення резильєнтності інтелектуальних систем. Зокрема, у межах держбюджетної теми «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.) виконано дослідження, пов'язані з розробленням концепції, принципів, методів і моделей оцінювання та забезпечення резильєнтності СІАД до різнотипних збурюючих чинників. У межах теми «Розроблення системи керування безпілотним літальним апаратом на основі інтелектуального аналізу оптичного зображення» (Сумський державний

університет, № Д/Р 0125U001029, 2025 р.) розроблялися інформаційні технології забезпечення резильєнтності СІАД на борту БПЛА за обмежених обчислювальних ресурсів та впливу різнотипних збурень.

У межах науково-дослідної роботи «Виконання завдань перспективного плану розвитку наукового напряму "Технічні науки" Сумського державного університету» (№ Д/Р 0121U112684, 2024–2025 рр.) розроблялися нейромережна модель СІАД із керованою структурною реконфігурацією та модель формування збурюючих впливів для оптимізації обчислювальної ефективності й резильєнтності бортової СІАД БПЛА під час аналізу сенсорних даних. За темою «Інформаційна технологія забезпечення резильєнтності інтелектуальної бортової системи малогабаритних літальних апаратів» (№ Д/Р 0124U000548, 2024–2025 рр.) досліджувалися нейромережні моделі СІАД із паралельною корекцією модулів та швидкою адаптацією до нових реалізацій збурень і змін умов функціонування.

Крім того, у межах держбюджетної теми «Інформаційна технологія забезпечення резильєнтності систем штучного інтелекту для захисту кіберфізичних систем» (Сумський державний університет, № Д/Р 0122U000782, 2022–2024 рр.) виконано систематизацію типів збурень і засобів захисту СІАД, розроблено методи мета-оптимізації резильєнтності та модель операцій машинного навчання (MLOps), призначену для підтримання резильєнтності до різнотипних збурюючих впливів протягом життєвого циклу системи.

Наведений зв'язок із науково-дослідними роботами свідчить, що результати дисертації формувалися послідовно в межах взаємопов'язаних досліджень із гарантоздатності інтелектуальних систем, резильєнтності систем штучного інтелекту, ресурсообмежених бортових СІАД та інтелектуального аналізу сенсорних даних.

СТРУКТУРА, ЛОГІКА ТА ЗМІСТ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

Дисертація складається зі вступу, шести розділів, висновків, переліку використаних джерел і семи додатків. Повний обсяг роботи становить 406 сторінок, основна частина викладена на 322 сторінках. Перелік використаних джерел містить 191 найменування і займає 23 сторінки, додатки викладено на 41 сторінці. Дисертація містить 46 рисунків і 46 таблиць в основному тексті.

У вступі обґрунтовано актуальність обраної теми, сформульовано науково-прикладну проблему, мету та десять завдань дослідження, визначено об'єкт, предмет і методи дослідження, наведено положення наукової новизни, практичне значення результатів, відомості про їх апробацію, публікації та особистий внесок здобувача. Окремо розкрито зв'язок роботи з науковими програмами, планами і темами.

У першому розділі здійснено аналіз проблеми створення резильєнтних систем інтелектуального аналізу даних. Розглянуто сутність концепції

резильєнтності, загрози та збурюючі впливи на СІАД, сфери їх застосування, для яких вимоги до резильєнтності є критичними, а також проведено критичний аналіз відомих підходів. За результатами аналізу сформульовано науково-прикладну проблему та постановку задач дослідження.

Другий розділ формує методологічне ядро дисертації. У ньому запропоновано концепцію, принципи і структуру методології створення резильєнтних СІАД, розкрито принципи всебічного врахування синергетичного впливу збурюючих чинників, мета-оптимізації резильєнтності та зміни реконфігураційних надбудов, розроблено модель формування синтетичних збурюючих впливів, метод оцінювання резильєнтності та модель операцій машинного навчання для створення і експлуатаційної підтримки резильєнтних СІАД.

Третій розділ присвячено розробленню та дослідженню нейромережних моделей СІАД із параметричною реконфігурацією модулів. Обґрунтовано модель паралельної корекції модулів, розглянуто архітектури адаптерів і мета-адаптерів та експериментально досліджено їх вплив на резильєнтність за різних типів збурень.

У четвертому розділі розроблено і досліджено моделі СІАД із керованою структурною реконфігурацією. Розглянуто динамічні нейромережі з проміжними відгалуженнями та вентильними модулями, методи їх навчання і механізми умовної активації обчислювальних модулів за наявності збурень та ресурсних обмежень.

П'ятий розділ присвячено методам оптимізації резильєнтності СІАД. Запропоновано градієнтний та еволюційний алгоритми реалізації методу мета-оптимізації резильєнтності, метод багатоетапного навчання СІАД із керованою структурною реконфігурацією, а також проведено комплексні експериментальні дослідження резильєнтності нейромережевих моделей і функціонування СІАД у конвеєрі операцій машинного навчання.

У шостому розділі розроблено інформаційні технології оцінювання та забезпечення резильєнтності СІАД, формалізовано перетворення інформації в IDEF0-моделях, описано інструментальні засоби реалізації та наведено результати практичного впровадження.

У висновках узагальнено основні наукові та практичні результати. У додатках наведено відомості про програмну реалізацію інформаційної технології забезпечення резильєнтності СІАД, список публікацій здобувача, акти впровадження, розгорнуті оглядові таблиці та IDEF0-діаграми інформаційних технологій.

Структура дисертації відповідає логіці розв'язання поставленої науково-прикладної проблеми. Матеріал викладено послідовно із застосуванням усталеної наукової термінології, використані положення інших авторів супроводжуються відповідними посиланнями.

Аналіз змісту дисертації та поданих відомостей не дає підстав вважати, що робота містить ознаки академічного плагіату, фабрикації чи фальсифікації. Результати, що належать співавторам і були відображені в їхніх захищених дисертаціях, у роботі окремо відмежовано від особистого внеску В. В. Москаленка.

НАУКОВА НОВИЗНА РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

У дисертаційній роботі наведено розв'язання актуальної науково-прикладної проблеми створення резильєнтних систем інтелектуального аналізу даних, що функціонують за умов впливу різнотипних збурюючих чинників та ресурсних обмежень. При цьому отримано такі наукові результати.

Вперше розроблено:

1) методологію створення резильєнтних систем інтелектуального аналізу даних, що включає концепцію, принципи і структуру та, на відміну від відомих підходів, базується на розвитку концепції ресурсообмежених резильєнтних систем, які функціонують в агресивному кіберфізичному середовищі, а також на принципах всебічного врахування синергетичності впливу збурюючих чинників, мета-оптимізації резильєнтності та зміни реконфігураційних надбудов, що дає змогу обґрунтовувати загальну структуру та вибір засобів забезпечення резильєнтності на різних етапах створення СІАД;

2) метод оцінювання резильєнтності СІАД, який 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 дає змогу обґрунтовувати вибір архітектурних рішень і значень параметрів резильєнтних систем;

3) метод мета-оптимізації резильєнтності СІАД, який використовує інтегральний показник резильєнтності як мета-ціль і реалізує мета-навчання за результатами траєкторій адаптації в умовах збурюючих впливів різної природи, що забезпечує узгоджене налаштування механізмів толерування впливів і динаміки адаптації з урахуванням ресурсних обмежень;

4) метод багатоетапного навчання СІАД із керованою структурною реконфігурацією для узгодження вимог резильєнтності та обчислювальної ефективності, який включає етапи навчання модулів СІАД із реконфігураційними надбудовами у незбуреному режимі, мета-навчання в режимі різнотипних збурень і адаптацію релевантних модулів на нових даних, що дає змогу сформувати здатність до адаптивного перерозподілу обчислювальних ресурсів під час парирування атак та збоїв.

Удосконалено:

5) модель операцій машинного навчання (MLOps) СІАД шляхом введення операцій постфактум мета-оптимізації резильєнтності, 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;

6) нейромережну модель СІАД із 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 за умов дії різнотипних збурюючих впливів.

Набули подальшого розвитку:

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

8) нейромережна модель СІАД із керованою структурною реконфігурацією шляхом введення диференційовних надбудов умовної активації модулів основної моделі, узгоджених із форматами її проміжних представлень, 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 результатів формує цілісну методологічну основу створення резильєнтних СІАД. Наукова новизна простежується на всіх рівнях дослідження — від концептуальних положень і способів оцінювання резильєнтності до методів мета-оптимізації, реконфігурації нейромережевих моделей та організації їх життєвого циклу. Важливою рисою роботи є взаємозв'язок отриманих результатів: моделі збурень і оцінювання формують основу для мета-оптимізації, а параметрична та структурна реконфігурація виступають механізмами практичного забезпечення резильєнтності за ресурсних обмежень.

ПРАКТИЧНЕ ЗНАЧЕННЯ РЕЗУЛЬТАТІВ РОБОТИ ТА ПОВНОТА ЇХ ВИКЛАДУ В НАУКОВИХ ПУБЛІКАЦІЯХ

Практична цінність роботи полягає в доведенні наукових положень до рівня двох взаємопов'язаних інформаційних технологій — оцінювання та забезпечення резильєнтності СІАД. Інформаційна технологія оцінювання охоплює формування сценаріїв збурюючих впливів, проведення контрольованих випробувань, побудову кривих резильєнтності, обчислення інтегрального показника, статистичне узагальнення результатів та, за необхідності, ймовірнісну верифікацію виконання порогових вимог.

Інформаційна технологія забезпечення резильєнтності регламентує використання параметричних і структурних реконфігураційних надбудов, мета-

оптимізації, багатоетапного навчання, калібрування невизначеності, адаптації під час тестування, керованої деградації та інших MLOps-процедур для підтримання прийнятного рівня резильєнтності під час створення, впровадження й експлуатаційного супроводу СІАД за обмежених обчислювальних, енергетичних і часових ресурсів.

Практичну значущість результатів підтверджено їх використанням у навчальному процесі та науково-дослідних роботах Національного аерокосмічного університету «Харківський авіаційний інститут» і Сумського державного університету, а також на підприємствах галузі. Зокрема, результати впроваджено в ТОВ «Jet Bee System», ТОВ «СМАРТ МАШІНЕРІ СОЛЮШНС» і ТОВ «Конструкторське бюро "Північна Слобожанщина"» під час модернізації безпілотних систем, а також у ТОВ «Molfar.AI» та ТОВ «РОЗУМНІ ТЕХНОЛОГІЇ "ТИТУЛ"» під час розроблення й модернізації систем моніторингу інфраструктурних об'єктів та місцевості. Впровадження підтверджено відповідними актами.

Основні результати дисертаційної роботи викладено у 27 наукових публікаціях, у тому числі у двох розділах колективних зарубіжних монографій, проіндексованих у Scopus, одній одноосібній вітчизняній монографії, 15 статтях у періодичних наукових виданнях, серед яких п'ять статей у виданнях Q1–Q2, дві — у виданнях Q3, а також статті у виданнях, що індексуються у Scopus та/або Web of Science. Результати апробовано у шести публікаціях у матеріалах і тезах наукових конференцій, чотири з яких проіндексовані у Scopus. Додатково наукові результати відображено у трьох свідоцтвах про реєстрацію авторського права на комп'ютерні програми.

Тематика публікацій охоплює ключові методологічні, математичні, нейромережні та інформаційно-технологічні результати дисертації. Задекларований особистий внесок здобувача у спільних публікаціях відповідає змісту дисертаційної роботи та положенням, що виносяться на захист.

ОБҐРУНТОВАНІСТЬ ТА ДОСТОВІРНІСТЬ НАУКОВИХ ПОЛОЖЕНЬ, ВИСНОВКІВ І РЕКОМЕНДАЦІЙ

Ступінь обґрунтованості наукових положень, висновків і рекомендацій. Обґрунтованість наукових положень забезпечується комплексним використанням методів системного аналізу, систематизації й таксономічного моделювання, онтологічного подання предметної області, теорії ймовірностей і математичної статистики, градієнтної та еволюційної оптимізації, мета-навчання, нейромережевого моделювання, стохастичного формування збурень, ін'єкції несправностей, доменної та тестової адаптації. Послідовність дослідження простежується від концептуального опису предметної області до математичних моделей, алгоритмічних методів та інформаційних технологій.

Позитивною рисою роботи є використання таксономії для ієрархічної систематизації понять і сценаріїв збурень та онтологічної діаграми для фіксації семантичних зв'язків між СІАД, класами збурень, етапами резильєнтного функціонування, показниками, принципами й засобами забезпечення. Оцінювання резильєнтності виконується за траєкторією зміни функціональної ефективності, що дозволяє враховувати не лише початкове просідання, а й динаміку відновлення. Для серій стохастичних випробувань застосовується статистичне узагальнення, а за наявності порогових вимог – ймовірнісна PAC-подібна процедура верифікації.

Достовірність висновків підсилюється експериментами на різних нейромережних архітектурах і наборах даних, дослідженням принципово різних класів збурень, абляційними порівняннями та аналізом базових і модифікованих конфігурацій. Практичну реалізованість підтверджують створені програмні засоби, інформаційні потоки й артефакти, описані в IDEF0-моделях, а також впровадження результатів у наукових установах, закладах освіти та на підприємствах.

ЗАУВАЖЕННЯ ЩОДО ПОЛОЖЕНЬ ДИСЕРТАЦІЇ ТА ДИСКУСІЙНІ ПИТАННЯ

1. У другому розділі таксономія резильєнтності використовується для ієрархічної систематизації понять і контролю повноти сценаріїв, а онтологічна діаграма – як «спільний словник», що фіксує семантичні зв'язки між поняттями. Водночас онтологічне подання залишається переважно концептуально-графічним. Доцільно було б чіткіше показати, як воно може бути формалізоване у машинно-оброблюваному вигляді та безпосередньо використовуватися для автоматизованого формування сценаріїв, перевірки узгодженості термінів або вибору механізмів забезпечення резильєнтності.

2. У роботі свідомо окреслено СІАД як системи, де центральними є дані, навчувана модель і прийняття рішень, а чисто символічні системи знань винесено за межі дослідження. Разом з тим сучасні інтелектуальні інформаційні платформи дедалі частіше мають гібридну нейро-символьну структуру, поєднуючи машинне навчання, онтології, графи знань і правила. Доцільно було б чіткіше визначити межі перенесення запропонованої методології на такі гібридні системи та вказати, які елементи резильєнтності можуть оцінюватися на рівні всієї системи, а які – лише для її навчуваних компонентів.

3. Узагальнена модель збурень, запропонована у дисертації, охоплює впливи на вхідні дані, параметри моделей, проміжні представлення та розподіли даних. Водночас для сучасних великих мовних моделей, систем із доповненням генерації шляхом пошуку зовнішньої інформації (retrieval-augmented generation, RAG) та агентних інтелектуальних систем суттєвого значення набувають також збурення на семантичному та інформаційному рівнях. До них, зокрема, належать ін'єкція

шкідливих інструкцій у запит (prompt injection), отруєння джерел зовнішнього пошуку (retrieval poisoning), суперечливість або пошкодження баз знань, помилки зовнішніх програмних інструментів, а також порушення маршрутизації інформаційних запитів. У зв'язку з цим доцільно було б чіткіше визначити місце таких збурень у запропонованій таксономії та показати можливість розширення параметризованої моделі формування збурюючих впливів на рівень контексту, знань і зовнішніх інформаційних каналів.

4. Ймовірнісна верифікація резильєнтності є умовною щодо заданого класу сценаріїв, процедури їх семплювання та конкретної конфігурації СІАД. У той же час сама таксономія загроз, онтологічний опис предметної області та конфігурація моделі можуть змінюватися в процесі експлуатації або розвитку системи. Доцільно було б формалізувати політику версіонування цих артефактів і правило повторної верифікації: за яких змін попередній PAC-висновок ще може вважатися релевантним, а за яких система має проходити новий цикл оцінювання.

5. Інтегральний показник резильєнтності будується на нормалізованому показнику функціональної ефективності (Q(t)), що забезпечує універсальність запропонованого підходу до оцінювання. Водночас у різних предметних областях зміст показника (Q) може істотно відрізнятися: ним може бути, наприклад, точність класифікації (accuracy), середня точність детектування (mAP, mean Average Precision), функція корисності з урахуванням вартості помилок (cost-sensitive utility), показник ризику або показник якості інформаційного рішення. У зв'язку з цим доцільно було б чіткіше формалізувати процедуру приведення предметно-залежних показників функціональної ефективності до нормованої шкали (Q), а також визначити межі коректного порівняння значень інтегрального показника резильєнтності (R) для різних класів СІАД.

6. Принцип всебічного врахування синергетичності збурюючих чинників є одним із центральних положень методології, але синергетичність переважно встановлюється через порівняння одиничних і композитних сценаріїв та аналіз перехресного впливу механізмів захисту. Для підсилення формалізації доцільно було б увести окремий індекс або статистичний критерій взаємодії, який дозволяв би кількісно розрізняти адитивний, антагоністичний і синергетичний характер ефектів.

7. У розділі 6 інформаційні технології оцінювання та забезпечення резильєнтності подано окремо, хоча в експлуатаційному життєвому циклі вони утворюють замкнений контур. Було б корисно ще виразніше показати інформаційний зворотний зв'язок між ними: як каталоги сценаріїв, версії таксономії та онтології, журнали випробувань, статистичні оцінки, конфігурації моделей і результати верифікації накопичуються в спільному інформаційному просторі та використовуються для наступних циклів реконфігурації й мета-оптимізації.

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

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 в умовах різнотипних збурюючих впливів та ресурсних обмежень. Отримані результати мають методологічну цілісність, теоретичне обґрунтування, експериментальне підтвердження та практичне впровадження.

За актуальністю, науковою новизною, теоретичною і практичною значущістю, ступенем обґрунтованості та достовірності результатів, повнотою їх оприлюднення і рівнем виконання дисертаційна робота відповідає вимогам, що висуваються 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.

Опонент:
доктор технічних наук, професор,
заступник директора з наукової роботи
Національного центру
«Мала академія наук України»
МОН України та НАН України Олександр СТРИЖАК

Підпис Стрижака О.Є. засвідчую