

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

**МОСКАЛЕНКО В'ЯЧЕСЛАВ ВАСИЛЬОВИЧ**



УДК 004.9.05:681.5(043.5)

**МЕТОДОЛОГІЧНІ ОСНОВИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ  
СТВОРЕННЯ РЕЗИЛЬЄНТНИХ СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО  
АНАЛІЗУ ДАНИХ**

05.13.06 – інформаційні технології

**РЕФЕРАТ**

дисертації на здобуття наукового ступеня  
доктора технічних наук

Хмельницький – 2026

Дисертацією є рукопис.

Робота виконана в Національному аерокосмічному університеті «Харківський авіаційний інститут» Міністерства освіти і науки України.

Науковий консультант: член-кореспондент Національної академії наук України, доктор технічних наук, професор  
**Харченко Вячеслав Сергійович**,  
Національний аерокосмічний університет «Харківський авіаційний інститут», завідувач кафедри кібербезпеки та інтелектуальних інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор  
**Казимир Володимир Вікторович**,  
Національний університет «Чернігівська політехніка», професор кафедри інформаційних та комп'ютерних систем

докторка технічних наук, професорка  
**Арсірій Олена Олександрівна**,  
Національний університет «Одеська політехніка», завідувачка кафедри інформаційних систем

доктор технічних наук, старший науковий співробітник  
**Стрижак Олександр Євгенійович**,  
Національний центр «Мала академія наук України», старший науковий співробітник

Захист відбудеться «20» листопада 2026 р. о 10:00 годині на засіданні спеціалізованої вченої ради Д 70.052.06 у Хмельницькому національному університеті (29016, м. Хмельницький, вул. Кам'янецька, 112, навчальний корпус №1 Хмельницького національного університету, ауд. 1-210).

З дисертацією можна ознайомитися на офіційному веб-сайті Університету та в науково-технічній бібліотеці Хмельницького національного університету (29016, м. Хмельницький, вул. Кам'янецька, 110/1).

Реферат оприлюднено «12» жовтня 2026 р.

Вчений секретар  
спеціалізованої вченої ради  
к.т.н., доцент



А. О. Нічепорук

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність роботи.** Стрімка інтеграція систем інтелектуального аналізу даних (СІАД) у критично важливі інформаційно-керуючі системи посилює вимоги до їхньої надійності, безпеки, робастності та здатності швидко відновлювати функціональну ефективність у змінних умовах. На практиці СІАД зазнають впливу різнотипних збурюючих чинників: спотворень і атак на дані, пошкодження вагових параметрів та результатів проміжних обчислень, новизни в даних, дрейфу або зміни концепцій, домену, задач, а також працюють під жорсткими ресурсними обмеженнями (час, пам'ять, енергія).

Концепція резильєнтності як властивості системи зберігати прийнятний рівень функціонування під дією збурень і змін та відновлюватися й адаптуватися після них має міждисциплінарне походження. У науковий обіг її системне трактування було введено в екології К. С. Холлінгом, який пов'язував резильєнтність зі здатністю системи поглинати збурення без втрати базових структурно-функціональних характеристик [1]. Подальше становлення інженерного напрямку відображено в межах інженерії резильєнтності, пов'язаної з працями Е. Холлнагеля, Д. Вудса, Н. Левесона та ін., де резильєнтність розглядається через здатність складних людино-машинних і технічних систем завчасно готуватися, реагувати, відновлюватися, адаптуватися та навчатися в умовах невизначеності [2, 3]. У комп'ютерних системах резильєнтність концептуально пов'язують із гарантоздатністю сервісу: зокрема Ж.-К. Лапрі розглядав резильєнтність як розвиток концепції гарантоздатності в умовах змін, а в подальших працях це визначення узагальнювалося як збереження гарантоздатності за умов змін [4, 5]. Серед вітчизняних учених, які розвивали системні підходи до гарантоздатності, резильєнтності або кіберрезильєнтності комп'ютерних систем, помітне місце займають праці В. С. Харченка та його наукової школи: А. В. Горбенка – у частині гарантоздатних сервіс-орієнтованих і Web-систем [6–9], О. М. Одаруценка – у частині оцінювання гарантоздатності, готовності та функціональної безпеки комп'ютерних і програмно-технічних систем [10–12], О. В. Іванченка – у частині оцінювання ризиків, готовності та кібербезпеки критичних інформаційно-керуючих і хмарних систем [13, 14], С. М. Лисенка – у частині таксономічного й онтологічного опису резильєнтності комп'ютерних систем за наявності кіберзагроз [15], Ю. Л. Поночовного – у частині методології забезпечення гарантоздатності інформаційно-керуючих систем, а також моделей резильєнтних систем з урахуванням готовності, кібербезпеки та змін вимог [16, 17].

Наявні підходи до створення резильєнтних СІАД переважно фрагментарні і охоплюють окремі аспекти резильєнтності, але не враховують синергетичності впливу різнотипних збурюючих чинників і методів захисту, не забезпечують уніфікованої оцінки й оптимізації резильєнтності протягом усього життєвого циклу, а також рідко узгоджуються з практиками операцій машинного навчання (MLOps) та обмеженнями реального часу. Це ускладнює впровадження СІАД у сферах з підвищеними ризиками та відповідальністю, де потрібні інтегральні критерії оцінювання, керовані механізми адаптації та ресурсно-обмежені стратегії підвищення резильєнтності. Тому існує нагальна потреба у розробці методологічних основ та інформаційних технологій створення резильєнтних СІАД в умовах впливу

різнотипних збурень з урахуванням ресурсних обмежень.

Аналіз сучасного стану досліджень і практики створення резильєнтних СІАД виявив низку суттєвих протиріч, що обмежують їхню ефективність у критично важливих інформаційних системах. Зокрема, існують такі суперечності:

1. Між потребою в комплексному оцінюванні резильєнтності системи інтелектуального аналізу даних до різнотипних збурень (викривлення даних, пошкодження ваг, зміна середовища і задач та інше) і фрагментарністю наявних методів оцінювання. Недолік наявних підходів: метрики та бенчмарки перевіряють окремі аспекти (робастність до шуму, атак, відмовостійкість тощо) і не дають інтегральної оцінки та гарантій для обґрунтування вибору гіперпараметрів СІАД та архітектурних рішень.

2. Між потребою в забезпеченні комплексної резильєнтності системи інтелектуального аналізу даних до різнотипних збурень та різноманіттю методів забезпечення окремих аспектів резильєнтності, а також невідомою їхньою сумісністю в єдиній системі. Недолік існуючих підходів: бракує уніфікованих принципів комбінування, узгодження цілей і ваг, стандартів взаємодії методів без деградації загальної резильєнтності, а також відсутня уніфікована, сумісна «надбудова» для забезпечення резильєнтності систем інтелектуального аналізу даних.

3. Між вимогами реального часу й ресурсними обмеженнями і «важковаговістю» методів підвищення резильєнтності. Недолік існуючих підходів: відсутня спільна оптимізація «функціональна ефективність – резильєнтність – обчислювальна ефективність»; бракує моделей, що динамічно підлаштовують структуру та обчислення для підвищення резильєнтності до збурень в умовах обмежених ресурсів.

Для подолання зазначених протиріч пропонується: розробити концепцію, принципи і структуру методології забезпечення резильєнтності СІАД; розробити моделі і методи оцінювання резильєнтності СІАД; розробити моделі і методи оптимізації резильєнтності СІАД до різнотипних збурюючих чинників; розробити моделі і методи раціонального використання ресурсів з урахуванням вимог до резильєнтності СІАД; розробити моделі та методи операцій машинного навчання (MLOps) для забезпечення резильєнтності СІАД протягом їх життєвого циклу.

З огляду на викладене, розроблення методології, моделей, методів та інформаційної технології створення резильєнтних СІАД до різнотипних збурюючих впливів в умовах ресурсних обмежень є актуальною науково-прикладною проблемою.

**Зв'язок роботи з науковими програмами, планами, темами, грантами.** Наведені в дисертації дослідження проводилися у межах науково-дослідних робіт Міністерства освіти і науки України за держбюджетними темами: «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (НАКУ «ХАІ», № Д/Р 0122U001065, 2022-2023 рр.) – в 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»

(СумДУ, № 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 напрямку “Технічні науки” Сумського державного університету» (СумДУ, № Д/Р 0121U112684, 2024-2025 рр.) – в частині розроблення нейромережної 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.) – в частині розроблення нейромережних 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.) – в 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.

**Мета і завдання дослідження.** Мета дослідження – підвищення резильєнтності систем інтелектуального аналізу даних, що функціонують в умовах впливу різнотипних збурюючих чинників та обчислювальних, часових й інших ресурсних обмежень, шляхом розроблення методологічних основ їх створення, моделей, методів та інформаційних технологій оцінювання й забезпечення вимог до резильєнтності протягом життєвого циклу цих систем.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- 1) проаналізувати тенденції розвитку, математичний апарат, моделі і методи оцінювання та забезпечення вимог до показників резильєнтності СІАД, визначити суперечність та обґрунтувати науково-прикладну проблему;
- 2) розробити концепцію, принципи і структуру методології створення резильєнтних СІАД;
- 3) розробити модель формування синтетичних збурюючих впливів задля комплексного оцінювання резильєнтності системи;
- 4) розробити метод оцінювання резильєнтності СІАД для обґрунтування вибору архітектурних рішень та значень параметрів резильєнтних СІАД;
- 5) розробити модель операцій машинного навчання (MLOps) СІАД, що слугує основою для реалізації операційних елементів реалізації концепції резильєнтності СІАД;
- 6) розробити модель СІАД, здатну до параметричної реконфігурації для забезпечення резильєнтності в умовах дії збурюючих чинників та ресурсних обмежень;
- 7) розробити модель СІАД, здатну до структурної реконфігурації для забезпечення резильєнтності в умовах дії збурюючих чинників та ресурсних обмежень;
- 8) розробити метод мета-оптимізації резильєнтності СІАД, що забезпечує узгоджене налаштування механізмів толерування впливів і динаміки адаптації за

ресурсних обмежень;

9) розробити метод навчання СІАД зі структурною реконфігурацією для узгодження вимог резильєнтності та обчислювальної ефективності;

10) впровадити інформаційні технології оцінювання та забезпечення резильєнтності СІАД для різних галузей застосування.

**Об'єкт дослідження** – процеси функціонування СІАД в умовах впливу збурюючих чинників та ресурсних обмежень.

**Предмет дослідження** – методологічні основи (концепція, принципи, структура), моделі, методи та інформаційні технології оцінювання та забезпечення резильєнтності СІАД.

**Методи дослідження.** Для виконання поставлених у дисертаційній роботі задач використано комплекс загальнонаукових, математичних, інформаційно-технологічних та експериментальних методів. Для аналізу стану проблеми, тенденцій розвитку, наявного математичного апарату, моделей і методів оцінювання та забезпечення резильєнтності систем інтелектуального аналізу даних використано методи аналізу предметної області, бібліометричного та контент-аналізу наукових публікацій, систематизації, класифікації й таксономічного моделювання. Ці методи дали змогу визначити наявні суперечності, обґрунтувати науково-прикладну проблему та сформулювати логіку подальшого дослідження. Для розроблення концепції, принципів і структури методології створення резильєнтних СІАД використано принципи й методи системного аналізу, багатокритеріального аналізу та оптимізації. Для формалізації збурюючих впливів і оцінювання резильєнтності застосовано методи класифікації збурюючих чинників, стохастичного та змагального моделювання, ін'єкції несправностей, моделювання дрейфу даних і концепцій, а також апарат інженерії резильєнтності, теорії ймовірностей і математичної статистики. Для розроблення моделей СІАД, здатних до параметричної та структурної реконфігурації, використано методи нейромережевого моделювання, параметрично-ефективного перенесення навчання, адаптерного налаштування, побудови динамічних нейромереж, умовних обчислень, вентильного керування модулями, раннього завершення обчислень і регуляризації обчислювальних витрат. Для розроблення методів мета-оптимізації резильєнтності та навчання СІАД з урахуванням ресурсних обмежень використано методи градієнтної й еволюційної оптимізації, мета-навчання, змагального навчання, навчання з ін'єктованими несправностями, аналізу обчислювальної складності та оптимізації з ресурсними обмеженнями. Для розроблення моделі операцій машинного навчання резильєнтної СІАД використано методи моделювання процесів життєвого циклу та MLOps, принципи моніторингу, зворотного зв'язку й післярозгортального супроводу моделей, а також методи доменної адаптації та адаптації під час тестування. Для експериментального дослідження запропонованих моделей, методів і операційних процедур використано методи комп'ютерного моделювання, планування та проведення обчислювальних експериментів, порівняльного оцінювання, абляційного аналізу й статистичної обробки результатів. Для впровадження інформаційних технологій оцінювання та забезпечення резильєнтності СІАД використано методи формалізації процесів і даних, IDEF0-моделювання, алгоритмічного та програмно-інженерного моделювання, а також

інструменти розроблення, тестування й розгортання інформаційних технологій.

**Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.** Обґрунтованість і достовірність наукових положень, висновків та рекомендацій дисертації забезпечуються коректним застосуванням методів системного аналізу, теорії ймовірностей і математичної статистики, оптимізації, нейромережевого та комп'ютерного моделювання, а також узгодженістю результатів теоретичного аналізу з результатами серій стохастичних обчислювальних експериментів, проведенням порівняльного й абляційного аналізу, статистичним узагальненням показників резильєнтності, програмною реалізацією запропонованих моделей і методів та практичним впровадженням результатів дослідження.

**Наукова новизна отриманих результатів.** Наукові результати дисертаційного дослідження полягають у такому:

а) вперше розроблено:

1) методологію (концепцію, принципи і структуру) створення резильєнтних систем інтелектуального аналізу даних (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) 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) 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;

4) 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 парирования атак та збоїв;

б) удосконалено:

1) 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;

2) 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 ресурсно-ефективне підвищення резильєнтності в умовах дії різнотипних збурюючих впливів;

в) отримали подальший розвиток:

1) 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;

2) нейромережну модель СІАД з керованою структурною реконфігурацією шляхом введення диференційованих 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.

**Практичне значення отриманих результатів** полягає в доведенні розроблених методологічних положень, моделей і методів до рівня прикладних інформаційних технологій оцінювання та забезпечення резильєнтності, призначених для створення і супроводу резильєнтних СІАД. Запропоновані результати дають змогу подолати обмеження фрагментарного підходу до проектування, випробування, впровадження та експлуатаційної підтримки СІАД шляхом формалізованого врахування різнотипних збурюючих чинників, інтегрального оцінювання резильєнтності, використання реконфігураційних надбудов, мета-оптимізації та MLOps-процедур підтримання резильєнтності в умовах ресурсних обмежень.

У дисертаційному дослідженні отримано такі практичні результати:

– розроблено інформаційну технологію оцінювання резильєнтності СІАД, яка забезпечує формування сценаріїв збурюючих впливів, проведення контрольованих випробувань, обчислення інтегрального показника резильєнтності та статистичне узагальнення результатів оцінювання для обґрунтування рішень під час створення резильєнтних СІАД;

– розроблено інформаційну технологію забезпечення резильєнтності СІАД, яка регламентує використання параметричних і структурних реконфігураційних надбудов, мета-оптимізації, багатоетапного навчання, адаптації та MLOps-процедур для підтримання прийняттого рівня резильєнтності під час створення, впровадження та експлуатаційного супроводу СІАД за обмежених обчислювальних, енергетичних і часових ресурсів;

– теоретичні положення дисертації доведено до прикладних інженерних методик, рекомендацій та інструментальних засобів, придатних для використання в організаціях, що здійснюють створення, впровадження або модернізацію інтелектуальних кіберфізичних систем з підвищеними вимогами до резильєнтності в

умовах впливу різнотипних збурюючих чинників.

Практичне значення отриманих результатів підтверджується актами впровадження (див. додаток В) розроблених принципів, моделей та методів під час виконання науково-дослідних проєктів та у навчальний процес Національного аерокосмічного університету «Харківський авіаційний інститут» (акт впровадження від 29.08.2025) і Сумського державного університету (акт впровадження від 20.08.2025), у галузевих підприємствах, зокрема в ТОВ «Jet Bee System» (акт впровадження від 20.12.2024), ТОВ «СМАРТ МАШІНЕРІ СОЛЮШНС» (акт впровадження від 07.10.2025), ТОВ «Конструкторське бюро “Північна Слобожанщина”» (акт впровадження від 05.09.2025) під час модернізації безпілотних систем, та в ТОВ «Molfar.AI» (акт впровадження від 05.05.2023), ТОВ «РОЗУМНІ ТЕХНОЛОГІЇ “ТИТУЛ”» (акт впровадження від 21.05.2023) під час розроблення та модернізації систем моніторингу інфраструктурних об’єктів та місцевості.

**Особистий внесок здобувача.** Основні наукові результати, що виносяться на захист, отримані здобувачем особисто. У роботах, опублікованих одноосібно, здобувачем отримано такі результати: [5] – метод мета-навчання для оптимізації резильєнтності та модель паралельної параметричної корекції модулів СІАД на основі адаптерних і мета-адаптерних надбудов; [15] – підхід до багатостадійної організації навчання класифікаційної СІАД з функціональним розділенням процедур формування ознакового подання та вирішувальних правил; [16] – положення щодо еволюційної оптимізації параметрів нейромережових моделей та функціонально-вартісного вибору компромісних рішень між функціональною ефективністю, ресурсними витратами і втратами від недостатнього рівня ефективності системи.

У працях, опублікованих у співавторстві, особистий внесок здобувача полягає в наведених нижче постановках задач, концептуальних і методичних положеннях, моделях, методах та алгоритмах, які безпосередньо відображають або становлять основу подальшого розвитку результатів дисертаційного дослідження, а саме: [1] – метод оцінювання резильєнтності СІАД на основі інтегрального показника, що обчислюється за траєкторією зміни функціональної ефективності під час адаптації; [2] – розроблення концептуальних положень і методології дослідження резильєнтності СІАД до різнотипних збурень, математичної моделі та алгоритму навчання класифікатора; формалізація сценаріїв змагальних впливів, ін’єкцій несправностей і дрейфу концепції як основи моделі формування збурюючих впливів; [3] – методологічні основи створення резильєнтних СІАД, таксономія збурень і вразливостей, онтологічне подання резильєнтності СІАД та підхід до її ймовірнісної верифікації; [4] – базові положення моделі керованої структурної реконфігурації нейромережової СІАД на основі проміжних відгалужень для раннього прийняття рішень; [6] – модель операцій машинного навчання для створення та експлуатаційної підтримки резильєнтних СІАД; [7] – базові положення нейромережової моделі СІАД з керованою структурною реконфігурацією на основі вентильних модулів та положення щодо багатоетапного навчання такої моделі; [8] – положення принципу зміни реконфігураційних надбудов та узгодження функціональної ефективності, робастності й обчислювальних витрат у динамічній моделі детектування.

У працях [9]–[11] особистий внесок здобувача полягає у постановці задач та методичному обґрунтуванні побудови класифікаційних систем за умов обмеженості й незбалансованості навчальних даних із послідовною організацією процесів формування моделі та її вирішувальних правил; [12] – постановка задачі та методичне обґрунтування побудови багатошарової моделі детектування шкідливого трафіку з урахуванням функціональної ефективності та обчислювальних витрат; [13] – постановка задачі та методичне обґрунтування ресурсоефективного навчання доменно-залежної частини нейромережевої моделі; [14] – концептуальне та методичне обґрунтування побудови автономної системи візуальної навігації з паралельним нейромережевим контуром корекції; [17] – концептуалізація та методичне обґрунтування підвищення робастності класифікаційної моделі шляхом поєднання регуляризованого ознакового подання із завадостійкими інформаційно-екстремальними вирішувальними правилами; [18] – методичне обґрунтування застосування регуляризації ознакового простору і контейнерного подання класів для підвищення робастності класифікаційних рішень; [19] – розроблення нейромережевої моделі СІАД з параметричною реконфігурацією на основі паралельної корекції модулів та еволюційного алгоритму реалізації методу мета-оптимізації резильєнтності; формалізація мета-цілі та процедури мета-оновлення параметрів, аналіз і узагальнення результатів; [20] – модель операцій машинного навчання для ресурсообмежених резильєнтних СІАД та положення щодо післярозгортальної адаптації на основі параметрично-ефективних реконфігураційних надбудов; [21] – постановка задачі та формування методичних вимог до ресурсоефективної адаптації попередньо навченої нейромережевої моделі шляхом локалізації корекції у малопараметричному контурі; [22] – постановка задачі та методичне обґрунтування поетапного формування ресурсощадної багатошарової моделі з функціональним розділенням процедур формування ознакового подання та побудови обчислювально ефективних вирішувальних правил; [23] – положення щодо керованої деградації СІАД як способу підтримання прийняттого рівня функціональної ефективності за недостатності ресурсів або дії збурюючих впливів; [24] – положення щодо динамічного реконфігурування обчислень нейромережевої СІАД для реалізації керованої деградації за ресурсних обмежень; [25] – програмна реалізація генератора альтернативних гіпотез для ймовірнісної верифікації резильєнтності класифікатора зображень до змагальних атак і пошкодження тензорів нейромережі; [26] – програмна реалізація навчання класифікатора зображень на змагальних зразках різного типу для підвищення робастності до шумових збурень і змагальних атак; [27] – програмна реалізація внутрішнього контуру адаптації параметрів нейромережевої моделі на траєкторіях впливу збурень для мета-оптимізації резильєнтності СІАД.

У роботах, опублікованих у співавторстві, співавторам належать такі результати: [1] – програмна реалізація окремих процедур навчання й експериментального дослідження нейромережевої моделі, опрацювання та візуалізація результатів (Москаленко А. С.); [2] – програмна реалізація та проведення експериментів із перевірки резильєнтності до ін'єкцій несправностей (Москаленко А. С.), програмна реалізація та проведення експериментів із перевірки резильєнтності до змагальних атак (Коробов А. Г.), програмна реалізація згорткової

нейромережі з інформаційним пляшковим горлом та гіперсферичними контейнерами (Зарецький М. О.); [3] – узагальнення положень інженерії гарантоздатності, функціональної безпеки та кіберрезильєнтності комп'ютерних систем (Харченко В. С.), опрацювання джерел щодо методів підвищення робастності нейромережевих класифікаторів (Москаленко А. С.), аналіз підходів до подання знань і предметних областей штучного інтелекту (Кузіков Б. О.); [4] – концептуальна постановка та наукове консультування експериментального дослідження (Харченко В. С.), програмна реалізація процедур моделювання змагальних атак, ін'єкцій несправностей і дрейфу концепції (Москаленко А. С.), валідація експериментальних процедур, опрацювання та візуалізація результатів (Петров С.); [6] – обґрунтування прикладних вимог до надійності, безпеки та контролю ризиків у медичних діагностичних системах (Харченко В. С.); [7] – наукове консультування та обґрунтування постановки дослідження ресурсообмеженої резильєнтної СІАД (Харченко В. С.), валідація теоретичних та експериментальних результатів (Семенов С.); [8] – аналіз методів детектування об'єктів, динамічних нейромереж і засобів підвищення робастності та програмна реалізація окремих процедур моделювання збурень (Коробов А. Г.), математичний опис прикладної моделі детектування та аналіз експериментальних залежностей між показниками mAP, FLOPs, рівнем динамічного стиснення і типом збурення (Москаленко Ю. В.).

У праці [9] Зарецькому М. О. належать формування вхідного математичного опису, розроблення глибокої моделі розпізнавання контексту відеоінспекції з урахуванням міжкадрових залежностей та проведення експериментальних досліджень; Москаленку А. С. – програмна реалізація процедур підготовки відеокадрів; Паничу А. О. – підготовка та структуризація експериментальних даних; Лисяку В. – аналіз предметних особливостей та інтерпретація результатів. У праці [10] Зарецькому М. О. належить багатоетапний метод навчання глибокої моделі з ініціалізацією вагових коефіцієнтів у процесі контрастного самонавчання; Москаленку А. С. – програмна реалізація процедур формування навчальних пар і пакетів даних; Коробову А. Г. – програмне моделювання та налаштування експериментів; Ковальському Я. Ю. – підготовка і структуризація розмічених даних. У праці [11] Зарецькому М. О. належать формування вхідного математичного опису, розроблення глибокої моделі розпізнавання рівня води з урахуванням міжкадрових залежностей та проведення експериментальних досліджень; Коробову А. Г. – підготовка даних і проведення обчислювальних експериментів; Ковальському Я. Ю. і Паничу А. О. – підготовка та структуризація даних; Шаєхову А. Ф. – аналіз предметних особливостей і уточнення складу класів; Семашку В. А. – перевірка експериментальних вибірок та первинне опрацювання результатів. Результати М. О. Зарецького, зазначені для [9]–[11], відображено в його захищеній дисертації.

У праці [12] Зарецькому М. О. належить алгоритм оцінювання ефективності інформаційно-екстремальних вирішувальних правил; Москаленку А. С. – аналіз методів розрідженого кодування, ансамблів дерев та інформаційно-екстремального навчання; Кудрявцеву А. М. – програмна підготовка експериментальних даних; Семашку В. А. – перевірка експериментальних процедур і первинне опрацювання результатів. У праці [13] Зарецькому М. О. належить аналіз існуючих алгоритмів

детектування об'єктів за умов ресурсних та інформаційних обмежень; Москаленку А. С. – аналіз підходів до використання попередньо навчених згорткових нейромереж та перенесення знань; Коробову А. Г. – програмна реалізація та експериментальне налаштування процедур детектування. У праці [14] Москаленку А. С. належить аналіз підходів до автономної візуальної навігації компактних БПЛА; Коробову А. Г. – комплексний критерій оптимізації параметрів вирішувальних правил системи автономної навігації; Семашку В. А. – підготовка графічних матеріалів і візуалізація результатів. Комплексний критерій оптимізації системи автономної навігації відображено у захищеній дисертації А. Г. Коробова.

У праці [17] Зарецькому М. О. належать розроблення моделі та алгоритму навчання для розпізнавання дефектів труб за орієнтації камери вперед уздовж труби та проведення експериментальних досліджень; Москаленку А. С. – аналіз методів регуляризації, дискретного подання ознак і завадостійкого кодування; Лисюку В. – підготовка даних та предметна інтерпретація результатів. У праці [18] Бойку М. В. належать розроблення моделей ідентифікації блоків бінарних даних на основі багат шарових згорткових нейромереж із додатковим регуляризуючим відгалуженням, проведення експериментів, аналіз та візуалізація результатів. У праці [19] Коробову А. Г. належать програмно-експериментальне забезпечення дослідження та реалізація окремих процедур моделювання збурень; Кудрявцеву А. М. – підготовка експериментальних сценаріїв і налаштування процедур еволюційного пошуку; Бойку М. В. – аналіз сучасних систем розпізнавання зображень в умовах збурюючих впливів. Результати М. В. Бойка, зазначені для [18] і [19], враховано відповідно до формулювань його захищеної дисертації.

У праці [20] Москаленку А. С. належать аналіз підходів MLOps та засобів налаштування моделей; Кудрявцеву А. М. – програмно-експериментальна реалізація сценаріїв збурюючих впливів; Москаленку Ю. В. – розроблення експериментального протоколу перевірки ресурсообмеженої СІАД на послідовних етапах життєвого циклу. У праці [21] Бойку М. В. належать аналіз існуючих методів ідентифікації блоків бінарних даних, розроблення методу навчання й адаптації моделі для підвищення точності класифікації нових зразків, мало представлених у навчальній вибірці, а також аналіз і візуалізація результатів. У праці [22] Москаленку А. С. належать аналіз методів розрідженого кодування, конкурентного навчання та дистиляції знань; Шаєхову А. Ф. – підготовка і перевірка наборів мережевого трафіку; Зарецькому М. О. – метод обчислення еталонного вектора кожного класу в двійковому просторі для синтезу інформаційно-екстремальних вирішувальних правил. Зазначені результати М. В. Бойка та М. О. Зарецького відображено в їхніх захищених дисертаціях.

У праці [23] Москвіну Д. О. належать аналіз відомих підходів до керованої деградації систем штучного інтелекту та підготовка матеріалів конференційної апробації; [24] – Москаленку Ю. В. належать аналіз архітектур динамічних нейромереж та підготовка експериментальних матеріалів, Рубану І. О. – програмна реалізація окремих експериментальних процедур і візуалізація результатів; [25] – Москаленку А. С. належать програмна реалізація процедур підготовки тестових зображень і формування пакетів даних, Коробову А. Г. – моделювання змагальних збурень, Зарецькому М. О. – моделювання пошкоджень тензорів нейромережі та

реєстрація результатів випробувань; [26] – Москаленку А. С. належать програмна реалізація підготовки навчальних і тестових вибірок, Зарецькому М. О. – моделювання шумових збурень, Коробову А. Г. – обчислення показників точності й робастності та первинне опрацювання результатів; [27] – Коробову А. Г. належать програмна реалізація окремих сценаріїв збурюючих впливів і експериментальних процедур, Зарецькому М. О. – підготовка вхідних даних і обчислення базових показників якості, Москаленку Ю. В. – реалізація сценаріїв серійних обчислювальних експериментів, Рубану І. О. – візуалізація динаміки показників якості під час адаптації.

Результати, віднесені до особистого внеску А. Г. Коробова, М. О. Зарецького та М. В. Бойка у їхніх захищених дисертаціях, не віднесено до особистого внеску В. В. Москаленка. До наукових результатів, що виносяться на захист як особистий внесок здобувача, віднесено лише належні В. В. Москаленку постановки задач, концептуальні й методологічні положення, моделі, методи та алгоритми зі спільних публікацій, а також результати їх подальшого розвитку й узагальнення в межах запропонованої методології створення резильєнтних СІАД, моделей параметричної та керованої структурної реконфігурації, методу мета-оптимізації резильєнтності та методу багатоетапного навчання.

**Апробація результатів дисертації.** Результати дослідження доповідалися на міжнародних та галузевих науково-технічних конференціях, на науково-технічних семінарах 2020–2025 рр., а саме: Міжгалузевому семінарі «Критичні комп'ютерні технології та системи» на кафедрі комп'ютерних систем і мереж Національного аерокосмічного університету «ХАІ» (м. Харків, 27 вересня 2021 р., 26 грудня 2024 р.); Міжнародному воркшопі «Advances & Challenges in Computing (A2C)» в Науково-дослідного інституту інтелектуальних комп'ютерних систем Західноукраїнського Національного університету (м. Тернопіль, 26 березня 2025 р.); Міжнародній науковій конференції «IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (7–9 вересня 2023 р., Дортмунд, Німеччина); Міжнародному воркшопі «Computer Modeling and Intelligent Systems (CMIS)» (27 квітня 2020, 27 березня 2024 р., м. Запоріжжя, Україна); Міжнародній науково-практичній конференції «Information Control Systems and Technologies (ICST-ODESA-2024) (23–25 вересня 2023 р., Одеса, Україна); Міжнародній науковій конференції молодих учених «Інформатика, Математика, Автоматика» (ІМА) (24–28 квітня 2023 р., 22–26 квітня 2024 р.).

**Публікації.** Результати дисертаційної роботи викладено в 27 наукових публікаціях, у тому числі: 2 розділи в колективних зарубіжних монографіях [15, 17] (всі проіндексовані у наукометричній базі даних Scopus), 1 одноосібна вітчизняна монографія [16]; 15 статей у періодичних наукових виданнях, серед яких 1 стаття у фаховому виданні групи Б [18], 5 статей у виданнях, що індексовані в БД SCOPUS та Web of Science, віднесених відповідно до класифікації SCImago Journal and Country Rank до першого або другого квартиля (Q1-Q2) [3, 4, 6, 7, 14]; 2 статті у виданнях, що індексовані в БД SCOPUS, віднесених відповідно до класифікації SCImago Journal and Country Rank до третього квартиля (Q3) [1, 8]; 7 статей у виданнях, що індексовані в БД SCOPUS та/або Web of Science, віднесених

відповідно до класифікації SCImago Journal and Country Rank до четвертого квартиля (Q4) чи без квартиля [2, 5, 9, 10, 11, 12, 13]; 6 публікацій у матеріалах і тезах наукових конференцій [19–24] (4 з яких [19–22] у наукових виданнях, проіндексованих у наукометричній базі даних Scopus); 3 публікації, які додатково відображають наукові результати дисертації, серед яких три свідоцтва про реєстрацію авторського права на твір (комп'ютерна програма) [25–27].

**Структура і обсяг дисертації.** Дисертація складається зі вступу, шести розділів, висновків, переліку використаних джерел і додатків. Повний обсяг дисертації становить 406 сторінок. Основна частина дисертації 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 та 7 додатків.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертаційного дослідження, сформульовано науково-прикладну проблему створення резильєнтних СІАД, що функціонують в умовах впливу різнотипних збурюючих чинників та ресурсних обмежень. Визначено мету, завдання, об'єкт, предмет і методи дослідження. Подано наукову новизну, практичне значення отриманих результатів, відомості про особистий внесок здобувача, апробацію, публікації, впровадження результатів, зв'язок роботи з науковими програмами, планами, темами та грантами. Наведено характеристику структури й обсягу дисертаційної роботи.

У **першому розділі** проведено аналіз проблеми створення резильєнтних систем інтелектуального аналізу даних. При цьому розкрито сутність концепції резильєнтних систем. Показано, що для таких систем резильєнтність не може бути зведена лише до надійності, відмовостійкості або кібербезпеки, оскільки має охоплювати здатність до підготовки, поглинання збурень, підтримання прийнятного рівня функціональної ефективності, відновлення та адаптації після впливу деструктивних чинників. Систематизовано основні класи загроз і збурюючих впливів на СІАД, зокрема апаратні та програмні збої, ін'єкції бітових інверсій у параметри й проміжні обчислення нейромережних моделей, змагальні атаки на дані та модель, дрейф даних і концепцій, поява новизни, даних поза навчальним розподілом, пропуски та помилки в даних. Виявлено, що одна й та сама СІАД у процесі життєвого циклу може зазнавати впливу різних за природою збурюючих чинників, які потребують різних механізмів виявлення, поглинання, корекції, адаптації або відновлення. Це обґрунтовує необхідність не ізольованого розгляду окремих типів загроз, а формування узгодженого підходу до їх моделювання, оцінювання та врахування під час створення резильєнтних СІАД.

Показано, що в критичних, кіберфізичних, медичних, безпекових, фінансових та інших предметних галузях недостатній рівень резильєнтності може призводити до істотних функціональних, економічних, соціальних, медичних, безпекових або правових наслідків. Встановлено, що для таких умов недостатньо забезпечити лише високу точність моделей на етапі навчання або валідації; необхідною є підтримка функціональної ефективності СІАД протягом життєвого циклу – під час

розгортання, експлуатації, моніторингу, парирування збурень і дрейфу та, за потреби, керованої деградації. Це обґрунтовує доцільність розвитку MLOps-орієнтованого контуру підтримки резильєнтності СІАД у реальних умовах функціонування.

Проаналізовано основні підходи до створення резильєнтних СІАД, зокрема структурну надмірність, диверсність, робастну оптимізацію, змагальне навчання, засоби виявлення дрейфу та даних поза навчальним розподілом, активне й безперервне навчання, доменну адаптацію, мета-навчання, адаптивне виведення та керовану реконфігурацію нейромережних моделей. Виявлено, що наявні методи здебільшого орієнтовані на окремі типи загроз або окремі етапи резильєнтного функціонування, а їх поєднання може призводити до несумісності цілей, надмірних обчислювальних витрат або зниження стійкості до інших типів збурень.

Обґрунтовано доцільність розгляду параметричної та структурної реконфігурації як ресурсоефективних механізмів керованої зміни поведінки СІАД без повного перенавчання або перебудови базової моделі. Показано, що параметрично-ефективна корекція окремих підмножин параметрів або адаптерних надбудов може використовуватися для адаптації та оптимізації високорівневих показників, тоді як динамічні моделі з перемиканням між гілками, раннім виходом або зміною активної частини обчислювального графа створюють передумови для узгодження резильєнтності, функціональної ефективності та обчислювальних витрат.

Таким чином, на основі виявлених суперечностей між потребою в комплексній резильєнтності СІАД, фрагментарністю наявних засобів її оцінювання й забезпечення та жорсткими ресурсними обмеженнями обґрунтовано необхідність формування єдиної методологічної основи створення резильєнтних СІАД. Така методологія має поєднувати моделі збурюючих впливів, інтегральне оцінювання резильєнтності, мета-оптимізацію, адаптацію, параметричну та структурну реконфігурацію, а також інформаційно-технологічні засоби забезпечення резильєнтності протягом життєвого циклу СІАД.

**Другий розділ** дисертації присвячений розробленню методологічних основ створення резильєнтних СІАД, що функціонують за впливу різнотипних збурюючих чинників і ресурсних обмежень. Методологія охоплює концепцію, принципи, моделі, методи та інформаційні технології оцінювання і забезпечення резильєнтності. Її основу становлять принципи всебічного врахування синергетичності впливу збурюючих чинників, мета-оптимізації резильєнтності та зміни реконфігураційних надбудов. Принцип всебічного врахування синергетичності передбачає оцінювання узгодженої роботи всього комплексу механізмів забезпечення резильєнтності за дії кожного класу збурень. При цьому враховуються негативна синергетичність, пов'язана з конфліктами між окремими засобами захисту та надмірними ресурсними витратами, і позитивна синергетичність, що виникає під час спільної оптимізації системи на множині різнотипних збурень. Принцип мета-оптимізації визначає резильєнтність як мета-ціль, що характеризується функціоналом над траєкторією зміни функціональної ефективності під час поглинання збурення та подальшої адаптації. Принцип зміни реконфігураційних надбудов задає конструктивну основу керованої параметричної

та структурної реконфігурації СІАД за обмежених обчислювальних, часових та енергетичних ресурсів.

Ієрархію та взаємозв'язок елементів розробленої методології наведено на рисунку 1.

Концептуальний рівень конкретизується системою принципів, які визначають вимоги до моделей формування збурень, операцій машинного навчання та нейромережових моделей із параметричною і структурною реконфігурацією. На методичному рівні передбачено оцінювання та мета-оптимізацію резильєнтності, а також багатоетапне навчання моделей із керованою структурною реконфігурацією. Результати інтегруються в інформаційні технології оцінювання та забезпечення резильєнтності СІАД.

Запропонована модель формування синтетичних збурюючих впливів для комплексного оцінювання резильєнтності СІАД, у якій різні класи збурень подано сімейством параметризованих операторів

$$\tau_{s,\zeta}: a \mapsto a', \zeta \in \Omega_s(b), \quad (1)$$

де  $s$  – клас збурення;  $a, a'$  – початковий і збурений носії впливу, якими можуть бути вхідні дані, параметри моделі, проміжні тензори або розподіли даних;  $\zeta$  – параметри конкретної реалізації;  $\Omega_s(b)$  – область допустимих значень, обмежена бюджетом  $b$ .

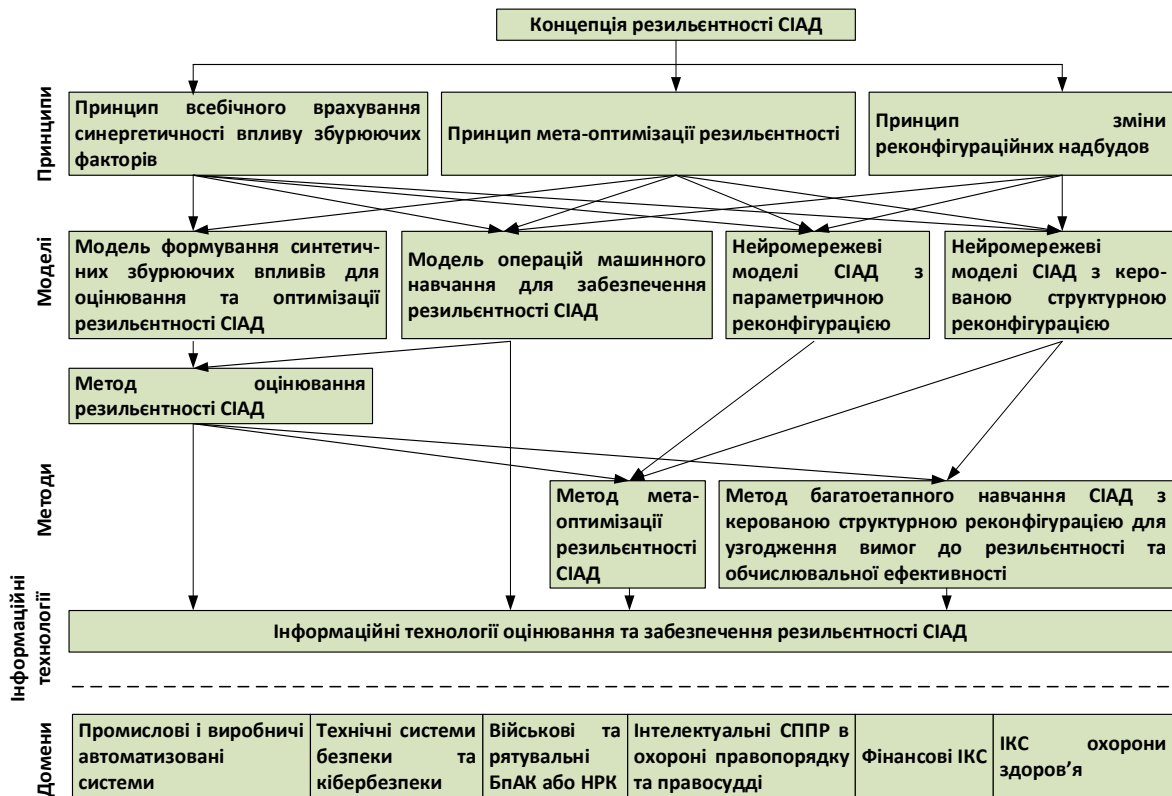


Рисунок 1 – Структура і взаємозв'язок елементів методології

Деструктивність сформованого впливу оцінюється за зміною показника функціональної ефективності СІАД:

$$Q_s(\zeta, M) = \chi(Q(M_{s,\zeta}, D_{s,\zeta}^{val})), \quad (2)$$

де  $Q(\cdot)$  – показник функціональної ефективності, що обчислюється на валідаційній

вибірці  $D_{s,\zeta}^{val}$ ;  $\chi(\cdot)$  – монотонне перетворення, яке приводить показник  $Q(\cdot)$  до форми, в якій більші значення відповідають більшій деградації функціональної ефективності;  $M_{s,\zeta}$  – стан або режим виконання моделі під дією збурення  $\tau_{s,\zeta}$ .

Для стрес-тестування здійснюється пошук найбільш несприятливої допустимої реалізації збурення, що реалізується за допомогою еволюційної стратегії СМА-ES

$$\zeta^* = \arg \max_{\zeta \in \Omega_s(b)} Q_s(\zeta, M). \quad (3)$$

Це дає змогу за єдиною процедурою формувати репрезентативні та граничні реалізації змагальних атак, пошкоджень параметрів і проміжних обчислень, а також здійснювати пошук даних поза межами навчального розподілу.

Розроблено метод оцінювання резильєнтності СІАД, який ґрунтується на аналізі траєкторії зміни показника функціональної ефективності після дії збурення та в процесі адаптації в межах установленого ресурсного бюджету. Крива резильєнтності відображає глибину просідання функціональної ефективності, час реагування і відновлення, втрати ефективності, робастність та швидкість відновлення системи (рис. 2). Інтегральний показник резильєнтності узагальнює ці характеристики протягом заданого бюджету кроків адаптації.

Для одночасного врахування змінних часу і функціональної ефективності під час оцінювання резильєнтності системи були розроблені різноманітні варіанти інтегральних показників. Ці показники, як правило, характеризують різницю або відношення номінальної функціональної ефективності та втрати функціональної ефективності в часі внаслідок збурюючих впливів. Для зручності інтегральний показник можна виразити у нормалізованій формі

$$R = \frac{\int_{t_0}^{t_1} Q(t) dt}{\int_{t_0}^{t_1} Q^{no\ min\ al}(t) dt}, \quad t_1 = t_0 + T_c \quad (4)$$

де  $Q(t)$  – нормалізований додатньо визначений показник функціональної ефективності під час відновлення і адаптації, поданий у шкалі, в якій більшому значенню показника відповідає вищий рівень функціональної ефективності системи;

$Q^{no\ min\ al}(t)$  – нормалізований додатньо визначений показник функціональної ефективності в нормальних (номінальних, штатних) умовах, що вводиться до формули для відображення значень інтегрального показника резильєнтності в інтервал  $[0, 1]$ ;

$t_0$  – момент початку дії збурюючого впливу або початку інтервалу оцінювання резильєнтності, з якого фіксується траєкторія зміни функціональної ефективності СІАД;

$T_c$  – бюджет кроків адаптації, що обирається з точки зору допустимих витрат ресурсів і втрат внаслідок деградації функціональної ефективності.

Запропонована схема емпіричного тестування передбачає формування заданого типу збурення, тестування й адаптацію моделі протягом обмеженої кількості кроків, побудову кривої функціональної ефективності та обчислення інтегрального показника резильєнтності (рис. 3).

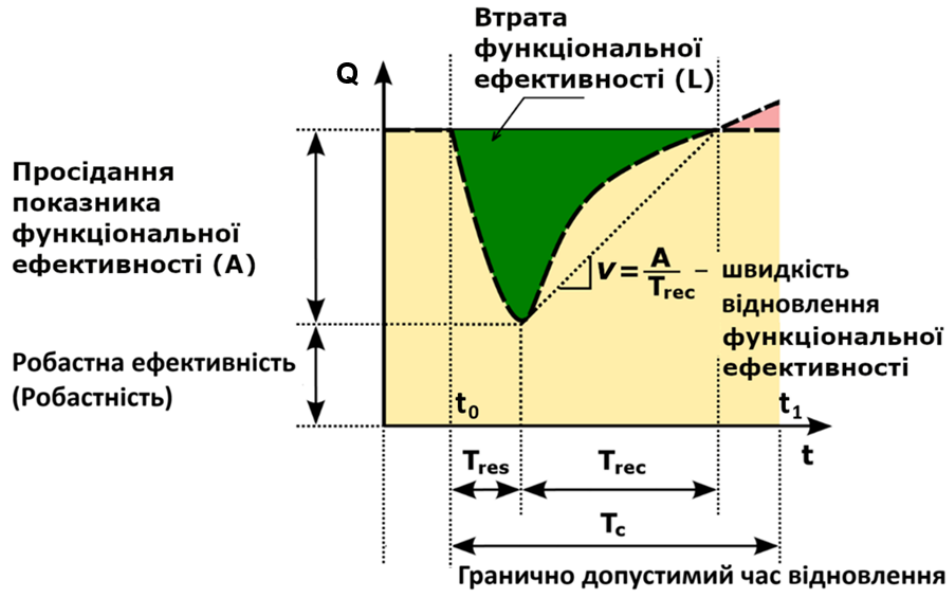


Рисунок 2 – Ілюстрація кривої резильєнтності та основних її показників

Для тестування готується набір даних  $\mathcal{D}$  та модель  $M$ , для яких може бути сформовано збурюючий вплив типу  $s$  з параметрами  $\zeta$  на основі пошукового алгоритму з параметрами  $\beta$ . Крива резильєнтності будується для  $T_c$  кроків адаптації з розміром міні-пакету  $n$ . На всій траєкторії адаптації обчислюється показник функціональної ефективності  $Q(t)$  і один раз на всю траєкторію рахується інтегральний показник резильєнтності  $R(Q, T_c)$ . Для серії кривих резильєнтності обчислюються статистичні характеристики, наприклад медіанне значення (MED) та міжквартильний розмах (IQR).

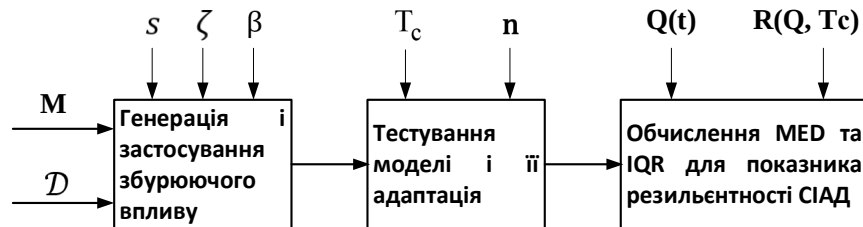


Рисунок 3 – Схема емпіричного тестування СІАД на резильєнтність

Для статистичного підтвердження виконання вимог до резильєнтності запропоновано метод РАС-верифікації, у якому подія недостатньої резильєнтності визначається умовою

$$R_{\tau}(T_c) < R_{\min}(T_c), \quad (5)$$

де  $R_{\min}(T_c)$  – мінімально допустиме значення інтегрального показника резильєнтності за встановленого бюджету адаптації  $T_c$ , визначене на основі допустимого часу відновлення, граничної траєкторії функціональної ефективності та бюджету накопичених втрат.

Вимога РАС-верифікації резильєнтності СІАД формулюється як

$$P(R_{\tau}(T_c) < R_{\min}(T_c)) \leq \Theta, \quad (6)$$

де  $R_{\tau}(T_c)$  – інтегральний показник резильєнтності СІАД до реалізації збурення  $\tau$ , обчислений у межах бюджету адаптації  $T_c$ ;  $R_{\min}(T_c)$  – мінімально допустиме

значення показника резильєнтності за цього бюджету адаптації;  $\Theta$  – максимально допустима ймовірність невиконання встановленої вимоги.

Умова (6) має підтверджуватися з рівнем довіри не меншим ніж  $1 - \delta$ , де  $\delta$  визначає допустимий ризик помилкового висновку. Для практичної перевірки умови (6) ймовірність недостатньої резильєнтності оцінюється за результатами серії стохастичних випробувань

$$\hat{p}_N = \frac{1}{N} \sum_{i=1}^N I \{R_i \leq R_{\min}(T_c)\}, \quad (7)$$

де  $N$  – кількість проведених випробувань;  $R_i$  – значення інтегрального показника резильєнтності, отримане в  $i$ -му випробуванні;  $I\{\cdot\}$  – індикаторна функція, яка дорівнює одиниці в разі невиконання вимоги до резильєнтності та нулю в іншому випадку;  $\hat{p}_N$  – емпірична оцінка ймовірності недостатньої резильєнтності.

Для скорочення обсягу випробувань використано послідовність альтернативних інтервалів  $(\theta_{1j}, \theta_{2j})$ , для кожного з яких необхідна кількість тестів визначається за оцінкою Чернова:

$$N_j = \frac{(\sqrt{3\theta_{1j}} + \sqrt{2\theta_{2j}})^2}{(\theta_{2j} - \theta_{1j})^2} \ln \frac{1}{\delta_j}, \quad \sum_j \delta_j \leq \delta. \quad (8)$$

Послідовність формування альтернативних інтервалів, визначення необхідної кількості випробувань та перевірки умов прийняття або відхилення гіпотези наведено на рисунку 4.

Завдяки залежності  $N_j \sim (\theta_{2j} - \theta_{1j})^{-2}$  широкі початкові інтервали дають змогу достроково підтвердити або спростувати вимогу, якщо оцінка  $\hat{p}_N$  достатньо віддалена від порога  $\Theta$ . Параметри верифікації визначаються з урахуванням критичності конкретної функції СІАД, допустимого часу відновлення, доступних обчислювальних та енергетичних ресурсів, бюджету накопичених втрат і загального бюджету ризику. Верифікація застосовується як завершальний етап оцінювання для підтвердження відповідності вибраної конфігурації СІАД установленим вимогам.

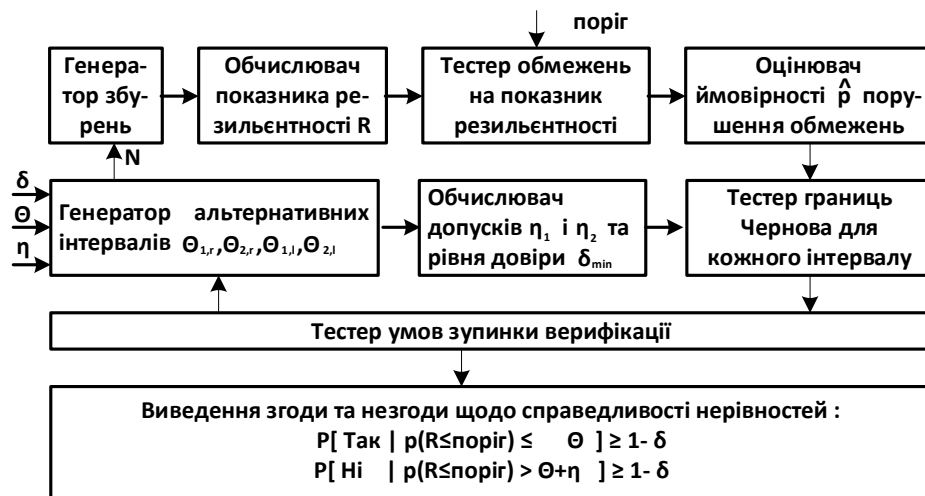


Рисунок 4 – Функціональна схема реалізації методу верифікації резильєнтності СІАД на основі статистичного тестування РАС-умов

Для підтримання резильєнтності СІАД у процесі експлуатації удосконалено модель операцій машинного навчання шляхом введення постфактум калібрування невизначеності, моніторингу стану даних і функціональної ефективності, адаптації під час тестування та переходу до керованої деградації. Послідовність відповідних операцій наведено на рисунку 5.

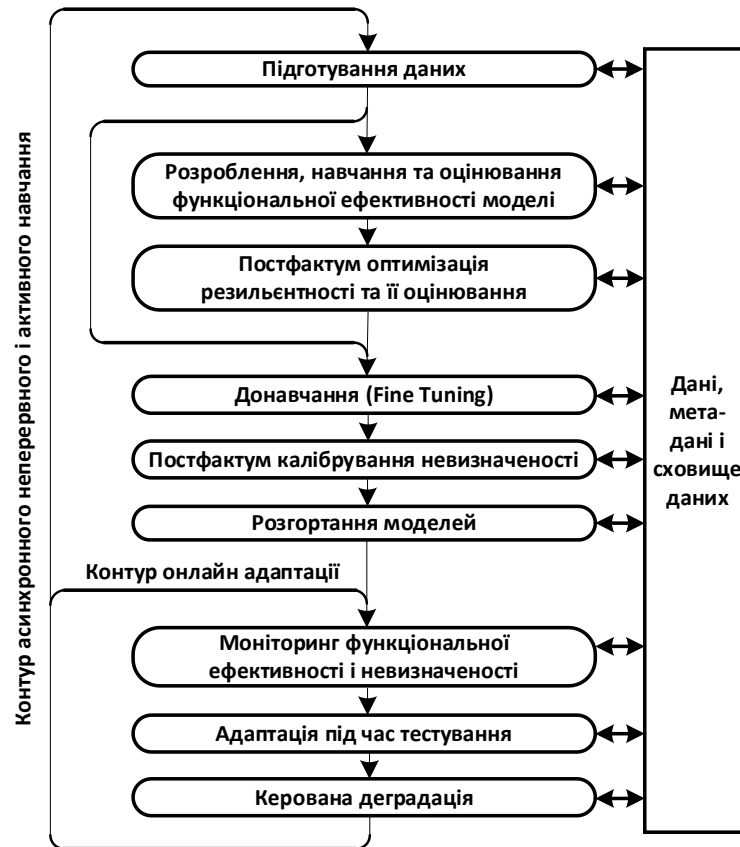


Рисунок 5 – Операції машинного навчання для забезпечення резильєнтності СІАД

Після розгортання СІАД здійснюються безперервний моніторинг вхідних даних, прогнозів і рівня невизначеності, а також виявлення дрейфу та інших збурень. За наявності розмічених даних або зворотного зв'язку оператора виконується швидка адаптація релевантних модулів. Якщо нові дані не мають розмітки, але характеризуються підвищеною невизначеністю, застосовується адаптація під час тестування. При цьому коригуються переважно релевантна підмножина параметрів базової моделі або параметри реконфігураційних надбудов, що зменшує обчислювальні витрати й ризик руйнівного перенавчання. Якщо адаптація не забезпечує прийнятної достовірності рішення, система переходить до спрощеного режиму функціонування, відмови від рішення або залучення оператора.

Отже, удосконалена MLOps-модель забезпечує незалежне розроблення базової функціональності та механізмів резильєнтності, а також їх узгоджену взаємодію під час експлуатації, що спрощує модернізацію СІАД і забезпечує ресурсоефективне поглинання збурень, відновлення та керовану деградацію.

У **третьому розділі** розроблено та досліджено нейромережну модель СІАД із параметричною реконфігурацією модулів, призначену для ресурсоефективного

поглинання збурень і швидкого відновлення функціональної ефективності без повного перенавчання базової нейромережі.

Запропонований підхід ґрунтується на локалізації адаптивних змін у додаткових реконфігураційних надбудовах. Параметри попередньо навченої базової моделі зберігаються фіксованими, тоді як параметри адаптерів налаштовуються відповідно до поточних умов. Це дає змогу зменшити кількість змінюваних параметрів і тривалість адаптації, а також знизити ризик катастрофічного забування раніше сформованих властивостей моделі.

Для узгодження вимог стабільності й пластичності удосконалено модель паралельної корекції шляхом розділення параметрів коригувальної гілки за функціональними ролями та часовими масштабами налаштування. Замість одного адаптера запропоновано каскадну композицію «мета-адаптер – адаптер – мета-адаптер»:

$$x_{k+1} = B_k(x_k) + \Delta_k(x_k), \quad \Delta_k(x_k) = M_{2,k} \left( A_k(M_{1,k}(x_k)) \right), \quad (9)$$

де  $B_k(\cdot)$  – заморожений оператор -го блока базової нейромережі;

$A_k(\cdot)$  – «швидкий» адаптер із параметрами  $\varphi_k$ , які можуть оперативно донавчатися відповідно до поточних умов;

$M_{1,k}(\cdot)$  і  $M_{2,k}(\cdot)$  – «повільні» мета-адаптери з параметрами  $\omega_{1,k}$  та  $\omega_{2,k}$ , які налаштовуються на множині сценаріїв збурень.

Перший мета-адаптер виконує мета-кероване узгодження вхідних ознак, формуючи представлення, придатне для швидкої та стабільної адаптації центрального адаптера. Другий мета-адаптер калібрує сформовану поправку перед її додаванням до виходу базового модуля та обмежує надмірні зміни представлень. Отже, мета-адаптери акумулюють узагальнені стратегії протидії збуренням, а центральний адаптер забезпечує оперативне відновлення функціональної ефективності в конкретному експлуатаційному сценарії. Схему запропонованої корекції наведено на рисунку 6.

Для реалізації коригувальних надбудов досліджено повнозв'язні, згорткові, залишкові та полегшені згорткові архітектури адаптерів. Найбільш поширеною є bottleneck-архітектура, у якій корекція формується через проміжний простір малої розмірності

$$A(x) = W_{\uparrow} \sigma(W_{\downarrow} x), \quad (10)$$

де  $W_{\downarrow} \in \mathbb{R}^{m \times d}$  – матриця зменшення розмірності;  $W_{\uparrow} \in \mathbb{R}^{d \times m}$  – матриця відновлення розмірності;  $\sigma(\cdot)$  – нелінійне перетворення;  $m \ll d$ .

Кількість параметрів такого адаптера становить приблизно  $2dm$ , що істотно менше за  $d^2$  параметрів повнорозмірного коригувального перетворення. Bottleneck-структура виконує не лише функцію скорочення ресурсних витрат, але й роль структурної регуляризації, оскільки обмежує поправку невеликою кількістю латентних напрямів у просторі ознак.

Для просторово організованих представлень у проведених дослідженнях переважно використано згорткові адаптери зі стисканням каналів. Базові

повнозв'язний і згортковий варіанти наведено на рисунку 7; залишкові та полегшені 1D-згорткові реалізації розглядалися як альтернативні архітектури.

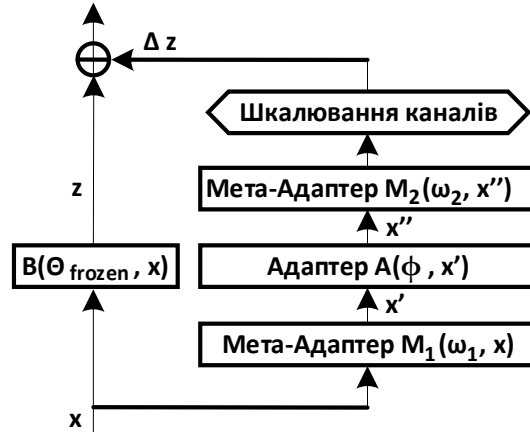


Рисунок 6 – Схема паралельної корекції модулів базової моделі на основі адаптерів і мета-адаптерів

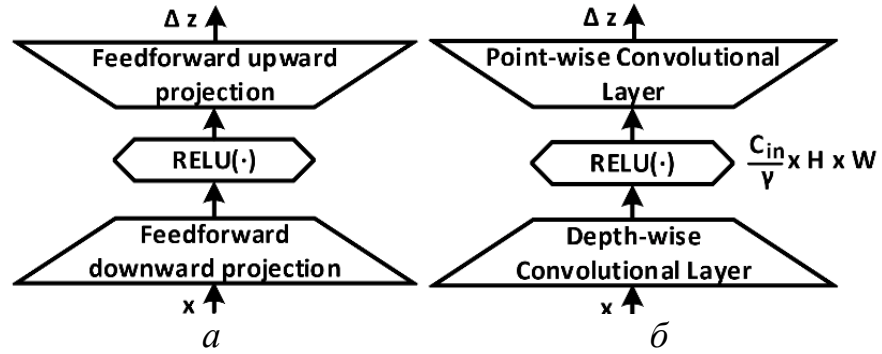


Рисунок 7 – Поширені архітектури адаптерів: а – двошаровий повнозв'язний адаптер зі стисканням розмірності; б – двошаровий згортковий адаптер зі стисканням каналів

Для безпечного підключення адаптерів використано нейтральну ініціалізацію, за якої на початку навчання  $A(x) \approx 0$ , тому вихід реконфігурованого модуля залишається близьким до виходу базової моделі. Внесок адаптера регулюється коефіцієнтом масштабу  $\alpha$

$$y = B(x) + \alpha A(x). \quad (11)$$

Коефіцієнти масштабу дозволяють обмежувати потенційно негативний вплив ще не налаштованої або пошкодженої коригувальної гілки.

Експериментальні дослідження проведено з використанням базової моделі ResNet-18 і наборів даних CIFAR-10 та CIFAR-100. CIFAR-10 використовувався для формування базової моделі, а з CIFAR-100 формувалися нові задачі для перевірки швидкої адаптації. Під час експлуатаційної адаптації параметри базової моделі та мета-адаптерів фіксувалися, а змінювалися лише параметри центральних адаптерів.

Досліджувалися ін'єкції випадкових бітових інверсій у параметри нейромережі, змагальні атаки ухилення та їх композитний вплив. Частка пошкоджених ваг змінювалася від 0,1 до 0,6; для змагальних збурень використовувалася безградієнтна атака СМА-ES. Для кожного рівня збурення результати усереднювалися за 100 стохастичними реалізаціями.

За ін'єкції інверсії одиничних бітів із часткою пошкоджених ваг 0,6 точність базової моделі становила 75,4 %, тоді як використання запропонованої параметричної реконфігурації забезпечило 82,3 % та інтегральний показник резильєнтності 0,877. За змагальної атаки СМА-ES точність базової моделі становила 74,8 %, а запропонованої моделі – 76,5 % за значення інтегрального показника резильєнтності 0,851.

Найбільш виражену перевагу отримано за композитного впливу різнотипних збурень: одночасна дія змагального збурення та ін'єкції бітових інверсій із часткою пошкоджених ваг 0,6 знижувала точність базової моделі до 55,8 %, тоді як модель із паралельною параметричною реконфігурацією забезпечувала 75,9 % за інтегрального показника резильєнтності 0,844. Це підтверджує здатність реконфігураційної надбудови зменшувати негативний синергетичний ефект одночасної дії різнотипних збурень.

Таким чином, у третьому розділі удосконалено нейромережну модель СІАД із параметричною реконфігурацією завдяки реалізації паралельної корекції модулів у вигляді каскадної адаптерної надбудови та розділенню параметрів за режимами мета-оптимізації й оперативної адаптації. Запропонована модель забезпечує ресурсоефективне підвищення резильєнтності до різнотипних і композитних збурюючих впливів.

**У четвертому розділі** розроблено та досліджено нейромережні моделі СІАД з керованою структурною реконфігурацією, під якою розуміється здатність моделі змінювати активну частину обчислювального графа залежно від властивостей вхідних даних, типу та інтенсивності збурюючого впливу і доступного ресурсного бюджету. На відміну від параметричної реконфігурації, за якої структура моделі залишається незмінною, керована структурна реконфігурація передбачає адаптивний вибір глибини, маршруту та складу виконуваних обчислень.

Запропоновано два взаємодоповнювальні способи її реалізації. Перший, макроструктурний, ґрунтується на застосуванні проміжних відгалужень і забезпечує адаптивний вибір глибини виведення та рівня деталізації рішення. Другий, мікроструктурний, передбачає використання вентильних модулів для активації або пропуску окремих структурних блоків базової нейромережі. Поєднання цих способів створює передумови для узгодження функціональної ефективності, резильєнтності та обчислювальних витрат СІАД.

Для реалізації макроструктурної реконфігурації розроблено багатосекційну модель резильєнтного класифікатора зображень, уздовж спільного екстрактора ознак якого розташовано проміжні голови прийняття рішень. Кожна голова формує самостійний прогноз на відповідному рівні глибини, що дає змогу завершувати обчислення після досягнення заданої достовірності або продовжувати оброблення для складніших чи збурених зразків. Архітектуру моделі наведено на рисунку 8.

Для реалізації керованої деградації проміжним виходам поставлено у відповідність різні ієрархічні рівні класифікації. Якщо достовірність деталізованого прогнозу є недостатньою, модель переходить до узагальненого рішення на рівні суперкласу. Якщо прийнятний рівень достовірності не досягається на жодному рівні, формується відмова від прийняття рішення, а відповідний зразок передається до буфера для подальшого маркування або адаптації.



Для  $k$ -го блока з одним обхідним з'єднанням формування вихідного тензора під час навчання описується виразом

$$z_k = z_{k-1} + g_k(z_{k-1})f_k(z_{k-1}), \quad (13)$$

де  $z_{k-1}$  і  $z_k$  – відповідно вхідний і вихідний тензори блока;  $f_k(\cdot)$  – перетворення, реалізоване основним структурним блоком;  $g_k(\cdot)$  – функція вентильного модуля, яка під час навчання формує релаксоване значення в інтервалі від нуля до одиниці.

У режимі виведення релаксоване рішення замінюється бінарним, тому активна структура моделі визначається правилом

$$z_k = \begin{cases} z_{k-1}, & g_k(z_{k-1}) = 0, \\ z_{k-1} + f_k(z_{k-1}), & g_k(z_{k-1}) = 1. \end{cases} \quad (14)$$

Отже, за нульового виходу вентильного модуля основний блок пропускається, а вхідний тензор передається через обхідне з'єднання; за одиничного виходу блок виконується повністю.

Вентильний модуль може також керувати складеною структурною одиницею, що містить декілька перетворень з окремими обхідними з'єднаннями. Такий варіант використано для трансформерних енкодерів, у яких блок багатоголової самоуваги та багат шаровий перцептрон мають власні залишкові з'єднання. Схему структурної одиниці з двома обхідними з'єднаннями наведено на рисунку 9.

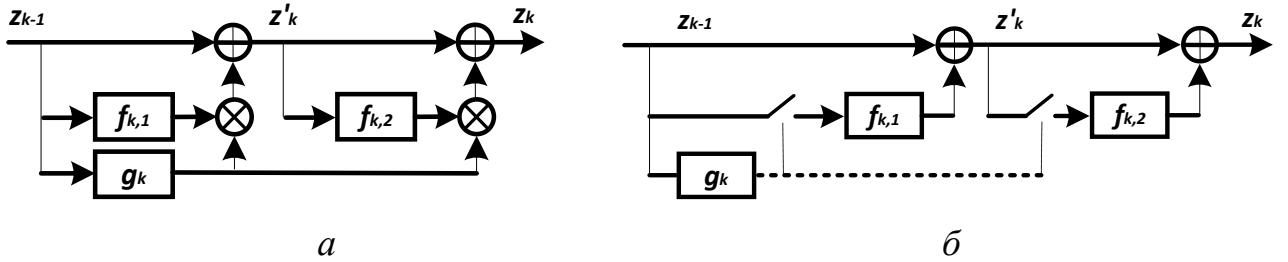


Рисунок 9 – Схематична ілюстрація структурних одиниць динамічної нейронної мережі з двома обхідними з'єднаннями: а – режим навчання; б – режим виведення

Оскільки рішення про виконання або пропуск блока є дискретним і в безпосередній формі недиференційовним, для навчання вентильних модулів використано релаксацію Gumbel–Softmax. На етапі навчання вона забезпечує стохастичне дослідження альтернативних маршрутів обчислень і проходження градієнта через вентильну надбудову, а в режимі виведення замінюється жорстким бінарним рішенням. Архітектуру вентильного модуля наведено на рисунку 10.

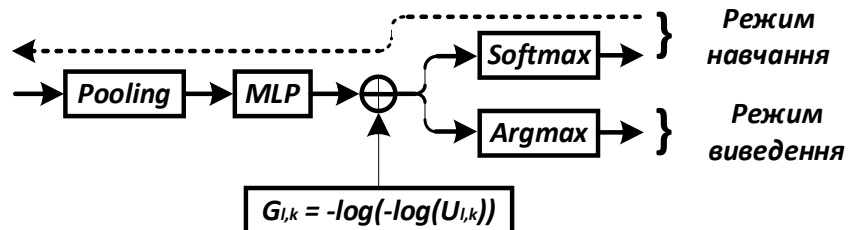


Рисунок 10 – Архітектура вентильного модуля нейронної мережі для реалізації керованої структурної реконфігурації

Вентильний модуль містить засіб агрегування вхідного тензора та малорозмірний багатoshаровий перцептрон із двома виходами, які відповідають рішенням про пропуск або виконання керованого блока.

Для згорткових мереж агрегування реалізовано глобальним усередненням просторових ознак. У візуальному трансформері послідовність токенів попередньо перетворюється на двовимірну сітку, після чого обробляється легкою згорткою та операцією зменшення просторової розмірності. Такий спосіб під'єднання вентиля до входу трансформерного енкодера наведено на рисунку 11.

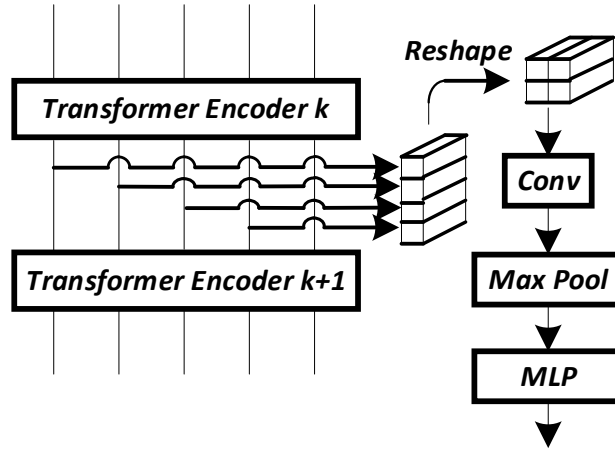


Рисунок 11 – Під'єднання вентильного модуля до входу трансформерного енкодера

Навчання моделі з вентильними модулями здійснюється за композитною функцією втрат

$$L = \lambda_{\text{base}} L_{\text{base}} + \lambda_{\text{usage}} L_{\text{usage}}, \quad (15)$$

де  $L_{\text{base}}$  – функція втрат основної задачі аналізу даних;  $L_{\text{usage}}$  – ресурсна регуляризаційна складова;  $\lambda_{\text{base}}$  і  $\lambda_{\text{usage}}$  – вагові коефіцієнти відповідних складових.

Ресурсний регуляризатор визначено як

$$L_{\text{usage}} = \frac{1}{K} \sum_{k=1}^K \left( \frac{1}{n} \sum_{i=1}^n g_{k,i} - t_k \right)^2, \quad (16)$$

де  $K$  – кількість вентильних модулів;  $n$  – кількість зразків у навчальному мініпакеті;  $g_{k,i}$  – вихід  $i$ -го вентиля для  $k$ -го зразка;  $t_k$  – задана цільова середня частота виконання  $k$ -го блока.

Якщо цільовий рівень є однаковим для всіх блоків, приймається  $t_k = t$ , де  $t$  – коефіцієнт динамічного стиснення. Наприклад, значення  $t = 0,6$  задає режим, за якого модель у середньому активує близько 60 % керованих блоків.

У моделі також використано функцію активації LeakyReLU6, яка обмежує великі додатні значення активацій і водночас зберігає ненульову градієнтну провідність у від'ємній області. Обмеження діапазону проміжних представлень зменшує ризик лавиноподібного поширення аномальних значень, спричинених змагальними збуреннями або пошкодженням параметрів, тоді як ненульовий

від’ємний нахил сприяє ефективному донавчанню та адаптації. У вентиляльній мережі це стабілізує як основний прогноз, так і рішення модулів структурного перемикавання.

Експериментальне дослідження моделі з проміжними відгалуженнями виконано на наборах даних CIFAR-10 і CIFAR-100 за умов ін’єкції бітових несправностей, змагальних атак, появи нових класів і реального дрейфу концепцій. Встановлено, що класифікатор верхнього ієрархічного рівня краще поглинає збурення та забезпечує швидше відновлення, хоча формує менш деталізований результат. Це підтверджує доцільність використання ієрархічного прогнозування як механізму керованої деградації.

Коли частка тензорів з ін’єкцією інверсії одиничних біт (bit-flip) становила 0,6 для CIFAR-10 точність нижнього ієрархічного рівня після збурення становила 0,532, а після адаптації підвищувалася до 0,851. Для рівня суперкласів відповідні значення становили 0,721 і 0,881. Для CIFAR-100 точність нижнього рівня відновлювалася з 0,357 до 0,758, а точність на рівні суперкласів – з 0,665 до 0,910.

Після додавання нових класів відновлення функціональної ефективності потребувало не більше 56 мініпакетів для CIFAR-10 та 62 мініпакетів для CIFAR-100. За реального дрейфу між трьома класами максимальна кількість кроків становила відповідно 95 і 97, що більш ніж у 32 рази менше за кількість кроків навчання моделі з початкового стану.

Абляційне дослідження підтвердило суттєвий внесок проміжних виходів у резильєнтність. За частки пошкоджених тензорів 0,3 їх використання підвищило точність моделі на базі ResNet-блоків з 0,802 до 0,852 і скоротило медіанну кількість кроків відновлення зі 151 до 25. За змагальної  $L_\infty$ -атаки з рівнем збурення  $\varepsilon = 3$  точність зросла з 0,723 до 0,762, а кількість кроків відновлення зменшилася з 270 до 41. Отже, проміжні відгалуження виконують не лише функцію раннього завершення обчислень, а й формують додаткові точки відновлення та інформативний навчальний сигнал для ранніх шарів мережі.

Залежність обчислювальної ефективності багатовихідної моделі від інтенсивності збурень наведено на рисунку 12. Підвищення інтенсивності змагальної атаки або частки ушкоджених тензорів збільшує відношення  $T_{\text{adap}}/T_{\text{full}}$ , оскільки для формування надійного рішення модель частіше залучає глибші секції.

Експериментальні дослідження моделей CIAД з керованою структурною реконфігурацією проводилися для різних типів та інтенсивностей збурень і підтвердили ефективність обох запропонованих механізмів – проміжних відгалужень і вентиляльного керування активною структурою нейромережі.

Окремо досліджено вентиляльні моделі на базі ResNet-110 та DeiT-S, для яких керована структурна реконфігурація реалізується шляхом вибіркового виконання структурних блоків. За коефіцієнта динамічного стиснення 0,6 в умовах ін’єкції несправностей модель ResNet-110 забезпечила точність 87,9 % при обчислювальних витратах 310,66 MFLOPs, що приблизно на 39 % менше порівняно з виконанням повної мережі. Для DeiT-S за аналогічного режиму отримано точність 89,2 % при 6,55 GFLOPs, тобто зі скороченням обчислювальних витрат приблизно на 38 %.

За змагальних атак вентиляльна ResNet-110 забезпечила точність 86,8 % при 312,01 MFLOPs, що відповідає зменшенню обчислювальних витрат приблизно на 39 %, а DeiT-S – точність 87,1 % при 6,95 GFLOPs зі скороченням витрат приблизно на

34 %. Отримані результати підтверджують, що керована структурна реконфігурація дозволяє адаптивно скорочувати обсяг виконуваних обчислень без суттєвої втрати функціональної ефективності в умовах збурень.

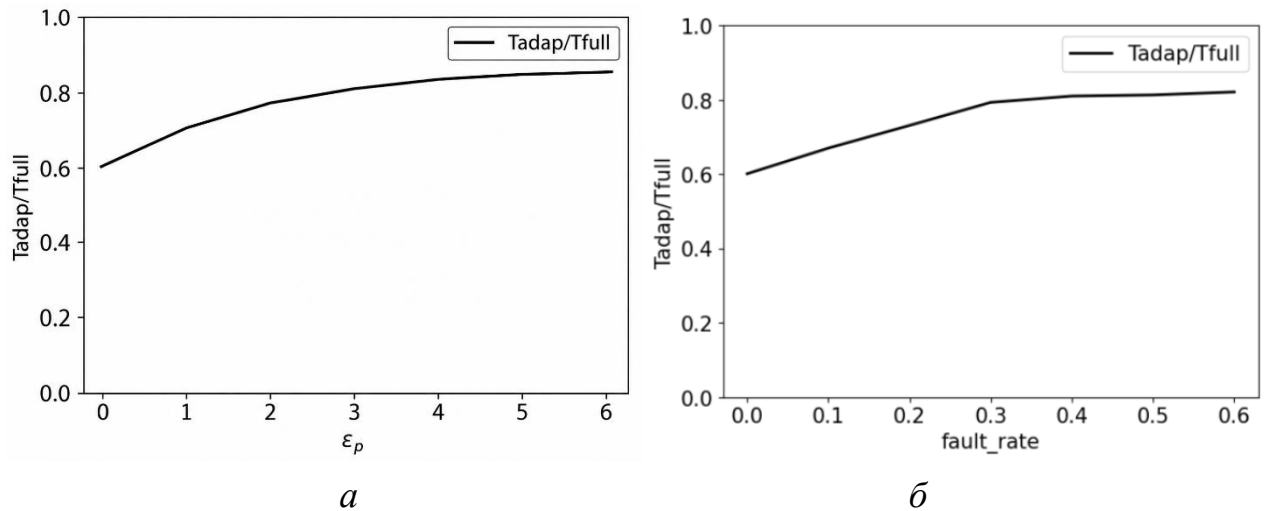


Рисунок 12 – Залежність відношення середнього часу виведення в адаптивному режимі  $T_{\text{adap}}$  до часу виведення через усю мережу  $T_{\text{full}}$  від:  $a$  – максимального рівня збурення змагальної  $L_{\infty}$ -атаки;  $б$  – частка тензорів, ушкоджених інверсіями бітів (bit-flip)

Таким чином, проміжні відгалуження забезпечують насамперед прискорення відновлення та керовану деградацію за рахунок вибору рівня деталізації рішення, тоді як вентильні модулі реалізують ресурсно-адаптивне керування активною частиною обчислювального графа. Сукупно ці механізми забезпечують узгодження функціональної ефективності, резильєнтності та обчислювальних витрат СІАД.

Дослідження вентильних моделей на базі ResNet-110 та DeiT-S засвідчило наявність раціонального діапазону коефіцієнта динамічного стиснення. За  $t \approx 0,6$  забезпечується скорочення обчислювальної складності більш ніж на 30 % без погіршення, а в окремих сценаріях – із підвищенням точності та інтегрального показника резильєнтності. Подальше зменшення  $t$  спричиняє дефіцит інформаційної місткості активної підструктури і призводить до зниження функціональної ефективності.

Заміна ReLU на LeakyReLU6 додатково підвищила значення інтегрального показника резильєнтності для всіх досліджених типів збурень. Для ResNet-110 за ін'єкції бітових несправностей значення  $R$  зросло з 0,953 до 0,988, за змагальних атак – з 0,891 до 0,917, а за раптової зміни задачі – з 0,978 до 0,988. Для DeiT-S відповідні значення зросли з 0,950 до 0,979, з 0,884 до 0,923 та з 0,911 до 0,935.

Результати для задачі детектування об'єктів на аерознімках підтвердили переносимість запропонованого підходу на складнішу прикладну модель. За  $t = 0,6$  середні обчислювальні витрати в умовах ін'єкції несправностей зменшилися з 109,2 до 83,7 FLOPs при підвищенні  $mAP@0,5$  з 0,72 до 0,73. В умовах змагальної атаки витрати зменшилися зі 109,0 до 82,9 FLOPs за збереження  $mAP@0,5 = 0,69$ . Отже, для детектора досягнуто скорочення обчислювальних витрат приблизно на 22–24 % без зниження функціональної ефективності в збурених умовах.

У п'ятому розділі розроблено та експериментально досліджено методи оптимізації резильєнтності СІАД, спрямовані на узгоджене налаштування механізмів поглинання різнотипних збурень, швидкого відновлення функціональної ефективності та раціонального використання обчислювальних ресурсів. На відміну від традиційних підходів, орієнтованих переважно на підвищення робастності моделі в окремому фіксованому стані, запропоновані методи враховують повну траєкторію її адаптації після дії збурення.

Об'єктами оптимізації є параметри реконфігураційних надбудов, розроблених у третьому та четвертому розділах: адаптерів, мета-адаптерів, вентильних модулів і правил вибору активної підструктури нейромережі. Базова модель забезпечує виконання основної задачі у штатних умовах, тоді як реконфігураційні надбудови формують здатність СІАД поглинати збурення, адаптуватися до нових умов і відновлювати функціональну ефективність за обмеженої кількості кроків донавчання.

Задачу мета-оптимізації резильєнтності подано у двоконтурній формі

$$(\omega^*, \varphi^*) = \arg \max_{\omega, \varphi} \mathbb{E}_{\tau \sim p(\tau)} [R_\tau(U_\tau(\theta, \omega, \varphi; T))], \quad (17)$$

де  $\theta$  – параметри базової нейромережі;  $\varphi$  – параметри, що оперативно адаптуються, зокрема параметри адаптерів або навчуваних блоків;  $\omega$  – мета-параметри реконфігураційних надбудов, зокрема мета-адаптерів або вентильних модулів;  $\tau$  – реалізація збурюючого впливу;  $p(\tau)$  – розподіл сценаріїв збурень;  $U_\tau$  – оператор, який формує збурення та виконує  $T$  кроків внутрішньої адаптації;  $R_\tau$  – інтегральний показник резильєнтності для відповідного сценарію.

Внутрішній контур виконує адаптацію моделі до конкретної реалізації збурення, а зовнішній контур налаштовує початкові параметри та механізми реконфігурації таким чином, щоб забезпечити високу резильєнтність у середньому на множині сценаріїв. Як збурення розглянуто змагальні впливи на вхідні дані, ін'єкції несправностей у параметри та проміжні обчислення, а також зміну задачі, домену або розподілу даних.

Інтегральний показник резильєнтності визначено як нормовану площу під дискретною траєкторією функціональної ефективності протягом заданого бюджету адаптації

$$R_\tau = \frac{1}{Q_0 T} \sum_{t=1}^T Q_\tau(t), \quad (18)$$

де  $Q_\tau(t)$  – значення показника функціональної ефективності після  $t$ -го кроку адаптації в умовах збурення  $\tau$ ;  $Q_0$  – значення цього показника у номінальних умовах;  $T$  – допустима кількість кроків адаптації.

Така ціль одночасно враховує глибину початкової деградації, здатність моделі поглинати збурення, швидкість відновлення та рівень функціональної ефективності, досягнутий у межах заданого ресурсного бюджету.

Розроблено дві реалізації мета-оптимізації, які відрізняються способом передавання інформації про резильєнтність до параметрів моделі. У диференційованому градієнтному алгоритмі інтегральний показник оптимізується

опосередковано за диференційовним проксі-функціоналом, утвореним із значень функції втрат уздовж траєкторії адаптації

$$(\omega^*, \varphi^*) = \arg \min_{\omega, \varphi} \mathbb{E}_{\tau \sim p(\tau)} [L_\tau(U_\tau(\theta, \omega, \varphi; T))], \quad (19)$$

де  $L_\tau$  – функція втрат основної задачі в умовах збурення  $\tau$ .

Мінімізація цієї функції забезпечує непряме підвищення інтегрального показника резильєнтності за умови узгодженості функції втрат із прикладним показником функціональної ефективності.

У внутрішньому контурі оновлюються локальні копії параметрів швидких адаптерів, тоді як параметри мета-адаптерів залишаються фіксованими, але впливають на напрям градієнтного оновлення через перед- і післяперетворення ознак. У зовнішньому контурі параметри мета-адаптерів та початкова конфігурація швидких адаптерів оновлюються за результатами множини траєкторій адаптації.

Диференційований градієнтний алгоритм мета-оптимізації є обчислювально ефективною реалізацією мета-оптимізації, однак його результат залежить від відповідності диференційовної функції втрат фактичній прикладній метриці. Для прямої оптимізації виміряного показника резильєнтності розроблено еволюційний алгоритм мета-оптимізації, який розглядає внутрішню адаптацію та оцінювання резильєнтності як функцію «чорної скриньки».

Позначимо  $\psi = [\omega, \varphi]$  об'єднаний вектор мета-оптимізованих параметрів, а функцію мета-цілі визначимо як

$$F(\psi) = \mathbb{E}_{\tau \sim p(\tau)} [R_\tau(U_\tau(\psi))]. \quad (20)$$

Для оцінювання напряму покращення гауссівсько-згладженої цілі використано антиподний оцінювач

$$\widehat{\nabla_\psi \tilde{F}_\sigma} = \frac{1}{2\sigma S} \sum_{s=1}^S [F(\psi + \sigma \mu_s) - F(\psi - \sigma \mu_s)], \quad (21)$$

де  $\mu_s$  – випадковий вектор із нормального розподілу;  $\sigma$  – масштаб параметричної мутації;  $S$  – кількість досліджуваних напрямів.

Для кожної додатної та від'ємної мутації виконується повна внутрішня адаптація, після чого безпосередньо обчислюється інтегральний показник резильєнтності. Антиподна схема зменшує дисперсію оцінювання та підвищує стабільність оновлень у стохастичних сценаріях ін'єкції несправностей і формування змагальних зразків.

Еволюційний алгоритм мета-оптимізації не потребує диференційовності показника резильєнтності, прикладної метрики або оператора адаптації, тому може застосовуватися до моделей із дискретними структурними перемикаваннями, процедурами ін'єкції несправностей і спеціалізованими алгоритмами адаптації під час тестування. Водночас він потребує багаторазового виконання траєкторій адаптації для протилежно збурених конфігурацій параметрів і тому є більш ресурсоємним. Обидва алгоритми передбачено виконувати офлайн на серверній, хмарній або наземній обчислювальній платформі, а на ресурсообмежений пристрій передавати вже мета-оптимізовану модель СІАД.

Для узгодження резильєнтності та обчислювальної ефективності вперше розроблено багатоетапний метод навчання СІАД з керованою структурною реконфігурацією. Метод передбачає послідовне формування початкової конфігурації моделі з вентильними та, за потреби, адаптерними надбудовами і її навчання в незбуреному режимі з ресурсною регуляризацією. Далі здійснюється мета-навчання на траєкторіях адаптації до різнотипних збурень. На етапі експлуатації передбачено адаптацію під час тестування на нових нерозмічених даних, а за наявності зворотного зв'язку у вигляді ручної розмітки – локальне донавчання релевантних модулів.

У режимі адаптації під час тестування оновлюються лише параметри модулів, які були активовані під час прямого проходу. Селективне оновлення подано у вигляді

$$\varphi \leftarrow \varphi - \alpha(M_A \odot \nabla_{\varphi} L_{\text{TТА}}), \quad (22)$$

де  $\varphi$  – вектор параметрів, потенційно доступних для адаптації;  $\alpha$  – швидкість адаптації;  $L_{\text{TТА}}$  – функція втрат адаптації під час тестування;  $M_A$  – бінарна або блочно-бінарна маска параметрів активованих модулів;  $\odot$  – поелементне множення.

Експериментальне дослідження градієнтної та еволюційної реалізацій мета-оптимізації проведено на задачах класифікації зображень із використанням різних рівнів ін'єкції несправностей, змагальних збурень та зміни задачі. Базову ResNet-18 попередньо навчено на CIFAR-10, а допоміжні задачі адаптації сформовано на основі CIFAR-100 за схемою навчання на малій кількості прикладів. Для кожного рівня ін'єкції несправностей і змагального впливу результати усереднювалися за 100 стохастичними реалізаціями, а резильєнтність до зміни задачі оцінювалася за п'ятьма незалежними реалізаціями. Наведені далі числові результати є найбільш показовими прикладами з ширшої серії проведених експериментів.

За ін'єкції інверсії одиничних бітів із часткою пошкоджених ваг 0,6 точність базової моделі становила 75,4 %, після спеціалізованого навчання адаптерів – 80,1 %, а після градієнтної мета-оптимізації – 84,9 %; інтегральний показник резильєнтності зріс з 0,831 до 0,917. За найбільш інтенсивного з досліджених змагальних збурень точність відповідних конфігурацій становила 74,8 %, 75,9 % і 77,7 %, а інтегральний показник резильєнтності після мета-оптимізації зріс з 0,821 до 0,897.

Порівняння з класичним MAML підтвердило перевагу постановки, орієнтованої на всю траєкторію деградації та відновлення. За ін'єкції несправностей приріст інтегрального показника резильєнтності порівняно з класичним MAML перевищив 5 %, а за змагальних атак – 6 %. Еволюційна реалізація забезпечила додатковий приріст показника резильєнтності понад 1,5 % порівняно з градієнтною. За частки пошкоджених ваг 0,6 отримано точність 85,0 % та інтегральний показник резильєнтності 0,941, а за найбільш інтенсивного змагального збурення – відповідно 83,5 % і 0,919. Водночас критерій ранньої зупинки для еволюційної реалізації досягався за 233 мета-ітерації порівняно зі 150 для градієнтної.

Ефективність мета-оптимізації перевірено також у поєднанні з керованою структурною реконфігурацією на динамічних моделях ResNet-110 і DeiT-S. За коефіцієнта динамічного стиснення 0,6 для ResNet-110 в умовах ін'єкції

несправностей отримано точність 89,9 % та інтегральний показник резильєнтності 0,988 при 312,30 MFLOPs замість 510,48 MFLOPs для повної мережі. Для DeiT-S відповідні значення становили 92,2 %, 0,979 та 7,04 GFLOPs замість 10,56 GFLOPs. За змагальних атак інтегральний показник резильєнтності після мета-оптимізації зріс на 16,9 % для ResNet-110 та на 21,6 % для DeiT-S. Загалом керована структурна реконфігурація забезпечила зменшення обчислювальних витрат більш ніж на 30 % зі збереженням або підвищенням функціональної ефективності та резильєнтності. Додатково підтверджено позитивний вплив LeakyReLU6: зокрема, для ResNet-110 за ін'єкції несправностей інтегральний показник резильєнтності зріс з 0,953 до 0,988, а для DeiT-S за змагальних атак – з 0,884 до 0,923.

Запропоновані методи інтегровано в удосконалений MLOps-конвеєр, доповнений постфактум мета-оптимізацією резильєнтності, калібруванням прогностичної невизначеності та адаптацією під час тестування. Для MobileViT на першому збуреному етапі точність за ін'єкції несправностей підвищилася з 0,802 до 0,920, а за змагальної атаки – з 0,720 до 0,850; за зміни задачі інтегральний показник резильєнтності зріс з 0,751 до 0,830.

Переносимість запропонованого підходу додатково перевірено на медичних наборах DermaMNIST, BloodMNIST і PathMNIST із використанням моделей ResNet-18 та MedViT-T. Під час переходу до BloodMNIST введення оптимізації резильєнтності підвищило інтегральний показник з 0,68 до 0,80 для ResNet-18 та з 0,66 до 0,71 для MedViT-T. Калібрування невизначеності забезпечило можливість відхилення недостатньо достовірних прогнозів і переходу до керованої деградації, а адаптація під час тестування – відновлення функціональної ефективності за нових реалізацій збурень без оперативно доступної розмітки.

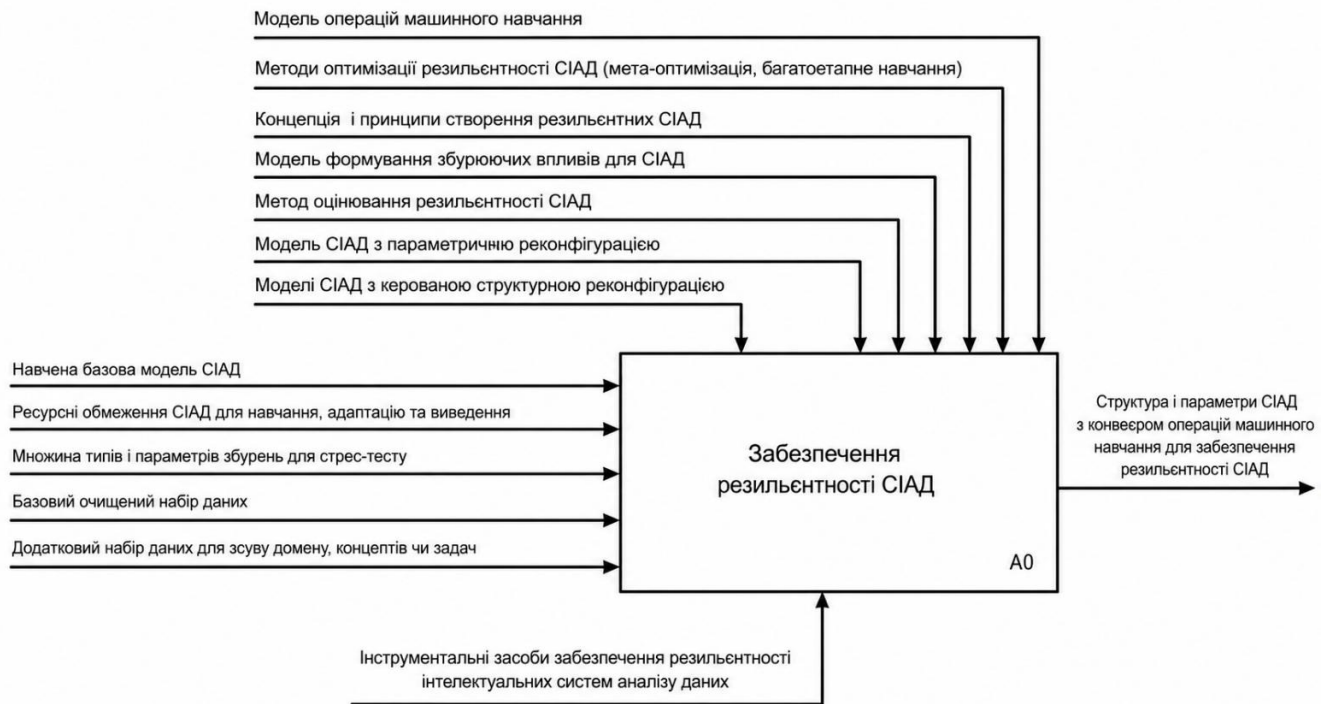
Отримані результати підтверджують можливість підвищення резильєнтності та швидкості відновлення за обчислювальних обмежень і становлять алгоритмічну основу інформаційних технологій, розроблених у шостому розділі.

**У шостому розділі** розроблено та впроваджено дві взаємопов'язані інформаційні технології: забезпечення резильєнтності та оцінювання і верифікації резильєнтності СІАД. Їх загальні верхньорівневі функціональні моделі A0, формалізовані засобами IDEF0, наведено на рисунку 13.

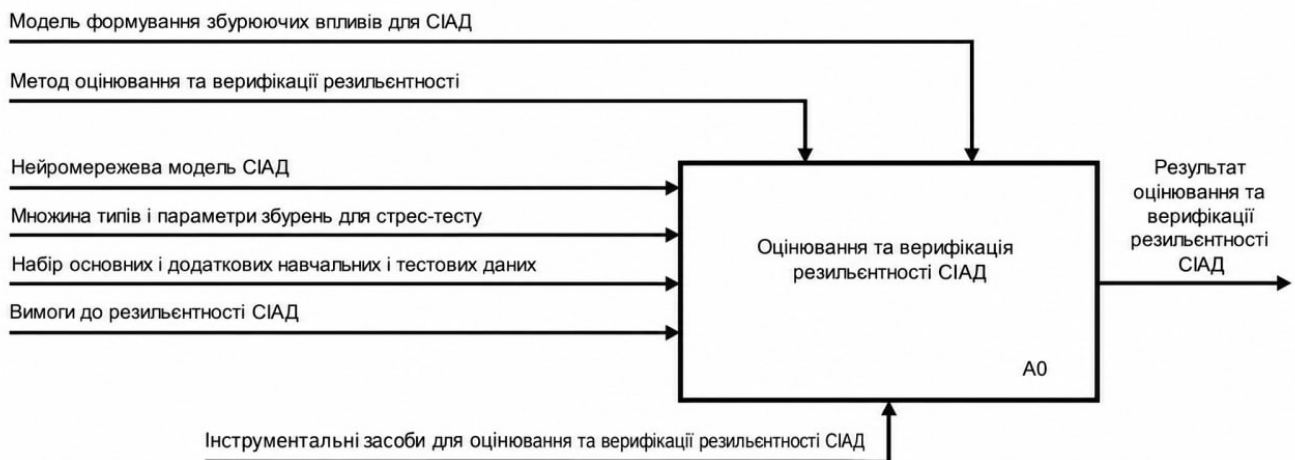
Інформаційна технологія забезпечення резильєнтності перетворює базову модель, набори даних, профіль збурюючих впливів і ресурсні обмеження на цільову конфігурацію СІАД із визначеними структурою, параметрами та правилами реконфігурації, процедурами адаптації й MLOps-конвеєром експлуатаційної підтримки. Технологія охоплює формування вимог до резильєнтності, оцінювання базової конфігурації, під'єднання та налаштування реконфігураційних надбудов, оптимізацію резильєнтності з урахуванням ресурсних обмежень та інтеграцію моделі в експлуатаційний MLOps-контур.

Інформаційна технологія оцінювання та верифікації резильєнтності виконує функцію контрольного контуру створення й експлуатації СІАД. На вході використовуються нейромережева модель, множина типів і параметрів збурень, основні й додаткові набори даних та вимоги до резильєнтності; керувальними впливами є модель формування збурень і метод оцінювання та верифікації резильєнтності. Технологія забезпечує контрольовані випробування з адаптацією,

обчислення і статистичне узагальнення показників та, за потреби, ймовірнісну верифікацію відповідності заданим вимогам.



*a*



*б*

Рисунок 13 – Загальні верхньорівневі IDEF0-моделі інформаційних технологій: *a* – забезпечення резильєнтності СІАД; *б* – оцінювання та верифікації резильєнтності СІАД

Для практичної реалізації інформаційних технологій розроблено дослідницький програмний комплекс мовою Python із використанням бібліотеки PyTorch. Його компонентна архітектура охоплює нейронмережні моделі з параметричною і структурною реконфігурацією, генератори різноманітних збурюючих впливів та процедури оцінювання і верифікації резильєнтності, мета-оптимізації, багаторівневого навчання, адаптації під час тестування й калібрування невизначеності (рис. 14).

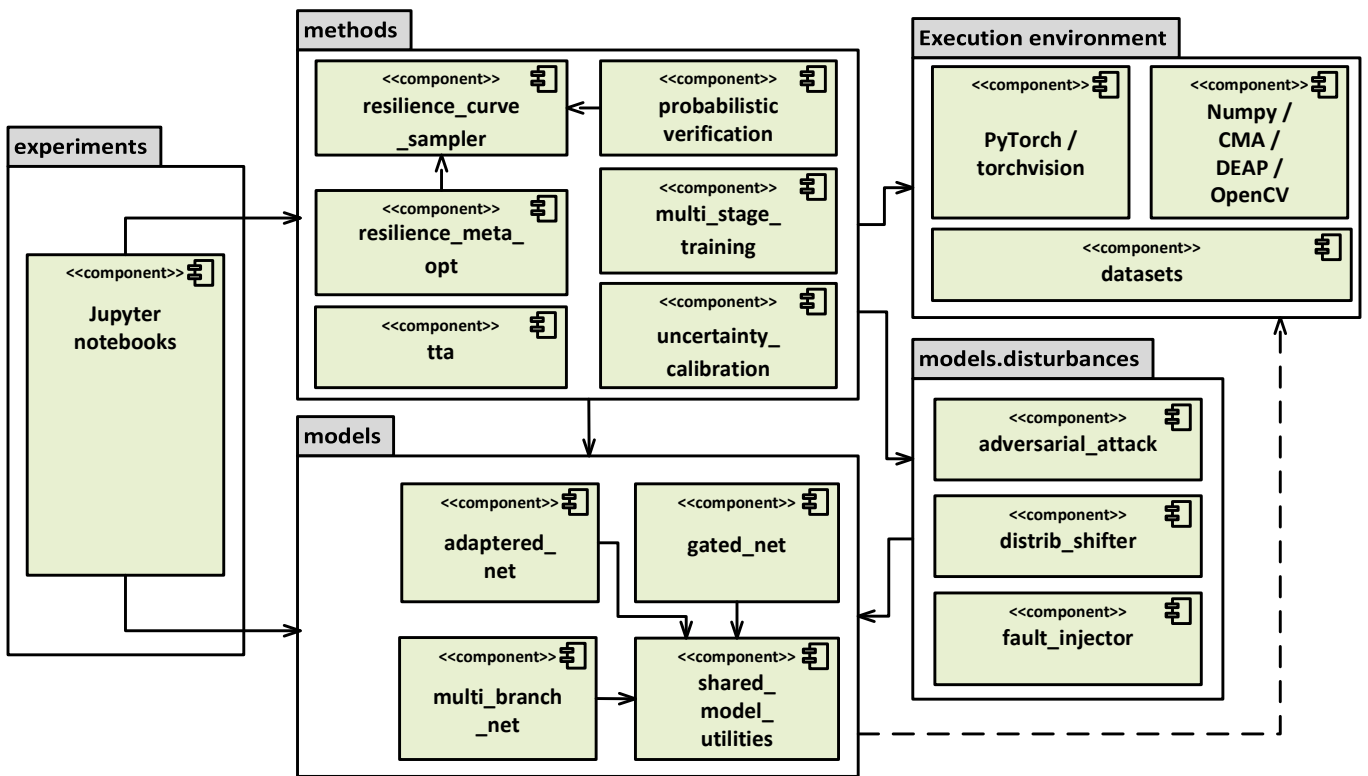


Рисунок 14 – UML-діаграма компонентів інструментальних програмних засобів оцінювання та забезпечення резильєнтності СІАД

На рівні моделей комплекс містить реалізації СІАД із паралельною корекцією за допомогою адаптерів і мета-адаптерів, вентильним керуванням обчислювальними блоками та проміжними відгалуженнями. Методичний рівень охоплює формування змагальних впливів, ін'єкцію бітових несправностей і моделювання зсувів даних, а також побудову та статистичне узагальнення траєкторій резильєнтності, мета-оптимізацію, адаптацію і постфактум калібрування невизначеності.

Практичну придатність розроблених інформаційних технологій підтверджено їх застосуванням у бортових системах машинного зору безпілотних апаратів, наземних роботизованих комплексах, хмарних сервісах відеоаналітики, а також у науково-дослідній та освітній діяльності.

## ВИСНОВКИ

У дисертаційній роботі досягнуто мету дослідження, яка полягає у підвищенні резильєнтності систем інтелектуального аналізу даних, що функціонують в умовах різнотипних збурюючих впливів, обчислювальних, часових та інших ресурсних обмежень, із забезпеченням раціонального рівня ресурсної ефективності. Досягнення цієї мети забезпечено шляхом розроблення методологічних основ, моделей і методів оцінювання, мета-оптимізації, параметричної та структурної реконфігурації СІАД, а також інформаційних технологій оцінювання та забезпечення резильєнтності СІАД. Сукупність отриманих результатів забезпечує розв'язання актуальної науково-прикладної проблеми створення резильєнтних СІАД, здатних підтримувати прийнятний рівень функціональної ефективності, відновлюватися та адаптуватися до дії різнотипних збурюючих чинників за умов

обмеженого ресурсного забезпечення.

1. Проведено аналіз сучасного стану проблеми створення резильєнтних систем інтелектуального аналізу даних (СІАД). Систематизовано загрози (апаратні збої, змагальні атаки, дрейф концепцій) та механізми протидії. Проаналізовано основні підходи до створення резильєнтних СІАД, математичний апарат, методи оцінювання та забезпечення резильєнтності СІАД. Виявлені суперечності між потребою в комплексній резильєнтності СІАД, фрагментарністю наявних засобів її забезпечення та жорсткими ресурсними обмеженнями в галузях практичного застосування. Обґрунтовано науково-прикладну проблему та методику досліджень. Отримані результати визначають вимоги до концепції, принципів і структури методології створення резильєнтних СІАД.

2. Розроблено концепцію, принципи і структуру методології створення резильєнтних СІАД, яка поєднує етапи підготовки до дії збурень, їх поглинання, відновлення функціональної ефективності, адаптації та керованої деградації. Запропонована методологія забезпечує системне узгодження цілей резильєнтності, функціональної ефективності та ресурсних витрат, що створює наукову основу для побудови СІАД, здатних підтримувати прийнятний рівень функціонування в агресивному кіберфізичному середовищі.

3. Розроблено модель формування збурюючих впливів, яка забезпечує відтворення різнотипних сценаріїв порушення штатного функціонування СІАД, зокрема впливів на вхідні дані, параметри моделі, проміжні обчислення та розподіл даних. Використання цієї моделі дозволяє формувати комплексні випробування, необхідні для оцінювання здатності СІАД поглинати збурення, відновлювати функціональну ефективність і адаптуватися до нових умов функціонування.

4. 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. Це надає змогу порівнювати альтернативні конфігурації СІАД, обґрунтовувати вибір архітектурних рішень, гіперпараметрів, складу реконфігураційних надбудов і режимів їх використання, а також статистично підтверджувати відповідність обраних рішень заданим вимогам до резильєнтності з урахуванням допустимого ризику, ресурсного бюджету та рівня статистичної довіри.

5. Розроблено модель операції машинного навчання для забезпечення резильєнтності СІАД, яка інтегрує процедури оцінювання, моніторингу, мета-оптимізації, калібрування невизначеності, адаптації під час тестування та керованої деградації в єдиний життєвий цикл створення й експлуатаційної підтримки системи. Це дозволяє розглядати резильєнтність не як властивість, що формується лише на етапі навчання моделі, а як підтримувану в експлуатації характеристику СІАД, яка коригується відповідно до зміни даних, задач, середовища та доступного ресурсного бюджету.

6. Розроблено модель СІАД з параметричною реконфігурацією, що реалізує ресурсоефективну корекцію поведінки базової нейромережної моделі без її повного перенавчання або перебудови. Використання каскадних адаптерних надбудов із розділенням параметрів мета-оптимізації та оперативної адаптації забезпечує

підвищення резильєнтності СІАД до різнотипних збурюючих впливів за обмежених обчислювальних ресурсів. Отримані результати підтверджують доцільність параметричної реконфігурації як засобу швидкого відновлення функціональної ефективності системи після впливу збурень.

7. Розроблено моделі СІАД зі структурною реконфігурацією, у яких активна частина обчислювального графа змінюється залежно від стану даних, проявів збурень, рівня невизначеності та ресурсних обмежень. Запропоновані механізми умовної активації модулів, проміжних відгалужень, вентиляного керування та модифікованої функції активації з насиченням і витоком сприяють обмеженню поширення збурень у глибині моделі та забезпечують можливість адаптивного перерозподілу обчислень. Це дозволяє підвищувати резильєнтність СІАД без пропорційного збільшення обчислювальної складності.

8. Розроблено метод мета-оптимізації резильєнтності СІАД, який використовує інтегральний показник резильєнтності як мета-ціль і виконує налаштування реконфігураційних механізмів за результатами адаптації системи до різнотипних збурюючих впливів. Метод забезпечує узгодження механізмів толерування впливів, параметрів адаптації та ресурсних обмежень, що дозволяє підвищити не лише робастність системи в момент дії збурення, а й її здатність до швидкого відновлення та подальшої адаптації.

9. Розроблено метод багатоетапного навчання СІАД зі структурною реконфігурацією, орієнтований на узгодження вимог резильєнтності та обчислювальної ефективності. Метод передбачає послідовне формування базової функціональної спроможності моделі, навчання реконфігураційних надбудов у незбуреному режимі, мета-навчання в умовах різнотипних збурень та адаптацію релевантних модулів на нових даних. Це забезпечує здатність СІАД раціонально використовувати обчислювальні ресурси, активувати складніші обчислювальні траєкторії для складних або збурених зразків і зменшувати витрати в умовах меншої невизначеності.

10. Розроблено та впроваджено інформаційні технології оцінювання та забезпечення резильєнтності СІАД для різних галузей застосування. Запропоновані технологічні рішення доведено до рівня програмних засобів, інженерних методик і моделей процесів, що забезпечують генерацію збурюючих впливів, проведення випробувань з адаптацією, обчислення інтегральних і статистичних показників резильєнтності, статистично обґрунтований вибір раціональних конфігурацій, мета-оптимізацію, адаптацію та підтримку функціонування СІАД в умовах ресурсних обмежень. Практичне впровадження результатів підтверджує можливість їх використання для модернізації інтелектуальних кіберфізичних, безпекових, інфраструктурних і бортових систем, де застосування класичних підходів до відмовостійкості є обмеженим через надмірні ресурсні витрати.

Практична значущість отриманих результатів у ресурсному аспекті полягає в можливості забезпечення прийнятного рівня резильєнтності СІАД без застосування надмірно ресурсомістких схем класичної відмовостійкості, повного дублювання моделей або регулярного повного перенавчання. Це досягається завдяки використанню реконфігураційних надбудов, параметрично ефективної адаптації, мета-оптимізації та динамічного перерозподілу обчислень, що розширює

можливості впровадження резильєнтних СІАД на пристроях з обмеженими обчислювальними, енергетичними та часовими ресурсами.

### СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

**Праці, в яких опубліковано основні наукові результати дисертації:**

*Публікації в іноземних виданнях та фахових виданнях, які включені до міжнародних наукових баз даних:*

1. Moskalenko V. V., Moskalenko A. S. Neural network based image classifier resilient to destructive perturbation influences: architecture and training method. *Radioelectronic and Computer Systems*. 2022. № 3. P. 95– 109. DOI: <https://doi.org/10.32620/reks.2022.3.07>. (Індексована в наукометричній базі **Scopus**, що відноситься до Q3 відповідно до SCImago Journal & Country Rank).

2. Moskalenko V. V., Moskalenko A. S., Korobov A. G., Zaretsky M. O. Image classifier resilient to adversarial attacks, fault injections and concept drift – model architecture and training algorithm. *Radio Electronics, Computer Science, Control*. 2022. № 3. P. 86. DOI: 10.15588/1607-3274-2022-3-9. (Індексована в наукометричній базі **Web of Science**)

3. Moskalenko V. V., Kharchenko V., Moskalenko A., Kuzikov B. Resilience and resilient systems of artificial intelligence: taxonomy, models and methods. *Algorithms*. 2023. Vol. 16, № 3. P. 165. DOI: 10.3390/a16030165. (Індексована в наукометричній базі **Web of Science** та **Scopus**, що відноситься до Q2 відповідно до SCImago Journal & Country Rank)

4. Moskalenko V. V., Kharchenko V., Moskalenko A., Petrov S. Model and Training Method of the Resilient Image Classifier Considering Faults, Concept Drift, and Adversarial Attacks. *Algorithms*. 2022. Vol. 15, № 10. P. 1– 24. DOI: 10.3390/a15100384. (Індексована в наукометричній базі **Web of Science** та **Scopus**, що відноситься до Q2 відповідно до SCImago Journal & Country Rank)

5. Moskalenko V. V. Model-agnostic meta-learning for resilience optimization of artificial intelligence system. *Radio Electronics, Computer Science, Control*. 2023. № 2. P. 79. DOI: 10.15588/1607–3274–2023–2–9 (Індексована в наукометричній базі **Web of Science**)

6. Moskalenko V.V., Kharchenko V. Resilience-aware MLOps for AI-based medical diagnostic system. *Frontiers in Public Health*. 2024. Vol. 12. P. 1342937. DOI: 10.3389/fpubh.2024.1342937. (Індексована в наукометричній базі **Web of Science** та **Scopus**, що відноситься до Q1 відповідно до SCImago Journal & Country Rank)

7. Moskalenko V. V., Kharchenko V., Semenov S. Model and method for providing resilience to resource-constrained AI-system. *Sensors*. 2024. Vol. 24, № 18. P. 5951. DOI: 10.3390/s24185951. (Індексована в наукометричній базі **Web of Science** та **Scopus**, що відноситься до Q1 відповідно до SCImago Journal & Country Rank)

8. Moskalenko V. V., Korobov A.G, Moskalenko Y.V. Object detection with affordable robustness for UAV aerial imagery: model and providing method. *Radioelectronic and Computer Systems*. 2024. № 3. P. 55– 66. DOI: 10.32620/reks.2024.3.04. (Індексована в наукометричній базі **Scopus** та відноситься до Q3 відповідно до SCImago Journal & Country Rank)

9. Moskalenko V. V., Zaretsky M. O., Moskalenko A. S., Panych A. O., Lysyuk V. V. A model and training method for context classification in CCTV sewer inspection

video frames. Radio Electronics, Computer Science, Control. 2021. № 3. P. 97– 108. DOI: 10.15588/1607–3274–2021–3–9. (Індексована в наукометричній базі **Web of Science**)

10. Москаленко В. В., Зарецький М. О., Москаленко А. С., Коробов А. Г., Ковальський Я. Ю. Багатоетапний метод глибинного навчання з попереднім самонавчанням для класифікаційного аналізу дефектів стічних труб. Радіоелектронні і комп'ютерні системи. 2021. № 4. С. 71– 81. DOI: 10.32620/reks.2021.4.06. (Індексована в наукометричній базі **Scopus**)

11. Москаленко В. В., Зарецький М. О., Коробов А. Г., Ковальський Я. Ю., Шаєхов А. Ф., Семашко В. А., та ін. Модель та метод навчання для класифікаційного аналізу рівня води в стічних трубах за даними відеоінспекції. Радіоелектронні і комп'ютерні системи. 2021. № 2. С. 4– 15. DOI: 10.32620/reks.2021.2.01. (Індексована в наукометричній базі **Scopus**)

12. Москаленко В. В., Зарецький М. О., Москаленко А. С., Кудрявцев А. М., Семашко В. А. Багатошарова модель та метод навчання для детектування шкідливого трафіка на основі ансамблю дерев рішень. Radioelectronic and Computer Systems. 2020. № 2. С. 92– 101. DOI: 10.32620/reks.2020.2.08 (Індексована в наукометричній базі **Scopus**)

13. Moskalenko V. V., Moskalenko A. S., Korobov A. G., Zaretsky M. O. A model and training algorithm of small-sized object detection system for a compact aerial drone. Radio Electronics, Computer Science, Control. 2019. № 1. P. 110– 121. DOI: 10.15588/1607-3274-2019-1-11 (Індексована в наукометричній базі **Web of Science**)

14. Moskalenko V. V., Moskalenko A.S., Korobov A.G., Semashko V. The model and training algorithm of compact drone autonomous visual navigation system. Data. 2019. Vol. 4, № 1. P. 4. DOI: 10.3390/data4010004. (Індексована в наукометричній базі **Web of Science** та **Scopus**, що відноситься до Q2 відповідно до SCImago Journal & Country Rank).

#### ***Монографії (або розділи у колективних монографіях)***

15. Moskalenko V. Robust model and training method for malware recognition in IoT devices. In: Advancements in Cybersecurity. CRC Press, 2025. P. 292– 309. DOI: 10.1201/9781003546153-13. (Індексована в наукометричній базі **Scopus**)

16. Москаленко В. В. Моделі і методи інтелектуального аналізу багатовимірних даних за умов апіорної невизначеності : монографія. Суми : СумДУ, 2020. 184 с. URL: [https://essuir.sumdu.edu.ua/bitstream-download/123456789/77692/3/Moskalenko\\_analiz\\_danykh.pdf](https://essuir.sumdu.edu.ua/bitstream-download/123456789/77692/3/Moskalenko_analiz_danykh.pdf).

17. Moskalenko V., Zaretskyi M., Moskalenko A., Lysyuk V. Sewer pipe defects classification based on deep convolutional network with information-extreme error-correction decision rules. In: Communications in Computer and Information Science. Cham: Springer, 2020. P. 253– 263. DOI: 10.1007/978-3-030-61656-4\_16 (Індексована в наукометричній базі **Scopus**).

#### ***Статті у наукових виданнях, включених до переліку фахових видань України:***

18. Moskalenko V.V., Boiko M. Improved binary data block classification model for file carving problems. Herald of Khmelnytskyi National University. Technical Sciences. 2025. Vol. 353, № 3.2. P. 13– 21. DOI: 10.31891/2307-5732-2025-353-1.

#### ***Праці, що підтверджують апробацію матеріалів дисертації:***

19. Moskalenko V.V., Korobov A.G., Kudravcev A., Boiko M. Meta-learning with evolutionary strategy for resilience optimization of image recognition system. In: 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2023). IEEE, 2023. P. 978–982. DOI: 10.1109/IDAACS58523.2023.10348942. (Індексована у наукометричній базі **Scopus**)

20. Moskalenko V., Moskalenko A., Kudriavcev A., Moskalenko Y. Resilience-aware MLOps for resource-constrained AI-system. In: Proceedings of the International Workshop on Computer Modeling and Intelligent Systems (CMIS 2024), 27 March 2024, Zaporizhzhia, Ukraine. CEUR-WS, 2024. URL: <https://ceur-ws.org/Vol-3702/paper38.pdf>. (Індексована в наукометричній базі **Scopus**)

21. Boiko M., Moskalenko V. Neural model and training method for robust and resource-efficient data block identification. In: ICST-2024: XII International Scientific and Practical Conference «Information Control Systems and Technologies (ICST-ODESA-2024)». CEUR-WS, 2024. 13 p. URL: <https://ceur-ws.org/Vol-3790/paper35.pdf>. (Індексована в наукометричній базі **Scopus**)

22. Moskalenko V., Moskalenko A., Shaiekhov A., Zaretskyi M. Multi-layer model and training method for information-extreme malware traffic detector. In: The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS 2020), 27 April – 1 May 2020. CEUR-WS, 2020. P. 288–299. URL: <https://ceur-ws.org/Vol-2608/paper22.pdf>. (Індексована в наукометричній базі **Scopus**)

23. Москаленко В. В., Москвін Д. О. Методи витонченої деградації систем штучного інтелекту. Міжнародна наукова конференція молодих учених «Інформатика, математика, автоматика» (ІМА-2023), 24–28 квітня 2023 р., Суми, Україна – Астана, Казахстан: матеріали конференції. 2023. С. 45–46. URL: [https://itp.elit.sumdu.edu.ua/wp-content/uploads/2023/05/Abstracts\\_Book\\_IMA-2023.pdf](https://itp.elit.sumdu.edu.ua/wp-content/uploads/2023/05/Abstracts_Book_IMA-2023.pdf).

24. Moskalenko V. V., Moskalenko Y. V., Ruban I. O. Affordable resilience of AI-system based on dynamic deep neural network. Міжнародна наукова конференція молодих учених «Інформатика, математика, автоматика» (ІМА-2024), 22–26 квітня 2024 р., Суми, Україна – Астана, Казахстан: матеріали конференції. 2024. С. 46–47. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059494.pdf>.

***Праці, які додатково відображають наукові результати дисертації:***

25. Свідоцтво про реєстрацію авторського права на твір № 114795. Програма для ймовірнісної сертифікації резильєнтності класифікатора зображень до протиборчих атак і пошкодження тензорів нейромережі / Москаленко В. В., Москаленко А. С., Зарецький М. О., Коробов А. Г.; Сумський державний університет. Заявл. 14.09.2022. Опубл. 24.10.2022. URL: <https://iprop-ua.com/cr/9vuxat8i/>.

26. Свідоцтво про реєстрацію авторського права на твір № 113206. Програма машинного навчання класифікатора зображень з підвищеною робастністю до шуму і змагальних атак / Москаленко В. В., Москаленко А. С., Зарецький М. О., Коробов А. Г.; Сумський державний університет. Заявл. 06.06.2022. Опубл. 29.07.2022. URL: <https://iprop-ua.com/cr/xmu4mecx/>.

27. Свідоцтво про реєстрацію авторського права на твір № 7123. Мета-навчання для підвищення резильєнтності нейромережної системи аналізу даних /

Москаленко В'ячеслав Васильович, Коробов Артем Геннадійович, Зарецький Микола Олександрович, Москаленко Юрій Васильович, Рубан Іван Олегович. Заявл. 2024. Опубл. 16.05.2024. URL: <https://sis.nipo.gov.ua/uk/search/detail/1812643/>.

## АНОТАЦІЇ

**Москаленко В. В. Методологічні основи та інформаційні технології створення резильєнтних систем інтелектуального аналізу даних.** – *На правах рукопису.*

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології (12 – Інформаційні технології). – Хмельницький національний університет, Хмельницький, 2026.

У дисертації сформульовано й вирішено актуальну науково-прикладну проблему створення резильєнтних систем інтелектуального аналізу даних (СІАД), що функціонують в умовах різнотипних збурюючих чинників та ресурсних обмежень. Метою роботи є підвищення резильєнтності СІАД шляхом розроблення методологічних основ, моделей, методів та інформаційних технологій її оцінювання і забезпечення протягом життєвого циклу систем.

Вперше розроблено методологію створення резильєнтних СІАД, що включає концепцію, принципи і структуру та базується на розвитку концепції ресурсообмежених резильєнтних систем, принципах всебічного врахування синергетичності збурюючих чинників, мета-оптимізації резильєнтності та зміни реконфігураційних надбудов. Методологія забезпечує узгоджений вибір засобів підготовки до збурень, їх поглинання, відновлення функціональної ефективності та адаптації з урахуванням обчислювальних, часових й інших ресурсних обмежень.

Вперше розроблено метод оцінювання резильєнтності СІАД, який ґрунтується на обчисленні інтегрального показника за траєкторією зміни функціональної ефективності під час адаптації до збурення та статистичному узагальненні результатів серії стохастичних випробувань. Метод дає змогу враховувати глибину деградації, швидкість відновлення, досягнутий після адаптації рівень функціональної ефективності та ресурсний бюджет. Його доповнено процедурою ймовірнісної РАС-верифікації виконання порогових вимог до резильєнтності.

Вперше розроблено метод мета-оптимізації резильєнтності СІАД, у якому інтегральний показник резильєнтності використовується як мета-ціль, а налаштування здійснюється за результатами траєкторій адаптації до збурень різної природи. Це забезпечує узгоджене налаштування механізмів толерування збурень і динаміки адаптації за ресурсних обмежень. Вперше розроблено багатоетапний метод навчання СІАД з керованою структурною реконфігурацією, що включає навчання в незбуреному режимі, мета-навчання за різнотипних збурень та післярозгортальну адаптацію релевантних модулів.

Удосконалено модель операцій машинного навчання СІАД шляхом введення постфактум мета-оптимізації резильєнтності, калібрування невизначеності, моніторингу функціональної ефективності й невизначеності, адаптації під час тестування та сценаріїв керованої деградації. Удосконалено нейромережну модель СІАД з параметричною реконфігурацією на основі каскадної адаптерної надбудови з

розділенням параметрів за режимами мета-оптимізації та оперативної адаптації, що забезпечує ресурсоефективну корекцію моделі без повного перенавчання базової нейромережі.

Набула подальшого розвитку модель формування синтетичних збурюючих впливів на основі уніфікованої модель-агностичної стратегії пошуку, що дає змогу формувати різнотипні реалізації збурень із заданими бюджетними обмеженнями без доступу до градієнтів або внутрішньої структури СІАД. Набула подальшого розвитку нейромережна модель СІАД з керованою структурною реконфігурацією шляхом введення диференційовних надбудов умовної активації модулів та модифікованої функції активації з насиченням і витоком, що дає змогу адаптивно змінювати активну частину обчислювального графа та обмежувати поширення збурень у глибині моделі.

Практичне значення результатів полягає у створенні інформаційних технологій оцінювання та забезпечення резильєнтності СІАД, що інтегрують формування сценаріїв збурень, контрольовані випробування, обчислення і статистичне узагальнення показника резильєнтності, мета-оптимізацію, параметричну і структурну реконфігурацію та MLOps-процедури експлуатаційної підтримки. Результати впроваджено в освітню й науково-дослідну діяльність та на підприємствах галузі.

**Ключові слова:** система інтелектуального аналізу даних, нейромережева модель, метод навчання, мета-навчання, оптимізація, робастність, адаптація, резильєнтність, несправність, змагальна атака, дрейф концепцій.

**Moskalenko V. V. Methodological Foundations and Information Technologies for the Development of Resilient Intelligent Data Analysis Systems.** – *On the rights of the Manuscript.*

Dissertation for the degree of Doctor of Technical Sciences in specialty 05.13.06 – Information Technologies (12 – Information Technologies). – Khmelnytskyi National University, Khmelnytskyi, 2026.

The dissertation formulates and solves an important scientific and applied problem of developing resilient intelligent data analysis systems (IDAS) operating under heterogeneous disturbances and computational, temporal, and other resource constraints. The aim of the research is to improve IDAS resilience by developing methodological foundations, models, methods, and information technologies for resilience assessment and assurance throughout the system life cycle.

For the first time, a methodology for the development of resilient IDAS has been proposed. It comprises a concept, principles, and a structural framework and is based on the further development of the concept of resource-constrained resilient systems, as well as on the principles of comprehensive consideration of the synergistic effects of disturbances, resilience meta-optimization, and modification of reconfiguration add-ons. The methodology provides a coordinated basis for selecting mechanisms of preparation for disturbances, their absorption, recovery of functional efficiency, and subsequent adaptation under resource constraints.

For the first time, a method for assessing IDAS resilience has been developed based on calculating an integral resilience indicator along trajectories of functional-efficiency changes during adaptation to disturbances and statistically aggregating the results over a

series of stochastically generated trials. The method accounts for the depth of performance degradation, recovery dynamics, the functional-efficiency level achieved after adaptation, and the available resource budget. The assessment method is supplemented by a probabilistic PAC-verification procedure for checking compliance with specified threshold resilience requirements.

For the first time, an IDAS resilience meta-optimization method has been developed that uses the integral resilience indicator as a meta-objective and performs meta-learning based on adaptation trajectories under heterogeneous disturbances. This enables coordinated tuning of disturbance-tolerance mechanisms and adaptation dynamics while accounting for resource constraints. For the first time, a multi-stage training method for IDAS with controlled structural reconfiguration has also been developed. It combines training under undisturbed conditions, meta-learning under heterogeneous disturbances, and post-deployment adaptation of relevant modules to new data, thereby enabling adaptive redistribution of computational resources.

The machine learning operations model for IDAS has been improved by introducing post hoc resilience meta-optimization, uncertainty calibration, monitoring of functional efficiency and uncertainty, test-time adaptation, and controlled-degradation scenarios. These procedures provide operational support for resilience throughout the IDAS life cycle.

The neural-network IDAS model with parametric reconfiguration has been improved through parallel module correction implemented as a cascaded adapter-based add-on with parameter separation between meta-optimization and operational adaptation modes. This enables resource-efficient adaptation without complete retraining of the base neural network and reduces the computational and memory costs of resilience assurance.

The model for generating synthetic disturbances has been further developed using a unified model-agnostic search strategy. Different disturbance classes are represented by parameterized operators subject to predefined budgets, while particular realizations can be produced either by representative sampling or by directed search for boundary cases without access to gradients or the internal structure of the IDAS model.

The neural-network IDAS model with controlled structural reconfiguration has been further developed by introducing differentiable add-ons for conditional activation of base-model modules and a modified activation function with saturation and leakage. This makes it possible to adaptively modify the active part of the computational graph depending on the current state of the data, disturbance manifestations, uncertainty, and the available resource budget, as well as to limit disturbance propagation through deeper model layers.

The practical significance of the obtained results consists in developing information technologies for IDAS resilience assessment and assurance. They integrate disturbance-scenario generation, controlled testing, calculation and statistical aggregation of resilience indicators, meta-optimization, parametric and structural reconfiguration, and MLOps procedures for operational resilience support. The research results have been implemented in educational and research activities and at industrial enterprises.

**Keywords:** intelligent data analysis system, neural network model, training method, meta-learning, optimization, robustness, adaptation, resilience, fault, adversarial attack, concept drift.