

Міністерство освіти та науки України
Сумський державний університет
(СумДУ)
Адреса: 40007, м. Суми, вул. Римського-Корсакова, 2
тел. (0542) 33-54-79 факс (0542) 33-54-79

ПОГОДЖУЮ
Проректор з наукової роботи
д-р. фіз.-мат. наук, професор

_____ Анатолій ЧОРНОУС

ПРОМІЖНИЙ ЗВІТ
за результатами виконання етапу наукової (науково-технічної) роботи
(звіт про проміжні результати проекту)
*«Інформаційна технологія забезпечення резильєнтності систем штучного
інтелекту для захисту кібер-фізичних систем»*

Науковий керівник проекту,
доцент, канд. техн. наук

В'ячеслав МОСКАЛЕНКО

Підготовку звіту завершено 22 грудня 2023 р.
основна частина

1. Номер державної реєстрації проєкту: 0122U000782
2. Номер договору, за яким надається фінансування (за наявності): -
3. Найменування організації-виконавця проєкту/грантоотримувача: Сумський державний університет
4. Прізвище та ім'я наукового керівника (головного дослідника, principal investigator (PI)) проєкту: Москаленко В'ячеслав
5. Місце основної роботи наукового керівника: кафедра комп'ютерних наук Сумського державного університету
6. Терміни та тривалість виконання проєкту:
 - Тривалість проєкту 36 місяців
 - Початок 01.01.2022
 - Закінчення 31.12.2024
 - Тривалість звітнього етапу 12 місяців
 - Початок 01.01.2023
 - Закінчення 31.12.2023
7. Обсяги фінансування проєкту:
 - Загальний обсяг фінансування:
 - за запитом (заявкою) 2298,1 тис.грн (*формат 1000,5*)
 - фактичний 2298,1 тис.грн
 - Обсяг фінансування звітнього етапу:
 - за запитом (заявкою) 772,800 тис.грн
 - фактичний 772,800 тис.грн
8. Перелік виконавців з оплатою праці:
 - молоді вчені*
 - Москаленко В'ячеслав Васильович, доцент кафедри комп'ютерних наук, пнс;
 - Москаленко Альона Сергіївна, старший викладач кафедри комп'ютерних наук, снс;
 - Коробов Артем Геннадійович, старший викладач кафедри комп'ютерних наук, снс;
 - Бойко Ольга Василівна, старший викладач кафедри інформаційних технологій, снс;
 - Нагорний Володимир В'ячеславович, доцент кафедри інформаційних технологій, снс;
 - аспіранти*
 - Кудрявцев Антон Михайлович, аспірант кафедри комп'ютерних наук, договір ЦПХ;
 - Мироненко Микита Ігорович, аспірант кафедри комп'ютерних наук, договір ЦПХ;
 - Зарецький Микола Олександрович, аспірант кафедри комп'ютерних наук, мнс;
 - студенти*
 - Москвін Данііл Михайлович, студент кафедри комп'ютерних наук, договір ЦПХ;
 - Хібарний Тарас Олегович, студент кафедри комп'ютерних наук, договір ЦПХ.

(Додаток 1 до звіту).
9. Стислий зміст проєкту в цілому (актуальність, мета, основні завдання, ідеї, гіпотези тощо) (до 20 рядків):

Технології штучного інтелекту стають невід'ємною їх частиною кіберфізичних систем і виконують функції кіберзахисту, механізмів адаптації, функціональної діагностики, предиктивного обслуговування тощо. Проте самі технології штучного

інтелекту мають ряд вразливостей і їх використання в складі об'єктів критичної інфраструктури чи системах військового призначення під дією деструктивних збурень може призвести до значних матеріальних збитків і небажаних людських жертв.

Метою проєкту є розроблення інформаційної технології забезпечення резильєнтності систем штучного інтелекту до комплексного впливу деструктивних збурень, характерних для кіберфізичних систем. Для досягнення поставленої мети планується вирішити такі завдання: 1) аналіз деструктивних впливів на системи штучного інтелекту в середовищі кіберфізичних систем та існуючих методів захисту для розроблення архітектури генератора комплексних деструктивних впливів; 2) розроблення моделей і методів вимірювання, оптимізації та сертифікації резильєнтності систем штучного інтелекту до комплексного впливу деструктивних збурень; 3) розроблення проактивних та реактивних моделей і методів забезпечення резильєнтності систем штучного інтелекту; 4) розроблення моделей і методів керованої деградації та алгоритмів динамічного функціонально-вартісного аналізу елементів захисту від деструктивних впливів за умов ресурсних та інформаційних обмежень; 5) програмна реалізація та впровадження резильєнтних систем штучного інтелекту для захисту кібер-фізичних систем різного призначення.

10. Основні результати виконання попереднього (за наявності) етапу (до 20 рядків):

1. Систематизуючі таблиці, таксономічні та онтологічні схеми, що описують характеристики деструктивних впливів та існуючих методів захисту систем штучного.

2. Структурні схеми та алгоритми оцінювання резильєнтності інтелектуального алгоритму до інжекції несправностей в пам'яті, шуму протиборчих атак та дрейфу концепцій.

3. Структурні схеми, алгоритми та програмна реалізація для генерації деструктивних збурень та ймовірнісної сертифікації резильєнтності інтелектуальної системи.

4. Програмна реалізація робастних алгоритмів класифікаційного аналізу зображень.

11. Номер та назва звітнього етапу (за наявності):

2-й етап. Розроблення комплексних методів захисту системи штучного інтелекту від деструктивних впливів, характерних для кіберфізичних систем

12. Опис процесу реалізації (хід виконання, які дослідження проводились, які методики використовувались тощо) проєкту за звітнім етапом (до 50 рядків):

На початку II етапу виконання наукової роботи здійснювався аналіз існуючих моделей і методів забезпечення резильєнтності інтелектуальних інформаційних систем до різнотипних збурюючих впливів, побудовано порівняльні таблиці, онтологічні та таксономічні схеми. За результатами аналізу було запропоновано алгоритми мета-навчання, що оптимізують інтегральний критерій резильєнтності до збурень, і забезпечують робастність та швидку адаптацію до нових реалізацій збурень. Імітаційне моделювання здійснювалося для системи класифікаційного аналізу, оскільки вони вважаються найбільш вразливими до різного роду збурень. При цьому навчальні і тестові дані формувалися з відкритих наборів даних CIFAR-10 та CIFAR-100, що полегшує відтворення результатів, а також порівняння з результатами інших

дослідників. Експериментально доведено перевагу мета-навчання на результатах адаптації до синтетичних збурень з точки зору резильєнтності до нових реалізацій збурень порівняно зі звичайним навчання в умовах дії збурень.

13. Результати виконання звітнього етапу відповідно до технічного завдання/календарного плану:

13.1 Заплановані завдання звітнього етапу проєкту (*перерахуйте завдання звітнього етапу, окреслені у запиті (технічному завданні/календарному плані) проєкту*) (до 20 рядків):

1. Моделі систем штучного інтелекту з проактивним захистом.
2. Моделі систем штучного інтелекту з реактивним захистом.
3. Методи навчання та мета-навчання для супротиву деструктивним збуренням.
4. Інформаційне та алгоритмічне забезпечення для комплексного захисту систем штучного інтелекту.

13.2 Отримані результати звітнього етапу проєкту (*опишіть отримані результати виконавцями протягом звітнього періоду, посилаючись на заплановані та досягнуті цілі, задачі та індикатори виконання, згадані в технічному завданні/календарному плані дослідження. Включіть посилання на публікації у наукових виданнях, інші показники з п. 18, що є підтвердженням досягнення результатів виконання етапу, якщо такі показники передбачені*) (до 70 рядків):

1. Систематизуючі порівняльні таблиці, онтологічні та таксономічні схеми методів забезпечення резильєнтності систем штучного інтелекту на різних етапах протидії різнотипним збурюючим впливам [1, 3, 6, 9]. Цей результат частково забезпечує заплановані результати 1 та 2.
2. Метод підвищення резильєнтності інтелектуальної системи до деструктивних збурень шляхом ресурсоефективного доповнення моделі аналізу даних згортковими адаптерами та мета-адаптерами, які оптимізуються в процесі мета-навчання [9, 2, 12, 13]. Цей результат у поєднанні з попереднім результатом остаточно забезпечує заплановані результати 1 та 2.
3. Градієнтний метод мета-навчання для оптимізації резильєнтності системи штучного інтелекту до протиборчих атак, відмов у пам'яті [2]. Цей результат забезпечує запланований результат 3, але тільки для диференційованих моделей і метрик продуктивності чи їх сурогатних версій. Експериментально підтверджено підвищення інтегрального критерію резильєнтності порівняно з традиційним навчання в умовах дії збурень.
4. Метод мета-навчання нейронних мереж для оптимізації недиференційованих метрик продуктивності і резильєнтності шляхом оцінювання градієнту на результатах адаптації зі збуреними версіями параметрів [2, 6]. Цей результат забезпечує запланований результат 3 для моделей будь-якої архітектури, однак потребує більше ітерацій. Експериментально підтверджено підвищення інтегрального критерію резильєнтності порівняно з традиційним навчання в умовах дії збурень.
5. Інформаційне та алгоритмічне забезпечення інтелектуальної системи з оптимізованою моделлю аналізу даних для підвищення резильєнтності в

режимах прийняття рішень та адаптації [4, 5, 6, 7, 10, 11]. Цей результат забезпечує 4 запланований результат. При цьому з'ясовано перспективи використання принципів резильєнтності для систем інтелектуального аналізу даних до задач діагностування метало-оброблювального інструменту, керування розподілом електроенергії та комп'ютерно-технічної криміналістичної експертизи документів [3, 4, 5, 10].

13.3 Відхилення від календарного плану дослідження (за наявності) *(вказіть та детально обґрунтуйте можливі відхилення від технічного завдання/календарного плану дослідження та їх потенційний вплив на подальше виконання проєкту (до 30 рядків):*

Суттєвих відхилень немає, проте було виявлено що питання реактивного і проактивного захисту інтелектуальних систем можливо вирішувати уніфікованим шляхом за рахунок вибору надстройок над основною моделлю та застосування мета-навчання на результатах адаптації до збурень. Це не впливає на подальше виконання проєкту.

14. Наукова цінність і актуальність отриманих результатів (науково-технічної продукції), їх порівняння з українськими та/або кращими закордонними аналогами (до 30 рядків):

Існуючі моделі і методи забезпечення резильєнтності інтелектуальних систем сфокусовані лише на одному з аспектів резильєнтності, наприклад робастності або здатності до адаптації на невеликій кількості навчальних зразків. На відміну від існуючих моделей і методів, запропоновані моделі і методи сфокусовані на одночасному забезпеченні як робастності, так і здатності до швидкої адаптації до збурень.

Існуючі моделі і методи забезпечення резильєнтності інтелектуальних систем сфокусовані на захисті від одного з типів збурюючого впливу. При цьому не гарантується сумісність даних методів за умови їх одночасного застосування, що може нівелювати їх ефективність. На відміну від існуючих моделей і методів, запропоновані моделі і методи що передбачають одночасний захист від різнотипних збурень без змін базової моделі за рахунок додавання універсальних адаптерів та мета-адаптерів. Мета-адаптери налаштовуються під час мета-навчання, а адаптери налаштовуються під час точної настройки під конкретну задачу.

Більшість методів навчання та мета-навчання є градієнтними і підходять лише для диференційованих моделей штучного інтелекту. Крім того і цільова функція або функція втрат так само не можуть кодувати валідаційну метрику, а тим більше інтегральний критерій резильєнтності. На відміну від існуючих методів, пропонується метод мета-навчання здатний оптимізувати недиференційований прямий критерій резильєнтності за рахунок оцінювання градієнту на результатах адаптації до збурень.

15. Практична цінність результатів для потреб оборони, безпеки, економіки та/або суспільства України (у разі наявності) (до 30 рядків):

Запропоновані моделі і методи дозволяють підвищити рівень автономності і

живучості інтелектуальних систем за умов впливу збурюючих факторів, що має практичну цінність для роботизованих систем військового призначення. Запропоновані алгоритми дозволяють здійснювати оптимізацію резильєнтності, тобто робастності і швидкості відновлення ефективності, для інтелектуальних систем за умов ресурсних обмежень, що актуально для малогабаритних безпілотних апаратів.

Тобто найбільш актуальним місцем застосування резильєнтних систем штучного інтелекту є безпілотні апарати та інтелектуальні автоматизовані системи військового призначення, оскільки це забезпечує підвищення їх автономності, надійності, живучості, відмовостійкості в умовах комплексного впливу деструктивних збурень.

Реалізація запропонованих моделей і методів частково впроваджена шляхом надання послуг з розроблення програмного забезпечення резильєнтної системи машинного зору для відслідковування об'єктів інтересу в рамках виконання договору № 52.17-2023.СП/01 від 25.10.2023 між СумДУ та ТОВ "АЙ ЕС АР ДЕФЕНС", а також послуг "Дослідження та розробка систем машинного зору для роботизованого комплексу" в рамках виконання договору № 15.01-2023.СП/01 від 02.11.2023 між СумДУ та ФОП ЛЕОНТЬЄВ Петро Володимирович, а також шляхом виконання робіт з удосконалення технології навігації безпілотних апаратів за підтримки субвенції з обласного бюджету згідно розпорядження голови Сумської ОДА від 11.08.2023 р. № 387 - ОД.

16. Основні кількісні показники/індикатори* виконання звітнього етапу **за темою** проекту (у звіті залишити лише ті показники з таблиці, які планувались у запиті (заявці/договорі на отримання фінансування (надання грантової підтримки)), із зазначенням відповідного фактичного кількісного виконання цих показників/індикаторів. Якщо у запиті (заявці тощо) кількісні показники не планувались, то у звіті можуть зазначатись лише показники у разі їх наявності виконання):

№ з/п	Показники/індикатори	Заплановано (відповідно до запиту на фінансування /ТЗ/КП тощо), кількість	Виконано (за результатами етапу), кількість
1.	Публікація результатів:	3	9
1.1.	Статті у журналах, що індексуються наукометричними базами даних: - Scopus та/або Web of Science Core Collection, всього, од.	2	5
	з них із кuartилем Q1 і Q2 на момент опублікування, од.	0	1
	з них із кuartилем Q3 і Q4 на момент опублікування, од.	2	4
1.2.	Статті у виданнях, які містять інформацію з обмеженим доступом (для проєктів оборонного та/або подвійного призначення), од.	0	0
1.3.	Статті у наукових журналах (без кuartилу), збірниках наукових праць, матеріалах конференцій тощо, що індексуються наукометричними базами даних Scopus або Web of Science Core Collection (крім тих, що увійшли до п.1.1), од.	1	2
1.4.	Статті у фахових виданнях України категорії «Б», од.	0	0
1.5.	Статті у періодичних виданнях інших країн, що мають ISSN, од.	0	0
1.6.	Публікації у матеріалах конференцій, тезах доповідей та виданнях, що	0	2

№ з/п	Показники/індикатори	Заплановано (відповідно до запиту на фінансування /ТЗ/КП тощо), кількість	Виконано (за результатами етапу), кількість
	не включені до переліку наукових фахових видань України та не індексуються наукометричними базами даних Scopus або Web of Science Core Collection, од.		
1.7.	Монографії та розділи монографій, опубліковані (або підготовлені і подані до друку) у закордонних видавництвах іноземними мовами, од.	0	0
1.8.	Монографії та розділи монографій, опубліковані (або підготовлені і подані до друку) в українських видавництвах, од.	0	0
1.9.	Монографії та розділи монографій, опубліковані (або підготовлені і подані до друку) з обмеженим доступом (для проєктів оборонного та/або подвійного призначення), од.	0	0
1.10.	Підручники, навчальні посібники, од.	0	0
1.11.	Словники, довідники, енциклопедії, видані українськими та/або закордонними видавництвами, од.	0	0
1.12.	Інші публікації, які не описані у пп. 1.1-1.11, од.	0	0
2.	Презентація та дисемінація результатів:	1	2
2.1.	Міжнародні науково-комунікативні заходи, конференції, од.	1	2
2.2.	Всеукраїнські та регіональні науково-технічні/промислові виставкові заходи, од.	0	0
2.3.	Представлення розробки/бізнес-плану/результатів проєкту на:	0	0
	- інноваційних фестивалях, од.	0	0
	- конкурсах стартапів, од.	0	0
	- акселераційних програмах, од.	0	0
	- хакатонах, од.	0	0
2.4.	Науково-популярні публікації з метою поширення інформації про результати проєкту для загальної (широкої) аудиторії, од.	0	0
2.5.	Представлення інформації про результати проєкту на науково-популяризаційних заходах (Дні науки, Наукові пікніки тощо), од.	0	0
2.6.	Інші заходи, які не описані у пп. 2.1-2.5, од.	0	0
3.	Підготовка наукових кадрів:	0	2
3.1.	Захищено дисертацій доктора наук авторами проєкту або під консультуванням авторів у рамках тематики проєкту, од.	0	0
3.2.	Захищено дисертацій доктора філософії авторами проєкту або під керівництвом авторів у рамках тематики проєкту, од.	0	2
4.	Охоронні документи на об'єкти права інтелектуальної власності (ОПІВ)	2	2
4.1.	Отримано патентів України на винахід, од.	0	0
4.2.	Отримано патентів України на промисловий зразок, од.	0	0
4.3.	Отримано патентів України на корисну модель, од.	1	0
4.4.	Отримано охоронний документ на ОПІВ інших країн, од.	0	0
4.5.	Інші ОПІВ, які не описані у пп. 4.1-4.4, од.	1	2
4.6.	Подано заявок на отримання охоронного документу на ОПІВ України та /або інших країн, од.	0	0
5.	Впровадження та використання наукових або науково-технічних (прикладних) результатів:	1	4
5.1.	Підписання (укладання) договорів (угод) організацією-виконавцем проєкту (грантоотримувачем) на впровадження (використання) результатів проєкту (окрім індивідуальних), серед них:	1	3
5.1.1.	Господарських договорів/контрактів, од./тис.грн	1/ 56,00	3/ 129,137
5.1.2.	Ліцензійних договорів/договорів на ноу-хау, од./тис.грн	0	0
5.1.3.	Грантових угод (держаного рівня), од./тис.грн	0	0
5.1.4.	Грантових угод (міжнародного рівня), од./тис.грн	0	0
5.1.5.	Інші договори (угоди), які не описані у пп. 5.1.1-5.1.3, од./тис.грн	0	1/ 40,000

№ з/п	Показники/індикатори	Заплановано (відповідно до запиту на фінансування /ТЗ/КП тощо), кількість	Виконано (за результатами етапу), кількість
5.2.	Документально підтверджено використання результатів у практиці органів державної/місцевої влади, суспільних практиках тощо, од.	0	0
5.3.	Проведено маркетингові дослідження, перемовини з потенційними замовниками із підписанням протоколу (меморандуму, угоди) про наміри комерційного впровадження результатів, од.	0	0
5.4.	Подано заявок на державні, міжнародні наукові гранти (окрім індивідуальних), од.	0	0
5.5.	Впроваджено у освітній процес ЗВО/НУ з відповідним підтвердженням, од.	0	1
5.6.	Інші варіанти впровадження, які не описані у пп. 5.1-5.5, од.	0	0
6.	Створено чи істотно удосконалено/покращено існуючі:	1	1
6.1.	Пристрої (макет, експериментальний/дослідний зразок), од.	0	0
6.2.	Матеріали, процеси, технології, технологічні регламенти, цифрові продукти та електронні сервіси, од.	1	1
6.3.	ТУ, ДСТУ, будівельні норми, зареєстровані проекти законодавчих актів, од.	0	0
6.4.	Наукові (науково-технічні) послуги, од.	0	0
6.5.	Іншу продукцію, яка не описана у пп. 6.1-6.4, од.	0	0
7.	Участь з оплатою у виконанні проєкту (штатних одиниць/осіб) згідно з Додатком 1:	6	10
7.1.	Студентів (здобувачів вищої освіти I-II рівнів), шт.од./ осіб	1	2
7.2.	Аспірантів (здобувачів вищої освіти III рівня), шт.од./ осіб	1	3
7.3.	Молодих вчених, шт.од./ осіб	4	5

* - до показників/індикаторів таблиці п. 16 не можуть бути включені будь-які публікації (включно із співавторством), конференції, впровадження, охоронні документи на об'єкти права інтелектуальної власності тощо держав (їх представників), визнаних в установленому порядку державою-агресором або державою-окупантом, або держав, що не визнають тимчасово окуповані, починаючи з березня 2014 року, території України такими, що належать Україні.

17. Відхилення від запланованих показників/індикаторів, зазначених у п. 16 (у разі наявності зазначити і обґрунтувати причини таких відхилень та їх вплив на подальше виконання проєкту) (до 20 рядків):

Було заплановано 1 патент на корисну модель та 1 авторське свідоцтво. Натомість було зроблено два авторські свідоцтва, а патент перебуває на етапі формування заявки. Це пов'язано з тим, що під час виконання господарських договорів були з'ясовані нові факти, врахування яких потребує додаткового часу, але збільшить комерційну цінність даного охоронного документу.

18. Вихідні дані щодо показників виконання відповідно до пунктів п. 16 (зазначити дані про публікації, конференції, захисти дисертацій, отримання ОПВ, впровадження, створення НТП, залучення молодих вчених, студентів, аспірантів тощо) з додаванням WEB-посилання (за наявності) на ресурси, де вони розміщені (Додаток 2 до звіту):

Публікації у періодичних виданнях

1. Moskalenko, V., Kharchenko, V., Moskalenko, A., & Kuzikov, B. (2023). Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods. In

Algorithms (Vol. 16, Issue 3, p. 165). MDPI AG. <https://doi.org/10.3390/a16030165> (**Scopus, Web of Science, Q2**)

2. Moskalenko, V. V. (2023). MODEL-AGNOSTIC META-LEARNING FOR RESILIENCE OPTIMIZATION OF ARTIFICIAL INTELLIGENCE SYSTEM. In Radio Electronics, Computer Science, Control (Issue 2, p. 79). National University “Zaporizhzhia Polytechnic” <https://doi.org/10.15588/1607-3274-2023-2-9> (**Web of Science, Q4**)

3. Boiko, M., Moskalenko, V., & Shovkoplias, O. (2023). Advanced file carving: ontology, models and methods. In Radioelectronic and Computer Systems (Issue 3, pp. 204–216). National Aerospace University - Kharkiv Aviation Institute. <https://doi.org/10.32620/reks.2023.3.16> (**Scopus, Q3**)

4. Panda, A., Nahorni, V. A Forecasting the Cutting Tool Life Considering as a Blow-up Mode Its Operation. MM Science Journal, №2, pp. 6478–6483 (2023). DOI : 10.17973/MMSJ.2023_06_2023019. (**Scopus**)

5. Nahorni, V., Cataldi, D., Straser, V. NEW EFFECTIVE DISASTER FORECASTING METHODOLOGY. MM Science Journal, №3, pp. 6662-6667 (2023). DOI : 10.17973/MMSJ.2023_10_2023017. (**Scopus**)

Публікації у матеріалах конференцій

6. Moskalenko V.V. Meta-learning with evolutionary strategy for resilience optimization of image recognition system. Proceedings of The 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 7-9 September, 2023, Dortmund, Germany, 5 p. (**Scopus, In press**)

7. Olha Boiko, Vira Shendryk, Reza Malekian, Anton Komin, Paul Davidsson, Towards Data Integration for Hybrid Energy System Decision-Making Processes: Challenges and Architecture, International Conference on Information and Software Technologies 2023 (ICIST 2023), Springer Communications in Computer and Information Science, 2023 (**Scopus, In press**).

8. М. О. Зарецький, “Нейромережеве вимірювання рівня води в трубопроводі водовідведення за даними відеоінспекції,” Міжнародна наукова конференція молодих учених Інформатика, Математика, Автоматика, ІМА-2023. Суми, Україна - Астана, Казахстан, 24–28 квітня 2023, С. 45-46. Available:https://essuir.sumdu.edu.ua/bitstream-download/123456789/91550/1/Conf_IMA_2023.pdf

9. Москаленко В.В. Методи забезпечення резильєнтності систем штучного інтелекту/ Москаленко В.В, Москвін Д. О. // Міжнародна наукова конференція молодих учених Інформатика, Математика, Автоматика, ІМА-2023. – Суми, Україна - Астана, Казахстан, 24–28 квітня 2023, ст. 145. - https://itp.elit.sumdu.edu.ua/wp-content/uploads/2023/05/Abstracts_Book_IMA-2023.pdf

Охоронні документи на об'єкти права інтелектуальної власності

10. Свідоцтво про реєстрацію авторського права на твір «Мобільний iOS додаток прогнозування споживання електричної енергії промисловим підприємством з

безперервним циклом виробництва», №121810, Україна / Бойко О. В.; СумДУ; опубл. 11.12.2023.

11. Свідоцтво про реєстрацію авторського права на твір «Інтелектуальний детектор дронів та гелікоптерів за акустичним сигналом з підвищеним рівнем робастності до фонових завад» № 116160 Україна / Москаленко В.В., Москаленко А.С., Зарецький М.О, Коробов А. Г.; СумДУ; опубл. 2023-01-25.

Захищені дисертаційні роботи

12. Зарецький Микола Олександрович «Моделі та методи інтелектуальної інформаційної технології оцінювання функціонального стану труб водовідведення », спеціальність 122 – Комп'ютерні науки, дата захисту – 06.09.2023 р. Місце захисту – Сумський державний університет. <https://svr.naqa.gov.ua/#/defense/1975>.

13. Мироненко Микита Ігорович «Моделі і методи інформаційної технології машинного навчання автономного безпілотного літального апарату для відеомоніторингу місцевості», спеціальність 122 – Комп'ютерні науки, дата захисту - 24.11.2023 р. Місце захисту – Сумський державний університет. <https://svr.naqa.gov.ua/#/defense/2550>.

19. Рішення наукової ради Сумського державного університету щодо результатів розгляду проміжного звіту: про відповідність виконаних за проектом робіт технічному завданню/календарному плану, протокол № 9 від 30 листопада 2023 р.

(Додаток 3 до звіту)

20. Анотація основних результатів звітної етапу проекту *(готується українською та англійською мовами (до 30 рядків кожною мовою), у форматі, придатному для розуміння загальною аудиторією (науково-популярним стилем) (Додаток 4 до звіту).*

Додаток 1 до проміжного звіту

Перелік виконавців проєкту з оплатою праці

№	Прізвище, ім'я, науковий ступінь, вчене звання (особистий підпис, у разі необхідності)	Основне місце роботи або здобуття освіти	Зазначити вік та наявність статусу молодого вченого (на момент подання звіту)	Посада за проєктом (або договір ЦПХ) та роль у проєкті (керівник, відповідальний виконавець, студент, аспірант тощо)	Основні завдання у проєкті (стисло зазначити функції)
1	Москаленко В'ячеслав Васильович	Сумський державний університет, кафедра комп'ютерних наук	34 роки, молодий вчений	пнс, керівник проєкту	Формулювання завдань, координація і підготовка звітів про їх виконання, а також участь у виконанні досліджень, аналізі результатів і написанні наукових праць.
2	Москаленко Альона Сергіївна	Сумський державний університет, кафедра комп'ютерних наук	31 рік, молодий вчений	снс, відповідальний виконавець	Формування звітної документації, ведення таблицю обліку використання робочого часу, участь виконанні досліджень і написанні наукових праць.
3	Коробов Артем Геннадійович	Сумський державний університет, кафедра комп'ютерних наук	30 рік, молодий вчений	снс, виконавець	Проведення експериментальних досліджень та аналіз результатів, написання публікацій та розроблення програмного забезпечення.
4	Зарецький Микола Олександрович	Сумський державний університет, кафедра комп'ютерних наук	31 рік, молодий вчений	мнс, виконавець	Проведення експериментальних досліджень, аналіз ефективності застосування розроблених алгоритмів в галузях моніторингу технічних та інфраструктурних об'єктів.
є	Бойко Ольга Василівна	Сумський державний університет, кафедра інформаційних технологій	33 роки, молодий вчений	снс, виконавець	Розроблення програмного забезпечення та аналіз ефективності застосування розроблених алгоритмів

№	Прізвище, ім'я, науковий ступінь, вчене звання (особистий підпис, у разі необхідності)	Основне місце роботи або здобуття освіти	Зазначити вік та наявність статусу молодого вченого (на момент подання звіту)	Посада за проектом (або договір ЦПХ) та роль у проєкті (керівник, відповідальний виконавець, виконавець, студент, аспірант тощо)	Основні завдання у проєкті (стисло зазначити функції)
					в галузях моніторингу технічних та інфраструктурних об'єктів.
6	Нагорний Володимир В'ячеславович	Сумський державний університет, кафедра інформаційних технологій	34 роки, молодий вчений	снс, виконавець	Розроблення програмного забезпечення та аналіз ефективності застосування розроблених алгоритмів в галузях моніторингу технічних та інфраструктурних об'єктів.
7	Мироненко Микита Ігорович	Сумський державний університет, кафедра комп'ютерних наук	27 років	Договір ЦПХ, аспірант	Розроблення моделей адаптерів та мета-адаптерів для оптимізації резильєнтності систем штучного інтелекту до збурень.
8	Кудрявцев Антон Михайлович	Сумський державний університет, кафедра комп'ютерних наук	24 роки	Договір ЦПХ, аспірант	Програмна реалізація алгоритму мета-навчання для оптимізації резильєнтності.
9	Москвін Данііл Олександрович	Сумський державний університет, кафедра комп'ютерних наук	21 рік	Договір ЦПХ, студент	Проведення експериментальних досліджень резильєнтності систем класифікаційного аналізу.
10	Хібарний Тарас Олегович	Сумський державний університет, кафедра комп'ютерних наук	21 рік	Договір ЦПХ, студент	Програмна реалізація алгоритму оптимізації резильєнтності систем штучного інтелекту до деструктивних впливів.

Додаток 2
до проміжного звіту

Копії наукових публікацій, охоронних документів, іншої друкованої наукової продукції

Додаток 3
до проміжного звіту

Копія витягу з протоколу засідання відповідної ради (органу) щодо результатів розгляду проміжного звіту

Додаток 4 до проміжного звіту

Під час виконання НДР систематизовано методи забезпечення резильєнтності систем штучного інтелекту на різних етапах протидії різнотипним збурюючим впливам. Крім того було запропоновано метод підвищення резильєнтності інтелектуальної системи до деструктивних збурень шляхом ресурсоефективного доповнення моделі аналізу даних згортковими адаптерами та мета-адаптерами, які оптимізуються в процесі мета-навчання. Для навчання адаптерів та мета-адаптерів розроблено градієнтний метод мета-навчання, що здійснює оптимізацію резильєнтності системи штучного інтелекту до протиборчих атак, відмов у пам'яті та зміни задач. Отримали подальшого розвитку методи мета-навчання нейронних мереж для оптимізації недиференційованих метрик продуктивності і резильєнтності шляхом оцінювання градієнту на результатах адаптації зі збуреними версіями параметрів. Експериментально доведено перевагу мета-навчання на результатах адаптації до синтетичних збурень з точки зору резильєнтності до нових реалізацій збурень порівняно зі звичайним навчання в умовах дії збурень.

Запропоновані моделі і методи дозволяють підвищити рівень автономності і живучості інтелектуальних систем за умов впливу збурюючих факторів, що має практичну цінність для роботизованих систем військового призначення. Крім того, запропоновані алгоритми дозволяють здійснювати оптимізацію резильєнтності, тобто робастності і швидкості відновлення ефективності, для інтелектуальних систем за умов ресурсних обмежень, що актуально для малогабаритних безпілотних апаратів. Реалізація моделей і методів частково впроваджена шляхом надання послуг з розроблення програмного забезпечення резильєнтної системи машинного зору для відслідковування об'єктів інтересу, послуг з розроблення систем машинного зору для роботизованого комплексу, а також виконання робіт з удосконалення технології навігації БПЛА за кошти субвенції з обласного бюджету згідно розпорядження голови Сумської ОДА від 11.08.2023 р. № 387-ОД. Одержані результати частково впроваджені у навчальний процес, зокрема під час викладання дисциплін «Мови програмування інтелектуальних систем» та «Вступ до науки про дані».

During the scientific research work, methods for ensuring the resilience of artificial intelligence systems were systematically organized at various stages of countering different types of disruptive influences. Additionally, a method for enhancing the resilience of an intelligent system to destructive disturbances was proposed, through resource-efficient augmentation of the data analysis model with convolutional adapters and meta-adapters, which are optimized during meta-learning. A gradient method for meta-learning was developed to train these adapters and meta-adapters, optimizing the resilience of the artificial intelligence system to adversarial attacks, memory failures, and task changes. Further developments were made in the methods of meta-learning of neural networks for optimizing non-differentiable performance and resilience metrics by evaluating the gradient on the results of adaptation with disturbed versions of parameters. The advantage of meta-learning in adapting to synthetic disturbances in terms of resilience to new implementations of disturbances compared to conventional training under disturbance conditions was experimentally proven.

The proposed models and methods enhance the level of autonomy and survivability of intelligent systems under the influence of disruptive factors, which is of practical value for robotic systems of military purpose. Moreover, the proposed algorithms enable the optimization of resilience, i.e., robustness and recovery speed, for intelligent systems under resource constraints, which is relevant for small unmanned aerial vehicles. The implementation of these models and methods has been partially introduced through the provision of services for developing software for a resilient machine vision system for tracking objects of interest, developing machine vision systems for a robotic complex, and improving UAV navigation technology with funds from a regional budget subsidy according to the order of the head of the Sumy Regional State Administration dated 11.08.2023, No. 387-OD. The obtained results have been partially implemented in the educational process, particularly in the teaching of the disciplines "Programming Languages for Intelligent Systems" and "Introduction to Data Science".