Облікова картка НДДКР

Державний обліковий номер: 0225U002644

Державний реєстраційний номер: 0123U102106

Відкрита

Дата реєстрації: 25-03-2025

1. Етапи виконання

Номер етапу: 2

Назва етапу: Теоретичні та експериментальні дослідження з розробки кейс-орієнтованих методів оцінювання, інтерфейсів та технології верифікації ПСКЗ

Початок етапу: 01-2024

Закінчення етапу: 12-2024

Вид звітного документа: Остаточний звіт

2. Виконавець

Назва організації: Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"

Код ЄДРПОУ/ІПН: 02066769

Підпорядкованість: Міністерство освіти і науки України

Адреса: вул. Чкалова, буд. 17, м. Харків, Харківський р-н., Харківська обл., 61070, Україна

Телефон: 380573151131

Телефон: 380573151056

E-mail: khai@khai.edu

WWW: http://www.khai.edu

3. Власник результатів НДДКР (продукції)

Назва організації: Міністерство освіти і науки України

Код ЄДРПОУ/ІПН: 38621185

Адреса: проспект Берестейський, буд. 10, м. Київ, 01135, Україна

Підпорядкованість: Кабінет Міністрів України

Телефон: 380444813221

E-mail: mon@mon.gov.ua

WWW: https://mon.gov.ua/ua

4. Джерела та напрями фінансування

Підстава для проведення робіт: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

КПКВК: 2201040

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

Джерело фінансування: 7713 - кошти держбюджету

Фактичний обсяг фінансування за звітний етап: 873.936 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Методи та кейс-технології доказового оцінювання кібербезпеки програмовних систем для забезпечення захисту критичної IT-інфраструктури

Назва роботи (англ)

Methods and case-technologies of evidence-based assessment of software systems cybersecurity to ensure protection of critical IT infrastructure

Реферат (укр)

Розглянуто комплексний підхід до проблеми верифікації та пошуку вразливостей в ПЛІС та апаратному забезпеченні з використанням інсерційного моделювання. Математичний апарат алгебри поведінок дає змогу представити моделі ПЛІС та апаратного забезпечення у зрозумілому алгебраїчному вигляді та використати відповідні методи пошуку вразливостей та формальної верифікації. Розроблено алгебраїчні моделі для опису і виявлення вразливостей в специфікаціях електронних проєктів на різних етапах життєвого циклу, які на відміну від відомих базуються на семантиці інсерційного моделювання мовою алгебри поведінок і дозволяють забезпечити гарантовану повноту верифікації і тестування HDL компонент, електронних проєктів для ПЛІС в цілому, логіки користувацьких додатків ПСКЗ. Розроблено послідовність верифікації із використанням алгебраїчних моделей і методи тестування шляхом генерації тестів із моделей, побудованих на різних етапах розроблення, які на відміну від відомих базуються на автоматичній генерації Message sequence chart, що дозволяє забезпечити гарантовану повноту верифікації і тестування HDL компонент, електронних проєктів для ПЛІС в цілому, логіки користувацьких додатків ПСКЗ. Запропоновано комплекс складових забезпечення кібербезпеки платформ FPGA as a Service, що відповідає сучасним загрозам таких систем та включає регулярне оновлення програмного забезпечення, моніторинг та аналіз безпеки, аудит та тестування на проникнення, відповідність стандартам безпеки та навчання персоналу.

Реферат (англ)

A comprehensive approach to verifying and finding vulnerabilities in FPGAs and hardware using insertion modeling is considered. The mathematical apparatus of the algebra of behaviors makes it possible to present the FPGA and hardware models in a comprehensible algebraic form and to use the appropriate methods of finding vulnerabilities and formal verification. Algebraic models have been developed for the description and detection of vulnerabilities in the specifications of electronic projects at various stages of the life cycle, which, unlike the known ones, are based on the semantics of insertion modeling in the language of the algebra of behavior and allow to ensure the guaranteed completeness of verification and testing of HDL components, electronic projects for FPGAs in general, logic programmable systems of critical applications (PSCA) user applications. A verification sequence has been developed using algebraic models and testing methods by generating tests from models built at various stages of development, which, unlike known ones, are based on the automatic generation of a Message sequence chart, which allows for guaranteed completeness of verification and testing of HDL components, electronic projects for FPGAs in general, the logic of user applications of PSCA. A set of components for ensuring the cybersecurity of FPGA as a Service platforms is proposed, which meets modern threats of such systems and includes regular software updates, security monitoring and analysis, audit and penetration testing, compliance with security standards, and personnel training.

Індекс УДК: 519.718.2, , 511.6

Коди тематичних рубрик НТІ: 28.27.27, 20.56, 27.15.25

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Спосіб резервування системи штучного інтелекту

Назва продукції (англ): A way to back up an artificial intelligence system

Очікувані результати: Технології

Галузь застосування: Побудова та аналіз безпеки програмовних систем критичного застосування

Опис продукції (укр): Спосіб резервування системи штучного інтелекту шляхом паралельного використання кількох каналів ШІ, побудованих, зокрема, на основі штучних нейромереж, які отримують однакові вхідні дані. Працездатність каналів контролюється вбудованими засобами, а результати аналізуються для вибору даних одного з працездатних каналів. У разі відмови всіх каналів формується сигнал відмови. Особливість методу — використання різних моделей нейромереж, навчених на різних датасетах із застосуванням різних методів. Визначають зони невизначеної та потенційно небезпечної поведінки, які оновлюються після кожного донавчання або зміни моделі. Вибір вихідних даних здійснюється з урахуванням відповідності вхідних даних цим зонам. Якщо всі канали працездатні й вхідні дані не входять до небезпечних зон — використовується канал з найвищим пріоритетом. Якщо частина каналів перебуває в зоні небезпеки — вибір здійснюється з безпечних каналів. Сигнал відмови формується також за відсутності таких каналів. Сигнал невизначеності виникає, коли всі працездатні канали мають вхідні дані в зоні невизначеності, проте видача можлива, якщо така невизначеність допустима. Сигнал небезпеки формується у випадку, коли всі канали отримують дані із зон потенційної загрози. Запропонований спосіб резервування забезпечує підвищену надійність та безпеку роботи штучного інтелекту в програмованих системах критичного застосування за рахунок багатоканальної обробки даних із контролем працездатності та аналізом потенційно небезпечної поведінки. Це дозволяє вчасно виявляти відмови, невизначені або небезпечні стани й забезпечувати стабільну роботу системи навіть за умов часткових збоїв.

Соціально-економічна спрямованість НТП: Зменшення зносу обладнання

Стадія завершеності НТП: Дослідний зразок

Впровадження НТП: Не впроваджено

Строки впровадження: 01.202412.2024

Виробник продукції: Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"

Споживачі продукції: Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"

Перспективні ринки: Системи забезпечення безпеки об'єктів критичних інфраструктур

Права інтелектуальної власності: Отримано патент

Форми та умови передачі продукції: Продаж патента

7. Бібліографічний опис

Kharchenko, K., Ponochovnyi, Y., Babeshko, I. Multi-fragmental and Multi-phase Availability Models of the Safety-critical I&C Systems with Two-cascade Redundancy Authors. International Journal of electronics and telecommunications, 2024, Vol. 70 No. 1. PP. 211-218. doi: 10.24425/ijet.2024.149533

Kharchenko, V., Ponochovnyi, Y., Dotsenko, S., Illiashenko, O., Ivasiuk, O. Models of Resilient Systems with Online Verification Considering Changing Requirements and Latent Failures. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) System Dependability - Theory and Applications. DepCoS-RELCOMEX 2024. Lecture Notes in Networks and Systems, vol 1026. Springer, Cham. doi:10.1007/978-3-031-61857-4_9

Kharchenko, V., Odarushchenko, O. Trustworthy AI Systems from Un-trustworthy Components: Development von Neumann's Paradigm using Principle of Diversity. ProfIT AI 2024: 4th International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2024), September 25–27, 2024, Cambridge, MA, USA. PP. 392-404.

Tetskyi, A., Perepelitsyn, A., Illiashenko, O. Morozova, O., Uzun, D. Ensuring Cybersecurity of FPGA as a Service with the Use of Penetration Testing of Components. Radioelectronic and Computer Systems, 2024, no. 2(110). PP. 164-172 doi: 10.32620/reks.2024.2.13

Tetskyi, A., Uzun, D. Intrusion Detection and Prevention Systems as a Component of Ensuring Compliance with Regulatory

Documents. Radioelectronic and Computer Systems, 2024, no. 3(111). PP. 166-174 doi: 10.32620/reks.2024.3.11

Тецький, А.Г., Перепелицин, А.Є. Можливості використання апаратних прискорювачів у системах виявлення та запобігання вторгненням. Авіаційно-космічна техніка і технологія, 2024, No 6(200). С 94-102. doi: 10.32620/aktt.2024.6.09

Харченко В. С., Одарущенко О. М., Фесенко Г. В., Одарущенко О. Б. Спосіб резервування системи штучного інтелекту : пат. на кор. модель 156654 Україна, № u202304653; заявл. 03.10.2023 ; опубл. 24.07.2024, Бюл. № 30. 4 с. URL: https://sis.nipo.gov.ua/uk/search/detail/1809682/

Лісних, О.І., Морозова, О.І., Тецький, А.Є. Комп'ютерна програма «Вебсервіс з підписування файлів на основі цифрового підпису українського стандарту». Заяв. r202400369 від 03.12.2024

Комп'ютерна програма «Вебсервіс вибору інструментальних засобів тестування на проникнення». Заяв. c202409961 від 09.12.2024

8. Звітна документація

Кількість сторінок в звіті: 80

Мова звіту: Українська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Ілляшенко Олег Олександрович (к. т. н., доц.)

Бабешко Євген Васильович (к. т. н., доц.)

Летичевський Олександр Олександрович (д.ф.-м.н., с.н.с.)

Одарущенко Олег Миколайович (д. т. н., професор)

Тецький Артем Григорович (к. т. н.)

Керівник організації:

Литвинов Олексій Миколайович (д. ю. н., професор)

Керівники роботи:

Ілляшенко Олег Олександрович (к. т. н., доц.)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.