Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U000724

Особливі позначки: відкрита

Дата реєстрації: 31-03-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сєргєєв Євгеній Віталійович

2. Yevhenii V. Sierhieiev

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп’ютерна інженерія

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп’ютерна інженерія

Дата захисту:

Спеціальність за освітою: Комп'ютерні інженерія

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 12573

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.41, 50.53, 50.05, 50.05.13

Тема дисертації:

1. Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем

2. Methods and means of detecting vulnerabilities in computer system software

Реферат:

1. Вирішення задачі підвищення точності виявлення вразливостей у програмному забезпеченні комп'ютерних систем є однією з актуальних проблем інформаційної безпеки. Серед найбільш небезпечних помилок мов C/C++ залишаються переповнення буфера, що призводять до неконтрольованого перезапису пам'яті та можливості виконання довільного коду. Існуючі інструменти статичного та динамічного аналізу мають обмеження щодо точності, повноти та масштабованості, що зумовлює необхідність створення нових підходів, здатних формалізувати природу вразливостей та забезпечити їх автоматизоване виявлення в промислових проєктах і конвеєрах автоматизованого збирання та розгортання (CI/CD). У дисертації здійснено аналіз сучасних методів і засобів виявлення вразливостей типу переповнення буфера у програмному забезпеченні мов C/C++, підходів статичного аналізу, методів машинного навчання та нейромережевих моделей, а також можливостей їх інтеграції у процеси DevSecOps. Розроблено орієнтовану графову модель переповнення буфера, що формалізує потоки даних і керування у програмах C/C++ та забезпечує основу для кількісної оцінки ризику експлуатації вразливостей. Запропоновано метод

автоматизованого виявлення переповнень буфера, який враховує просторові та контекстні залежності між елементами програмного коду на основі графових моделей і нейромережевих архітектур типу YOLO та Transformer. Розроблено метод підготовки навчальних даних для нейронних детекторів на основі сегментації орієнтованих графів програми та перетворення інформативних підграфів у багатоканальні зображення з класами стек, купа та помилка на одиницю. Також запропоновано метод композитної оцінки ризику експлуатації виявлених вразливостей з інтеграцією в конвеєри автоматизованого збирання та розгортання для автоматизованого визначення пріоритету виправлень і блокування небезпечних збірок. Проведено експериментальні дослідження запропонованих моделей і методів. Об'єктом дослідження є процес виявлення та аналізу вразливостей у програмному забезпеченні комп'ютерних систем. Предметом дослідження є методи представлення переповнення буфера, методи автоматизованого виявлення вразливостей типу переповнення буферу у коді C/C++, методи оцінювання ризику та алгоритми інтеграції результатів у конвеєри автоматизованого збирання та розгортання. Метою дисертаційного дослідження є підвищення точності виявлення вразливостей у програмному забезпеченні комп'ютерних систем шляхом формалізації переповнення буфера, створення нейромережевих детекторів та впровадження механізмів композитної оцінки ризику для автоматизованого прийняття рішень. Наукова новизна отриманих результатів полягає в удосконаленні моделі процесу виявлення вразливостей, що передбачає інтеграцію графової моделі програми, нейромережевого детектора та модуля композитної оцінки ризику у конвеєри автоматизованого збирання та розгортання. Розроблено метод автоматизованого виявлення вразливостей типу «переповнення буфера», який враховує просторові та контекстні залежності елементів коду на основі графових моделей і нейромережевих архітектур YOLO/Transformer, що забезпечує підвищення точності та повноти детектування. Запропоновано метод підготовки даних для навчання нейронних моделей на основі сегментації орієнтованих графів і перетворення підграфів у багатоканальні зображення, що дає змогу формувати відтворювані навчальні вибірки. Розроблено метод композитної оцінки ризику експлуатації вразливостей, інтегрований у CI/CD-конвеєри для автоматизованого ранжування вразливостей і блокування небезпечних збірок. Практичне значення отриманих результатів полягає у створенні комплексу моделей, методів і програмних засобів для автоматизованого виявлення переповнення буфера в програмному забезпеченні комп'ютерних систем. Використання запропонованих підходів забезпечує підвищення точності та швидкодії аналізу коду і можливість інтеграції засобів виявлення вразливостей у процеси безперервної інтеграції та розгортання. Ефективність рішень підтверджено експериментальними дослідженнями, які показали покращення точності та повноти виявлення вразливостей і можливість автоматизованого визначення пріоритету їх усунення. Результати дослідження впроваджено в діяльність ТОВ «Nolt technologies» та ТОВ «ІТТ» (м. Хмельницький), а також у навчальний процес Хмельницького національного університету при викладанні дисциплін для здобувачів спеціальності F7 «Комп'ютерна інженерія». У роботі наведено результати аналізу предметної області, розроблено формальні моделі переповнення буфера, нейромережеві методи їх виявлення, програмну реалізацію запропонованих рішень і результати експериментальних досліджень їх ефективності.

2. Improving the accuracy of vulnerability detection in computer system software remains a significant information security challenge. Among the most critical classes of software vulnerabilities in C/C++ programs are buffer overflows, which may result in uncontrolled memory overwriting and enable arbitrary code execution. Despite numerous static and dynamic analysis tools, existing approaches often suffer from limited accuracy, incomplete coverage, and insufficient scalability for large-scale software systems. These limitations motivate the development of new methods capable of formally representing vulnerability patterns and enabling their automated detection within industrial software development environments and continuous integration and continuous deployment (CI/CD) pipelines. This dissertation analyses approaches to detecting buffer overflow vulnerabilities in C/C++ software, including static analysis, machine learning, and neural network models, as well as their integration into DevSecOps practices. A directed graph model of buffer overflow vulnerabilities is proposed to represent data and control flows in C/C++ programs and support quantitative exploitation risk assessment. Furthermore, a method for automated buffer overflow detection is developed that captures spatial and contextual

relationships between program elements using graph representations and YOLO/Transformer neural architectures. A training data preparation method for neural detectors is introduced based on the segmentation of directed program graphs and the transformation of informative subgraphs into multi-channel image representations corresponding to stack, heap, and off-by-one vulnerability classes. In addition, a composite risk assessment method integrated into CI/CD pipelines is proposed to support automated vulnerability prioritisation and prevent unsafe builds. The object of the study is the process of identifying and analyzing vulnerabilities in computer system software. The subject of the research is methods for representing buffer overflows, methods for automated detection of buffer overflow vulnerabilities in C/C++ code, risk assessment methods, and algorithms for integrating results into CI/CD pipelines. The dissertation research aims to enhance the effectiveness of vulnerability detection techniques in software by formalising buffer overflows, developing neural network detectors, and implementing composite risk assessment mechanisms for automated decision-making. The scientific novelty of the obtained results lies in the improvement of the vulnerability detection process model through the integration of a program graph representation, a neural network detector, and a composite risk assessment module into automated build and deployment pipelines. A method for automated detection of buffer overflow vulnerabilities based on graph representations of program code and YOLO/Transformer neural network architectures is developed, enabling improved detection accuracy and completeness. A method for preparing training data for neural models based on the segmentation of directed graphs and the transformation of subgraphs into multi-channel images is proposed, enabling the generation of reproducible training datasets. Furthermore, a composite risk assessment method integrated into CI/CD pipelines is developed to support automated vulnerability ranking and the prevention of unsafe software builds. The practical significance of the obtained results lies in the development of a set of models, methods, and software tools for the automated detection of buffer overflow vulnerabilities in computer system software. The proposed approaches improve the accuracy and efficiency of code analysis and enable the integration of vulnerability detection tools into continuous integration and deployment processes. The effectiveness of the proposed solutions is confirmed by experimental studies demonstrating improved accuracy and completeness of vulnerability detection as well as the capability for automated prioritisation of vulnerability remediation. The results of the research have been implemented in the activities of Nolt Technologies LLC and ITT LLC (Khmelnytskyi, Ukraine), as well as in the educational process of Khmelnytskyi National University in courses taught for students of specialty F7 “Computer Engineering”. The dissertation presents the results of the analysis of the research domain, develops formal models of buffer overflow vulnerabilities, proposes neural network methods for their detection, describes the software implementation of the proposed solutions, and provides the results of experimental studies evaluating their effectiveness.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Sierhieiev, Ye., Kashtalian, A., Kovalchuk, V., Savenko, O., Ivanchenko, O. (2024). Effectiveness and improvement of SAST in the context of SQL Injection vulnerabilities. Information Technology: Computer Science, Software Engineering and Cyber Security, 3, 149–158.
- Сєргєєв Є. В., Савенко О. С. Виявлення вразливостей переповнення буфера в системному програмному забезпеченні на основі графа та моделі трансформатора. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2025. № 6. С. 318–327.
- Підготовка даних на основі графіків для виявлення вразливостей переповнення буфера в коді в рамках CI/CD-процесів. Herald of Khmelnytskyi National University. Technical Sciences. 2026. № 361(1). Pp.

316–322.

- Сергєєв Є. Композитна оцінка ризику переповнення буфера і її трансляція в дії CI/CD. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. 2025. № 84(4). Pp. 89–94.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0124U000980 0126U002082

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Кльоц Юрій Павлович

2. Yurii P. Klots

Кваліфікація: к.т.н., доц., 05.13.13

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація: 2007р, ДК №041583

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Савенко Олег Станіславович

2. Oleg S. Savenko

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Ткачук Ростислав Львович

2. Rostyslav L. Tkachuk

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Львівський державний університет безпеки життєдіяльності

Код за ЄДРПОУ: 08571340

Місцезнаходження: вул. Клепарівська, Львів, 79007, Україна

Форма власності: Державна

Сфера управління: Державна служба України з надзвичайних ситуацій

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Козак Руслан Орестович

2. Ruslan O. Kozak

Кваліфікація: к. т. н., доц.

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Тернопільський національний технічний університет імені Івана Пулюя

Код за ЄДРПОУ: 05408102

Місцезнаходження: вул. Руська, Тернопіль, Тернопільський р-н., 46001, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кисіль Тетяна Миколаївна

2. Tetiana M. Kysil

Кваліфікація: к. ф.-м. н., доц., 01.01.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Капустян Марія Вікторівна
2. Maria V. Kapustian

Кваліфікація: к.т.н., доц., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Лисенко Сергій Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Лисенко Сергій Миколайович
Відповідальний за підготовку облікових документів	Синюк Олег Миколайович
Реєстратор	Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна