РЕЦЕНЗІЯ

на дисертаційну роботу
Куб'юка Євгенія Юрійовича
на тему «Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 122 – Комп'ютерні науки

Актуальність теми дисертації.

Забезпечення кібербезпеки є необхідною умовою існування сучасних держав. Одним зі шляхів випробовування кібербезпеки є кібератаки на держоргани, оборono-промисловий комплекс, інфраструктурні об'єкти, IT-мережі через програмне забезпечення, яке використовується. Стрімке зростання кількості вразливостей у програмному забезпеченні та їх активна експлуатація зловмисниками вимагають розробки нових ефективних методів автоматичного аналізу програмного коду. Застосування технологій штучного інтелекту відкриває широкі можливості для своєчасного виявлення складних і прихованих дефектів безпеки на ранніх етапах життєвого циклу ПЗ. Тому дослідження, спрямовані на пришвидшення та підвищення точності виявлення вразливостей програмного коду, є актуальними.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- вперше запропоновано гібридний метод аналізу програмного коду, що поєднує методи глибокого навчання та методи виявлення подібності коду для пошуку та класифікації вразливості в коді, який дозволяє ефективно виконувати пошук вразливостей в коді, а також класифікувати з високою точністю знайдені вразливості.
- вперше запропоновано метод класифікації вразливостей в програмному коді з використанням ковзного хешування абстрактного синтаксичного дерева, який відрізняється від існуючих методів тим, що використовує метод виявлення подібності коду для ефективної класифікації вразливостей без необхідності використання навчальної вибірки великого об'єму.
- отримав подальший розвиток метод побудови проміжного представлення програмного коду у вигляді кодового гаджету, який відрізняється від існуючих методів наявністю обмеження по розміру локального контексту відносно

ключової точки, що дозволило зменшити результуючий розмір кодових гаджетів та підвищити точність класифікації при подальшому аналізі нейронною мережею.

Наукові результати дисертаційного є достатньо обґрунтованими та достовірними. В роботі коректно застосовано математичний апарат, сучасні методи аналізу даних та експериментальні методики. Достовірність підтверджується результатами обчислювальних експериментів з виявлення вразливостей програмного коду на реальних наборах даних, а також апробацією на наукових конференціях та в рецензованих фахових виданнях.

Наукові дослідження були виконані здобувачем на кафедрі системного проектування згідно Тематичному плану виконання науково-дослідних робіт КПІ ім. Ігоря Сікорського: ініціативна тема СП 2023-2 «Забезпечення захищеності і цифрової доступності веб-застосунків інтелектуальних розподілених середовищ» (номер держреєстрації 0123U101334).

Практичне значення одержаних результатів полягає у розробці методів розробки програмного забезпечення виявлення вразливостей програмного коду, які апробовані в лабораторії Platform Security Lab українського центру із досліджень та розробки в галузі кібербезпеки Самсунг РиД Інституту України.

Отже, в дисертаційній роботі поставлене наукове завдання розробки методів та засобів автоматизованого аналізу програмного коду щодо вразливостей безпеки виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Куб'юка Є.Ю. повністю відповідає Стандарту вищої освіти зі спеціальності 122 «Комп'ютерні науки» та напрямкам досліджень відповідно до освітньої програми Комп'ютерні науки.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям інформаційні технології.

За результатом аналізу звіту подібності з перевірки дисертаційної роботи на текстові співпадіння визначено, що дисертаційна робота Куб'юка Євгенія Юрійовича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою. Стиль викладення є послідовним, матеріал подається у логічній та доступній для розуміння формі. Дисертант коректно застосовує загальноприйняту термінологію в галузі інформаційних технологій.

Дисертація складається з вступу, 4 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 140 сторінок.

У вступі розглядається актуальність проблеми кібербезпеки, Визначається мета та основні завдання дослідження, обґрунтовуються наукова новизна та практична значущість роботи.

У першому розділі розкрито сучасний стан та проблеми аналізу безпеки програмного коду, проведено порівняльний аналіз існуючих підходів та відповідних методів виявлення вразливостей. Визначено напрями подальших досліджень.

У другому розділі представлено архітектуру запропонованої гібридної системи пошуку та класифікації вразливостей; наведено математичні моделі складових компонент цієї системи: контекстно-залежного аналізу вразливостей на основі глибинних нейронних мереж та класифікації вразливостей за відомими шаблонами на основі ковзного хешування абстрактних синтаксичних дерев AST.

В третьому розділі представлено запропоновані методи визначення вразливостей, що базуються:

- на нейронній мережі BLSTM, яка забезпечує контекстний аналіз, враховуючи як попередні, так і наступні фрагменти коду при ідентифікації вразливостей;
- на ковзному хешуванні вузлів AST і порівнянні з прикладами створеної бази типових вразливостей.

В розділі коректно представлено всі етапи застосування зазначених методів.

У четвертому розділі наведено опис програмної реалізації гібридної системи визначення вразливостей, визначено всі використані спеціалізовані програмні засоби, представлено результати експериментальних випробовувань на відкритих наборах даних та реальних проектах.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 5 наукових публікаціях здобувача, серед яких: 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 1 публікація в збірнику матеріалів конференції.

Також результати дисертації були апробовані на 1 науковій фаховій конференції.

Публікації здобувача повною мірою розкривають сутність проведених досліджень, отримані наукові результати та їх практичне значення. У роботах, написаних у співавторстві, особистий внесок дисертанта є визначальним і полягає у формулюванні ідей, розробці моделей та алгоритмів, проведенні експериментальних досліджень.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

Незважаючи на загальну позитивну оцінку роботи, варто зазначити деякі недоліки:

1. Наявні помилки в оформленні дисертаційної роботи, зокрема, в списку публікацій здобувача за темою дисертації (с. 14) для першої статті не вказано назву журнала.
2. Не наведено чіткої постановки задачі обчислювальних експериментів для порівняльного аналізу результатів виявлення вразливостей запропонованого методу та інших моделей.
3. За результатами обчислювальних експериментів запропонований метод класифікації вразливостей демонструє зниження якості при збільшенні кількості класів понад 50, що в деякій мірі обмежує його широке використання для великої номенклатури вразливостей.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Куб'юка Євгенія Юрійовича на тему «Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для галузі інформаційних технологій. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про

присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Куб'юк Євгеній Юрійович заслуговує на присудження ступеня доктора філософії в галузі знань «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Рецензент:
доцент кафедри
цифрових технологій в енергетиці
Національного технічного
університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»,
к.т.н., доцент /_____/ Світлана ШАПОВАЛОВА

Підпис Шаповалової
ЗАСВІДЧУЮ
Відділ кадрів
підпис пр-ще

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
Відділ кадрів і архівної справи № 6

М.П. «06» червня 2024 року