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.

Проблема кібербезпеки в наш час набуває все більшої ваги та гостроти. Зростання кількості вразливостей в програмному забезпеченні та їх активна експлуатація зловмисниками створюють реальні загрози для індивідуальних користувачів, підприємств та цілих держав. У цьому контексті розробка нових ефективних методів автоматизованого пошуку та класифікації вразливостей у програмному коді є надзвичайно актуальним завданням.

Застосування сучасних технологій штучного інтелекту надає можливості для створення інтелектуальних систем аналізу безпеки програмного коду, здатних виявляти приховані дефекти на ранніх етапах розробки. Це дозволяє знизити ризики та усунути вразливості ще до їх потрапляння у готові програмні продукти та системи. Крім того, автоматизація процесів класифікації вразливостей відповідно до загальноприйнятої таксономії CWE спрощує пріоритезацію та виправлення виявлених дефектів безпеки.

Тому дисертаційне дослідження Куб'юка Є.Ю., присвячене розробці гібридного методу пошуку та класифікації вразливостей із використанням методів глибокого навчання у поєднанні з методами аналізу подібності коду, є надзвичайно актуальним та своєчасним.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

Вперше запропоновано гібридний метод аналізу програмного коду, який поєднує методи глибокого навчання та методи виявлення подібності коду для пошуку та класифікації вразливості в коді, що дозволяє ефективно виконувати пошук вразливостей в коді, а також класифікувати з високою точністю знайдені вразливості.

Отримав подальший розвиток метод побудови проміжного представлення програмного коду у вигляді кодового гаджету, який відрізняється від існуючих методів наявністю обмеження щодо розміру локального контексту відносно

ключової точки, що дозволило зменшити результуючий розмір кодових гаджетів та підвищити точність класифікації при подальшому аналізі з використанням нейронної мережі.

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.

Наукові результати дисертаційного дослідження є добре обґрунтованими та достовірними. В роботі застосовано коректний математичний апарат, сучасні методи аналізу даних та експериментальні методики. Достовірність та обґрунтованість отриманих результатів підтверджується застосуванням сучасних методів аналізу даних, математичного моделювання та експериментальної валідації на реальних проєктах.

Наукові дослідження виконано здобувачем на кафедрі системного проектування КПІ ім. Ігоря Сікорського в рамках ініціативної теми під керівництвом доцента кафедри системного проектування Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», к.т.н., с.н.с., Кисельова Геннадія Дмитровича .

Отже, поставлене в дисертаційній роботі наукове завдання розробки методів та засобів автоматизованого аналізу програмного коду на предмет виявлення вразливостей в ньому 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 та комунікаційні технології. Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, 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.

Дисертація написана українською мовою. Стиль викладення послідовний, матеріал подається у логічній та зрозумілій формі із застосуванням загальноприйнятої термінології в галузі інформаційних технологій та кібербезпеки.

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

У вступі обґрунтовано актуальність дослідження, сформульовано мету, завдання, об'єкт, предмет і методи дослідження, розкрито наукову новизну та практичне значення отриманих результатів.

У першому розділі представлено результати аналізу сучасного стану проблеми кібербезпеки та автоматизації аналізу вразливостей в програмному забезпеченні.

У другому розділі представлено математичне моделювання об’єкта дослідження, зокрема методів побудови проміжного представлення коду, пошуку вразливостей та класифікації вразливостей.

Третій розділ присвячено деталізованому опису розроблених моделей та алгоритмів, включно з побудовою проміжного представлення коду, архітектурою нейронної мережі та методом ковзного хешування AST.

У четвертому розділі наведено результати експериментальних досліджень системи на відкритих наборах даних та на проектах з відкритим вихідним кодом. Підтверджено практичну цінність розробки.

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. Можливість адаптації розроблених методів для підтримки більш широкого спектру мов програмування, окрім C/C++, потребує детальнішого дослідження у зв'язку з особливостями синтаксичних конструкцій інших мов програмування.
2. У роботі доцільно було б більш детально проаналізувати часову складність та ресурсоємність розроблених алгоритмів на різних етапах аналізу коду. Це дозволило б краще оцінити можливості їх масштабування для великих програмних проєктів.
3. В роботі в незначній мірі наявні стилістичні помилки, зокрема на стор. 22 помилка перехресного посилання.
4. У роботі блок-схеми алгоритмів представлені у невідповідності до вимог ДСТУ. Рекомендується оформити їх згідно стандарту ДСТУ ISO 5807:2016, використовуючи стандартні графічні елементи, коректне відображення потоку керування та підписи всіх елементів схеми.
5. Кроки алгоритмів потребують більш детального пояснення. Доцільно додати словесний опис під кожною блок-схемою, роз'яснити призначення та зміст кожного кроку, навести приклади вхідних/вихідних даних для ключових етапів.

Вважаю, що висловлені зауваження не є визначальними, 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:

Професор кафедри інформаційних

технологій в телекомунікаціях
Національного технічного
університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»,
д.т.н., професор Лариса ГЛОБА

Підпис
ЗАСВІДЧУЮ
Відділ кадрів та діловодства
пр-ще

М.П.

«__10__» _червня_ 2024_ року