

ВІДГУК

офіційного опонента 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.

Стрімке зростання кількості вразливостей у програмному забезпеченні та їх активна експлуатація зловмисниками вимагає розробки ефективних автоматизованих методів їх виявлення та усунення. Запропонований здобувачем гібридний підхід до аналізу програмного коду, що поєднує методи глибокого навчання та пошуку подібності, має значний потенціал для вирішення цього завдання. Розроблені моделі та алгоритми дозволяють суттєво підвищити точність та швидкість детекції вразливостей, що є вкрай важливим для забезпечення захищеності сучасних програмних систем. То ж тема дослідження, що присвячена аналізу програмного коду з використанням гібридного методу пошуку та класифікації вразливостей, є актуальною в контексті сучасних викликів кібербезпеки.

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.

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.

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.

Достовірність отриманих результатів забезпечується використанням репрезентативних наборів даних (SARD), коректністю математичних моделей та ретельністю проведення експериментальних досліджень. Обґрунтованість висновків підтверджується узгодженістю теоретичних положень з практикою.

Теоретичні та практичні результати дисертаційного дослідження використані в проекті СП 2023-2 «Забезпечення захищеності і цифрової доступності і цифрової доступності веб-застосунків інтелектуальних розподілених середовищ» (номер держреєстрації 0123U101334) та впроваджені в навчальний процес кафедри системного проектування КПП імені Ігоря Сікорського за напрямком 122 – комп'ютерні науки.

Наукові дослідження дисертаційної роботи у контексті вирішення завдань автоматизації аналізу програмного коду, з урахуванням застосування запропонованого методу, спростило процес ручного аналізу програмного коду на предмет вразливостей спеціалістами з кібербезпеки та дозволило підвищити якість продукту. Розглянуті та запропоновані у дисертаційній роботі методи використано при розробці пропозицій щодо майбутніх проектів. Це підтверджується Актом впровадження результатів досліджень в Самсунг РнД Інститут Україна, лабораторія "Platform Security Lab".

Отже, в дисертаційній роботі поставлене наукове завдання 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 напрямкам досліджень відповідно до освітньої програми Інформаційні технології.

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.

Дисертаційна робота написана українською мовою. Текст викладено послідовно та логічно, з дотриманням наукового стилю. Використано загальноприйняту термінологію. Матеріал подано доступно та аргументовано.

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

У вступі обґрунтовано актуальність теми, сформульовано мету та завдання дослідження, окреслено наукову новизну та практичну цінність результатів.

У першому розділі проведено аналіз сучасного стану у сфері кібербезпеки та тенденцій зростання кількості вразливостей у програмному забезпеченні. Розглянуто ключові стандарти та методології забезпечення безпеки програмного забезпечення (ПЗ). Проаналізовано сучасні виклики, пов'язані зі зростанням

складності систем та появою нових технологій. Розглянуто існуючі стандарти та методології забезпечення безпеки ПЗ. Досліджено можливості методів штучного інтелекту, зокрема машинного навчання, для автоматизації процесів аналізу безпеки коду. Розглянуто різні архітектури нейронних мереж та їх застосування для детекції вразливостей. Проаналізовано переваги та недоліки підходів.

У другому розділі здійснено математичне моделювання задачі побудови проміжного представлення коду, пошуку та класифікації вразливостей, запропоновано гібридний підхід на основі нейронних мереж та методу виявлення подібності коду.

У третьому розділі представлено розробку ключових модулів запропонованої системи аналізу програмного коду з використанням гібридного методу пошуку та класифікації вразливостей.

У четвертому розділі представлено результати експериментальної оцінки системи, порівняння з існуючими аналогами та приклади практичного застосування. Завданням експериментальної частини було визначити ефективність окремих компонентів системи, що вирішувалось шляхом безпосереднього пошуку вразливостей у коді та подальшою класифікацією виявлених вразливостей згідно таксономії CWE. Таким чином, на основі експериментальних досліджень підтверджена гіпотеза щодо підвищення ефективності пошуку та класифікації вразливостей за рахунок поєднання глибокого навчання з алгоритмами, заснованими на структурному аналізі коду.

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.

Наукові публікації повною мірою відображають зміст дисертації, написані на належному фаховому рівні та не містять порушень академічної доброчесності.

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

Недоліки та зауваження до дисертаційної роботи.

1. В роботі не достатньо висвітлено можливість розширення методу для підтримки інших мов програмування, окрім C/C++. Здобувачем визначено, що підтримка інших популярних мов, таких як Java, JavaScript чи Python, залишається обмеженою. Таким чином, також незрозумілим є в чому полягає саме це обмеження?

2. В дисертації не розглянуто питання адаптації методу до нових типів вразливостей, що можуть з'являтися з часом. Опис процедури розширення бази знань та перенавчання моделей був би корисним доповненням.

3. В роботі присутні в незначній кількості стилістичні та граматичні помилки.

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 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

ОФІЦІЙНИЙ ОПОНЕНТ:

професор кафедри кібербезпеки та
захисту інформації факультету
інформаційних технологій Київського
національного університету
імені Тараса Шевченка
доктор технічних наук, професор

Сергій БУЧИК

М.П.

«29» листопада 2024 року

Підпис професора Бучика С.С. засвідчую.

Заступник декана факультету інформаційних
технологій з наукової роботи
кандидат технічних наук



Григорій ГНАТІЄНКО