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.

У сучасному світі, де програмне забезпечення забезпечує роботу всього - від фінансових транзакцій до систем охорони здоров'я, усунення вразливостей у коді програмних систем стало більш важливим, ніж будь коли. Якщо ці вразливості не усунути, програмні системи можуть стати вразливими до зловмисних атак. Наразі відбувається збільшення кількості зареєстрованих вразливостей в Національній базі даних вразливостей США (NVD) на 20% у 2022 році порівняно з 2021 роком та на 13% більше у 2023 році ніж у 2022 році. Крім того, 75% успішних кібератак базувалися на експлуатації вже відомих вразливостей. Тому розробка ефективних автоматизованих систем аналізу коду програмних систем на основі технологій штучного інтелекту є вкрай важливим завданням для підвищення рівня кіберзахисту сучасних інформаційних систем. Зважаючи на те, що тема дисертації присвячена вирішенню важливої науково прикладної проблеми, вважаю її актуальною.

Актуальність теми додатково підтверджується Планом заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України (затвердженого розпорядженням Кабінета Міністрів України від 19 грудня 2023 р. № 1163-р), пріоритетами та напрямами забезпечення кібербезпеки України, як передбачено Стратегією кібербезпеки України (затверджена Указом Президента України від 15 березня 2016 року № 96).

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 наукових результатів забезпечується ґрунтовним аналізом сучасного стану проблеми, використанням адекватних математичних моделей та методів дослідження, детальним описом та обґрунтуванням запропонованих рішень, ретельною перевіркою результатів запропонованих методів аналізу програмного коду з використанням гібридного методу пошуку та класифікації вразливостей, а також експериментальним підтвердженням ефективності розробленої системи на реальних проектах з відкритим вихідним кодом.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач Куб'юк Є.Ю. 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. Матеріал дисертації викладено послідовно, доступно, з використанням загальноприйнятої термінології. Дисертаційна робота являє собою наукову працю, яка містить сукупність наукових положень та результатів, виставлених автором для публічного захисту, має внутрішню єдність та свідчить про особистий внесок автора у науку.

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, визначено об'єкт, предмет та методи дослідження, розкрито наукову новизну та практичне значення отриманих 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 ПЗ, зокрема Microsoft SDL, OWASP та ISO 27034.

У другому розділі сформульовано постановку задачі дослідження та побудовано її математичну модель. Розроблено та наведено математичний опис гібридного методу аналізу програмного коду, що поєднує методи глибокого навчання та методи виявлення подібності коду для пошуку та класифікації вразливості в коді. Формалізовано функції перетворення даних на вході та виході системи. Розроблено метод побудови проміжного представлення програмного коду у вигляді кодового гаджету. Розглянуто різні моделі подання програмного коду та обґрунтовано доцільність використання абстрактних синтаксичних дерев. Розроблено метод класифікації вразливостей в програмному коді з використанням ковзного хешування абстрактного синтаксичного дерева та наведено його математичний опис.

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

У четвертому розділі представлено експериментальні дослідження розробленої системи аналізу програмного коду з використанням спеціалізованих наборів даних та кодових баз реальних проектів. Представлено аналіз отриманих результатів та порівняння з існуючими аналогами за критеріями якості та продуктивності.

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 варто було б більш детально розкрити процедуру формування бази знань еталонних хешів вразливостей для методу класифікації, зокрема описати критерії відбору та представлення різних класів CWE у базі.

2. У роботі варто було б приділити більше уваги аналізу впливу розміру кодових гаджетів на якість роботи нейромережевої моделі та навести відповідні експериментальні результати.

3. Оскільки забезпечення безпеки та достовірність отриманих результатів аналізу програмного коду залежить від поточного стану комп'ютерної системи

доцільно було б зосередитись на виявленні слабких ланок, несправностей, ізоляції загроз безпеки з метою зменшення ризиків та ймовірності реалізації загроз інформаційній безпеці комп'ютерної системи.

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.

Офіційний опонент:
Професор кафедри
інфокомунікаційної інженерії
ім. В.В. Поповського
Харківського національного
університету радіоелектроніки,
д.т.н., професор /_____/ Тамара РАДІВІЛОВА

Підписи Радівілової Т.А. засвідчую.

Начальник юридичного відділу ХНУРЕ Даніл ЧУЛКОВ

МП «29» травня 2024 року