ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного технічного
університету України
“Київський політехнічний
інститут
імені Ігоря Сікорського”
к.філос.н., проф.

_____Анатолій МЕЛЬНИЧЕНКО

“ 12 ” 03 2024 р.

ВИТЯГ

з протоколу № 9 від 28 лютого 2024 р. розширеного засідання
кафедри системного проектування
Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”

БУЛИ ПРИСУТНІ:

- з кафедри системного проектування:
  зав. каф., д.т.н., професор Мухін В.Є.;
  професор, д.т.н., професор Петренко А.І.;
  професор, д.т.н., професор Рогоза В.С.;
  доцент, к.т.н., ст.н.с. Кисельов Г.Д.;
  доцент, к.т.н., ст.н.с. Стіканов В.Ю.;
  доцент, к.т.н., доцент Артюхов В.Г.;
  доцент, к.т.н. Харченко К.В.
  доцент, к.т.н. Гіоргізова-Гай В.Ш.
  доцент, к.т.н. Безносик О.Ю.;
  доцент, к.т.н. Булах Б.В.;
  старший викладач Іщенко Г.В.
  старший викладач Британов О.А.;
  асистент Ткачук А.В.;
  асистент Яковчук О.К.;
  асистент Клещ К.О.;

- з інших кафедр КПІ ім. Ігоря Сікорського:
  професор кафедри інформаційних технологій в телекомунікаціях, д.т.н., професор Глоба Л.С.
  доцент кафедри цифрових технологій в енергетиці, к.т.н., доцент Шаповалова С.І.

СЛУХАЛИ:

1. Повідомлення аспіранта кафедри системного проектування Куб'юка Євгенія Юрійовича за матеріалами дисертаційної роботи "Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей", поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 122 - Комп'ютерні науки.

Тему дисертаційної роботи "Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей" затверджено на засіданні Вченої ради КПІ ім. Ігоря Сікорського (протокол №11 від 30 листопада 2020 року) та перезатверджено на засіданні Вченої ради Інституту прикладного системного аналізу (протокол №10 від 28 листопада 2023 року).

Науковим керівником затверджений доцент, кандидат технічних наук, старший науковий співробітник Кисельов Г.Д.

2. Запитання до здобувача.

Запитання по темі дисертації ставили:
зав. каф., д.т.н., професор Мухін В.Є.;
професор, д.т.н., професор Петренко А.І.;
професор, д.т.н., професор Рогоза В.С.;
доцент, к.т.н. Гіоргізова-Гай В.Ш.
доцент, к.т.н. Булах Б.В.;
доцент, к.т.н. Шаповалова С.І.;

3. Виступи за обговореною роботою.

В обговоренні дисертації взяли участь:
зав. каф., д.т.н., професор Мухін В.Є.;
професор, д.т.н., професор Петренко А.І.;
професор, д.т.н., професор Рогоза В.С.;
доцент, к.т.н., ст.н.с. Кисельов Г.Д.;
доцент, к.т.н. Гіоргізова-Гай В.Ш.
доцент, к.т.н. Булах Б.В.;
професор, д.т.н. Глоба Л.С.;
доцент, к.т.н. Шаповалова С.І.;

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження:

1. **Актуальність теми дослідження** полягає в тому, що на даний час спостерігається стрімке зростання кількості вразливостей у програмному забезпеченні, які активно використовуються зловмисниками. Це потребує розробки ефективних автоматизованих методів своєчасного виявлення та усунення вразливостей у програмному коді. Застосування передових технологій штучного інтелекту надає нові можливості для вирішення цієї задачі за рахунок здатності виявляти складні шаблони та аномалії, характерні для різних класів вразливостей.

2. **Зв'язок роботи з науковими програмами, планами, темами**.

Наукові дослідження виконувались в рамках тематичного плану науково-дослідних робіт кафедри системного проектування, зокрема в рамках ініціативної теми «Забезпечення захищеності і цифрової доступності веб-застосунків інтелектуальних розподілених середовищ» (тема СП 2023-2) (номер держреєстрації 0123U101334), що виконується згідно Тематичного плану виконання ініціативних кафедральних науково-дослідних робіт Навчально-наукового інституту прикладного системного аналізу КПІ ім. Ігоря Сікорського

На основі отриманих теоретичних і практичних результатів дисертаційного дослідження створено методичне забезпечення лабораторних робіт з дисципліни «Сучасні технології проектування програмних систем», яке впроваджено у навчальному процесі кафедри системного проектування.

3. **Наукова новизна отриманих результатів**.

У дисертації вперше одержані такі нові наукові результати:

- 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.

4. Теоретичне та практичне значення результатів роботи полягає в тому, що розроблений метод дозволяє знаходити вразливості в програмному коді, написаному на мові C/C++, а також класифікувати тип знайденої вразливості, що дозволяє спростити процес пріоретизації та виправлення знайдених вразливостей для розробників програмних продуктів.

Технологія пошуку та класифікації вразливостей успішно впроваджена в процеси аналізу програмного коду компанії Samsung R&D Institute Ukraine. Методи представлення коду у вигляді сукупності кодових гаджетів та пошуку клонів у коді використовуються як частина автоматизованої системи аналізу програмного забезпечення. Особливістю підходу є висока точність пошуку та класифікації вразливостей в C/C++ коді при збереженні швидкодії аналізу. Застосування запропонованого методу спростило процес ручної перевірки коду спеціалістами з кібербезпеки в рамках оцінки безпеки програмних продуктів компанії та дозволило підвищити їх якість. Крім того, описані в дисертації методи розглядаються при формуванні пропозицій щодо майбутніх проектів компанії.

Розроблені методи було протестовано на реальних проектах з відкритим вихідним кодом. Зокрема, за допомогою розробленої системи аналізу програмного коду вдалося знайти вразливість в проекті з відкритим вихідним кодом - Microsoft Terminal.

5. Апробація/використання результатів дисертації

Основні положення та отримані наукові результати, що викладені в даній дисертаційний роботі, пройшли апробацію на XVII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 25-26 квітня 2019 р.)

6. Дотримання принципів академічної доброчесності

За результатами науково-технічної експертизи дисертація Куб'юка Є.Ю. визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача. За результатами досліджень опубліковано 5 наукових праць, у тому числі:

- 4 статті у наукових фахових виданнях України за спеціальністю 122 – Комп'ютерні науки в т.ч. 1 стаття в якій число співавторів (разом зі здобувачем) більше двох осіб.
- 1 публікація в збірнику матеріалів конференції.

Статті у наукових фахових виданнях України

1. Kubiuk, Y., Chernousov, A., Savchenko, A., Osadchyi, S., Kostenko, Y., & Likhomanov, D. (2019). Deep learning based automatic software defects detection framework.

Здобувачем запропоновано архітектуру системи, розроблено нейромережеву модель пошуку вразливостей, проведено експерименти.

2. Kubiuk, Y., & Kyselov, G. (2021). Comparative analysis of approaches to source code vulnerability detection based on deep learning methods. Technology audit and production reserves, 3(2), 59.

Здобувачем проведено аналіз існуючих методів детекції вразливостей, сформульовано вимоги до удосконалення підходів, запропоновано концепцію поєднання методів.

3. Kaliuzhna, T., & Kubiuk, Y. (2022). Analysis of machine learning methods in the task of searching duplicates in the software code. Technology audit and production reserves, 4(2 (66)), 6-13.

Здобувач приймав участь у проведенні аналізу ефективності методів машинного навчання для пошуку дублікатів коду, а також визначав експерименти, що мають бути проведені при вирішення задач пошуку подібності коду та пошуку вразливостей.

4. Kubiuk, Y., & Kyselov, G. (2023). Development of an algorithm for code clone detection in source code based on abstract syntax tree. Technology audit and production reserves, 4(2 (72)), 33-36.

Здобувачем запропоновано метод детекції клонів коду на основі ковзного хешування AST та алгоритм його роботи, проведено експерименти та проаналізовано результати.

Наукові праці, які засвідчують апробацію матеріалів дисертації та інші публікації

5. Черноусов, А. В., Савченко, А. Ю., & Куб'юк, Є. Ю. Методи виявлення помилок безпеки в програмному забезпеченні на основі глибинного навчання, XVII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 25-26 квітня 2019 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2019.

Здобувачем досліджено ефективність методів глибинного навчання для детекції дефектів ПЗ, проаналізовано архітектури нейромереж, розроблено рекомендації щодо застосування.

Якість та кількість публікацій відповідають "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".

ВВАЖАТИ, що дисертаційна робота Куб'юка Є. Ю. "Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей", що подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки за своїм науковим рівнем, новизною отриманих результатів, теоретичною та практичною цінністю, змістом та оформленням повністю відповідає вимогам, що пред'являють до дисертацій на здобуття

ступеня доктора філософії та відповідає напрямку наукового дослідження освітньо-наукової програми КПІ ім. Ігоря Сікорського Комп'ютерні науки зі спеціальності 122 Комп'ютерні науки.

РЕКОМЕНДУВАТИ:

1. Дисертаційну роботу "Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей", подану Куб'юком Євгенієм Юрійовичем на здобуття наукового ступеня доктора філософії, до захисту у разовій спеціалізованій вченій раді.

2. Вченій раді КПІ ім. Ігоря Сікорського утворити разову спеціалізовану вчену раду у складі:

Голова:

д.т.н., професор, декан факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», **Корнага Ярослав Ігорович**;

Члени:

Рецензенти:

д.т.н., професор, професор кафедри інформаційних технологій в телекомунікаціях Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», **Глоба Лариса Сергіївна;**

к.т.н., доцент, доцент кафедри цифрових технологій в енергетиці Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», **Шаповалова Світлана Ігорівна;**

Опоненти:

д.т.н., професор, професор кафедри інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелектроніки **Радівілова Тамара Анатоліївна;**

д.т.н., професор, професор кафедри кібербезпеки та захисту інформації Київського Національного Університету ім. Тараса Шевченка **Бучик Сергій Степанович**

Головуючий на засіданні
д.т.н., професор,
зав. каф. системного проектування _____ Вадим МУХІН

Вчений секретар кафедри
системного проектування, к.т.н. _____ Олександр БЕЗНОСИК