

РЕЦЕНЗІЯ

офіційного рецензента, кандидата технічних наук, доцента, завідувачки
кафедри прикладної математики та інформаційних технологій
Навчально-наукового інституту
комп'ютерних систем Національного університету «Одеська політехніка»
Волкової Наталії Павлівни
на дисертаційну роботу здобувача
Терещенка Олександра Ігоровича
«Методи і моделі машинного навчання для виявлення та класифікації
вразливостей смарт-контрактів»,
що подану до захисту в разову спеціалізовану вчену раду
Національного університету «Одеська політехніка»
Міністерства освіти і науки України
на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки
галузь знань 12 – Інформаційні технології

1. Актуальність теми дисертації

Актуальність теми дисертаційної роботи зумовлена активним впровадженням смарт-контрактів у сучасних цифрових системах, насамперед у децентралізованих фінансових платформах і сервісах управління. Смарт-контракти забезпечують автоматизоване виконання бізнес-логіки без участі посередників, проте наявність помилок у програмному коді може призводити до суттєвих порушень функціонування систем і значних фінансових втрат, що висуває підвищені вимоги до їх безпеки.

Традиційні методи аналізу смарт-контрактів, зокрема експертний аудит і класичний статичний аналіз, є ефективними, але характеризуються високою трудомісткістю, обмеженою масштабованістю та залежністю від людського фактора. Автоматизовані інструменти на основі правил і шаблонів не завжди здатні виявляти складні або нові класи вразливостей і часто мають обмежені можливості інтерпретації результатів.

У зв'язку з цим особливої актуальності набуває застосування методів машинного навчання та глибоких нейронних мереж для автоматизованого аналізу програмного коду смарт-контрактів. Такий підхід дозволяє поєднати вимоги до точності, масштабованості та надійності виявлення вразливостей і сприяє підвищенню рівня безпеки сучасних блокчейн-систем.

Отже, дисертаційна робота Терещенка Олександра Ігоровича, присвячена розробці та вдосконаленню методів і моделей машинного навчання для багатоміткового виявлення, класифікації та локалізації вразливостей у смарт-контрактах, спрямована на розв'язання актуальної науково-технічної та прикладної задачі й відповідає сучасним потребам розвитку інформаційних технологій.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій сформульованих у дисертації

Наукові положення та висновки, викладені у дисертаційній роботі, сформульовані на основі цілісної методології дослідження, що поєднує сучасні підходи до аналізу програмного коду зі статистично обґрунтованими методами оцінювання результатів. Обрані методи дослідження відповідають поставленим завданням і забезпечують коректне розв'язання задачі виявлення, класифікації та локалізації вразливостей у смарт-контрактах.

Математичний і алгоритмічний апарат, використаний у роботі, узгоджується з загальноприйнятими підходами в галузі комп'ютерних наук і базується на перевірених концепціях представлення програмного коду, оптимізації та статистичного аналізу. Усі припущення, покладені в основу запропонованих моделей, є чітко визначеними, внутрішньо несуперечливими та такими, що не виходять за межі сучасних наукових уявлень про безпеку смарт-контрактів.

Вагомим аргументом на користь обґрунтованості отриманих результатів є їх систематична перевірка в ході експериментальних досліджень. Запропоновані методи було апробовано на різноманітних наборах даних смарт-контрактів із використанням стандартних критеріїв оцінювання, що дозволило проаналізувати стійкість результатів і підтвердити їх відтворюваність. Отримані експериментальні дані узгоджуються з теоретичними положеннями роботи та підтверджують доцільність запропонованих підходів.

З урахуванням наведеного можна зробити висновок, що наукові положення, висновки та рекомендації дисертаційної роботи є методологічно виваженими, логічно обґрунтованими та підтвердженими результатами експериментальної перевірки.

3. Наукова новизна одержаних результатів

Наукові завдання дослідження сформульовані на основі детального аналізу сучасної фахової та періодичної наукової літератури відповідно до тематики роботи.

Наукова новизна результатів дисертаційного дослідження полягає у наступному:

- *вперше запропоновано комбінований метод формування навчального датасету за рахунок поєднання автоматичного інжектування аномальних конструкцій у коректний код смарт-контрактів із генерацією додаткових прикладів великою мовною моделлю з подальшою верифікацією, що дозволило забезпечити збалансованість вибірки;*

- *вперше побудовано модель CodeBERT-GDLA на основі вдосконалення архітектур BiGRU-ATT і CodeBERT-BiGRU за допомогою запропонованих методів графового зсуву і дворівневої графово-орієнтованої уваги, що*

дозволило підвищити ефективність виявлення та класифікації вразливостей при інтелектуальному аналізі вихідного коду смарт-контрактів;

– удосконалено метод регуляризації для калібрування ймовірнісних оцінок багатоміткової класифікації вразливостей смарт-контрактів за рахунок застосування оптимізації очікуваної калібрувальної похибки, температурного масштабування та фокального приглушення надмірної впевненості безпосередньо в процесі навчання моделі CodeBERT-GDLA, що забезпечує зниження її надмірної впевненості та підвищує надійність результатів інтелектуального аналізу вихідного коду смарт-контрактів;

– отримав подальший розвиток метод слабосупервізованого виділення вразливих фрагментів коду за рахунок інтеграції САМ-узгодженої уваги з причинно-орієнтованою регуляризацією, що забезпечує підвищення ефективності локалізації вразливостей при інтелектуальному аналізі вихідного коду смарт-контрактів.

Положення, що визначають наукову новизну та виносяться на захист, сформульовані з урахуванням тематики дослідження, узгоджуються з метою дисертаційної роботи та реалізовані у повному обсязі, що свідчить про належний рівень володіння здобувачем методологією наукової діяльності.

4. Повнота викладення результатів дисертації в опублікованих працях

Результати дисертаційного дослідження послідовно відображені в опублікованих наукових працях здобувача, які охоплюють усі ключові напрями та етапи виконаної роботи. Публікації відображають розвиток основних наукових ідей дисертації – від постановки задачі та вибору методів до аналізу отриманих результатів і формулювання узагальнених висновків.

Аналіз змісту наукових праць і внеску здобувача свідчить, що результати, винесені на захист, отримані ним особисто впродовж 2022-2025 років та систематизовані при підготовці дисертаційної роботи. Основні положення дисертації апробовані у 11 наукових публікаціях, зокрема у фахових виданнях України категорій «А» і «Б», зарубіжних наукових журналах, що індексуються у міжнародних наукометричних базах, а також у матеріалах міжнародних наукових конференцій.

Суттєвим є те, що частина публікацій виконана одноосібно, що підтверджує самостійність здобувача у формуванні наукових результатів. Загалом обсяг і характер публікацій свідчать про достатню повноту викладення результатів дисертаційного дослідження та їх відповідність вимогам до робіт освітньо-наукового рівня.

5. Значення роботи для науки та практики

Одержані у дисертаційній роботі результати мають вагоме значення для розвитку наукових підходів у галузі автоматизованого аналізу безпеки програмного коду. Запропоновані методи та моделі машинного навчання

доповнюють існуючі дослідження у сфері виявлення вразливостей смарт-контрактів і сприяють подальшому розвитку інтелектуальних методів аналізу програмних систем.

Практична цінність роботи полягає у можливості застосування отриманих результатів у реальних процесах аналізу безпеки смарт-контрактів на етапах розробки та передрозгортальної перевірки. Запропоновані підходи дозволяють підвищити ефективність автоматизованого аналізу, зменшити залежність від ручного аудиту та знизити ризики експлуатації програмних вразливостей. Розроблені рішення реалізовані у формі програмних компонентів, придатних для інтеграції в існуючі системи аудиту.

Практична придатність результатів підтверджується їх використанням у діяльності ТОВ НВО «Діскрет» та ТОВ НВП «КАРЕ», а також застосуванням у навчальному процесі Національного університету «Одеська політехніка».

6. Відсутність (наявність) порушення академічної доброчесності

Дисертація містить результати власних досліджень автора. Всі використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Фактів порушення академічної доброчесності в дисертації здобувача не виявлено.

7. Дискусійні положення та зауваження щодо змісту дисертації

1. При описі математичних моделей основна увага приділяється формальному викладу. Було б корисно додатково надати інтуїтивне пояснення окремих формул, що спростило б сприйняття матеріалу для читачів, які не спеціалізуються безпосередньо у відповідному підрозділі машинного навчання.

2. Окремо доречним було б додатково уточнити, як контролювався можливий “витік інформації” між вибірками (наприклад, дублікати/похідні версії контрактів або схожі шаблони після нормалізації), адже в домені смарт-контрактів поширені копії коду.

3. Окремі формули містять гіперпараметри, значення яких визначалися експериментально. Було б корисно коротко зазначити принципи їх підбору або межі зміни під час експериментальних досліджень.

4. У розділі, присвяченому формальному опису запропонованих моделей, наведено низку математичних співвідношень. Доцільно було б більш детально пояснити алгоритмічний зміст окремих параметрів, що входять до формул, а також їх вплив на результати моделювання.

5. З методичної точки зору, бажано в одному місці подати “обмеження застосовності”: обмеження щодо мов/версій Solidity, переносимість на інші блокчейни/VM, чутливість до стилю коду й шаблонності, тощо. Це зробило б висновки ще більш обґрунтованими.

Зазначені зауваження мають дискусійний характер, не впливають на загальну позитивну оцінку дисертаційної роботи та не знижують наукової і практичної цінності отриманих результатів.

8. Загальний висновок про відповідність роботи встановленим вимогам

Дисертаційна робота Терещенка Олександра Ігоровича «Методи і моделі машинного навчання для виявлення та класифікації вразливостей смарт-контрактів» є логічно завершеним, самостійно виконаним науковим дослідженням, що характеризується цілісністю викладу та науково-прикладною спрямованістю. Тема та зміст роботи повністю відповідають вимогам спеціальності 122 «Комп'ютерні науки».

Беручи до уваги актуальність обраної тематики, рівень обґрунтованості наукових положень, висновків і рекомендацій, їх наукову новизну та практичну значущість, повноту відображення результатів у наукових публікаціях, а також відсутність порушень принципів академічної доброчесності, можна зробити висновок, що дисертаційна робота відповідає вимогам «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 року №44 із змінами. У зв'язку з цим автор роботи, Терещенко Олександр Ігорович, заслуговує на присудження наукового ступеня доктора філософії у галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Офіційний рецензент:
Завідувач кафедри прикладної
математики та інформаційних технологій
навчально-наукового інституту
комп'ютерних систем
Національного університету
«Одеська політехніка», кандидат
технічних наук, доцент

Наталія ВОЛКОВА