ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА
Гожого Олександра Петровича,
доктора технічних наук, професора, професора кафедри інтелектуальних інформаційних систем
Чорноморського національного університету імені Петра Могили
на дисертаційну роботу
Терещенка Олександра Ігоровича
на тему:
«Методи і моделі машинного навчання для виявлення та класифікації вразливостей смарт-контрактів»,
що представлена на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки
галузь знань 12 – Інформаційні технології

1. **Актуальність теми дисертації**

Актуальність теми зумовлена стрімким зростанням масштабів використання смарт-контрактів у блокчейн-екосистемах, зокрема у сфері децентралізованих фінансів, цифрових сервісів, управління активами та автоматизованого виконання угод, що вимагає високого рівня безпеки програмного коду та надійності його функціонування в умовах реального середовища. Смарт-контракти оперують значними фінансовими ресурсами та виконуються без можливості подальшого втручання, що робить помилки й вразливості у коді критично небезпечними.

Існуючі підходи до забезпечення безпеки смарт-контрактів характеризуються низкою обмежень, пов'язаних із високою трудомісткістю експертного аудиту, обмеженою масштабованістю формальних методів, значною кількістю хибнопозитивних спрацювань у статичних аналізаторах, а також недостатньою здатністю автоматизованих інструментів виявляти складні або нові класи вразливостей. Це ускладнює їх ефективне застосування у великих блокчейн-екосистемах та у швидких циклах розробки.

Особливу роль у сучасних системах аналізу безпеки відіграють методи машинного навчання, які дозволяють автоматизувати аналіз програмного коду та виявляти приховані закономірності, недоступні традиційним правилам і шаблонам. Водночас на практиці такі моделі часто характеризуються недостатньою інтерпретованістю, нестійкістю до змін і рефакторингу коду, а також надмірною впевненістю у прогнозах, що ускладнює їх використання у відповідальних production-сценаріях.

Недосконалість існуючих підходів до автоматизованого аналізу смарт-контрактів призводить до неповного виявлення вразливостей, складності їх локалізації у вихідному коді та підвищених ризиків експлуатації помилок після розгортання контрактів. Це негативно впливає на безпеку блокчейн-систем, довіру користувачів і стабільність децентралізованих сервісів.

У зв'язку з цим розробка та удосконалення методів і моделей машинного навчання для багатоміткового виявлення, класифікації та локалізації вразливостей у смарт-контрактах, які поєднують високу точність, масштабованість, інтерпретованість і надійність, є важливим науковим і прикладним завданням. Його вирішення сприятиме підвищенню рівня безпеки блокчейн-екосистем та розвитку інтелектуальних засобів аналізу програмного коду.

Таким чином, дисертаційна робота Терещенка Олександра Ігоровича, присвячена розробці методів і моделей машинного навчання для виявлення, класифікації та локалізації вразливостей у смарт-контрактах, є актуальною та своєчасною.

2. Аналіз змісту та форми дисертаційної роботи

Дисертаційну роботу написано українською мовою з використанням наукового стилю та загальноприйнятої термінології в галузі комп'ютерних наук, машинного навчання та аналізу програмного коду. Матеріал викладено логічно, послідовно та зрозуміло. У кожному розділі наведено посилання на відповідні наукові джерела, а також представлені результати власних досліджень автора. Структура роботи відповідає поставленій меті та сформульованим завданням, що сприяє цілісності сприйняття матеріалу та можливості практичного використання отриманих результатів.

Перший розділ дисертації має теоретико-аналітичний характер і слугує методологічною основою для подальших наукових розробок. У ньому проведено ґрунтовний огляд сучасних підходів до виявлення вразливостей у смарт-контрактах, включаючи формальні методи, статичний і динамічний аналіз, а також методи на основі машинного навчання. Автором систематизовано переваги та обмеження кожного підходу з точки зору точності, масштабованості, інтерпретованості та практичної придатності. Особливу увагу приділено методам глибокого навчання та трансформерним моделям для аналізу коду, а також проблемам багатоміткової детекції, локалізації вразливостей і надійності прогнозів. Розділ завершується формулюванням наукової проблеми, мети та завдань дослідження.

У другому розділі дисертації розглянуто питання формування навчальних даних для задач автоматизованого аналізу безпеки смарт-

контрактів. Запропоновано комбінований підхід до створення збалансованого датасету, який поєднує автоматичне інжектування вразливостей у коректний код із контекстно узгодженою генерацією та модифікацією прикладів за допомогою великої мовної моделі. Описано процедури валідації згенерованих даних та забезпечення коректності анотацій. Наведено характеристику сформованого корпусу смарт-контрактів і обґрунтовано його придатність для навчання та порівняльної оцінки моделей машинного навчання.

У третьому розділі дисертації подано розробку та дослідження моделей машинного навчання для багатоміткового виявлення і слабосупервізованої локалізації вразливостей у смарт-контрактах. Розглянуто базові архітектури та запропоновано удосконалену модель CodeBERT-GDLA з графово-орієнтованим дворівневим механізмом уваги. Описано використання структурної інформації коду у вигляді синтаксичних і семантичних графів, механізми узгодження уваги з CAM-методами та причинно-орієнтовану регуляризацію для підвищення інтерпретованості результатів. Наведено результати експериментальних досліджень, що підтверджують підвищення ефективності запропонованих моделей за показниками точності, стабільності та якості локалізації порівняно з відомими аналогами. Проведено абляційний аналіз і дослідження стійкості до змін і рефакторингу коду.

У четвертому розділі дисертації розглянуто прикладні аспекти реалізації та апробації розроблених методів у вигляді програмного засобу автоматизованого аудиту смарт-контрактів. Описано архітектуру програмної системи, її основні функціональні модулі, інтерфейси взаємодії та сценарії використання. Проведено тестування розробленого інструменту в реалістичних умовах із використанням реальних смарт-контрактів. Зроблено висновки про практичну придатність запропонованих рішень для використання у системах аудиту смарт-контрактів.

У висновках дисертації узагальнено основні результати дослідження, сформульовано наукові та практичні висновки щодо ефективності запропонованих моделей і методів машинного навчання для виявлення, класифікації та локалізації вразливостей у смарт-контрактах. Підкреслено можливість практичного використання отриманих результатів у системах забезпечення безпеки блокчейн-застосунків.

У додатках наведено матеріали, що доповнюють основний зміст роботи, зокрема акти впровадження, фрагменти програмного коду та інші допоміжні відомості. Анотація дисертації коректно та стисло відображає її основні положення.

3. **Ступінь обґрунтованості наукових положень, висновків і рекомендацій**

Наукові положення та висновки, викладені в дисертаційній роботі, характеризуються належним рівнем обґрунтованості, що зумовлено системним підходом до дослідження та використанням широкого кола актуальних наукових джерел. У роботі опрацьовано сучасні праці, присвячені питанням безпеки програмного забезпечення, аналізу програмного коду, машинного навчання, теорії графів, методів математичної статистики та оптимізації, що забезпечує теоретичну цілісність і міждисциплінарний характер дослідження. Обрані методи та підходи узгоджуються з поточними тенденціями розвитку комп'ютерних наук і відповідають практиці їх застосування у наукових дослідженнях.

Достовірність отриманих результатів підтверджується проведенням серії експериментів на репрезентативних вибірках смарт-контрактів, зокрема як на реальних даних, так і на синтетично сформованих наборах. Оцінювання ефективності запропонованих моделей здійснювалося із застосуванням загальноприйнятих показників якості, що дозволяє коректно порівнювати результати з існуючими підходами. Отримані експериментальні дані демонструють узгодженість теоретичних припущень із практичними результатами та підтверджують працездатність запропонованих методів для задач виявлення, класифікації та локалізації вразливостей у смарт-контрактах.

Додатковим чинником обґрунтованості наукових висновків є коректне використання математичного апарату, сучасних інструментів комп'ютерного моделювання та методів аналізу даних. Запропоновані методи і моделі пройшли практичну апробацію, результати якої свідчать про їх прикладну цінність та можливість використання в реальних умовах. Підтвердженням цього є матеріали експериментів і прикладів застосування, наведені у додатках до дисертаційної роботи.

4. **Практична значимість розроблених моделей та методів**

Практична цінність результатів, отриманих у межах дисертаційної роботи, полягає в можливості їх безпосереднього застосування у задачах аналізу безпеки смарт-контрактів у реальних умовах. Запропоновані методи та моделі реалізовано у вигляді програмних рішень, орієнтованих на автоматизований аналіз програмного коду, що забезпечує виявлення потенційних вразливостей, їх класифікацію та визначення локалізації у структурі смарт-контрактів. Це створює передумови для використання розроблених інструментів як на етапі розробки програмних продуктів, так і

під час попередньої перевірки перед розгортанням у блокчейн-середовищі, а також для їх інтеграції у наявні системи аудиту безпеки.

Застосування запропонованих підходів дозволяє підвищити продуктивність автоматизованого аналізу програмного коду за рахунок зменшення залежності від ручних процедур перевірки, що, у свою чергу, сприяє скороченню часу проведення аудиту та зниженню ймовірності пропуску критичних вразливостей. Це є особливо актуальним для сучасних блокчейн-платформ і систем децентралізованих фінансів, де помилки у смарт-контрактах можуть призводити до значних фінансових втрат.

Практична придатність і ефективність запропонованих методів підтверджується їх впровадженням у діяльність товариства з обмеженою відповідальністю НВО «Діскрет» та науково-виробничого підприємства «КАРЕ». Окрім того, результати дослідження були використані в освітньому процесі Національного університету «Одеська політехніка», що свідчить про можливість їх застосування не лише у прикладних, а й у навчальних та науково-методичних цілях.

5. Новизна наукових положень, висновків та рекомендацій

Наукові завдання дослідження визначені на підставі системного опрацювання актуальних наукових публікацій, зокрема фахових монографій і статей у періодичних виданнях, що безпосередньо стосуються обраної тематики дисертаційної роботи.

Наукова новизна результатів дисертаційного дослідження полягає у отриманні нових теоретичних і прикладних положень, спрямованих на розв’язання актуальних задач аналізу безпеки смарт-контрактів:

– *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 багатомітковоі 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 CAM-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 у повній відповідності до мети та завдань дисертації, логічно випливають із проведених досліджень і реалізовані в повному обсязі. Це свідчить про належний рівень володіння здобувачем методологією наукових досліджень і здатність самостійно розв’язувати складні науково-прикладні задачі.

6. Рекомендації щодо використання результатів дисертації

Результати дисертаційного дослідження доцільно застосовувати у практиці автоматизованого аналізу безпеки смарт-контрактів, зокрема в межах сучасних блокчейн-платформ. Запропоновані моделі та методи можуть використовуватися на різних етапах життєвого циклу програмного забезпечення – від розробки та тестування до попередньої перевірки перед впровадженням у продуктивне середовище. Їх застосування забезпечує підтримку процесів виявлення, класифікації та локалізації вразливостей у програмному коді, а також сприяє підвищенню обґрунтованості рішень, що приймаються під час аудиту смарт-контрактів у системах децентралізованих фінансів.

Отримані наукові результати можуть бути використані під час проєктування та подальшого вдосконалення програмних засобів автоматизованого аудиту смарт-контрактів, у тому числі як елементи інтелектуальних модулів аналізу коду.

Окрім прикладного застосування, матеріали дисертаційної роботи можуть бути використані в освітній і науково-дослідній діяльності. Зокрема, результати дослідження є доцільними для використання у навчальному процесі під час викладання дисциплін, пов’язаних із машинним навчанням, аналізом програмного коду, безпекою програмного забезпечення та розробкою інтелектуальних систем.

7. **Повнота викладу в наукових публікаціях, зарахованих за темою дисертації, відсутність порушення академічної доброчесності**

Основні наукові положення та практичні результати дисертаційного дослідження були апробовані шляхом доповідей і обговорення на міжнародних та всеукраїнських науково-практичних конференціях, зокрема: міжнародній науково-практичній конференції Modern Information Technology 2023 / Сучасні Інформаційні Технології 2023 (м. Одеса, 18-19 травня 2023 р.); XIII International Scientific and Practical Conference “Social Ways of Training Specialists in the Social Sphere and Inclusive Education” (м. Прага, Чеська Республіка, 1-3 квітня 2024 р.); VI International Scientific Conference “Traditional and Innovative Approaches to Scientific Research” (м. Вінниця, Україна, 8 березня 2024 р.); X International Scientific and Practical Conference “Informatics. Culture. Technology” (вересень 2024 р.); VIII International Scientific Conference “Розвиток наукової думки постіндустріального суспільства: сучасний дискурс” (жовтень 2025 р.). Участь у зазначених наукових заходах сприяла обговоренню та уточненню отриманих результатів, а також підтвердила їх наукову актуальність.

Основні наукові результати, отримані в межах дисертаційного дослідження, оприлюднено у 11 наукових працях. До них належать статті, опубліковані у фахових наукових виданнях України категорій «А» та «Б», публікації у зарубіжних наукових журналах, що індексуються у міжнародних наукометричних базах даних, а також тези доповідей, представлені на міжнародних наукових конференціях. Це свідчить про повне виконання встановлених вимог щодо кількості та рівня публікацій за тематикою дисертації.

Оприлюднення результатів дослідження у рецензованих наукових виданнях і матеріалах наукових конференцій, які передбачають обов’язкову експертну оцінку та перевірку поданих матеріалів на наявність неправомірних запозичень, підтверджує дотримання здобувачем принципів академічної доброчесності. Аналіз змісту дисертаційної роботи та відповідних публікацій не виявив ознак порушення норм академічної етики та доброчесності.

8. **Зауваження згідно змісту та оформлення дисертаційної роботи**

1. У роботі застосовано низку показників для оцінювання якості (зокрема метрик локалізації на кшталт IoU@τ, Hit@K тощо). Доцільно було б додатково коротко прокоментувати чутливість результатів до вибору порогів/параметрів метрик (типові значення, допустимі межі зміни), щоб читачеві було легше інтерпретувати практичний сенс наведених показників.

2. В розділі 2.3 бажано б навести приклад реалізації методу ін’єкції вразливостей у смарт-контракти на основі великих мовних моделей.

3. З опису попередньої обробки даних розділ 2.2.5 не зовсім зрозуміла послідовність процедур попередньої обробки даних. Було б доцільно представити більш детально загальний опис кроків попередньої обробки.

4. На рисунку 3.7 представлена загальна архітектура моделі CodeBERT-BiGRU. Бажано б було представити детально опис архітектури моделі CodeBERT-BiGRU для вирішення конкретного завдання.

5. В експериментальній частині наведено результати навчання та порівняння моделей, однак для підвищення відтворюваності було б корисно більш явно зафіксувати ключові налаштування експериментів (seed, критерій “кращої” епохи/чекпойнта, умови ранньої зупинки, принцип формування train/val/test).

6. Для практичного застосування запропонованого підходу доцільно було б додати короткі оцінки обчислювальної складності/продуктивності (орієнтовний час аналізу на типових розмірах контрактів, вимоги до ресурсів), оскільки це підсилює прикладну частину, не змінюючи суті отриманих результатів.

7. У тексті дисертації подекуди трапляються поодинокі стилістичні та термінологічні неточності, які, однак, не впливають на основні наукові положення та результати дослідження.

8. Дисертація містить значну кількість англомовних термінів і абревіатур, притаманних тематиці машинного навчання та аналізу програмного коду. З метою полегшення сприйняття матеріалу доцільно в окремих випадках наводити українські відповідники або короткі пояснення цих термінів при їх першому використанні.

Наведені зауваження мають рекомендаційний характер, не впливають суттєво на загальну позитивну оцінку дисертаційної роботи та не знижують її наукового рівня і практичної цінності.

9. Загальний висновок

Перелічені зауваження не є принциповими і такими, що піддають сумніву результати дослідження та ніяким чином не зменшують наукову та практичну цінність роботи та позитивне враження від впровадження її результатів.

Дисертаційна робота, яка представлена на відгук, є закінченою кваліфікаційною науковою працею, яка містить раніше не захищені наукові

положення та одержані автором нові науково обґрунтовані результати в області виявлення вразливостей смарт-контрактів.

У підсумку, з огляду на актуальність вирішеної науково-практичної задачі підвищення ефективності виявлення, класифікації та локалізації вразливостей у смарт-контрактах, вагомий внесок автора у розвиток методів інтелектуального аналізу програмного коду, високий науково-методичний рівень проведених досліджень та отримані результати практичного впровадження, вважаю, що дисертаційна робота «Методи і моделі машинного навчання для виявлення та класифікації вразливостей смарт-контрактів» відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету Міністрів України від 12 січня 2022 р. №44, а її автор Терещенко Олександр Ігорович заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю – 122 Комп’ютерні науки, галузь знань – 12 Інформаційні технології.

Офіційний опонент,
доктор технічних наук, професор,
професор кафедри інтелектуальних
інформаційних систем
Чорноморського національного
університету імені Петра Могили Олександр ГОЖИЙ