Голові разової спеціалізованої
вченої ради PhD 12573
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКО

РЕЦЕНЗІЯ

на дисертаційне дослідження Сєргєєва Євгенія Віталійовича
за темою «Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем», подане на здобуття
ступеня доктора філософії
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дослідження та її зв'язок із планами наукових робіт університету.

У сучасному цифровому світі, де інформаційні технології проникають у всі сфери нашого життя, безпека програмного забезпечення та надійність комп'ютерних систем набувають вирішального значення. Сфера IT відіграє важливу роль не тільки у повсякденному житті людини, але й у функціонуванні критично важливої інфраструктури, що робить питання захисту даних особливо актуальним. Розвиток комп'ютерного простору відкрив нові можливості для зловмисників, змушуючи дослідників та розробників шукати новітні методи боротьби з кіберзагрозами.

Актуальність теми виявлення вразливостей в програмному забезпеченні посилюється також швидкістю розвитку кіберзагроз, що вимагає не лише реактивних дій по їх нейтралізації, але й превентивних заходів, спрямованих на попередження атак. В цьому контексті, важливою стає розробка комплексних методів, які поєднують різні підходи та технології для забезпечення максимальної ефективності захисту. Дослідження у цій області може внести значний вклад у розвиток галузі, визначаючи нові ніші для застосування передових технологій. Зокрема, розробка спеціалізованих інструментів для виявлення вразливостей у специфічних типах програмного забезпечення або під час використання конкретних технологій може запропонувати цінні рішення для захисту комп'ютерних систем.

Саме розв'язанню однієї з окреслених проблем присвячено дисертаційне дослідження Сєргєєва Є. В., в якому актуальною науковою задачею є розробка моделей, методів та засобів виявлення вразливостей у системного програмному забезпеченні комп'ютерних систем, орієнтованих на формалізоване представлення програмних об'єктів, кількісну оцінку ризику експлуатації та

інтеграцію розроблених рішень у сучасні технології розробки й супроводу програмного забезпечення, для підвищення точності виявлення.

Дисертаційна робота виконана у рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер держреєстрації 0124U000980); держбюджетної науково-дослідної теми №1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер держреєстрації 0126U002082), в яких автор дисертації був виконавцем

Загалом, обраний дисертантом напрям досліджень є актуальною науково-прикладною задачею.

Формулювання наукової задачі, мети й задачі дослідження.

Здобувачем правильно визначено об'єкт і предмет дослідження, відповідно до висунутої заздалегідь гіпотези дослідження. Так, *об'єктом* дослідження є процес виявлення та аналізу вразливостей у програмному забезпеченні комп'ютерних систем. *Предметом* дослідження є методи представлення переповнення буфера, методи автоматизованого виявлення вразливостей типу переповнення буферу у коді C/C++, методи оцінювання ризику та алгоритми інтеграції результатів у конвеєри автоматизованого збирання та розгортання.

Метою роботи є підвищення точності виявлення вразливостей у програмному забезпеченні комп'ютерних систем шляхом формалізації переповнення буфера, створення нейромережевих детекторів та впровадження механізмів композитної оцінки ризику для автоматизованого прийняття рішень.

Наукова новизна отриманих автором результатів полягає в наступному:

1) удосконалено модель процесу виявлення вразливостей, в якій на відміну від відомих передбачено інтеграцію графової моделі, нейромережевого детектора та модуля композитної оцінки ризику в конвеєри автоматизованого збирання та розгортання, що дає змогу забезпечити підтримку повного циклу аналізу, тобто від початкового коду до блокування небезпечних збірок;

2) розроблено новий метод автоматизованого виявлення вразливостей «переповнення буфера», який на відміну від відомих враховує просторові й контекстні залежності між елементами програмного коду на основі графових моделей та нейромережевої архітектури YOLO/Transformer, що дало змогу підвищити точність і повноту виявлення переповнень буфера у системному програмному забезпеченні;

3) розроблено новий метод підготовки та обробки даних для тренування нейронних детекторів, який на відміну від відомих характеризується побудовою та сегментацією орієнтованих графів і перетворенням інформативних підграфів у багатоканальні зображення з класами стек, купа та off-by-one помилки, що дало змогу формувати відтворювані навчальні вибірки, узгоджені з кореневими

причинами вразливостей, та підвищити ефективність навчання нейромережевих архітектур для обробки зображень;

4) розроблено новий метод композитної оцінки ризику експлуатації виявлених вразливостей, який на відміну від відомих характеризується інтеграцією у конвеєри автоматизованого збирання та розгортання та узгодженням показників ризику з результатами нейромережевого детектування, що дає змогу автоматизувати визначення пріоритету виправлень, ранжування вразливостей за рівнем ризику і блокування небезпечних збірок.

Короткий аналіз основного змісту дисертації.

У вступі автором обґрунтовано актуальність теми, визначено мету, основні завдання, предмет та об'єкт дослідження, наведено наукову новизну, практичне значення одержаних результатів.

У першому розділі здійснено аналіз предметної області дослідження, класифікацію вразливостей програмного забезпечення та розглянуто відомі методи їх виявлення, зокрема статичний і динамічний аналіз, підходи машинного навчання та глибинних нейронних мереж. Проаналізовано існуючі інструменти виявлення переповнення буфера та їх інтеграцію в процеси розробки ПЗ, охарактеризовано вимоги DevSecOps-підходів та виявлено недоліки наявних рішень.

Проведений здобувачем аналіз підтвердив необхідність і перспективність розробки нових, більш досконалих моделей та алгоритмів аналізу коду. Отримані результати стали основою для подальшого формулювання задач, а також дозволили обґрунтувати доцільність використання адаптованих нейромережевих моделей, зокрема YOLO, для автоматизованого виявлення вразливостей типу переповнення буферу.

У другому розділі розроблено формальну модель вразливостей переповнення буфера на основі уніфікованого графа програми з анотаціями буферів, операцій роботи з пам'яттю та потоків даних. Визначено локальні та шляхові показники ризику, побудовано математичну модель композитної оцінки ризику експлуатації вразливостей, сформульовано критерії віднесення буферів до класів Stack/Heap/Off-by-one та вимоги до відтворюваності побудови графів.

Також встановлено, що розроблені моделі можуть бути інтегровані у конвеєрах автоматизованого збирання та розгортання для автоматизованого аналізу безпеки на ранніх етапах розробки. Використання цих моделей у статичному та динамічному аналізі дозволить виявляти вразливості до їхнього впровадження у виробниче середовище. Крім того, інтеграція з існуючими інструментами аналізу коду, такими як SonarQube або Checkmarx, забезпечить їхню ефективність у великих масштабах. Такий підхід сприятиме зниженню ризиків, економії ресурсів та підвищенню загальної стійкості ПЗКС до кіберзагроз.

У третьому розділі розроблено нейромережеві методи виявлення вразливостей переповнення буфера на основі графових представлень коду: метод YOLO-типу, що працює з растрованими підграфами; метод на основі трансформерної архітектури. Також описано процеси навчання і валідації, а також етапи постобробки результатів і оцінювання їх якості, включаючи аналіз чутливості та абляційні дослідження. Для гарантії відтворюваності експериментів було зафіксовано набір гіперпараметрів для навчання, визначено функцію втрат і аугментації, а також інформативно описано апаратну платформу, на якій проводилося навчання (зокрема конфігурацію GPU). Описано метод підготовки даних на основі вибору інформативних підграфів, їх нормалізації та перетворення у багатоканальні зображення, наведено схему навчання і валідації моделей, а також показано інтеграцію результатів аналізу в метод композитної оцінки ризику.

У четвертому розділі представлено програмну реалізацію запропонованих моделей і методів, описано архітектуру програмного комплексу для виявлення переповнення буфера та обчислення композитної оцінки ризику, інтеграцію детектора в конвеєри автоматизованого збирання та розгортання, а також наведено результати експериментальних досліджень, порівняння з відомими інструментами статичного аналізу та нейромережевими підходами, виконано аналіз точності, повноти та продуктивності запропонованих рішень.

У висновках представлено отримані наукові та практичні результати дослідження.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Наукові положення, висновки і рекомендації дисертаційної роботи Сєргєєва Є. В. достатньо обґрунтовані коректним застосуванням методів математичного моделювання, підкріплені успішною реалізацією та практичним впровадженням результатів дисертаційного дослідження. При розв'язанні поставленої науково-прикладної задачі використано теорію графів, елементи абстрактної алгебри, методи машинного навчання, теоретичні основи інформаційних технологій, методи захисту інформації та статистичні методи оцінки якості.

Практичне значення одержаних результатів. Практичне значення отриманих результатів роботи полягає у тому, що за результатами виконаних досліджень розроблено комплекс моделей та методів виявлення вразливостей типу переповнення буферу у програмному забезпеченні комп'ютерних систем та програмні засоби для їх застосування. Використання запропонованих методів дозволяє підвищити точність і швидкодію аналізу коду та інтегрувати автоматизоване виявлення вразливостей у конвеєри автоматизованого збирання та розгортання. Ефективність розроблених рішень підтверджено експериментальними дослідженнями. Нейромережевий детектор на основі

графових моделей показав покращення точності та повноти виявлення, а метод композитної оцінки ризику забезпечує автоматизований пріоритет вразливостей.

У результаті проведених експериментальних досліджень було доведено точність роботи розробленої моделі та методів: використання запропонованого нейромережевого детектора на основі графових представлень коду забезпечує підвищення точності та повноти виявлення переповнення буфера і зменшує час аналізу порівняно з базовими статичними інструментами. Запропонований метод композитної оцінки ризику дає можливість автоматизувати пріоритезацію виявлених вразливостей і прийняття рішень щодо блокування або дозволу збірок у конвеєрах автоматизованого збирання та розгортання.

Особистий внесок здобувача. Всі основні результати дисертаційного дослідження, які представлені до захисту, отримані автором особисто. Постановка наукових задач, розроблення моделей, методів, програмних засобів та проведення експериментальних досліджень виконані у межах єдиної наукової концепції. За результатами проведених досліджень основні наукові результати опубліковано у 4 наукових статтях у фахових наукових журналах України. Апробація засвідчена публікаціями 6 праць в матеріалах міжнародних та всеукраїнських конференцій, з яких 3 праці індексовані у наукометричній базі Scopus і отримано одне авторське свідоцтво на твір.

Апробація матеріалів дисертації.

Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідалися на міжнародних та всеукраїнських науково-практичних конференціях: 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2024), Khmelnytskyi, Ukraine, March 2024; 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS-2024), Khmelnytskyi, Ukraine, June 28, 2024; 2nd International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS-2025), Khmelnytskyi, Ukraine, July 4, 2025; The 2nd International Workshop on Advanced Applied Information Technologies: AI & DSS (AdvAIT-2025), Khmelnytskyi, Ukraine, December 5, 2025; 2024 IEEE 14th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024), Athens, Greece, October 11–13, 2024; International Workshop on Applied Intelligent Security Systems in Law Enforcement (AISSLE-2025), Vinnytsia, Ukraine, October, 30–31, 2025; наукових семінарах кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету

Структура та обсяг дисертації.

Дисертаційна робота має логічну структуру і складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та чотирьох додатків. Повний обсяг роботи містить 233

сторінки друкованого тексту, з них анотація – на 10 стор., зміст – на 2 стор., перелік скорочень – на 1 стор., основний текст – на 150 стор., список із 157 використаних джерел – на 19 стор., додатки – на 37 стор. Дисертація містить 14 рисунків та 23 таблиці.

Зауваження.

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. У першому розділі достатньо ґрунтовно розглянуто вразливості, характерні для системного програмного забезпечення, написаного мовами C/C++. Разом з тим у роботі майже не приділено уваги впливу компіляторних і платформних механізмів захисту, таких як stack canaries, ASLR, DEP та інші засоби захисної компіляції, які в сучасних умовах також істотно впливають на практику виявлення та експлуатації вразливостей.

2. У другому розділі область дослідження обґрунтовано переважно на прикладах системного та вбудованого програмного забезпечення, зокрема FreeRTOS, ZephyrOS, NuttX RTOS і платформи Arduino. Водночас у тексті недостатньо чітко окреслено, якою мірою запропоновані моделі та методи можуть бути безпосередньо перенесені на інші класи програмного забезпечення комп'ютерних систем, що дещо звужує сприйняття універсальності отриманих результатів.

3. У третьому розділі розглянуто два нейромережеві підходи — YOLO-типу та на основі трансформерної архітектури. Проте в роботі не в повній мірі висвітлено питання вибору між цими підходами для практичного використання, зокрема залежно від розміру програмного проєкту, складності графового подання коду та вимог до швидкодії аналізу.

4. У четвертому розділі детально описано інтеграцію запропонованих рішень у CI/CD-конвеєри та механізми блокування небезпечних збірок. Разом з тим дискусійним залишається питання поведінки системи у випадках прикордонних або суперечливих результатів детектування, коли рівень ризику є проміжним, а рішення щодо автоматичного блокування або пропуску збірки потребує додаткового обґрунтування.

5. У дисертації зазначено, що достовірність результатів забезпечується використанням open-source проєктів і синтетичних прикладів. Однак у роботі було б доцільно дещо ширше розкрити співвідношення між реальними та синтетичними даними у формуванні навчальних і тестових вибірок, оскільки це має значення для оцінювання узагальнювальної здатності запропонованих моделей.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

Загальний висновок.

Вважаю, що дисертаційна робота Сєргєєва Євгенія Віталійовича на тему «Методи та засоби виявлення вразливостей у програмному забезпеченні комп'ютерних систем» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеним науковим дослідженням.

Робота містить нові науково обґрунтовані теоретичні й експериментальні результати в галузі 12 «Інформаційні технології» і за своїм науковим рівнем, практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 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 (зі змінами внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Сєргєєв Євгеній Віталійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:
кандидат фізико-математичних наук,
доцент, доцент, кафедри комп'ютерної
інженерії та інформаційних систем
Хмельницького національного університету _____ Тетяна КИСІЛЬ

ВІДДІЛ КАДРІВ
Підпис дійсний
Засвідчую
І.С.Мартинюк

«Підпис Тетяни КИСІЛЬ засвідчую»
Проректор з наукової роботи
Хмельницького національного університету _____ Олег СИНЮК