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.

Сучасний комп'ютерний світ об'єднує складні обчислювальні пристрої, системи обробки даних, телекомунікації та програмне забезпечення разом із засобами його створення. У взаємодії ці елементи формують критично важливу інфраструктуру, що забезпечує роботу державних, військових, промислових, фінансових і побутових систем. Зі зростанням складності програм, масштабів розподілених обчислень і обсягів коду збільшується і кількість потенційних вразливостей.

Під програмним забезпеченням комп'ютерних систем розуміють системні компоненти, які безпосередньо працюють із ресурсами платформи — пам'яттю, процесором, пристроями введення-виведення та інтерфейсами операційних систем. До них належать операційні системи, драйвери, служби, прошивки, вбудоване ПЗ та системні бібліотеки, що відповідають за керування ресурсами й виконання базових операцій.

Чим важливіша сфера застосування ІТ, тим вищі вимоги до надійності та безпеки програмного забезпечення, яке забезпечує обробку, передачу й зберігання даних. Зловмисники використовують вразливості в коді, що може призвести до порушення конфіденційності, цілісності й доступності інформації або навіть до відмови роботи критичних систем. Особливо небезпечними є помилки роботи з пам'яттю, зокрема переповнення буферів, які залишаються одними з найпоширеніших і найскладніших для виявлення, особливо в мовах C/C++.

Саме розв'язанню однієї з окреслених проблем присвячено дисертаційне дослідження Сєргєєва Є. В. У роботі, з метою підвищення точності та ефективності виявлення вразливостей у програмному забезпеченні комп'ютерних систем, запропоновано підхід, що базується на формалізації

процесів переповнення буфера, розробленні нейромережевих детекторів та застосуванні механізмів композитної оцінки ризику для підтримки автоматизованого прийняття рішень в умовах наявності як відомих, так і нових типів загроз.

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.

Мету дисертаційної роботи визначено як 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.

Поставленої мети досягнено в результаті розв'язання таких *завдань:* 1) проведено системний аналіз існуючих підходів до виявлення вразливостей у програмному забезпеченні, визначено їх переваги й недоліки та сформувано вимоги до автоматизованих засобів детектування переповнення буфера; 2) створено формальні моделі класів вразливості типу переповнення буфера у вигляді орієнтованого графа з атрибутами вузлів і ребер, що відображають залежності між даними й керуванням; 3) удосконалено модель процесу виявлення вразливості типу переповнення буфера, в якій здійснено інтеграцію графової моделі, нейромережевого детектора та модуля композитної оцінки ризику в конвеєри автоматизованого збирання та розгортання, для забезпечення підтримки повного циклу аналізу коду та підвищення точності виявлення вразливості типу переповнення буфера; 4) розроблено метод машинного виявлення переповнення буфера з використанням нейромережевої архітектури YOLO/Transformer, визначено правила сегментації графів та формування навчальних вибірок; 5) розроблено метод підготовки та обробки даних на основі

розмітки початкового коду, побудові та сегментуванні орієнтованих графів, перетворенні підграфів у багатоканальні зображення з класами Stack/Heap/Off-by-one; 6) розроблено метод композитної оцінки ризику та алгоритм інтеграції в конвеєрах автоматизованого збирання та розгортання для кількісного оцінювання критичності виявлених вразливостей та автоматизованого управління процесом розгортання; 7) реалізовано прототипи програмних засобів та проведено експериментальні дослідження, інтегровано їх у середовища розробки, оцінено точність і швидкодію порівняно з існуючими сканерами та сформулювано практичні рекомендації.

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 й 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.

У другому розділі розроблено формальні моделі вразливостей ПЗКС з фокусом на переповнення буферу, а також створено інструментарій для аналізу кодової бази. Виявлено ключові умови, за яких виникають вразливості, сформульовано моделі ризику, ідентифіковано шаблони на основі даних із баз CVE, NVD, OWASP. Створені графічні представлення ризиків дозволяють візуалізувати взаємозв'язки між компонентами програми операційної системи та локалізувати ризикові зони. 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.

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. 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. В першому розділі досить детально проаналізовано вразливості, що виникають у системному програмному забезпеченні при використанні мов C та C++, однак майже не розглянуто роль супровідного інструментарію розробки, зокрема компіляторів, засобів налагодження та механізмів захисної компіляції, які також можуть істотно впливати на виявлення та попередження вразливостей.

2. Наведений у роботі опис інтеграції розроблених методів у CI/CD-конвеєр є достатньо інформативним, однак його було б доцільно доповнити більш детальним висвітленням питань практичного налаштування, зокрема вибору порогів спрацювання, правил блокування збірок та параметрів реагування відповідно до рівня критичності.

3. У третьому розділі, при описі методу підготовки даних на основі графових представлень коду та їх перетворення у багатоканальні зображення, було б доцільно ширше проаналізувати вплив параметрів растрування і агрегації ознак на збереження структурних властивостей графа, особливо у випадку щільно зв'язаних фрагментів коду.

4. У четвертому розділі наведено результати експериментальних досліджень та порівняння з відомими підходами. Разом з тим у роботі не повною мірою розкрито питання поведінки запропонованої системи в ситуаціях невизначеного або граничного рішення детектора, зокрема того, як у таких випадках мають розвиватися події в межах конвеєра автоматизованого збирання та розгортання.

5. Дисертація є достатньо ілюстрованою, однак окремі рисунки, зокрема пов'язані з графовим поданням коду та синтезом CFG/DFG, містять значну кількість деталей, що дещо зменшує їх читабельність і сприйняття. Окрім цього, в роботі трапляються окремі стилістичні, термінологічні та редакційні неточності.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий рівень проведеного дослідження.

Загальний висновок.

Вважаю, що дисертаційна робота Сєргєєва Євгенія Віталійовича на тему «Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем», 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. Дослідження містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі розроблення методів та засобів виявлення вразливостей в програмному забезпеченні комп'ютерних систем та застосування нейромережевих детекторів та впровадження механізмів композитної оцінки ризику для автоматизованого прийняття рішень.

Дисертаційна робота «Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем», яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 9 «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 (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 технічних наук, доцент,
доцент кафедри комп'ютерної
інженерії та інформаційних систем
Хмельницького національного університету _____ Марія КАПУСТЯН

ВІДДІЛ КАДРІВ
Підпис Капустян
Засвідчую
Начальник відділу кадрів
І.С.Мартинюк

«Підпис Марії КАПУСТЯН засвідчую»
Проректор з наукової роботи
Хмельницького національного університету _____ Олег СИНЮК