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

_____

29016, м. Хмельницький, вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
доктора технічних наук, професора Ткачука Ростислава Львовича
на дисертацію Сєргєєва Євгенія Віталійовича
на тему: «Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем», подану на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 123 «Комп'ютерна інженерія»

Актуальність теми дисертації. Сучасний етап розвитку інформаційних технологій характеризується інтенсивним ускладненням архітектур програмних систем, зростанням обсягів програмного коду та даних, що обробляються, а також підвищенням рівня інтеграції інформаційно-комунікаційних систем у всі сфери суспільного життя. За таких умов суттєво зростає значущість забезпечення інформаційної безпеки, зокрема у контексті функціонування об'єктів критичної інфраструктури.

Програмне забезпечення комп'ютерних систем, яке забезпечує взаємодію з базовими ресурсами обчислювальних платформ (оперативною пам'яттю, процесором, підсистемами введення-виведення), є системоутворювальним елементом сучасних інформаційно-комунікаційних середовищ. До його складу належать операційні системи, драйвери пристроїв, системні служби, мікропрограмне забезпечення, а також програмні бібліотеки різних рівнів.

Порушення функціонування зазначених компонентів або їх компрометація можуть призводити до критичних наслідків для безпеки інформаційних систем.

Збільшення складності програмних систем та обсягів їх коду об’єктивно супроводжується зростанням кількості вразливостей, експлуатація яких створює загрозу порушення базових властивостей інформаційної безпеки — конфіденційності, цілісності та доступності інформації, а також може спричиняти відмови у функціонуванні систем. Особливу небезпеку становлять вразливості, пов’язані з некоректною обробкою пам’яті, зокрема переповнення буфера, які є типовими для програмного забезпечення, розробленого із використанням мов C/C++.

Незважаючи на наявність значної кількості наукових праць, присвячених аналізу захищеності програмного забезпечення, проблема підвищення ефективності методів виявлення вразливостей у складних програмних системах не є вичерпаною. Подальшого розвитку потребують підходи, що базуються на поєднанні формальних моделей представлення програм із методами інтелектуального аналізу даних, що забезпечує підвищення точності та повноти ідентифікації потенційно небезпечних програмних конструкцій, а також створює передумови для їх інтеграції у процеси життєвого циклу розроблення програмного забезпечення. Актуальним є також розроблення інтелектуалізованих засобів, здатних виявляти як відомі, так і раніше неідентифіковані загрози на основі аналізу непрямих ознак їх прояву.

Зазначене зумовлює наукову та практичну актуальність теми дисертаційної роботи Сєргєєва Є. В., спрямованого на розв’язання науково-прикладного завдання підвищення точності виявлення вразливостей у програмному забезпеченні комп’ютерних систем шляхом формалізації процесів виникнення переповнення буфера, розроблення нейромережевих детекторів та впровадження механізмів композитної оцінки ризику для забезпечення підтримки автоматизованого прийняття рішень у сфері кібербезпеки.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано відповідно до напрямів науково-дослідної діяльності Хмельницького національного університету та пов'язане з реалізацією держбюджетних науково-дослідних тем. Зокрема, результати дослідження корелюють із завданнями теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак у корпоративних мережах із використанням хибних об'єктів атак та пасток» (номер державної реєстрації 0124U000980), а також теми №1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливу комп'ютерних атак» (номер державної реєстрації 0126U002082.

У межах виконання зазначених науково-дослідних тем здобувач брав участь як виконавець, що забезпечило практичну орієнтованість отриманих результатів, їх апробацію в умовах, наближених до реальних, а також відповідність сучасним тенденціям розвитку наукових досліджень у сфері кібербезпеки.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни. Наукова новизна результатів дисертаційної роботи 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.

Наукові положення, висновки та рекомендації, сформульовані у дисертаційній роботі Сєргєєва Є. В., характеризуються належним рівнем теоретичної обґрунтованості, методологічної цілісності та внутрішньої узгодженості. Їх обґрунтованість забезпечується коректним застосуванням апарату математичного моделювання, а також підтверджується результатами практичної реалізації та впровадження. У процесі розв’язання поставленого науково-прикладного завдання використано комплекс взаємодоповнювальних наукових підходів, зокрема теорію графів, елементи абстрактної алгебри, методи машинного навчання, теоретичні засади інформаційних технологій, методи забезпечення інформаційної безпеки, а також статистичні методи оцінювання якості результатів.

Обґрунтованість наукових положень і висновків базується на системному аналізі сучасних наукових джерел за тематикою дослідження, чіткій постановці мети та завдань, їх логічній узгодженості, застосуванні адекватного методичного апарату та коректному використанні математичних методів для формалізації та доведення отриманих результатів. Послідовність викладення матеріалу,

аргументованість проміжних і підсумкових тверджень, а також логічна завершеність висновків свідчать про належний рівень наукової культури дослідження.

Достовірність отриманих результатів забезпечується коректністю застосування використаних методів і підходів, узгодженістю теоретичних положень із результатами експериментальних досліджень, а також відтворюваністю отриманих результатів. Практична значущість роботи підтверджується результатами апробації розроблених методів і засобів, що засвідчує їх придатність до використання у сфері забезпечення кібербезпеки комп'ютерних систем.

Сформульовані у дисертації наукові положення, висновки та рекомендації є узагальненням результатів проведеного дослідження, що ґрунтується на поєднанні теоретичних положень і результатів експериментальної перевірки. Отримані результати відзначаються науковою обґрунтованістю, достовірністю та коректністю, що дозволяє вважати запропоновані рішення такими, що мають як теоретичну, так і прикладну цінність.

Таким чином, у дисертаційній роботі розв'язано поставлене науково-прикладне завдання, а здобувач продемонстрував належний рівень оволодіння методологією наукових досліджень, що відповідає сучасним вимогам до підготовки докторів філософії за спеціальністю 123 «Комп'ютерна інженерія».

Оцінка змісту дисертації, її завершеності та дотримання принципів академічної доброчесності. Зміст дисертаційної роботи Сєргєєва Є. В. відповідає вимогам чинного стандарту вищої освіти за спеціальністю 123 «Комп'ютерна інженерія» для третього (освітньо-наукового) рівня вищої освіти, а також узгоджується з положеннями освітньо-наукової програми Хмельницького національного університету «Комп'ютерна інженерія». Структура дисертації є логічно вмотивованою, характеризується послідовністю викладу матеріалу, внутрішньою цілісністю та завершеністю наукового дослідження. Це свідчить про сформованість системного наукового підходу

здобувача та наявність його особистого внеску у розвиток відповідного напряму комп’ютерної інженерії.

Дисертація є завершеною кваліфікаційною науковою працею, у якій у повному обсязі розкрито поставлену наукову проблему, здійснено теоретичне узагальнення та запропоновано її розв’язання, що супроводжується належним обґрунтуванням отриманих результатів, формулюванням висновків та практичних рекомендацій.

Результати перевірки дисертаційної роботи на відповідність принципам академічної доброчесності засвідчують відсутність ознак академічного плагіату та некоректних запозичень. Усі використані наукові положення, результати та текстові фрагменти, що належать іншим авторам, належним чином ідентифіковані та супроводжуються коректними бібліографічними посиланнями, що відповідає встановленим вимогам академічної етики та доброчесності.

Практичне значення одержаних результатів. За результатами проведеного дослідження розроблено комплекс взаємопов’язаних моделей, методів і програмних засобів, призначених для виявлення вразливостей типу переповнення буфера у програмному забезпеченні комп’ютерних систем. Запропоновані рішення забезпечують підвищення точності та оперативності аналізу програмного коду, а також створюють передумови для інтеграції автоматизованих засобів виявлення вразливостей у процеси безперервної інтеграції та розгортання (CI/CD).

Ефективність запропонованих методів і засобів підтверджується результатами експериментальних досліджень. Зокрема, використання нейромережевого детектора, побудованого на основі графових моделей представлення програмного коду, забезпечує підвищення показників точності та повноти виявлення вразливостей порівняно з традиційними методами статичного аналізу, а також сприяє зменшенню часових витрат на проведення аналізу. Запропонований метод композитної оцінки ризику дозволяє автоматизувати процес пріоритезації виявлених вразливостей та забезпечує

підтримку прийняття рішень щодо доцільності блокування або дозволу програмних збірок у межах автоматизованих процесів розроблення та розгортання.

Достовірність отриманих результатів підтверджується узгодженістю теоретичних положень із результатами експериментальної перевірки, що засвідчує ефективність розроблених моделей і методів у практичних умовах.

Практичну значущість результатів дисертаційної роботи підтверджено їх впровадженням у діяльність підприємств ТОВ «Nolt technologies» та ТОВ «ІТТ» (м. Хмельницький, Акти від 16.02.2026), а також використанням в освітньому процесі Хмельницького національного університету (Акт від 25.02.2026). Зокрема, результати дослідження застосовуються під час викладання дисциплін кафедри комп'ютерної інженерії та інформаційних систем для здобувачів спеціальності F7 «Комп'ютерна інженерія», зокрема «Безпека та захист комп'ютерних систем», «Моделювання та методи оптимізації в наукових та експериментальних дослідженнях», «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп'ютерних систем та мереж».

Мова та стиль викладення результатів. Дисертаційна робота виконана державною мовою та характеризується високим рівнем науково-технічного викладу, логічною послідовністю побудови та чіткістю формулювань. Текст дисертації сформульовано з використанням сучасного термінологічного апарату, що відповідає вимогам до наукових досліджень у галузі комп'ютерної інженерії. Виклад матеріалу є послідовним, структурованим і змістовно завершеним, що забезпечує належний рівень сприйняття та інтерпретації отриманих результатів.

Мовностилістичне оформлення роботи відповідає нормам наукового стилю, характеризується точністю, однозначністю та коректністю використання наукової термінології. Ілюстративний матеріал (таблиці, рисунки) органічно інтегрований у структуру роботи, сприяє підвищенню наочності викладених результатів та їх кращому розумінню.

Структурно дисертація відповідає встановленим вимогам і складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 233 сторінки друкованого тексту, з яких основний зміст викладено на 150 сторінках. Список використаних джерел налічує 157 найменувань. Робота містить 13 рисунків та 24 таблиці, що відповідає характеру та обсягу проведеного дослідження.

У вступі обґрунтовано актуальність теми дисертаційної роботи, визначено мету, завдання, об’єкт і предмет дослідження, наведено відомості про наукову новизну, практичне значення, апробацію результатів та їх зв’язок із науковими програмами.

У першому розділі здійснено аналіз предметної області, класифікацію вразливостей програмного забезпечення та огляд сучасних методів їх виявлення, включаючи статичний і динамічний аналіз, а також підходи машинного навчання. Визначено обмеження існуючих засобів і підходів.

У другому розділі розроблено формальну модель вразливостей переповнення буфера на основі графового представлення програм, визначено показники ризику та запропоновано модель композитної оцінки ризику їх експлуатації.

У третьому розділі запропоновано нейромережеві методи виявлення вразливостей на основі графових представлень програмного коду, зокрема підходи із використанням YOLO-подібних архітектур і трансформерних моделей, а також методи підготовки даних і інтеграції результатів аналізу.

У четвертому розділі наведено програмну реалізацію розроблених методів, описано архітектуру відповідного програмного комплексу, його інтеграцію в процеси автоматизованого розроблення, а також результати експериментальної перевірки ефективності запропонованих рішень.

У висновках узагальнено основні результати дисертаційної роботи.

У додатках подано матеріали, що підтверджують апробацію та впровадження отриманих результатів.

Оформлення дисертації здійснено відповідно до чинних нормативних вимог, визначених наказом Міністерства освіти і науки України від 12.01.2017 № 40 «Про затвердження вимог до оформлення дисертацій».

Оприлюднення результатів дисертаційної роботи. Основні результати дисертаційної роботи пройшли належну апробацію та оприлюднені у наукових публікаціях. Зокрема, ключові положення роботи відображено у 4 наукових статтях, опублікованих у фахових виданнях України, а також у 6 публікаціях у матеріалах міжнародних та всеукраїнських науково-практичних конференцій, з яких 3 індексовано у наукометричній базі Scopus. Додатково результати дослідження підтверджено наявністю авторського свідоцтва на твір.

Аналіз змісту наукових публікацій засвідчує, що вони повною мірою відображають основні результати дисертаційної роботи, характеризуються належним науковим рівнем та відповідають вимогам академічної доброчесності. У публікаціях забезпечено дотримання принципів коректного цитування та належного оформлення бібліографічних посилань.

Таким чином, результати дисертаційної роботи отримали належне висвітлення у наукових працях здобувача, що підтверджує їх апробацію, достовірність та наукову значущість.

Недоліки та зауваження до дисертаційної роботи:

1. У першому розділі дисертації в межах аналізу предметної області розглянуто широкий спектр вразливостей, зокрема пов’язаних як із порушенням цілісності пам’яті, так і з SQL-ін’єкціями, XSS-атаками та логічними помилками. Водночас основний зміст дослідження зосереджено на проблематиці переповнення буфера, що обумовлює доцільність більш чіткого окреслення меж дослідження з метою підвищення логічної узгодженості та цілісності викладу матеріалу.

2. У таблиці 2.1. «Інтеграція типових класів вразливостей у три узагальнені категорії» (с. 66) запропоновано узагальнення шести базових класів

вразливостей у три інтегровані категорії. Такий підхід є обґрунтованим у контексті задач автоматизованого аналізу, однак віднесення таких типів вразливостей, як Integer Overflow та Race Conditions, до відповідних узагальнених класів має дискусійний характер і потребує додаткового теоретичного обґрунтування.

3. На рисунках 3.1 (с. 95) та 3.2 (с. 96), які ілюструють графове подання програмного коду та процес синтезу CFG/DFG, відображено важливі аспекти запропонованого підходу. Разом із тим, унаслідок високої насиченості елементами та позначеннями, окремі фрагменти візуалізації є недостатньо чіткими, що певною мірою ускладнює їх інтерпретацію.

4. У четвертому розділі наведено результати порівняльного аналізу запропонованого підходу зі статичними аналізаторами та моделлю GraphCodeBERT. Водночас відсутність прямого зіставлення з підходами, що базуються на графових нейронних мережах (GNN), яке пояснюється відмінностями у постановках задач і протоколах оцінювання, залишає відкритим питання щодо повноти проведеного порівняльного аналізу.

5. У частині, присвяченій науковій новизні, де запропоновано метод автоматизованого виявлення вразливостей типу «переповнення буфера» на основі графових моделей і архітектури YOLO, отримані результати є обґрунтованими та переконливими. Разом із тим доцільним видається більш чітке виокремлення авторського внеску здобувача та складових, що базуються на адаптації відомих нейромережевих підходів.

6. Запропонований метод підготовки та обробки даних для навчання нейромережевих детекторів, зокрема побудова орієнтованих графів і трансформація підграфів у багатоканальні зображення, становить науковий інтерес. Водночас дискусійним залишається питання повноти збереження суттєвих структурних характеристик вихідного програмного коду при такому перетворенні, особливо для складних і щільно зв’язаних графових структур.

7. У тексті дисертації має місце окрема термінологічна неузгодженість, зокрема паралельне використання варіантів «імовірність» та «ймовірність», що потребує уніфікації відповідно до норм сучасної української наукової мови.

8. У роботі виявлено поодинокі редакційні та стилістичні неточності. Зокрема, у змісті використано формулювання «Підготовки даних для виявлення переповнень пам’яті», а в одному із завдань дослідження — конструкцію «на основі розмітки початкового коду, побудові та сегментуванні…», що потребують стилістичного та граматичного узгодження.

Наведені зауваження мають рекомендаційний характер, не є принциповими та не впливають на загальну позитивну оцінку дисертаційної роботи, її наукову новизну, теоретичну значущість і практичну цінність.

Висновок про дисертаційну роботу. Узагальнюючи результати проведеного аналізу, слід зазначити, що дисертаційна робота Сєргєєва Євгенія Віталійовича на тему «Методи та засоби виявлення вразливостей у програмному забезпеченні комп’ютерних систем» є завершеним науковим дослідженням, виконаним на належному теоретичному та науково-прикладному рівнях. Отримані результати характеризуються науковою новизною, теоретичною обґрунтованістю та практичною значущістю, а їх сукупність забезпечує розв’язання актуального науково-прикладного завдання у галузі кібербезпеки та комп’ютерної інженерії.

Дисертаційна робота виконана з дотриманням принципів академічної доброчесності.

За рівнем актуальності, ступенем наукової новизни, обґрунтованістю отриманих результатів і практичною цінністю дисертація відповідає вимогам чинного законодавства України, зокрема положенням пунктів 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 року № 44 (зі змінами, внесеними згідно з Постановами КМ № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024).

З огляду на викладене, вважаю, що Сєргєєв Євгеній Віталійович заслуговує на присудження ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 123 «Комп'ютерна інженерія».

Офіційний опонент
професор кафедри управління
інформаційною безпекою
Львівського державного університету
безпеки життєдіяльності
доктор технічних наук, професор _____ Ростислав ТКАЧУК