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
кандидата технічних наук, доцента **Козака Руслана Орестовича**
на дисертаційну роботу **Сєргєєва Євгенія Віталійовича**
на тему: «Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем»,
подану до захисту на здобуття наукового ступеня **доктора філософії**
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дисертаційної роботи

Сучасний комп'ютерний світ є складною системою обчислювальних пристроїв, технологій обробки даних, телекомунікацій та програмного забезпечення. Їх взаємодія формує критичну інфраструктуру, що забезпечує функціонування державних, військових, промислових і фінансових систем. Зі зростанням складності програм і обсягів коду збільшується й кількість потенційних вразливостей.

Під програмним забезпеченням комп'ютерних систем розуміють системні компоненти, що взаємодіють із ресурсами платформи. До них належать операційні системи, драйвери, служби, прошивки та бібліотеки, які забезпечують базові функції управління ресурсами. З підвищенням відповідальності сфер застосування зростають вимоги до безпеки ПЗ. Вразливості в коді можуть призвести до порушення конфіденційності, цілісності та доступності даних або навіть до відмови систем. Особливо небезпечними є помилки роботи з пам'яттю, зокрема переповнення буфера в мовах C/C++.

Незважаючи на існуючі дослідження, актуальним залишається підвищення точності методів виявлення вразливостей шляхом поєднання формальних моделей аналізу коду з інтелектуальними підходами, зокрема нейронними мережами.

2. Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження виконувалось 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.

3. Наукова новизна отриманих результатів.

До основних наукових результатів дисертаційної роботи варто віднести:

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.

4. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації адекватно і в повній мірі відображає її зміст.

У *вступі* обґрунтовано актуальність теми дисертації, визначено мету, предмет та об'єкт дослідження, визначені основні завдання, відображено наукову новизну і практичне значення отриманих 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 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 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.

В цьому ж розділі 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.

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. 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.

У *додатках* представлено наукові публікації, в яких відображено основні наукові результати роботи, акти впровадження результатів роботи.

5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність.

Сформульовані у дисертації наукові положення, висновки та рекомендації є аргументованими і підкріплені практичною реалізацією.

Наукова обґрунтованість положень і висновків дисертації забезпечена аналізом літературних джерел, чітким формулюванням завдань дослідження та використанням сучасних методологічних підходів.

Достовірність одержаних результатів підтверджена їх апробацією на міжнародних та всеукраїнських наукових конференціях, а також практичним впровадженням.

6. Практичні результати роботи

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.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «Nolt technologies» (м.Хмельницький, Акт від 16.02.2026), ТОВ «ІТТ» (м. Хмельницький, Акт від 16.02.2026), а також, в освітньому процесі Хмельницького національного університету (Акт від 25.02.2026) при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для здобувачів спеціальності F7(123) Комп'ютерна інженерія, зокрема в курсах «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».

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях.

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.

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

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.

Усі сформовані наукові положення і результати дисертації повністю викладено в опублікованих працях.

8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи викладено в логічній послідовності. Дисертація містить достатню кількість ілюстративного матеріалу – схем, рисунків, графіків і таблиць. Мова викладу, стиль та оформлення роботи повністю відповідають установленим вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

Зауваження та рекомендації до дисертації:

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 інших засобів захисної компіляції, які в сучасних умовах також істотно впливають на практику виявлення та експлуатації вразливостей.

2. У другому розділі побудовано формальні моделі вразливостей переповнення буфера та запропоновано математичні залежності для їх опису. Водночас було б доцільно чіткіше окреслити межі застосування цих моделей для різних середовищ виконання, зокрема для систем із відмінними механізмами керування пам'яттю та різними реалізаціями алокаторів.

3. У третьому розділі розглянуто як YOLO-подібний підхід, так і трансформерну архітектуру для виявлення вразливостей. Проте в роботі не в повній мірі висвітлено питання практичного вибору між цими підходами залежно від складності програмного проєкту, вимог до швидкодії та доступних обчислювальних ресурсів.

4. У четвертому розділі наведено результати експериментальних досліджень і показано ефективність запропонованого підходу. Разом з тим робота виглядала б ще більш завершеною за наявності детальнішого аналізу

часових витрат окремих етапів повного конвеєра, зокрема побудови графів, їх растрування, нейромережевого аналізу та постобробки результатів.

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

6. Наукову новизну, пов'язану з удосконаленням моделі процесу виявлення вразливостей шляхом інтеграції графової моделі, нейромережевого детектора та модуля композитної оцінки ризику в конвеєри автоматизованого збирання та розгортання, загалом сформульовано переконливо. Водночас залишається питання більш чіткого розмежування власне наукової складової цієї моделі та її прикладної реалізації в CI/CD-середовищі.

7. У пункті наукової новизни, де йдеться про метод композитної оцінки ризику експлуатації виявлених вразливостей, слушно підкреслено його зв'язок із результатами нейромережевого детектування та автоматизацією пріоритезації виправлень. Разом з тим певну наукову дискусію викликає питання більш розгорнутого обґрунтування вибору окремих показників ризику та їх впливу на підсумкове ранжування вразливостей.

Зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Сєргєєва Євгенія Віталійовича на тему «Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем», що 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 йому наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент,
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Тернопільського національного
технічного університету
імені Івана Пулюя _____ Руслан КОЗАК

Підпис доцента кафедри кібербезпеки
Тернопільського національного технічного
університету імені Івана Пулюя
к.т.н., доцента Козака Р. О.
засвідчую:
Вчений секретар
Тернопільського національного
технічного університету
імені Івана Пулюя _____ Галина КРАМАР