Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії ___Сєргєєв Євгеній Віталійович_____,
(власне ім'я, прізвище здобувача (ки))
__1997_ року народження, громадянин (ка) _____України_____,
(назва держави, громадянином якої є здобувач (ка))
освіта вища: закінчив (ла) у __2021__ році Хмельницький національний університет_____
(найменування закладу вищої освіти)
за спеціальністю (спеціальностями) 123 Комп'ютерна інженерія,
(за дипломом)
працює молодшим науковим співробітником
(посада)
в Хмельницькому національному університеті Міністерства освіти і науки України,
м. Хмельницький
(місце основної роботи, підпорядкування, місто)
виконав (ла) акредитовану освітньо-наукову програму «Комп'ютерна інженерія» Хмельницького національного університету
Разова спеціалізована вчена рада, утворена наказом Хмельницького національного університету
(повне найменування закладу вищої освіти
Міністерства освіти і науки України, м. Хмельницький від « 30 » 03 2026 року № 41-ас
(наукової установи), підпорядкування (у родовому відмінку), місто)
у складі:
Голови разової
спеціалізованої вченої ради – Сергія ЛИСЕНКА, доктора технічних наук, професора, професора кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Рецензентів - Тетяни КИСІЛЬ, кандидата фізико-математичних наук, доцента доцента кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Марії КАПУСТЯН, кандидата технічних наук, доцента, доцента кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Офіційних опонентів - Ростислава ТКАЧУКА, доктора технічних наук, професора, професора кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Руслана КОЗАКА, кандидата технічних наук, доцента, доцента кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
на засіданні «22» травня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології
(галузь знань)
Євгенію СЄРГЄЄВУ
(власне ім'я, прізвище здобувача (ки) у давальному відмінку)

на підставі публічного захисту дисертації «МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ КОМП'ЮТЕРНИХ СИСТЕМ»

(назва дисертації)

за спеціальністю (спеціальностями) 123 – Комп'ютерна інженерія

(код і найменування спеціальності (спеціальностей)

.

відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Дисертацію виконано у (в) Хмельницькому національному університеті Міністерства освіти і

(повне найменування закладу вищої освіти

науки України, м. Хмельницький

(найменування закладу вищої освіти (наукової установи), підпорядкування, місто)

Наукові керівники: Олег САВЕНКО, доктор технічних наук, професор,

(власне ім'я, прізвище, науковий ступінь,

професор, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету; Юрій КЛЬОЦ, кандидат технічних наук, доцент, завідувач кафедри кібербезпеки Хмельницького національного університету.

(вчене звання, місце роботи, посада)

Дисертацію подано у вигляді спеціально підготовленого рукопису. Дисертація містить чотири нові науково обґрунтовані результати проведених здобувачем досліджень, які виконують конкретне наукове завдання виявлення переповнення буфера у програмному забезпеченні комп'ютерних систем і створення нейромережевих детекторів та впровадження механізмів композитної оцінки ризику для автоматизованого прийняття рішень, що має істотне значення для галузі знань 12 – Інформаційні технології. Дисертація виконана державною мовою. Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації». Загальний обсяг дисертаційної роботи становить 233 сторінки друкованого тексту, з них 150 сторінок основного тексту, що відповідає встановленим освітньо-науковою програмою «Комп'ютерна інженерія» Хмельницького національного університету максимальному та мінімальному обсягам основного тексту дисертації.

Здобувач має 10 наукових публікацій за темою дисертації, з них 4 статті у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б:

1.Сєргєєв Є., Каштальян А., Ковальчук В., Савенко О., Іванченко О. Ефективність і вдосконалення SAST у контексті SQL Injection вразливостей in the Information Technology: Computer Science, Software Engineering and Cyber Security 2024. №3. Pp. 149-158. https://doi.org/10.32782/IT/2024-3-16

2. Сєргєєв Є. В.; Савенко О. С. Виявлення вразливостей переповнення буфера в системному програмному забезпеченні на основі графа та моделі трансформатора. Вісник Хмельницького національного університету. Серія «Технічні науки». 2025. №6. С. 318-327. DOI https://doi.org/10.32782/2663-5941/2025.6.2/43

3. Сєргєєв Є. В. Підготовка даних на основі графіків для виявлення вразливостей переповнення буфера в коді в рамках CI/CD-процесів. Herald of Khmelnytskyi National University. Technical sciences 2026. №361(1). Pp. 316–322. https://doi.org/10.31891/2307-5732-2026-361-45

4.Сєргєєв, Є. В., Кльоц Ю. П. Композитна оцінка ризику переповнення буфера і її трансляція в дії CI/CD. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. 2025. №84(4). Pp. 89–94. https://doi.org/10.31891/2219-9365-2025-84-10

У дискусії взяли участь (голова, рецензенти, офіційні опоненти, інші присутні) та висловили зауваження:

Лисенко Сергій Миколайович, д.т.н., професор, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету; Кисіль Тетяна Миколаївна, к.ф.-м.н., доцент, доцент кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету; Капустян Марія Вікторівна, к.т.н., доцент, доцент

кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету; Ткачук Ростислав Львович, д.т.н., професор, начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності; Козак Руслан Орестович, к.т.н, доцент, доцент кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя.

Зауваження:

Кисіль Тетяна Миколаївна, к.ф.-м.н., доцент, доцент кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету:

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.

Капустян Марія Вікторівна, к.т.н., доцент, доцент кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету:

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.

Ткачук Ростислав Львович, д.т.н., професор, професор кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності:

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 10 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.

Козак Руслан Орестович, к.т.н, доцент, доцент кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя:

1) у першому розділі достатньо грунтовно 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.

Результати відкритого голосування:

«За» ___5___ членів ради,

«Проти» ___0___ членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує

_____Євгенію СЄРГЄЄВУ_____

(власне ім'я, прізвище, здобувача (ки) у давальному відмінку)

ступінь/ступеня доктора філософії з галузі знань _____12 – Інформаційні технології_____

(галузь знань)

за спеціальністю (спеціальностями) __123 – Комп'ютерна інженерія_____

(код і найменування спеціальності (спеціальностей)

_____.

відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої вченої ради _____ Сергій ЛИСЕНКО

(підпис) (власне ім'я та прізвище)

М.П.