*Зразок_1*

# ВИСНОВОК
## про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «*Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем*»
*(назва роботи)*

здобувача наукового ступеня доктора філософії

*Сергєєва Євгенія Віталійовича*
*(прізвище, ім'я, по батькові)*

з галузі знань *12 Інформаційні технології*
*(шифр, назва галузі знань)*

за спеціальністю *123 Комп'ютерна інженерія*.
*(шифр, назва спеціальності)*

Публічна презентація проведена на *кафедрі комп'ютерної інженерії та інформаційних систем*
*назва)*

« 4 » березня 2026 року, протокол № 18 .

**1. Обґрунтування вибору теми дослідження.** *Актуальність теми дисертаційної роботи зумовлена постійним зростанням кількості кіберзагроз, пов'язаних із вразливостями програмного забезпечення комп'ютерних систем, а також високою критичністю вразливостей класу переповнення буфера у програмному коді мов C/C++. Такі вразливості можуть призводити до неконтрольованого перезаписування пам'яті, порушення цілісності даних, відмов у роботі систем та довільного виконання коду. Наявні засоби статичного та динамічного аналізу не завжди забезпечують достатню точність, інтерпретованість і масштабованість у межах сучасних індустріальних проєктів та CI/CD-процесів. У зв'язку з цим розроблення методів і засобів виявлення вразливостей у програмному забезпеченні комп'ютерних систем, зокрема на основі графових моделей, нейромережевого аналізу та композитної оцінки ризику, є актуальним науковим завданням*

**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. Дослідження спрямовано на формування та реалізацію моделей і алгоритмів для автоматизованого пошуку небезпечних ділянок коду із застосуванням сучасних технологій машинного навчання.*

*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.*

*Пояснення: дисертація повинна містити наукові положення, нові науково обґрунтовані теоретичні та/або експериментальні результати проведених досліджень, що мають істотне значення для певної галузі знань та підтверджуються документами, які засвідчують проведення таких досліджень, а також свідчити про особистий внесок здобувача в науку та характеризуватися єдністю змісту.*

**5. Використання результатів роботи.** *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 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».*

**6. Особиста участь автора** в отриманні наукових та практичних результатів, що викладені в дисертаційній роботі. *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.*

Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету,

*(назва кафедри (відділу), назва установи)*

наукові керівники:

*доктор технічних наук, професор, професор кафедри комп'ютерної інженерії та інформаційних систем Савенко Олег Станіславович,*

*кандидат технічних наук, доцент, завідувач кафедри кібербезпеки Кльоц Юрій Павлович,*

*(науковий ступінь, вчене звання, посада, прізвище, ініціали)*

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Сергєєва Є. В.

*(прізвище, ініціали здобувача)*

є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.

**Дотримання академічної доброчесності.** Роботу Сергєєва Є. В. перевірено на плагіат програмним засобом «Strike Plagiarism». (№ 333291276 від 2/16/2026; схожість тексту дисертації укр. мовою - 3,77 %, англ. мовою - 6,90 %).

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

**7. Перелік публікацій за темою дисертації** із зазначенням особистого внеску здобувача.

*Статті у наукових фахових виданнях*

1. *Сергєєв Є. В., Каштальян А., Ковальчук В., Савенко О., Іванченко О. Ефективність і вдосконалення SAST у контексті SQL Injection вразливостей // Information Technology: Computer Science, Software Engineering and Cyber Security. 2024. № 3. С. 149–158. DOI: 10.32782/IT/2024-3-16. - здобувачем проаналізовано проблематику SQL Injection-вразливостей, узагальнено недоліки наявних SAST-підходів, запропоновано напрями підвищення ефективності виявлення та підготовлено основний зміст публікації.*
2. *Сергєєв Є. В., Савенко О. С. Виявлення вразливостей переповнення буфера в системному програмному забезпеченні на основі графа та моделі трансформатора // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2025. № 6. С. 318–327. DOI: 10.32782/2663-5941/2025.6.2/43. -здобувачем сформульовано постановку задачі виявлення buffer overflow у системному програмному забезпеченні, запропоновано графову репрезентацію коду, обґрунтовано використання трансформерної моделі, виконано аналіз результатів.*
3. *Сергєєв 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. DOI: 10.31891/2307-5732-2026-361-45.- здобувачем розроблено метод підготовки даних на основі графіків переповнення буфера.*
4. *Сергєєв Є. 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. DOI: 10.31891/2219-9365-2025-84-10. – здобувачем розроблено метод композитної оцінки ризику переповнення буфера.*

*Авторські свідоцтва*

5. *Сергєєв Є. В., Савенко О. С. Авторське свідоцтво №143407. Україна. Комп'ютерна програма «OverflowGuard: система аналізу переповнення буфера та оцінки ризику в CI/CD». Дата реєстрації: 23 лютого 2026 р.*

*Матеріали конференцій*

6. *Sierhieiev Yevheniy, Paiuk Vadym, Sachenko Anatoliy, Nicheporuk Andrii, Kwiecien Andrzej. A graph-based vulnerability detection method // CEUR Workshop Proceedings. 2024. Vol-3675. Pp. 343–355.*
*- здобувачем запропоновано graph-based метод виявлення вразливостей, визначено структуру моделі, проведено аналіз результатів та сформульовано висновки.*
7. *Sierhieiev Yevheniy, Paiuk Vadym, Nicheporuk Andrii, Kwiecien Andrzej, Huralnyk Oleksandr. Detection and prediction of the vulnerabilities in software systems based on behavioral analysis with machine learning // CEUR Workshop Proceedings. 2024. Vol-3736. Pp. 239–254. - здобувачем виконано аналіз підходів до поведінкового аналізу вразливостей, підготовлено постановку*

*задачі прогнозування та інтерпретовано результати застосування машинного навчання.*

8. *Sierhieiev Yevhenii, Savenko Oleg, Lips Silvia, Gaj Piotr. Graph-based data preparation for detecting buffer overflow vulnerabilities in code within CI/CD pipelines // CEUR Workshop Proceedings. 2025. Vol-4163. Pp. 1–10. - здобувачем розроблено підхід до підготовки графових даних для виявлення вразливостей переповнення буфера в коді в межах CI/CD, визначено етапи побудови та перетворення інформативних підграфів.*

9. *Savenko Oleg, Sierhieiev Yevhenii, Gaj Piotr, Balej Jiri. Using artificial intelligence in the context of buffer overflow vulnerabilities // CEUR Workshop Proceedings. 2025. Vol-4013. Pp. 211–220. - здобувачем узагальнено підхід до застосування штучного інтелекту для виявлення buffer overflow-вразливостей, сформульовано постановку задачі та взято участь у підготовці експериментальної частини.*

10. *Savenko Oleg, Gaj Piotr, Sierhieiev Yevhenii. Detection of buffer overflow vulnerabilities in system software based on a graph and transformer model // CEUR Workshop Proceedings. 2025. Vol-4126. Pp. 292–305. - здобувачем запропоновано графову модель подання фрагментів програмного коду та описано застосування transformer-based approach для детектування вразливостей переповнення буфера.*

11. *Sierhieiev Yevhenii, Paiuk Vadym, Savenko Oleg, Drozd Andriy. Improvement of effectiveness for Static Application Security Testing for detection of SQL Injection vulnerabilities // IEEE 14th International Conference on Dependable Systems, Services and Technologies (DESSERT-2024): Proceedings. Athens, Greece, Oct 11–13, 2024. Pp. 1–6. DOI: 10.1109/DESSERT65323.2024.11122171. – здобувачем окреслені напрями підвищення ефективності виявлення та підготовлено основний зміст публікації*

**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

У роботах, опублікованих одноосібно автором, отримано наступні результати: розроблено підхід до побудови графових моделей програмного коду та підготовки даних на їх основі для задачі виявлення вразливостей переповнення буфера у конвеєрах автоматизованого збирання та розгортання; запропоновано композитну оцінку ризику переповнення буфера та схему її інтеграції у конвеєрах автоматизованого збирання та розгортання для підтримки прийняття рішень щодо якості та безпеки програмного забезпечення.

У роботах, які опубліковані у співавторстві, автору належать основні ідеї, теоретична та практична розробка положень, відображених у характеристиці наукової новизни отриманих результатів, а саме: здійснено

формування вимог до сучасних статичних методів аналізу безпеки, розроблення підходів для підвищення ефективності SAST-засобів у контексті SQL-ін'єкцій, вдосконалення методу статичного тестування безпеки застосунків у контексті вразливостей SQL Injection; здійснено побудову графової моделі представлення програм та розроблення нейромережевого методу детектування на основі трансформерної архітектури; розроблення підходу до побудови графових моделей коду для задачі виявлення вразливостей, визначення схеми перетворення таких моделей у вхідні дані для нейронних мереж і обґрунтування переваг графового представлення порівняно з лінійним; розроблення формальних моделей вразливостей переповнення буфера та нейромережевого методу їх виявлення на основі архітектури YOLO з використанням графових представлень коду; розроблення підходу до аналізу поведінкових характеристик програмних систем з використанням методів машинного навчання для виявлення та прогнозування вразливостей, а також адаптація отриманих положень для формування показників ризику; розроблення програмного засобу «OverflowGuard: система аналізу переповнення буфера та оцінки ризику в CI/CD».

За результатами досліджень опубліковано 10 наукових праць, у тому числі 0 монографій, 4 статей у наукових фахових виданнях (з них 0 статей у періодичних наукових виданнях інших держав, які входять до ОЕСР та/або Європейського Союзу, фахових виданнях України категорії «А», або закордонних виданнях, що входять до WoS або Scopus) 0 патентів України, 6 публікацій в матеріалах конференцій.

**Особистий внесок здобувача:** *проведено аналіз ефективності SAST для виявлення SQL Injection-вразливостей, запропоновано підходи до покращення виявлення та узагальнено результати експериментів.*

ВВАЖАТИ, що дисертаційна робота ____ *Сергєєва Є. В.*
*(прізвище, ініціали здобувача)*

«*Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем*»,
*(назва)*

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 Постанови Кабінету Міністрів України від 12 січня 2022 р. № 44 «ПОРЯДОК присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» *(із змінами, внесеними згідно з Постановами КМ* № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024*)*, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності *123 Комп'ютерна інженерія*.
*(шифр, назва)*

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «*Методи та засоби виявлення вразливостей в програмному забезпеченні комп'ютерних систем*»,
*назва роботи*

подану *Сергєєвим Євгенієм Віталійовичем*
*прізвище, ім'я, по батькові*

на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації,
завідувачка кафедри КІІС,
*доктор філософії,*
*(науковий ступінь,*
*доцент*
*вчене звання, посада)* *Ольга ПАВЛОВА*
*Ім'я ПРІЗВИЩЕ*

Міністерство освіти і науки України
Хмельницький національний університет
ВІДДІЛ КАДРІВ
Ідентифікаційний код 02071234

Підпис дійсний
підпис
Засвідчую
Начальник відділу кадрів
І.С.Мартинюк