Голові разової спеціалізованої вченої ради
Тернопільського національного технічного
університету імені Івана Пулюя
доктору технічних наук, професору
Пастуху Олегу Анатолійовичу

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента Медзатого Дмитра Миколайовича
на дисертаційну роботу Ревнюка Олександра Андрійовича
на тему «Розробка інформаційної системи оцінювання якості захисту вебдодатків»,
подану до захисту на здобуття наукового ступеня доктора філософії в галузі знань
12 Інформаційні технології
за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації. За останнє десятиліття на ринку програмного забезпечення спостерігається стрімке зростання частки вебдодатків. Цьому сприяє як розвиток вебтехнологій (зокрема, PWA, SPA тощо), так і загальні тенденції цифрової трансформації економіки. Важливо також враховувати високі темпи впровадження та інтеграції компонентів штучного інтелекту у процеси розроблення програмного забезпечення. Усе це призводить до істотного збільшення кількості вебдодатків, зростання їхньої складності, а також обсягу конфіденційних і чутливих даних користувачів та бізнесів, які ці додатки обслуговують. Відповідно, зростає й площина можливих кіберзагроз, що робить вебдодатки однією з найпривабливіших цілей для зловмисників. Атаки стають дедалі витонченішими, а стандартні засоби захисту вже не здатні забезпечити належний рівень безпеки.

У таких умовах актуальним є створення ефективних інформаційних технологій, методів та засобів оцінювання захищеності вебдодатків, які б дозволяли своєчасно, оперативно та точно визначати рівень їхньої безпеки відповідно до міжнародних стандартів (OWASP, ISO/IEC 27002:2022, NIST SP 800-53 тощо).

Отже, з огляду на вище викладене, актуальною науково-практичною задачею є розроблення інформаційної системи оцінювання якості захисту вебдодатків, що дозволить автоматизувати процес оцінювання, зменшити вплив людського фактору та підвищити його швидкість і точність.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота Реанюка О.А. виконана на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя. Зміст дослідження відповідає тематиці науково-дослідних робіт Тернопільського національного технічного університету імені Івана Пулюя, зокрема за темою «Науково-методичні засади цифрової трансформації та сталого розвитку економіки» (№ держреєстрації ВК 75-24).

Оцінка обґрунтованості наукових результатів дисертації їх достовірності та новизни. Наукова новизна результатів дисертаційного дослідження полягає в наступному:

вперше розроблено:

1) метод формалізації якісні вимог стандарту ASVS (Application Security Verification Standard), розробленого та підтримуваного ініціативою OWASP (Open Web Application Security Project), який на відміну від відомих, представляє вимоги у вигляді системи кількісних критеріїв оцінки захищеності, узгоджених з положеннями інших галузевих стандартів, що забезпечило підвищення ефективності процесів контролю та управління безпекою вебдодатків;

2) метод оцінювання захищеності вебдодатків із використанням апарату нечіткої логіки для обробки експертних оцінок вагових коефіцієнтів вимог і критеріїв, що дало змогу врахувати та знизити невизначеність експертних суджень, підвищити об'єктивність процесу оцінювання в умовах неповноти вихідних даних та варіативності архітектурних рішень;

удосконалено:

3) метод вибору множини вимог і критеріїв, який на відміну від відомих, враховує архітектуру, функціональне призначення програмного продукту та ступінь

доступу до документації процесу розробки, що забезпечило універсальність запропонованого підходу для оцінювання рівня захищеності вебдодатків різних типів.

Наукові положення, висновки та рекомендації дисертаційної роботи Ревнюка О. А. є достатньо обґрунтованими завдяки коректному використанню математичного апарату, зокрема апарату теорії нечіткої логіки, і підкріплені ефективною реалізацією інформаційної системи підтримки методу кількісної оцінки рівня захищеності. Їхня доцільність та практична цінність підтверджуються результатами експериментального дослідження, проведеного із використанням тестового додатку, рекомендованого OWASP, що засвідчило відповідність отриманих практичних результатів теоретичним положенням.

Наукові положення та висновки, сформульовані автором у дисертаційній роботі, є достатньо обґрунтованими завдяки комплексному аналізу вебзастосунків як складних багатокомпонентних систем у контексті їх життєвого циклу, ґрунтовному дослідженню чинних міжнародних стандартів та традиційних підходів до тестування безпеки, коректному формулюванню мети й завдань дослідження, застосуванню сучасного наукового інструментарію, а також логічному, аргументованому та послідовному викладенню результатів.

Обґрунтованість і достовірність запропонованого у дисертації методу кількісного оцінювання рівня захищеності вебдодатків підтверджуються результатами експериментальної апробації, застосуванням сучасного математичного апарату та дотриманням вимог міжнародних стандартів у сфері безпеки. Формалізація якісних положень OWASP ASVS у вигляді системи кількісних критеріїв, впровадження механізмів нечіткої логіки для обробки експертних оцінок і реалізація адаптивної процедури вибору релевантних вимог та критеріїв забезпечують методологічну цілісність і практичну релевантність розробленого підходу.

Наукові положення, висновки та рекомендації, сформульовані у роботі, є логічним продовженням отриманих результатів та відзначаються чіткістю формулювання й аргументованістю. Результати верифікації створеної інформаційної системи свідчать про її функціональну коректність, ергономічність інтерфейсу та відповідність поставленим завданням. Таким чином, дисертаційна робота є завершеним дослідженням, результати якого можуть бути рекомендовані для практичного впровадження в системах оцінювання рівня безпеки вебдодатків у контексті сучасних безпекових викликів.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності. Дисертація складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел із 86 найменувань на 10 сторінках та 5 додатків на 13 сторінках. Загальний обсяг дослідження становить 173 сторінки друкованого тексту, з них 133 сторінки основного тексту. Дисертація містить 32 рисунки та 10 таблиць.

У вступі обґрунтовано актуальність теми дисертації, визначено мету, основні завдання, об'єкт і предмет дослідження, сформульовано наукову новизну та практичне значення отриманих результатів. Окреслено зв'язок роботи з науковими програмами і темами, подано відомості про апробацію результатів дослідження та публікації автора.

У першому розділі виконано аналіз структур вебдодатків, їхньої клієнт-серверної взаємодії та впливу моделей SDLC (Waterfall, V-модель, спіральна, інкрементна, RAD) на безпеку. Автором доведено переваги інкрементних моделей для систематичного інтегрування елементів інформаційної безпеки. На основі аналізу відкритих статистичних даних встановлено прямий кореляційний зв'язок між ускладненням архітектури вебсистем та підвищенням рівня потенційних загроз і системних вразливостей.

У другому розділі проаналізовано проблематику суб'єктивності експертних висновків і відсутність стандартизованих кількісних показників для оцінювання рівня безпеки вебзастосунків. Автором вперше представлено методологію кількісного

оцінювання захищеності вебсистем, що ґрунтується на структурному аналізі та селективному використанні критеріїв стандарту OWASP ASVS. Розроблено формалізовану систему критеріїв для відібраних вимог, що забезпечує впорядкований підхід до числового визначення показників безпеки. Описано підхід обчислення вагових коефіцієнтів із застосуванням математичного апарату теорії нечітких множин, що дало змогу зменшити вплив суб'єктивних чинників в експертних оцінках.

У третьому розділі представлено практичну апробацію розробленого методу оцінювання захищеності вебдодатків із використанням тестового середовища рекомендованого OWASP для досліджень та тестування, яке містить попередньо закладені вразливості різного рівня критичності. Результати дослідження дали змогу верифікувати ефективність запропонованого адаптивного підходу до кількісного оцінювання рівня безпеки та підтвердити його відповідність фактичним результатам виявлення критичних вразливостей, отриманим в межах незалежних досліджень.

У четвертому розділі, на основі запропонованого адаптивного методу, розроблено модель інформаційної системи для визначення рівня захищеності вебдодатків. Створено програмний комплекс, що автоматизує процес оцінювання показників безпеки, оптимізує процедуру верифікації відповідності вимогам стандарту OWASP ASVS та забезпечує прозорість і відтворюваність отриманих результатів. Розроблене програмне забезпечення включає механізми конфігурації параметрів оцінювання відповідно до особливостей цільового програмного продукту.

У висновках подано отримані наукові та практичні результати дослідження.

За своїм змістом дисертаційна робота здобувача Ревнюка О.А. повністю відповідає Стандарту вищої освіти зі спеціальності 122 – Комп'ютерні науки для третього (освітньо-наукового) рівня вищої освіти та освітньо-науковій програмі Тернопільського національного технічного університету імені Івана Пулюя «Комп'ютерні науки» за спеціальністю 122 – Комп'ютерні науки. Дисертаційна робота є завершеною науковою працею та свідчить про наявність особистого внеску здобувача у науковий напрям комп'ютерних наук.

Аналізуючи результати перевірки дисертаційної роботи, можна зробити висновок, що дисертаційна робота Ревнюка Олександра Андрійовича є результатом самостійно проведених досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані результати і тексти інших авторів мають належні посилання на відповідні джерела.

Практичне значення отриманих результатів. У результаті роботи над поставленою науково-практичною задачею, автором розроблено інформаційну систему автоматизованого кількісного оцінювання рівня захищеності вебдодатків, яка враховує індивідуальні характеристики програмних проєктів, мінімізує суб'єктивність і невизначеність експертних оцінок шляхом застосування апарату нечіткої логіки, уніфікує процес перевірки відповідності вимогам стандарту OWASP ASVS та формує зрозумілий числовий індикатор захищеності, що може бути використаний для прийняття обґрунтованих управлінських рішень щодо вдосконалення системи безпеки вебдодатків. Реалізація інформаційної системи на основі розроблених автором методів, забезпечує підвищення ступеня поінформованості розробників, архітекторів безпеки, інших представників команд та керівників проєктів щодо реального стану захищеності вебпродуктів та дозволяє оперативно вносити зміни у проєкт підвищуючи ефективність процесу розробки вебдодатків.

Результати дисертаційної роботи впроваджено у: ТОВ "САСДЖЕТ" та у навчальному процесі Тернопільського національного технічного університету імені Івана Пулюя в рамках викладання навчальних дисциплін.

Мова та стиль викладення результатів. Дисертаційну роботу написано українською мовою. Текст викладено логічно, послідовно та доступно для сприйняття, з дотриманням вимог до науково-технічного стилю. Робота характеризується високим технічним рівнем та використанням сучасної фахової термінології. Матеріал супроводжується достатньою кількістю таблиць і рисунків, що сприяє кращому розумінню змісту. Здобувачем застосовано загальноприйняту термінологію предметної галузі.

Дисертаційна робота оформлена відповідно до вимог МОН України від 12 січня 2017 р. №40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи. Основні результати дисертації опубліковані у 9 наукових працях з них 6 статей у фахових наукових журналах України включених на дату опублікування до переліку наукових фахових видань України категорії Б та 3 тези доповідей у матеріалах конференцій.

Також результати дисертації були апробовані на 3 міжнародних науково-технічних конференціях, а саме: IX, X науково-технічна конференція «Інформаційні моделі, системи та технології» (м. Тернопіль, 2021, 2022); XIV міжнародна науково-технічна конференція ITSEC: Безпека інформаційних технологій (м. Тернопіль, 2025).

Опубліковані праці віддзеркалюють повноту викладу результатів дисертаційної роботи. Науковий рівень публікацій – високий. У всіх публікаціях здобувачем дотримано принципів академічної доброчесності.

Таким чином, наукові результати, описані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. У роботі широко використовується термін «вебдодаток» та формулювання на кшталт «типова архітектура вебдодатку» (с. 59). Враховуючи значну різноманітність сучасних вебтехнологій і архітектурних підходів, доцільним є уточнення змісту цих понять у контексті дослідження, а також окреслення меж застосовності запропонованого методу. Крім того, варто було б розглянути особливості використання розроблених підходів щодо різних типів вебдодатків.

2. У описі практичного значення роботи (с. 19) автор стверджує, що розроблена інформаційна система дозволяє зменшити рівень суб'єктивності та невизначеності в процесі експертного оцінювання. Водночас у роботі відсутні кількісні показники або результати порівняльного аналізу, які б дозволили об'єктивно оцінити ефективність запропонованого підходу в цьому аспекті.

3. У розділі 1, на мою думку, недостатньо висвітлено питання автоматизованих засобів аналізу безпекової складової програмних проєктів. Зокрема, варто звернути увагу на можливості платформи GitHub, яка забезпечує широкий спектр інструментів — від аналізу залежностей у проєкті до виявлення вразливостей із використанням баз CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database) та GitHub Security Lab. Інтеграція результатів подібного автоматизованого аналізу могла б підвищити ефективність і обґрунтованість розроблюваного методу.

4. На рисунку 1.3 (с. 30) наведено абсолютну статистику вразливостей сайтів, побудованих на CMS. Для більшої інформативності доцільно було б нормалізувати ці данні, враховуючи розподіл частки ринку між різними CMS.

5. Розділ 2 роботи перевантажений оглядовим матеріалом. Зокрема, підрозділ 2.5.1 містить загальновідомі базові положення теорії нечіткої логіки, які не мають безпосередньої новизни в контексті дослідження. Доцільніше було б обмежитися відповідними літературними посиланнями або, за потреби, винести цей матеріал до додатків.

6. У розділі 2.4 автор акцентує увагу на адаптивній складовій розробленого методу, що дозволяє динамічно коригувати перелік вимог і критеріїв залежно від специфіки оцінюваного програмного проєкту. На підтвердження цього, в розділі 4.1, зокрема на рисунку 4.6 (с.134) подано реалізацію відповідного програмного модуля. Втім, у тексті дисертаційної роботи та інших публікаціях автора дана адаптивна компонента не отримала належної формалізації й деталізованого опису. Зокрема, залишається нез'ясованим характер кореляції між характеристиками проєкту та критеріальною моделлю оцінювання: чи передбачено пряме відображення одного параметра на фіксований набір критеріїв, чи використано іншу, більш складну форму кореляції. Відсутність такого уточнення ускладнює відтворення та верифікацію запропонованого методу.

7. У тексті роботи та на окремих ілюстраціях спостерігається неузгоджене використання термінів українською та англійською мовами. Наприклад, на рисунку

1.6 «Secure Development Lifecycle» усі етапи представлені виключно англійською мовою без перекладу або пояснення в основному тексті. На рисунку 1.7 «Доповнення до Secure Development Lifecycle» частина етапів подана українською, а частина — англійською, що створює термінологічну неузгодженість та ускладнює сприйняття матеріалу.

8. Робота містить деякі неточності у формулах, наприклад, у формулах 12, 13, 15, 16, 17, у першому елементі множин відсутня дужка що відкривається.

9. Деякі рисунки, зокрема 4.8, 4.9 та 4.10, мають надто низьку роздільну здатність і невдалий масштаб, що ускладнює їхнє сприйняття та аналіз.

10. Інтерфейс програмної реалізації запропонованого методу кількісної оцінки захищеності вебдодатків, описаний у розділі 4 дисертаційного дослідження, містить елементи як англійською, так і українською мовами. Зокрема, вимоги та розділи подано англійською, тоді як критерії та пояснення — українською. Така мовна неузгодженість суперечить загальноприйнятим практикам UI/UX-дизайну. Рекомендується забезпечити одномовність інтерфейсу або реалізувати багатомовність, що дозволить користувачеві обирати бажану мову інтерфейсу

11. У тексті роботи трапляються поодинокі граматичні та синтаксичні помилки. Наприклад, спостерігається неузгодженість роду числівника з іменником: на с. 29 — «один з джерел» замість правильного «одне з джерел», на с. 80 — «трьом різних експертам» замість «трьом різним експертам». Крім того, на с. 19 та 107 наявні зайві пробіли.

Однак, зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

Висновок про дисертаційну роботу. Вважаю, що дисертаційна робота здобувача наукового ступеня доктора філософії Ревнюка Олександра Андрійовича на тему «Розробка інформаційної системи оцінювання якості захисту вебдодатків» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеним, цілісним та самостійно виконаним науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує

наукове завдання, що має істотне значення для комп'ютерних наук. Дисертаційна робота за актуальністю теми, практичною цінністю і науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п. 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 р. № 44 (зі змінам, внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022 р., №502 від 19.05.2023 р., №507 від 03.05.2024 р.).

Здобувач Ревнюк Олександр Андрійович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент:
доцент кафедри комп'ютерної інженерії та інформаційних систем
Хмельницького національного університету,
кандидат технічних наук, доцент Д.М. Медзатий

«Підпис Медзатого Д.М. засвідчую»
Проректор з наукової-педагогічної роботи
Хмельницького національного університету В.Г. Лопатовський