Голові разової спеціалізованої вченої ради
Тернопільського національного
технічного університету імені Івана Пулюя
д.т.н., професору
Пастуху Олегу Анатолійовичу

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
доктора технічних наук, професора
Опірського Івана Романовича на дисертаційну роботу
Ревнюка Олександра Андрійовича,
«Розробка інформаційної системи оцінювання якості
захисту вебдодатків», подану до захисту на здобуття
наукового ступеня **доктора філософії** з галузі знань 12
«Інформаційні технології», спеціальності 122
«Комп'ютерні науки»

1. Актуальність теми дисертаційної роботи

Розвиток вебтехнологій та їх широке впровадження у всі сфери життєдіяльності суспільства стає ключовим фактором цифровізації економіки, покращення якості надання послуг та забезпечення ефективності бізнес-процесів. Вебдодатки, які охоплюють електронну комерцію, державні сервіси, фінансові системи та соціальні мережі, стали невід'ємною частиною сучасної інформаційної інфраструктури. Це особливо важливо в контексті прагнення України до цифровізації та автоматизації управління, оптимізації ресурсів та підвищення загальної якості надання послуг громадянам та бізнесу. Інтеграція інформаційних та комунікаційних технологій у процеси надання вебсервісів дає змогу гнучко реагувати на виклики, зумовлені кіберзагрозами, технологічними змінами або іншими надзвичайними ситуаціями, що підвищує стійкість цифрової інфраструктури. Автоматизація процесів виявлення вразливостей та використання великих за обсягом даних можуть значно підвищити ефективність системи захисту, оптимізувати споживання ресурсів безпеки, забезпечити ефективніший моніторинг стану захищеності вебзастосунків.

Розробка методів кількісного оцінювання захищеності вебзастосунків відіграє ключову роль у підвищенні ефективності, безпеки та стійкості цифрових середовищ. Вони надають можливості реалізувати високий рівень автоматизації, стандартизації та ефективності управління процесами забезпечення кібербезпеки. Проте на даний час немає загальноприйнятих підходів до формування уніфікованих метрик та методів комплексної оцінки рівня безпеки вебдодатків як цілісних систем, оцінювання показників їх впровадження в умовах різноманітності архітектурних рішень.

Все це зумовлює актуальність теми дисертаційної роботи Ревнюка Олександра Андрійовича, присвяченої розв'язанню задачі розроблення методів, засобів та підходів до кількісного оцінювання захищеності вебзастосунків та відомих методів виявлення вразливостей.

2. Зв'язок роботи з науковими програмами, темами

Дисертаційна робота Ревнюка О.А. виконана на кафедрі комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя. Дослідження, результати яких викладено в дисертації, виконано відповідно до пріоритетних напрямів науково-дослідних робіт Тернопільського національного технічного університету імені Івана Пулюя, в рамках виконання науково-дослідних робіт за темою «Науково-методичні засади цифрової трансформації та сталого розвитку економіки» (№ держреєстрації ВК 75-24).

3. Наукова новизна результатів дисертаційної роботи

Отримані наукові результати є розв'язком задачі розроблення методів, засобів та інструментів для кількісного оцінювання захищеності вебзастосунків.

При цьому автором вперше формалізовано якісні вимоги стандарту OWASP ASVS у вигляді системи кількісних критеріїв оцінки захищеності, узгоджених з іншими галузевими стандартами, що дає змогу підвищити ефективність контролю та управління комплексною безпекою вебдодатків.

Автором вперше обґрунтовано адаптивну процедуру вибору множини вимог та критеріїв в залежності від архітектури, функціональності продукту та доступу до документації процесу розробки вебдодатку, що дало можливість забезпечити універсальність підходу для оцінювання рівня захищеності вебдодатків різних типів та конфігурацій.

Вперше запропоновано метод оцінювання захищеності вебзастосунків з використанням системи нечіткої логіки для опрацювання експертних оцінок коефіцієнтів важливості вимог та критеріїв, що дало змогу врахувати невизначеність суджень експертів та забезпечити об'єктивність процесу оцінювання в умовах неповноти вихідних даних та різноманітності архітектурних рішень вебдодатків.

4. Короткий аналіз основного змісту дисертації

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

У першому розділі «Аналіз сучасних вебдодатків як багатокомпонентних систем у контексті життєвого циклу розробки програмного забезпечення» здійснено дослідження сучасних веб-застосунків як складних багатокомпонентних архітектур в рамках процесів створення програмного забезпечення. Виконано детальне порівняння традиційних та ітеративних підходів до розробки ПЗ, що дало можливість ідентифікувати ключові обмеження класичних методологій та обґрунтувати переваги інкрементальних моделей для систематичного інтегрування принципів інформаційної безпеки. Проаналізовано відкриті статистичні дані, які засвідчили прямий кореляційний зв'язок між ускладненням архітектури вебсистем та зростанням числа потенційних загроз безпеці й системних уразливостей.

У другому розділі «Розроблення адаптивного методу кількісної оцінки

захищеності вебдодатків» проаналізовано проблематику суб'єктивного характеру експертних висновків та брак стандартизованих кількісних показників при оцінюванні рівня безпеки веб-застосунків. Автором вперше представлено методологію кількісного оцінювання захищеності веб-систем, яка базується на структурному аналізі та селективному використанні критеріїв стандарту OWASP ASVS. Розроблено формалізовану систему критеріїв для відібраних вимог, що забезпечило створення упорядкованого підходу до числового визначення показників безпеки. Впровадження математичного апарату теорії нечітких множин для обчислення вагових коефіцієнтів дозволило зменшити вплив суб'єктивного фактора в експертних оцінках та покращити достовірність результатів аналізу.

У третьому розділі «Експериментальне дослідження рівня безпеки вебдодатку з використанням розробленого адаптивного методу» здійснено практичну апробацію методики оцінювання безпеки веб-систем на базі тестового середовища "OWASP Juice Shop", що містить заздалегідь закладені уразливості різного рівня критичності. Проведене експериментальне дослідження дозволило верифікувати ефективність запропонованого адаптивного підходу до кількісного оцінювання захищеності та підтвердити його відповідність результатам виявлення критичних вразливостей, отриманим в рамках незалежних досліджень. Отримано подальший розвиток теоретичних основ використання математичного апарату нечіткої логіки для підвищення об'єктивності та точності експертного визначення вагових коефіцієнтів при оцінюванні параметрів безпеки.

У четвертому розділі «Проєктування та розробка інформаційної системи кількісного оцінювання рівня захищеності вебдодатків» на базі створеного адаптивного методу розроблено архітектурну та логічну структуру інформаційної системи для кількісного визначення рівня захищеності веб-застосунків. Створено програмний комплекс для автоматизованого оцінювання показників безпеки, який оптимізує процедуру верифікації відповідності критеріям стандарту OWASP ASVS та гарантує транспарентність і reproducibility отриманих результатів. Система забезпечує можливість налаштування параметрів оцінювання відповідно до

специфічних вимог конкретних веб-додатків, що підвищує гнучкість та практичну застосовність розробленого підходу.

Проаналізувавши отримані експериментальні результати можна зробити висновок, що було досягнуто основні поставлені задачі дисертаційного дослідження.

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

Наукові положення, висновки і рекомендації дисертаційної роботи достатньо обґрунтовані коректним використанням математичного апарату нечіткої логіки, підкріплені ефективною реалізацією інформаційної системи підтримки методу визначення кількісної оцінки безпеки, успішним практичним впровадженням результатів дисертаційних досліджень через експериментальне дослідження на прикладі "OWASP Juice Shop", що продемонструвало відповідність теоретичних досліджень реальним результатам.

Обґрунтованість сформульованих у дисертаційній роботі наукових положень та висновків є достатньою. Вона базується на детальному аналізі вебдодатків як складних багатокомпонентних систем та їх життєвого циклу розробки, дослідженні існуючих міжнародних стандартів та традиційних методів тестування безпеки, чіткій постановці задач дослідження, використанні сучасних дослідницьких методів, обґрунтованому, аргументативному та якісному формулюванні висновків.

Достовірність та обґрунтованість запропонованого методу кількісного оцінювання рівня захищеності вебдодатків з урахуванням вимог міжнародних галузевих стандартів підтверджується результатами експериментальних досліджень і коректним застосуванням наукових підходів. Зокрема, формалізація якісних вимог стандарту OWASP ASVS у вигляді системи кількісних критеріїв, використання апарату нечіткої логіки для опрацювання експертних оцінок коефіцієнтів важливості, а також адаптивна процедура вибору множини вимог та

критеріїв забезпечують математично обґрунтовану основу для кількісного вимірювання безпекових параметрів.

Сформульовані в дисертаційній роботі наукові положення, висновки та рекомендації логічно випливають з отриманих результатів, що сформульовані за допомогою чітких та лаконічних трактувань. Верифікація розробленої інформаційної системи підтвердила коректність її функціонування та зручність користування. Тому можна стверджувати, що отримані у роботі висновки та практичні рішення коректні, достатньо обґрунтовані й можуть бути рекомендовані при формуванні систем оцінювання рівня захищеності вебдодатків в умовах сучасних загроз кібербезпеки.

6. Практичні результати роботи

Практичне значення одержаних результатів полягає, перш за все, у доведенні отриманих наукових результатів до конкретних методів, програмно-алгоритмічних комплексів та інформаційно-технологічних інструментів для реалізації системи кількісного оцінювання рівня захищеності вебдодатків. На основі яких було сформовано інформаційну систему для автоматизації запропонованого адаптивного методу з модульним розділенням функціональних компонентів та розроблено програмно-алгоритмічний комплекс для кількісного оцінювання показників захищеності вебдодатків відповідно до стандарту OWASP ASVS, що забезпечує підвищення ступеня поінформованості розробників, архітекторів безпеки, представників DevSecOps команд та керівників проєктів щодо реального стану захищеності вебпродуктів.

Використання розроблених методів дало змогу створити комплексну інформаційну систему для автоматизації процесів кількісного оцінювання рівня захищеності вебдодатків, що враховує індивідуальні характеристики проєктів, мінімізує суб'єктивність та невизначеність експертних оцінок через застосування апарату нечіткої логіки, уніфікує перевірку відповідності вебдодатку вимогам стандарту OWASP ASVS та надає зрозумілий числовий індикатор захищеності для

прийняття обґрунтованих управлінських рішень щодо вдосконалення системи захисту вебдодатків.

Результати дисертаційного дослідження знайшли практичне застосування в освітній діяльності Тернопільського національного технічного університету імені Івана Пулюя в рамках викладання навчальних дисциплін на двох кафедрах. Наукові розробки автора було впроваджено для забезпечення процедур внутрішнього аудиту інформаційної безпеки, покращення якості захисту веб-продуктів та оптимізації інтеграції безпекових вимог у життєвий цикл розробки програмного забезпечення (SDLC) в ТОВ "SaaSJet", що засвідчує практичну значущість та готовність розроблених методологій і інструментів до реального використання в промислових умовах.

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

Структура дисертаційної роботи включає вступну частину, чотири основні розділи, заключні висновки, бібліографію та додаткові матеріали. Загальний обсяг дослідження становить 173 сторінки, з яких безпосередньо основний зміст викладено на 133 сторінках. Бібліографічний список налічує 86 позицій. Робота оформлена згідно з усіма встановленими стандартами.

Дисертаційна робота має логічну та зв'язну структуру. Основні висновки і рекомендації логічно витікають з поданих у розділах роботи результатів. Список використаних джерел є репрезентативним та містить сучасні джерела, що відповідають предметній області дослідження.

Отримані результати дисертаційного дослідження свідчать про високу індивідуальність роботи. По всьому тексту дисертації простежується авторський стиль. У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без вказання посилань на відповідні джерела. Використання матеріалів інших дослідників здійснено з дотриманням вимог

наукової етики та містить належні посилання на відповідні джерела.

Результати дисертаційного дослідження висвітлено у 9 наукових публікаціях, з яких 6 статей надруковано у фахових наукових виданнях України та 3 матеріали представлено на конференціях міжнародного рівня. За кількісними та якісними показниками наукових публікацій дисертаційна робота цілком задовольняє критерії "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії". Ключові наукові положення дисертації адекватно представлено в опублікованих наукових працях автора.

Оприлюднення наукових результатів дисертанта у рецензованих наукових виданнях, що здійснюють контроль матеріалів на предмет відсутності неправомірних запозичень, є додатковим свідченням дотримання норм академічної доброчесності. За підсумками аналізу дисертаційної роботи Ревнюка О.А. фактів порушення академічної доброчесності не виявлено. Забезпечено дотримання критеріїв щодо кількісних та якісних показників публікацій.

8. Мова та стиль дисертаційної роботи

Дисертація написана логічно, доступно та зв'язно на високому фаховому рівні з використанням сучасної термінології предметної області кібербезпеки та оцінювання захищеності вебдодатків. Мова роботи є науковою, точною та зрозумілою. Викладення матеріалу характеризується послідовністю та структурованістю, що забезпечує належне сприйняття наукових результатів.

Тема, зміст та отримані наукові результати дисертаційної роботи повністю відповідають спеціальності 122 "Комп'ютерні науки", галузі знань 12 "Інформаційні технології".

9. Зауваження до дисертації:

1. У розділі 3.1.4 (стор. 118–119) автор порівнює запропонований метод із комерційними рішеннями, такими як Nessus та Acunetix, що згадуються на стор.

46 та 119. Проте аналіз обмежується загальними твердженнями, наприклад, що «більшість сканерів не зафіксували критичних вразливостей» (стор. 119), без детального розбору їхніх характеристик, таких як покриття вразливостей чи час виконання. Бажано б було доповнити порівняльний аналіз конкретними метриками, такими як типи виявлених вразливостей, точність чи швидкість роботи інструментів порівняно з авторським методом. Це підвищило б переконливість тверджень про переваги розробленої системи.

2. У розділі 4 (стор. 127–148), присвяченому практичній реалізації системи, описано архітектуру та функціонал (рис. 4.1, стор. 129), але не розглядається, як система справляється з обробкою великих вебдодатків чи одночасною роботою кількох користувачів. Наприклад, на стор. 136–137 згадується інтерфейс для оцінки проєктів, але немає даних про поведінку системи при збільшенні кількості вимог чи проєктів. Варто було б представити тестування продуктивності системи, наприклад, при обробці проєктів із тисячами вимог або при паралельній роботі кількох користувачів, що підтвердило б її застосовність у реальних умовах.

3. Робота базується на стандарті OWASP ASVS, але не враховує інші сучасні стандарти, такі як NIST SP 800-53 чи ISO/IEC 27002, які згадуються лише частково (наприклад, NIST SP 800-63B на стор. 61), що обмежує широту застосовності методу. Варто було б доповнити методологічну основу аналізом відповідності розробленої системи іншим стандартам безпеки, таким як ISO/IEC 27002, для забезпечення ширшої сумісності з міжнародними вимогами. Інтеграція додаткових стандартів підвищила б універсальність системи та її привабливість для організацій, які використовують різні стандарти безпеки.

4. У розділі 3 (стор. 93–119) для верифікації методу використано OWASP Juice Shop, яке є навчальним ресурсом із навмисно введеними вразливостями. Автор не зазначає, що це обмежує узагальнення результатів на реальні вебдодатки, де вразливості можуть бути менш очевидними. Використання лише навчального середовища знижує достовірність висновків про ефективність методу в реальних

умовах, що може викликати сумніви в його практичній застосовності для комерційних проєктів.

5. У розділі 2.3 (стор. 59–77) автор розробляє критерії оцінки вимог безпеки, використовуючи трирівневу шкалу (наприклад, критерій №4 на стор. 66–67). Проте не надано чіткого пояснення, чому обрано саме три рівні (0, 0,5, 1 бал), і як вони відображають реальні загрози чи критичність вимог. Відсутність обґрунтування шкали оцінки послаблює методологічну основу роботи, що може ускладнити відтворюваність результатів та їхню інтерпретацію іншими дослідниками чи практиками.

6. У роботі автор згадує організаційні аспекти, наприклад, інформування користувачів про зміну пароля (стор. 72), проте у роботі бракує аналізу процедурних факторів, таких як навчання персоналу чи реагування на інциденти, які є важливими для комплексної оцінки безпеки вебдодатків. Недостатня увага до організаційних аспектів обмежує цілісність запропонованого підходу, оскільки безпека залежить не лише від технічних заходів, а й від людських і процедурних факторів, що може призвести до недооцінки ризиків.

Наведені зауваження і дискусійні моменти вказують на деякі суперечливі аспекти дослідження, проте загалом вони засвідчують складність і багатогранність обраної теми, її практичну важливість та актуальність і суттєво не впливають на якісні характеристики дисертаційної роботи.

Висновок щодо дисертації в цілому

Дисертаційна робота Ревнюка Олександра Андрійовича «Розробка інформаційної системи оцінювання якості захисту вебдодатків» представляє собою завершену кваліфікаційну науково-дослідну працю, що включає нові теоретично обґрунтовані результати. У дисертації вирішено важливу науково-практичну проблему створення методології кількісного визначення рівня безпеки вебзастосунків та розроблення відповідного програмного комплексу для автоматизованого оцінювання захищеності.

Отримані наукові та практичні результати мають суттєве значення для розвитку галузі інформаційних технологій загалом та комп'ютерних наук зокрема. Тематика та зміст дисертаційного дослідження повністю відповідають профілю спеціальності 122 — "Комп'ютерні науки".

Отже, з урахуванням актуальності досліджуваної проблематики, наукової обґрунтованості теоретичних положень, висновків та практичних рекомендацій, викладених у дисертаційній роботі, їх інноваційного характеру та прикладного значення, адекватності представлення результатів дослідження у фахових публікаціях, дотримання норм академічної доброчесності, констатую, що дисертація повністю задовольняє критерії Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. No 44, які встановлюються для дисертаційних досліджень на здобуття наукового ступеня доктор філософії. Автор дисертації, Ревнюк Олександр Андрійович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 — "Комп'ютерні науки", галузь знань 12 «Інформаційні технології».

Офіційний опонент:
доктор технічних наук, професор,
завідувач кафедри захисту інформації
Національного університету
«Львівська політехніка» Іван ОПІРСЬКИЙ

Підпис д.т.н., професора Опірського І.Р. засвідчую
Проректор Національного університету
«Львівська політехніка» Роман ФЕДОРИШИН