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

РЕЦЕНЗІЯ

кандидата технічних наук, доцента **Яцишина Василя Володимировича**
на дисертаційну роботу **Ревнюка Олександра Андрійовича**
«Розробка інформаційної системи оцінювання якості захисту вебдодатків»,
подану до захисту на здобуття
наукового ступеня доктора філософії в галузі знань 12 «Інформаційні технології»
зі спеціальності 122 «Комп'ютерні науки»

Актуальність теми дисертаційної роботи та зв'язок з науковими напрямками, темами.

Вебдодатки сьогодні стали критично важливими для функціонування організацій різних сфер діяльності: від електронної комерції до державних сервісів і соціальних мереж. Вебтехнології забезпечують основу для ведення бізнесу, надання послуг та взаємодії з користувачами. Однак інтенсивний розвиток вебтехнологій супроводжується пропорційним зростанням кіберзагроз, що актуалізує потребу у розробці нових, ефективних методів забезпечення захищеності вебдодатків.

Особливу увагу привертає той факт, що незважаючи на значний прогрес у створенні автоматизованих засобів виявлення вразливостей та формування галузевих стандартів безпеки (OWASP, NIST, SANS), у сфері забезпечення захищеності вебдодатків спостерігається критична прогалина. Існуючі системи сканування безпеки, хоча й здатні виявляти широкий спектр вразливостей, демонструють істотні обмеження у верифікації критичних параметрів захисту та не забезпечують уніфікованих методів кількісної оцінки рівня захищеності вебдодатків як цілісних систем.

Актуальність дисертаційної роботи Ревнюка Олександра Андрійовича обумовлена існуючим парадоксом сучасного стану інформаційної безпеки: наявність потужних технологій виявлення вразливостей при відсутності науково обґрунтованих методів комплексної оцінки рівня безпеки вебдодатків та кількісних метрик оцінювання.

Відсутність стандартизованої системи обчислення ступеня захищеності вебдодатків суттєво ускладнює ідентифікацію потенційних векторів компрометації та розробку ефективних рішень для покращення рівня захисту.

Тема дисертаційної роботи Ревнюка О.А. відповідає окремим елементам фокусу освітньої програми “Комп’ютерні науки” для третього рівня освіти Тернопільського національного технічного університету імені Івана Пулюя. Дослідження виконано в рамках науково-дослідної роботи, що підтверджує її відповідність стратегічним напрямкам розвитку науки та практичним потребам забезпечення кібербезпеки. Розробка науково-обґрунтованого підходу до кількісного оцінювання захищеності вебзастосунків на основі галузевих стандартів та відомих методів виявлення вразливостей є актуальною науковою задачею, вирішення якої сприятиме підвищенню рівня захищеності критично важливих інформаційних систем.

Наукова новизна результатів дисертаційної роботи.

У дисертаційній роботі Ревнюка О.А. отримано такі основні наукові результати в рамках розробленого нового методу кількісного оцінювання безпеки вебдодатку:

– уперше формалізовано якісні вимоги стандарту OWASP Application Security Verification Standard (ASVS) у вигляді системи кількісних критеріїв оцінки захищеності, узгоджених з іншими галузевими стандартами, що дає змогу підвищити ефективність контролю та управління комплексною безпекою вебдодатків і забезпечує можливість об'єктивного порівняння рівня захищеності різних вебдодатків.

– уперше обґрунтовано адаптивну процедуру вибору множини вимог та критеріїв в залежності від архітектури, функціональності продукту та доступу до документації процесу розробки вебдодатку, що на відміну від статичних методів оцінювання дало можливість забезпечити універсальність підходу для оцінювання рівня захищеності вебдодатків різних типів і призначень.

– уперше запропоновано систему нечіткої логіки при опрацюванні експертних оцінок коефіцієнтів важливості вимог та критеріїв захищеності вебдодатків, що дає змогу врахувати невизначеність суджень експертів та забезпечити об'єктивність процесу оцінювання у порівнянні з традиційними експертними технологіями.

Практична цінність одержаних результатів.

Використання розроблених методів дало змогу програмно реалізувати комплексну інформаційну систему для автоматизації процесів кількісного оцінювання рівня захищеності вебдодатків. Застосування адаптивного методу кількісного оцінювання забезпечило можливість враховувати індивідуальні характеристики проєктів, мінімізувати суб'єктивність та невизначеність експертних оцінок через застосування апарату нечіткої логіки. Програмно реалізована інформаційна система забезпечує автоматизацію уніфікованої процедури перевірки відповідності вебдодатку вимогам стандарту OWASP ASVS та надає зрозумілий числовий індикатор захищеності. Це дає змогу приймати обґрунтовані управлінські рішення щодо вдосконалення системи захисту вебдодатків.

Результати дисертаційної роботи впроваджені: в Тернопільському національному технічному університету імені Івана Пулюя у навчальному процесі двох кафедр; для супроводу процесів внутрішнього аудиту безпеки, підвищення якості захисту вебпродуктів компанії та оптимізації процесів інтеграції вимог безпеки в життєвий цикл розробки (SDLC) в ТОВ “SaaSJet”.

Повнота викладу наукових положень та результатів в опублікованих працях, дотримання вимог академічної доброчесності.

Результати дисертаційного дослідження представлено у 9 наукових публікаціях, серед яких 6 статей опубліковано у наукових фахових виданнях України та 3 матеріали конференцій українського та міжнародного рівня. За кількістю та якістю наукових публікацій дисертаційна робота повністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії».

Публікація наукових результатів дисертанта у рецензованих виданнях, які здійснюють перевірку матеріалів на відсутність неправомірних запозичень, служить додатковим підтвердженням дотримання принципів академічної доброчесності. Використання у дисертаційній роботі результатів досліджень інших авторів здійснено з дотриманням вимог наукової етики та містить коректні посилання на відповідні джерела.

За результатами аналізу дисертаційної роботи Ревнюка О.А. порушень академічної доброчесності не встановлено.

Ступінь обґрунтованості та достовірність сформульованих в дисертації наукових положень, висновків і рекомендацій.

Наукові положення, висновки і рекомендації, представлені в дисертаційній роботі Ревнюка О.А., характеризуються високим рівнем обґрунтованості та достовірності. Це підтверджується практичним впровадженням отриманих результатів, що засвідчено відповідними актами впровадження, а також апробацією матеріалів дослідження на міжнародних наукових, науково-практичних та науково-технічних конференціях, де вони отримали схвальні відгуки наукової спільноти. Додатковим підтвердженням якості проведеного дослідження є позитивна оцінка результатів роботи під час їх обговорення на наукових семінарах кафедри комп'ютерних наук, що свідчить про їх науковий і практичний потенціал.

Оцінка змісту дисертації.

Дисертація складається з вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота викладена на 173 сторінках, включаючи 133 сторінки основного тексту. Перелік використаних джерел містить 86 найменувань.

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, зазначено зв'язок з науковими напрямками та програмами, сформульовані мета і завдання дослідження, об'єкт та предмет дослідження, викладені наукова новизна та практичне значення отриманих дисертантом результатів, подано дані про особистий внесок здобувача, апробацію наукових результатів та публікації.

У **першому розділі** проведено аналіз сучасних вебдодатків як багатокомпонентних систем у контексті життєвого циклу розробки програмного забезпечення. Здійснено порівняльний аналіз класичних та ітеративних моделей життєвого циклу ПЗ, що дало змогу виявити принципові обмеження лінійних моделей життєвого циклу та встановити переваги ітеративних підходів для безперервної інтеграції безпекових практик. Обґрунтовано доцільність і перспективність дослідження та імплементації методів кількісної оцінки захищеності вебдодатків з урахуванням їх індивідуальних характеристик.

У **другому розділі** досліджено проблему суб'єктивності експертних оцінок та відсутності уніфікованих кількісних метрик у задачах оцінювання безпеки вебдодатків. Автором уперше запропоновано метод кількісного оцінювання захищеності вебдодатків на основі структурного аналізу та адаптивного відбору вимог

стандарту OWASP ASVS. Для формалізації відібраних вимог розроблено систему критеріїв оцінювання, що дало змогу створити систематизований підхід до кількісного вимірювання рівня безпеки.

У **третьому розділі** проведено експериментальне дослідження рівня безпеки вебдодатку на прикладі спеціалізованого навчального середовища з попередньо вбудованими вразливостями. Це дало змогу на практиці оцінити розроблений адаптивний метод кількісної оцінки захищеності. Отримала подальший розвиток концепція використання апарату нечіткої логіки для підвищення точності та об'єктивності експертного оцінювання вагових коефіцієнтів.

У **четвертому розділі** на основі розробленого адаптивного методу спроєктовано архітектурну та логічну модель інформаційної системи кількісного оцінювання рівня захищеності вебдодатків. Розроблено інформаційну систему кількісної оцінки безпеки, яка спрощує процес перевірки на відповідність стандарту OWASP ASVS та забезпечує прозорість і відтворюваність результатів з можливістю адаптації параметрів оцінювання.

Висновки, отримані у дисертаційній роботі, підкреслюють та фокусують увагу на результатах наукової новизни та практичної цінності проведених досліджень. Дисертація містить ґрунтовний критичний аналіз сучасного стану наукових досліджень, які опубліковані провідними вітчизняними та закордонними вченими, про що свідчить перелік використаних джерел і посилання на них у тексті дисертації. Усі теоретичні та практичні положення дисертаційної роботи опубліковані у фахових наукових виданнях та апробовані на наукових і науково-практичних конференціях.

У **додатках** до дисертаційної роботи подано список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертаційної роботи, акти впровадження результатів дослідження, а також список відібраних вимог стандарту OWASP ASVS, що використовувались у розробленому методі оцінювання захищеності вебдодатків.

Відповідність дисертаційної роботи вимогам МОН України.

Дисертаційний матеріал представлено у логічній послідовності, із дотриманням структурованості та обґрунтованості викладу. Кожен із чотирьох розділів роботи має власні особливості, проте всі вони органічно взаємопов'язані, що демонструє цілісність та завершеність наукового дослідження.

Автор використовує оригінальний стиль подання матеріалу, а сформульовані висновки та пропозиції є логічним продовженням результатів, викладених у відповідних розділах. Дисертація є завершеним науковим дослідженням та використовує фахову термінологію галузі знань 12 «Інформаційні технології». Структура роботи, її зміст, послідовність викладу та повнота вирішених завдань цілком відповідають заявленій темі дослідження.

Тематика, зміст та наукові результати дисертаційної роботи Ревнюка О.А. відповідають вимогам спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Зауваження до дисертації:

1. У першому розділі дисертаційної роботи доцільно провести аналіз стандарту «ДСТУ ISO/IEC 25010:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Моделі якості системи та програмних засобів (ISO/IEC 25010:2011, IDT)» та визначити потенційні шляхи застосування його рекомендацій при оцінюванні вразливостей вебдодатків, зокрема характеристики захищеність з набором підхарактеристик: конфіденційність, цілісність, безвідмовність, обліковність та автентичність.

2. У роботі дисертантом запропоновано уніфіковану шкалу на основі принципу триточкової градації з кроком 0.5, що в недостатньому обсязі забезпечує гнучкість та інтерпретацію результатів оцінювання.

3. У роботі не запропоновано механізму та процедури комплексної інтегральної оцінки захищеності вебдодатків, а лише за окремими критеріями.

4. При визначенні вагових коефіцієнтів важливості критеріїв захищеності вебдодатків до запропонованої автором системи нечіткої логіки доцільно було б додати, наприклад, метод попарного порівняння Сааті чи алгоритму простого вибору, що дозволило б додатково знизити вплив суб’єктивного фактору кожного з експертів, які беруть участь в оцінюванні.

5. При практичній реалізації інформаційної системи оцінювання якості захисту веб-додатків недостатньо уваги приділено обґрунтуванню вибору типу бази даних, не в повному обсязі наведено опис структури бази даних на рівні полів таблиці та не зазначено до якої нормальної форми приведено базу даних.

6. У роботі чітко не представлено результати і критерії тестування розробленої інформаційної системи щодо визначення рівня коректності її функціонування та зручності використання.

7. У роботі варто було б навести порівняльну характеристику кількісних показників затрат часу експертів при використанні запропонованої методики і традиційного експертного оцінювання.

Варто відмітити, що зазначені зауваження не впливають на загальну позитивну оцінку одержаних наукових і практичних результатів дослідження.

Висновки щодо дисертації в цілому:

1. Дисертаційна робота Ревнюка Олександра Андрійовича на тему: «Розробка інформаційної системи оцінювання якості захисту вебдодатків» є завершеною кваліфікаційною науковою працею, у якій розв'язано важливу науково-практичну задачу імплементації методу кількісного оцінювання безпеки вебдодатків, що було покладено в основу спроєктованої інформаційної системи.

2. За темою та змістом дисертаційна робота відповідає спеціальності 122 «Комп'ютерні науки».

3. Вважаю, що дисертаційна робота "Розробка інформаційної системи оцінювання якості захисту вебдодатків" відповідає чинним вимогам наказу МОН України №40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертацій» із змінами, внесеними згідно з Наказом Міністерства освіти і науки № 759 від 31.05.2019 р., та 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 № 44 від 12 січня 2022 р., а її автор, Ревнюк Олександр Андрійович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», галузь знань 12 «Інформаційні технології».

ВІДДІЛ КАДРІВ 05408102

Підпис В.В. Яцишина
засвідчую:
Начальник відділу кадрів О. Лунєва

Рецензент — кандидат технічних наук,
доцент, зав. кафедри систем штучного інтелекту
та аналізу даних Тернопільського національного
технічного університету імені Івана Пулюя В.В. Яцишин