Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії РЕВНЮК Олександр Андрійович 1997 року народження, громадянин України, освіта вища: закінчив у 2020 році Тернопільський національний технічний університет імені Івана Пулюя за спеціальністю Кібербезпека, Міністерство освіти і науки України, м. Тернопіль, виконав акредитовану освітньо-наукову програму Комп'ютерні науки.

Разова спеціалізована вчена рада, утворена наказом ректора Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України, м. Тернопіль, від 23 червня 2025 року № 4/7-574 у складі:

Голови разової
спеціалізованої вченої ради – Олега ПАСТУХА, доктора технічних наук, професора, професора кафедри програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя;

Рецензентів – Марини ДЕРКАЧ, кандидатки технічних наук, доцентки, доцентки кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя;

Василя ЯЦИШИНА, кандидата технічних наук, доцента, завідувача кафедри систем штучного інтелекту та аналізу даних Тернопільського національного технічного університету імені Івана Пулюя;

Офіційних опонентів – Івана ОПІРСЬКОГО, доктора технічних наук, професора, завідувача кафедри захисту інформації Національного університету «Львівська політехніка»;

Дмитра МЕДЗАТОГО, кандидата технічних наук, доцента, доцента кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету,

на засіданні 13 серпня 2025 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології

Олександру РЕВНЮКУ

на підставі публічного захисту дисертації «Розробка інформаційної системи оцінювання якості захисту вебдодатків» за спеціальністю 122 Комп'ютерні науки.

Дисертацію виконано у Тернопільському національному технічному університеті імені Івана Пулюя, Міністерство освіти і науки України, м. Тернопіль.

Науковий керівник: Наталія ЗАГОРОДНА, кандидатка технічних наук, доцентка, завідувачка кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя.

Дисертацію подано у вигляді спеціально підготовленого рукопису, який містить нові науково обґрунтовані результати проведених здобувачем досліджень щодо інформаційної системи, що формалізує розроблені технології кількісного оцінювання рівня захищеності вебдодатку з урахуванням вимог галузевих стандартів, експертних оцінок, життєвого циклу розробки, специфіки функціоналу та архітектури.

Дисертаційну роботу виконано відповідно до напрямку науково-дослідних робіт Тернопільського національного технічного університету імені Івана Пулюя, а саме: науково-дослідної теми «Науково-методичні засади цифрової трансформації та сталого розвитку економіки» (№ державної реєстрації ВК 75-24).

Наукова новизна полягає в розробці нового методу кількісного оцінювання безпеки вебдодатку, покладеного в основу спроєктованої інформаційної системи.

Наукова новизна дисертаційного дослідження відображена у таких результатах:

– *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;

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;

запропоновано використання системи нечіткої логіки для опрацювання експертних оцінок коефіцієнтів важливості вимог та критеріїв, що дає змогу врахувати невизначеність суджень експертів та забезпечити об'єктивність процесу оцінювання.

Дисертація виконана державною мовою та оформлена згідно вимог, встановлених МОН. Дисертаційна робота викладена на 173 сторінках. Текст основної частини дисертації становить 6,1 авторських аркуша.

Результати дисертаційного дослідження висвітлено у 6 наукових працях, опублікованих у наукових фахових періодичних виданнях України:

1. Revniuk O. A., Zagorodna N. V., Kozak R. O., Karpinski M. P., Flud L. O. The improvement of web-application SDL process to prevent Insecure Design vulnerabilities. *Applied Aspects of Information Technology*. 2024. Vol. 7, № 2. P. 162–174. ISSN 2617-4316. DOI: https://doi.org/10.15276/aait.07.2024.12.

2. Ревнюк О., Постолюк А. Дослідження застосування адаптивних методик оцінювання ризиків безпеки для веб-додатків. *Computer Systems and Information Technologies*. 2024. № 3. С. 34–43. ISSN 2710-0766. DOI: https://doi.org/10.31891/csit-2024-3-5.

3. Ревнюк О. А., Загородна Н. В. Методологія кількісної оцінки захищеності веб-додатку електронної комерції на етапі експлуатації. *Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas*. 2024. № 2(57). С. 107–119. ISSN 1993-9965. DOI: https://doi.org/10.31471/1993-9965-2024-2(57)-107-119.

4. Revniuk O., Zagorodna N., Ulichev O. Adaptive methodology for computing the quantitative Security status indicator of web applications. *Central Ukrainian Scientific Bulletin Technical Sciences*. 2024. № 2(10). P. 3–10. ISSN 2664-262X. DOI: https://doi.org/10.32515/2664-262x.2024.10(41).2.3-10.

5. Ulichev O., Papizh L., Revniuk O. Advancements in software Testing: a scientific perspective. *Central Ukrainian Scientific Bulletin Technical Sciences*. 2024. № 1(10). P. 3–16. ISSN 2664-262X. DOI: https://doi.org/10.32515/2664-262x.2024.10(41).1.3-16.

6. Revniuk O., Zagorodna N., Kozak R., Yavorskyy B. I. Development of an information system for the quantitative assessment of web application security based on the OWASP ASVS standard. *Scientific Journal of the Ternopil National Technical University*. 2025. № 2(118). P. 56–65. ISSN 2522-4433. DOI: 10.33108/visnyk_tntu2025.02.056

У дискусії взяли участь офіційні опоненти, рецензенти та голова:

Іван ОПІРСЬКИЙ, доктор технічних наук, професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка» (офіційний опонент), наголосив на актуальності роботи, її новаторському характері, висловивши, водночас, наступні зауваження:

- 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.
- 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.

- 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.
- 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.
- 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.
- 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.

Дмитро МЕДЗАТИЙ, кандидат технічних наук, доцент, доцент кафедри комп’ютерної інженерії та інформаційних систем Хмельницького національного університету (офіційний опонент) загалом позитивно оцінив науковий рівень дисертації відзначивши практичну цінність розробленої інформаційної системи та можливість її використання аудиторами-початківцями, проте висловив наступні зауваження:

- 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.
- 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.
- у розділі 1 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.

- 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.
- 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.
- 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.
- 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.
- робота містить деякі неточності у формулах, наприклад, у формулах 12, 13, 15, 16, 17, у першому елементі множин відсутня дужка що відкривається.
- деякі рисунки, зокрема 4.8, 4.9 та 4.10, мають надто низьку роздільну здатність і невдалий масштаб, що ускладнює їхнє сприйняття та аналіз.
- 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
- 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.

Марина ДЕРКАЧ, кандидатка технічних наук, доцентка, доцентка кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя (рецензент), висловила загальне позитивне враження від дисертаційної роботи та відзначила обґрунтованість наукових положень, висновків та рекомендацій, що забезпечуються коректним використанням галузевих стандартів та усталених практик, а також вказала на деякі аспекти, які потребують уточнення, подальших досліджень та розвитку, зокрема:

- в розділі 1.2 наведено статистичні дані про вразливість вебсайтів, розроблених популярних платформах, зокрема WordPress, однак не враховано, що висока частка інцидентів може бути зумовлена саме широким розповсюдженням цієї платформи, а не лише її слабкими місцями безпеки. Варто було б додатково уточнити, чи наведені відсотки враховують ринкову частку платформ, чи лише абсолютну кількість інцидентів.
- у першому розділі акцент зроблено переважно на важливості врахування життєвого циклу розробки програмного забезпечення (SDLC) при оцінюванні рівня безпеки вебдодатків. Водночас недостатньо розкрито вплив архітектурної складності самого вебдодатку - від простих односторінкових рішень багаторівневих онлайн-платформ із динамічним контентом та інтеграцією з зовнішніми сервісами, - оскільки саме такі особливості можуть суттєво впливати на поверхню атаки та вимоги до захисту.

- доцільно було би вказати, що ефективне застосування запропонованого методу кількісної оцінки захищеності вебдодатків потребує повного доступу до внутрішньої документації розробника, зокрема технічних специфікацій, описів архітектури, моделей доступу та реалізованих функціональних вимог. Відсутність такої інформації в умовах зовнішнього аудиту або закритих систем може суттєво обмежити можливість проведення об'єктивної оцінки.
- доцільно було би провести експериментальне дослідження рівня безпеки вебдодатку не лише на прикладі навчального середовища "OWASP Juice Shop" з попередньо впровадженими вразливостями, а й на власноруч розробленій інформаційній системі. Це дозволить підтвердити практичну застосовність розробленого адаптивного методу кількісної оцінки захищеності, основаної на стандарті OWASP ASVS.
- на рисунку 4.1 не відображено безпекові механізми розробленої інформаційної системи, які є важливою складовою її архітектури. Для повноти представлення системи доцільно було би доповнити схему елементами, що реалізують основні заходи захисту.
- перелік використаних джерел, список публікацій здобувача за темою дисертації та відомості про відомості про апробацію результатів дисертаційної роботи інколи оформлено з порушенням вимог ДСТУ.

Василь ЯЦИШИН, кандидат технічних наук, доцент, завідувач кафедри систем штучного інтелекту та аналізу даних Тернопільського національного технічного університету імені Івана Пулюя (рецензент) відзначив високий рівень наукової компетентності автора та його спроможності вирішувати складні науково-практичні завдання та підкреслив важливість отриманих результатів, зокрема автоматизації процесу оцінювання та фахівців-тестувальників, однак зауважив:

- 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.
- 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.
- у роботі не запропоновано механізму та процедури комплексної інтегральної оцінки захищеності вебдодатків, а лише за окремими критеріями.
- 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.
- 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.
- у роботі чітко не представлено результати і критерії тестування розробленої інформаційної системи щодо визначення рівня коректності її функціонування та зручності використання.
- у роботі варто було б навести порівняльну характеристику кількісних показників затрат часу експертів при використанні запропонованої методики і традиційного експертного оцінювання.

Олег ПАСТУХ, доктор технічних наук, професор, професор кафедри програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя (голова разової спеціалізованої вченої ради) дав позитивну оцінку отриманим результатам, підкресливши цінність розробленої системи критеріїв, що формалізує оцінювання вимог захищеності вебдодатків та методу кількісної оцінки безпеки вебдодатку. Голова ради відзначив належний науковий рівень дисертаційної роботи та глибокі знання здобувача у тематиці дослідження.

Результати відкритого голосування:

«За» 5 членів ради,

«Проти» 0 членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує Олександру РЕВНЮКУ ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої вченої ради _____ Олег ПАСТУХ

(підпис) (власне ім'я та прізвище)

М.П.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ * 05408102