РЕЦЕНЗІЯ

рецензента, к.т.н., с.н.с., Ткачова Андрія Михайловича

на дисертаційну роботу **Звєрцевої Наталії Віталіївни**

«Моделі оцінки безпеки комп'ютерних систем»

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 122 – Комп'ютерні науки

Актуальність теми. Дисертація присвячена важливій науковій проблемі – оцінюванню рівня безпеки комп'ютерних систем з урахуванням сучасних тенденцій розвитку кіберпростору. В умовах активної цифровізації, розширення Інтернету речей, застосування штучного інтелекту та хмарних технологій, забезпечення стійкого кіберзахисту набуває критичної значущості.

Особливу увагу приділено складним гібридним загрозам, що поєднують елементи технічного впливу, соціальної інженерії та атак на інфраструктуру. Не менш актуальним є вплив постквантових технологій, які ставлять під сумнів ефективність традиційних криптографічних рішень.

У дисертації обгрунтовано потребу у створенні нових моделей оцінки безпеки, які здатні комплексно враховувати технічні, економічні та організаційні аспекти загроз. Запропонований підхід на основі комплексованих метрик і логіки гібридних впливів має як теоретичну, так і прикладну цінність для підвищення стійкості комп'ютерних систем до сучасних викликів.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконувалась відповідно до наукової програми 122 «Комп'ютерні науки», яка була впроваджена на кафедрі програмної інженерії та інтелектуальних технологій управління НТУ «ХПІ».

Проведені дослідження тісно пов'язана з кафедральною науково-дослідною роботою НТУ «ХПІ» «Розробка моделей, методів та

інформаційних технологій оцінювання складних багатоознакових об'єктів і систем» (0125U001121).

Наукова новизна одержаних результатів. Дисертація містить наукову новизну, з найбільш суттєвих доробок роботи можна назвати:

- розроблено модель оцінки захищеності комп'ютерної системи з урахуванням базових складових безпеки, гібридності та синергізму загроз;
- запропоновано метод безперервного функціонування системи безпеки для захисту критичних бізнес-процесів і своєчасного реагування на змішані атаки;
- розроблено модель визначення рівня безпеки на основі інтеграції метрик з урахуванням витрат атакуючого та рівня конфіденційності;
- удосконалено математичний апарат класифікації загроз з урахуванням їх гібридності, синергізму та впливу на критичні елементи мережі.

Вважаю, що робота дисертанта є внеском у розробку математичних моделей та обчислювальних методів оцінки рівня захищеності комп'ютерних систем.

Практична цінність одержаних результатів та рекомендації щодо їх подальшого використання. Дослідження має прикладне значення, оскільки автор запропонував нові підходи до оцінювання рівня безпеки комп'ютерних систем, що базуються на комплексуванні метрик та застосуванні методів математичного моделювання. Це дозволяє створювати структуровані моделі оцінки захищеності, здатні своєчасно виявляти ризики та адаптувати системи кібербезпеки до динамічного середовища загроз.

Повнота викладення матеріалів дисертації в наукових працях, які опубліковані автором. За результатами дослідження дисертаційної роботи опубліковано 15 наукових праць, з них у фахових наукових виданнях, ДАК Міністерства освіти і науки України – 3, у реферативній базі Scopus – 2, наукових праць, які засвідчують апробацію матеріалів дисертації – 10.

Зазначене вище дозволяє стверджувати, що представлена дисертаційна робота є самостійним, завершеним науковим дослідженням, результати якого мають значення для сфери кіберзахисту.

Аналіз змісту дисертації. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації. Робота Звєрцевої Н.В. є завершеною науковою роботою, містить анотацію – українською та англійською мовами, вступ, чотири розділи, висновки, список використаних джерел і чотири додатки.

Дисертація присвячена актуалізації та уточненню підходів до оцінювання рівня безпеки комп'ютерних систем в умовах сучасних загроз, зокрема гібридних і постквантових, а також вивченню можливостей практичної реалізації запропонованих моделей у різних аспектах функціонування соціокіберфізичних систем.

Об'єктом дослідження є процес створення та використання нових моделей і методів оцінки рівня безпеки комп'ютерних систем.

У *першому розділі* проведено комплексний аналіз сучасного стану інформаційної безпеки комп'ютерних систем, розглянуто класифікацію та особливості кібератак як джерел загроз, а також системи виявлення кібератак як невід'ємний елемент безпеки. Визначено проблеми ефективності існуючих методів класифікації атак та обґрунтовано потребу у створенні нових підходів. На основі проведеного аналізу сформульовано наукове завдання дослідження.

Другий розділ присвячено методології формування моделей загроз на основі метрик безпеки. Наведено обґрунтування вибору релевантних метрик для оцінювання загроз, проведено аналіз існуючих підходів до побудови моделей безпеки та визначено критерії інтеграції метрик для комплексного відображення ризиків. Узагальнено науково-технічні засади вибору оптимального підходу до побудови моделей оцінювання рівня захищеності комп'ютерних систем.

У третьому розділі викладено результати розробки трьох моделей оцінювання безпеки: моделі оцінки поточного стану захищеності комп'ютерної системи з урахуванням гібридності загроз; методу безперервного функціонування системи безпеки, що дозволяє забезпечити сталу захищеність критичних бізнес-процесів; а також моделі інтегрованої оцінки рівня безпеки, заснованої на комплексуванні метрик для соціокіберфізичних систем.

Четвертий розділ присвячено верифікації запропонованих моделей. Проведено оцінку ефективності моделі поточного стану безпеки, перевірено множину правил досяжності заданого рівня захищеності з урахуванням технічних і організаційних факторів. Запропоновано архітектуру та програмну реалізацію системи автоматизованого оцінювання рівня безпеки, що здатна підтримувати прийняття управлінських рішень в умовах змінного загрозового середовища.

Висновки, сформульовані у роботі, висвітлюють результати дослідження як вирішення висунутих в дисертації завдань. В цілому висновки відповідають вимогам, які висуваються до результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії.

Список літератури досить широко охоплює предметне поле дослідження, певною мірою відображає опрацювання автором значної кількості джерел доменного змісту, а також іноземних джерел.

Додатки містять інформацію про практичне впровадження результатів дисертації, розширений список задач дослідження та список публікацій здобувача.

Достовірність отриманих результатів та висновків. Достовірність отриманих результатів зумовлено поставленими метою та завданнями, а також використанням відповідної методології дослідження. Крім того, достовірність заявлених положень обгрунтовується комплексним підходом у

вивченні визначеного об'єкта, що також зумовлює і низку певних методів, які були використані в процесі дослідження.

Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових положень та результатів в опублікованих працях. Дисертація виконана з дотримання вимог академічної доброчесності, отримані результати дають підстави говорити про оригінальність роботи. У тексті містяться авторські ідеї, і не виявлено використання ідей інших науковців без посилання на їх роботи.

Основні ідеї автора та результати дослідження викладено у п'ятьох статтях, а також дисертант активно приймав участь в українських та закордонних конференціях, де була проведена апробація ідей, що викладено у дисертаційному дослідженні.

Недоліки та зауваження до дисертаційної роботи:

1. Обмежена увага до практичного тестування моделей у реальних середовищах: незважаючи на проведену верифікацію в четвертому розділі, у роботі недостатньо описано впровадження розробленої системи оцінювання безпеки в умовах реального мережевого середовища.

2. Недостатньо висвітлено адаптивність моделей в третьому розділі до нових типів загроз: розроблені підходи орієнтовані на виявлення гібридних атак, однак бракує опису механізмів динамічного оновлення моделей з урахуванням появи нових або непередбачуваних сценаріїв атак.

3. Безперечною перевагою роботи стало б висвітлення оцінки обчислювальної складності реалізації запропонованих моделей. У дисертації відсутній аналіз продуктивності моделей з точки зору споживання ресурсів (часу, пам'яті), що важливо для інтеграції в системи з обмеженими обчислювальними можливостями.

4. Існують недоліки оформлення матеріалу дисертаційної роботи, за текстом іноді зустрічаються друкарські, пунктуаційні та стилістичні помилки.

Проте наведені у результаті аналізу роботи зауваження не носять принципового характеру та жодним чином не знижують позитивне враження від роботи та її наукову та практичну цінність.

Висновки. Дисертаційна робота Звєрцевої Н.В. є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та практичну спрямованість. Тема дослідження відповідає галузі знань 12 – «Інформаційні технології» та спеціальності 122 – «Комп'ютерні науки».

Отже, враховуючи актуальність теми, отримані результати та певну практичну значущість вважаю, що дисертаційна робота Звєрцевої Наталії Віталіївни «Моделі оцінки безпеки комп'ютерних систем» відповідає вимогам 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціальної вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» від 12.01.2022 р. № 44 та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, а сам автор, Звєрцева Наталія Віталіївна, заслуговує присудження їй наукового ступеня доктора філософії зі спеціальності 122 – «Комп'ютерні науки».

Рецензент
доцент кафедри кібербезпеки національного
технічного університету «Харківський
політехнічний інститут»,
кандидат технічних наук Андрій ТКАЧОВ

«03» 07 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * Код 02071180 *

Підпис Ткачова
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"___" _____ 20___ р.