

РЕЦЕНЗІЯ

офіційного рецензента,
доцента кафедри інформаційних технологій та програмної інженерії
Національного університету «Чернігівська політехніка»,
кандидата фізико-математичних наук,
доцента **Акименка Андрія Миколайовича**
на дисертаційну роботу **Трунова Олексія Ігоровича**
**на тему «Інформаційна технологія підтримки прийняття рішень при
забезпеченні інформаційної безпеки транспортно-логістичного центру»,**
представлену на здобуття ступеня доктора філософії в галузі знань
12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

Актуальність теми дисертації

У сучасних умовах глобалізації та постійних геополітичних викликів транспортно-логістичні центри (ТЛЦ) перетворилися на стратегічно важливі об'єкти критичної інфраструктури. Особливого значення їхня стабільна робота набуває в контексті повномасштабної війни в Україні та завдань із подальшого інноваційного відновлення постраждалих регіонів, оскільки саме ТЛЦ забезпечують логістичний супровід сил оборони, доставку гуманітарних вантажів і загальну стійкість національної економіки.

Стрімкі процеси цифровізації та конвергенція інформаційних (ІТ) і операційних технологій роблять ТЛЦ вразливими до сучасних кіберзагроз (таких як програми-вимагачі, атаки на ланцюги постачання тощо). Кібервтручання в інформаційні системи логістичних комплексів здатне повністю паралізувати їхні операційні процеси, що створює пряму загрозу національній безпеці та обороноздатності держави.

Ефективне управління інформаційною безпекою (ІБ) у цій галузі суттєво ускладнюється високим рівнем невизначеності – браком ретроспективних даних, динамічністю кібератак та суб'єктивізмом експертних оцінок. Наявні методи аналізу ризиків здебільшого є фрагментарними, не враховують галузеву специфіку кіберфізичних систем ТЛЦ і мають обмежені можливості для обробки нечітких даних.

У зв'язку з цим актуальними є дослідження, спрямовані на інтелектуалізацію процесів захисту за допомогою апарату нечіткої логіки та обчислювального інтелекту. Розроблення нової інформаційної технології підтримки прийняття рішень, здатної здійснювати стратегічне оцінювання ризиків ІБ ТЛЦ в умовах нестабільності, є важливим і своєчасним науково-практичним завданням.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційне дослідження безпосередньо пов'язане з виконанням науково-дослідних робіт у сфері системного аналізу логістичних процесів та забезпечення ІБ критичної інфраструктури.

Основні наукові результати автором отримано в межах прикладного державного проєкту «Розробка інформаційно-аналітичної системи управління логістичними операціями інноваційного відновлення прикордонних регіонів для забезпечення національної безпеки» (державний реєстраційний номер 0124U000696), а також ініціативної науково-дослідної теми Національного університету «Чернігівська політехніка» – «Системний аналіз інформаційних процесів управління логістичною діяльністю» (державний реєстраційний номер 0124U003344).

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Усі сформульовані у дисертації наукові положення та висновки є належним чином аргументованими й логічно послідовними. Для розв'язання поставлених завдань здобувачем застосовано коректний математичний та інструментальний апарат, що відповідає предмету й меті дослідження: методи системного аналізу, теорію нечітких множин, нейронечітке моделювання (ANFIS), метод аналізу ієрархій (Fuzzy AHP) та стандарти функціонального моделювання (IDEF0, DFD, UML).

Достовірність отриманих результатів підтверджується імітаційним моделюванням, високою збіжністю експериментальних даних із теоретичними положеннями, а також успішним практичним впровадженням розробленої технології у діяльність ТОВ «СІБЕРТРАНС» та в освітній процес НУ «Чернігівська політехніка».

Наукова новизна дисертаційної роботи полягає у теоретичному обґрунтуванні та створенні нових методів і моделей оцінювання ризиків ІБ в умовах невизначеності інформаційного середовища ТЛЦ:

Вперше розроблено трирівневу ієрархічну модель класифікації факторів впливу на ризики ІБ ТЛЦ, яка дозволяє комплексно структурувати та враховувати взаємозв'язки між різнорідними чинниками кіберфізичного простору логістичних систем.

Вперше запропоновано гібридну концептуальну модель інтегрального оцінювання ризиків, яка поєднує експертну нечітку аналітику та адаптивне нейронечітке обчислювальне ядро (ANFIS) з поліноміальною апроксимацією другого порядку, що підвищує точність моніторингу безпеки за умов дефіциту статистичних даних.

Удосконалено метод Fuzzy AHP для пріоритезації чинників загрози, який інтегрує підходи Чанга та Баклі із одночасним врахуванням індексу когнітивної впевненості експерта, що усуває математичні похибки нульових ваг.

Набув подальшого розвитку метод обробки правил нечіткого виводу завдяки оригінальному дворівневому застосуванню логічного алгоритму Rete в нейронечіткій архітектурі, що забезпечило високу обчислювальну швидкість системи в режимі реального часу.

Одержані результати мають суттєве теоретичне та практичне значення для розвитку комп'ютерних наук у напрямі побудови інтелектуальних систем

підтримки прийняття рішень та управління кібербезпекою об'єктів критичної інфраструктури.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності

Зміст дисертаційної роботи Трунова О. І. та її тематична спрямованість повністю відображають сучасні тенденції розвитку методів обчислювального інтелекту, системного аналізу та інформаційної безпеки в складних системах. Кваліфікаційна праця є завершеним дослідженням, що безпосередньо відповідає профілю підготовки фахівців за спеціальністю 122 – Комп'ютерні науки.

Перевірка дисертаційної роботи на текстові збіги та аналіз звіту подібності підтверджують беззаперечне дотримання автором принципів академічної доброчесності. У тексті не виявлено ознак плагіату, фабрикації чи фальсифікації результатів. Наявні паралелі мають виключно коректний характер, пов'язані із загальноприйнятою науковою термінологією, нормативними формулюваннями чи посиланнями на власні попередні праці здобувача. Усі запозичені ідеї чи концепції інших дослідників супроводжуються точними бібліографічними посиланнями.

Матеріал дисертації викладено українською мовою з чітким дотриманням академічного стилю. Оформлення рукопису виконано відповідно до вимог Міністерства освіти і науки України (наказ № 40 від 12.01.2017 р.).

Дисертація складається зі вступної частини, чотирьох послідовних розділів, загальних висновків, списку використаних джерел (134 найменування) та 6 додатків. Загальний обсяг роботи становить 248 сторінок, з яких 164 сторінки займає основний текст (у роботі вміщено 51 рисунок та 36 таблиць).

У вступній частині автором обґрунтовано актуальність обраної теми, визначено об'єкт, предмет, мету та комплекс наукових завдань. Сформульовано наукову новизну, висвітлено практичну цінність результатів, а також наведено дані щодо апробації та впровадження роботи.

У першому розділі проведено аналіз ТЛЦ як кіберфізичного об'єкта захисту. Досліджено специфіку інформаційних процесів в умовах конвергенції ІТ/ОТ, сформовано модель кіберзагроз із урахуванням воєнних ризиків та доведено обмеженість класичних систем аналізу ризиків, що дозволило чітко формалізувати постановку задачі дослідження.

У другому розділі розроблено математичне забезпечення інформаційної технології. Запропоновано ієрархічну модель факторів впливу, нечітку модифікацію стратегічної матриці Дж. Х. Вілсона та вдосконалений метод Fuzzy АНР. Обґрунтовано адаптивну нейронечітку модель ANFIS із поліноміальною функцією другого ступеня та метод умовної оптимізації керованих чинників на основі символічного аналізу градієнтів, що дозволяє здійснювати прескриптивний аналіз.

У третьому розділі виконано проектування інформаційної технології підтримки прийняття рішень. За допомогою інструментів IDEF0, DFD та UML побудовано функціональні моделі та сценарії взаємодії користувачів. Обґрунтовано сервіс-орієнтовану архітектуру системи та детально описано програмну реалізацію обчислювальних модулів, зокрема автоматичної генерації бази знань та швидкого виведення Rete.

У четвертому розділі проведено імітаційне моделювання та практичну апробацію розробленої інформаційної технології підтримки прийняття рішень при забезпеченні ІБ ТЛЦ. На базі масиву даних підтверджено високу точність обчислювального ядра, доведено ефективність алгоритмів оптимізації виведення та обґрунтовано стратегічні рекомендації щодо захисту інформаційних ресурсів.

Оприлюднення результатів дисертаційної роботи

Основні положення та теоретико-прикладні результати дослідження достатньою мірою висвітлені у 19 наукових публікаціях автора. Серед них: 5 наукових статей у профільних виданнях (зокрема 3 статті у фахових виданнях України та 2 статті у міжнародних журналах, що індексуються наукометричними базами Scopus та Web of Science); 1 свідоцтво про реєстрацію авторського права на комп'ютерну програму; 14 публікацій апробаційного характеру у матеріалах міжнародних та всеукраїнських науково-практичних конференцій.

Опубліковані праці повною мірою відображають зміст дисертації, а хід дослідження пройшов належне рецензування та обговорення у фаховому науковому середовищі.

Недоліки та зауваження до дисертаційної роботи

Позитивно оцінюючи науковий рівень дисертаційної роботи, її методологічну завершеність та прикладне значення, доцільно висловити кілька зауважень, які мають переважно рекомендаційний характер:

1. У першому розділі поза аналітичним оглядом автора залишилися сучасні тенденції розвитку периферійних систем виявлення аномалій (Edge Computing) на рівні IoT-контролерів, автоматизованих візків (AGV) або WMS-сегмента складських зон, через що в роботі варто було чіткіше окреслити межі інтеграції розробленої технології з локальними засобами захисту.

2. Використаний у другому розділі метод Fuzzy АНР вимагає побудови громіздких матриць парних порівнянь, що суттєво перевантажує експертів за наявності трьох рівнів декомпозиції, проте в тексті роботи відсутнє чітке обґрунтування переваг цього підходу порівняно з простішим методом Fuzzy SAW або прямим бальним оцінюванням.

3. При побудові моделі ANFIS (розділ 2) здобувачем використано конфігурацію другого порядку з квадратичною функцією в консеквентах правил TSK, проте в роботі недостатньо обґрунтовано доцільність такого ускладнення математичного апарату та не наведено порівняльний аналіз помилок навчання (RMSE) для моделей різних порядків.

4. Запропонована у третьому розділі чотирирівнева сервіс-орієнтована архітектура (SOA) та використання шини повідомлень для логістичних центрів малого й середнього масштабу можуть бути надлишковими, що створює ризики додаткових затримок при передачі даних і ускладнює адміністрування системи.

5. Оцінку ефективності розроблених рішень у четвертому розділі проведено на вибірці з 3072 прецедентів (Accuracy = 95,2%), проте в тексті відсутній чіткий розподіл даних на реальні інциденти ТОВ «СІБЕРТРАНС» та штучно згенеровані рушієм Мамдані, а саму роботу доцільно було б доповнити результатами стрес-тестування системи на неструктурованих логах SIEM-систем.

6. У тексті роботи присутні поодинокі технічні неточності: в англomовному Abstract на с. 8 помилково вжито «Trade and Logistics Center» замість «Transport and Logistics Center», у таблиці 2.13 вказано оператор «sing» замість «sign». Деякі графічні матеріали є інформаційно перевантаженими через дрібний шрифт.

Проте висловлені побажання не мають принципового характеру, не зменшують загальну цінність дослідження та не впливають на підсумкову позитивну оцінку дисертації.

Висновок про дисертаційну роботу

Дисертаційна робота Трунова Олексія Ігоровича на тему «Інформаційна технологія підтримки прийняття рішень при забезпеченні інформаційної безпеки транспортно-логістичного центру» є завершеним, самостійним та глибоким науковим дослідженням, у якому вирішено актуальне науково-прикладне завдання у сфері комп'ютерного моделювання та захисту критичної інфраструктури.

Отримані автором результати є науково обґрунтованими, достовірними та мають вагомe теоретичне і практичне значення. За своїм науковим рівнем, обсягом проведених досліджень та оформленням дисертація повністю задовольняє всі вимоги, що висуваються до дисертацій на здобуття наукового ступеня доктора філософії, а її зміст відповідає спеціальності 122 – Комп'ютерні науки галузі знань 12 – Інформаційні технології.

Вважаю, що Трунов Олексій Ігорович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки.

Офіційний рецензент:

доцент кафедри інформаційних технологій
та програмної інженерії
Національного університету
«Чернігівська політехніка»,
кандидат фізико-математичних наук,
доцент

Андрій АКИМЕНКО