

ВІДГУК

офіційного опонента, **Зачка Олега Богдановича**, доктора технічних наук, професора, Заслуженого діяча науки і техніки України, професора кафедри права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності 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

Актуальність теми дисертаційного дослідження зумовлена стрімкою трансформацією сучасних транспортно-логістичних центрів (ТЛЦ) у складні кіберфізичні системи та їхньою роллю як стратегічних об'єктів критичної інфраструктури. В умовах повномасштабної війни в Україні та завдань повоєнного інноваційного відновлення прикордонних територій надійне функціонування ТЛЦ є базовою умовою для забезпечення логістики сил оборони, стабільності цивільного тилу та експортно-імпортного потенціалу держави.

Проте процеси активної цифровізації та конвергенції інформаційних (ІТ) й операційних технологій перетворюють ці центри на пріоритетні цілі для скоординованих кібератак. Навмисні дестабілізуючі кібервтручання (діяльність програм-вимагачів, злам систем управління ланцюгами постачання, витоки конфіденційних даних) здатні призвести до повного паралічу логістики, що створює прямі ризики для національної безпеки.

Традиційні системи управління та наявні стандарти (такі як NIST чи ISO/IEC 27005) ускладнюються у застосуванні через високий рівень невизначеності інформаційного середовища, фрагментарність оцінювання та

статичність класичних моделей ризику, які неспроможні оперативно опрацьовувати нечітку експертну інформацію.

У зв'язку з цим виникає гостра науково-практична потреба у створенні моделей комплексного аналізу та розробленні нових інформаційних технологій підтримки прийняття рішень при забезпеченні інформаційної безпеки об'єктів транспортно-логістичної інфраструктури. Поєднання методів експертної аналітики з гнучкими обчислювальними підходами та нейронечіткими системами дозволяє компенсувати дефіцит ретроспективних даних, підвищити стійкість логістичних вузлів та забезпечити адекватне прескриптивне управління безпекою в реальному часі.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційне дослідження виконано у безпосередньому зв'язку з пріоритетними науковими напрямами України щодо захисту критичної інфраструктури. Основні результати роботи отримано в межах виконання державного проєкту прикладного дослідження «Розробка інформаційно-аналітичної системи управління логістичними операціями інноваційного відновлення прикордонних регіонів для забезпечення національної безпеки» (державний реєстраційний номер 0124U000696), а також планової 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

Наукові результати, що отримані здобувачем, є цілком обґрунтованими та базуються на коректному застосуванні сучасного інструментарію комп'ютерних наук: методів системного аналізу, теорії нечітких множин, нейронечітких мереж ANFIS, концепції нечіткого аналізу ієрархій (Fuzzy АНР) та стандартів структурно-функціонального моделювання (IDEF0, DFD,

UML). Достовірність розроблених моделей підтверджена успішним навчанням інтелектуального ядра на реальному масиві з 3840 записів моніторингу діяльності ТЛЦ, високими показниками точності класифікації (Accuracy = 95,2%), а також узгодженістю експериментальних даних із практичними прецедентами. Практична цінність результатів засвідчена Свідощвом про реєстрацію авторського права на комп'ютерну програму № 143390, актами впровадження у діяльність ТОВ «СІБЕРТРАНС» та використанням в освітньому процесі НУ «Чернігівська політехніка».

Наукова новизна одержаних результатів полягає в оптимізації процесів інтелектуальної підтримки прийняття рішень та побудові гібридних моделей оцінювання ризиків ІБ за умов невизначеності:

Вперше розроблено трирівневу ієрархічну модель класифікації факторів впливу на рівень ризику ІБ ТЛЦ, яка системно структурує та формалізує взаємозалежність різнорідних чинників кіберфізичного простору логістичних систем.

Вперше запропоновано модель інтегрального оцінювання ризику ІБ, побудовану на поєднанні експертних оцінок та адаптивної системи ANFIS з поліноміальною функцією висновків другого порядку, що забезпечує високу точність аналізу в умовах початкового дефіциту статистичних даних.

Удосконалено метод Fuzzy АНР для пріоритезації факторів ризику, який поєднує підходи Чанга та Баклі із введенням коефіцієнта когнітивної впевненості аналітиків, що дозволило нейтралізувати проблему «нульових ваг».

Набув подальшого розвитку метод обробки правил нечіткого виводу за рахунок оригінального дворівневого впровадження логічного алгоритму Rete в архітектуру системи, що суттєво підвищило швидкість обчислень ризиків у реальному часі.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності

Дисертація Трунова О. І. – повністю відповідає вимогам Стандарту вищої освіти та тематиці досліджень за спеціальністю 122 – Комп’ютерні науки. Робота є цілісним, завершеним самостійним науковим дослідженням, яке відображає особистий внесок автора у розвиток інформаційних технологій захисту стратегічних логістичних вузлів.

Аналіз рукопису та звіту подібності дає підстави стверджувати, що дисертація виконана із суворим дотриманням принципів академічної доброчесності. Робота не містить ознак плагіату, фабрикації чи фальсифікації результатів. Наявні текстові збіги мають нормативний характер, оскільки зумовлені використанням стандартної термінології та коректним посиланням на спільні наукові праці здобувача, що супроводжуються точними бібліографічними реєстрами.

Мова та стиль викладення результатів

Дисертацію виконано українською мовою на належному науковому рівні. Матеріал викладено логічно, послідовно, із коректним застосуванням спеціалізованого понятійного апарату. Оформлення роботи відповідає вимогам наказу МОН України № 40 від 12.01.2017 р..

Дисертаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку джерел (134 найменування) та 6 додатків. Загальний обсяг становить 248 сторінок (основний текст – 164 сторінки, містить 51 рисунок та 36 таблиць).

У вступі обґрунтовано актуальність, сформульовано мету, об’єкт, предмет та 5 взаємопов’язаних завдань, визначено наукову новизну та прикладну цінність.

У першому розділі проведено аналіз ТЛЦ як об’єкта критичної інфраструктури в умовах конвергенції ІТ/ОТ. Описано специфічні бізнес-процеси, сформовано модель кіберзагроз з урахуванням воєнних ризиків та

обґрунтовано необхідність побудови інтелектуальної ІТ ППР за умов дефіциту ретроспективних даних.

У другому розділі побудовано математичний базис технології. Розроблено ієрархічну модель факторів ІБ, модифіковану матрицю Дж. Х. Вілсона з нечіткими координатами та систему ANFIS із поліноміальною функцією другого ступеня. Сформульовано задачу умовної оптимізації захисних чинників на основі символного аналізу градієнтів.

У третьому розділі здійснено архітектурне проектування ІТ ППР за допомогою методологій IDEF0, DFD, IDEF3 та UML. Обґрунтовано сервіс-орієнтовані рішення та детально описано програмну реалізацію модулів фазифікації, автоматизованої генерації бази знань Mamdani та оптимізованого виводу Rete.

У четвертому розділі наведено результати практичного впровадження вебзастосунку «SecureFuzzy». Експериментально підтверджено еволюційний розвиток моделі (зниження похибки до $RMSE = 0,0147$, зростання кореляції до 0,994 за 40 епох навчання). Математично доведено, що прескриптивні інвестиції в культуру ІБ (персонал) у 1,5 рази ефективніші за суто адміністративні заходи, та обґрунтовано параметри редукції бази знань.

Оприлюднення результатів дисертаційної роботи

Основні положення дослідження достатньою мірою відображені у 19 наукових публікаціях здобувача, зокрема: 5 статей у фахових виданнях (із них 2 статті індексуються у базах Scopus та Web of Science), 1 свідоцтво про реєстрацію авторського права та 14 тез доповідей на міжнародних і всеукраїнських наукових конференціях (включаючи конференції «МОДС», «INUDECO», «Юність науки» та ін.).

Публікації повною мірою висвітлюють зміст роботи та засвідчують належну апробацію результатів.

Недоліки та зауваження до дисертаційної роботи

Позитивно оцінюючи зміст та вагоме прикладне значення дисертаційного дослідження, вважаю за доцільне висловити декілька зауважень:

1. При побудові моделей багатокритеріального аналізу та в модулях фазифікації вхідних і вихідних лінгвістичних змінних ризику ІБ (п.п. 2.2) здобувачем використовуються уніфіковані симетричні трикутні нечіткі числа (TFN). Було б доцільно обґрунтувати відмову від застосування трапецієподібних чи гаусових функцій належності. Довести, що TFN спроможні достатньо точно описувати неоднозначність експертних суджень і нелінійні коливання параметрів кіберфізичних систем ТЛЦ.

2. Автор пропонує використовувати одночасно три різні бази даних (PostgreSQL, Neo4j, TimescaleDB). Проте в роботі недостатньо оцінено, як така складна структура вплине на загальну швидкість системи. Не наведено детального аналізу затримок часу, які виникатимуть при передачі та синхронізації потоків даних у реальному часі.

3. Для оптимізації логічного виведення в базі знань автор використовує дворівневий алгоритм Rete (підрозділ 3.4), що суттєво підвищує швидкість сортування потокових фактів. Проте в тексті розділу оцінено лише часові витрати на проходження фактів крізь статичний граф предикатів, але не наведено аналізу обчислювальної складності (О-нотація) процесу динамічної реконфігурації структури альфа- та бета-вузлів у випадку оперативної модифікації правил експертами.

4. Оцінюючи ефективність розробленої інформаційної технології у підрозділі 4.2, здобувач оперує переважно інтегральним показником загальної точності (*Accuracy*). Для систем підтримки прийняття рішень у сфері критичної інфраструктури, де вибірки безпекових інцидентів є сильно незбалансованими, використання лише фінального коефіцієнта $Accuracy$ є недостатнім. Робота суттєво виграла б від проведення наскрізного порівняльного аналізу метрик точності (*Precision*), повноти (*Recall*) та F_1 -score

на етапі базового нечіткого виведення, після первинного навчання ANFIS та на етапі її фінальної редукції за критерієм Стюдента. Це дозволило б наочно оцінити ймовірність пропуску критичних загроз на кожній стадії еволюції моделі.

5. При загалом грамотному та послідовному науковому викладі матеріалу, у тексті дисертаційного рукопису та в описі програмної реалізації (Розділи 3, 4) присутні поодинокі стилістичні неточності та використання виразів, властивих професійному IT-сленгу та інженерному жаргону (зокрема, вживання термінів «холодний старт» системи, «рушій» нечіткого виведення, «заморожування» або «відсів» коефіцієнтів). Зазначені поняття доцільно було б замінити на загальноприйняті терміни системного аналізу та комп'ютерних наук, що покращило б академічний стиль сприйняття роботи.

Зазначені зауваження мають рекомендаційний характер та не впливають на загальні позитивні висновки щодо наукового рівня дисертації, її новизни й практичного значення.

Висновок про дисертаційну роботу

На мою думку, дисертаційна робота Трунова Олексія Ігоровича на тему «Інформаційна технологія підтримки прийняття рішень при забезпеченні інформаційної безпеки транспортно-логістичного центру» є завершеним самостійним науковим дослідженням, у якому отримано обґрунтовані та достовірні результати, що мають суттєве теоретичне і практичне значення для розвитку методів обчислювального інтелекту у сфері кіберзахисту.

За змістом, структурою та рівнем виконання дисертація повністю задовольняє вимогам чинного законодавства України, що висуваються до дисертаційних робіт на здобуття наукового ступеня доктора філософії, а також 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 опонент:

професор кафедри права та менеджменту у сфері цивільного захисту

Львівського державного університету безпеки життєдіяльності,

доктор технічних наук, професор

Заслужений діяч науки й техніки України

 **Олег ЗАЧКО**

