

Голові разової спеціалізованої вченої ради  
Національного авіаційного університету  
доктору технічних наук, професору  
Одарченку Роману Сергійовичу

## **РЕЦЕНЗІЯ**

кандидата технічних наук, старшого дослідника, провідного наукового співробітника Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Національного авіаційного університету

**Охріменко Тетяни Олександрівни**

на дисертацію Положенцева Артема Анатолійовича

«Методи та засоби управління IT-інцидентами на об'єктах критичної інформаційної інфраструктури», представлену на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки галузі знань 12 – Інформаційні технології

### **1. Актуальність теми дисертаційного дослідження**

Дисертаційне дослідження присвячено важливій темі забезпечення надійного захисту критичної інфраструктури (КІ) в умовах швидкого розвитку інформаційних технологій та цифрової трансформації. Підхід до захисту критичної інформаційної інфраструктури (КІІ) від IT-інцидентів є надзвичайно важливим, оскільки будь-які порушення в роботі КІ можуть призвести до серйозних наслідків для економіки, громадського порядку, охорони здоров'я та інших життєво важливих секторів держави.

Актуальність теми дослідження полягає в тому, що в умовах зростаючої кількості та складності IT-загроз, необхідно розробляти нові методи оцінювання стану захищеності та управління IT-інцидентами для забезпечення надійного функціонування КІІ. Відсутність належного захисту може призвести до зупинки критичних функцій держави, що в свою чергу може мати катастрофічні наслідки для економіки та безпеки країни.

Дослідження спрямоване на вирішення важливих науково-технічних задач, що мають як теоретичне, так і практичне значення, зокрема розробка методів управління IT-інцидентами та IT-загрозами, які дозволять ефективно розподіляти ресурси для нейтралізації загроз. Практичне



значення одержаних результатів полягає у можливості їх використання відповідними органами для ефективного оцінювання стану захищеності КІІ та управління ІТ-загрозами.

Дисертаційне дослідження Положенцева А.А. має велике значення для забезпечення національної безпеки держави, адже захист ІТ-систем КІІ є ключовою складовою стабільного функціонування економіки, громадського порядку, охорони здоров'я та інших критично важливих секторів.

## **2. Зв'язок роботи з науковими програмами, планами, темами**

Результати дисертаційної роботи відображені у науково-дослідній роботі Національного авіаційного університету за темою «Алгоритмічно-програмне забезпечення універсальних методів захищеного передавання даних при використанні розвідувально-пошукового БПЛА» (держ. реєстр. № 0120U101400) (2023-2024 рр.).

## **3. Наукова новизна отриманих результатів**

Наукова новизна отриманих результатів дисертаційної роботи основним чином полягає у наступному:

- *вперше* розроблено метод управління ІТ-загрозами, який за рахунок синтезу методів багатокритеріального прийняття рішень, моделювання загроз та функції перспективної цінності, дає змогу ідентифікувати, оцінювати та пріоритизувати ІТ-загрози для оптимального розподілу ресурсів захисту критичної інфраструктури держави.
- *удосконалено* метод визначення пріоритетів ІТ-інцидентів, який за рахунок представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації, дозволяє кількісно оцінити пріоритети ІТ-інцидентів та управляти ними для забезпечення необхідного рівня захисту життєво важливих інтересів громадян, суспільства, держави та правопорядку;
- *отримав подальшого розвитку* метод оцінювання рівня захищеності, який за рахунок використання нових індикаторів ІТ-безпеки та рівня цифрової трансформації, а також розроблених рекомендацій для оптимізації захисту дає змогу визначити стан захищеності об'єктів критичної інфраструктури (сектору/підсектору чи держави в цілому), а також управляти захистом зазначених об'єктів в умовах виникнення ІТ-інцидентів.



#### **4. Практичне значення, отриманих результатів**

1. Отримані результати можуть бути використані відповідними органами для ефективного оцінювання стану захищеності сектору/підсектору КІІ, або управління ІТ-загрозами.

2. Реалізовано програмний застосунок, який автоматизує процес оцінки стану захищеності об'єктів критичної інформаційної інфраструктури, для забезпечення структурованого підходу до збору даних, проведення оцінювання рівня захищеності та надає конкретні рекомендації для покращення безпеки критичної інформаційної інфраструктури.

3. Реалізовано методику, яку можна використовувати для визначення пріоритетів ІТ-інцидентів, що дозволяє ефективно ідентифікувати та пріоритизувати інциденти на ОКІІ та оптимізувати розподіл ресурсів, забезпечуючи надійність та стійкість критичних інформаційних систем.

4. Реалізовано програмний застосунок для управління ІТ-загрозами критичної інформаційної інфраструктури, який шляхом синтезу багатокритеріального методу прийняття рішень TODIM та моделлю загроз STRIDE, дозволяє ефективно ідентифікувати, оцінювати та пріоритизувати загрози, враховуючи їхню ймовірність, потенційний збиток та складність реалізації.

5. Теоретичні результати дисертації та результати експериментальних досліджень впроваджені і використовуються у науково-дослідній діяльності НДЛ протидії кіберзагрозам авіаційної галузі НАУ (акт впровадження від 11.12.2023), а також у ДержНДІ технологій кібербезпеки та захисту інформації для підвищення ефективності підготовки фахівців з ІТ та забезпечення захисту ОКІ (акт впровадження від 14.06.2024).

#### **5. Мова та стиль викладення результатів**

Дисертаційна робота написана українською мовою, сформована послідовно та доступно, з використанням загальноприйнятої термінології, з урахуванням наукових проблем, тенденцій та вимог галузі.



## **6. Повнота оприлюднення результатів та дисертаційної роботи**

Основні наукові результати дисертаційної роботи опубліковані у 30 наукових працях, із них: 1 розділ у колективній монографії, 5 наукових статей, надрукованих у вітчизняних фахових наукових виданнях, 15 публікацій, включених до міжнародних наукометричних баз Scopus, а також 9 тез доповідей на науково-практичних конференціях.

## **7. Загальна характеристика структури роботи та змісту дисертаційного дослідження**

Дисертаційне складається з анотації, змісту, вступу, чотирьох розділів, висновку, списку використаних джерел та додатків. Повний обсяг роботи становить 180 сторінок друкованого тексту, з них анотація – на 4 стор., зміст на 2 стор., основний текст на 151 стор., список із 125 використаних джерел на 17 стор., додатки на 29 стор. Дисертація містить 30 рисунків та 38 таблиць.

У **вступі** автором сформульовано актуальність, мету, задачі дослідження, наукову новизну та практичну цінність отриманих результатів, представлено відомості щодо їх впровадження.

У **першому розділі** дисертаційного дослідження було детально проаналізовано основні підходи до захисту КІ України та інших країн світу. Також були проаналізовані сучасні методи управління ІТ-інцидентами, які дозволяють ефективно ідентифікувати, оцінювати та управляти ризиками, пов'язаними з ІТ-загрозами на об'єктах критичної інформаційної інфраструктури (ОКІІ). У ході дослідження визначено переваги та недоліки цих методів, а також можливості їх інтеграції для підвищення рівня захищеності КІ.

У **другому розділі** було удосконалено метод визначення рівня захищеності ОКІІ шляхом впровадження нових індикаторів ІТ-безпеки та рівня цифрової трансформації. Використання цих індикаторів дозволило детальніше оцінити стан безпеки та виявити слабкі місця і потенційні ризики. Крім цього, розроблені рекомендації щодо оптимізації захисту ОКІІ сприятимуть більш точному визначенню їхнього стану захищеності та ефективному управлінню захистом від ІТ-інцидентів.

У **третьому розділі** було удосконалено метод визначення пріоритетів ІТ-інцидентів шляхом створення ієрархічних структур елементів



потенційних загроз і розрахунку ймовірності їх реалізації. Також, у цьому розділі було розроблено метод оцінювання ІТ-загроз, який поєднує методи багатокритеріального прийняття рішень, моделювання загроз та функцію проспективної цінності, що дозволяє ідентифікувати, оцінювати та пріоритизувати ІТ-загрози для оптимального розподілу ресурсів захисту критичної інфраструктури держави.

У **четвертому розділі** на основі розробленого спеціалізованого програмного забезпечення були проведені експериментальні дослідження для різних секторів КІ, таких як цифрові технології, телекомунікації, енергетика, охорона здоров'я, транспорт тощо. Це дозволило верифікувати розроблені у роботі методи управління ІТ-інцидентами на ОКІІ.

У **висновках** стисло представлено основні наукові та практичні результати дисертаційної роботи.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та коди реалізації програмних застосунків.

Дисертаційна робота оформлена відповідно до вимог Наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

## **8. Недоліки та зауваження по роботі**

1. Метрики та індикатори, розроблені автором у розділі II для методу визначення пріоритетів ІТ-інцидентів на ОКІІ, можуть бути занадто поверхневими і не враховувати специфічні потреби та особливості різних галузей КІІ. Це може призвести до недостатньої точності та ефективності при застосуванні в різних умовах. Окрім того, запропоновані етапи і кроки можуть бути надто складними для практичного використання в реальних умовах. Особливо це стосується формування множин метрик та обчислення індексів, що може вимагати значних ресурсів та спеціальних знань, яких може не бути у всіх організацій.

2. У розділі III при розробці методу управління ІТ-загрозами на ОКІІ процес визначення вагових коефіцієнтів критеріїв та оцінки загроз значною мірою залежить від суб'єктивних оцінок експертів. Це може призвести до упередженості результатів, особливо якщо експерти мають різні погляди або недостатній досвід у певних аспектах загроз. А також, може знижувати точність та надійність оцінки ІТ-загроз.



3. Процес збору, оцінки та нормалізації даних може бути складним і ресурсоємним. У великих і складних системах, де кількість потенційних загроз і критеріїв значна, нормалізація даних може бути важкою для реалізації та підтримки. Це може призвести до затримок у процесі оцінки і необхідності залучення додаткових ресурсів.

Протре варто зазначити, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та значимість одержаних результатів.

## 9. Висновки

Вважаю, що дисертаційна робота здобувача Положенцева А.А. на тему «Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченою, цілісною, а сукупність практичних і теоретичних результатів має вагоме значення для галузі знань 12 «Інформаційні технології».

Таким чином дисертаційна робота відповідає вимогам пунктів 6-9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 № 44, а її автор Положенцев Артем Анатолійович заслуговує присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки галузі знань 12 – Інформаційні технології.

## РЕЦЕНЗЕНТ

п.н.с. НДІЛ протидії кіберзагрозам в  
авіаційній галузі Національного  
авіаційного університету  
к.т.н., ст. дослідник

*Тетяна Охрименко*

Тетяна ОХРИМЕНКО

«\_\_\_» \_\_\_\_\_ 2024 року



*22*