

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

РЕЦЕНЗІЯ

доктора технічних наук, професора
завідувача кафедри комп'ютерних інформаційних технологій

Савченко Аліни Станіславівни

на дисертаційну роботу Положенцева Артема Анатолійовича
«Методи та засоби управління ІТ-інцидентами на об'єктах критичної
інформаційної інфраструктури» подану на здобуття ступеня доктора
філософії, за спеціальністю 122 «Комп'ютерні науки»
галузь знань 12 «Інформаційні технології»

Актуальність теми дисертації

Актуальність дисертації обумовлена стрімким розвитком інформаційних технологій та цифрової трансформації, що робить захист ІТ-систем ключовою складовою національної безпеки. В умовах зростаючої кількості та складності ІТ-загроз, особливу увагу необхідно приділити захисту критичної інфраструктури (КІ), оскільки її надійність визначає стабільне функціонування економіки, громадського порядку, охорони здоров'я та інших життєво важливих секторів. Зростання кількості та складності ІТ-загроз вимагає розробки нових методів оцінки стану захищеності та управління ІТ-інцидентами, щоб забезпечити надійне функціонування критичної інформаційної інфраструктури (КІІ). Відсутність належного захисту може призвести до зупинки критичних функцій держави, що може мати катастрофічні наслідки для економіки та безпеки країни.

Таким чином, дисертаційне дослідження Положенцева Артема Анатолійовича, спрямоване на розробку ефективних методів управління та пріоритизації ІТ-інцидентами, є надзвичайно актуальним для оптимального розподілу ресурсів та забезпечення безпеки критичних інформаційних систем.

Дисертаційна робота безпосередньо пов'язана з «Основними науковими напрямками та найважливішими проблемами фундаментальних досліджень у

галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2024–2028 роки», виконана в межах наукового напрямку «Нові комп'ютерні засоби та технології інформатизації суспільства» визначеного пріоритетним у переліку актуальних проблем Міністерством освіти і науки України, концепції «Програми інформатизації НАН України на 2020-2024 роки за основними її напрямками». Теоретичні і практичні положення дисертаційної роботи були використані в науково-дослідних роботах, які виконувались у Національному авіаційному університеті, а саме «Алгоритмічно-програмне забезпечення універсальних методів захищеного передавання даних при використанні розвідувально-пошукового БПЛА (держ. реєстр. № 0120U101400).

Основний зміст роботи

У вступі обґрунтовано актуальність дисертації, визначено мету, об'єкт та предмет дослідження. Сформульовано проблему дисертаційного дослідження, наукові завдання, наведено основні наукові та практичні результати. Відзначено особистий внесок здобувача, апробацію результатів дисертаційної роботи на конференціях, наведено відомості про публікації та структуру роботи.

У першому розділі дисертації проведено всебічний аналіз основних підходів до захисту КІ в Україні та інших країнах світу. Розглянуто методи та стандарти, що використовуються для забезпечення безпеки КІ, включаючи підходи в США, Європейському Союзі, Великій Британії, Канаді, Німеччині, Австралії та Японії. Оцінено нормативні вимоги та практики, визначено ключові напрямки та методи покращення захисту критичної інфраструктури. Також проаналізовано сучасні методи управління ІТ-інцидентами, що дозволяють ефективно ідентифікувати, оцінювати та управляти ризиками, пов'язаними з ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури (ОКІІ). Визначено переваги та недоліки цих методів, а також можливості їх інтеграції для підвищення рівня захищеності КІ.

У другому розділі дисертації було удосконалено метод визначення рівня захищеності ОКІІ шляхом використання нових індикаторів ІТ-безпеки та рівня цифрової трансформації. Використання нових індикаторів дозволяє детальніше оцінити стан безпеки, аналіз цифрової трансформації допомагає виявити слабкі місця та потенційні ризики, а розроблені рекомендації щодо

оптимізації захисту об'єктів КІІ сприяють більш точному визначенню стану їх захищеності та ефективному управлінню захистом від ІТ-інцидентів.

У третьому розділі було удосконалено метод визначення пріоритетів ІТ-інцидентів шляхом представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації. Також було розроблено метод оцінювання ІТ-загроз, який, завдяки синтезу методів багатокритеріального прийняття рішень, моделювання загроз та функції перспективної цінності, 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 та інші. Це дозволило верифікувати розроблені у роботі методи управління ІТ-інцидентами на ОКІІ.

Основні висновки містять отримані у роботі наукові і практичні результати та відповідають заявленій меті і завданням дослідження.

Наукова новизна дисертаційної роботи

— **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.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується аргументованими результатами досліджень, співставленням з результатами математичного і програмного моделювання, а також їх верифікацією через автоматизацію процесів застосування розроблених методів управління ІТ-інцидентами.

Практичне значення одержаних результатів

1. 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.

2. 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.

3. 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.

4. Теоретичні результати дисертації та результати експериментальних досліджень впроваджені і використовуються у науково-дослідній діяльності НДІ 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).

Апробація результатів дисертації

Основні результати дисертаційної роботи були представлені та обговорені на таких міжнародних науково-технічних та науково-практичних

конференціях: «12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (м. Дортмунд, 2023), «1st International Workshop on Social Communication and Information Activity in Digital Humanities» (м. Львів, 2022), «VIII International conference “Information Technology and Implementation» (м. Київ, 2021), «The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security» (м. Хмельницький, 2022), «Перспективні напрямки захисту інформації», (м. Одеса, 2021).

Публікації

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.

Зауваження по роботі

1. Розроблений автором у другому розділі метод потребує більш чіткого визначення критеріїв оцінки ефективності рекомендацій щодо оптимізації захисту ОКП. Зокрема, необхідно уточнити, які кількісні або якісні показники можна використовувати для визначення «оптимального» або «достатнього» рівня захисту, а також для оцінки результатів впровадження рекомендацій. Більш чітке визначення критеріїв оцінки зробить рекомендації більш практичними та корисними для потенційних користувачів методу.
2. Метод визначення пріоритетів ІТ-інцидентів, запропонований у третьому розділі роботи, базується на використанні методу попарних порівнянь та може бути суб'єктивним та залежним від експертних оцінок. Це може призвести до неточних або помилкових визначень пріоритетів, особливо якщо експерти мають різні погляди або недостатню кількість вхідної інформації. Крім того, розроблений метод фокусується на статичній оцінці пріоритетів ІТ-інцидентів, не враховуючи динамічний характер ІТ-загроз.
3. На рис. 3.1. зображена схема реалізації методу визначення пріоритетів ІТ-загроз, проте на схемі відсутнє відображення вхідних та вихідних даних, що дещо ускладнює розуміння процесу роботи методу.

4. У четвертому розділі, при верифікації методу управління ІТ-загрозами, наведено вагові коефіцієнти для критеріїв оцінки загроз, але їх обґрунтування не є достатньо переконливим. На мою думку, варто було б провести більш детальний аналіз та аргументування вибору коефіцієнтів, можливо, з використанням експертних оцінок або статистичних даних.

Відзначені зауваження не ставлять під сумнів основні наукові та практичні результати і суттєво не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок

Дисертаційна робота Положенцева Артема Анатолійовича представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково-технічні результати, які дозволяють розвинути методи та засоби управління ІТ-інцидентами, що можуть бути використані відповідними органами для ефективного оцінювання стану захищеності сектору/підсектору критичної інформаційної інфраструктури, або управління ІТ-загрозами.

Вважаю, що дана дисертація відповідає вимогам до дисертаційного дослідження на здобуття ступеня доктора філософії, наведеним у Постанові Кабінету Міністрів України №4 від 12.01.2022 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії».

Дисертаційна робота може бути представлена для офіційного захисту у разовій спеціалізованій вченій раді, а її автор, Положенцев Артем Анатолійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», галузі знань 12 «Інформаційні технології».

РЕЦЕНЗЕНТ

доктор технічних наук, професор,
завідувач кафедри комп'ютерних
інформаційних технологій

Національного авіаційного університету

«13» 08 2024 року

А.Савченко

Аліна САВЧЕНКО



Вн. Лавр. Керменко