

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

ВІДГУК

офіційного опонента Смірнова Олексія Анатолійовича

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 галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертації

Дисертаційна робота Положенцева Артема Анатолійовича є актуальною у контексті сучасних викликів та загроз для критичної інформаційної інфраструктури. Управління ІТ-інцидентами та захист критичної інфраструктури є ключовими аспектами забезпечення національної безпеки і стабільності інформаційних систем.

Важливість дослідження зумовлена необхідністю створення ефективних методів для управління та пріоритизації ІТ-загроз, що дозволить оптимально розподіляти ресурси для їх нейтралізації. Сучасні методи оцінювання стану ІТ-систем повинні враховувати не лише технічні аспекти, але й рівень цифрової трансформації, а також бути адаптованими до постійно змінюваного ландшафту загроз.

Дисертаційна робота сприяє розвитку теоретичних і практичних знань у сфері управління ІТ-інцидентами і захисту критичної інфраструктури, що є надзвичайно важливим у контексті сучасних загроз та викликів забезпечення безпеки держави у інформаційному просторі.

Результати дослідження мають практичне значення для реалізації ефективних заходів безпеки, що допоможе організаціям і державним установам краще реагувати на ІТ-загрози і покращити захист критичної інформаційної інфраструктури.

Дисертаційна робота безпосередньо пов'язана з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2024–2028 роки», виконана в межах наукового напряму «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, 2023-2024 рр.).

2. 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 детальний аналіз існуючих методологій і стандартів у сфері ІТ-безпеки. Досліджено та систематизовано сучасні підходи до оцінювання стану захищеності об'єктів критичної інфраструктури, що дозволило виявити основні недоліки існуючих методів. Виявлено області, які потребують вдосконалення, зокрема, в аспектах адаптації до новітніх загроз та вимог цифрової трансформації.

У **другому розділі** було розроблено і вдосконалено метод визначення рівня захищеності об'єктів критичної інформаційної інфраструктури шляхом впровадження нових індикаторів ІТ-безпеки та рівня цифрової трансформації. Створено рекомендації для покращення управління захистом від ІТ-інцидентів. Окрім того, розроблено спеціалізоване програмне забезпечення, яке автоматизує процес визначення стану захищеності об'єктів критичної інформаційної інфраструктури, що підвищує ефективність та точність оцінювання.

У **третьому розділі** запропоновано удосконалений метод для визначення пріоритетів ІТ-інцидентів, який включає створення ієрархічних структур елементів потенційних загроз і розрахунок ймовірності їх реалізації. Розроблені ієрархічні структури дозволяють систематизувати та класифікувати потенційні ІТ-інциденти. Крім цього, було розроблено метод оцінювання ІТ-загроз для ідентифікації, оцінки та пріоритизації ІТ-загроз з метою оптимального розподілу ресурсів захисту критичної інформаційної інфраструктури. Окрім того, створено

спеціалізоване програмне забезпечення, яке дозволяє ефективно визначати пріоритети ІТ-загроз, що підвищує точність і оперативність процесу управління загрозами.

У **четвертому розділі** було проведено верифікацію розроблених методів для підтвердження їх ефективності та придатності до практичного застосування. Виконано тестування в реальних умовах, що підтвердило практичну ефективність методів. Виявлено потенційні напрямки для подальшого вдосконалення.

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

3. 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.

4. 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 та застосування розробленого програмного забезпечення.

5. 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).

6. Апробація результатів дисертації

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).

7. Публікації здобувача

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.

8. Недоліки дисертаційного дослідження

На мою думку, робота має наступні недоліки:

1. Розроблений у розділі II метод визначення стану захищеності об'єктів критичної інформаційної інфраструктури може не враховувати специфічні умови та особливості кожного об'єкту критичної інфраструктури. Наприклад, різні об'єкти можуть мати різні рівні розвитку цифрових технологій та IT-безпеки, що вимагає адаптивного підходу до оцінювання, який не завжди може бути реалізований в рамках запропонованого методу.

2. Розділ III зосереджений на технічних аспектах визначення пріоритетів IT-інцидентів, але мало уваги приділено людському фактору та організаційним аспектам. Наприклад, недостатньо розглянуто питання навчання персоналу, розробки внутрішніх політик та процедур, які є критично важливими для ефективного управління IT-інцидентами.

3. Застосування методу попарних порівнянь (у складі методу визначення пріоритетів IT-інцидентів) вимагає значних обчислювальних ресурсів, особливо при збільшенні кількості загроз і категорій. Це може призвести до значного збільшення часу та ресурсів, необхідних для обробки вхідних даних. Крім цього, математична складність алгоритмів і методів, які використовуються для обчислення пріоритетів може бути важко зрозумілою для кінцевих користувачів, що ускладнює інтерпретацію результатів і прийняття управлінських рішень.

4. У розділі III, розроблений метод управління IT-загрозами не враховує всі можливі загрози, особливо нові або нестандартні загрози, які можуть з'явитися внаслідок швидкого розвитку технологій або змін у середовищі застосування. Це може призвести до неповного або недостатньо актуального аналізу, що може вплинути на ефективність управління ризиками.

5. У розділі IV, при проведенні експериментального дослідження запропонованого методу оцінювання рівня захищеності об'єктів критичної інфраструктури, додаткові експерименти для верифікації роботи методу (рис. 4.4 –

рис. 4.6) недостатньо якісно і детально описані. Це ускладнює оцінку точності та достовірності отриманих результатів.

Проте, зазначені недоліки не знижують значущість основних наукових і практичних результатів і не впливають на загальну позитивну оцінку дисертаційної роботи.

9. Висновок

Дисертаційна робота Положенцева Артема Анатолійовича представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково-технічні результати з розроблення методів управління ІТ-інцидентами об'єктів критичної інформаційної інфраструктури. Проведено аналіз сучасних підходів до оцінювання стану захищеності об'єктів критичної інформаційної інфраструктури, удосконалено метод визначення рівня їх захищеності, створено рекомендації та спеціалізоване програмне забезпечення для автоматизації цих процесів. Удосконалено метод пріоритизації ІТ-інцидентів, розроблено метод оцінювання ІТ-загроз, а також спеціалізоване програмне забезпечення для їх ідентифікації та пріоритизації. Верифікація розроблених методів підтвердила їх ефективність і практичну застосовність, результати впроваджено в науково-дослідній діяльності та практичній підготовці фахівців.

Вважаю, що дана дисертація відповідає вимогам до дисертаційного дослідження на здобуття ступеня доктора філософії, наведеним у Постанові Кабінету Міністрів України №44 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.

Офіційний опонент:

доктор технічних наук, професор,
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор



Олексій СМІРНОВ

Підпис доктора технічних наук, професора, завідувача кафедрою кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету Смірнова Олексія Анатолійовича засвідчую:

Проректор з наукової роботи та міжнародних зв'язків

Цentrальноукраїнського національного технічного університету

Кандидат технічних наук, доцент



Андрій ТИХИЙ

« 12 » серпня 2024 року