ВІДГУК

офіційного опонента
кандидата технічних наук Цуркана Василя Васильовича
на дисертацію Сидоренко Вікторії Миколаївни
«Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі»,
представлену на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 21.05.01 – інформаційна безпека держави

Актуальність теми дисертаційного дослідження. Збільшення обсягів інформації, яка обробляється, а також концентрації засобів та ресурсів для захисту електронних інфраструктур різних типів зумовили необхідність ранжування інфраструктурних об'єктів, виділення найважливіших з них та появи поняття «критична інфраструктура». Зазвичай, до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення мегаполісів, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади. Водночас особливої уваги потребує транспортна галузь, так як є одним з важливіших секторів критичної інфраструктури держави. Несанкціоноване втручання в роботу транспортної системи може призвести до значних фінансових збитків, людських жертв та руйнування загальнодержавної інфраструктури. У рамках останньої, особливої уваги заслуговує авіаційна галузь (цивільна авіація), з огляду на необхідність забезпечення безперервної комунікації та взаємодії між стаціонарними наземними системами і рухомими повітряними суднами. Таким чином, важливим завданням стає визначення (ідентифікація) об'єктів, які є найбільш критичними, оцінювання рівня їх важливості для забезпечення постійного функціонування, запобігання виникненню переривань роботи та збоїв в автоматизованих системах, що забезпечують їх роботу.

Дисертаційна робота Сидоренко Вікторії Миколаївни присвячена *розв'язанню актуального науково-технічного завдання,* яке має теоретичне і практичне значення. Зокрема, направлена на розроблення методів ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі.

До того ж актуальність тематики дисертаційної роботи підтверджується цілою низкою науково дослідних та дослідно-конструкторських робіт, з якими вона тісно пов'язана, і в яких дисертант приймав участь як виконавець: НДР НАУ «Квантово-криптографічні методи захисту критичної інформаційної інфраструктури держави» (д.р. № 0111U000171), НДР ІПМЕ ім. Г.Є. Пухова НАН України «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики», шифр «МОД-Д» (д.р. № 0114U002361), а також у звіті ДКР Державного науково-дослідного інституту спеціального зв'язку та захисту інформації, шифр «Інфраструктура» (д.р. № 0114U000038д).

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій. Ступінь обґрунтованості наукових положень, висновків і рекомендацій у дисертації обумовлена коректністю застосування сучасних методів теорії захисту інформації (для визначення метрик у методі визначення рівня кібербезпеки), теорії множин (для формалізації етапів методу визначення рівня важливості критичних авіаційних інформаційних систем); системного та структурного аналізу (визначення відношень q-зв'язків кіберзагроз та критичних авіаційних інформаційних систем, ієрархічного представлення систем в уніфікованій моделі); теорії графів (для відображення елементів критичної інформаційної інфраструктури та їх функціональних процесів у методі ідентифікації об'єктів критичної інформаційної інфраструктури). Достовірність наукових положень та висновків підтверджено застосуванням розроблених методик та програмного засобу для проведення експериментів з метою підтвердження адекватності моделей і методів, що пропонуються в дисертаційній роботі.

Ідентичність змісту автореферату й основних положень дисертації. Автореферат і дисертація Сидоренко В.М., відповідно до вимог МОН України, розміщено в електронному репозитарії Національного авіаційного університету за місяць до захисту (26 квітня 2018 року) http://er.nau.edu.ua/handle/NAU/33987.

Проаналізувавши автореферат і дисертацію здобувача, можна зробити висновки, що в авторефераті з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертаційної роботи. Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 167 сторінок основного тексту, 54 рисунки, 49 таблиць, 16 сторінок додатків. Список використаних джерел містить 151 найменування і займає 16 сторінок. Загальний обсяг роботи 199 сторінок.

Результати дисертації Сидоренко В.М. викладено послідовно та структуровано відповідно до поставлених задач дослідження.

У вступі автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета і задачі дослідження, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробування та впровадження.

У першому розділі дисертації проаналізовано наукову літературу за темою дисертаційної роботи. За результатами проведеного аналізу встановлено, що відомі підходи до ідентифікації об'єктів критичної інфраструктури орієнтовані, як правило, на економічні, екологічні, техногенні та інші системи безпеки держави і переважна їх більшість не враховує повної множини параметрів та особливостей інформаційної складової критичної інфраструктури. Крім того, за результатами аналізу було виділено низку методів оцінювання критичності інформаційно-телекомунікаційних систем як об'єктів критичної інформаційної інфраструктури держави; встановлено, що вибір методів розрахунку критичності залежить від конкретних обставин: масштабу і складу інформаційно-телекомунікаційних систем, інформації, що обробляється у цій системі, складу і використовуваних засобів безпеки, наявності кваліфікованих експертів тощо.

Також визначено, що найбільш універсальним серед проаналізованих методів є метод FMECA, у якому кожен вид відмови (порушення безперервної роботи) ранжується з урахуванням двох складових критичності – ймовірності та тяжкості наслідків відмови.

Другий розділ присвячений формуванню переліку об'єктів критичної інформаційної інфраструктури держави шляхом розроблення уніфікованої моделі даних та методу ідентифікації об'єктів критичної інформаційної інфраструктури в авіаційній галузі. Зазначена модель дозволяє формалізувати процес формування переліку таких об'єктів та визначити їх зв'язність (співвідношення q-зв'язків множин кіберзагроз та критичних авіаційних інформаційних систем), а розроблений метод ідентифікації об'єктів критичної інформаційної інфраструктури дає можливість ідентифікувати елементи галузі критичної інформаційної інфраструктури, визначати їх взаємовплив та вплив на функціональні операції критичних авіаційних інформаційних систем.

У третьому розділі наведено розроблені методи визначення рівня важливості критичної інформаційної інфраструктури та рівня її кібербезпеки. Запропонований метод визначення рівня важливості критичної інформаційної інфраструктури в авіаційній галузі дозволяє оцінювати критичність об'єктів та ранжувати їх для адекватного застосування коригувальних заходів (превентивних та контрзаходів у процесі забезпечення кібербезпеки). Інший метод, орієнтований на визначення рівня кібербезпеки галузі критичної інформаційної інфраструктури держави, дає можливість розрахувати кількісні параметри, які характеризують захищеність певної галузі критичної інфраструктури, регіону, держави тощо. Зазначений метод є корисним як в контексті кібербезпеки системи критичної інфраструктури, так і для проведення аудиту кібербезпеки відповідно до чинних стандартів.

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням розроблених методів. Розроблено відповідну методику проведення експериментального дослідження, визначено мету та задачі експериментів, вхідні та вихідні параметри, гіпотезу і критерії дослідження, достатність експериментальних об'єктів та послідовність необхідних дій. На основі запропонованої у другому розділі дисертації уніфікованої моделі даних було розроблено методику, за допомогою якої сформовано перелік об'єктів критичної інформаційної інфраструктури для авіаційної галузі, у результаті чого (при $l = 4$) виділено 3 множини категорій, 17 множин систем, 97 множин підсистем та 125 підсистем критичних авіаційних інформаційних систем. Також, було проведено експериментальне дослідження методу ідентифікації об'єктів критичної інформаційної інфраструктури в авіаційній галузі з використанням розробленого програмного застосунку. Крім того, визначено найбільш критичну серед критичних авіаційних інформаційних систем, що досліджуються.

У додатках вміщено акти впровадження результатів дисертаційної роботи та коди розробленого програмного забезпечення.

Для основних положень дисертації та змісту автореферату характерна повна ідентичність. Крім того, варто зауважити, що дисертаційна робота оформлена відповідно до чинних вимог 2017 року.

За своїм змістом та отриманими результатами дисертаційна робота відповідає формулі та пунктам напрямів досліджень паспорту спеціальності 21.05.01 – інформаційна безпека держави.

Наукове та практичне значення отриманих результатів роботи. Наукова новизна отриманих результатів роботи полягає у наступному:

– вперше розроблено уніфіковану модель даних, яка за рахунок мультирівневої деталізації критичних авіаційних інформаційних систем, ієрархічного представлення множин, що характеризують системи та їх компоненти, а також введення матриці інцедентності кібербезпеки критичної інфраструктури, її симплексних комплексів та Q-аналізу, дозволяє формалізувати процес формування переліку об'єктів критичної інформаційної інфраструктури держави та визначити їх зв'язність (співвідношення q-зв'язків множин кіберзагроз та критичних авіаційних інформаційних систем);

– вперше розроблено метод ідентифікації, який за рахунок графоаналітичного відображення елементів критичної інфраструктури і їх функціональних процесів, формування можливих чинників і функцій впливу, а також матриці впливу елементів інфраструктури на функціональні операції, дає можливість визначити (ідентифікувати) елементи галузі критичної інформаційної інфраструктури, їх взаємовплив та вплив на функціональні операції критичної авіаційної інформаційної системи;

– удосконалено метод визначення рівня важливості, який за рахунок ієрархічного відображення множин, що характеризують критичні авіаційні інформаційні системи різних рівнів деталізації, їх функції, порушення безперервності роботи, відповідні ознаки і наслідки, а також побудови тривимірної матриці критичності, причинно-наслідкової діаграми Ісікави і узгодження вагових коефіцієнтів критичності, дозволяє оцінювати критичність об'єктів критичної інформаційної інфраструктури авіаційної галузі та ранжувати їх для адекватного застосування коригувальних заходів;

– отримав подальшого розвитку метод оцінювання рівня кібербезпеки, який за рахунок представлення множин метрик кібербезпеки і метрик розвитку та впровадження інформаційно-комунікаційних технологій у вигляді зв'язаних списків, а також обчислення індексу кібербезпеки та відповідних метрик, дає можливість розрахувати кількісні параметри, які характеризують захищеність певної галузі чи критичної інформаційної інфраструктури держави в цілому.

Практичне значення результатів дисертації полягає у такому:

– створено методику, яка дозволяє формувати перелік об'єктів критичної інформаційної інфраструктури певної галузі та на загальнодержавному рівні;

– реалізовано програмний застосунок, який можна використовувати для ідентифікації елементів критичної інформаційної інфраструктури та визначення їх впливу на функціональні операції;

– створено методику визначення рівня важливості об'єктів критичної інформаційної інфраструктури, яка дає змогу кількісно оцінювати рівень важливості критичних авіаційних інформаційних систем різних категорій та їх компонентів;

– результати дисертації впроваджені і використовуються у діяльності ТОВ «Акссонсофт», Державного науково-дослідного інституту спеціального зв'язку та захисту інформації, Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, а також у навчальному процесі кафедри безпеки інформаційних технологій НАУ для підвищення ефективності підготовки фахівців з кібербезпеки.

Повнота викладу результатів дисертаційної роботи в опублікованих працях та їх апробація. Результати виконання досліджень опубліковано у 26 наукових працях, у тому числі: 1 розділ у колективній монографії закордоном англійською мовою, 10 наукових статей (3 – у закордонних рецензованих виданнях (1 з яких входить до бази даних Scopus), 7 – у вітчизняних фахових наукових журналах), а також 15 матеріалів і тез доповідей на конференціях.

Дисертація Сидоренко В.М. має достатній рівень апробації на наукових конференціях і семінарах в Україні та закордоном – серед найвагоміших наукових заходів я відзначив би такі: МНТК «ITSEC: Безпека інформаційних технологій» (Київ, 2016 р.), МНПК «Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК)» (Київ, 2014 – 2016 рр.), ВНПК «Інноваційний потенціал світової науки — XXI сторіччя» (Запоріжжя, 2013 р.), НПК «Механізми управління безпекою підприємств в сучасних умовах господарювання» (Київ, 2013 р.), НПК «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2014 р.), Всесвітній конгрес «Авіація у XXI столітті» – «Безпека в авіації та космічні технології» (Київ, 2014 р.), ВНПК «Проблеми і перспективи розвитку авіації та космонавтики» (Київ, 2015 р.), НПК «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Київ, 2016 – 2018 рр.), МНК «Украйна – България – Европейски Съюз: съвременно състояние и перспективи» (Варна, 2014 р.), Міжвідомчий міжрегіональний семінар Наукової ради НАН України «Технічні засоби захисту інформації» (Київ, 2017 р.).

Зауваження та недоліки. Незважаючи на достатній рівень виконаних наукових досліджень до дисертаційної роботи є такі зауваження:

1. Недостатність описання варіантів представлення категорій систем у певній галузі критичної інфраструктури. Зокрема, доцільно деталізувати описання обумовленості представлення множин варіантами: з індексом, з індексом імені об'єкту та іменем об'єкту.

2. Недостатність описання вибору діаграми Ісікави для складання переліку коригувальних заходів. Зокрема, доцільно деталізувати описання обумовленості виявлення причинно-наслідкових закономірностей виникнення переривань роботи D_i компонента C_i за діаграмою Ісікави.

3. Недостатність описання вибору технологічної платформи 1С для проведення експериментальних досліджень методу ідентифікації об'єктів критичної інформаційної інфраструктури авіаційної галузі.

4. Наявність окремих стилістичних і орфографічних помилок. Наприклад: пропущене слово «інтересів» у словосполученні «…життєво важливих інтересів…» (с. 21, табл. 1.1).

Висновки. Зазначені у відгуку зауваження не зменшують теоретичної та практичної цінності дисертаційної роботи Сидоренко Вікторії Миколаївни. Загалом, вона характеризується внутрішньою єдністю, виконана на належному науковому рівні та є завершеною працею. У ній отримано нові науково обґрунтовані результати, що в сукупності вирішують науково-технічне завдання зі розроблення методів ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі.

Дисертаційна робота Сидоренко В.М. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 № 567 (зі змінами). Тому її автор заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави.

Офіційний опонент
доцент кафедри кібербезпеки та застосування
автоматизованих інформаційних систем та технологій
ІСЗЗІ КПІ ім. Ігоря Сікорського
кандидат технічних наук В.В. Цуркан

Підпис кандидата технічних наук Цуркана Василя Васильовича засвідчую.

Начальник відділу кадрової роботи
ІСЗЗІ КПІ ім. Ігоря Сікорського В.М. Грищук