Голові спеціалізованої вченої
ради Д 26.062.17
Національного авіаційного університету
03680, м. Київ, проспект
Космонавта Комарова, 1

ВІДГУК
офіційного опонента

завідувача кафедри комп'ютерних та інформаційно-вимірювальних технологій
Одеської державної академії технічного регулювання та якості,
доктора технічних наук, доцента
Казакової Надії Феліксівни,
на дисертацію Сидоренко Вікторії Миколаївни
на тему «Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі»,
що представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 «Інформаційна безпека держави»

Актуальність теми дисертаційного дослідження

Розвиток новітніх інформаційно-комунікаційних технологій (ІКТ) спричинив феноменальну залежність суспільства від сервісів, які надають різноманітні галузі інфраструктури. Якість та доступність таких послуг є одними з головних показників розвитку інфраструктури держави, а забезпечення їх захисту (кібербезпеки ((КБ) та стабільного функціонування є найважливішою і обов'язковою складовою національної безпеки розвинених держав. 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 базового поняття «критична інфраструктура» (КІ). У більшості розвинених держав світу КІ є чітко визначеною і, як правило, включає в себе нафто- та газопроводи, канали швидкісного та урядового зв'язку, системи життєзабезпечення суспільства, військово-промисловий комплекс, енергетичну та транспортну систему тощо. 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. З огляду на це, важливим завданням стає визначення (ідентифікація) об'єктів, які є найбільш критичними, оцінювання рівня їх важливості для забезпечення постійного функціонування, запобігання виникненню переривань роботи (порушень

безперервності функціонування) та збоїв в автоматизованих системах (так званих, критичних авіаційних інформаційних системах – КАІС), що забезпечують їх роботу. Саме з цих позицій, дисертаційна робота Сидоренко Вікторії Миколаївни присвячена *розв'язанню актуального науково-технічного завдання,* яке має теоретичне і практичне значення, зокрема спрямована на розроблення методів ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Викладені наукові положення, методики, висновки і рекомендації є повністю обґрунтованими, а достовірність запропонованих дисертантом гіпотез і математичних моделей підтверджується відповідними експериментальними даними та результатами верифікації запропонованих моделей і методів. Отримані, під час експериментів, дані відповідають теоретичним висновкам роботи і повністю підтверджують їх. До того ж, коректно застосовані методи теорії захисту інформації, теорії множин, системного та структурного аналізу та теорії графів.

Робота має чітку послідовність постановки задач та отриманих рішень, достатню доказову базу та аргументованість результатів. Використано сучасний математичний апарат для реалізації сформованої мети, як розвиток теоретичних основ і дослідження запропонованих рішень.

Обрані здобувачем початкові передумови і рішення, представлені у вигляді математичних моделей, алгоритмів і структурних схем, не викликають сумнівів в коректності визначення, обґрунтованості висновків і рекомендацій.

Порівняльні оцінки запропонованих автором нових рішень щодо результатів, які отримані провідними вченими та дослідниками в галузі, достатньо аргументовані та відповідають списку приведених першоджерел.

Висновки та рекомендації, які сформульовані в дисертаційній роботі, враховують сутність та актуальність науково-технічної задачі роботи та її мету. Представляється, що вони є придатними для практичного використання.

Ідентичність змісту автореферату й основних положень дисертації

Проаналізувавши автореферат і дисертацію здобувача, можна зробити висновки, що в авторефераті з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертаційної роботи. Для основних положень дисертації та змісту автореферату характерна повна ідентичність. Крім того, варто зауважити, що дисертаційна робота оформлена відповідно до чинних вимог 2017 року.

Автореферат і дисертація Сидоренко В.М., відповідно до вимог МОН України, були розміщені в електронному депозитарії Національного авіаційного

університету за місяць до захисту (26 квітня 2018 року) http://er.nau.edu.ua/handle/NAU/33987

Стиль викладення автореферату в цілому забезпечує повноту та доступність сприйняття. Наукові завдання дослідження та шляхи їх вирішення викладені чітко і лаконічно. З тексту зрозуміла наукова і практична значущість роботи та особистий внесок здобувача.

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.

Зміст роботи відповідає поставленому науковому завданню та сформульованим задачам. Їх рішення є суттю та змістом виконаних досліджень, які відповідають паспорту спеціальності 21.05.01 – «Інформаційна безпека держави».

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 апробації 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 КІ 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 КІ (критичної інформаційної інфраструктури – КІІ). Крім того, за результатами аналізу було виділено низку методів оцінювання критичності ІТС як об'єктів КІІ держави; встановлено, що вибір методів розрахунку критичності залежить від конкретних обставин: масштабу і складу ІТС, 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 КІІ держави шляхом розроблення уніфікованої моделі даних та методу ідентифікації об'єктів КІІ в авіаційній галузі. Зазначена модель дозволяє формалізувати процес формування переліку об'єктів КІІ держави та визначити їх зв'язність (співвідношення q-зв'язків множин кіберзагроз та КАІС), а розроблений метод ідентифікації об'єктів КІІ дає можливість ідентифікувати елементи галузі КІІ, визначати їх взаємовплив та вплив на функціональні операції КАІС.

У **третьому розділі** наведено розроблення методів визначення рівня важливості КІІ та рівня КБ галузі КІІ держави. Запропонований метод визначення рівня важливості КІІ в авіаційній галузі дозволяє оцінювати критичність об'єктів КІІ

та ранжувати їх для адекватного застосування коригувальних заходів (превентивних та контрзаходів у процесі забезпечення КБ). Інший метод, орієнтований на визначення рівня КБ галузі КІІ держави, дає можливість розрахувати кількісні параметри, які характеризують захищеність певної галузі КІ, регіону, держави тощо. Зазначений метод є корисним як в контексті КБ в системи КІ, 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, обґрунтовано доцільність вибору бази експериментів, 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 КІІ для авіаційної галузі, у результаті чого (при l=4) виділено 3 множини категорій, 17 множин систем, 97 множин підсистем та 125 підсистем КАІС. Також, було проведено експериментальне дослідження методу ідентифікації об'єктів КІІ в авіаційній галузі з використанням розробленого програмного застосунку. Крім того, визначено найбільш критичну серед досліджуваних КАІС, а, використавши останній запропонований метод, встановлено що для авіаційної галузі рівень кібербезпеки становить 7%.

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

Наукова цінність 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.

Основні наукові положення дисертації 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.

Крім того, зазначені положення дисертаційної роботи пройшли обов'язкову і достатню апробацію на наукових конференціях та семінарах в Україні і закордоном.

Значення результатів для практики

Отримані в дисертаційній роботі результати можуть бути використані відповідними державними органами для формування переліку об'єктів КІІ з метою застосування адекватних механізмів захисту. Практична цінність роботи полягає у такому:

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

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

– створено методику визначення рівня важливості об'єктів КІІ, яка дає змогу кількісно оцінювати рівень важливості КАІС різних категорій та їх компонентів;

– результати дисертації впроваджені і використовуються у діяльності ТОВ «Акссонсофт», ДержНДІ Спецзв'язку, ІПМЕ ім. Г.Є. Пухова НАН України, а також у навчальному процесі кафедри безпеки інформаційних технологій НАУ для підвищення ефективності підготовки фахівців з КБ.

Зауваження та недоліки

1. Перший науковий результат здобувача, а саме уніфікована модель даних, яка дозволяє формалізувати процес формування переліку об'єктів критичної інформаційної інфраструктури держави та визначити їх зв'язність (стор. 58-62 дисертації). Проте, не зрозумілим залишається співвідношення зв'язності в контексті визначених категорій кібератак на критичні авіаційні інформаційні системи. Про що свідчить збільшення зв'язності – про більший чи менший рівень захищеності? А також, не зрозуміло як ці результати використовуються у подальшому для оцінювання критичності.

2. На сторінці 88 роботи автор пропонує матрицю інцедентності (вираз 2.10), проте з її математичного опису не зрозуміло і дисертант не обґрунтовує чому елементи матриці приймають значення виключно «0» та «1». Як бути, наприклад, у випадку, якщо певна загроза реалізована частково – можливо було б доцільно врахувати і такі випадки шляхом розширення (деталізації) шкали, експертного оцінювання тощо.

3. На стор. 109 дисертаційної роботи здобувач наводить схему відображення розробленого методу визначення рівня важливості об'єктів критичної інформаційної інфраструктури (рис. 3.1). Проте, на мою думку, не зовсім обґрунтованою є зазначена послідовність етапів методу – для прикладу, етап 7 міг бути другим або третім, так як усі вхідні дані є доступними до реалізації попередніх 6 етапів.

4. Назва четвертого розділу «Експериментальне дослідження розроблених методів оцінювання стану кібербезпеки», на мій погляд, є не зовсім вдалою. У цьому розділі, крім методу оцінювання стану кібербезпеки, автор також досліджує і інші два методи (ідентифікації та оцінювання критичності об'єктів критичної інфраструктури), тому варто було б назву сформулювати більш загальною.

5. Дисертант пропонує методику, за допомогою якої сформовано перелік об'єктів критичної інфраструктури авіаційної галузі, у результаті чого, загалом виділено ідентифіковано більше 200 критичних авіаційних інформаційних систем різного рівня деталізації. Проте, наведений експеримент стосується лише трьох таких систем, які хоч і відносяться до принципово різних категорій, проте не дають змогу говорити про рівень критичності усіх ідентифікованих систем. Було б добре, на основі теоретичних результатів здобувача у подальшому розробити автоматизовану систему, що дозволила б і ідентифікувати об'єкти критичної інфраструктури і визначати їх рівень критичності.

6. Деякі рисунки, наведені дисертантом, є низької якості, що робить їх неінформативними і незрозумілими (наприклад, рис.1.6 на стор. 46, рис. 2.4 на стор. 73, рис.2.8 на стор. 95 тощо).

7. Тексти дисертаційної роботи та автореферату містять велику кількість скорочень, абревіатур, спеціальних позначень та формул, що значно ускладнює загальний процес оцінки роботи при її читанні. До того ж, не всі абревіатури та скорочення пояснені у відповідному переліку, що наведений на стор. 11 дисертації.

Слід зазначити, що наведені зауваження та недоліки не є принциповими щодо вирішення науково-прикладного завдання, яке є суттю дослідження, суттєво не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової цінності та практичної значимості.

Висновки

В цілому, дисертаційна робота Сидоренко Вікторії Миколаївни є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку теорії й практики кібербезпеки та захисту інформації. Усі одержані наукові результати можуть застосовуватися у різних галузях критичної інфраструктури держави для формування та забезпечення системи кібербезпеки. Отже, вважаю, що дисертаційна робота «Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі» повністю відповідає чинним вимогам МОН України, зокрема «Порядку присудження наукових ступенів», затвердженого Постановою КМУ від 24.07.2013 р. № 567 (із змінами, внесеними згідно з Постановами КМУ № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р. № 567 від 27.07.2016 р.) та відповідає паспорту спеціальності 21.05.01 – «Інформаційна безпека держави», а її автор Сидоренко Вікторія Миколаївна гідний присудження наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – «Інформаційна безпека держави».

Офіційний опонент
завідувач кафедри комп'ютерних та
інформаційно-вимірювальних технологій
Одеської державної академія технічного регулювання та якості
доктор технічних наук, доцент Н.Ф. Казакова

Підпис Казакової Н. Ф. ЗАСВІДЧУЮ.
Вчений секретар С.В. Добровольська