67-72-107/2
20.05.2021

ВІДГУК

офіційного опонента

на дисертаційну роботу **Салієвої Ольги Володимирівни**

«Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання»,

подану на здобуття наукового ступеня доктора філософії за спеціальністю 125 — Кібербезпека (Галузь знань 12 — Інформаційні технології)

Актуальність теми дисертації

Динамічний розвиток процесу інформатизації сучасного суспільства зумовив не тільки підвищення ефективності усіх видів людської діяльності, але і низку небезпек, пов'язаних із впливом потенційних загроз інформаційній безпеці. Це призводить до підвищення вимог до захищеності систем захисту інформації, порушення функціонування яких може спричинити вкрай важкі наслідки.

Тому дослідження щодо підвищення рівня захищеності систем захисту інформації в умовах реалізації загроз є важливим та актуальним науковим завданням, вирішення якого можливе, зокрема, за допомогою методів статистичного аналізу. Але дані методи потребують складних розрахунків, наявності достатньо повної вхідної інформації та тривалого часу для опрацювання необхідних даних. У зв'язку з цим застосування методів когнітивного моделювання є доцільним, адже здатне вирішити вищезазначені проблеми за рахунок використання нечітких когнітивних карт, яким властива простота, наочність, гнучкість, конструктивність, адаптація до невизначеності вхідних даних, використання знань і досвіду експертів предметної області.

Зв'язок роботи із науковими програмами, планами, темами

Дисертаційна робота Салієвої О.В. виконана за планом наукових досліджень, проваджених кафедрою менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.

Науково-дослідна робота проводилась відповідно до тематики науково-дослідної роботи Вінницького національного технічного університету. Зокрема, робота над дисертацією проводилася у рамках науково-дослідних та науково-технічних робіт зі створення комплексних систем захисту інформації в автоматизованих системах: режимно-секретного органу відокремленого підрозділу «Південно-Західна електроенергетична система» приватного акціонерного товариства «Національна енергетична компанія «Укренерго»

(№5261 від 27.05.2019 р.); Хмельницького зонального відділу Військової служби правопорядку (№5267 від 11.07.2019 р.); Головного управління Пенсійного фонду України у Вінницькій області (№5284 від 27.02.2020 р.).

Ступінь обґрунтованості, наукових положень та висновків, їх достовірність

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою й базується на детальному аналізі інформаційних джерел за даною проблемою, чіткій постановці мети і задач дисертації, використанні сучасних методів дослідження, а також у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих моделей систем захисту інформації, що циркулює в інформаційних системах, забезпечується коректним використанням апарату когнітивного моделювання і прийнятих допущень. Адекватність розроблених моделей підтверджується результатами експериментальних досліджень.

Достовірність отриманих результатів впливу загроз на рівень захищеності систем захисту інформації, що циркулює в інформаційних системах, підтверджено на основі множинного регресійного аналізу. Крім того, за допомогою методів симпліціального аналізу підтверджено результати структурного аналізу розробленої когнітивної моделі для дослідження рівня захищеності об'єкта критичної інфраструктури.

Тому можна стверджувати, що висновки та практичні рішення, наведені у роботі, коректні, достатньо обґрунтовані та заслуговують на увагу й можуть бути рекомендовані до використання для підвищенні рівня захищеності систем захисту інформації, що циркулює в інформаційних системах.

Важливість результатів, що отримані в роботі для науки та практичного використання

Одержані наукові результати є важливими для підвищення рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, створенням функціональних когнітивних моделей для оцінювання рівня їхньої захищеності та програмних засобів реалізації цих моделей.

Основними науково-обґрунтованими результатами є:

вперше

– запропоновано модель оцінювання рівня захищеності об'єкта критичної інфраструктури на основі когнітивного підходу, який дозволяє спростити необхідні розрахунки та зменшити час обробки вхідної інформації,

наглядно представити досліджувану систему, підвищити масштабованість моделі, визначити найвагоміші фактори, провести сценарне моделювання, в результаті якого визначено, що рівень захищеності об'єкта критичної інфраструктури підвищиться на 2% при максимально позитивному впливі найвагоміших факторів;

– запропоновано модель оцінювання рівня захищеності системи захисту інформації на основі когнітивного підходу, який надає можливість покращити наочність представлення даних, використовувати неповну, нечітку інформацію та суб'єктивні судження експертів предметної області, врахувати як кількісні так і якісні фактори, що впливають на захищеність системи захисту інформації, виявити найвагоміші фактори, провести сценарне моделювання розвитку ситуації, в результаті якого визначено, що рівень захищеності досліджуваної системи підвищиться на 19% при максимально позитивному впливі найвагоміших факторів;

удосконалено

– когнітивну модель для оцінювання рівня захищеності комп'ютерної мережі, яка більш точно відображає предметну область та надає можливість краще враховувати мінливість характеру процесів, що відбуваються у досліджуваній системі в часі, визначити найвагоміші мережеві загрози, провести сценарне моделювання розвитку ситуації, у результаті якого визначено, що рівень захищеності мережі підвищиться на 63 % при максимальному послабленні впливу найвагоміших загроз;

набув подальшого розвитку

– підхід до визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури й системи захисту інформації та допустимих витрат на її забезпечення на основі ранжування загроз із використанням теорії нечітких відношень, який надає можливість зменшити час обробки вхідної інформації та спростити проміжні розрахунки, проводити як кількісне, так і якісне оцінювання даних.

Практичне значення отриманих результатів роботи полягає у:

– розробці структури програми для реалізації оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, у вигляді семи взаємозалежних програмних модулів та їх програмної реалізації;

– розробці програмних засобів для реалізації оцінювання рівня

захищеності систем захисту інформації, що циркулює в інформаційних системах, за запропонованими когнітивними моделями;

– підтвердженні на основі регресійного аналізу достовірності впливу загроз на рівень захищеності систем захисту інформації, визначеного за результатами когнітивного моделювання;

– визначенні та порівнянні рівнів впливу загроз на захищеність об'єкта критичної інфраструктури у різні моменти часу за допомогою динамічного часового аналізу;

– формуванні множини управляючих концептів та встановлення взаємозв'язних концептів для когнітивної моделі дослідження рівня захищеності об'єкта критичної інфраструктури, що дозволить підвищити рівень захищеності досліджуваного об'єкта;

– визначенні зміни рівня захищеності системи захисту інформації, шляхом введення імпульсних впливів у концепти відповідної когнітивної карти, що надало змогу прослідкувати еволюційний розвиток системи.

Повнота висвітлення результатів в опублікованих працях, апробація роботи

Наукові положення та отримані результати достатньо повно представлені в опублікованих автором наукових працях та апробовані на науково-технічних конференціях.

Результати дисертації опубліковано у 18 наукових працях, у тому числі: 10 статей у наукових фахових виданнях України, 1 – у виданні, що індексується у Scopus, 7 – у матеріалах і тезах конференцій.

Структура дисертації цілком відповідає логіці й послідовності вирішення поставлених задач. Наукова робота складається зі вступу, чотирьох розділів, висновків, переліку використаних джерел та додатків.

У вступі обґрунтовано актуальність теми, а також наведено об'єкт, предмет і мету дослідження, положення наукової новизни і практичної цінності; визначено основні методи дослідження; надано інформацію про особистий внесок здобувача в спільних публікаціях, апробаціях на науково-технічних та науково-практичних конференціях.

У першому розділі автором виконано критичний аналіз літературних джерел, висвітлено результати попередніх досліджень, окреслено коло невирішених завдань, що потребують подальших наукових досліджень для їх практичного використання.

Проведений аналіз дозволив зробити висновки про те, що більшість з наведених методів оцінювання впливу загроз на рівень інформаційної

безпеки потребують складних розрахунків й тривалого часу для опрацювання необхідних даних. У той час, аналіз моделей розроблених на основі нечітких когнітивних карт показав, що застосування когнітивного підходу дозволяє вирішити вищезазначені питання та володіє низкою переваг. Тому даний підхід було обрано автором для розробки та аналізу моделей оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах.

У другому розділі розроблено функціональні когнітивні моделі, які дозволяють визначити найвагоміші загрози, з точки зору вивчення даної проблеми, та проаналізувати відносну зміну рівня захищеності комп'ютерної мережі, системи захисту інформації та об'єкта критичної інфраструктури при впливі даних загроз. Проведено структурно-топологічний аналіз побудованих нечітких когнітивних карт, у результаті якого визначено концепти, які мають найвищу структурну значимість та здійснено сценарне моделювання для оцінювання відносної зміни рівня захищеності досліджуваних систем при максимальному впливі цих концептів. Це дозволило визначити на скільки відсотків підвищиться рівень захищеності систем захисту інформації при найбільш позитивному впливі найвагоміших загроз.

Третій розділ присвячено дослідженню розроблених когнітивних моделей. Зокрема, на основі множинного регресійного аналізу було доведено достовірність впливу загроз на рівень захищеності систем захисту інформації, що циркулює в інформаційних системах, визначеного за сценарним моделюванням.

Використовуючи апарат симпліціального аналізу, сформовано множину управляючих концептів та встановлено зв'язні концепти для когнітивної моделі дослідження захищеності об'єкта критичної інфраструктури. Вивчення взаємозв'язків всередині кожного блоку зв'язних концептів симпліціального комплексу сприятиме підвищенню захищеності досліджуваного об'єкта.

На основі теорії нечітких відношень здійснено ранжування загроз системи захисту інформації та об'єкта критичної інфраструктури. Пропорційно до рангів загроз визначено допустиму інтенсивність зниження рівня захищеності цих систем та витрати на її забезпечення, що сприятиме впровадженню необхідних механізмів захисту досліджуваних об'єктів із достатньою забезпеченістю резервними ресурсами, які здатні у разі реалізації загроз швидко відновити втрачені функції.

У четвертому розділі здійснено розробку програмного забезпечення для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах. Запропоновано структуру програми у вигляді семи взаємозалежних програмних модулів, здійснено їх програмну реалізацію, продемонстровано застосування програмних модулів.

Крім того, проведено аналіз у часі розроблених у другому розділі роботи когнітивних моделей. Так, на основі динамічної каузальної алгебри визначено вплив найвагоміших концептів нечіткої когнітивної карти на захищеність об'єкта критичної інфраструктури у різні моменти часу. Це дозволяє спрогнозувати розвиток ситуації у часі для забезпечення стійкого та безпечного функціонування об'єкта критичної інфраструктури.

Також проведено дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи захисту інформації при впливі потенційних загроз. Проведений імітаційний експеримент ілюструє можливі варіанти розвитку ситуації у віртуальному середовищі, що дозволяє згенерувати найбажаніший варіант розвитку ситуації та вчасно вжити комплексні заходи для підвищення захищеності досліджуваної системи.

У висновках сформульовані основні результати дисертаційної роботи.

Відсутність (наявність) порушення академічної доброчесності

У дисертаційній роботі відсутні порушення академічної доброчесності. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Зауваження щодо змісту і результатів роботи:

1. У першому розділі дисертації автором практично не розглянуто наукових робіт іноземних авторів (хоча у вступі дисертант наводить перелік закордонних авторів, які займаються дослідженнями у цій галузі), що не дозволяє визначити місце отриманих результатів у глобальному світовому масштабі, порівнявши їх за певними критеріями.

2. У розділі 2 дисертантом не описано, які типові значення може приймати такий показник структурної складності розроблених нечітких когнітивних карт, як щільність – це ускладнює загальне розуміння ефективності запропонованих моделей оцінювання рівня захищеності об'єкта критичної інфраструктури на основі когнітивного підходу.

3. В описі наукової новизни (стор. 21-22) дисертант наводить кількісні показники, що відображають перевагу отриманих результатів над аналогами. Проте, як правило, наукова новизна містить якісний ефект, а кількісні показники виносяться до практичної цінності роботи.

4. У підрозділі 3.2 дисертаційної роботи немає чітких пояснень і обґрунтування, чому при проведенні симпліціального аналізу автором було побудовано симпліціальний комплекс лише за рядками матриці суміжності нечіткої когнітивної карти для дослідження захищеності об'єкта критичної інфраструктури.

5. У таблицях 3.9 та 3.12 у стовпцях 3–6 не зрозуміло звідки беруться числа записані у вигляді дробу.

6. У підрозділі 4.1 не описано, яким чином при здійсненні динамічного часового аналізу задається вектор порогів вершин. Крім того, відсутня методика експериментального дослідження, використання якої дозволило б повторити експеримент в аналогічних умовах.

7. У підрозділах 4.3 – 4.4 було розроблено програмний засіб для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, проте не зазначено потенційних його користувачів, що могло б підкреслити актуальність і визначити напрямки подальшого впровадження результатів дисертації.

8. 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. 17 дисертації.

9. У роботі мають місце окремі граматичні помилки.

Однак зазначені зауваження не носять принциповий характер і не знижують цінності проведеного здобувачем дослідження, актуальності, новизни та практичної значущості дисертаційної роботи.

Висновки щодо відповідності дисертації встановленим вимогам

Дисертаційна робота за актуальністю, науковою новизною, практичним

значенням, особистим внеском автора, обсягом і рівнем публікацій, достовірністю відповідає встановленим вимогам до дисертацій.

Результати роботи викладено чітко, послідовно та логічно, висновки за розділами та загальні висновки дисертації містять якісні і кількісні наукові та практичні результати.

За поставленою метою та вирішеними задачами, об'єктом та предметом досліджень, отриманими результатами робота Салієвої Ольги Володимирівни відповідає спеціальності 125 – Кібербезпека.

Основні результати дисертації мають практичне впровадження.

Висновки щодо дисертації в цілому

За результатами аналізу змісту дисертації вважаю, що дисертація Салієвої Ольги Володимирівни є завершеним науковим дослідженням, у якому вирішена важлива науково-технічна задача щодо підвищення рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, створенням функціональних когнітивних моделей для оцінювання рівня їхньої захищеності та програмних засобів реалізації цих моделей.

Враховуючи актуальність, наукову новизну і практичне значення одержаних результатів, вважаю, що дисертаційна робота «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» цілком відповідає вимогам «Порядку проведення експерименту з присудження ступеня доктора філософії» (Постанови Кабінету Міністрів України №167 від 06 березня 2019 року), а її авторка Салієва Ольга Володимирівна заслуговує присудження ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Офіційний опонент
заступник декана факультету
кібербезпеки, комп'ютерної та
програмної інженерії Національного
авіаційного університету,
доктор технічних наук, доцент С. О. Гнатюк

«18» травня 2021 р.

Підпис гр. Гнатюка С.О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Лепешкін