№67-72-107/1
19.05.2021 р.

ВІДГУК

офіційного опонента – доктора технічних наук, професора
Смірнова Олексія Анатолійовича 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

Актуальність теми дослідження

Широкомасштабне впровадження інформаційних систем та технологій в усі сфери суспільної діяльності надає безліч нових можливостей, забезпечує швидке та ефективне надання різноманітних послуг населенню. У зв'язку з цим необхідно приділяти значну увагу надійному та безпечному їхньому функціонуванню та забезпеченню належного рівня захищеності систем захисту інформації. Адже виведення з ладу або руйнування даних систем може призвести до значних матеріальних, фінансових, репутаційних та інших збитків.

Таким чином, актуальним є наукове завдання спрямоване на підвищення рівня захищеності систем захисту інформації. При цьому варто врахувати те, що вирішення даного завдання безпосередньо пов'язане з людським фактором і характеризується високим ступенем невизначеності та складністю строгої формалізації загроз інформаційній безпеці. Тому під час проведення досліджень, що складають зміст роботи, доцільним є використання когнітивного підходу, який надає можливість враховувати як кількісні так і якісні фактори, опрацьовувати доступну експертну інформацію, не потребуючи при цьому великого обсягу експериментальних досліджень та часу на їх опрацювання.

Дисертаційна робота виконана у межах науково-дослідної роботи кафедри «Менеджменту та безпеки інформаційних систем» Вінницького національного технічного університету в рамках науково-дослідних та науково-технічних робіт, пов'язаних зі створенням 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.).

Загальна характеристика дисертаційної роботи

Дисертаційна робота Салієвої О.В. є завершеною науковою працею, яка складається зі вступу, чотирьох розділів, висновків, списку використаних джерел кількістю 118 найменувань, вміщує 30 рисунків, 21 таблицю та 5 додатків.

У вступі аргументовано висвітлено актуальність теми дисертаційного дослідження, наведена загальна характеристика роботи, сформульовано мету, об'єкт, предмет, завдання наукового дослідження, наукову новизну та практичну цінність роботи, визначено особистий внесок здобувачки, наведені дані про апробацію результатів роботи та публікації за темою дослідження.

У першому розділі проведено аналіз літературних джерел, висвітлено результати попередніх досліджень, зокрема, проаналізовано існуючі методи оцінювання впливу загроз на рівень інформаційної безпеки та моделі на основі нечіткої логіки та когнітивного моделювання. Показано, що переважна більшість з них орієнтована на проведення аналізу стану інформаційної безпеки й оцінювання ризиків та не вирішують питання безпосереднього визначення рівня захищеності систем в умовах реалізації загроз, що, у свою чергу, обумовило вибір мети та задач дослідження.

Другий розділ дисертації присвячений розробці та аналізу когнітивних моделей (на основі нечітких когнітивних карт) для визначення рівня захищеності комп'ютерної мережі, системи захисту інформації та об'єкта критичної інфраструктури, при впливі на них потенційних загроз. Досліджено системні показники когнітивних карт, визначено найвагоміші концепти для кожної системи та проведено моделювання сценаріїв розвитку ситуацій, при яких визначається відносна зміна рівня захищеності даних об'єктів при екстремальних значеннях впливу найвагоміших концептів.

У третьому розділі основна увага приділена дослідженню розроблених на основі когнітивного підходу моделей. Так, для перевірки отриманих за сценарним моделюванням результатів було проведено регресійний аналіз та доведено достовірність впливу загроз на рівень захищеності комп'ютерної мережі, системи захисту інформації та об'єкта критичної інфраструктури.

Використання симпліціального аналізу дозволило автору визначити управляючі концепти когнітивної карти для дослідження рівня захищеності об'єкта критичної інфраструктури та зв'язні компоненти системи й суттєві

зв'язки між ними. Також було показано, що найвагоміші концепти даної моделі визначенні за когнітивним підходом, увійшли до множини управляючих, це, у свою чергу, доводить достовірність отриманих у другому розділі результатів.

Застосовуючи нечітку математику, визначено ранги загроз об'єкту критичної інфраструктури та системі захисту інформації. На основі отриманих значень запропоновано розподіл допустимих витрат на захищеність даних систем та допустиму інтенсивність зниження рівня їхньої захищеності, що сприятиме раціональному використанню ресурсів та засобів для попередження, усунення або ж зменшення сили впливу вірогідних загроз інформаційній безпеці.

У четвертому розділі проведено динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури, що дозволяє розглянути та порівняти вплив одних концептів досліджуваної системи на інші. Також досліджено еволюційний розвиток системи у цілому за допомогою методів імпульсного моделювання. Крім того, розроблено структуру та модулі програми для оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах.

Висновки до розділів та загальні висновки сформульовані достатньо чітко, є обґрунтованими і відповідають змісту, головній меті та завданням дисертаційної роботи.

Повнота викладення наукових положень і висновків в опублікованих працях, апробація роботи

Достатня кількість публікацій здобувача, що пройшли апробацію на міжнародних науково-технічних та науково-практичних конференціях, відображає основні наукові положення та висновки, що отримані в результаті дисертаційних досліджень.

За темою дисертації опубліковано 18 друкованих робіт: 10 статей у наукових виданнях з переліку фахових видань України, 1 стаття у науковому журналі, що входить до наукометричної бази SCOPUS, 7 тез доповідей науково-технічних та науково-практичних конференцій.

Наукова новизна одержаних результатів

Наукову новизну проблеми, що вивчається автором, можна оцінити відразу в науковому та практичному аспектах.

У дисертаційній роботі отримано такі наукові результати:

1. Вперше запропоновано когнітивну модель оцінювання рівня захищеності об'єкта критичної інфраструктури, що базується на нечіткій

когнітивній карті та надає можливість спростити розрахунки та зменшити час обробки інформації, покращити наочність представлення даних, враховувати як кількісні, так і якісні фактори, легко розширити кількість факторів, введенням додаткових вершин і дуг графа когнітивної карти, визначити найвагоміші фактори та проводити сценарне моделювання, у результаті якого при максимально позитивному впливі даних факторів встановлено підвищення рівня захищеності об'єкта критичної інфраструктури на 2 %.

2. Вперше запропоновано когнітивну модель оцінювання рівня захищеності системи захисту інформації, що базується на нечіткій когнітивній карті та дозволяє збільшити швидкість обробки інформації та зменшити час на її опрацювання, покращити наочність представлення даних, використовувати суб'єктивні судження експертів, виявляти найвагоміші фактори та проводити сценарне моделювання, у результаті якого при максимально позитивному впливі даних факторів встановлено підвищення рівня захищеності системи захисту інформації на 19 %.

3. Удосконалено когнітивну модель для оцінювання рівня захищеності комп'ютерної мережі з використанням нечітких когнітивних карт, яка відображає предметну область точніше та надає можливість краще враховувати мінливість характеру процесів, які відбуваються у часі в досліджуваній системі, визначити найвагоміші загрози комп'ютерної мережі та проводити сценарне моделювання, у результаті якого при максимальному послабленні впливу найвагоміших загроз встановлено підвищення рівня захищеності комп'ютерної мережі на 63 %.

4. Дістав подальшого розвитку підхід до визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури і системи захисту інформації та допустимих витрат на забезпечення захищеності, ранжуванням загроз на основі теорії нечітких відношень, який надає можливість спростити проміжні розрахунки, зменшити час обробки вхідної інформації, проводити не тільки кількісне, а й якісне оцінювання як вхідних даних, так і вихідних результатів.

Шляхи використання наукових та практичних результатів роботи і ступінь їх реалізації

Цінність наукових результатів роботи полягає у тому, що в ній запропоновано рішення важливого наукового завдання – підвищення рівня захищеності систем захисту інформації, що циркулює в інформаційних системах.

Практична корисність роботи обумовлена тим, що здобувачем розроблено програмне забезпечення для реалізації когнітивних моделей оцінювання рівня захищеності систем захисту інформації.

Розроблені моделі на основі когнітивного підходу були апробовані у Головному управлінні Пенсійного фонду України у Вінницькій області, Хмельницькому зональному відділі Військової служби правопорядку, відокремленому підрозділі «Південно-Західна електроенергетична система» ПАТ «Національна енергетична компанія «Укренерго та у навчальному процесі Вінницького національного технічного університету на кафедрі менеджменту та безпеки інформаційних систем для підготовки фахівців за спеціальністю 125 «Кібербезпека».

Оцінювання обґрунтованості та достовірності наукових положень і висновків, сформульованих у дисертації

Обґрунтованість та достовірність наукових положень і висновків підтверджена аргументованою постановкою мети й задач дослідження, наведеною у розділах 2, 3 і 4, результатами когнітивного моделювання та впровадженням розроблених моделей та засобів. Теоретичні дослідження виконано з використанням сучасних методів інтелектуального аналізу даних. Достовірність отриманих результатів підтверджується їх узгодженням із отриманими внаслідок проведення регресійного та симпліціального аналізу висновками. Обґрунтованість наукових результатів забезпечується коректністю виконаних аналітичних розрахунків та результатами експериментальних досліджень, науковими публікаціями у фахових виданнях України та у міжнародному науковому виданні, що індексується у наукометричній базі Scopus, доповідями на наукових конференціях та семінарах різного рівня.

Оформлення дисертації

Оформлення дисертаційної роботи відповідає ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення» та вимогам Атестаційної колегії МОН України. Мова і стиль викладення дисертації чітко висвітлюють одержані науково-практичні результати.

Апробація результатів дисертаційного дослідження

Варто відзначити достатність оприлюднення результатів. При цьому матеріали дисертації доповідались на конференціях міжнародного та всеукраїнського рівнів, а також висвітлені у відомих у науковому світі фахових журналах, зокрема з інформаційної безпеки.

Відсутність (наявність) порушень академічної доброчесності

У роботі відсутні порушення академічної доброчесності. Посилання на використання ідей, результатів та тексту інших авторів є коректними.

Зауваження щодо змісту та результатів дисертаційної роботи

1. У параграфах 1.2 - 1.3 деякі переліки доцільніше було б представити у вигляді структурних схем.
2. У параграфах 2.1 - 2.3 не зазначено яким чином опрацьовувалися результати експертного опитування.
3. У дисертаційній роботі не зазначено чи існує можливість масштабувати розроблені моделі, враховуючи появу нових загроз.
4. На с. 99 визначено перший структурний вектор комплексу $K_x(Y;\lambda)$, який дорівнює $Q_x = \{1\,2\,3\,5\,7\,10\,12\,1\}$. Проте окремі числа даного вектору повинні відділятися комами, так як це робиться на с. 96.
5. У параграфі 3.2 доцільно замінити термін «управляючі» концепти на «керовані».
6. У параграфі 4.2 доцільно було б довести імпульсну стійкість орграфа.
7. У параграфі 4.4 занадто детально описано застосування програмних модулів створеного додатку для оцінювання рівня захищеності систем захисту інформації.
8. У тексті дисертації мають місце деякі граматичні помилки та описки.

Проте зазначені недоліки та зауваження суттєвим чином не знижують цінність та науковий рівень роботи. Висновки та положення у роботі добре обґрунтовані здобувачем та відповідають поставленій меті і задачам.

Висновок про відповідність дисертаційної роботи вимогам

Робота, виконана Салієвою Ольгою Володимирівною, за актуальністю, науковою новизною, практичною цінністю, особистим внеском і рівнем публікацій відповідає встановленим вимогам до дисертацій.

За поставленою метою та завданням, об'єктом та предметом, результатами та висновками дисертація за темою «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» відповідає спеціальності 125 «Кібербезпека».

Висновок щодо дисертації в цілому

Дисертаційна робота Салієвої Ольги Володимирівни «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання», представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12

«Інформаційні технології») є актуальною завершеною науковою працею, що виконана на належному науково-теоретичному рівні з логічним та доступним викладеним матеріалом.

У роботі вирішується важливе наукове завдання, що полягає у підвищенні 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.

Здобувачка Салієва Ольга Володимирівна заслуговує присудження їй ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»).

Офіційний опонент,
Завідувач кафедри кібербезпеки та
програмного забезпечення
Центральноукраїнського національного
технічного університету, доктор технічних
наук, професор О. А. Смірнов

“____” _____ 2021 року

Підпис проф. Смірнова О.А. засвідчую:
Проректор з наукової роботи
Центральноукраїнського національного
технічного університету,
доктор економічних наук, професор О.М. Левченко

“____” _____ 2021 року