РЕЦЕНЗІЯ

на дисертаційну роботу
Полуциганової Вікторії Ігорівни
на тему «Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 125 – Кібербезпека та захист інформації

Актуальність теми дисертації.

Безпека кіберсистем різних установ державного та приватного сектору має велике значення особливо в умовах воєнного стану, бо порушення цілісності та отримання доступу до чутливої інформації можуть призвести до непередбачуваних наслідків. Подібні ситуації виникають у хмарних середовищах, системах критичної інфраструктури тощо та можуть призвести до серйозних фінансових та репутаційних втрат. Кожній такій системі характерні певні типи вразливостей, що породжують загрози різного рівня критичності від втрати доступу до підсистем та даних до руйнування системи в цілому. Це підтверджується реалізаціями атак на різні кіберсистеми по всьому світу.

Побудова моделей, аналіз та класифікація загроз залежить від вразливостей, які присутні в системі, стають все більш складними і вимагають системних та ефективних підходів для їх аналізу та управління. Зв'язок загроз та вразливостей досліджувався у деяких сучасних роботах і був формалізований у вигляді матриць інцидентності, але в недостатній мірі описується характер цих зв'язків. Складна структура сумісності між вразливостями, таким чином, може бути задана у вигляді симплеційного комплексу, що враховує наявність та структуру зв'язків високого порядку у системі вразливостей. Використання інструментарію Q-аналізу для уточнення структурних характеристик комплексу і подальшого їх застосування для аналізу системи дає можливість отримувати надійніші оцінки ризику.

На даний час існуючі методи і методології моделювання та дослідження безпеки кіберсистем, розроблені інформаційні технології та програмні забезпечення не завжди дають високі показники адекватності та якісні оцінки ризику. Тому виникає необхідність у дослідженні та вирішенні задач розробки процедур оцінювання ризиків, удосконаленні та впровадженні нових підходів для забезпечення безпеки кіберсистем.

Оцінювання ризиків при реалізації вразливостей є актуальною задачею для створення систем захисту кіберсистем. Запропонований метод включає

урахування впливу структурних особливостей у взаємозалежності між вразливостями та загрозами та допомагає точніше оцінити рівень ризику та зрозуміти його природу та характер. Тому подане авторкою дослідження, спрямоване на створення ефективного методу для аналізу ризиків, має безумовну актуальність.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- Вперше побудовано модель зв'язків загроз та вразливостей у кіберсистемі у вигляді симплеціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків;
- Вперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу;
- Вперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак;
- Розроблено процедуру побудови байєсівської оцінки ризику з врахуванням структури вразливостей системи та складеної функції втрат.

Достовірність отриманих результатів забезпечується коректним застосуванням понять і математичного апарату структурного аналізу, теорії ймовірностей, теорії ризику, адекватність і ефективність яких підтверджується великим досвідом їх використання. Аналіз досліджених у роботі прикладів підтверджує як можливість практичного застосування, так і ефективність розробленого методу оцінювання ризику та відповідних обчислювальних процедур.

Наукові дослідження були виконані здобувачем на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського в рамках НДР «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» державний реєстраційний номер 0124U001957 під керівництвом доцентом кафедри інформаційної безпеки, к.ф.-м.н., с.н.с. Смирновим Сергієм Анатолійовичем.

Наукові напрацювання дисертаційного дослідження використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, а також у процесі розроблення Загальних правил

обміну інформацією про кіберінциденти, затверджених рішенням НКЦК. Теоретичні та практичні результати наукового дослідження використані для вдосконалення державної політики з питань національної безпеки у сфері забезпечення кібербезпеки, насамперед щодо підвищення рівня кіберзахисту інформаційно-комунікаційних систем об'єктів критичної інфраструктури, зокрема паливно-енергетичного сектору.

Теоретичні та практичні результати застосовуються у навчальному процесі кафедри інформаційної безпеки НТУУ «КПІ ім. Ігоря Сікорського» при підготовці та викладанні курсів «Рішення в умовах невизначеності та ризику», «Проблеми кібербезпеки критичної інфраструктури», «Математичні моделі кібербезпеки».

Отже, в дисертаційній роботі поставлене наукове завдання аналізу та синтезу моделей і методів оцінювання ризиків з врахуванням структурних властивостей сукупності зв'язків загроз та вразливостей кіберсистем виконано повністю, здобувачка повною мірою оволоділа методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Полуциганової В. І. повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації та напрямкам досліджень відповідно до освітньої програми Кібербезпека.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям 12 Інформаційні технології.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Полуциганової Вікторії Ігорівни є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою.

Матеріал дисертаційної роботи повністю відповідає вимогам щодо грамотності та стилю викладення результатів. Автор роботи при викладені матеріалу дотримається сучасної загальноприйнятої у даній сфері науки термінології.

Дисертація складається з вступу, 4 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 207 сторінок.

У вступі обґрунтовано актуальність теми дисертації, зазначено зв'язок з науковими програмами, планами та темами, сформульовано мету та задачі дослідження. Також охарактеризовано наукову новизну та практичне значення одержаних результатів, наведено інформацію про впровадження результатів роботи, їх апробацію та публікації.

У першому розділі міститься поточний стан методології оцінювання ризику, аналізу структури складних кіберсистем, аналізу вразливостей та загроз безпеки кіберсистем та описано сучасний стан вивчення проблем, схожих до тих, що розглядаються в дисертаційній роботі. Наведено огляд основних підходів на які спираються методи структурного аналізу розроблені у дисертаційному дослідженні, а саме Q-аналіз, топологічний аналіз, симплеціальний аналіз. Проведено аналіз основних етапів життєвого циклу вразливостей у кіберсистемі. Розглянуто основні методики оцінювання ризику на основі підходів Вальда та Байєса.

У другому розділі проведено виявлення та аналіз основних метрик для структурного опису систем вразливостей та загроз у кіберсистемі. Встановлено, що основними характеристикам, що є достатніми для однозначного завдання (та відновлення) структури складної системи являються локальні карти, структурне дерево та структурні графи симплекційного комплексу. В розділі розроблено алгоритми переходу від довільної матриці інцидентності вразливостей та загроз до побудови матриці симплекційного комплексу, побудови структурних характеристик комплексу на її основі. Наведено класифікацію та структурний аналіз системи вразливостей, що може суттєво допомогти в попереджені та подоланні несприятливих наслідків реалізації загроз. Для детального аналізу структурних особливостей комплексу було застосовано на прикладі алгоритми, розроблені у другому розділі. Створено алгоритм для класифікації типів загроз в залежності від сумісності вразливостей.

У третьому розділі побудовано метод оцінювання ризиків на основі інформації про складну структуру залежностей вразливостей та загроз і втратах при інцидентах. Для врахування впливу наявних взаємозв'язків між вразливостями використовувалась модель взаємодії між вразливостями та загрозами на основі відповідного симплеційного комплексу. В ході дослідження проводились уточнення оцінок відповідних ймовірностей та втрат. В роботі сформовано методику оцінки ризику на основі складної структури, що визначається системою загроз та вразливостей кіберсистеми. Визначено, що такий підхід для розрахунку будь-якої адитивної по структурних компонентах характеристики комплексу буде коректним, якщо він наслідує процедуру

синтезу комплексу з урахуванням «включення-виключення» внесків від компонент.

В четвертому розділі проведено дослідження практичного прикладу на основі методів розроблених у дисертації. Розглянуто систему загроз і вразливостей інформаційної підсистеми критичної інфраструктури. Їх пов'язано із потенційно вразливими компонентами, на які саме і можуть спрямовуватись кібератаки. Проведено структурний аналіз для виявлення можливих сумісних реалізацій загроз, які проявляються через складну структуру взаємозалежностей між вразливостями та загрозами. Побудовано локальні карти, структурні графи та структурне дерево за розробленими в другому розділі алгоритмами. Проведено класифікацію вразливостей на основі параметрів для даної системи загроз. Проведено детальний аналіз отриманої оцінки ризику в залежності від ймовірності виникнення загроз, продиктовані профілем атак на систему, а також використовуючи експертні оцінки втрат від їх реалізації.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких: 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України.

Також результати дисертації були апробовані на 8 наукових фахових конференціях.

Усі публікації здобувачки мають високий науковий рівень. У них детально розкриваються основні наукові результати виконаного дослідження. Особистий внесок здобувачки до публікацій за співавторством вагомий, особливо у описі експериментальних частин роботи. Принципів академічної доброчесності у жодній з публікацій не порушено.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. В першому розділі проведена завелика деталізація методів характерних для даного дослідження, але не наведено достатній мірі порівняльний аналіз моделей ризиків.

2. При описі алгоритмів, розроблених на основі Q-аналізу, не наведені характеристики їх складності. Доцільно було провести аналіз залежності роботи алгоритмів від кількості елементів симплекційного комплексу.

3. Використання складного ілюстративного матеріалу в тексті дисертації, які доречніше було винести у додатки.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Полуциганової Вікторії Ігорівни на тему «Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах», виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для Інформаційних технологій. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Полуциганова Вікторія Ігорівна заслуговує на присудження ступеня доктора філософії в галузі знань Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Рецензент:
Завідувач кафедри інформаційної
безпеки КПІ ім. Ігоря Сікорського
д.т.н., професор /_____/ Дмитро ЛАНДЕ

Підпис гр._____
ЗАСВІДЧУЮ
Відділ кадрів та діловодства
_____ (_____)
підпис пр-ще

М.П. «____» _____ 20___ року