ВІДГУК

офіційного опонента
доктора технічних наук, професора Наконечного Володимира Сергійовича
на дисертаційну роботу Звєрцевої Наталії Віталіївни
«Моделі оцінки безпеки комп'ютерних систем»,
представлену на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки

Актуальність теми.

У сучасних умовах стрімкої цифрової трансформації, зумовленої розвитком смарт-технологій, інтернету речей, штучного інтелекту, мобільних платформ та мереж нового покоління, значно розширюється сфера використання комп'ютерних систем у критично важливих галузях – від медицини до державного управління. Водночас, динаміка технологічного прогресу супроводжується зростанням кількості й складності кіберзагроз. Особливої уваги заслуговує виклик, пов'язаний із настанням постквантової епохи. Впровадження квантових обчислювальних систем ставить під сумнів ефективність існуючих криптографічних протоколів – як симетричних, так і асиметричних, – що є основою більшості сучасних систем інформаційної безпеки. Це створює потребу в перегляді концептуальних підходів до захисту інформації та у розробці нових моделей оцінки безпеки в умовах нової обчислювальної парадигми. Актуальність роботи Звєрцевої Наталії Віталіївни зумовлюється як практичними викликами у сфері кіберзахисту, так і необхідністю формулювання і вирішення нових наукових задач безпеки в умовах постквантових загроз.

Дисертаційна робота Звєрцевої Наталії Віталіївни «Моделі оцінки безпеки комп'ютерних систем» спрямована на вирішення критично важливого науково-технічного завдання – підвищення рівня безпеки комп'ютерних систем шляхом розробки та впровадження моделей оцінювання безпеки з використанням комплексованих метрик. Запропонований підхід дозволяє здійснювати всебічний аналіз захищеності систем, виявляти потенційні вразливості та своєчасно реагувати на загрози. Це забезпечує підвищення ефективності заходів кіберзахисту та є необхідною умовою для створення адаптивних, стійких до атак інформаційних систем.

Тема пов'язана з виконанням науково-дослідних робіт кафедри «Програмна інженерія та інтелектуальні технології управління» НТУ «ХПІ». Здобувачка брала участь у науково-дослідній роботі К8018 «Розробка моделей, методів та інформаційних технологій оцінювання складних багатоознакових об'єктів і систем» №ДР 0125U001121, де здобувачка була виконавцем розділу.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Положення та висновки, наведені в дисертаційній роботі Звєрцевої Н.В., в

достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні теорії ймовірностей і математичної статистики, використаних для дослідження моделей та методів оцінки безпеки комп'ютерних систем. Дослідження виконані з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати дослідження перевірені шляхом проведення практичних експериментів, що підтверджує обґрунтованість наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Достовірність результатів досліджень.

Достовірність результатів теоретичних досліджень підтверджується результатами відповідних експериментальних досліджень. Отримані наукові результати впроваджені у програмний модуль аналізу стану безпеки та виявлення потенційних вразливостей у комп'ютерних мережах.

До основних нових наукових результатів дисертації слід віднести наступне:

– *вперше* розроблено модель оцінки поточного стану рівня захищеності комп'ютерної системи, що дозволяє враховувати складові безпеки та ознаки гібридності та синергізму загроз на комп'ютерні системи;

– *вперше* запропоновано метод безперервного функціонування безпеки комп'ютерної системи, що дозволяє формувати контур безпеки безперервних бізнес-процесів комп'ютерної системи та забезпечити своєчасне формування превентивних заходів проти цільових (змішаних) атак;

– *вперше* запропоновано модель визначення рівня безпеки на основі комплексування різних метрик з метою одержання об'єктивної оцінки поточного стану рівня захищеності соціокіберфізичних систем, з урахуванням не лише обчислювальних та фінансових витрат зловмисника на реалізацію цільової атаки, а й рівня таємності;

– *отримав подальший розвиток* математичний апарат формування класифікатора загроз на основі обліку їх синергізму та гібридності, а також впливу загроз на критичні точки інфраструктури комп'ютерної мережі.

Значимість отриманих результатів для науки і практичного використання.

Практична цінність отриманих результатів досліджень полягає у використанні їх:

1) у ТОВ «НІКС СОЛЮШЕНС ЛТД» (м. Харків) – ІТ-компанія, що займається розробкою програмного забезпечення;

2) в Національному технічному університеті «Харківський політехнічний інститут» (м. Харків) при розробці і впровадженні в навчальний процес кафедри «Програмна інженерія та інтелектуальні технології управління».

Повнота викладення результатів досліджень в опублікованих працях.

У відкритому друці за темою дисертації опубліковано 15 наукових праць, з них: 5 статей, з яких 2 статті включено до наукометричної бази Scopus та/або Web of Science Core Collection, при цьому 2 статті опубліковано в журналах, віднесених до третього Q3 квартиля; 3 статті – в збірниках наукових праць, що входять до переліку фахових Міністерства освіти і науки України видань категорії Б; 10 публікацій – тези доповідей на конференціях (з яких 4 роботи видано в закордонних видавництвах). Участь здобувачки у роботах, що опубліковані у співавторстві зазначена у дисертаційній роботі.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. №44.

Оцінка змісту дисертаційної роботи.

Дисертаційна робота Звєрцевої Н.В. складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та чотирьох додатків.

У вступі дисертації обґрунтовано актуальність дослідження, сформульовано мету, завдання, об'єкт і предмет дослідження, визначено наукову новизну та практичну цінність результатів. Описано використані методи дослідження, подано відомості про апробацію та публікації за темою.

Перший розділ містить аналітичний огляд поточного стану інформаційної безпеки комп'ютерних систем у контексті впровадження інтелектуальних технологій та появи постквантових загроз. Розглянуто сучасні методи оцінювання рівня безпеки, системи виявлення атак і загрози гібридного типу. Сформульовано наукову проблему, яка полягає у необхідності нових класифікаційних підходів до опису загроз як основи для побудови ефективних моделей захисту.

У другому розділі проаналізовано існуючі метрики оцінювання безпеки та обґрунтовано вибір комплексованого підходу. Запропоновано структуру інтегрованої моделі, що поєднує переваги різних типів метрик. Обґрунтовано доцільність застосування нечітких множин та логіки причинно-наслідкових зв'язків.

Третій розділ присвячено розробці моделей оцінювання поточного рівня захищеності комп'ютерної системи. Запропоновано метод забезпечення безперервності функціонування системи безпеки з урахуванням динаміки кіберзагроз. Сформовано архітектуру багатоконтурної системи оцінювання, адаптованої до різних типів інформаційних активів.

У четвертому розділі описано процес верифікації моделей. Створено набір досяжності цільових показників безпеки, враховано технічні й управлінські чинники. Реалізовано прототип програмного засобу для автоматизованої оцінки загроз та підтримки прийняття рішень у сфері кібербезпеки.

У висновках підведено підсумки виконаного дослідження, підтверджено досягнення поставленої мети, наведено основні теоретичні та практичні результати, які виносяться на захист. Визначено напрями подальших досліджень.

Список використаних джерел із 130 найменувань досить повний і включає вітчизняні та зарубіжні публікації.

Анотація відображає основний зміст дисертації та достатньо повно розкриває наукові результати та практичну цінність роботи.

Академічна доброчесність.

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено.

Усі результати, які винесено авторкою на захист, отримані самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

По дисертаційній роботі можна зробити наступні зауваження:

1. З дисертаційної роботи не зрозуміло яким чином враховуються комплексування цільових (змішаних) атак з методами соціальної інженерії під час формування моделі загроз (п.1.1, стор. 17).

2. На стор. 23 наведений рис. 1.3, який визначає дерево залежностей із ймовірностями реалізації загроз, але не зрозуміло, яким чином отримані початкові результати ймовірностей загроз, та на скільки ці показники враховуються під час формування моделі потокового стану безпеки.

3. З дисертаційної роботи (п. 2.3 Науково-технічне обґрунтування вибору підходу до оцінювання метрик безпеки комп'ютерних систем) наведені основні етапи лінгвістичної класифікації вихідної сукупності даних загроз та її верифікацію як квазистатистики, але не зрозуміло, чому пропонується ефективність такого підходу у порівнянні з методикою FAIR, яка не підтримується з 2021 року.

4. На рис. 3.1 (стор. 89) представлена структура класифікатора загроз, але не зрозуміло, яким чином враховується вибір вагових коефіцієнтів α_i прояву i-ї вразливості/загрози залежно від умов їх прояву під час формування загальної оцінки цільової загрози, а також в динаміці оцінити поточний стан рівня захищеності з урахуванням рівня секретності інформаційного ресурсу.

5. В дисертаційної роботі на стор. 104 наведена таблиця порівняння елементів моделі та концепцій ризику, але не зрозуміло, чому саме ці моделі визначені, та яким чином визначені показники у таблиці.

6. З дисертаційної роботи не зрозуміло, які обчислювальні та енергетичні витрати потрібні для реалізації запропонованих підходів до формування об'єктивної оцінки потокового стану захищеності на основі оцінки взаємозв'язку цілей та

функціональності критичних (безперервних) бізнес-процесів компанії/організації/підприємства, та які економічні витрати для цього потрібні.

Слід зазначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Загальний висновок та оцінка дисертації.

Дисертаційна робота Звєрцевої Наталії Віталіївни «Моделі оцінки безпеки комп'ютерних систем» є завершеним, самостійним науковим дослідженням. У роботі комплексно вирішено актуальну задачу підвищення рівня безпеки комп'ютерних систем на основі використання запропонованих моделей оцінки безпеки з комплексированими метриками на основі розроблення нових та удосконалення існуючих моделей і методів оцінки безпеки комп'ютерних систем у постквантовий період.

За рівнем наукової новизни, практичною цінністю результатів, обґрунтованістю висновків, повнотою апробації та дотриманням принципів академічної доброчесності, дисертаційна робота відповідає спеціальності 122 – «Комп'ютерні науки»., вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23.03.2016 №261 (зі змінами), 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 (зі змінами), а здобувачка Звєрцева Наталія Віталіївна заслуговує присудження наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки».

Офіційний опонент
доктор технічних наук, професор,
професор кафедри
кібербезпеки та захисту інформації,
факультету інформаційних технологій,
Київського національного університету
імені Тараса Шевченка
«27» червня 2025р.

Володимир НАКОНЕЧНИЙ

Підпис
Вчений секретар
КАРАУЛЬ