ВІДГУК

офіційного опонента

професора кафедри транспортного зв'язку

Українського державного університету залізничного транспорту

доктора технічних наук, професора Трубчанінової Карини Артурівні

на дисертаційну роботу Челак Віктора Володимировича

«Методи та засоби захисту інформації в комп'ютерних системах та мережах»,

представлену на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

Актуальність теми

В сучасному світі, інформаційні технології розвиваються з надмірно високою інтенсивністю. Щодня виходять оновлення програмних продуктів від простих консольних утиліт до операційних систем. Необхідність в постійних оновленнях виникає через велику кількість помилок в програмних продуктах, серед яких високій відсоток займають вразливості. Захист комп'ютерних систем та мереж від шкідливого програмного забезпечення, загроз та вторгнень, які користуються вразливостями є одним з важливих та пріоритетних напрямків комп'ютерної інженерії. Саме тому дисертаційна робота Челака Віктора Володимировича, що пропонує нові методи ідентифікації стану комп'ютерних систем є актуальною.

У дисертаційній роботі вирішена науково-технічна задача розробки методів ідентифікації стану комп'ютерних систем з метою підвищення показників точності та швидкості систем виявлення вторгнень. Застосування розроблених програмних компонентів, які реалізують запропоновані методи, дозволяє досягти необхідної захищеності систем на підприємствах різних сфер обслуговування.

Тема пов'язана з виконанням науково-дослідних робіт кафедри «КІП» НТУ «ХПІ», а саме:

1) Науково-дослідній роботі ДР №0122U200526 «Моделі і методи обробки та захисту інформації в комп'ютерних системах», де здобувач був керівником цієї роботи;

2) Науково-дослідній роботі ДР №0122U200527 «Моделі і методи обробки

даних і розподілу мережних ресурсів в комп'ютерних системах», де здобув був виконавцем.

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

Положення та висновки, наведені в дисертаційній роботі Челака Віктора Володимировича, є обґрунтованими базуються на використанні технологій машинного навчання, теорії алгоритмів та структур даних, нечіткої логіки та теорії прийняття рішень.

Дослідження виконані з використанням сучасних комп’ютерних системах, кафедри, віртуальних машин та бази шкідливого програмного забезпечення. Результати 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.

Наукові результати застосовані під час експлуатації програмного забезпечення, що реалізують запропоновані методи. Наукові результати впроваджені в двох компаніях, що дозволяє підтвердити їх достовірність.

До основних нових наукових результатів дисертації слід віднести наступне:

- вперше запропоновано метод побудови дерева з багатовимірними вузлами рішень, що дозволило підвищити точність ідентифікації її стану за рахунок кластеризації вихідних даних та збільшити оперативність ідентифікації завдяки зменшенню кількості розгалужень дерев рішень**.**

- вперше запропоновано метод побудови нечіткого дерева рішень, який за рахунок використання спеціальної автоматизованої процедури формування нечітких множин та їх функцій належності підвищує точність та оперативність ідентифікації стану комп’ютерних систем та мереж**.**

- удосконалено метод побудови дерева рішень, час навчання моделі якої менший за існуючи класичні алгоритми побудови дерев рішень, завдяки використанню направленого вибору ознак, використанню у якості критерію прийняття рішень мінімальної помилки класифікації та застосуванню алгоритму бінарного пошуку для визначення оптимального значення порогу розщеплення вузла дерева рішень**.**

- удосконалено ансамблевий метод бустинг за рахунок використання у якості базових моделей розроблених дерев з одновимірними вузлами рішень та спеціальної процедури попередньої обробки даних, що дозволило підвищити точність ідентифікації стану комп'ютерних систем**.**

Значимість отриманих результатів для науки і практичного використання.

Представлені в дисертаційній роботі Челака Віктора Володимировича методи мають наступні переваги:

– метод та програмне забезпечення побудови дерев з багатовимірними вузлами рішень дозволяє підвищити оперативність ідентифікації стану комп'ютерних систем до 50%, точність до 12% при наявності даних з високими коефіцієнтами кореляції;

– метод та програмне забезпечення формування нечітких множин та їх функцій належності для побудови нечітких дерев рішень дозволяє підвищити точність класифікації до 30% при умовах великої кількості даних на межі розмежування класів та швидкість до 23%, порівнюючи з класичними деревами рішень;

– удосконалений метод та програмне забезпечення побудови дерев з одновимірними вузлами рішень дозволяє зменшити час навчання до 4,5 раз;

– удосконалений ансамблевий метод класифікації та програмне забезпечення дозволяє підвищити точність класифікації до 32%.

Результати були впроваджені:

– в системах безпеки компанії SoftInWay, Inc;

– в системах захисту інформації ТОВ «ФТ ГРУП»;

– в навчальному процесі Національного технічного університету «ХПІ» в дисциплінах: «Reverse Programming» та «Розробка систем антивірусного захисту».

Повнота викладення результатів досліджень в опублікованих працях.

Результати досліджень опубліковані у 30 роботі, серед яких: 1 стаття у періодичному науковому фаховому виданні категорії «А», яка проіндексовано в базі даних Web of Science Core Collection, 2 статі з двома співавторами в фаховому виданні України категорії «Б» та 6 статей з трьома та більшою кількістю співавторів в фахових виданнях України категорії «Б». Усі публікації відповідають тематиці дисертації. Участь здобувача 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 Челака Віктора Володимировича складається зі вступу, п’яти розділів, висновків, списку використаних джерел, 6 додатків.

У вступі обґрунтовано актуальність теми дисертації, показано її наукову та практичну значимість, представлено мета і задачі дослідження, сформульовано об’єкт та предмет дослідження, описано зв’язок дисертації з науковими темами, наведено апробацію дисертаційної роботи та список публікацій.

В першому розділі виконано аналіз науково-технічної проблеми захисту даних в комп’ютерних системах та мережах, проаналізовано такі технології захисту інформації: антивірусні системи, системи запобігання та виявлення вторгнень, брандмауери. Більша частина розділу присвячена аналітичному огляду існуючих інтелектуальних методів, розглянуто сучасні наукові праці та виділені їх недоліки, що не дозволяють в повній мірі досягти поставленої мети дисертаційній роботі.

У другому розділі описана розробка методу ідентифікації стану комп’ютерних систем та мереж. Представлено формальний опис задачі класифікації даних та класичні дерева рішень. В кінці розділу проведено порівняльне дослідження якості запропонованого методу з багатовимірними ознаками в порівняні з існуючими рішеннями на основі технології машинного навчання.

В третьому розділі розглянуто основні положення нечіткої логіки, систем нечіткого виведення. Досліджено евристичний сканер на основі аналізу PE-структури файлу. Описано класичний метод побудови нечітких дерев рішень. Запропоновано спеціальну процедуру побудови нечітких множин та параметрів їх функцій належності, яка дозволяє зменшити вплив експертів на якість результуючої моделі.

В четвертому розділі обґрунтовується використання методу бустингу для задач ідентифікації стану комп’ютерних систем та мереж. В якості базового класифікатору застосовується метод на основі дерев з одновимірними вузлами рішень, що розроблено в другому розділу. Для інтеграції дерев з одновимірними вузлами рішень в ансамбль бустинг, здобувачем було зроблені відповідні модифікації функції помилки, які вводять вагові коефіцієнти зразків навчальної вибірки.

В п’ятому розділі проведена оцінка ефективності та оперативності розроблених методів ідентифікації комп’ютерних систем та мереж.

Висновки до розділів та результати дисертаційного дослідження сформульовані чітко та відповідають змісту дисертаційної роботи.

Список використаних джерел містить 167 найменувань, які рівномірно розподілені між п’ятьма розділами.

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

В додатках А, Б та В представлено публікації, фрагменти програмних компонентів та акти впровадження. В додатках Г, Д та Е наведено матеріали, які доповнюють дисертацію, що дозволяє краще зрозуміти принцип роботи розроблених методів, їх технічну складову та детальніше ознайомитись з метриками якості бінарної класифікації.

Академічна доброчесність

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

Усі результати, які винесено автором 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. В другому розділі, в частині розробки методу ідентифікації стану комп'ютерних систем на основі побудови дерева з багатовимірними вузлами прийняття рішень, відсутнє обґрунтування вибору способу визначення міри відстані між кластерами та інших гіперпараметрів алгоритму кластеризації DBSCAN. Крім того, виходячи з тексту дисертації не зрозуміло, чи було виконано аналіз інших алгоритмів кластеризації.

2. В третьому розділі занадто стисло описано алгоритм методу ідентифікації стану комп'ютерних систем на базі систем нечіткого виведення та його архітектурні особливості, що ускладнює розуміння відмінності його від евристичного сканера.

3. В четвертому розділі, в підрозділі опису процедури попередньої обробки даних, недостатньо висвітлено процес та критерії оцінки інформативності та вибору ознак об'єктів моделі.

4. В п'ятому розділі, інформація щодо інтерфейсу WMI, який використовується для збору даних та формування навчальної вибірки, є надмірною.

Вказані недоліки не впливають на загальну позитивну оцінку виконаної роботи. Дисертація є актуальною і має високу наукову цінність та практичну значущість.

ВИСНОВОК

Дисертаційна робота Челака Віктора Володимировича «Методи та засоби захисту інформації в комп'ютерних системах та мережах» за своїм змістом

відповідає спеціальності 123 Комп'ютерна інженерія. Дисертація є завершеною науково-дослідною роботою, розв'язує важливу науково-технічну задачу, яка полягає в підвищенні точності та швидкості ідентифікації стану комп'ютерних систем та мереж завдяки удосконаленню та розробці нових методів і програмних засобів.

Подана дисертаційна робота Челака Віктора Володимировича «Методи та засоби захисту інформації в комп'ютерних системах та мережах» відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пунктів 6, 7, 8 і 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 КМУ від 12.01.2022 р. №44, а здобувач Челак Віктор Володимирович заслуговує присудження наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент
доктор технічних наук, професор,
професор кафедри транспортного зв'язку
Українського державного університету
залізничного транспорту Карина ТРУБЧАНІНОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ * Український державний університет залізничного транспорту * №01116472

Особистий підпис
засвідчую 19.10 2023 р.
Завідуючий канцелярією
УкрДУЗТ

Карина Трубчанінова
Тетяна Шевченко