РЕЦЕНЗІЯ

рецензента, к.т.н., доцента Подорожняка Андрія Олексійовича

на дисертаційну роботу **Челака Віктора Володимировича**

«Методи та засоби захисту інформації в

комп’ютерних системах та мережах»

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп’ютерна інженерія

1. Актуальність теми

Одним із перспективних напрямків захисту інформації в комп'ютерних системах та мережах є розробка систем виявлення вторгнень, які дозволяють вчасно ідентифікувати аномальний стан, визначити джерело або причину такого функціонування системи та видалити загрозу. Саме тому дисертаційна робота Челака Віктора Володимировича, "Методи та засоби захисту інформації в комп'ютерних системах та мережах", є актуальною, особливо в умовах постійного зростання кількості загроз. Робота спрямована на вирішення завдання підвищення точності та швидкості ідентифікації стану комп'ютерних систем та мереж завдяки розробці нових методів на основі технології машинного навчання та має наукове та практичне значення.

2. Зв’язок роботи з науковими програмами, планами, темами

Дисертація виконувалась відповідно до наукової програми 123 «Комп’ютерна інженерія» та була впроваджена на кафедрі комп’ютерної інженерії та програмування, навчально-науковому інституту комп’ютерних наук та інформаційних технологій, НТУ «ХПІ».

Здобувач брав участь у двох науково-дослідних роботах: «Моделі і методи обробки та захисту інформації в комп'ютерних системах» (ДР №0122U200526) та «Моделі і методи обробки даних і розподілу мережних ресурсів в комп'ютерних системах» (ДР №0122U200527).

3. Аналіз змісту дисертації. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

Робота Челака В.В. є завершеною науковою роботою, містить дві анотації (українською та англійською мовами), вступ, п’ять розділів, висновки, список використаних джерел і додатки, які підтверджують достовірність отриманих результатів та доповнюють дисертаційну роботу.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної задачі, пов'язаної з розробкою та подальшим удосконалення методів та засобів ідентифікації стану комп'ютерних систем та мереж для захисту даних в умовах зовнішніх впливів.

У вступі обґрунтовано актуальність дослідження у галузі захисту інформації в комп’ютерних системах та мережах, вказано зв'язок роботи з актуальними науковими програмами і темами, відзначено наукову новизну та практичне значення отриманих результатів, надано інформацію про особистий внесок автора та перелік публікацій за темою дисертації.

У першому розділі досліджено проблеми захисту даних в комп’ютерних системах та мережах, проаналізовані загрози та фактори, що впливають на їх безпеку. Проведено аналіз антивірусних програм та систем захисту.

В другому розділі наведено формальну постановку задачі класифікації стану комп’ютерних систем та запропоновано алгоритм для побудови дерев рішень, що використовують одновимірні ознаки та функцію помилки. Друга частина розділу присвячена розробці методів багатовимірного аналізу для підвищення швидкості і точності ідентифікації.

У третьому розділі досліджено методи ідентифікації на основі нечіткої логіки та розроблено алгоритм побудови нечітких дерев рішень, враховуючи особливості програмного забезпечення.

У четвертому розділі розглянуті ансамблеві методи машинного навчання та їх застосування для підвищення точності класифікації.

У п'ятому розділі проведено аналіз показників функціонування комп’ютерних систем та методів збору даних для ідентифікації стану систем.

Розроблено програмні компоненти запропонованих методів та проведено ефективність порівняння з класичними методами.

У висновках наведено основні результати та вирішені наукові задачі дослідження.

4. Наукова новизна одержаних результатів

Дисертація містить наукову новизну, з найбільш суттєвих доробок роботи можна назвати:

– удосконалено метод побудови дерева рішень, за рахунок використання у якості критерію прийняття рішень мінімальної помилки класифікації, використання направленого вибору ознак та застосування алгоритму бінарного пошуку для визначення оптимального значення порогу розщеплення вузла дерев рішень, що дозволило зменшити час навчання моделі;

– вперше запропоновано метод побудови дерева з багатовимірними вузлами рішень, що надало можливість формувати деревоподібні моделі з урахуванням кореляційних зв’язків між показниками функціонування комп’ютерних систем, дозволило підвищити точність ідентифікації її стану за рахунок кластеризації вихідних даних та збільшити оперативність ідентифікації завдяки зменшенню кількості розгалужень дерево рішень;

–вперше запропоновано метод побудови нечіткого дерева рішень, який відрізняється від відомих наявністю спеціальної автоматизованої процедури формування нечітких множин та їх функцій належності, що дозволило підвищити точність та оперативність ідентифікації стану комп’ютерних систем;

– удосконалено ансамблевий метод класифікації на основі мета-алгоритму бустінгу за допомогою використання у якості базових моделей розроблених дерев рішень та процедури попередньої обробки даних, що надало можливість підвищити точність ідентифікації стану комп’ютерних систем.

5. Достовірність отриманих результатів та висновків

Достовірність отриманих результатів зумовлено поставленими метою та завданнями, а також використанням відповідної методології дослідження. Крім того, достовірність заявлених положень обґрунтовується комплексним

підходом у вивченні визначеного об’єкта, що також обґрунтовує використання методів дослідження.

6. Практична цінність одержаних результатів та рекомендації щодо їх подальшого використання

Практична цінність отриманих результатів полягає в успішному впровадженні результатів дослідження в діяльності компаній SoftInWay, Inc. та ТОВ «ФТ ГРУП», а також у навчальному процесі Національного технічного університету «ХПІ».

Серед практичних здобутків можна виділити наступні методи: розроблений метод та відповідне програмне забезпечення для побудови дерев з багатовимірними вузлами рішень призводять до зменшення кількості розгалужень, що підвищує оперативність ідентифікації стану комп'ютерних систем до 50% і підвищує точність до 12%; розроблений метод та програмне забезпечення для формування нечітких множин та їх функцій належності з метою побудови нечітких дерев рішень підвищують точність класифікації до 30% при обробці великого обсягу даних, розташованих на межі розмежування класів, підвищують швидкість роботи класифікатора до 23%, порівняно з класичними деревами рішень; вдосконалений метод дозволяє скоротити час навчання дерев з одновимірними вузлами рішень до 4,5 разів; вдосконалений ансамблевий метод класифікації на основі мета-алгоритму бустінгу забезпечує підвищену точність класифікації до 32%.

В окремому підрозділі здобувачем були сформульовані практичні рекомендації щодо застосування розроблених методів відповідно до характеристик вхідних навчальних наборів даних.

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових положень та результатів в опублікованих працях

Дисертація була виконана відповідно до наукових стандартів та академічної доброчесності. Отримані результати підтверджують оригінальність

дослідження. У тексті присутні авторські ідеї, і не виявлено використання концепцій інших вчених без належних посилань.

Основні ідеї автора та результати дослідження були опубліковані у 30 наукових працях, серед яких 13 статей, 1 розділ колективної монографії та 16 матеріалів апробаційного характеру (із них матеріалів 5 проіндексовані в наукометричній базі даних Scopus).

8. Недоліки та зауваження до дисертаційної роботи

1. В другому розділі зазначено, що поєднання вихідних даних в багатовимірні ознаки виконується на основі методу кореляційних плеяд, однак не розкрито сутність цього методу та вибір порогового значення.

2. У другому розділі занадто детально описані дерева з точки зору алгоритмів та структур даних, вказано багато прикладів не пов'язаних з теорію прийняття рішень або задачами класифікації та регресії. Доцільно було б зменшити обсяг цього підрозділу, та більш детальніше розглянути саме побудову дерев класифікації та регресії.

3. Із дисертаційної роботи, не зрозуміло, при побудові якої моделі використовуються дані, отримані за результатами аналізу *PE*-структури файлу.

4. В п'ятому розділі, доцільніше було б порівнювати ансамблевий класифікатор на основі бустингу з ансамблями, які використовують інші мета-алгоритми класифікації даних.

Вищенаведені недоліки не впливають на позитивне рішення цієї рецензії, та мають рекомендаційний характер для подальших досліджень здобувача за тематикою дисертації.

9. Висновки

Дисертаційна робота Челака В.В. є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тема дослідження відповідає спеціальності 123 – «Комп'ютерна інженерія».

Отже, враховуючи актуальність теми, отримані результати та певну практичну значущість вважаю, що дисертаційна робота Челака Віктора

Володимировича «Методи та засоби захисту інформації в комп'ютерних системах та мережах» відповідає вимогам 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціальної вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» від 12.01.2022 р. № 44 та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, а здобувач Челак Віктор Володимирович, заслуговує присудження йому наукового ступеня доктора філософії зі спеціальності 123 «Комп'ютерна інженерія».

Рецензент – кандидат технічних наук, доцент,
професор кафедри Комп'ютерної інженерії та програмування
Національного технічного університету
«Харківський політехнічний інститут» Андрій ПОДОРОЖНЯК

«19» жовтня 2023

Підпис проф. Андрія Подорожняка
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО-ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"19" 10 2023 р.
ЗАЙЦЕВ Ю. І.