ВІДГУК

офіційного опонента

завідувача кафедри електронних обчислювальних машин

Харківського національного університету радіоелектроніки,

доктора технічних наук, професора Коваленка Андрія Анатолійовича

на дисертаційну роботу Челака 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

Методи та апаратно-програмні засоби захисту інформації в комп'ютерних системах та мережах є одним з пріоритетних наукових напрямків галузі інформаційних технологій. Це пов'язано з постійнім ростом обсягів інформації, її вартості та збільшенням кількості шкідливого програмного забезпечення, мета якого полягає в знищенні, модифікації або несанкціонованому копіюванні конфіденційних даних. Підвищення вимог до точності та швидкості виявлення загроз, шкідливого програмного забезпечення, аномалій та вразливостей не дозволяє методам ідентифікації стану комп'ютерних систем, що існують, відповідати сучасним потребам. Для вирішення цієї наукової задачі необхідно удосконалювати або розробляти нові методи ідентифікації стану комп'ютерної системи. Дисертаційна робота Челака Віктора Володимировича спрямована на розробку таких методів та реалізацію їх у формі програмних засобів.

Тема дисертаційної роботи безпосередньо пов'язана з виконанням науково-дослідних робіт кафедри «Комп'ютерна інженерія та програмування» НТУ «ХПІ». Здобувач брав участь у двох науково-дослідних роботах:

1. НДР «Моделі і методи обробки та захисту інформації в комп'ютерних системах» (ДР №0122U200526), де замовником виступало ТОВ «Передові цифрові рішення», а здобувач виконував обов'язки керівника цього цієї НДР;

2. НДР «Моделі і методи обробки даних і розподілу мережних ресурсів в комп'ютерних системах» (ДР №0122U200527), де замовником виступала компанія «LineUp», а здобувач брав участь у якості виконавця.

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

Положення та висновки, що наведено в дисертаційній роботі Челака Віктора Володимировича є достатньо обґрунтованими та логічно сформульованими. Їх основою є системність та послідовність у проведенні критичного аналізу методів та засобів виявлення вторгнень у комп'ютерні системи та мережі, використання досвіду побудови моделей машинного навчання та обробки вихідних даних.

Робота відзначається широким спектром використаних сучасних методів комп'ютерного моделювання, зокрема, ансамблевих методів, що дозволило автору не лише дати об'єктивну оцінку ідентифікації стану комп'ютерних систем а й розробити шляхи підвищення оперативності та якості даного процесу.

Сформульовані пропозиції є конкретними, стосуються важливих аспектів, відзначаються науковою новизною та свідчать про вагомий внесок автора у розвиток теорії та практики ідентифікації стану комп'ютерних систем з метою захисту даних. Апробація нових наукових результатів дисертації проводилася на багатьох симпозіумах та конференціях. Розроблені в дисертаційній роботі положення знайшли впровадження системах захисту інформації ряду компаній.

Достовірність результатів досліджень.

Достовірність результатів теоретичних досліджень підтверджується результатами відповідних експериментальних досліджень.

Наукові результати застосовані під час створення програмних засобів ідентифікації стану комп'ютерних систем.

До основних нових наукових результатів дисертації слід віднести наступне:

1. *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 та мереж, що дозволило підвищити точність ідентифікації її стану за рахунок кластеризації вихідних даних та збільшити оперативність ідентифікації завдяки зменшенню кількості розгалужень дерев рішень.

2. *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 та мереж.

3. *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 дерева рішень, що дозволило зменшити час навчання моделі.

4. *Удосконалено* ансамблевий метод класифікації на основі мета-алгоритму Boosting 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.

Значимість отриманих результатів для науки і практичного використання.

Серед практичного значення отриманих результатів можна виділити підвищення точності та швидкості ідентифікації стану комп'ютерних систем, а саме:

– розроблено метод та програмне забезпечення побудови дерев з багатовимірними вузлами рішень, що дозволило зменшити кількість розгалужень та підвищити оперативність ідентифікації стану комп'ютерних систем до 50%, точність до 12%;

– розроблено метод та програмне забезпечення формування нечітких множин та їх функцій належності для побудови нечітких дерев рішень, що дозволило підвищити точність класифікації до 30% за умов великої кількості даних на межі розмежування класів та швидкість до 23% у порівнянні з класичними деревами рішень;

– удосконалено метод та розроблено програмне забезпечення побудови дерева рішень, що дозволило зменшити час навчання дерев з одновимірними вузлами рішень до 4,5 раз;

– удосконалено ансамблевий метод класифікації на основі мета-алгоритму бустінгу та розроблено програмне забезпечення, яке моделює його роботу, що

дозволило підвищити точність класифікації до 32%.

Практична цінність полягає у використанні результатів досліджень:

– в системах безпеки компанії SoftInWay, Inc., головний філіал якої знаходиться в США;

– в системах захисту інформації ТОВ «ФТ ГРУП», офіс якої знаходиться в м. Харків;

– в навчальному процесі кафедри «Комп'ютерної інженерії та програмування» в рамках дисциплін освітніх програм 123 спеціальності: «Розробка систем антивірусного захисту» та «Reverse Programming». (в Національному технічному університеті «Харківський політехнічний інститут»).

Повнота викладення результатів досліджень в опублікованих працях.

Результати досліджень опубліковані у 30 роботах, серед яких: 1 стаття у науковому фаховому виданні України категорії «А» (індексується в базі Web of Science Core Collection), 2 статті у співавторстві з науковим керівником та 6 статей у співавторстві з двома ті більше особами у наукових фахових виданнях України категорії «Б», 4 статті в наукових виданнях України та інших держав (Узбекистан та США), 1 розділ колективної монографії у співавторстві та 16 матеріалів міжнародних конференцій.

Участь здобувача у роботах, що опубліковані у співавторстві зазначена у дисертаційній роботі.

За темою дисертації зараховано 9 публікацій, які 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: 1 стаття у періодичному науковому фаховому виданні категорії «А», яка проіндексовано в базі даних Web of Science Core Collection, 2 статі з двома співавторами (разом із здобувачем) у науковому фаховому виданні України категорії «Б» та 6 статей з трьома та більшою кількістю співавторів у наукових фахових виданнях України категорії «Б» (кожна стаття прирівнюється до 0,5 публікації). Таким чином, виходячи з вимог 8 пункту вищенаведеної постанови,

наукові результати дисертації висвітлені у 6 наукових публікаціях здобувача, що є достатнім для дисертації рівня доктора філософії.

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 наукове та практичне значення, сформульовано мету і наукові задачі дослідження, які необхідно вирішити для її досягнення, описано зв’язок дисертації з науковими планами та темами, приведено апробацію дисертаційної роботи та особистий внесок здобувача в публікаціях.

У першому розділі виконано постановку науково-прикладної задачі захисту даних в комп’ютерних системах та мережах. Проаналізовано основні загрози та фактори, які впливають на функціонування комп’ютерних систем та мереж. Досліджено існуючі методи вирішення задачі та визначено їх основні недоліки. Обґрунтовано вибір методів для подальшого дослідження.

У другому розділі розглянуто алгоритми дерев рішень, наведено визначення поняттям одновимірних та багатовимірних ознак, розроблено метод ідентифікації стану комп’ютерних систем на основі дерев з одновимірними вузлами рішень. Запропоновано метод ідентифікації стану комп’ютерних систем та мереж на основі дерев з багатовимірними вузлами рішень, обґрунтовано його ефективність за умови даних, що мають високі кореляційні зв’язки.

У третьому розділі досліджено використання нечіткої логіки. Доведено, що одним із її недоліків є відсутність автоматичної процедури формування правил, нечітких множин, їх кількості, що робить систему неефективною для задач ідентифікації, коли обсяг даних значний та потребує багато часу та ресурсів.

Запропоновано метод побудови нечітких дерев рішень, який включає автоматичну процедуру фазифікації атрибутів вихідних даних та побудову функції належності. При цьому фазифікація атрибутів відбувається за рахунок статистичного аналізу атрибутів або їх кластеризації.

У четвертому розділі досліджено ансамблеві методи, які поєднують композиції розроблених однорідних базових моделей, що підвищує точність та стійкість алгоритму класифікації за рахунок усереднення чи зважування різних прогнозів. Описано процедуру попередньої обробки даних та процес налаштування класифікатору.

П’ятий розділ містить результати експериментальних досліджень, а саме: вибір показників функціонування комп’ютерних систем та мереж, процес збору вихідних даних для нормального та аномального стану системи, попередню обробку таких даних, формування збалансованої навчальної та тестової вибірки, оцінку отриманих результатів. В розділі приведено вичерпний аналіз ефективності розроблених методів, виконано їх порівняльний аналіз з існуючими методами машинного навчання.

Висновки до розділів сформульовано чітко, вони відповідають змісту дисертаційної роботи та містять основні результати дисертаційного дослідження.

Список використаних джерел складається зі 167 найменувань, є повним і включає зарубіжні публікації, які також опубліковані в базі IEEE.

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

В додатку А представлено список наукових праць здобувача за темою дисертації. В додатку Б представлено фрагменти текстів програм методів ідентифікації стану комп’ютерних систем та мереж. В додатку В зазначено акти впровадження наукових результатів. В додатку Г представлено розрахунки, які допомагають зрозуміти принцип роботи запропонованих методів шляхом вирішуванням меншої за обсягом даних задачі. В додатку Д представлено опис та аналіз метрик якості бінарної класифікації, що дозволяє більш детальніше зрозуміти практичні результати побудованих моделей машинного навчання, які наведено в розділі 5. В додатку Е зазначено структурні схеми розроблених програмних засобів

та їх опис, що доповнює уявлення про програмну реалізацію запропонованих.

Академічна доброчесність

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

Наукові результати, які винесено здобувачем на захист, отримано самостійно і висвітлено в опублікованих роботах. У роботах, опублікованих у співавторстві, використано тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

По дисертаційній роботі можна зробити наступні зауваження:

1. Тема дисертаційної роботи є занадто узагальненою для рівня дисертації доктора філософії. Хоча в роботі було розглянуто різні методи захисту інформації, основну увагу приділено методам ідентифікації стану комп'ютерних систем та мереж, а також системам виявлення вторгнень.

2. У другому розділі в частині опису функції помилки відсутнє обґрунтування вагових коефіцієнтів помилок першого та другого роду. Здобувач робить акценти стосовно пріоритетності помилок другого роду над помилками першого роду в задачах захисту інформації, однак, незрозуміло, яким саме способом було отримано значення вагового коефіцієнту для помилок другого роду (пропуск загрози).

3. У четвертому розділі обґрунтовується спочатку вибір мета-алгоритму Boosting, а потім й базового методу з цієї групи ансамблів, що є надлишковим. Достатньо було вказати лише ті особливості обраного методу, які будуть мати значні переваги в задачі ідентифікації стану комп'ютерних систем.

4. У п'ятому розділі, при аналізі даних використовується метод головних компонент. Частина, що описує його використання та результати обробки, є занадто стислою для розуміння доцільності використання такого аналізу в рамках попередньої обробки даних.

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, яка розв'язує важливу науково-прикладну задачу, яка полягає в підвищенні захищеності комп'ютерних систем та мереж завдяки розробці нових методів та програмних засобах ідентифікації стану таких систем.

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
завідувач кафедри електронних обчислювальних машин
Харківського національного університету радіоелектроніки

Андрій КОВАЛЕНКО

"20" жовтня 2023 р.

ПІДПИС ЗАСВІДЧУЮ
В.о. ректора
доктор технічних наук, професор

Ігор РУБАН

"20" жовтня 2023 р.