ВІДГУК

офіційного опонента

професора кафедри транспортного зв'язку

Українського державного університету залізничного транспорту,

доктора технічних наук, професора Трубчанінової Карини Артурівни

на дисертаційну роботу Горносталя Олексія Андрійовича

«Ансамблевий метод ідентифікації стану комп'ютерних систем»,

представлену на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

Актуальність теми

Роль інформаційних систем у житті сучасної людини неможливо недооцінити, адже вони супроводжують людство майже всюди: від банківських та державних установ до медичної сфери. Незважаючи на їх стрімкий розвиток, питання безпеки інформаційних систем залишається дуже актуальним. Саме тому наукова задача виявлення та запобігання вторгненням у комп'ютерні системи є критичною для забезпечення безпеки даних, захисту від крадіжок інформації та збереження функціональності комп'ютерних систем. Для вирішення цієї задачі використовуються системи ідентифікації вторгнень, які дозволяють виявляти аномалії та зловживання, аналізуючи набори статистичних даних.

В дисертаційній роботі Горносталя Олексія Андрійовича розглядається ефективність використання ансамблевих методів машинного навчання з метою ідентифікації стану комп'ютерної системи. При цьому пропонуються як вдосконалення існуючих підходів, так і розробка нових методів.

Використання методів машинного навчання у виявленні та ідентифікації станів комп'ютерних систем є обґрунтованим з точки зору обробки великих обсягів даних та аналізу складних залежностей. Машинне навчання дозволяє ефективно виявляти аномальні патерни та потенційні загрози без постійного втручання оператора, автоматично виділяючи складні зв'язки між атрибутами даних та вихідною змінною або міткою в задачах класифікації.

Використання саме ансамблевих методів сприяє покращенню точності та стійкості результатів завдяки комбінації декількох моделей машинного навчання, допомагає уникнути перенавчання та забезпечує кращу узагальнюючу здатність.

Крім того, такий підхід забезпечує стійкість до шуму та покращує загальну ефективність системи виявлення та ідентифікації потенційних вторгнень. Завдяки цьому можна стверджувати, що проблематика дисертаційної роботи є актуальною, що також підтверджується участю здобувача у науково-дослідній роботі «Моделі і методи обробки та захисту інформації в комп'ютерних системах» (ДР №0122U200526) за замовленням ТОВ «Передові цифрові рішення», де він був у ролі відповідального виконавця.

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

Дисертаційна робота «Ансамблевий метод ідентифікації стану комп’ютерних систем» Горносталя Олексія Андрійовича є завершеною науковою роботою, містить дві анотації – українською та англійською мовами, вступ, чотири розділи, висновки, списку використаних джерел та 3 додатків.

Вступ містить обґрунтування актуальності обраної теми, огляд дослідників, які зробили найбільший внесок у цьому напрямку, а також розглядається зв’язок роботи з планом науково-дослідних робіт кафедри “Комп’ютерна інженерія та програмування” НТУ “ХПІ”. Крім того, сформульовано мету, об’єкт, предмет задачі та методи дослідження. Окрему увагу приділено науковій новизні, практичним значенням результатів дослідження та особистому внеску здобувача в публікаціях за темою дисертації та матеріалах міжнародних конференцій в рамках апробації.

Перший розділ містить основні фактори ризику при експлуатації комп’ютерних систем та обґрунтування актуальності дисертаційного дослідження, Розглянуто основні види загроз у комп’ютерних системах, а також особливості систем виявлення вторгнень. Досліджено існуючі методи ідентифікації стану комп'ютерної системи та їх основні обмеження, підкреслено ефективність використання ансамблевих класифікаторів. Визначено мету і задачі дисертаційного дослідження.

У другому розділі розглядається застосування беггінг-ансамблів на основі дерев рішень для ідентифікації стану комп’ютерних систем та виконується оцінка

ефективності їх роботи в задачах класифікації. Крім того, розглянуто основні етапи попередньої обробки даних та її потенційний вплив на процес ідентифікації. Досліджено ефективність використання попередньої обробки даних, вибору процедури формування вхідних послідовностей. Розглянуто підходи щодо видалення аномалій у вхідних даних та методи зменшення простору ознак. Виконано налаштування параметрів мета-алгоритму ансамблю та базових моделей.

Третій розділ містить дослідження різних підходів ансамблювання базових моделей беггінг-класифікаторів. Досліджено особливості використання процедури ансамблевої обрізки, зваженого голосування, калібрування впевненості та мета-адаптації. Досліджено ефективність використання багатошарового перцептрону у якості базової моделі ансамблю, розглянуто різні підходи ансамблювання з метою підвищення якості моделі.

У четвертому розділі розглянуто поняття гетерогенних ансамблів, переваги їх застосування. Обґрунтовано вибір методів машинного навчання у якості базових моделей беггінг-ансамблю. Запропоновано метод побудови гетерогенного ансамблю, що передбачає триетапний відбір базових класифікаторів та їх поєднання за допомогою беггінг-процедури Pasting. Використання цього методу дозволяє підвищити якість класифікації, а також формувати ансамблю в залежності від потреб, використовуючи різні значення параметрів налаштування.

За результатами досліджень сформовані відповідні рекомендації з використання отриманих результатів.

У висновках представлені основні науково-практичні результати дисертаційного дослідження, а також їх впровадження. Список використаних джерел містить 137 найменувань.

Додатки містить список публікацій здобувача за темою дисертації, основні складові програм, розроблених в рамках експериментальних досліджень та акти

Достовірність результатів досліджень

Достовірність отриманих результатів зумовлено поставленими метою та завданнями, а також використанням відповідної методології дослідження. Вона

обґрунтовується комплексним підходом у вивченні визначеного об’єкта та підтверджується ретельним планування усіх етапів дослідження. При цьому використовуються сучасні підходи до оцінки ефективності класифікаційних моделей, виконується порівняльний аналіз з іншими моделями, що підтверджує їх достовірними

Наукова новизна одержаних результатів

Дисертація містить наукову новизну. З найбільш суттєвих доробок роботи можна назвати:

1. Отримав подальший розвиток метод ідентифікації стану комп’ютерних систем, який передбачає використання беггінг-ансамблю з деревами рішень, попередню обробку даних з видаленням аномалій методами машинного навчання та з відбором атрибутів фільтраційними методами, а також застосування процедури вибору того, як формуються вхідні дані та обираються оптимальні параметри налаштування дерев та ансамблю.

2. Отримав подальший розвиток метод ідентифікації стану комп’ютерних систем на основі беггінг-ансамблю з багатошаровим перцептроном у якості базової моделі та з процедурою вибору оптимальних налаштувань як окремих класифікаторів, так і їх комбінації.

3. Удосконалено метод ідентифікації стану комп’ютерних систем на основі однорідного (гомогенного) беггінг-ансамблю, шо використовує поєднання процедур ансамблевої обрізки та зваженого голосування.

4. Вперше запропоновано метод ідентифікації стану комп’ютерних систем, що містить процедуру побудови неоднорідного (гетерогенного) беггінг-ансамблю шляхом поетапного відбору базових моделей та їх поєднання за допомогою беггінг-процедури Pasting**.**

Значимість отриманих результатів для науки і практичного використання

Практичне значення отриманих результатів полягає у підвищенні якості ідентифікації стану комп'ютерної системи за рахунок удосконалення та розробки методів класифікації на основі ансамблевих методів.

Вдосконалені та запропоновані у роботі методи ідентифікації стану комп'ютерних систем, що використовують різні модифікації беггінг-ансамблів, дозволяють підвищити якість класифікації, а також збільшити швидкість навчання.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження. Результати дисертації впроваджені та використані в діяльності підприємства ТОВ «Передові цифрові рішення», а також використовуються в навчальному процесі НТУ «Харківський політехнічний інститут».

Повнота викладення результатів досліджень в опублікованих працях

Результати проміжних досліджень представлені на 15 міжнародних наукових конференціях, а також у 5 публікаціях, серед яких 1 стаття у співавторстві з двома чи більше особами в науковому фаховому виданні України категорії «Б», 1 стаття у співавторстві з науковим керівником у науковому фаховому виданні України, що індексується у базі Scopus та 3 статті у співавторстві з науковим керівником у наукових фахових виданнях України категорії «Б».

Згідно з поточними вимогами пункту 8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затверджений Постановою КМУ від 12.01.2022 р. №44, зараховуються 4.5 статті, а саме 4 статті у співавторстві з науковим керівником та 1 стаття з чотирма співавторами, що прирівнюється до 0.5 публікації.

Кількість та зміст опублікованих статей відповідає чинним вимогам.

Оформлення дисертації та дотримання вимог академічної доброчесності

Надану здобувачем дисертацію виконано відповідно «Вимог до оформлення дисертації», затверджених наказом Міністерства освіти і науки України від 12.01.2017 № 40 та із змінами, внесеними згідно з Наказом Міністерства освіти і науки № 759 від 31.05.2019.

Порушень академічної доброчесності (академічного плагіату, самоплагіату, фабрикації, фальсифікації) в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено, про що свідчить аналіз звітів перевірки дисертації на наявність плагіату.

Недоліки та зауваження до дисертаційної роботи

1. У першому розділі на рис. 1.2 наведено структуру виявлення вторгнень, яка включає виявлення аномалій та зловживань. Але, надалі не наведено, яке саме завдання вирішують запропоновані у дисертаційній роботі методи.

2. У другому розділі наведено різні метрики оцінки якості класифікації, але не обґрунтовано їх подальший вибір. Наприклад, не зрозуміло чому метрика NPV – прогностична значущість негативного результату, надалі не використовується для оцінки моделей.

3. У третьому розділі на рис. 3.1 наведено дослідження залежності точності класифікації беггінг-ансамбля від алгоритму формування вибірок даних, але в тексті дисертації не наведено, яким чином формувалося значення індексу класифікатора в рейтинговому списку.

4. У висновках не зазначені особливості можливого комплексного використання вдосконалених та запропонованих в роботі методів ідентифікації стану комп’ютерних систем, що базуються на ансамблевих класифікаторах. Водночас кожен з розділів, в яких розглядуються елементи наукової новизни та експериментальні дослідження, містить власні вичерпні рекомендації.

5. У роботі було б доцільним провести дослідження відносно порогу прийняття рішення класифікатора для балансування помилок першого та другого роду.

Не зважаючи на ці зауваження, необхідно відзначити комплексний підхід та

важливість отриманих наукових результатів, які представлені у роботі. Ці фактори зумовлюють результуючу позитивну оцінку роботи.

ВИСНОВОК

Дисертаційна робота Горносталя Олексія Андрійовича «Ансамблевий метод ідентифікації стану комп'ютерних систем» відповідає спеціальності 123 – Комп'ютерна інженерія та є завершеною науково-дослідною роботою. В рамках дисертації розглядається та вирішується актуальна науково-практична задача ідентифікації стану комп'ютерних систем за допомогою методів машинного навчання, а саме ансамблевих класифікаторів. При цьому здобувач пропонує як вдосконалення існуючих підходів, так і нові методи, а також досліджує їх ефективність за допомогою серії експериментів. За результатами досліджень у дисертаційній роботі формуються відповідні рекомендації щодо подальшого застосування отриманих результатів.

Проаналізувавши зміст дисертаційної роботи Горносталя Олексія Андрійовича «Ансамблевий метод ідентифікації стану комп'ютерних систем» та результати викладених досліджень вважаю, що вона відповідає 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, та відповідає «Вимогам до оформлення дисертації», затверджених наказом Міністерства освіти і науки України від 12.01.2017 № 40, а сам здобувач Горносталь Олексій Андрійович заслуговує присудження йому 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**

Карина Трубчанінова

Особистий підпис
засвідчую 29.05 2024 р.
Завідуючий канцелярією
УкрДУЗТ
Шелько