РЕЦЕНЗІЯ

рецензента, доктора філософії, доцента Коппа Андрія Михайловича

на дисертаційну роботу **Бондаренка Кирила Олександровича**

“Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки”

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 125 – Кібербезпека та захист інформації

Детальний аналіз дисертаційної роботи Бондаренка Кирила Олександровича на тему “Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки”, що представлена для захисту на здобуття наукового ступеня доктора філософії у Національному технічному університеті “Харківський політехнічний інститут”, дає змогу зробити комплексний висновок щодо її актуальності, ступеня обґрунтованості наукових положень, висновків, рекомендацій, достовірності та значущості отриманих результатів, наукової новизни, теоретичної та практичної цінності, надати загальну оцінку дисертації.

1. Актуальність теми та зв’язок з науковими планами і програмами

Організація сучасних мереж щодо складності їх логічної та фізичної складових призводить до певних складностей при розв’язанні питань управління та захисту мереж. За умов проведення діагностики та захисту ресурсів мережі, центральним питанням вирішення основних завдань, щодо забезпечення зазначених складових, виступає оперативне виявлення станів мережі, які спонукають до втрати повної або часткової її працездатності. Також до наслідків можна віднести знищення, спотворення або витоку інформації, причинами яких виступають відмови, збої випадкового характеру або отримання зловмисником несанкціонованого доступу, проникнення зловмисного програмного забезпечення та інших загроз інформаційної безпеки. Раннє виявлення таких станів дозволить своєчасно вжити заходів

щодо протидії загрозам і, відповідно, запобігатиме можливим катастрофічним наслідкам. Тому представлені в роботі методи виявлення аномалій мережі є актуальними та представляють інтерес для захисту інформації.

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

Дисертація виконувалась відповідно до наукової програми 125 "Кібербезпека", яка була впроваджена на кафедрі кібербезпеки, навчально-наукового інституту комп'ютерних наук та інформаційних технологій НТУ "ХПІ".

Проведені дослідження тісно пов'язані з кафедральними науково-дослідними роботами НТУ "ХПІ" "Моделювання соціо-кіберфізичних систем" (ДР № 0123U101018, 2023), "Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі" (ДР №0123U101020, 2023-2025рр.) та "Розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки та підвищення рівня її ефективності у кіберпросторі" (ДР№ 0123U101018, 2023-2025рр.).

3. Наукова новизна одержаних результатів

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

- обґрунтування вибору метрики Махаланобіса у якості основи для визначення аномалій,

- надання більш повної оцінки для визначення спостереження як аномального використання факту, що тільки міра близькості за Махаланобісом бере до уваги корельованість спостережень, яка враховує геометрію розкиду спостережень нормального режиму роботи;

- реалізовані структурні схеми модулів у відповідному програмному забезпеченні моделювання нейронної мережи, що дозволило виявити переваги запропонованих методів над існуючими

Вважаю, що робота дисертанта є внеском у розробку математичних моделей та обчислювальних методів виявлення аномалій в системах безпеки.

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

Дослідження має певну практичну цінність, оскільки автор у якості математичних моделей пропонує нові підходи, які базуються на побудові випадкового лісу з використанням генетичних алгоритмів, що дозволяє побудувати структурні схеми модулів виявлення аномалій у системах кібербезпеки.

5. Повнота викладення матеріалів дисертації в наукових працях, які опубліковані автором.

За результатами дослідження дисертаційної роботи опубліковано 8 наукових праць, з них у фахових наукових виданнях, рекомендованих ДАК Міністерства освіти і науки України – 4, у реферативній базі Scopus – 2, наукових праць, які засвідчують апробацію матеріалів дисертації – 2. Зазначене вище дозволяє стверджувати, що представлена дисертаційна робота є самостійним, завершеним науковим дослідженням, результати якого мають значення для сфери кіберзахисту.

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

Робота Бондаренка К. О. є завершеною науковою роботою, містить анотацію – українською та англійською мовами, вступ, три розділи, висновки, список використаних джерел і додаток.

Дисертація присвячена розробка ефективних комплексних методів виявлення аномалій мережі за інтегральними характеристиками трафіку на основі сучасної теоретичної бази, що визначило напрям дисертаційного дослідження.

Об'єктом дослідження є процеси виявлення аномалій в системах безпеки захисту інформації.

Практичні розробки в галузі виявлення порушень інформаційної безпеки та мережевих аномалій ведуться як університетськими науковими центрами, так і найбільшими комерційними. Однак завдання надійного виявлення мережевих аномалій остаточно не вирішено, про що свідчать аналітичні звіти центрів Інтернет-безпеки, найбільших операторів та координаторів зв'язку, виробників мережного обладнання та систем виявлення вторгнень, а також досвід експлуатації комп'ютерних мереж та магістральних Інтернет-каналів.

В першому розділі узагальнено аналіз сучасного стану виявлення аномалій в системах безпеки, розглянуті мережеві аномалії, їх походження та таксономія. Виявлені джерела походження аномалій в системах безпеки. Наведено зіставлення аномалій з кібератаками, які здійснюються на комп'ютерні системи та мережі та представлено причинно-наслідковий зв'язок між атаками зловмисників, мережевими аномаліями та їх наслідками для безпеки мережі організації.

В другому розділі проаналізовано існуючі теоретичні моделі виявлення аномалій: операційна модель, модель середнього значення та середньоквадратичного відхилення, багатоваріаційна модель, модель марківського процесу, модель часових серій. Запропоновано алгоритм виявлення вторгнень.

Третій розділ дисертації присвячено визначенню ключових моментів штучних нейронних мереж та глибокого навчання при використанні у системах безпеки. Сформульовані відповідності використовуваних методів машинного навчання штучних нейронних мереж та задач кібербезпеки. Наведені таксономії виявлення вторгнень з урахуванням контрольованого та неконтрольованого виявлення вторгнень на основі машинного навчання. Розроблена математична модель виявлення аномалій та вторгнень на основі генетичних алгоритмів. Визначено, яким чином може бути наведена характеристика мережевого трафіку з використанням генетичного алгоритму.

Визначені етапи побудови моделі випадкового лісу з урахуванням генетичного алгоритму для системи виявлення вторгнень.

Четвертий розділ присвячено запропонуванню підходу, який послідовно класифікує відомий трафік атак на різні типи атак та паралельно відокремлює аномалії від звичайного трафіку. Особливу увагу заслуговує демонстрація застосування моделі виявлення зловживань до набору даних KDD CUP 99.

Висновки, сформульовані у роботі, висвітлюють результати дослідження як вирішення висунутих в дисертації завдань. В цілому висновки відповідають вимогам, які висуваються до результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії.

Список літератури досить широко охоплює предметне поле дослідження, певною мірою відображає опрацювання автором значної кількості джерел щодо захисту інформації (в тому числі вітчизняні), математичної статистки, а також іноземних джерел.

Додаток містить інформацію про практичне впровадження результатів дисертації.

7. 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 зумовлює і низку певних методів, які були використані в процесі дослідження.

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

Дисертація виконана з дотримання вимог академічної доброчесності, отримані результати дають підстави говорити про оригінальність роботи. У

тексті містяться авторські ідеї, і не виявлено використання ідей інших науковців без посилання на їх роботи.

Основні ідеї автора та результати дослідження викладено у чотирьох фахових статтях, двох статтях Scopus, а також дисертант активно приймав участь в українських та закордонних конференціях, де була проведена апробація ідей, що викладено у дисертаційному дослідженні.

9. Недоліки та зауваження до дисертаційної роботи

1. У першому розділі (табл. 1.4) розглядається взаємозв'язок послуг безпеки та аномалій, але серед послуг не має автентичності, тому не зрозуміло чи є аномалії на послугу автентичності, та які можуть бути наслідки.

2. Під час розгляду систем виявлення аномалій (п.1.3–1.4) не розглянуті IPS та SIEM платформи. У чому різниця між ними та IDS з точки зору функціональності?

3. У висновках до кожного розділу необхідно було виокремити які саме пункти наукової новизни були розроблено у розділі.

4. У табл. 2.5 розглядаються міри близькості для даних числового, категоріального та змішаного типу, але не зрозуміло, який підхід вважається кращим та чому.

Проте наведені у результаті аналізу роботи зауваження не носять принципового характеру та жодним чином не знижують позитивне враження від роботи та її наукову та практичну цінність.

10. Висновки

Дисертаційна робота Бондаренка К. О. є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Гема дослідження відповідає галузі знань 12 – "Інформаційні технології" та спеціальності 125 – "Кібербезпека та захист інформації".

Отже, враховуючи актуальність теми, отримані результати та певну практичну значущість вважаю, що дисертаційна робота Бондаренка Кирила Олександровича "Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки" 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 сам автор, Бондаренко Кирило Олександрович, заслуговує присудження йому наукового ступеня доктора філософії зі спеціальності 125 "Кібербезпека та захист інформації".

Рецензент – доктор філософії, доцент,
завідувач кафедри програмної інженерії
та інтелектуальних технологій управління
Національного технічного університету
"Харківський політехнічний інститут" Андрій КОПП

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"23" 07
ЗАЙЦЕВ Ю. І.