ВІДГУК

офіційного опонента
Смірнова Олексія Анатолійовича
на дисертаційну роботу Бондаренка Кирила Олександровича
«Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки»,
представлену на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – Кібербезпека та захист інформації

Актуальність теми.

При вирішенні завдань, пов'язаних з діагностикою та захистом мережевих ресурсів, центральним питанням є оперативне виявлення станів мережі, що призводять до втрати повної або часткової її працездатності, знищення, спотворення або витоку інформації, що є наслідком відмов, збоїв випадкового характеру або результатом отримання зловмисником несанкціонованого доступу до мережевих ресурсів, проникнення мережевих хробаків, вірусів та інших загроз інформаційної безпеки. Раннє виявлення таких станів дозволить своєчасно вжити заходів щодо протидії загрозам і, відповідно, запобігатиме можливим катастрофічним наслідкам.

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.

Таким чином, актуальним науково-технічним завданням є розробка ефективних комплексних методів виявлення аномалій мережі за інтегральними характеристиками трафіку на основі сучасної теоретичної бази, що визначило напрям дисертаційного дослідження.

Дисертація присвячена вирішенню завдання забезпечення належного рівня безпеки об'єктів, які повинно бути захищено, шляхом розробки та впровадження математичних моделей та обчислювальних методів виявлення аномалій в системах безпеки. Завдяки використанню розроблених моделей та методів інтелектуального аналізу даних та нейронних мереж для виявлення аномалій стає можливим виявляти та попереджувати невідомі системі безпеки атаки, що є необхідною умовою для підвищення рівня кібербезпеки будь-якої системи.

Дисертаційна робота виконана на кафедрі кібербезпеки НТУ "Харківський політехнічний інститут" у межах ініціативної науко-дослідної роботі "Моделювання соціо-кіберфізичних систем" (ДР № 0123U101018, 2023), де здобувач був виконавцем розділу. Дисертаційна робота є частиною досліджень науково-дослідних робіт НТУ "ХПІ": "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.), де здобувач також був виконавцем розділу.

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

Положення та висновки, наведені в дисертаційній роботі Бондаренка К.О., в достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні математичного апарату теорії інформації для опису мережевих аномалій з використанням ентропії Шенона; інтелктуального аналізу даних для побудови дерев класифікації аномалій в комп'ютерних мережах; нейрокомп'ютінгу для побудови та навчання штучної нейронної мережи виявлення та класифікації аномалій у комп'ютерних та комунікаційних системах; багатовимірного аналізу даних для побудови таксономій методів виявлення вторгнень на основі аномалій.

Дослідження виконані з використанням математичного апарату та сучасного комп'ютерного моделювання. 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 створення інтегрованої системи виявлення вторгнень з використанням штучної нейронної мережі багатошарового перцептрону.

До основних нових наукових результатів дисертації слід віднести наступне:

– *обґрунтовано* вибір метрики Махаланобіса як основи для визначення аномалій, що базується на тому факті, що тільки міра близькості за Махаланобісом бере до уваги корельованість спостережень і, отже, враховує геометрію розкиду спостережень нормального режиму роботи, що дозволяє надати більш повні оцінки для визначення спостереження як аномального;

– *удосконалено* систему причинно-наслідкових зв'язків між атаками зловмисників, мережевими аномаліями та їх наслідками для безпеки мережі організації та структура, що дозволяє визначити вплив аномалій мережевих послуг на цілі безпеки та якості обслуговування;

– *удосконалено* математичну модель виявлення аномалій та вторгнень на основі генетичних алгоритмів, що дозволяє визначити характеристика мережевого трафіку з використанням генетичного алгоритму;

– *удосконалено* підхід, який послідовно класифікує відомий трафік атак на різні типи атак та паралельно відокремлює аномалії від звичайного трафіку, в основі якого лежить розроблена ієрархічна послідовна модель із класифікаторами двійкового дерева рішень на кожному рівні.

Значимість отриманих результатів для науки і практичного використання.

Розроблені у роботі математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки, а саме: моделі побудови випадкового лісу з використанням генетичних алгоритмів, методи нейрокомп'ютінгу дозволили побудувати структурні схеми модулів виявлення аномалій у системах кібербезпеки. Структурні схеми модулів, представлені у дисертаційному дослідженні, реалізовані у відповідному програмному забезпеченні моделювання нейронної мережи, що дозволило виявити переваги запропонованих методів над існуючими.

Теоретичні та практичні результати дисертаційної роботи використано і впроваджено:

– у діяльності ТОВ "Мікрокрипт Текнолоджис" (Харків);

- у навчальний процес для викладання дисциплін "Основи криптографічного захисту", "Комплексні системи захисту інформації" для студентів спеціальності 125 "Кібербезпека та захист інформації", а також "Основи кібербезпеки" для студентів, за спеціальностями 256 "Національна безпека" та 257 "Управління інформаційною безпекою" НТУ "ХПІ".

Повнота викладення результатів досліджень в опублікованих працях.

Результати досліджень опубліковані у 6 роботах, серед яких: 4 статті у наукових періодичних виданнях, що внесені до фахових видань України, 2 статті у наукових виданнях, проіндексованих у міжнародній наукометричній базі даних Scopus. Апробаційні матеріали представлені на 2 міжнародних науково-технічних конференціях.

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 Бондаренка Кирила Олександровича складається з анотації двома мовами, вступу, чотирьох розділів, висновків, списку використаних джерел та 4 додатків. Загальний обсяг роботи викладено на 182 сторінках, серед них: 24 рисунка по тексту, 12 рисунків на 12 окремих сторінках, 17 таблиць по тексту, список використаних джерел з 212 найменувань на 29 сторінках та додатків на 32 сторінках.

У *вступі* обгрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача. Подано відомості про апробацію результатів роботи, особистий внесок здобувача та його публікації.

У *першому розділі* виконано 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. Побудовано відображення впливу аномалій мережевих послуг на цілі безпеки та якості обслуговування. Наведена таксономія методів виявлення вторгнень на основі аномалій, яка грунтується на статистиці, когнітивній основі або знаннях, машинному навчанні або м'яких обчисленнях, інтелектуальному аналізі даних, ідентифікації намірів користувача та комп'ютерної імунології. Сформульовані актуальні проблеми в системах виявлення вторгнень на основі аномалій, що визначають актуальність теми дисертаційної роботи.

У *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. Проаналізовані атрибути заходів та методів виявлення аномалій, що дозволило визначити відповідні методи виявлення аномалії. Проаналізовані традиційні метрики оцінки аномалій для даних числового, категоріального та змішаного типу в системах безпеки. Проведений аналіз метрик аномалій на основі мір близькості дозволив обгрунтувати вибір міри близькості Махалонобіса як основи метрики аномалій. Обгрунтування базується на тому факті, що міра близькості Махалонобіса враховує корельованість спостережень і геометрію розкиду спостережень нормального режиму роботи та дає більш обґрунтовані оцінки для віднесення спостереження до аномального.

У *третьому розділі* проаналізовані різні методи виявлення аномалій на основі машинного навчання. Визначені ключові моменти штучних нейронних мереж та глибокого навчання при використанні в 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.

В *четвертому розділі* запропоновано підхід, який послідовно класифікує відомий трафік атак на різні типи атак та паралельно відокремлює аномалії від звичайного трафіку. Продемонстровано застосування моделі виявлення зловживань щодо набору даних KDD CUP 99. Побудовано набір правил, який містить правила для визначення як звичайного функціонування системи, так і реалізації атак. Запропоновано використання генетичного алгоритму для вибору відповідних значень параметрів, оптимізації RF-класифікатора та підвищення точності

класифікації нормального та аномального мережевого трафіку. Автономну систему виявлення вторгнень реалізовано з використанням побудованої штучної нейронної мережі багаторівневого перцептрона (MLP) та методів побудови дерев класифікації у пакеті Statistica.

У *висновках* дисертаційної роботи викладено основні результати які випливають з проведених досліджень, представлено та охарактеризовано показники ефективності при використанні запропонованих рішень.

Висновки до розділів та за результатами роботи сформульовані чітко та відповідають змісту дисертаційної роботи.

Список використаних джерел із 212 найменувань досить повний і включає вітчизняні та зарубіжні публікації.

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

Академічна доброчесність

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, 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:

Основні наукові результати ґрунтуються на використанні нейроних мереж та дерев класифікації при виявлені аномалій у мережевому трафіку, проте, обґрунтування вибору типу нейронної мережі при цьому відсутнє, хоча і представлені інші типи нейронних мереж. Доцільно було б навести порівняння ефективності роботи розробленого методу на основі використання багато-шарового перцептрону з іншими типами нейронних мереж.

В дисертації слабко обґрунтовано рішення про використання програмного забезпечення для розробки нейронної мережі та дерев класифікації для реалізації задач, поставлених в роботі. Вважаю доцільним зробити порівняння вибраного програмного забезпечення з пакетом проєктування нейронних мереж у програмному забезпеченні MATLAB.

В роботі не наведені витрати часу на навчання побудованої нейронної мережі. Це було б доцільним зробити для вирішення питання про використання нейронної мережі та її адаптації до появи нових видів втручання (а відповідно і аномалій) у реальному часі функціонування.

Існують недоліки оформлення матеріалу дисертаційної роботи, за текстом іноді зустрічаються друкарські, пунктуаційні та стилістичні помилки.

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

ВИСНОВОК

Дисертаційна робота Бондаренка Кирила Олександровича "Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки" за своїм змістом відповідає спеціальності 125 – Кібербезпека та захист інформації. Дисертація є завершеною науково-дослідною роботою, яка розв'язує важливу науково-практичну задачу, яка полягає в забезпеченні належного рівня безпеки об'єктів, які повинно бути захищено, шляхом розробки та впровадження математичних моделей та обчислювальних методів виявлення аномалій в системах безпеки.

Подана дисертаційна робота "Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки" Бондаренка К. О. відповідає спеціальності 125 – "кібербезпека та захист інформації", відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пуиктів 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 Бондаренко Кирило Олександрович заслуговує присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний опонент:

доктор технічних наук, професор,
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор,

Олексій СМІРНОВ

«24» липня 2024 року

Підпис доктора технічних наук, професора, завідувача кафедрою кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету Смірнова Олексія Анатолійовича засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету
кандидат технічних наук, доцент

Андрій ТИХИЙ