ВІДГУК

офіційного опонента

Лаптєва Олександра Анатолійовича

на дисертаційну роботу Бондаренко Кирило 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

Складність логічної та фізичної організації сучасних інформаційних мереж призводить до об’єктивних труднощів при розв’язанні питань управління та захисту інформаційних мереж. При вирішенні завдань, пов’язаних з діагностикою та захистом інформаційних мережевих ресурсів, центральним питанням є оперативне виявлення станів мереж. Раннє виявлення станів втрати повної або часткової працездатності дозволить своєчасно вжити заходів щодо протидії загрозам і, відповідно, запобігатиме можливим катастрофічним наслідкам. Серед численних робіт з моніторингу останнім часом зростає кількість публікацій, присвячених виявленню мережевих аномалій. Для розв’язання цієї задачі застосовується ряд відомих математичних методів обробки, аналізу та моделювання сигналів. 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.

Тому дисертаційна робота Бондаренка Кирила Олександровича, що спрямована на вирішення наукового завдання з розробки ефективних комплексних методів виявлення аномалій мережі за інтегральними характеристиками трафіку на основі сучасної теоретичної бази, є актуальною.

У дисертаційній роботі поставлена наукове завдання з розробки ефективних комплексних методів виявлення аномалій мережі за інтегральними

характеристиками трафіку.

Розробленні 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 нейроної мережи, що дозволяє виявити переваги запропонованих методів над існуючими.

Тема пов'язана з виконанням науково-дослідних робіт 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 був виконавцем розділу.

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

Положення та висновки, наведені в дисертаційній роботі Бондаренко Кирило Олександрович, 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 імовірності та математичної статистики, дисперсійного, кореляційного і спектрального аналізу, методів математичного та імітаційного моделювання з використанням ліцензійного програмного забезпечення.

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 наукових результатів, висновків і рекомендацій підтверджено чисельними експериментами, математичним моделюванням, збіжністю результатів експериментів з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів з результатами обчислювальних експериментів.

До основних нових наукових результатів дисертації слід віднести наступне:

1. Вперше 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.

2. 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.

3. Удосконалено математичну модель виявлення аномалій та вторгнень на основі генетичних алгоритмів, що дозволяє визначити характеристика мережевого трафіку з використанням генетичного алгоритму.

4. 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.

Практична цінність полягає у використанні та впроваджені результатів досліджень:

– в систему безпеки ТОВ “Мікрокрипт Текнолоджис” (м. Харків) у вигляді програмних бібліотек модулів;

– в SIEM-підсистему Інтернет-банкінгу “PLPay” ТОВ “Сайфер ІТ” (м. Київ);

– 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” (м. Харків).

Повнота викладення результатів досліджень в опублікованих працях.

Результати досліджень опубліковані у 8 наукових роботах, серед яких: 1 стаття – у науковому фаховому виданні України категорії “А”, 3 статті – у наукових фахових видання України категорії “Б”, 1 статті – у науко метричному виданні Scopus, 2 – у матеріалах конференцій. 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 зі вступу, чотирох розділів, висновків, списку використаних джерел, 5 додатків.

У вступі обґрунтовано 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 ґрунтується 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 у системах безпеки. Проведений аналіз метрик аномалій на основі мір близькості дозволив обґрунтувати вибір міри близькості Махалонобіса як основи метрики аномалій. Обґрунтування 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 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.

У 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 до 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.

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

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:

1. Дисертант вирішує наукове –технічне завдання – само визначення не існує вже 10 років. Існує для кандидатів Тільки наукове завдання.

2. При обґрунтуванні наукового завдання було би за доцільно навести економічні показники у вигляді графіків або таблиць, які би підкреслювали значимось наукового завдання.

3. У другому розділі запропоновано алгоритм виявлення вторгнень, якій складається із чотирьох основних етапів: генерування вектору сесії, генерування порогового вектору і вектор Бернуллі, генерування вагової мітки вторгнення, обчислення норма підозрілості. Але у наукових результатах його не вказано.

4. У досліджені не читко визначені математичні аспекти, а саме які обмеження використовувались при розробки математичної моделі. Не у явному вигляді наведена розроблена математична модель, що затрудняє розуміння розробки автора.

5. У роботі розроблено висновок, що різні штучні нейронні мережі та методи глибокого навчання, що обговорювалися вище, а також їх варіанти або модифіковані підходи можуть відігравати значну роль для задоволення поточних потреб у контексті кібербезпеки. Але зараз штучний інтелект сам створює проблеми кібербезпеки. Робота була би більш розвинута, якби дисертант більше уваги приділив саме кібератакам за допомогою штучного інтелекту, виявленню загроз що створює штучний інтелект та можливостям виявляти за допомогою штучного інтелекту кібератак, які створює сам штучний інтелект.

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

7. При огляді наукової думки за темою дисертації та досягнень різних вчених, слабко проаналізований внесок вчених з розвинутих країн світу (США, європейських країн, Японії, тощо).

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 наукове завдання, яке полягає у розробки ефективних комплексних методів виявлення аномалій мережі за інтегральними характеристиками трафіку на основі

сучасної теоретичної бази, що визначило напрям дисертаційного дослідження.

Подана дисертаційна робота “Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки” Бондаренко Кирило Олександровича відповідає спеціальності 125 – Кібербезпека та захист інформації, 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 Бондаренко Кирило Олександрович заслуговує присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний опонент
Доцент кафедри кібербезпеки та захисту інформації КНУ імені Тараса Шевченка, д.т.н., с.н.с. Олександр ЛАПТЄВ

Підпис засвідчую
Вчений секретар НДЧ
Караульна Н.В.
25.07 2024 р.