РЕЦЕНЗІЯ

рецензента, доктора технічних наук, професора Кучука Георгія Анатолійовича

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

Ступінь актуальності теми дисертаційної роботи. Для виявлення інформаційних загроз використовуються різні спеціалізовані засоби. При розв’язанні проблем діагностики мереж застосовуються засоби систем управління, аналізатори мережевих протоколів, системи навантажувального тестування, системи мережевого моніторингу. Проблеми захисту інформаційних ресурсів мереж вирішуються за допомогою міжмережевих екранів, антивірусів, систем виявлення атак, систем контролю цілісності, криптографічних засобів захисту. Характерними особливостями використання цих систем є або їх періодичне та короткочасне застосування для розв’язання певної проблеми, або постійне використання, але зі статичними налаштуваннями. В результаті методи аналізу, що використовуються в сучасних системах, спрямовані на виявлення відомих і точно описаних типів впливів, але часто не здатні виявити їх модифікації або нові типи, що робить їх використання малоефективним. Тому тема дисертаційної роботи Бондаренка Кирила Олександровича “Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки”, яка спрямована на забезпечення належного рівня безпеки захищаємих об’єктів шляхом розробки та впровадження математичних моделей та обчислювальних методів виявлення аномалій в системах безпеки, є актуальною з наукової та практичної точок зору та має важливу технічну значущість.

Зв’язок теми дисертаційної роботи з науковими планами, програмами, фундаментальними та прикладними дослідженнями. Тематика дисертаційної роботи відповідає пріоритетним напрямам розвитку науки і

техніки в Україні з розділу «Інформаційні та комунікаційні технології». Дисертація виконувалась відповідно до напрямів досліджень кафедри кібербезпеки навчально-наукового інституту комп'ютерних наук та інформаційних технологій НТУ "ХПІ". Теоретичні та практичні результати дисертаційної роботи було використано і впроваджено в систему безпеки ТОВ "Мікрокрипт Текнолоджис" (м. Харків), в SIEM-підсистему Інтернет-банкінгу "PLPay" ТОВ "Сайфер ІТ" (м. Київ), а також у навчальний процес НТУ "ХПІ" для викладання дисциплін "Основи криптографічного захисту", "Комплексні системи захисту інформації".

Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі. Ґрунтовно проаналізувавши дисертаційну роботу можна відмітити, що наукові положення, висновки та рекомендації, що висвітлені в роботі, є достатніми, повними, а також належними чином повністю обґрунтованими. Для їх отримання та підтвердження автором було проведено як теоретичні, так і емпіричні, експериментальні дослідження, при цьому використовувалися вітчизняні та міжнародні вузькопрофільні та актуальні джерела. Достовірність положень і висновків зроблених автором підтверджується використанням класичних і сучасних методів досліджень, зокрема глибоким логічним аналізом літературних джерел, коректністю поставлених актуальних завдань, що потребують розв'язання та вирішення. Результати експериментальних та теоретичних досліджень доповідались та обговорювались на міжнародних науково-технічних конференціях, а також опубліковані в наукових фахових виданнях. Крім того, про достовірність отриманих результатів свідчить їх взаємоузгодженість, відповідність літературним даним і позитивні результати впровадження. У результаті проведення дисертаційного дослідження дисертанту вдалось розкрити та вирішити в повному обсязі мету та завдання, що були сформовані на початку роботи. До кожного пункту роботи приведені логічні висновки, які дозволяють коротко та повно зрозуміти суть кожного етапу дослідження та практичну значущість отриманих результатів. Також

достовірність заявлених положень обґрунтовується комплексним підходом у вивченні визначеного об'єкта.

Вищевикладене свідчить про обґрунтованість та достовірність наукових положень, висновків і рекомендацій, що викладено у дисертаційній роботі Бондаренка Кирила Олександровича.

Наукова новизна положень, висновків та рекомендацій, сформульованих у дисертації. Наукова новизна отриманих результатів обумовлена теоретичним узагальненням і новим рішенням важливого наукового завдання, сутність якого полягає в розробці ефективних комплексних методів виявлення аномалій мережі за інтегральними характеристиками трафіку на основі сучасної теоретичної бази. У дисертаційній роботі отримані такі основні науково обґрунтовані результати:

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.

2. Удосконалено систему причинно-наслідкових зв'язків між атаками зловмисників, мережевими аномаліями та їх наслідками для безпеки мережі організації та структура.

3. Удосконалено математичну модель виявлення аномалій та вторгнень на основі генетичних алгоритмів.

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.

Наукова та практична цінність одержаних результатів. Робота має чітку послідовність постановки задач та отриманих рішень, достатню доказову базу та аргументованість результатів. Використано сучасний математичний апарат для реалізації сформованої мети. Порівняльні оцінки запропонованих автором нових рішень щодо результатів, які отримані провідними вченими та дослідниками в галузі, достатньо аргументовані та відповідають списку

приведених першоджерел. Висновки та рекомендації, які сформульовані в дисертаційній роботі, враховують сутність та актуальність наукового завдання роботи та її мету, вони є придатними для 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.

Результати дисертації впровадженні та використані в в систему безпеки ТОВ "Мікрокрипт Текнолоджис" (м. Харків), в SIEM-підсистему Інтернет-банкінгу "PLPay" ТОВ "Сайфер ІТ" (м. Київ), а також використовуються в навчальному процесі Національного технічного університету "ХПІ".

Повнота викладення наукових і прикладних результатів дисертації в опублікованих працях. Основні ідеї здобувача та результати дослідження достатньо повно викладені у одноосібній статті у фаховому журналі категорії Б, у статтях із співавторами у фаховому журналі категорії А (3 квартіль) та у фаховому журналі категорії Б, що відповідає вимогам МОН України до опублікування результатів досліджень на здобуття наукового ступеня доктора філософії. Достатню апробацію результати досліджень отримали на 2 міжнародних конгресах з індексацією матеріалів у СКОПУС та 2 міжнародних науково-технічних конференціях.

Оцінка змісту дисертації, її завершеності й оформлення. Побудова дисертації відповідає прийнятим для наукового дослідження нормам. Усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві.

Дисертація написана грамотною науковою мовою та оформлена відповідно до існуючих нормативних документів, текст і графічний матеріал виконані акуратно з використанням комп'ютерної техніки.

Дисертація складається з анотацій, вступу, 4 розділів, висновків, списку використаних джерел і 5 додатків. Обсяг основного тексту дисертації (без анотацій, змісту, списку використаних джерел і додатків) становить 118 сторінок, що відповідає встановленим вимогам.

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета і задачі дослідження, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У першому розділі дисертації наведено зіставлення аномалій з кібератаками, які здійснюються на комп'ютерні системи та мережі, а також 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.

У другому розділі 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 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 включає побудову набору правил. Вони представлені правилами 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.

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

Список використаних джерел широко охоплює предметне поле дослідження, певною мірою відображає опрацювання автором значної кількості джерел пов'язаних з захистом інформації, інтелектуальними методами та метриками оцінки їх ефективності.

Додатки містять додаткову інформацію про проведені здобувачем дослідження, публікації здобувача та практичне впровадження результатів дисертації.

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.

Зауваження до дисертаційної роботи. В процесі ознайомлення з роботою позитивне враження справило докладне обґрунтовування усіх висунутих у роботі положень, використання сучасних математичних методів.

Але при цьому виникли такі зауваження:

1. У першому розділі здобувачем проведений детальний аналіз сучасного стану виявлення аномалій у системах безпеки. Але постановочна частина дисертації виглядала б краще, якби більш наглядно (у вигляді діаграм та графіків) були б наведені результати аналітичного огляду основних

характеристик розглянутих підходів щодо виявлення вторгнень на основі аномалій. Це підвищило б ступінь обґрунтованості зробленого автором висновку щодо необхідності розробки ефективних комплексних методів виявлення аномалій мережі за інтегральними характеристиками трафіку на основі сучасної теоретичної бази.

2. У підрозділі 2.3 роботи розглянуті оцінювальні метрики, що використовуються для виявлення та класифікації аномалій на основі мір близькості, та доведена суттєва перевага метрики Махалонобіса над евклідовою метрикою. Але слід зазначити, що обґрунтованість зробленого вибору міри близькості Махалонобіса як основи метрики аномалій підвищилась би у разі порівняння обраної метрики ще з декількома застосованими на сьогодні метриками.

3. У підрозділі 3.2 здобувач запропонував математичну модель системи інформаційної безпеки на основі використання генетичного алгоритму для аналізу характеру мережного трафіку, але не розглянув питання щодо адекватності розробленої моделі реальному мережному процесу.

4. У підрозділі 4.2 здобувачем розглянуто класифікацію аномалій з використанням моделі випадкового лісу на основі генетичного алгоритму виявлення мережних атак. Бажано було б при цьому навести інформацію щодо можливих мережних атак, зокрема, виділити, на які протоколи ці атаки "націлені".

Відповідність дисертації встановленим вимогам і загальні висновки. Зазначені недоліки не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової та практичної цінності. Вони не є визначальними і можуть бути враховані як напрямки подальших досліджень.

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

За змістом, актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота "Математичні моделі та обчислювальні методи виявлення аномалій в системах безпеки" відповідає вимогам п.п. 6–9 "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", із змінами, внесеними згідно з Постановою Кабінету Міністрів України № 341 від 21.03.2022, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор, Бондаренко Кирило Олександрович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Рецензент – професор кафедри комп'ютерної
інженерії та програмування
Національного технічного університету
"Харківський політехнічний інститут"
доктор технічних наук, професор Георгій КУЧУК

Підпис проф Георгія Кучука
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО-ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ЗАЙЦЕВ Ю. І.
"22" 08 2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет "Харківський політехнічний інститут"
код 02071180