Голові разової спеціалізованої вченої ради за спеціальністю 122 «Комп'ютерні науки» в галузі знань 12 «Інформаційні технології» Національного технічного університету «Дніпровська політехніка», м. Дніпро, д.т.н., професору, професору кафедри програмного забезпечення комп'ютерних систем
Борису МОРОЗУ

рецензента, д.т.н., професора, завідувача кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка», м. Дніпро
Михайла АЛЕКСЄЄВА

РЕЦЕНЗІЯ

д.т.н., професора, завідувача кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка»
АЛЕКСЄЄВА Михайла Олександровича
на дисертаційну роботу **МЄШКОВА Вадима Ігоровича**
«Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак», подану на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки»

1. Актуальність теми дисертації

Дисертаційна робота Мєшкова Вадима Ігоровича присвячена важливій науково-прикладній задачі розроблення інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. Актуальність такого напряму дослідження визначається тим, що сучасні комп'ютерні мережі функціонують в умовах постійного зростання обсягів переданих даних, ускладнення структури мережевих взаємодій та підвищення інтенсивності кіберзагроз.

Традиційні засоби виявлення атак, що переважно орієнтовані на використання сигнатур або заздалегідь визначених правил, не завжди здатні ефективно реагувати на нові, модифіковані або комбіновані види атак. У зв'язку з цим особливого значення набувають інформаційні технології, що

використовують методи машинного навчання для аналізу мережевого трафіку, виявлення прихованих закономірностей у даних та автоматизованого прийняття рішень щодо наявності атакувальної активності.

Важливість дисертаційного дослідження посилюється тим, що в роботі розглядається не лише задача встановлення факту атаки, а й задача подальшого розпізнавання її типу. Такий підхід є практично доцільним для систем кібербезпеки, оскільки дозволяє не обмежуватися загальним повідомленням про інцидент, а формувати більш інформативні результати моніторингу, придатні для подальшого аналізу та реагування.

Обрана тема дисертації є своєчасною, відповідає сучасним потребам розвитку інформаційних технологій і кібербезпеки та має вагоме значення для створення ефективних програмних засобів інтелектуального аналізу мережевого трафіку в системах виявлення атак.

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

Рецензована дисертаційна робота виконувалася в межах наукової діяльності Національного технічного університету «Дніпровська політехніка» та відповідає напряму досліджень кафедри безпеки інформації та телекомунікацій. Зміст роботи узгоджується з тематикою науково-дослідної роботи «Інтелектуальні методи моделювання процесів в інформаційно-телекомунікаційних системах критичної інфраструктури» з державним обліковим номером 0225U004731, із терміном виконання 2024-2025 рр.

У межах зазначеного наукового напряму дисертантом розглянуто питання, безпосередньо пов'язані з інтелектуальним аналізом мережевого трафіку, підготовкою даних для задач виявлення атак, побудовою моделей машинного навчання та оцінюванням їх ефективності. Отримані результати спрямовані на вдосконалення інформаційних технологій моніторингу комп'ютерних мереж і можуть розглядатися як складова наукових досліджень у сфері захисту інформаційно-телекомунікаційних систем.

Таким чином, тема дисертації має чіткий зв'язок із науковими планами та дослідницькою тематикою закладу, а виконані здобувачем розробки відповідають актуальним завданням інтелектуального моделювання, аналізу даних і забезпечення кібербезпеки інформаційних систем.

3. Обґрунтованість і достовірність наукових положень, висновків та рекомендацій

Наукові положення та висновки, сформульовані в дисертації Мєшкова Вадима Ігоровича, мають належний рівень обґрунтованості, оскільки базуються

на послідовному поєднанні теоретичного аналізу предметної області, формалізації задачі інтелектуального виявлення атак, програмної реалізації запропонованої інформаційної технології та експериментальної перевірки її ефективності.

Достовірність результатів забезпечується використанням репрезентативного набору даних CIC-IDS2017, на основі якого проведено дослідження для двох постановок задачі: бінарного виявлення атакувального трафіку та багатокласового розпізнавання типів атак. У роботі обґрунтовано, що результативність інтелектуального виявлення атак залежить не лише від вибору моделі машинного навчання, а й від якості підготовки даних, правильності формування ознакового простору та коректності системи оцінювання.

Важливою передумовою надійності отриманих результатів є реалізація повного циклу обробки мережевого трафіку: очищення даних, уніфікація ознак, стандартизація числових характеристик, зниження розмірності, формування вибірок, балансування даних, навчання моделей та оцінювання якості класифікації. Така послідовність зменшує вплив випадкових похибок, дублювання, пропущених або некоректних значень на кінцеві результати дослідження.

Експериментальна частина роботи побудована з використанням комплексу взаємодоповнювальних метрик, зокрема accuracy, precision, recall, F1-score, ROC-AUC, Precision–Recall-кривих, матриць помилок і п'ятикратної перехресної перевірки. Це дозволяє оцінювати моделі не лише за загальною точністю, а й з урахуванням повноти виявлення атак, рівня помилкових спрацювань та здатності моделей працювати з різними класами трафіку.

Додатково слід відзначити, що автор не обмежився перевіркою одного алгоритму, а виконав порівняння кількох моделей машинного навчання. Для задачі бінарного виявлення атак досліджено логістичну регресію та метод опорних векторів, а для багатокласового розпізнавання типів атак – дерево рішень, випадковий ліс і метод k-найближчих сусідів. Це підвищує переконливість зроблених висновків і дає змогу обґрунтовано визначити ефективні конфігурації моделей для різних режимів функціонування інформаційної технології.

Таким чином, наукові положення, висновки та рекомендації дисертаційної роботи є логічно узгодженими, методично обґрунтованими та підтвердженими результатами експериментального дослідження. Використані методи й засоби оцінювання відповідають поставленій меті роботи та забезпечують достатній рівень достовірності одержаних результатів.

4. Оцінка наукової новизни результатів дисертації

У дисертаційній роботі Мєшкова Вадима Ігоровича отримано результати, які мають ознаки наукової новизни та відповідають заявленій меті дослідження. Їх сутність полягає у формуванні комплексного підходу до інтелектуального моніторингу мережевого трафіку, в якому поєднано підготовку даних, побудову ознакового простору, навчання моделей машинного навчання та оцінювання результатів класифікації в межах єдиної інформаційної технології.

Найбільш вагомим результатом роботи є розроблення інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. Її відмінність полягає в тому, що вона забезпечує не лише виконання окремої процедури класифікації, а повний цикл опрацювання мережевих даних: від попередньої підготовки та формування вибірок до навчання моделей і комплексної перевірки їх ефективності. У дисертації зазначено, що технологія орієнтована на дві взаємопов'язані постановки задачі – бінарне виявлення атак і багатокласове розпізнавання їх типів.

Наукову цінність має також удосконалення методу підготовки даних, класифікації та оцінювання мережевого трафіку. Запропонований підхід об'єднує процедури очищення, уніфікації, стандартизації, аналізу ознак, зниження розмірності, балансування вибірок і навчання моделей машинного навчання. Завдяки такому поєднанню підготовка даних розглядається як невід'ємна частина процесу побудови ефективної системи виявлення атак, а не як допоміжний технічний етап.

Окремо слід відзначити розвиток підходів до оцінювання моделей машинного навчання в задачах аналізу мережевого трафіку. У роботі використано систему взаємодоповнювальних показників, що дозволяє оцінювати результати не лише за загальною точністю, а й за покласовими характеристиками, повнотою виявлення атак, рівнем помилкових рішень та стабільністю моделей під час перехресної перевірки.

Наукова новизна дисертації полягає у створенні та експериментальному підтвердженні цілісного програмно-методичного підходу до інтелектуального моніторингу мережевого трафіку. Отримані результати поглиблюють науково-прикладні засади побудови інтелектуальних компонентів систем виявлення атак і є значущими для розвитку інформаційних технологій у сфері кібербезпеки.

5. Оцінка структури, змісту, завершеності та оформлення дисертаційної роботи

Структура дисертаційної роботи Мєшкова Вадима Ігоровича відповідає логіці науково-прикладного дослідження у галузі 12 «Інформаційні технології», спеціальності 122 «Комп'ютерні науки». Матеріал подано у послідовності, яка

дозволяє простежити весь шлях розв'язання поставленої задачі: від аналізу сучасного стану систем виявлення атак до формування методу, розроблення інформаційної технології, її програмної реалізації та експериментальної перевірки.

У вступі визначено актуальність теми, мету, завдання, об'єкт і предмет дослідження, наведено наукову новизну, практичне значення отриманих результатів, відомості про апробацію та публікації здобувача. Це створює необхідну основу для розуміння загальної спрямованості дисертаційної роботи.

Перший розділ має аналітичний характер. У ньому розглянуто сучасні підходи до моніторингу мережевого трафіку, класифікацію IDS-систем, методи виявлення атак і особливості застосування машинного навчання в задачах аналізу трафіку. Такий огляд є доцільним, оскільки дає змогу обґрунтувати вибір напряму подальшого дослідження.

У другому розділі сформовано методичну основу роботи. Автор розглядає задачу виявлення атак у двох постановках – бінарній та багатокласовій, обґрунтовує використання набору даних CIC-IDS2017, описує процедури очищення, уніфікації, стандартизації, аналізу ознак, зниження розмірності та балансування вибірок. Саме цей розділ забезпечує перехід від загальної постановки задачі до конкретної послідовності обробки даних мережевого трафіку.

Третій розділ присвячено безпосередньо розробленню інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі. У ньому подано архітектуру технології, описано конвеєр обробки даних, двоетапну схему класифікації, вибір програмних засобів і структуру програмного модуля. Важливо, що технологія орієнтована на повний цикл роботи з мережевими даними – від попередньої підготовки до класифікації та використання результатів у системах виявлення атак.

У четвертому розділі наведено експериментальну перевірку запропонованих рішень. Результати дослідження подано для двох режимів функціонування технології: первинного виявлення атакувального трафіку та подальшого розпізнавання типів атак. Така побудова експериментальної частини є виправданою, оскільки відповідає загальній логіці запропонованої двоетапної схеми аналізу мережевого трафіку.

Зміст дисертації відповідає її темі та поставленій меті. Розділи взаємопов'язані між собою, висновки випливають із проведених досліджень, а запропоновані методичні положення доведені до рівня програмної реалізації та експериментальної оцінки. Оформлення роботи загалом відповідає вимогам до кваліфікаційних наукових праць: матеріал викладено науковим стилем, із використанням фахової термінології, таблиць, рисунків і результатів експериментального аналізу. Дисертаційна робота є структурно завершеною,

змістовно цілісною та оформленою на належному науково-технічному рівні.

6. Практичне значення результатів дисертаційної роботи

Практичне значення дисертаційної роботи Мєшкова Вадима Ігоровича полягає в тому, що запропоновані в ній методичні, алгоритмічні та програмні рішення можуть бути використані для створення інтелектуальних компонентів систем виявлення атак у комп'ютерних мережах.

Розроблена інформаційна технологія забезпечує автоматизоване опрацювання мережевого трафіку, підготовку даних до аналізу, формування ознакового простору, навчання моделей машинного навчання та оцінювання результатів класифікації. Її прикладна цінність полягає в можливості поєднання двох практично важливих задач: первинного виявлення атакувальної активності та подальшого визначення типу атаки. У дисертації зазначено, що така технологія може бути використана як основа для побудови інтелектуальних компонентів IDS у комп'ютерних мережах.

Важливим є те, що результати роботи не залишилися на рівні теоретичних положень. У межах дослідження створено програмну реалізацію, яка охоплює завантаження й інтеграцію даних, їх очищення, обробку пропущених і некоректних значень, стандартизацію ознак, формування вибірок для бінарної та багатокласової класифікації, навчання моделей, а також візуалізацію отриманих результатів. Це свідчить про достатній рівень прикладної завершеності дисертаційної роботи.

Практична придатність отриманих результатів підтверджується тим, що розроблена технологія забезпечує моніторинг мережевого трафіку, своєчасне виявлення атакувальної активності та деталізацію інцидентів за типами атак, що підвищує ефективність підтримки прийняття рішень у сфері кібербезпеки. Результати дисертаційної роботи впроваджено в діяльність ТОВ «Центум-Д» та в освітній процес Національного технічного університету «Дніпровська політехніка».

Практична цінність дисертаційної роботи полягає у можливості використання її результатів як у прикладних задачах кіберзахисту корпоративних мереж, так і в освітньому процесі та подальших науково-прикладних дослідженнях з інтелектуального аналізу мережевого трафіку.

7. Повнота оприлюднення та апробації результатів дисертації

Основні результати дисертаційної роботи Мєшкова Вадима Ігоровича належним чином представлені в наукових публікаціях, що відповідають тематиці дослідження та розкривають його ключові положення. Зокрема, у фахових

виданнях України опубліковано праці (4 роботи), присвячені методам машинного навчання для бінарної та багатокласової класифікації мережевого трафіку, попередній обробці даних для інтелектуальних систем виявлення атак, підвищенню кібербезпеки електронних комунікаційних систем, а також аналізу систем інтелектуального моніторингу трафіку комп'ютерної мережі.

Публікації здобувача відображають основні етапи виконаного дослідження: аналіз предметної області, формування підходів до підготовки даних, використання моделей машинного навчання для класифікації мережевого трафіку та обґрунтування інформаційної технології інтелектуального моніторингу. Це дає підстави вважати, що наукові результати дисертації достатньо повно висвітлені у відкритому науковому друці.

Апробація результатів здійснювалася шляхом їх представлення на науково-технічних і науково-практичних конференціях. У матеріалах конференцій висвітлено питання архітектури інформаційної технології, кореляційного аналізу показників набору даних CSE-CIC-IDS2017, перспективних напрямів моніторингу мережевого трафіку для IDS, аналізу наборів даних, сучасних систем моніторингу трафіку, ідентифікації та прогнозування мережевого трафіку, а також розроблення інформаційної технології інтелектуального моніторингу для систем виявлення атак.

Отже, тематика, зміст і кількість опублікованих праць та апробаційних матеріалів свідчать про достатній рівень оприлюднення результатів дисертаційного дослідження. Основні положення роботи пройшли належне обговорення в науковому середовищі та відповідають змісту дисертації.

8. Відповідність дисертаційної роботи спеціальності 122 «Комп'ютерні науки»

Зміст дисертаційної роботи Мєшкова Вадима Ігоровича повністю узгоджується з предметною областю спеціальності 122 «Комп'ютерні науки». Дослідження спрямоване на розроблення інформаційної технології, алгоритмічне забезпечення процесів обробки даних, застосування методів машинного навчання та створення програмної реалізації для автоматизованого аналізу мережевого трафіку.

У роботі розглянуто типові для комп'ютерних наук задачі: попередню обробку великих обсягів даних, формування ознакового простору, зниження розмірності, побудову класифікаційних моделей, програмну реалізацію інформаційної технології та експериментальне оцінювання її ефективності. Такі складові безпосередньо відповідають напряму розроблення методів, моделей, алгоритмів і програмних засобів опрацювання інформації.

Окремо слід відзначити, що дисертаційна робота має чітку інформаційно-

технологічну спрямованість: запропоновані рішення орієнтовані на автоматизацію процесу моніторингу мережевого трафіку, підтримку прийняття рішень у системах виявлення атак і підвищення ефективності інтелектуального аналізу даних у задачах кібербезпеки.

Таким чином, тема, мета, завдання, методи дослідження, отримані наукові результати та практична реалізація дисертаційної роботи відповідають спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

9. Дотримання вимог академічної доброчесності

Аналіз дисертаційної роботи Мєшкова Вадима Ігоровича дає підстави зробити висновок про дотримання здобувачем принципів академічної доброчесності. У роботі використано наукові джерела, нормативні та довідкові матеріали, результати попередніх досліджень інших авторів із належним посиланням на відповідні публікації.

Подані в дисертації наукові результати, висновки та практичні розробки узгоджуються з тематикою власних публікацій здобувача і відображають особистий внесок автора у розв'язання поставленої науково-прикладної задачі. Виклад матеріалу свідчить про самостійне опрацювання предметної області, виконання експериментальних досліджень і формування авторських висновків щодо ефективності запропонованої інформаційної технології.

Під час ознайомлення з дисертацією не встановлено ознак неправомірного запозичення тексту, некоректного використання результатів інших дослідників, фабрикації або фальсифікації експериментальних даних. Отже, дисертаційна робота відповідає вимогам академічної доброчесності, що висуваються до кваліфікаційних наукових праць.

10. Дискусійні положення та зауваження до дисертаційної роботи

Позитивно оцінюючи дисертаційну роботу Мєшкова Вадима Ігоровича, слід зазначити окремі положення, які мають дискусійний характер і можуть бути враховані автором у подальших дослідженнях.

1. У дисертаційній роботі запропоновано інформаційну технологію інтелектуального моніторингу мережевого трафіку, однак доцільно було б детальніше визначити вимоги до вхідних даних, які повинні надходити до такої технології. Зокрема, варто було б конкретизувати, чи передбачається робота лише з потоковими характеристиками трафіку, чи також можливе використання пакетних, сесійних або журналових даних із мережевих пристроїв.

2. У роботі використано процедури зниження розмірності ознакового

простору, що є обґрунтованим з погляду зменшення надлишковості даних. Водночас бажано було б ширше проаналізувати, чи не призводить таке зниження розмірності до втрати специфічних ознак, характерних для окремих типів атак, особливо тих, що мають малу представленість у вибірці.

3. У дисертації наведено результати класифікації мережевого трафіку, однак питання оцінювання впевненості моделей у прийнятих рішеннях розкрито недостатньо. Для практичного застосування систем виявлення атак корисним було б врахування не лише класу, визначеного моделлю, а й рівня довіри до такого рішення, що може бути важливим під час пріоритезації інцидентів.

4. Доцільно було б окремо розглянути вплив можливих похибок розмітки даних на результати навчання та оцінювання моделей. У наборах мережевого трафіку помилки маркування або неоднозначність віднесення окремих записів до класів можуть впливати на якість класифікації, тому аналіз стійкості запропонованої технології до таких факторів посилив би експериментальну частину роботи.

5. У роботі основну увагу приділено технічним аспектам підготовки даних і побудови моделей машинного навчання, однак питання захисту самих даних мережевого трафіку в процесі їх зберігання, обробки та використання розкрито обмежено. З огляду на те, що мережевий трафік може містити чутливу інформацію, доцільно було б окреслити вимоги до безпечного поводження з такими даними під час практичного впровадження запропонованої технології.

Зазначені зауваження не знижують наукової новизни, достовірності та практичної значущості результатів дисертаційної роботи. Вони мають рекомендаційний характер і можуть бути враховані під час подальшого розвитку інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак.

11. Загальний висновок

Дисертаційна робота Мєшкова Вадима Ігоровича «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак» є завершеною кваліфікаційною науковою працею, у якій отримано науково обґрунтовані та практично значущі результати для розв'язання задач інтелектуального аналізу мережевого трафіку.

У дисертації розроблено інформаційну технологію, що забезпечує підготовку даних, формування ознакового простору, застосування моделей машинного навчання та оцінювання результатів класифікації мережевого трафіку в задачах виявлення атак і розпізнавання їх типів. Запропоновані рішення мають наукову новизну, підтверджені результатами експериментальних досліджень і можуть бути використані для побудови інтелектуальних компонентів систем

кібербезпеки.

Зміст дисертації відповідає заявленій темі, меті та завданням дослідження. Основні результати достатньо повно відображені в наукових публікаціях здобувача, апробовані на наукових конференціях і мають практичне впровадження. Зауваження, наведені в рецензії, не впливають на загальну позитивну оцінку роботи та не знижують її наукової і практичної цінності.

Вважаю, що дисертаційна робота Мєшкова Вадима Ігоровича відповідає вимогам, які висуваються до дисертацій на здобуття ступеня доктора філософії (відповідно вимогам чинному Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженому постановою Кабінету Міністрів України від 12.01.2022 № 44), а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Рецензент:
д.т.н., професор, завідувач
кафедри програмного забезпечення
комп'ютерних систем,
НТУ «Дніпровська політехніка» Михайло АЛЕКСЄЄВ