РЕЦЕНЗІЯ

професора кафедри комп'ютерних систем, мереж та кібербезпеки
Національного університету біоресурсів і природокористування України,
доктора технічних наук, професора **КРИВОРУЧКО Олени Володимирівни**
на дисертацію **ШТАНЬКА Вадима Ігоровича**
на тему: **«Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак»**,
подану на здобуття ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки»
галузі знань 12 «Інформаційні технології»

Актуальність обраної теми. Дисертація В. І. Штанька присвячена дослідженню проблеми створення інформаційної технології аналізу мережевих атак, що має важливе значення для розвитку сучасних систем виявлення вторгнень.

Актуальність теми зумовлена зростанням складності кібератак та необхідністю підвищення ефективності систем виявлення вторгнень у сучасних інформаційно-комунікаційних мережах.

Додаткової уваги заслуговує акцент здобувача на проблемі статистичних відмінностей мережевого трафіку між середовищами навчання та експлуатації. У дисертації показано, що параметри трафіку у цільовому середовищі можуть суттєво відрізнятися через топологію мережі, фонове навантаження й особливості сценаріїв атак, що призводить до неконтрольованого зростання помилок класифікації.

Таким чином, розроблення інформаційної технології, що поєднує дворівневу ієрархічну класифікацію, механізми оцінювання статистичних розбіжностей мережевого трафіку та політику керованої відмови від рішення в умовах невизначеності, є актуальним завданням у сфері інтелектуального аналізу мережевих даних.

Структура та зміст дисертації. Дисертація складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел та додатків. Робота викладена на 183 сторінках і містить рисунки, таблиці та список літератури.

У **вступі** обґрунтовано актуальність теми, сформульовано мету та завдання дослідження; визначено об'єкт і предмет; викладено наукову новизну й практичне значення; наведено дані щодо апробації, публікацій та впровадження результатів. Зокрема мета роботи визначена як підвищення ефективності виявлення та класифікації мережевих атак в умовах варіативної зміни характеристик трафіку шляхом розроблення дворівневої інформаційної технології на основі ієрархії моделей машинного навчання.

У **першому розділі** виконано аналіз сучасного стану та тенденцій розвитку методів машинного навчання у системах виявлення вторгнень. Розглянуто основні підходи до побудови систем аналізу мережевого трафіку, типові архітектурні рішення та проблеми їх практичного застосування. Увагу приділено методологічним обмеженням традиційних схем

оцінювання ефективності моделей, зокрема пов’язаним із використанням контрольованих підвибірок одного набору даних та перенесенням моделей у нові середовища. Автором показано, що високі результати, отримані на ізольованих наборах даних, не гарантують стабільної роботи систем виявлення вторгнень у реальних мережевих умовах, де характеристики трафіку можуть істотно змінюватися.

Другий розділ присвячено розробленню методів та моделей прийняття рішень у дворівневій системі виявлення вторгнень. У розділі розглянуто використання ймовірнісних і ансамблевих методів машинного навчання для побудови ієрархічної моделі аналізу мережевого трафіку. Запропоновано теоретичну модель дворівневої системи прийняття рішень на основі баєсівської мінімізації ризику, що реалізує первинну фільтрацію мережевого трафіку та подальшу уточнену класифікацію типів атак. Окрему увагу приділено математичній моделі оцінювання доменного зсуву мережевого трафіку на основі інформаційної дивергенції, що дозволяє адаптивно налаштовувати поріг прийняття рішень у системі.

У **третьому розділі** подано результати експериментального дослідження запропонованих моделей та проведено їх аналіз у різних умовах функціонування системи.

У **висновках** узагальнено основні результати проведеного дослідження, сформульовано положення наукової новизни та практичної значущості роботи, а також окреслено перспективні напрями подальшого розвитку запропонованого підходу за умов гетерогенності мережевих середовищ та зростання складності мережевих атак.

Ступінь обґрунтованості, новизни та достовірності наукових положень, висновків і рекомендацій. Ступінь обґрунтованості результатів підтверджується використанням сучасних методів машинного навчання, проведенням експериментальних досліджень та порівнянням отриманих результатів із результатами інших дослідників.

Достовірність результатів посилюється застосуванням віконного (синхронного) аналізу метрик якості, що дозволяє оцінювати не лише середній рівень ефективності, а й варіативність показників у часі. Здобувач наводить агреговані оцінки зокрема для сценаріїв навчання та тестування в одному домені, у різних доменах та у змішаних умовах. Зокрема, у змішаних умовах середні значення Accuracy та F1 зростають від ≈0.49/≈0.41 (номінально) до ≈0.68/≈0.62 (селективно), що інтерпретується як «стабілізуючий ефект» механізму відмови за умов неоднорідності статистичного профілю середовища.

Коректність експериментального підходу підсилюється тим, що автор розділяє «верхню межу» ефективності, досяжну в статистично узгодженому домені, і поведінку моделі за умов різкого доменного зсуву, що є принципово важливим для прикладних IDS.

Новизна наукових положень, висновків і рекомендацій

До найсуттєвіших наукових результатів, отриманих у дисертації, можна віднести наступне:

Уперше розроблено інформаційну технологію аналізу мережевих атак у віртуалізованому середовищі, яка реалізує замкнений цикл «генерація – маркування – потокова класифікація» та використовує детерміноване маркування пакетів на етапі емуляції, що забезпечує формування верифікованих наборів даних для навчання моделей без необхідності евристичної розмітки.

Удосконалено метод виявлення вторгнень шляхом синтезу моделі налаштування порогів класифікації на основі мінімізації баєсівського ризику з урахуванням кількісної оцінки стохастичного зсуву домену на базі зваженої KL-дивергенції, що дозволяє автоматично коригувати чутливість системи до змін параметрів мережевого трафіку та мінімізувати вартість помилкових рішень.

Набув подальшого розвитку метод оцінювання ефективності IDS шляхом переходу від статичних метрик до синхронного віконного аналізу показників надійності, що дає змогу виявляти деградацію якості класифікації при зміні статистичного профілю трафіку та фіксувати момент втрати релевантності моделей.

Набув подальшого розвитку метод проєктування архітектури систем виявлення вторгнень шляхом впровадження дворівневої ієрархічної структури класифікаторів на основі наївного баєсівського класифікатора та випадкового лісу із впровадженням класу невизначеності «Unknown» та механізму відмови від рішення, що забезпечує узгодженість між обчислювальною ефективністю первинної фільтрації трафіку та точністю атрибуції типу атаки.

Практична значущість дисертаційного дослідження. У дисертації розроблено моделі та методи аналізу мережевого трафіку, які склали наукову основу для створення практичного інструментарію виявлення та класифікації мережевих атак у інформаційно-комунікаційних системах. Практична значущість отриманих результатів полягає у можливості використання запропонованих методів та моделей для аналізу мережевого трафіку та підвищення ефективності систем виявлення вторгнень:

Метод дворівневої класифікації мережевого трафіку, що поєднує первинну фільтрацію підозрілої мережевої активності з подальшою уточненою класифікацією типів атак.

Метод реалізації механізму відмови від рішення та введення класу невизначеності «Unknown», що забезпечує зменшення ризику помилкової класифікації в умовах невідомих або нетипових мережевих подій.

Методика формування маркованого мережевого трафіку для навчання та тестування моделей машинного навчання.

Зазначено, що результати дисертації впроваджено у навчальний процес кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, що підтверджено актом про впровадження.

Повнота викладення результатів дослідження в опублікованих наукових працях. Основні результати дослідження відображено у 7 наукових працях, серед яких стаття у науковому виданні, включеному до міжнародних наукометричних баз даних Scopus та/або Web of Science Core Collection, стаття у наукових виданнях, включеному до Переліку наукових фахових видань України, 5 тез наукових доповідей. Основні науково-прикладні результати дисертації опубліковано в періодичних наукових виданнях, вони охоплюють усі наукові положення, що виносяться на захист.

Недоліки та зауваження до представленої роботи

Водночас дисертація не позбавлена окремих недоліків, до яких можна віднести наступне:

1. У дисертації наведено опис експериментального середовища та процедури проведення експериментальних досліджень, однак окремі аспекти організації експериментального конвеєра та забезпечення відтворюваності отриманих результатів висвітлено досить стисло. Більш детальне представлення конфігурації експериментального середовища, параметрів генерації трафіку та процедур обробки даних сприяло б підвищенню рівня відтворюваності запропонованих експериментів.

2. У роботі використано механізм віконної агрегації мережевого трафіку для формування статистичних ознак. Водночас вибір параметрів агрегаційного вікна та їх вплив на оперативність виявлення атак і стабільність показників ефективності моделі обґрунтовано недостатньо детально, що могло б бути розглянуто ширше з урахуванням різних сценаріїв мережевого навантаження.

3. Проведений у роботі порівняльний аналіз моделей машинного навчання дозволяє оцінити ефективність запропонованого підходу. Водночас доцільним виглядало б розширення цього аналізу шляхом включення додаткових базових або контрольних моделей, що дало б змогу більш повно продемонструвати переваги розробленої інформаційної технології.

4. Практичні аспекти масштабування запропонованої системи висвітлено обмежено. Зокрема, певний інтерес становив би більш детальний аналіз впливу зростання обсягів мережевого трафіку на продуктивність класифікації та обчислювальні ресурси системи.

5. У роботі лише частково розглянуто питання адаптації запропонованої моделі до змін характеристик мережевого трафіку в динамічних умовах функціонування сучасних мереж. Більш детальне дослідження цього аспекту могло б додатково підтвердити стійкість запропонованого підходу до появи нових або модифікованих типів мережевих атак.

Вважаю, що наведені зауваження мають рекомендаційний характер і не зменшують загальної наукової новизни та практичної значущості отриманих результатів. Дисертація характеризується методичною завершеністю, логічною структурованістю, достатньою аргументованістю положень і належним рівнем апробації.

Висновок. Дисертація Штанька Вадима Ігоровича на тему: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак», подана на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», є завершеним науковим дослідженням, яке розв'язує актуальну науково-прикладну задачу у сфері аналізу мережевого трафіку.

Дисертація за актуальністю, практичною цінністю та науковою новизною відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України № 44 від 12 січня 2022 року, а Штанько Вадим Ігорович заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Рецензент професор кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, доктор технічних наук, професор Олена КРИВОРУЧКО