РЕЦЕНЗІЯ

доцента кафедри комп'ютерних систем, мереж та кібербезпеки
Національного університету біоресурсів і природокористування України,
кандидата технічних наук, доцента **САГУНА Андрія Вікторовича**
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 теми дослідження

Актуальність теми дисертаційного дослідження зумовлена зростанням обсягів мережевого трафіку та постійним підвищенням складності атак та кількості кіберзагроз у сучасних інформаційно-комунікаційних системах.

Серед таких загроз особливе місце займають атаки типу DoS та DDoS, які характеризуються складною топологією розподіленості джерел втручань, високим рівнем автоматизації та здатністю порушувати доступність критично важливих інформаційних ресурсів.

У сучасних умовах традиційні сигнатурні методи виявлення атак не завжди забезпечують необхідну ефективність, оскільки характеристики мережевого трафіку можуть суттєво змінюватися, а нові сценарії атак з'являються швидше, ніж оновлюються сигнатурні бази. У зв'язку з цим при сучасному підході значна увага приділяється розвитку інтелектуальних систем аналізу мережевого трафіку, які використовують методи машинного навчання та дозволяють автоматизувати процес виявлення і класифікації мережевих атак.

Водночас застосування інтелектуальних методів аналізу мережевого трафіку супроводжується низкою проблем, зокрема зниженням ефективності моделей при зміні статистичних характеристик мережевого середовища. Це обумовлює необхідність розвитку інформаційних технологій аналізу мережевого трафіку, які поєднують математично обґрунтовані методи прийняття рішень із моделями машинного навчання для забезпечення підвищеної стабільності функціонування систем аналізу мережевих даних у змінних умовах експлуатації. Таким чином, тематика дисертаційного дослідження є актуальною та відповідає сучасним напрямам розвитку інформаційних технологій і систем інтелектуального аналізу даних.

Структура та зміст дисертації

Дисертація складається з анотації, вступу, трьох розділів, загальних висновків, списку використаних джерел і додатків. У роботі розглянуто теоретичні засади аналізу мережевого трафіку, запропоновано модель дворівневої системи прийняття рішень та наведено результати експериментального дослідження її ефективності.

У вступі обґрунтовано актуальність теми дослідження, пов'язану зі зростанням складності кіберзагроз та необхідністю підвищення ефективності інтелектуальних систем виявлення вторгнень. Визначено мету, завдання, об'єкт і предмет дослідження, окреслено наукову новизну та практичне значення результатів, а також обґрунтовано доцільність використання методів машинного навчання для аналізу мережевого трафіку.

У першому розділі виконано аналіз сучасного стану методів машинного навчання у системах виявлення вторгнень, розглянуто підходи до моделювання мережевих атак та дослідження експериментальних середовищ. Проаналізовано відкриті набори даних

для задач IDS та інструментальні системи моніторингу мережевого трафіку, що дозволило сформулювати наукове завдання підвищення ефективності систем виявлення атак.

У другому розділі запропоновано математичну модель дворівневої системи прийняття рішень, що поєднує первинну бінарну фільтрацію мережевого трафіку та подальшу багатокласову атрибуцію типів атак. Обґрунтовано використання критерію мінімізації баєсівського ризику та розроблено підхід до оцінювання доменного зсуву мережевого трафіку на основі дивергенції Кульбака-Лейблера.

У третьому розділі описано інструментальну реалізацію запропонованої інформаційної технології, архітектуру програмних модулів та експериментальне середовище на базі GNS3 і VirtualBox. Наведено результати експериментальних досліджень, що підтверджують ефективність запропонованої дворівневої моделі аналізу мережевих атак.

У висновках узагальнено результати дослідження та показано, що запропонована інформаційна технологія дозволяє підвищити ефективність виявлення та класифікації мережевих атак в умовах змінних характеристик мережевого трафіку.

Ступінь обґрунтованості наукових положень,
висновків і рекомендацій та їхня достовірність

Наукові положення та висновки роботи обґрунтовані використанням математичного апарату теорії ймовірностей і прийняття рішень, а також експериментальною перевіркою запропонованих моделей у контрольованому середовищі.

Теоретична частина дослідження базується на апараті теорії ймовірностей і прийняття рішень. Для першого рівня системи сформульовано порогове правило в термінах очікуваного баєсівського ризику з урахуванням різної вартості помилок, що дозволяє інтерпретувати поріг як параметр політики безпеки. Для другого рівня формалізовано механізм відмови від рішення, за якого стан «Unknown» розглядається як керований результат політики прийняття рішень за умов підвищеної невизначеності. Порогова політика при цьому пов’язується з кількісною оцінкою статистичних відмінностей мережевого трафіку: у разі істотної відмінності статистичних характеристик поточного трафіку від еталонного підвищується поріг упевненості та зростає частка відмов від автоматичної атрибуції.

Достовірність отриманих результатів підтверджується експериментальною частиною дослідження. У роботі використано, як публічні набори даних, так і власний мережевий трафік, сформований в ізольованому віртуалізованому середовищі, що забезпечує відтворюваність сценаріїв та контрольованість маркування. Оцінювання ефективності виконано не лише за усередненими показниками якості, а й за допомогою синхронного віконного аналізу, який дозволяє відстежувати зміну точності класифікації у часі та порівнювати роботу моделей у різних режимах експлуатації. Таке поєднання формалізованих моделей і експериментальної перевірки забезпечує належний рівень достовірності отриманих висновків та підвищують точність класифікації.

Новизна наукових положень, висновків і рекомендацій

У дисертації запропоновано підхід до побудови дворівневої системи аналізу мережевого трафіку, що поєднує первинну фільтрацію пакетів та подальшу класифікацію типів атак із використанням методів машинного навчання.

По-перше, реалізовано інформаційну технологію віртуалізованого експерименту із замкненим циклом «генерація – маркування – потокова класифікація», де верифікованість даних забезпечується детермінованим маркуванням на етапі емуляції. Такий підхід зменшує залежність від евристичних процедур подальшої розмітки, підвищує відтворюваність результатів та забезпечує кращу контрольованість експериментального середовища.

По-друге, запропоновано порогову модель прийняття рішень на основі мінімізації очікуваного ризику, де пороги мають операційний зміст через вартості помилок і вартості відмови. Важливо, що доменний зсув введено кількісно (через зважену KL-дивергенцію) і використано як керуючий сигнал для адаптивного налаштування порогу прийняття рішень.

По-третє, метод оцінювання ефективності моделі розвинуто шляхом переходу від статичних метрик до синхронного віконного аналізу показників надійності, що дозволяє фіксувати не лише «середній рівень якості», а і її стабільність у часі та ознаки деградації.

По-четверте, запропоновано дворівневу ієрархію класифікаторів (швидка первинна фільтрація та поглиблена атрибуція) з механізмом «Unknown» і відмовою від рішення, що узгоджує вимоги швидкодії з вимогами коректної інтерпретації типу атаки.

Теоретична цінність і практична значущість наукових результатів

Теоретичне значення дослідження полягає у формалізації IDS, як системи прийняття рішень з асиметрією ризиків та у введенні керованої відмови як інструменту мінімізації небажаних наслідків хибної атрибуції вхідної інформації. У роботі «адаптивність» інтерпретується не як разове перенавчання, а як корекція політики (порогів) на підставі кількісної оцінки розбіжності розподілів ознак; отже, адаптація описується як керована зміна режиму прийняття рішень за умов доменної нестабільності.

Практична значущість отриманих результатів полягає у можливості використання запропонованих моделей та алгоритмів під час створення систем аналізу мережевого трафіку та виявлення атак у інформаційно-комунікаційних мережах. Запропоновані підходи створюють методичну основу для побудови інтелектуальних систем аналізу мережевого трафіку та можуть бути використані під час розроблення програмних засобів моніторингу мережевої активності. До практично значущих результатів належать удосконалення методу дворівневої класифікації мережевого трафіку, що поєднує первинну фільтрацію підозрілої мережевої активності з подальшою деталізованою класифікацією типів атак, метод прийняття рішень із використанням механізму відмови від класифікації у випадках невизначеності, а також методика формування маркованих наборів мережевого трафіку та експериментального оцінювання моделей у контрольованому середовищі, що створює основу для розроблення та дослідження програмних засобів аналізу мережевого трафіку і алгоритмів виявлення атак.

Розроблені моделі та методи реалізовано у вигляді програмного інструментарію для збору, агрегації та класифікації мережевого трафіку, а також перевірено у віртуалізованому експериментальному середовищі. Отримані результати можуть бути використані під час дослідження та розроблення систем аналізу мережевого трафіку, а також у навчальному процесі підготовки фахівців з комп’ютерних наук та інформаційних технологій. Зазначено, що результати дисертації впроваджено у навчальний процес кафедри комп’ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, що підтверджено відповідним актом впровадження.

Повнота викладення наукових результатів дисертації в опублікованих наукових працях

Основні результати дослідження відображено у 7 наукових працях та апробовано на всеукраїнських і міжнародних наукових заходах. Тематика публікацій узгоджується з ключовими компонентами дисертації. Окремо слід підкреслити, що апробація результатів у різних формах (статті й тези наукових доповідей) забезпечує достатню повноту висвітлення основних положень дослідження.

Дискусійні положення та недоліки дисертації

Водночас у роботі є окремі питання, які потребують додаткового обговорення:

1) недостатньо розгорнуте систематизоване зіставлення запропонованої інформаційної технології з існуючими програмно-інструментальними IDS/IPS-рішеннями (як відкритими, так і комерційними). Більш доцільно було б представити більш структуроване порівняння з погляду архітектурних підходів, механізмів адаптації до зміни мережевого трафіку та опис стратегій роботи з невизначеністю;

2) у зв'язку з тим, що дана інформаційна технологія має практичну направленість, то бажано було б навести орієнтовне відносне зіставлення часових характеристик і експлуатаційних обмежень запропонованої моделі;

3) механізм адаптивності на основі оцінки доменного зсуву за допомогою зваженої KL-дивергенції має достатній рівень і глибину обґрунтування, але його ефективність значною мірою залежить від вибору параметрів моделі. Тому, доцільним видається розширення аналізу чутливості, що дозволило б показати вплив зміни параметрів на показники якості класифікації та частку випадків відмови від автоматичної атрибуції;

4) у зв'язку з тим, що параметри віконної агрегації мережевого трафіку суттєво впливають на баланс між оперативністю виявлення атак і статистичною стійкістю оцінок, то бажано було б більш системно обґрунтувати вибір інтервалу агрегації та продемонструвати вплив зміни цього параметра на стабільність оцінювання, метрики якості та затримку виявлення загроз;

5) експериментальна частина дослідження переважно зосереджена на сценаріях DoS/DDoS-атак. Але, на практиці так часто в аналогічних системах фіксуються також і SNMP-атаки тощо. Тому, для підсилення узагальненості результатів доцільним було б розширення експериментальної бази синтетичної вибірки вхідного мережевого трафіку шляхом включення інших класів загроз або використання інших незалежних наборів даних із різними характеристиками мережевого трафіку.

Узагальнюючи зазначене, можна констатувати, що наведені зауваження носять дискусійний або рекомендаційний характер і не впливають на загальне враження від дисертації.

Дані зауваження не знижують наукову новизну, практичну цінність та актуальність результатів дослідження. Вони також не впливають на загальну позитивну оцінку дисертації.

Загальний висновок

Таким чином, дисертація Штанька Вадима Ігоровича є завершеним науковим дослідженням, у якому вирішено актуальне завдання підвищення ефективності аналізу мережевого трафіку та виявлення атак.

Актуальність теми дисертації, ступінь обґрунтованості наукових здобутків, висновків і рекомендацій, новизна і повнота їх висвітлення у наукових виданнях, рівень апробації отриманих результатів відповідають 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 від 12 січня 2022 року № 44, а здобувач Штанько Вадим Ігорович заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Рецензент доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, кандидат технічних наук, доцент Андрій САГУН