ВІДГУК

офіційного опонента професора кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, доктора технічних наук, професора ТОЛЮПИ Сергія Васильовича 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

У сучасних умовах розвитку інформаційних технологій, хмарних сервісів та мережевої взаємодії істотно зростає залежність функціонування інформаційно-комунікаційних систем від надійності засобів виявлення та протидії мережевим атакам. Особливої актуальності набувають атаки типу DDoS, які характеризуються масштабністю, автоматизацією та здатністю порушувати працездатність критично важливих сервісів. За таких умов традиційні сигнатурні засоби не завжди забезпечують належний рівень ефективності, що зумовлює необхідність розроблення інтелектуальних методів аналізу мережевого трафіку.

У практиці застосування систем виявлення вторгнень однією з ключових проблем залишається зниження ефективності роботи моделей при зміні характеристик мережевого трафіку, а також ризик помилкової класифікації мережевих подій. Це зумовлює потребу в розробленні підходів, які б поєднували достатню швидкодію, адаптивність і надійність прийняття рішень. Саме цим визначається актуальність обраної теми дисертаційного дослідження.

Зв'язок теми дисертації з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертацію виконано відповідно до актуальних напрямів наукових досліджень у сфері інформаційно-комунікаційних технологій, систем штучного інтелекту та комп'ютерних мереж. Тема дослідження відповідає науковим напрямам факультету інформаційних технологій і кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їхня достовірність

Наукові положення, висновки та рекомендації, сформульовані у дисертації, є достатньо обґрунтованими. На користь цього свідчить наступне:

– здобувачем опрацьовано значний обсяг сучасних наукових джерел за тематикою дослідження;

– у роботі використано коректний математичний апарат, а також сучасні методи аналізу даних і машинного навчання;

– достовірність отриманих результатів підтверджено експериментально на публічному та власному наборах даних;

– результати дослідження пройшли апробацію та відображені у наукових публікаціях здобувача.

Мова та стиль викладення результатів

Дисертацію написано українською мовою.

Робота є логічно структурованою, виклад матеріалу послідовний та доступний для сприйняття. Автор коректно використовує загальноприйняту наукову термінологію.

Дисертація складається з анотації, вступу, трьох розділів, загальних висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 183 сторінки, у роботі наведено 26 рисунків і 5 таблиць, список використаних джерел містить 126 найменувань.

У вступі обґрунтовано актуальність теми, сформульовано мету та завдання, визначено наукову новизну й практичне значення, наведено апробацію та публікації.

У першому розділі здійснено аналіз сучасного стану підходів до інтелектуального виявлення мережевих атак, проблематики доменного зсуву та питань організації експериментальної верифікації в контрольованих середовищах, що підводить до формулювання актуального наукового завдання – підвищення ефективності IDS за рахунок дворівневої архітектури та керованої політики прийняття рішень.

У другому розділі розроблено теоретичні засади дворівневої системи аналізу мережевого трафіку, обґрунтовано вибір методів машинного навчання та підходи до прийняття рішень в умовах невизначеності.

У третьому розділі наведено практичну реалізацію запропонованих рішень, описано експериментальне середовище, результати перевірки моделі та їх аналіз.

Новизна наукових положень, висновків і рекомендацій

Представлені в дисертації положення, постановка завдань, їх вирішення та узагальнені висновки є результатом самостійно виконаної наукової праці. У дисертації обґрунтовано низку положень, що відповідають критеріям наукової новизни, зокрема:

– уперше розроблено інформаційну технологію аналізу мережевих атак у віртуалізованому середовищі, яка забезпечує формування експериментальних наборів даних та їх подальшу потокову обробку для класифікації мережевих атак;

– удосконалено метод виявлення вторгнень шляхом синтезу моделі налаштування порогів класифікації на основі критерію мінімізації баєсівського ризику з урахуванням кількісної оцінки доменного зсуву на основі зваженої дивергенції Кульбака-Лейблера,

що дозволяє автоматизувати коригування чутливості системи та мінімізувати вартість помилкових рішень при зміні мережевого середовища;

– подальшого розвитку набули метод оцінювання ефективності систем через синхронний віконний аналіз показників надійності для виявлення деградації якості; метод проєктування архітектури IDS через впровадження дворівневої ієрархії класифікаторів з механізмом відмови від рішення, що узгоджує обчислювальну ефективність первинної фільтрації з точністю атрибуції типу атаки.

Отримані результати можуть слугувати теоретичною та технологічною основою для розвитку адаптивних IDS-рішень у змінних мережевих доменах.

Теоретична цінність і практична значущість наукових результатів

Наукові положення, висновки та рекомендації дисертації мають теоретичну цінність і практичну значущість. Отримані результати є внеском у розвиток інформаційних технологій кіберзахисту, зокрема в частині архітектур IDS, які працюють в умовах змін характеристик мережевого трафіку та мають механізм керованої відмови від рішення у невизначених випадках.

Теоретичне значення полягає в обґрунтуванні дворівневої моделі прийняття рішень та формалізації порогового налаштування через мінімізацію баєсівського ризику з кількісним урахуванням зсуву домену.

Практична цінність одержаних результатів полягає в реалізації запропонованих підходів у вигляді програмних засобів аналізу мережевого трафіку та створенні експериментального середовища для дослідження мережевих атак. Це дає можливість використовувати результати роботи як у навчальному процесі, так і в подальших прикладних дослідженнях у сфері побудови адаптивних IDS.

Результати дисертації впроваджено у навчальний процес кафедри комп’ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України.

Повнота викладення наукових результатів дисертації в опублікованих працях, апробація

Результати дисертації відображено у 7 публікаціях, з 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 на всеукраїнських і міжнародних наукових конференціях. Аналіз публікацій автора дозволяє зробити висновок про повноту викладення основних наукових положень дисертаційного дослідження у науковій літературі.

Відсутність (наявність) порушення академічної доброчесності

За результатами ознайомлення зі змістом дисертації та наведеним апаратом посилань ознак порушення академічної доброчесності не виявлено; запозичення оформлено коректно й у межах академічної практики. Перевірка дисертації проводилася за допомогою сервісу StrikePlagiarism.

Дискусійні положення та недоліки дисертації

Відзначаючи позитивні сторони роботи, слід звернути увагу на певні зауваження та дискусійні положення, які потребують додаткового уточнення або можуть бути підґрунтям для розвитку теми:

1. У дисертації запропоновано дворівневу ієрархічну модель класифікації мережевого трафіку, в якій на першому рівні використано алгоритм Naive Bayes як швидкий первинний фільтр, а на другому – Random Forest як багатокласовий класифікатор. Водночас обґрунтування вибору такої конфігурації могло б бути посилене шляхом проведення ширшого порівняльного аналізу з іншими сучасними методами машинного навчання та ансамблевими підходами за єдиною методикою експериментального оцінювання, зокрема в умовах доменного зсуву.

2. Експериментальна частина роботи переважно зосереджена на дослідженні сценаріїв DDoS-атак та їх перевірці у віртуалізованому середовищі. Водночас доцільним є розширення спектра досліджуваних кіберзагроз шляхом включення інших класів атак, зокрема багатостадійних атак, атак на прикладні сервіси, а також атак у середовищах IoT/IIoT, що дозволило б додатково оцінити універсальність запропонованої технології.

3. У роботі запропоновано підхід до оцінювання доменного зсуву на основі зваженої дивергенції Кульбака-Лейблера з адаптивним налаштуванням порогових значень прийняття рішень. Водночас питання формування вагових коефіцієнтів ознак та оцінювання чутливості алгоритму до їх варіювання висвітлено обмежено. Більш детальне дослідження цього аспекту могло б сприяти глибшому розумінню впливу параметризації моделі на баланс між повнотою виявлення атак і точністю класифікації.

4. У дисертації наведено результати експериментального оцінювання ефективності запропонованих методів і моделей. Водночас доцільним є більш розгорнутий аналіз стабільності функціонування підходу за умов змінних характеристик мережевого трафіку, зокрема при варіації інтенсивності атак, обсягу фонового трафіку та параметрів мережевого навантаження.

5. Окремі аспекти практичної реалізації запропонованої технології в системах моніторингу та аналізу мережевого трафіку висвітлено стисло. Зокрема, доцільним є розширення обговорення особливостей інтеграції розроблених алгоритмів у наявні системи

моніторингу та інцидент-менеджменту, а також можливих обмежень їх застосування у великомасштабних інформаційно-телекомунікаційних інфраструктурах.

Наведені зауваження не мають принципового характеру та не знижують загальної позитивної оцінки дисертації. Вони носять дискусійний і рекомендаційний характер та можуть бути враховані автором у подальших наукових дослідженнях.

Висновки про відповідність дисертації встановленим вимогам

Вважаю, що дисертація Штанька Вадима Ігоровича на тему: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак» є завершеною самостійною науковою працею, у якій вирішено актуальне науково-практичне завдання.

За актуальністю теми, рівнем наукової новизни, обґрунтованістю та практичною цінністю результатів, повнотою викладення в наукових публікаціях, відсутністю порушень академічної доброчесності, вважаю, що дисертація відповідає вимогам чинного законодавства України, які передбачені Порядком 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.

Автор дисертації Штанько Вадим Ігорович заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп’ютерні науки» галузі знань 12 «Інформаційні технології».

Офіційний опонент професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, доктор технічних наук, професор Сергій ТОЛЮПА