ВІДГУК
офіційного опонента
завідувача кафедри комп'ютерних наук
Чернівецького національного університету імені Юрія Федьковича,
доктора фізико-математичних наук, професора УШЕНКА Юрія Олександровича,
на дисертацію ШТАНЬКА Вадима Ігоровича на тему:
«Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак»,
яка подана на здобуття ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки»
галузі знань 12 «Інформаційні технології»

Актуальність дисертаційного дослідження. Актуальність дисертаційного дослідження Штанька Вадима Ігоровича визначається зростанням інтенсивності та ускладненням кібератак у сучасних інформаційно-комунікаційних системах. Насамперед це стосується атак класу DDoS, які здатні порушувати працездатність критично важливих інформаційних ресурсів і сервісів. В умовах швидкої еволюції шкідливих сценаріїв і зміни характеристик мережевого трафіку традиційні сигнатурні рішення дедалі частіше втрачають ефективність, що зумовлює потребу в інтелектуальних системах виявлення вторгнень, здатних адаптивно приймати рішення за неповної, нестабільної або статистично змінної інформації. У роботі акцентується увага на підвищенні надійності прийняття рішень у системах виявлення вторгнень, а також на забезпеченні стабільної роботи таких систем у випадку зміни характеристик мережевого трафіку. З огляду на науково-практичний характер проблематики та її безпосередній зв'язок із завданнями кіберзахисту, дисертація має значну практичну та наукову цінність.

Зв'язок роботи з державними програмами, планами, темами. Дисертація Штанька Вадима Ігоровича виконана в Національному університеті біоресурсів і природокористування України та узгоджується з пріоритетними напрямами наукових досліджень, визначеними постановою Кабінету Міністрів України № 476-2024-п. Робота належить до таких науково-технологічних напрямів, як «Інформаційні та комунікаційні технології», «Системи штучного інтелекту», «Інтелектуальні інтерактивні інформаційно-аналітичні системи», а також «Інформаційно-комунікаційні системи та мережі», оскільки присвячена розробленню програмно-алгоритмічних засобів аналізу мережевого трафіку із застосуванням методів машинного навчання. Розроблена інформаційна технологія базується на сучасних підходах до оброблення даних, адаптивного прийняття рішень та створення інтелектуальних інформаційних систем, що відповідає державним пріоритетам розвитку цифрових технологій і систем штучного інтелекту.

Ступінь обґрунтованості наукових положень, висновків, рекомендацій, сформульованих у дисертації. Наукові положення, висновки та рекомендації, сформульовані

у дисертації, мають високий ступінь обґрунтованості, що забезпечується поєднанням теоретично обґрунтованих моделей порогового прийняття рішень із практичною реалізацією та експериментальною верифікацією в контрольованому віртуалізованому середовищі. Автором послідовно застосовано апарат теорії прийняття рішень і мінімізації очікуваного ризику для формалізації порогів у дворівневій моделі та використано кількісну оцінку доменного зсуву, що дозволяє враховувати зміну статистичних характеристик мережевого трафіку. Експериментальна частина підтверджує працездатність запропонованої інформаційної технології: наведено результати оцінювання на публічному наборі USB-IDS-1 і на власноруч сформованих верифікованих даних, а також показано часову ефективність обробки вікон і потоків, що є важливим для режимів, наближених до реального часу. Узгодженість теоретичних положень і практичної реалізації свідчить про надійність та інженерну завершеність запропонованих рішень.

Структура дисертації. Дисертація Штанька Вадима Ігоровича складається з анотації, вступу, трьох основних розділів, загальних висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 183 сторінки. Робота містить рисунки, таблиці та список використаних джерел, що охоплює сучасні наукові праці з тематики дослідження.

У *вступі* обґрунтовано актуальність теми, сформульовано мету і завдання, визначено об’єкт і предмет дослідження, а також наведено наукову новизну, практичне значення, апробацію та відомості про публікації.

Перший розділ присвячено аналізу сучасного стану та тенденцій розвитку методів машинного навчання у системах виявлення вторгнень. Розглянуто підходи до моделювання та симуляції мережевих атак в експериментальних середовищах, дослідження багаторівневих класифікаторів і багатоступеневих систем ухвалення рішень, а також проведено огляд інструментальних IDS-рішень і наборів даних, зокрема публічного набору USB-IDS-1.

У *другому розділі* сформовано теоретичні та технологічні засади дворівневої моделі прийняття рішень в IDS. Запропоновано порогові правила для первинної детекції та багатокласової атрибуції з механізмом відмови від рішення; обґрунтовано використання критерію мінімізації баєсівського ризику та показано можливість адаптивного налаштування порогів відповідно до рівня статистичної невідповідності доменів, оціненої через зважену KL-дивергенцію. Окремо розглянуто інтеграцію оцінювання якості в цикл обробки трафіку та синхронний віконний аналіз метрик.

Третій розділ містить опис практичної реалізації інформаційної технології, побудови тренувальних модулів і конвеєра оброблення даних, методики формування верифікованих маркованих наборів у віртуалізованому середовищі на базі GNS3 і VirtualBox, а також

експериментальну перевірку ефективності й часових характеристик роботи запропонованої дворівневої системи.

У *висновках* підсумовано результати дослідження; *додатки* містять акт впровадження, список опублікованих праць автора, лістинг програмного забезпечення.

Наукова новизна. Результати та висновки дисертації, які становлять наукову новизну, пов'язані з розробленням інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак.

1. Вперше реалізовано замкнений цикл «генерація – маркування – потокова класифікація» у віртуалізованому середовищі з детермінованим маркуванням пакетів на етапі емуляції, що забезпечує формування верифікованих наборів даних без евристичної розмітки.

2. Удосконалено метод налаштування порогів класифікації шляхом синтезу порогової моделі на основі мінімізації баєсівського ризику з урахуванням кількісної оцінки стохастичного доменного зсуву, що дозволяє коригувати чутливість системи до змін параметрів мережевого трафіку.

3. Набув подальшого розвитку метод проєктування архітектури IDS шляхом впровадження дворівневої ієрархічної структури класифікаторів (первинна фільтрація та поглиблена атрибуція) із введенням класу невизначеності «Unknown» та механізму відмови від рішення.

4. Набув подальшого розвитку метод оцінювання ефективності шляхом переходу від статичних метрик до синхронного віконного аналізу показників надійності, що дозволяє фіксувати деградацію якості при зміні статистичного профілю трафіку.

Розроблені в межах дослідження методи, моделі та інформаційна технологія мають значний потенціал практичного використання під час створення та розвитку адаптивних систем виявлення вторгнень у динамічних мережевих середовищах.

Практичне значення дисертації полягає у розробленні методів, математичних моделей та інформаційної технології аналізу мережевого трафіку із застосуванням методів машинного навчання, що дозволяють підвищити ефективність виявлення та класифікації мережевих атак в умовах змінних характеристик трафіку; які можуть бути використані при створенні та дослідженні систем аналізу мережевого трафіку:

1. Розроблення методів і технології аналізу мережевого трафіку:

– Запропоновано інформаційну технологію аналізу мережевого трафіку, що поєднує первинну фільтрацію підозрілої мережевої активності з подальшою класифікацією типів атак на основі моделей машинного навчання. Це дозволяє підвищити ефективність обробки мережевих даних у змінних умовах функціонування.

– Розроблені методи прийняття рішень передбачають використання механізму відмови від рішення («Unknown»), що зменшує ризик помилкової класифікації у випадках невизначеності або появи нових типів мережевої активності.

2. Формування інструментальної бази для дослідження мережевого трафіку:

– Створено експериментальне середовище для моделювання сценаріїв мережевої активності та формування маркованих наборів даних, що забезпечує можливість дослідження ефективності алгоритмів аналізу мережевого трафіку.

– Запропонований підхід дозволяє проводити експериментальну перевірку методів і моделей в умовах змінних характеристик мережевого середовища.

Практична значущість підтверджується результатами експериментальних досліджень ефективності запропонованих методів і моделей, а також впровадженням результатів дисертаційного дослідження у навчальний процес підготовки фахівців з комп'ютерних наук та інформаційних технологій.

Дискусійні положення та зауваження до змісту дисертаційного дослідження

1. У роботі експериментальну перевірку запропонованих методів виконано на публічному наборі даних USB-IDS-1, а також на власному верифікованому наборі мережевого трафіку, сформованому в ізольованому середовищі емуляції. Водночас додаткове тестування запропонованої інформаційної технології на кількох незалежних публічних наборах даних дозволило б розширити емпіричну базу дослідження та більш повно оцінити ефективність підходу в різних умовах формування вхідних даних.

2. У роботі використано сформований набір статистичних ознак мережевого трафіку, що забезпечує ефективне виконання задачі класифікації атак. Водночас доцільним є більш детальне дослідження інформативності окремих ознак або їх підмножин, зокрема із застосуванням методів оцінювання важливості ознак, що дозволило б додатково обґрунтувати їх вибір у межах запропонованої моделі.

3. Доцільним є більш розгорнутий аналіз чутливості результатів класифікації до змін структури вхідних даних та варіацій статистичних характеристик мережевого трафіку, що дозволило б глибше оцінити стійкість запропонованого підходу в умовах доменного зсуву.

4. Запропонована архітектура інформаційної технології продемонструвала ефективність у дослідницькому середовищі. Водночас перспективним напрямом подальших досліджень є детальніше вивчення питань масштабування підходу при обробці значних обсягів мережевого трафіку, характерних для сучасних інформаційно-телекомунікаційних систем.

5. Більш детальне висвітлення аспектів інтеграції розробленої технології в існуючі системи моніторингу мережевого трафіку та засоби забезпечення мережевої безпеки сприяло б оцінюванню її практичної придатності та умов впровадження у реальних інфраструктурах.

Зазначені зауваження мають переважно рекомендаційний або дискусійний характер і не знижують загальної наукової цінності та практичної значущості дисертації.

Загальний висновок. У дисертації Штанька Вадима Ігоровича отримано результати, що мають наукову новизну та практичну значущість у сфері аналізу мережевого трафіку та систем виявлення вторгнень. Робота присвячена вирішенню важливого науково-практичного завдання зі створення інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак із керованим прийняттям рішень в умовах варіативної зміни характеристик трафіку та доменного зсуву. Висновки та основні положення дисертації відзначаються логічністю, методичною коректністю та підтверджені експериментально.

Дисертація на тему: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак», подана на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології», є завершеною науковою роботою, результати якої за своїм науково-теоретичним рівнем, новизною та практичним значенням відповідають вимогам чинного 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 (зі змінами), а її автор Штанько Вадим Ігорович заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Офіційний опонент завідувач кафедри комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича, доктор фізико-математичних наук, професор Юрій УШЕНКО