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

офіційного опонента, к.т.н., доцента, старшого викладача кафедри автоматизації виробничих процесів, Центральноукраїнського національного технічного університету, м. Кропивницький
Тетяни СМІРНОВОЇ

ВІДГУК

офіційного опонента , к.т.н., доцента, старшого викладача кафедри автоматизації виробничих процесів, Центральноукраїнського національного технічного університету, м. Кропивницький
СМІРНОВОЇ Тетяни Віталіївни
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 дисертаційної роботи

Обрана тема дисертаційної роботи Мєшкова Вадима Ігоровича є актуальною, оскільки пов'язана з одним із важливих напрямів розвитку сучасних комп'ютерних наук – створенням інформаційних технологій інтелектуального аналізу даних для задач кібербезпеки. У сучасних комп'ютерних мережах постійно зростають обсяги трафіку, ускладнюється структура мережевих взаємодій, а характер атакувальної активності стає дедалі більш динамічним і важкопрогнозованим.

Особливої уваги потребує проблема своєчасного виявлення нових, модифікованих і малопоширених атак, для яких традиційні сигнатурні підходи не завжди є достатньо ефективними. За таких умов актуальним є застосування методів машинного навчання, здатних виявляти статистичні залежності в мережевому трафіку, класифікувати його стани та підтримувати прийняття рішень щодо наявності атакувальної активності й типу загрози. У дисертації зазначено, що метою роботи є підвищення ефективності виявлення атак і розпізнавання їх типів шляхом розроблення інформаційної технології, яка функціонує у бінарному та багатокласовому режимах аналізу.

Важливим є те, що дисертаційне дослідження не обмежується лише вибором окремих моделей машинного навчання, а спрямоване на побудову цілісної технології опрацювання мережевого трафіку. Такий підхід охоплює підготовку даних, формування ознакового простору, побудову класифікаційних моделей, оцінювання їх ефективності та подальше використання отриманих результатів у системах виявлення атак.

Тема дисертаційної роботи є своєчасною та практично значущою, відповідає сучасним потребам підвищення рівня захищеності комп'ютерних мереж і спрямована на розвиток інформаційних технологій інтелектуального моніторингу трафіку для систем виявлення атак.

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

Дисертаційну роботу Мєшкова Вадима Ігоровича виконано в Національному технічному університеті «Дніпровська політехніка» відповідно до плану науково-дослідної діяльності кафедри безпеки інформації та телекомунікацій.

Тематика дослідження пов'язана з науково-дослідною роботою «Інтелектуальні методи моделювання процесів в інформаційно-телекомунікаційних системах критичної інфраструктури» з державним обліковим номером 0225U004731. Термін виконання роботи визначено на 2024-2025 рр.

У межах зазначеного напряму здобувачем виконано дослідження, спрямовані на розроблення інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі, підготовку даних мережевого трафіку, побудову моделей машинного навчання та експериментальне оцінювання їх ефективності.

Таким чином, дисертаційна робота має безпосередній зв'язок із науковими планами Національного технічного університету «Дніпровська політехніка», а її результати відповідають напряму досліджень, пов'язаних із моделюванням,

аналізом і захистом інформаційно-телекомунікаційних систем критичної інфраструктури.

3. Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій

Наукові положення, висновки й рекомендації, подані в дисертаційній роботі Мєшкова Вадима Ігоровича, можна вважати достатньо обґрунтованими, оскільки вони спираються на послідовне застосування методів аналізу даних, машинного навчання, статистичного оцінювання та експериментальної перевірки результатів.

Достовірність одержаних результатів забезпечується тим, що дослідження побудовано на чіткій логіці: від аналізу предметної області та вибору набору даних CIC-IDS2017 до формування методу підготовки даних, побудови інформаційної технології, програмної реалізації та перевірки її ефективності у двох режимах – бінарного виявлення атак і багатокласового розпізнавання їх типів. У дисертації зазначено, що ефективність інтелектуального виявлення атак залежить не лише від вибору моделі машинного навчання, а й від якості підготовки даних, коректності формування ознакового простору та обґрунтованості системи оцінювання результатів.

Обґрунтованим є також вибір етапів дослідження: очищення, уніфікація та стандартизація даних, аналіз ознак і зниження розмірності, формування та балансування вибірок, навчання моделей машинного навчання й оцінювання їх якості. Така послідовність дозволяє зменшити вплив випадкових або некоректних даних на результати класифікації та забезпечує порівнюваність результатів для різних моделей.

Експериментальна частина роботи підтверджує достовірність сформульованих висновків. Для оцінювання моделей використано фіксований поділ вибірок на навчальну й тестову частини, п'ятикратну перехресну перевірку, а також систему взаємодоповнювальних метрик: accuracy, precision, recall, F1-score, ROC-AUC, Precision–Recall-криві та матриці помилок. Це дає змогу оцінити якість моделей не за одним показником, а комплексно, з урахуванням специфіки задач виявлення атак.

Слід відзначити, що автором розглянуто декілька моделей машинного навчання для різних постановок задачі, що підвищує переконливість порівняльного аналізу. Для бінарного виявлення атак досліджено логістичну регресію та метод опорних векторів, а для багатокласового розпізнавання типів атак – випадковий ліс, дерево рішень і метод k-найближчих сусідів. Отримані

результати узгоджуються з поставленою метою роботи та підтверджують працездатність запропонованої інформаційної технології.

Наукові положення, висновки та рекомендації дисертаційної роботи мають належний рівень обґрунтованості й достовірності, а використана методика дослідження є коректною для розв'язання задач інтелектуального моніторингу мережевого трафіку в системах виявлення атак.

4. Наукова новизна одержаних результатів

Наукова новизна дисертаційної роботи Мєшкова Вадима Ігоровича визначається тим, що в ній запропоновано цілісний підхід до інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, який поєднує етапи підготовки даних, побудови ознакового простору, навчання моделей машинного навчання та комплексного оцінювання результатів класифікації.

До основних результатів, що мають ознаки наукової новизни, слід віднести розроблення інформаційної технології інтелектуального моніторингу мережевого трафіку, яка забезпечує послідовне виконання всіх основних процедур аналізу – від завантаження та попередньої обробки даних до виявлення атакувальної активності й розпізнавання конкретних типів атак. Важливо, що запропонована технологія орієнтована не на ізольоване застосування окремого класифікатора, а на функціонування єдиного програмно-методичного конвеєра аналізу мережевого трафіку.

Суттєвим науковим результатом є удосконалення методу підготовки, класифікації та оцінювання мережевого трафіку для систем виявлення атак. У межах цього методу об'єднано процедури очищення й уніфікації даних, стандартизації числових ознак, аналізу інформативності ознакового простору, зниження розмірності, формування збалансованих вибірок, навчання моделей машинного навчання та оцінювання якості їх роботи. Така послідовність дозволяє підвищити точність експериментального дослідження та забезпечити порівнюваність результатів різних моделей.

Окремо слід відзначити розвиток методичних положень щодо оцінювання ефективності моделей машинного навчання в задачах моніторингу мережевого трафіку. У роботі використано комплексний підхід до оцінювання, який враховує не лише загальну точність класифікації, а й показники precision, recall, F1-score, ROC-AUC, Precision–Recall-криві, матриці помилок і результати перехресної перевірки. Це є важливим для задач кібербезпеки, де помилкові спрацювання та пропущені атаки мають різні практичні наслідки.

Наукова новизна роботи також проявляється у двоетапній логіці розв'язання задачі: спочатку здійснюється бінарне відокремлення нормального трафіку від атакувального, а далі – багатокласове розпізнавання типу виявленої атаки. Такий підхід відповідає практичній логіці функціонування систем виявлення атак і дає змогу поєднати задачу первинного виявлення інциденту із задачею його подальшої деталізації.

Одержані в дисертаційній роботі результати мають наукову новизну, є змістовно пов'язаними з поставленою метою дослідження та становлять внесок у розвиток інформаційних технологій інтелектуального аналізу мережевого трафіку для систем виявлення атак.

5. Аналіз змісту дисертаційної роботи

Дисертаційна робота Мєшкова Вадима Ігоровича побудована послідовно та відповідає логіці виконання науково-прикладного дослідження: від аналізу стану проблеми до розроблення методу, створення інформаційної технології, її програмної реалізації та експериментальної перевірки. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Така структура є виправданою для дослідження, спрямованого на розроблення інформаційної технології інтелектуального моніторингу мережевого трафіку.

У вступі здобувачем визначено наукову проблему, обґрунтовано актуальність теми, сформульовано мету, завдання, об'єкт і предмет дослідження, а також подано відомості щодо наукової новизни, практичного значення та апробації результатів. Вступна частина дає цілісне уявлення про спрямованість роботи та її місце в межах спеціальності 122 «Комп'ютерні науки».

У першому розділі розглянуто теоретичні основи моніторингу мережевого трафіку та виявлення атак. Автор аналізує сучасні IDS/IPS-системи, підходи до виявлення загроз, методи інтелектуального аналізу трафіку, а також типові прояви атак у мережевих даних. Цей розділ створює необхідну теоретичну базу для подальшого формування власного підходу.

У другому розділі основну увагу приділено методу підготовки даних, класифікації та оцінювання мережевого трафіку. У роботі розглянуто використання набору CIC-IDS2017, процедури очищення й уніфікації даних, стандартизації ознак, аналізу ознакового простору, зниження розмірності, формування вибірок для бінарної та багатокласової класифікації. Важливим є те, що ці процедури подано як взаємопов'язані етапи єдиного процесу, а не як окремі технічні операції.

У третьому розділі представлено інформаційну технологію інтелектуального моніторингу трафіку комп'ютерної мережі та її програмну

реалізацію. Здобувач описує архітектуру технології, конвеєр обробки мережевого трафіку, двоетапну схему класифікації, вибір програмних засобів і структуру програмного модуля. Окремо розкрито реалізацію процедур завантаження даних, попередньої обробки, формування ознакового простору, навчання моделей машинного навчання та візуалізації результатів.

У четвертому розділі наведено результати експериментального дослідження ефективності запропонованої інформаційної технології. Дослідження проведено для двох режимів: бінарного виявлення атакувального трафіку та багатокласового розпізнавання типів атак. Отримані результати свідчать про працездатність розробленої технології та підтверджують доцільність використання запропонованого підходу для побудови інтелектуальних компонентів систем виявлення атак.

Загалом зміст дисертації відповідає її темі, меті та поставленим завданням. Матеріал викладено логічно, розділи взаємно доповнюють один одного, а висновки узгоджуються з результатами проведених досліджень. Робота справляє враження завершеного науково-прикладного дослідження, у якому запропоновані теоретичні та методичні положення доведені до рівня програмної реалізації й експериментальної перевірки.

6. Практичне значення одержаних результатів

Практична цінність дисертаційної роботи полягає у створенні програмної реалізації інформаційної технології, призначеної для інтелектуального аналізу трафіку комп'ютерної мережі в задачах виявлення атак. Розроблене рішення може бути використане як основа для побудови або вдосконалення програмних компонентів систем виявлення атак, орієнтованих на автоматизовану обробку мережевих даних.

Запропонована технологія забезпечує підготовку вхідних даних, формування ознакового простору, навчання моделей машинного навчання та оцінювання результатів класифікації. Її прикладна значущість полягає також у можливості роботи у двох режимах: виявлення факту атакувальної активності та подальше визначення типу атаки. Це підвищує інформативність результатів моніторингу та може бути корисним для підтримки прийняття рішень у сфері кібербезпеки.

Окремо слід відзначити, що розроблений програмний модуль може застосовуватися для проведення експериментальних досліджень, порівняння моделей машинного навчання та оцінювання їх ефективності на наборах даних мережевого трафіку. Практичне значення роботи підтверджується також

впровадженням її результатів у діяльність ТОВ «Центум-Д» та в освітній процес Національного технічного університету «Дніпровська політехніка».

7. Повнота викладення результатів у наукових публікаціях та апробація

Результати дисертаційного дослідження Мєшкова Вадима Ігоровича належним чином представлені в наукових публікаціях здобувача. Опубліковані праці охоплюють основні складові дисертації: аналіз систем інтелектуального моніторингу мережевого трафіку, методи машинного навчання для бінарної та багатокласової класифікації, попередню обробку даних, а також питання підвищення кібербезпеки інформаційних систем.

За темою дисертації опубліковано 4 наукові праці у фахових виданнях України категорії Б. Тематика цих публікацій відповідає змісту дисертаційної роботи та відображає ключові етапи проведеного дослідження – від аналізу предметної області до розроблення й оцінювання методів інтелектуального аналізу мережевого трафіку.

Апробацію результатів здійснено шляхом представлення матеріалів на міжнародних і всеукраїнських науково-практичних конференціях. У тезах доповідей висвітлено питання архітектури інформаційної технології, аналізу наборів даних мережевого трафіку, кореляційного аналізу ознак, ідентифікації трафіку, а також розроблення інформаційної технології інтелектуального моніторингу для систем виявлення атак.

Таким чином, кількість, зміст і спрямованість опублікованих праць дають підстави стверджувати, що основні наукові положення, практичні результати та висновки дисертаційної роботи достатньо повно апробовані й оприлюднені в науковому середовищі.

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

Дисертаційна робота Мєшкова Вадима Ігоровича відповідає спеціальності 122 «Комп'ютерні науки», оскільки її зміст безпосередньо пов'язаний із розробленням інформаційної технології, алгоритмізацією процесів обробки даних, застосуванням методів машинного навчання та створенням програмного інструментарію для аналізу мережевого трафіку.

У дисертації розглянуто задачі, характерні для галузі комп'ютерних наук: підготовка й опрацювання великих масивів даних, формування ознакового простору, побудова класифікаційних моделей, оцінювання якості алгоритмів, програмна реалізація інформаційної технології та експериментальна перевірка її

ефективності. Розроблена технологія призначена для автоматизованої обробки даних мережевих потоків, побудови інформаційних моделей трафіку та виявлення атак із використанням методів машинного навчання.

Одержані результати мають чітку спрямованість на розвиток методів і засобів інтелектуального аналізу даних, програмних компонентів систем виявлення атак та інформаційних технологій підтримки прийняття рішень у сфері кібербезпеки. Це підтверджує відповідність теми, мети, завдань, наукової новизни та практичних результатів дисертації спеціальності 122 «Комп'ютерні науки».

9. Дотримання принципів академічної доброчесності

Ознайомлення зі змістом дисертаційної роботи Мєшкова Вадима Ігоровича дає підстави стверджувати, що дослідження виконано з дотриманням вимог академічної доброчесності. На титульній сторінці дисертації зазначено, що робота містить результати власних досліджень, а використані ідеї, результати й тексти інших авторів мають посилання на відповідні джерела.

Основні положення, висновки та практичні результати дисертації відповідають тематиці опублікованих праць здобувача. У роботі коректно відображено науковий доробок автора, а результати, отримані у співавторстві, подано з урахуванням особистого внеску здобувача.

Під час аналізу дисертаційної роботи не виявлено ознак некоректного використання наукових джерел, привласнення чужих результатів, фабрикації або фальсифікації даних. Це дає підстави вважати, що дисертаційна робота відповідає принципам академічної доброчесності та вимогам до кваліфікаційних наукових праць.

10. Дискусійні положення та зауваження до дисертаційної роботи

Загалом 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 роботі варто було б чіткіше розмежувати етапи попередньої обробки даних, які виконуються до поділу вибірки на навчальну і тестову частини, та етапи, що мають застосовуватися лише до навчальної вибірки. Це є важливим для уникнення потенційного витоку інформації з тестових даних під час стандартизації, зниження розмірності або балансування вибірок.

2. Автором наведено результати застосування кількох моделей машинного навчання, проте питання вибору конкретних алгоритмів можна було б

обґрунтувати ширше. Зокрема, доцільно було б пояснити, чому саме обрані моделі є найбільш придатними для запропонованої двоетапної схеми класифікації, а також окремо порівняти їх із альтернативними підходами інтелектуального аналізу трафіку.

3. У дисертації доцільно було б докладніше показати внесок окремих етапів запропонованої технології у кінцевий результат класифікації. Зокрема, корисним був би абляційний аналіз, який дозволив би оцінити вплив очищення даних, стандартизації, зниження розмірності, балансування вибірок та вибору моделі на загальну ефективність виявлення атак.

4. У роботі наведено результати порівняння моделей за основними метриками якості, однак недостатньо розкрито питання вибору порогів прийняття рішень. Для практичного використання в системах виявлення атак важливо мати можливість змінювати поріг спрацювання залежно від допустимого рівня ризику, критичності мережі та вимог до чутливості системи.

5. Було б доцільно ширше висвітлити питання інтерпретованості результатів класифікації. У практичній діяльності фахівця з кібербезпеки важливо не лише отримати рішення про наявність атаки або її тип, а й мати пояснення, які ознаки трафіку найбільше вплинули на таке рішення. Це підвищило б довіру до запропонованої інформаційної технології та її придатність для використання в аналітичних підсистемах кібербезпеки.

6. Дисертаційну роботу можна було б посилити детальнішим описом умов відтворюваності експериментів, зокрема версій використаних програмних бібліотек, параметрів середовища виконання, способу фіксації випадкових станів генераторів, конфігурацій моделей та структури програмних сценаріїв. Це підвищило б можливість незалежної перевірки отриманих результатів.

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

11. Загальний висновок

Дисертаційна робота Мєшкова Вадима Ігоровича на тему «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак» є самостійним, завершеним і цілісним науковим дослідженням, у якому отримано результати, що мають наукове та практичне значення для розвитку інформаційних технологій інтелектуального аналізу мережевого трафіку.

У роботі обґрунтовано актуальність задачі виявлення атак у комп'ютерних мережах, розроблено метод підготовки, класифікації та оцінювання мережевого трафіку, запропоновано інформаційну технологію інтелектуального моніторингу, виконано її програмну реалізацію та проведено експериментальну перевірку ефективності. Отримані результати підтверджують доцільність використання методів машинного навчання для бінарного виявлення атакувальної активності та багатокласового розпізнавання типів атак.

Наукові положення і висновки дисертації є обґрунтованими, результати дослідження достатньо апробовані та висвітлені в наукових публікаціях здобувача. Висловлені зауваження мають дискусійний і рекомендаційний характер та не впливають на загальну позитивну оцінку дисертаційної роботи.

За змістом, рівнем наукової новизни, практичною спрямованістю та повнотою вирішення поставлених завдань дисертаційна робота відповідає спеціальності 122 «Комп'ютерні науки» та 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.

З огляду на викладене, дисертаційна робота Мєшкова Вадима Ігоровича заслуговує на позитивну оцінку, а її автор – на присудження наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Офіційний опонент:
старший викладач кафедри автоматизації
виробничих процесів
Центральноукраїнського національного
технічного університету,
кандидат технічних наук, доцент Тетяна СМІРНОВА

Підпис доцента Смірнової Т.В. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного
технічного університету,
кандидат технічних наук, доцент
"15" липня 2026 року Андрій ТИХИЙ