РІШЕННЯ
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки»

Здобувач ступеня доктора філософії **МЄШКОВ Вадим Ігорович**, 1984 р.н., громадянин України, освіта повна вища, у 2006 році закінчив Національний гірничий університет, факультет інформаційних технологій, за спеціальністю «Захист інформації в комп'ютерних системах та мережах», отримав диплом магістра. З жовтня 2022 р. є аспірантом НТУ «Дніпровська політехніка» вечірньої форми навчання за спеціальністю 122 «Комп'ютерні науки».

Виконав акредитовану освітньо-наукову програму «Комп'ютерні науки». Дисертацію виконано на кафедрі програмного забезпечення комп'ютерних систем Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Науковий керівник: доктор технічних науки, професор, завідувач кафедри безпеки інформації та телекомунікацій **КОРНІЄНКО Валерій Іванович**, Національний технічний університет «Дніпровська політехніка», Міністерства освіти і науки України.

Разова спеціалізована вчена рада, утворена рішенням Вченої ради Національного технічного університету «Дніпровська політехніка», МОН України, м. Дніпро від «30» червня 2026 року Протокол № 18, Наказ від «30» червня 2026 року № 111 у складі:

Голова разової спеціалізованої вченої ради – **МОРОЗ Борис Іванович**, доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Рецензенти:

АЛЕКСЄЄВ Михайло Олександрович, доктор технічних наук, професор, завідувач кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

ГЕРАСІНА Олександра Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформації та телекомунікацій, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Офіційні опоненти:

ГУЛАК Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка, Київського столичного університету імені Бориса Грінченка, м. Київ.

СМІРНОВА Тетяна Віталіївна, кандидат технічних наук, доцент, старший викладач кафедри автоматизації виробничих процесів,

Центральноукраїнського національного технічного університету, м. Кропивницький.

На засіданні «04» серпня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 «Інформаційні технології» **МЄШКОВУ Вадиму Ігоровичу** на підставі публічного захисту дисертації «**Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак**» за спеціальністю 122 «Комп'ютерні науки».

Дисертацію подано у вигляді спеціально підготовленого рукопису, українською мовою.

Наукова новизна одержаних результатів:

вперше розроблено інформаційну технологію інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, яка, на відміну від існуючих науково-технічних рішень, забезпечує в межах єдиного програмного модуля повний цикл підготовки даних мережевого трафіку, формування ознакового простору, побудови вибірок, балансування, навчання моделей машинного навчання та комплексного оцінювання результатів для двох взаємопов'язаних постановок задачі – бінарного виявлення атак і багатокласового розпізнавання їх типів;

удосконалено метод підготовки даних, класифікації та оцінювання мережевого трафіку для систем виявлення атак, який відрізняється інтегрованим поєднанням процедур попередньої обробки даних, аналізу та зниження розмірності ознакового простору, формування й балансування вибірок, навчання моделей машинного навчання та оцінювання їх якості, що забезпечує підвищення ефективності підготовки даних і розв'язання задач бінарного виявлення атак та багатокласового розпізнавання їх типів;

набули подальшого розвитку методичні положення комплексного оцінювання ефективності моделей машинного навчання в задачах моніторингу мережевого трафіку, які відрізняються уніфікованим поєднанням покласових метрик якості класифікації, ROC-AUC, Precision–Recall-кривих, матриць помилок і п'ятикратної перехресної перевірки та дають змогу визначати ефективні конфігурації моделей для двох режимів функціонування інформаційної технології: первинного бінарного виявлення атак і подальшого багатокласового розпізнавання їх типів.

Практичне значення одержаних результатів.

Практичне значення одержаних результатів полягає у розробці програмної реалізації інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі, яка може бути використане як основа для побудови інтелектуальних компонентів сучасних систем виявлення атак. Запропонована інформаційна технологія забезпечує автоматизований аналіз мережевого трафіку, підготовку вхідних даних до класифікації, виявлення атакувальної

активності в бінарному режимі та розпізнавання типів атак у багатокласовому режимі, що підвищує ефективність підтримки прийняття рішень у сфері кібербезпеки.

Практична цінність результатів дослідження полягає також у можливості використання розробленого програмного модуля для проведення експериментальних досліджень у задачах інтелектуального моніторингу мережевого трафіку, порівняльного аналізу моделей машинного навчання та оцінювання їх ефективності на основі набору даних CIC-IDS2017. Реалізована інформаційна технологія дозволяє відтворювати повний цикл обробки даних мережевого трафіку – від їх інтеграції, очищення, стандартизації та формування ознакового простору до навчання моделей і комплексного оцінювання результатів.

Одержані результати можуть бути використані в діяльності фахівців з кібербезпеки, під час розроблення та вдосконалення систем виявлення атак, а також у науково-дослідній та освітній діяльності закладів вищої освіти для підготовки здобувачів за спеціальностями, пов'язаними з комп'ютерними науками та кібербезпекою.

Здобувачем МЄШКОВИМ Вадимом Ігоровичем за темою дисертації опубліковано 11 робіт, з яких 4 статті включено до переліку фахових видань (категорія Б) (в т.ч. 3 – одноосібних), затверджених МОН України за спеціальністю дисертації, та 7 – публікації у матеріалах конференцій/симпозіумів (у тому числі 5 міжнародних), зокрема:

1. Мєшков В. Методи машинного навчання для бінарної та багатокласової класифікації мережевого трафіку у системах виявлення атак. *Таврійський науковий вісник. Серія: Технічні науки.* 2025, Т. 1, № 4. С. 182-196. DOI: https://doi.org/10.32782/tnv-tech.2025.4.1.20.

2. Мєшков В. Метод попередньої обробки даних для створення інформаційних моделей в інтелектуальних системах виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2025, №2. С. 108-114, DOI: https://doi.org/10.32782/IT/2025-2-11.

3. Сафаров О., Корнієнко В., Горєв В., Мєшков В. Підвищення кібербезпеки електронних комунікаційних систем медичного призначення. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2024, № 2, С. 128-133, DOI: https://doi.org/10.32782/IT/2024-2-16.

4. Мєшков В. Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023, № 1, С. 85-92, DOI: https://doi.org/10.32782/IT/2023-1-11.

У дискусії взяли участь усі члени разової спеціалізованої вченої ради.

Голова ради доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем Національного технічного університету «Дніпровська політехніка» **МОРОЗ Борис Іванович**:

Запитання № 1:

У дисертаційній роботі запропоновано інформаційну технологію інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. У чому полягає її відмінність від традиційного підходу до побудови систем виявлення вторгнень?

Запитання № 2:

Які результати дисертаційного дослідження, на Вашу думку, мають найбільше практичне значення для подальшого розвитку інтелектуальних систем кібербезпеки?

Здобувач **МЄШКОВ В.І.,** відповіді на запитання:

Відповідь на запитання № 1:

Відмінність запропонованої інформаційної технології полягає в тому, що вона орієнтована не лише на безпосередню класифікацію мережевого трафіку, а на реалізацію повного циклу інтелектуального аналізу даних для задач IDS. У роботі послідовно поєднано етапи підготовки даних, очищення, уніфікації, стандартизації, формування ознакового простору, зниження розмірності, балансування вибірок, навчання моделей машинного навчання та комплексного оцінювання результатів.

Традиційні IDS часто базуються на сигнатурному підході, який ефективний для відомих атак, але має обмеження під час виявлення нових, модифікованих або нетипових загроз. Запропонована технологія використовує методи машинного навчання, що дозволяє аналізувати статистичні закономірності в мережевому трафіку та виявляти ознаки атакувальної активності на основі поведінкових характеристик.

Крім того, у роботі передбачено два режими аналізу: бінарне виявлення факту атаки та багатокласове розпізнавання її типу. Це підвищує практичну інформативність результатів, оскільки система не лише визначає наявність атаки, а й деталізує її характер для подальшої підтримки прийняття рішень фахівцем із кібербезпеки.

Відповідь на запитання № 2:

Найбільше практичне значення має розроблена інформаційна технологія, яка може бути використана як основа для створення програмних компонентів інтелектуального аналізу мережевого трафіку в системах виявлення атак. Вона дозволяє автоматизувати ключові етапи роботи з мережевими даними: від попередньої обробки та формування вибірок до навчання моделей і оцінювання якості класифікації.

Практично важливим результатом є також реалізація двоетапного підходу:

спочатку визначається наявність атакувальної активності, а потім виконується розпізнавання типу атаки. Такий підхід відповідає логіці роботи реальних систем кібербезпеки, де важливо не лише зафіксувати інцидент, а й надати аналітику додаткову інформацію про його характер.

Крім того, значущими є результати порівняльного оцінювання моделей машинного навчання за комплексом метрик, що дозволяє обґрунтовано обирати моделі для різних режимів класифікації. Отримані результати можуть бути використані як у практичній діяльності підприємств та організацій, що експлуатують комп'ютерні мережі, так і в освітньому процесі під час підготовки фахівців зі спеціальності 122 «Комп'ютерні науки» та суміжних напрямів кібербезпеки.

Рецензент доктор технічних наук, професор, завідувач кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка» **АЛЕКСЄЄВ Михайло Олександрович.** Рецензія є позитивною. Зауваження та дискусійні положення:

1. У дисертаційній роботі запропоновано інформаційну технологію інтелектуального моніторингу мережевого трафіку, однак доцільно було б детальніше визначити вимоги до вхідних даних, які повинні надходити до такої технології. Зокрема, варто було б конкретизувати, чи передбачається робота лише з потоковими характеристиками трафіку, чи також можливе використання пакетних, сесійних або журналових даних із мережевих пристроїв.

2. У роботі використано процедури зниження розмірності ознакового простору, що є обґрунтованим з погляду зменшення надлишковості даних. Водночас бажано було б ширше проаналізувати, чи не призводить таке зниження розмірності до втрати специфічних ознак, характерних для окремих типів атак, особливо тих, що мають малу представленість у вибірці.

3. У дисертації наведено результати класифікації мережевого трафіку, однак питання оцінювання впевненості моделей у прийнятих рішеннях розкрито недостатньо. Для практичного застосування систем виявлення атак корисним було б врахування не лише класу, визначеного моделлю, а й рівня довіри до такого рішення, що може бути важливим під час пріоритезації інцидентів.

4. Доцільно було б окремо розглянути вплив можливих похибок розмітки даних на результати навчання та оцінювання моделей. У наборах мережевого трафіку помилки маркування або неоднозначність віднесення окремих записів до класів можуть впливати на якість класифікації, тому аналіз стійкості запропонованої технології до таких факторів посилив би експериментальну частину роботи.

5. У роботі основну увагу приділено технічним аспектам підготовки даних і побудови моделей машинного навчання, однак питання захисту самих даних

мережевого трафіку в процесі їх зберігання, обробки та використання розкрито обмежено. З огляду на те, що мережевий трафік може містити чутливу інформацію, доцільно було б окреслити вимоги до безпечного поводження з такими даними під час практичного впровадження запропонованої технології.

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

Запитання № 1:

У дисертаційній роботі запропоновано інформаційну технологію інтелектуального моніторингу мережевого трафіку. Які саме типи вхідних даних передбачено використовувати в межах цієї технології: потокові характеристики трафіку, пакетні дані, сесійні ознаки чи журнальні записи мережевого обладнання?

Запитання № 2:

У роботі використано процедури зниження розмірності ознакового простору. Як у дисертації враховано ризик втрати специфічних ознак, важливих для розпізнавання окремих або малопоширених типів атак?

Здобувач **МЄШКОВ В.І.,** відповідь на запитання:

Відповідь на запитання № 1:

У межах дисертаційного дослідження основну увагу було зосереджено на використанні ознак мережевих потоків, оскільки саме такий формат даних подано в наборі CIC-IDS2017, який використано як експериментальну основу роботи. Ці ознаки відображають статистичні та часові характеристики мережевих з'єднань, зокрема параметри тривалості потоків, кількості пакетів, обсягів переданих даних, швидкості передавання, інтервалів між пакетами та інших характеристик мережевої активності.

Запропонована інформаційна технологія орієнтована передусім на роботу з табличним ознаковим поданням мережевого трафіку, придатним для застосування методів машинного навчання. Водночас її структура не обмежується лише конкретним набором CIC-IDS2017. За умови попереднього перетворення пакетних, сесійних або журнальних даних у формалізований ознаковий простір вони також можуть бути використані як вхідні дані для цієї технології.

Таким чином, базовим типом вхідних даних у роботі є потокові характеристики мережевого трафіку, однак у подальшому технологія може бути розширена для використання інших джерел даних, зокрема журналів IDS/IPS,

NetFlow/IPFIX-записів, сесійних характеристик або агрегованих даних із мережевого обладнання. Основною умовою є приведення таких даних до узгодженої структури ознак, необхідної для навчання та застосування моделей машинного навчання.

Відповідь на запитання № 2:

Зниження розмірності ознакового простору в роботі застосовувалося з метою зменшення надлишковості даних, усунення взаємозалежних ознак і підвищення стабільності роботи моделей машинного навчання. Перед цим виконувались аналіз ознак, кореляційний аналіз і стандартизація числових характеристик, що дозволило сформувати більш узгоджений простір даних для подальшої класифікації.

Ризик втрати інформативних ознак справді є важливим для задач багатокласового розпізнавання атак, особливо для класів із малою кількістю прикладів. У роботі цей ризик частково враховано через подальше експериментальне оцінювання моделей за покласовими метриками precision, recall і F1-score, а також за матрицями помилок. Це дозволяє виявити, для яких класів атак якість розпізнавання є достатньою, а для яких вона потребує покращення.

Водночас більш детальний аналіз впливу зниження розмірності на окремі класи атак є перспективним напрямом подальших досліджень. Зокрема, доцільно додатково порівнювати результати класифікації до і після зниження розмірності, оцінювати внесок окремих ознак у розпізнавання рідкісних атак і за потреби використовувати комбіновані підходи, коли частина критично важливих ознак зберігається незалежно від загальної процедури скорочення ознакового простору.

Рецензент кандидат технічних наук, доцент, доцент кафедри безпеки інформації та телекомунікацій, Національного технічного університету «Дніпровська політехніка» **ГЕРАСІНА Олександра Володимирівна.** Рецензія є позитивною. Зауваження та дискусійні положення:

1. У дисертації доцільно було б більш чітко розмежувати процедури попередньої обробки даних, які виконуються до поділу вибірки на навчальну і тестову частини, а також процедури, які мають виконуватися лише на навчальних даних. Це важливо для уникнення потенційного витоку інформації з тестової вибірки під час стандартизації, зниження розмірності або балансування даних.

2. У дисертаційній роботі значну увагу приділено порівнянню моделей машинного навчання за узагальненими метриками, однак доцільно було б детальніше проаналізувати покласову поведінку моделей для окремих типів атак. Такий аналіз дав би змогу краще визначити, для яких саме класів атак

запропонована технологія демонструє найвищу ефективність, а для яких потребує додаткового налаштування або розширення навчальної вибірки.

3. При моделюванні та статистичній обробці експериментальних даних недостатню увагу приділено визначенню адекватності моделей та значущості отриманих результатів.

4. У роботі недостатньо уваги приділено питанню обмежень запропонованої технології під час аналізу зашифрованого або частково прихованого трафіку. Оскільки в сучасних мережах значна частина взаємодій відбувається із застосуванням шифрування, доцільно було б окремо зазначити, які саме ознаки залишаються доступними для аналізу та як це може впливати на якість виявлення атак.

5. В роботі мають місце деякі граматичні та стилістичні помилки; декілька раз зустрічаються введення одних й тих самих скорочень: наприклад, «системи виявлення атак (СВА)» наведено тричі – на стор. 2, 3, 20, але такого небагато по усьому тексту дисертації.

Вказані зауваження не знижують загального позитивного враження від дисертації, як з точки зору актуальності теми, так і з точки зору наукової новизни та практичної цінності отриманих результатів.

Запитання № 1:

У дисертаційній роботі основну увагу приділено метрикам якості класифікації моделей. Як у практичному застосуванні запропонованої інформаційної технології можна враховувати вибір порогу прийняття рішень залежно від критичності мережі та допустимого рівня помилкових спрацювань?

Здобувач **МЄШКОВ В.І.,** відповідь на запитання:

Відповідь на запитання № 1:

У дисертаційній роботі основну увагу було зосереджено на порівняльному оцінюванні моделей машинного навчання за уніфікованою системою метрик: accuracy, precision, recall, F1-score, ROC-AUC, Precision–Recall-кривими та матрицями помилок. Такий підхід дозволив комплексно оцінити якість моделей у задачах бінарного виявлення атак і багатокласового розпізнавання їх типів.

У практичних системах виявлення атак вибір порогу прийняття рішення справді має важливе значення. Для мереж із високими вимогами до безпеки доцільно знижувати поріг спрацювання, щоб підвищити ймовірність виявлення атакувального трафіку, навіть якщо це збільшує кількість хибнопозитивних спрацювань. Для менш критичних або ресурсно обмежених середовищ поріг може бути підвищений, щоб зменшити навантаження на аналітиків безпеки та кількість помилкових тривог.

Офіційний опонент доктор технічних наук, професор, професор кафедри

інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка, Київського столичного університету імені Бориса Грінченка, м. Київ **ГУЛАК Геннадій Миколайович.** Відгук є позитивним. Зауваження та дискусійні положення:

1. У дисертаційній роботі основну увагу приділено моделям машинного навчання, зокрема логістичній регресії, методу опорних векторів, дереву рішень, випадковому лісу та методу k-найближчих сусідів. Разом із тим доцільно було б ширше розглянути можливість порівняння запропонованого підходу із сучасними методами глибокого навчання, зокрема нейронними мережами, автоенкодерами або рекурентними моделями, які також застосовуються для аналізу мережевого трафіку та виявлення аномалій.

2. У роботі запропоновано архітектуру інформаційної технології та описано її програмну реалізацію, однак питання інтеграції розробленого рішення в реальні IDS/IPS-системи розкрито недостатньо детально. Було б доцільно конкретизувати можливі сценарії практичного впровадження технології, зокрема її взаємодію з існуючими засобами моніторингу, джерелами мережевого трафіку, журналами подій, SIEM-системами та іншими компонентами інфраструктури кібербезпеки.

3. Експериментальне дослідження виконано на основі набору даних CIC-IDS2017, який є поширеним і репрезентативним для задач дослідження систем виявлення атак. Водночас додаткова перевірка запропонованої інформаційної технології на інших наборах даних або на фрагментах реального мережевого трафіку дала б змогу ширше оцінити її узагальнювальну здатність, стійкість до зміни структури трафіку та придатність до використання в різних мережевих середовищах.

4. У дисертації наведено результати навчання та оцінювання моделей машинного навчання, однак процедуру вибору й налаштування гіперпараметрів окремих моделей можна було б подати більш докладно. Зокрема, доцільно було б показати, яким чином зміна ключових параметрів моделей впливає на точність, повноту, F1-score, кількість помилкових спрацювань і пропущених атак, оскільки це має важливе значення для практичного застосування систем виявлення атак.

5. Дискусійним залишається питання стійкості розробленої інформаційної технології до зміни характеристик мережевого трафіку в часі. У реальних комп'ютерних мережах структура трафіку, поведінка користувачів і характер атак можуть істотно змінюватися. Тому в подальших дослідженнях доцільно було б розглянути механізми періодичного перенавчання моделей, адаптації до нових типів атак і виявлення деградації якості класифікації в процесі експлуатації.

6. У роботі використано комплексну систему метрик оцінювання якості моделей, що є позитивною стороною дослідження. Разом із тим варто було б ширше проаналізувати практичні наслідки помилкових спрацювань і пропусків атак для реальних систем кібербезпеки. Наприклад, у промислових або корпоративних мережах хибнопозитивні спрацювання можуть перевантажувати аналітиків безпеки, тоді як хибнонегативні результати можуть призводити до пропуску критичних інцидентів.

7. Доцільно було б детальніше висвітлити питання обчислювальної складності та швидкодії запропонованої інформаційної технології. Для практичного використання в системах моніторингу мережевого трафіку важливими є не лише показники точності класифікації, а й час обробки даних, вимоги до оперативної пам'яті, масштабованість рішення та можливість роботи з великими потоками трафіку в умовах, наближених до реального часу.

Зазначені зауваження мають переважно дискусійний і рекомендаційний характер, не знижують достовірності основних наукових положень, висновків і практичних результатів дисертаційної роботи, а також можуть бути враховані автором у подальших дослідженнях, спрямованих на розвиток інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак.

Запитання № 1:

У дисертаційній роботі для бінарного виявлення атак і багатокласового розпізнавання їх типів використано переважно класичні моделі машинного навчання: логістичну регресію, метод опорних векторів, дерево рішень, випадковий ліс і метод k-найближчих сусідів. Чим обґрунтовано вибір саме цих моделей, а не сучасних методів глибокого навчання?

Запитання № 2:

Експериментальне дослідження виконано на наборі даних CIC-IDS2017. Яким чином можна забезпечити придатність запропонованої інформаційної технології до використання в реальних мережевих середовищах, де структура трафіку та характер атак можуть змінюватися з часом?

Здобувач **МЄШКОВ В.І.,** відповідь на запитання:

Відповідь на запитання № 1:

Вибір зазначених моделей був зумовлений метою дисертаційного дослідження – розробити інформаційну технологію інтелектуального моніторингу мережевого трафіку, яка забезпечує відтворюваний повний цикл підготовки даних, навчання моделей і комплексного оцінювання результатів у двох режимах: бінарному та багатокласовому.

Класичні моделі машинного навчання були обрані тому, що вони добре працюють із табличними ознаками мережевого трафіку, мають нижчі вимоги до обчислювальних ресурсів, є більш інтерпретованими та придатними для

порівняльного аналізу в умовах однаково підготовленого ознакового простору. Крім того, такі моделі дозволяють чітко оцінити вплив попередньої обробки даних, стандартизації, зниження розмірності та балансування вибірок на якість класифікації.

Методи глибокого навчання дійсно є перспективними для задач виявлення атак, однак вони потребують більших обсягів даних, складнішого налаштування архітектури, вищих обчислювальних ресурсів і окремого аналізу інтерпретованості результатів. Тому в межах цієї дисертаційної роботи основну увагу було зосереджено на побудові цілісної інформаційної технології з використанням моделей, які є ефективними, відтворюваними та практично придатними для інтеграції в інтелектуальні компоненти IDS. Порівняння із сучасними нейромережевими підходами розглядається як перспективний напрям подальших досліджень.

Відповідь на запитання № 2:

Набір даних CIC-IDS2017 було обрано як репрезентативну експериментальну основу, оскільки він містить як нормальний трафік, так і різні типи атак, має поширене використання в дослідженнях IDS і дозволяє виконати відтворюване порівняння моделей машинного навчання.

Водночас запропонована інформаційна технологія не прив'язана виключно до цього набору даних. Її структура передбачає послідовне виконання універсальних етапів: завантаження та уніфікацію даних, очищення, обробку пропущених і некоректних значень, стандартизацію ознак, формування вибірок, балансування класів, навчання моделей та оцінювання результатів. За наявності інших джерел мережевого трафіку ці етапи можуть бути адаптовані до нового ознакового простору та нових класів атак.

Для практичного використання в реальних IDS/IPS-системах доцільно передбачити періодичне оновлення навчальних вибірок, повторне навчання моделей, контроль зміни якості класифікації та перевірку технології на нових наборах даних або фрагментах реального мережевого трафіку. Таким чином, розроблена інформаційна технологія може розглядатися як базова програмно-методична основа, яка в подальшому може бути розширена механізмами адаптації до зміни характеристик трафіку та появи нових типів атак.

Офіційний опонент кандидат технічних наук, доцент, старший викладач кафедри автоматизації виробничих процесів, Центральноукраїнського національного технічного університету, м. Кропивницький **СМІРНОВА Тетяна Віталіївна.** Відгук є позитивним. Зауваження та дискусійні положення:

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.

Запитання № 1:

У дисертаційній роботі передбачено послідовне виконання процедур очищення, стандартизації, зниження розмірності та балансування даних. Яким чином у роботі забезпечено коректність попередньої обробки даних і

недопущення впливу тестової вибірки на процес навчання моделей?

Запитання № 2:

У роботі використано декілька моделей машинного навчання та систему метрик оцінювання. Як можна визначити внесок окремих етапів запропонованої інформаційної технології – очищення даних, стандартизації, зниження розмірності, балансування вибірок – у підсумкову якість виявлення атак?

Здобувач **МЄШКОВ В.І.,** відповідь на запитання:

Відповідь на запитання № 1:

Коректність попередньої обробки даних забезпечувалася шляхом побудови послідовного конвеєра обробки мережевого трафіку. На початковому етапі виконувалися загальні технічні процедури, необхідні для приведення набору даних до придатного для аналізу стану: уніфікація структури ознак, видалення дублікатів, опрацювання пропущених і нескінченних значень, а також формування узгодженого ознакового простору.

Після цього формувалися вибірки для бінарної та багатокласової класифікації. Для зменшення ризику некоректного впливу тестових даних на навчання моделей процедури масштабування, зниження розмірності та балансування розглядалися як етапи, які мають виконуватися з урахуванням поділу даних на навчальну та тестову частини. Зокрема, параметри стандартизації та перетворення ознакового простору повинні визначатися на навчальній вибірці, а потім застосовуватися до тестових даних за вже встановленими параметрами.

У роботі основний акцент зроблено на методичній послідовності побудови інформаційної технології та порівняльному оцінюванні моделей за однакових умов підготовки даних. Водночас зауваження щодо ще чіткішого формального розмежування етапів попередньої обробки є слушним і може бути враховане під час подальшого вдосконалення програмної реалізації, зокрема шляхом оформлення всіх процедур у вигляді єдиного відтворюваного ML-конвеєра.

Відповідь на запитання № 2:

Внесок окремих етапів інформаційної технології можна визначати шляхом поетапного порівняльного експерименту, тобто абляційного аналізу. Його суть полягає в тому, що базова модель оцінюється на повному конвеєрі обробки даних, а потім окремі етапи послідовно виключаються або замінюються спрощеними варіантами. Наприклад, можна порівняти результати класифікації без балансування вибірок, без зниження розмірності, без стандартизації або без окремих процедур очищення даних.

У дисертаційній роботі вплив запропонованої технології оцінювався через кінцеві результати класифікації в бінарному та багатокласовому режимах, а також через комплекс метрик: accuracy, precision, recall, F1-score, ROC-AUC, Precision–Recall-криві та матриці помилок. Такий підхід дозволив встановити

загальну ефективність побудованого конвеєра та порівняти моделі машинного навчання в однакових умовах.

Разом із тим окремий абляційний аналіз справді дав би змогу детальніше кількісно оцінити внесок кожної процедури в кінцевий результат. Це є перспективним напрямом подальших досліджень, оскільки дозволить не лише підтвердити ефективність інформаційної технології загалом, а й оптимізувати її структуру, залишивши найбільш значущі етапи для практичного використання в системах виявлення атак.

Результати відкритого голосування:

«За» 5 (п'ять) членів ради,

«Проти» 0 (нуль) членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує **МЄШКОВУ Вадиму Ігоровичу** ступінь доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Голова разової спеціалізованої вченої ради _____ Борис МОРОЗ