УДК 004.05+004.89 **DOI:10.15330/itee.2025.3.04**

І. Я. САВКА, канд. фіз-мат. наук, М. С. ДУТЧАК, О. Т. КОВАЛЬ

ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ЯКОСТІ ПЗ ДЛЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ ВІД МЕТОДІВ ВИБОРУ ОЗНАК У МОДЕЛЯХ МАШИННОГО НАВЧАННЯ

Вступ

Стрімке зростання масштабів і складності кібератак, поява нових типів загроз та збільшення обсягів мережевого трафіку зумовлюють підвищені вимоги до систем виявлення вторгнень (Intrusion Detection Systems, IDS) [1]. Такі системи мають не лише забезпечувати високий рівень виявлення атак, а й гарантувати прийнятну швидкодію, стабільність роботи та здатність до масштабування в умовах реальних мережевих навантажень. Суттєву роль у розвитку IDS відіграють методи машинного навчання (ML), які дозволяють створювати аномальні та гібридні системи виявлення загроз. Водночас на практиці ML-базовані IDS часто стикаються з проблемами високої кількості хибних спрацювань, значних обчислювальних витрат та чутливості до якості вихідних даних. Одним із ключових чинників, що визначає ефективність таких систем для аналізу мережевого трафіку, є відбір інформативних ознак (Feature Selection, FS) із множини наявних характеристик. Саме відбір ознак впливає на точність класифікації, час навчання та прогнозування, необхідний обсяг ресурсів і можливості масштабування IDS. Більшість існуючих досліджень, присвячених застосуванню FS у задачах виявлення вторгнень, зосереджуються переважно на покращенні окремих класифікаційних метрик (accuracy, precision, F1, recall тощо). При цьому якість програмного забезпечення IDS як цілісного продукту, у розумінні стандарту якості, наприклад ISO/IEC 25010, розглядається недостатньо. Недостатньо формалізованими залишаються питання того, як різні підходи до відбору ознак впливають на баланс між функціональними та нефункціональними характеристиками IDS систем, а також, яким чином враховувати разові витрати на виконання процедури FS у загальній оцінці якості.

Аналіз останніх досліджень та публікацій

Застосування технік відбору ознак у ML-базованих IDS є важливим кроком, що покращує ефективність, точність та інтерпретованість моделі шляхом зменшення розмірності та усунення зайвих атрибутів даних [5, 6]. У табл. 1 наведена порівняльна характеристика основних методів вибору ознак: фільтраційні (Filter), обгорткові (Wrapper) та вбудовані (Embedded) [3]. Крім того, у деяких дослідженнях використовується комбінований підхід, що часто дає кращий результат, ніж кожен окремо.

Таблиця 1

Підхід (Feature Selection)	**Опис та характеристики**	**Приклади методів**
Filter (фільтраційний)	Відбір ознак на основі статистичних критеріїв, незалежно від моделі класифікації. Швидкий і не призводить до перенавчання під конкретний алгоритм, але може не врахувати спільний ефект ознак.	Information Gain, χ^2-тест, коеф. кореляції, ReliefF, відбір на основі варіації.
Wrapper (обгортковий)	Пошук оптимальної підмножини ознак шляхом багаторазового навчання і оцінки моделі. Забезпечує високі результати для обраної моделі, але дуже затратний за часом і обчисленнями.	Recursive Feature Elimination (RFE), покроковий пошук вперед/назад, генетичні алгоритми, метод рою часток (PSO).
Embedded (вбудований)	Відбір ознак під час навчання моделі. Модель сама визначає важливість ознак і може відкинути неважливі. Ефективніший за wrapper щодо ресурсів, враховує взаємодію з моделлю.	Дерева рішень, Random Forest (Gini importance), L1-регуляризована логістична регресія (LASSO).

За даними експериментів [2, 4, 7], модель, навчена на найбільш релевантних ознаках, досягає майже такої ж точності детекції, як і модель на повному наборі ознак. При цьому, обсяг даних скорочується, а час обробки суттєво зменшується. В окремих випадках відбір ознак навіть може підвищити точність виявлення, оскільки модель не враховує шумові фактори. Практичні експерименти підтверджують, що різні методи FS впливають на якість IDS по-різному. Наприклад, дослідження впливу фільтраційних методів на продуктивність чотирьох класифікаторів (MLP, SVM, XGBoost, Random Forest) показало, що за умови правильного вибору підмножини ознак можна значно зменшити їх кількість без погіршення якості детекції атак [6]. У роботі [8] запропоновано гібридну багатоетапну схему FS, що дозволило зменшити кількість ознак з 42 до 23 та підвищити точність класифікації аномалій з 82.25% до 84.24%. З іншого боку, невдале вилучення ключових ознак може погіршити ефективність IDS. Наприклад, якщо відкинути параметр, який критично відрізняє певну атаку від нормального трафіку, класифікатор може почати плутати цю атаку з легітимною активністю. Тому процес відбору ознак має проводитися обережно, з оцінкою впливу кожної вилученої ознаки на результат. Для цього зазвичай будують графіки залежності метрик моделі від кількості ознак або порогу значущості та вибирають компромісний набір.

Формулювання цілей статті

Попри значну кількість досліджень, присвячених методам відбору ознак, все ще недостатньо вивченими залишаються питання комплексного впливу різних підходів до відбору ознак не тільки на точність виявлення атак, але й на інші критично важливі характеристики якості IDS. Крім того, у науковій літературі фактично відсутні підходи до формалізації узагальненого показника якості IDS, який би інтегрував функціональні та нефункціональні характеристики системи та дозволяв об’єктивно порівнювати різні методи відбору ознак у єдиному числовому вимірі. Бракує також і методики, яка враховувала б ресурсні витрати, пов’язані зі застосуванням відбору ознак, зокрема час навчання, швидкість прогнозування та масштабованість моделі при роботі з великими масивами даних.

З огляду на зазначені проблеми, у межах даного дослідження ставиться завдання експериментального дослідження залежності якості ПЗ від методів вибору ознак у моделях ML, а також розроблення методики комплексної оцінки якості IDS з урахуванням впливу різних підходів до відбору ознак та побудови інтегрального показника якості.

Методологія та основний матеріал досліджень

Для оцінки якості ПЗ доцільно керуватися міжнародним стандартом ISO/IEC 25010 [10], що визначає модель якості ПЗ та описує сукупність характеристик, серед яких для IDS особливо важливими є наступні ключові групи.

Функціональна придатність (Functional Suitability) – здатність ПЗ коректно виконувати потрібні функції та досягати поставлених цілей. У даному дослідженні функціональна придатність

$$F_{func} = \frac{Accuracy + F1}{2}$$

представлена через метрики $Accuracy$ (загальна частка правильних спрацювань) та $F1$-score (гармонійне середнє влучності та повноти), що разом відображають здатність IDS правильно класифікувати трафік.

Надійність (Reliability) – здатність системи підтримувати необхідний рівень виконання функцій відповідно до заданих умов протягом певного часу. Для IDS критерієм надійності роботи можна вважати стійкість до хибних спрацювань та помилок. Для вимірювання показника надійності $F_{rel} = Precision$ використано влучність $Precision$ (точність позитивного прогнозу), що характеризує частку дійсних атак серед усіх спрацювань системи.

Продуктивність (Performance Efficiency) – характеристика, що відображає швидкодію та оптимальність використання ресурсів ПЗ. Продуктивність пропонується визначати як

зважене середнє між ефективністю процесу навчання F_{train} та ефективністю прогнозування F_{infer}:

$$F_{perf} = \alpha * F_{train} + (1 - \alpha) * F_{infer},$$

де коефіцієнт $\alpha \in [0, 1]$ дозволяє задати пріоритетність. Для оцінювання метрики F_{train} використовується формула:

$$F_{train} = \exp\left(-\beta * \frac{T_{eff}}{T_{train}^{base}}\right),$$

де $\beta > 0$ – коефіцієнт згладжування, що керує чутливістю метрики до часу навчання, а T_{train}^{base} – час навчання тієї ж моделі без відбору ознак (на повному наборі ознак). Тут величина T_{eff} є ефективним часом навчання з урахуванням процедури відбору ознак FS і визначається як $T_{eff} = T_{train} + \frac{T_{FS}}{K}$, де T_{train} – фактично виміряний час навчання моделі з використанням певного методу FS, T_{FS} – час, витрачений на виконання процедури FS, K – кількість планових перенавчань моделі протягом певного періоду її використання.

Показник ефективності прогнозування $F_{infer} = 1 - \frac{T_{predict}}{T_{max}}$ характеризує ефективність часу роботи моделі під час класифікації мережевого з'єднання чи пакету. Для його обчислення порівнюється швидкодія моделей відносно найповільнішої з них. Тут $T_{predict}$ – час прогнозування конкретним алгоритмом, а T_{max} – максимальний час прогнозування серед усіх порівнюваних випадків. F_{infer} показує, наскільки даний алгоритм швидший за найповільніший еталон. Для швидших моделей значення показника наближається до 1, що відображає їх відносний виграш у швидкодії.

Масштабованість (Scalability) – у стандарті ця характеристика прямо не виділена, але у контексті оцінки IDS ми вводимо її як важливий показник якості такого ПЗ. Масштабованість описує здатність системи ефективно працювати зі збільшенням обсягу даних чи навантаження. Показник масштабованості F_{scale} характеризує здатність IDS-моделі ефективно працювати зі зростаючими обсягами даних і кількістю ознак. Зменшення розмірності, як правило, спрощує розгортання, перенесення та паралельну обробку моделі. Кількісну оцінку цього ефекту задаємо формулою:

$$F_{scale} = \max\left\{0, 1 - \frac{N}{N_{base}}\right\},$$

де N – кількість ознак після застосування певного FS-методу, а N_{base} – кількість ознак у початковому датасеті (noFS). За відсутності скорочення кількості ознак показник масштабованості набуває нульового значення, а у разі зменшення розмірності F_{scale} відображає відносну частку усунених ознак.

Об'єднавши описані складові, загальну оцінку якості IDS-моделі визначаємо через інтегральний показник формулою:

$$Q = w_1 * F_{func} + w_2 * F_{rel} + w_3 * F_{perf} + w_4 * F_{scale},$$

де w_1, w_2, w_3, w_4 – ваги, що відображають пріоритетність відповідних характеристик. У межах даного дослідження для визначення ваг використовується метод аналізу ієрархій (Analytic Hierarchy Process, AHP). Побудова ваг здійснюється на основі попарних порівнянь критеріїв, які виконуються експертом із використанням вербально-числової шкали Сааті. Зазначена шкала дає змогу формалізувати суб'єктивні експертні судження шляхом їх відображення у числові оцінки інтенсивності переваги одного критерію над іншим.

На основі цього був розроблений модульний веб-застосунок на базі Streamlit із багаторівневою архітектурою, що розділяє ядро для обробки даних і алгоритмів IDS та веб-

інтерфейс для взаємодії з користувачем, з підтримкою повного циклу експериментів і швидкого перерахунку показників якості (див. рис. 1-5).

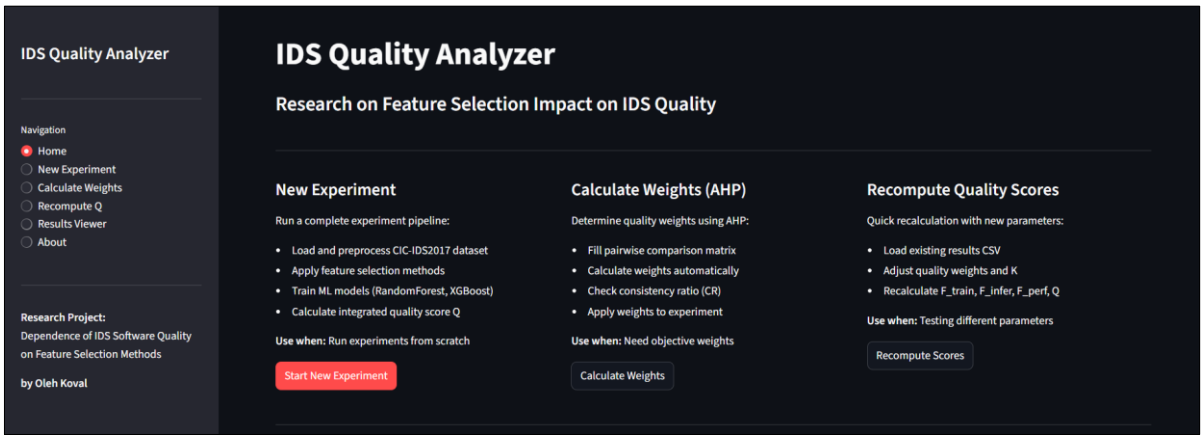

Рис. 1. Головна сторінка веб-застосунку

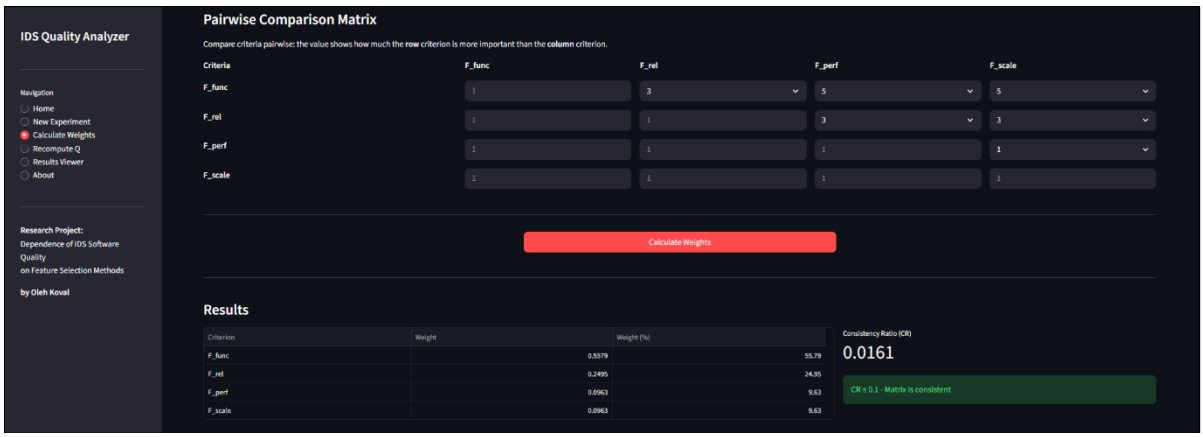

Рис. 2. Приклад обрахунку ваг за методом AHP

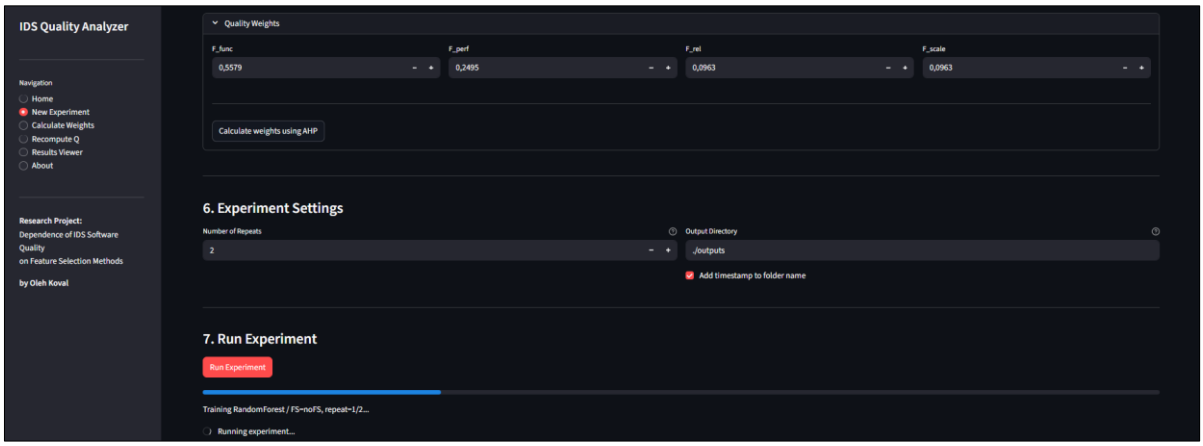

Рис. 3. Процес проведення експерименту

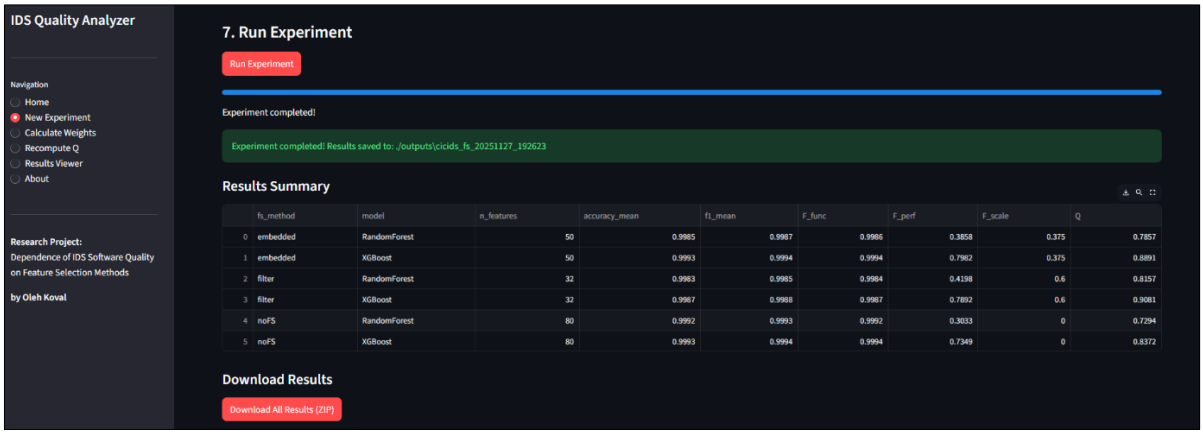

Рис. 4. Успішне завершення проведення експерименту

Рис. 5. Візуалізація показників після перерахунку

Результати експерименту та їх інтерпретація

У дослідженні використано відкритий набір даних CIC-IDS2017 [9], що містить детальні записи мережевого трафіку, мітки атак та нормальної діяльності, а також охоплює широкий спектр різновидів атак (DoS, DDoS, Web-Attacks, Infiltration, Botnet, Brute-force тощо). Перевагою CIC-IDS2017 є те, що він має реалістичний трафік за декілька днів, кожен з яких присвячений певним атакам. Всього набір містить ~3 млн мережевих сесій з 80 різними ознаками.

Для досягнення цілей даного дослідження дані було підготовлено як задачу бінарної класифікації: кожен запис позначено як «нормальний» або «атака» (всі типи атак об'єднані в один «шкідливий» клас). Оригінальні CSV-файли датасету було об'єднано та випадковим чином розбито на навчальну і тестову вибірки у співвідношенні 70/30. Перед навчанням моделей здійснено базове попереднє оброблення даних: очищено або видалено записи з відсутніми значеннями полів (деякі сесії мали некоректні значення через помилки збору даних), категоріальні атрибути (тип протоколу, служби тощо) перетворено на числові через one-hot кодування або зіставлення категорій з числами. Також було виконано нормалізацію числових ознак (методом мін-макс до інтервалу [0;1]) задля прискорення сходження алгоритмів навчання і щоб жодна ознака не домінувала за масштабом.

Було розглянуто три популярних підходи до FS (див. табл. 1), які відрізняються за способом відбору ознак, а також контрольний випадок без відбору (noFS). Для побудови IDS-моделі використано два алгоритми машинного навчання: Random Forest (RF) і XGBoost (XGB) з базовими параметрами. Для кожного з чотирьох сценаріїв відбору ознак (noFS, Filter, Embedded, Wrapper) і двох моделей (Random Forest, XGBoost) було виконано повний

цикл: відбір ознак (для трьох методів FS), навчання моделі на навчальній вибірці, тестування на тестовій, вимірювання часу навчання та прогнозування, а також обчислення метричних показників Accuracy, Precision, Recall, F1. Щоб зменшити випадкові флуктуації часу (відхилення від середнього), кожен експеримент повторювався двічі, а середні значення часу навчання і прогнозування визначалися за результатами усереднення повторів. Вимірювання часу виконувалося за допомогою функції time.perf_counter() у Python. Метрики точності обчислювалися засобами пакета sklearn.metrics.

У наведених табл. 2 і табл. 3 представлені основні результати дослідження із використанням таких параметрів $\alpha = \beta = 0.5, K = 36, w_1 = 0.55, w_2 = 0.25, w_3 = w_4 = 0.1$.

Таблиця 2

	Метод	**Модель**	N	T_{train}	T_{FS}	T_{eff}	F_{train}	$T_{predict}$	F_{infer}
1	embedded	RF	52	56.30	161	60.79	0.60	0.67	0.009
2	embedded	XGBoost	52	5.20	161	9.68	0.55	0.23	0.66
3	filter	RF	32	28.97	80	31.19	0.77	0.49	0.28
4	filter	XGBoost	32	4.68	80	6.89	0.65	0.18	0.73
5	wrapper	RF	20	24.42	1590	68.60	0.56	0.43	0.37
6	wrapper	XGBoost	20	3.03	1590	47.20	0.05	0.17	0.74
7	noFS	RF	80	59.50	0	59.50	0.61	0.68	0.0
8	noFS	XGBoost	80	8.06	0	8.06	0.61	0.20	0.7

Таблиця 3

	Метод	**Модель**	N	F_{func}	F_{rel}	F_{perf}	F_{scale}	Q
1	embedded	RF	52	0.99	0.99	0.30	0.35	0.763
2	embedded	XGBoost	52	0.99	0.99	0.60	0.35	0.839
3	filter	RF	32	0.99	0.99	0.52	0.60	0.842
4	filter	XGBoost	32	0.99	0.99	0.69	0.60	0.885
5	wrapper	RF	20	0.99	0.99	0.46	0.75	0.842
6	wrapper	XGBoost	20	0.99	1.0	0.40	0.75	0.825
7	noFS	RF	80	0.99	0.99	0.30	0.0	0.729
8	noFS	XGBoost	80	0.99	0.99	0.65	0.0	0.817

В усіх проведених експериментах використання методів відбору ознак FS не погіршило здатність моделей виявляти атаки. Алгоритми FS здатні вилучити до 75% ознак (як у випадку wrapper, 20 із 80) без втрати інформації, необхідної для правильної класифікації. З точки зору IDS, це означає, що можна значно спростити моделі та вхідні дані, зберігши той самий рівень детекції атак. Такий висновок узгоджується з результатами робіт [7, 8], де також відзначалося, що видалення нерелевантних ознак часто не знижує, а інколи навіть підвищує точність моделі за рахунок усунення шуму та колінеарності.

Найбільші відмінності між підходами проявилися саме в нефункціональних аспектах. Без застосування FS (noFS) система демонструє найгірші показники як за швидкодією, так і за масштабованістю. Це цілком очікувано, адже моделі з 80 ознаками мають більший обсяг обчислень. Застосування будь-якого з методів FS істотно підвищує продуктивність F_perf. Найбільший приріст продуктивності забезпечив фільтраційний метод (див. табл. 3). Це пояснюється оптимальним співвідношенням, а саме помірний час виконання FS (80 с.) та суттєве зменшення кількості ознак, і як наслідок – помітне прискорення як навчання, так і прогнозування. Embedded дав менший виграш через відносно невелике скорочення ознак і значний час FS, а wrapper – через надто великий час на FS, який зменшив виграш від скорочення ознак у термінах ефективного часу.

Щодо масштабованості F_scale з точки зору можливості розгортання IDS на великі дані, то тут лідером став wrapper, оскільки модель з 20 ознаками може обробляти значно більші потоки трафіку без перевантаження, ніж модель з 80 ознаками. Фільтраційний підхід та

embedded теж значно підвищили масштабованість моделі (на 60% і 35% відповідно). Проте на практиці, wrapper-відбір ознак доцільний лише якщо система має ресурси виконати цей відбір офлайн, інакше тривале очікування може нівелювати користь.

Проаналізувавши показники надійності, продуктивності та масштабованості, було обчислено значення інтегрального показника Q для різних підходів (рис. 6). Найкращим підходом виявився фільтраційний FS із XGBoost, $Q = 0.885$. Це може слугувати рекомендацією: спочатку відсіяти явно зайві параметри швидким статистичним методом, а потім застосувати потужний алгоритм класифікації. Така комбінація забезпечить високу якість виявлення при оптимальній продуктивності та масштабованості.

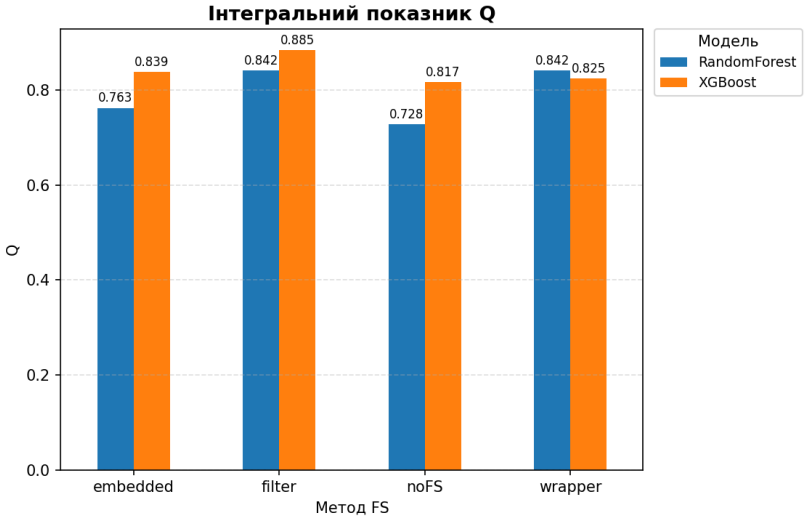

Рис. 6. Значення інтегрального показника Q

Висновки

У роботі виконано дослідження проблеми оцінювання якості програмного забезпечення систем виявлення вторгнень (IDS), побудованих на основі методів машинного навчання та різних підходів до відбору ознак Feature Selection. На основі аналізу було розроблено методику комплексної оцінки якості систем із урахуванням впливу методів відбору ознак, що об'єднує функціональні й нефункціональні характеристики системи відповідно до моделі ISO/IEC 25010. Обґрунтовано вибір основних показників якості систем для виявлення вторгнень: функціональної придатності, надійності, продуктивності та масштабованості. Для кожного з них запропоновано формули кількісної оцінки, на основі яких формується інтегральний показник якості.

Результати демонструють, що вибір методу FS та зменшення простору ознак суттєво впливають на продуктивність і масштабованість IDS, що обґрунтовує включення цього фактору до комплексної оцінки якості сучасних систем виявлення вторгнень.

Практичним результатом дослідження є розроблений програмний засіб для кількісного оцінювання якості систем для виявлення вторгнень, який автоматизує повний цикл експериментів з порівнянням різних методів відбору ознак та ML-моделей на основі відкритих датасетів мережевого трафіку, з подальшим обчисленням інтегрального показника якості та побудовою візуалізацій результатів.

Список літератури:

1. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, Jul. 2019. doi: https://doi.org/10.1186/s42400-019-0038-7.

2. S. Maza and M. Touahria, "Feature Selection Algorithms in Intrusion Detection System: A Survey," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 10, Oct. 2018. doi: https://doi.org/10.3837/tiis.2018.10.024.

3. N. Pudjihartono, T. Fadason, A. W. Kempa-Liehr, and J. M. O'Sullivan, “A Review of Feature Selection Methods for Machine Learning-Based Disease Risk Prediction,” *Frontiers in Bioinformatics*, vol. 2, Jun. 2022. doi: https://doi.org/10.3389/fbinf.2022.927312.

4. H. Abubaker, F. Muchtar, A. R. Khairuddin, A. N. A. Nuar, Z. M. Yunos, and C. Salimun, “Exploring Important Factors in Predicting Heart Disease Based on Ensemble- Extra Feature Selection Approach,” *Baghdad Science Journal*, vol. 21, no. 2(SI), p. 0812, Feb. 2024. doi: https://doi.org/10.21123/bsj.2024.9711.

5. S. M. Kasongo and Y. Sun, “Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset,” *Journal of Big Data*, vol. 7, no. 1, Nov. 2020. doi: https://doi.org/10.1186/s40537-020-00379-6.

6. H. Zouhri, A. Idri, and A. Ratnani, “Evaluating the impact of filter-based feature selection in intrusion detection systems,” *International Journal of Information Security*, vol. 23, pp. 759–785. Oct. 2023. doi: https://doi.org/10.1007/s10207-023-00767-y.

7. B. Reis, E. Maia, and I. Praça, “Selection and Performance Analysis of CICIDS2017 Features Importance,” in *Foundations and Practice of Security*. Cham: Springer Int. Publishing, 2020, pp. 56–71. doi: https://doi.org/10.1007/978-3-030-45371-8_4.

8. Y. Yin *et al.*, “IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset,” *Journal of Big Data*, vol. 10, no. 1, Feb. 2023. doi: https://doi.org/10.1186/s40537-023-00694-8.

9. Canadian Institute for Cybersecurity, *Intrusion Detection Evaluation Dataset (CICIDS2017)*, University of New Brunswick, 2018. [Online]. URL: https://www.unb.ca/cic/datasets/ids-2017.html (accessed: Sep. 25, 2025).

10.ДСТУ ISO/IEC 25010:2016. *Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Моделі якості системи та програмних засобів*, 2016.

Надійшла до редколегії 14.11.2025

Відомості про авторів:

Савка Іван Ярославович – кандидат фіз.-мат. наук, старший викладач кафедри інформаційних технологій, Карпатський національний університет імені Василя Стефаника / Vasyl Stefanyk Carpathian National University, Україна; email: ivan.savka@cnu.edu.ua; ORCID: https://orcid.org/0000-0002-3442-5547

Дутчак Марія Степанівна – викладач кафедри інформаційних технологій Карпатський національний університет імені Василя Стефаника / Vasyl Stefanyk Carpathian National University, Україна; email: mariia.dutchak@cnu.edu.ua; ORCID: https://orcid.org/0000-0002-3337-5613

Коваль Олег Тарасович – магістрант кафедри інформаційних технологій, Карпатський національний університет імені Василя Стефаника / Vasyl Stefanyk Carpathian National University, Україна; email: oleh.koval.20@pnu.edu.ua