https://doi.org/10.31891/2307-5732-2025-349-82
УДК 004.056.5

ПЕТЛЯК НАТАЛІЯ
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua

ГІБРИДНИЙ МЕТОД ТА СИСТЕМА ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

У статті запропоновано гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах (ІКС), що поєднує сигнатурний аналіз, метод на основі самоподібності та нечіткий метод. Реалізація методу виконана на базі модульної архітектури системи Snort 3 з використанням власного програмного модуля, що інтегрує зовнішню бібліотеку аналізу трафіку. Запропонований підхід дозволяє підвищити достовірність виявлення загроз за рахунок комплексної оцінки ризиків та адаптації до змін у мережевому середовищі. Проведено багаторівневе тестування системи в умовах лабораторного та реального трафіку. За результатами експериментів доведено переваги гібридного методу в порівнянні з традиційними системами виявлення (Snort, Suricata) за ключовими метриками якості: точність, повнота, специфічність та F1-міра. Окремо проаналізовано вплив реалізованої системи на ресурсне навантаження ІКС. Показано, що використання гібридного методу забезпечує ефективне виявлення атак при нижчому завантаженні процесора, що підвищує стійкість та масштабованість мережевої інфраструктури.

Ключові слова: гібридний метод, виявлення аномального трафіку, інформаційно-комунікаційна система, Snort 3, самоподібність, нечітка логіка, сигнатурний аналіз, аналіз трафіку.

PETLIAK NATALIIA
Khmelnytskyi National University

HYBRID METHOD AND SYSTEM FOR DETECTING ABNORMAL TRAFFIC IN INFORMATION AND COMMUNICATION SYSTEMS

The article presents the implementation and assessment of the reliability of a hybrid method for detecting anomalous traffic in information and communication systems (ICS), which combines classical approaches to signature-based detection with a self-similarity-based method and a fuzzy method. The purpose of the study is to increase the reliability of detecting attacks in a network environment with dynamically changing traffic parameters, reduce the number of false positives, and ensure the rational use of computing resources. The proposed approach is based on the use of Snort 3, an open-source platform for detecting and preventing intrusions that has a modular architecture and supports multi-threaded processing. Based on the Snort 3 API, a separate module has been developed that performs a full cycle of network traffic analysis: capture, decoding, classification, risk assessment, and decision-making. The system implements three complementary components: signature detection, traffic classification by self-similarity, and fuzzy risk assessment. The key innovation is the use of the Hurst metric to detect long-term dependencies in time series, which allows for effective identification of atypical or hidden activity, including zero-day attacks. To verify the system's performance, a large-scale test environment was created with two isolated subnets, traffic generators, port mirroring, and a server platform emulating the ICS. A dataset of over 5.4 million records was collected with clear labeling of normal and abnormal traffic. In addition to laboratory modeling, testing was performed in real-world network operation conditions, which allowed taking into account the impact of background noise, extraneous activity, and traffic variability. To evaluate the results, commonly used metrics were used - TP, FP, TN, FN, as well as derived indicators: Precision, Recall, Accuracy, Specificity, and F1-measure. A comparative analysis of the effectiveness of the developed system with traditional solutions - the original Snort and the Suricata system - was conducted. According to all metrics, the hybrid model demonstrated higher attack detection reliability, better ability to distinguish between anomalous and normal traffic, as well as a lower level of type II errors. In particular, in laboratory conditions, Accuracy was achieved - 99.12%, Precision - 99.44%, Recall - 99.62%, F1-score - 99.53%. In real traffic conditions, accuracy remained high, and the average processor load when using the hybrid system was the lowest among the tested solutions - 40.5%. The results obtained indicate the prospects of the hybrid approach in the context of the development of new generation cyber defense systems. The proposed model demonstrates the ability to flexibly scale, effectively adapt to changes in the environment, and a high level of detection reliability without excessive load on the infrastructure. In practical terms, the development can be used as a standalone system or as a module in complex solutions for detecting and countering intrusions in the ICS.

Keywords: hybrid method, anomalous traffic detection, information and communication system, Snort 3, self-similarity, fuzzy logic, signature analysis, traffic analysis.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Стрімкий розвиток інформаційно-комунікаційних систем (ІКС), розширення цифрових інфраструктур, зростання обсягів даних, що передаються мережею, а також підвищення складності й інтенсивності кіберзагроз висувають нові вимоги до систем виявлення аномального трафіку. Сучасні засоби захисту повинні не лише фіксувати відомі типи атак, але й адаптивно реагувати на невідомі, нестандартні або модифіковані загрози, зокрема атаки нульового дня, внутрішні порушення політик доступу, витоки даних та приховані форми зловмисної активності. У той же час, на практиці більшість систем виявлення вторгнень, що базуються виключно на сигнатурному аналізі, демонструють обмежені можливості у виявленні нових загроз або тих, що маскуються під легітимний трафік. Їхня ефективність суттєво знижується в умовах динамічного, насиченого середовища з великою кількістю фонових з'єднань. Крім того, такі системи часто створюють надмірне навантаження на обчислювальні ресурси та генерують велику кількість хибнопозитивних спрацювань, що ускладнює роботу аналітиків і знижує оперативність реагування.

З іншого боку, методи поведінкової аналітики та інтелектуального аналізу даних, хоч і демонструють високу здатність до виявлення нетипових шаблонів, потребують високої обчислювальної потужності та складного навчання. Тому актуальним є пошук комбінованих підходів, які б об'єднували переваги сигнатурного, поведінкового та статистичного аналізу, дозволяючи підвищити точність, достовірність і адаптивність систем виявлення загроз.

Аналіз досліджень та публікацій

Aklil Kiflay та колеги [1] запропонували мультимодальну систему виявлення мережевих вторгнень з використанням машинного навчання. Вона об'єднує аналіз мережевого потоку та вмісту пакетів, використовуючи дві моделі Random Forest. Система базується на soft voting для об'єднання результатів та тестувалася на наборі UNSW-NB15, досягаючи точності 98-99%. Хоча вона має обмежену масштабованість, система показує низький рівень хибнопозитивних спрацювань та гнучке налаштування.

Метод SPAFIS, представлений в [2], дозволяє адаптуватися до нових даних у режимі реального часу. Він базується на нечіткій логіці та створює правила типу IF-THEN на основі потоків трафіку. Система має здатність автономно оновлювати свої прототипи, підвищуючи ефективність та прозорість. Підтримується аналіз потоків у режимі онлайн, а вплив на продуктивність залишається низьким.

Гібридна система [3] поєднує алгоритм C5 Decision Tree та LSTM для виявлення як відомих, так і нових атак. Особливість полягає в самовідновленні бази сигнатур, що дозволяє оновлювати правила автоматично. Система здатна працювати з великими обсягами даних у реальному часі, формуючи звіти про свою роботу. Виявляються такі атаки як DoS, експлойти, бекдори, зі зниженим рівнем хибних спрацювань.

Робота [4] акцентує увагу на виявленні атак нульового дня з використанням методу машинного навчання. Для цього застосовуються підходи на основі закону Бенфорда, які дозволяють виявляти аномальні параметри трафіку. Пропонуються напівавтоматичні моделі, що адаптуються до обмежених даних. Завдяки цьому система знижує хибнопозитивні спрацьовування та забезпечує інтеграцію з різними середовищами.

Дослідження Mahmoud Said El Sayed [5] зосереджено на боротьбі з DDoS-атаками у SDN-мережах. Впроваджено глибоке навчання разом із вибором ознак через Information Gain і Random Forest. Система адаптується до різних обсягів трафіку та дозволяє формувати гнучкі звіти для адміністраторів. Результати тестування на кількох датасетах підтверджують її ефективність і сумісність із безпековими рішеннями.

У [6] описується система, яка поєднує сигнатурний та аномальний підходи у триетапній моделі. Спочатку використовується набір правил, потім глибока нейромережа ResNet50, після чого результати об'єднуються. Це дозволяє виявляти як відомі, так і нові атаки, з високою точністю в понад 98%. Гнучке налаштування та сумісність з ОС роблять систему придатною для широкого впровадження.

Sivasankari Nitiynandan [7] досліджує способи протидії атакам типу "людина посередині" в IoT-мережах. Для цього застосовуються три регресійні моделі, з яких найефективнішою є GPR. Вона дозволяє вузлам самостійно визначати безпечний маршрут без централізованого контролера. Система легко налаштовується та ефективно масштабується.

Робота [8] описує гібридну систему, яка поєднує нечітку логіку, нейронні мережі та генетичні алгоритми. Завдяки цьому забезпечується висока точність виявлення та стабільність у великих мережах. Система класифікує вхідний трафік у реальному часі та швидко реагує на нові загрози. Вона має гнучке налаштування та підтримує інтеграцію з іншими системами безпеки.

У дослідженні Радівілової [9] аналізуються статистичні методи виявлення аномалій у телекомунікаційних мережах. Випробувано кілька підходів, з яких найточнішим виявилося дерево рішень. Незважаючи на складність налаштувань, метод забезпечує точність 96% при аналізі понад трьох мільйонів пакетів. Атаки, що досліджувались, включають DDoS, ARP flood та HTTP flood.

Система [10] об'єднує LSTM і нечітку логіку для виявлення відхилень у поведінці мережевого трафіку. Для цього використовується створення цифрового підпису потоків і встановлення порогів нормальності за допомогою математичних методів. Завдяки динамічному керуванню потоками система блокує або перенаправляє загрозливий трафік. Це гарантує стабільність навіть під час активних атак.

Метод, описаний у [11], базується на машинному навчанні для класифікації зашифрованого трафіку. Найкращі результати демонструє алгоритм випадкових лісів, з точністю понад 87%. Метод не аналізує глибоко пакети, що зменшує ризики порушення конфіденційності. Однак він не справляється з UDP-трафіком та невідомими інструментами.

У FuzHD++ [12] поєднано заповнення відсутніх даних і виявлення аномальних вузлів у IoT. Метод використовує профіль матриці та алгоритм найближчих сусідів. Нечіткі правила дозволяють точно визначати відхилення у поведінці вузлів. Хоча точність висока, метод обмежений у виявленні деяких типів атак.

Liangchen Chen [13] пропонує кластеризаційний метод DPC-GS-MND для виявлення аномалій. Він використовує пікову щільність і взаємний ступінь сусідства для автоматичного визначення центрів кластерів. Метод демонструє високу точність і низькі витрати, але потребує ручного налаштування параметрів. Це ускладнює його адаптацію до різних умов.

Метод у [14] базується на поєднанні найменших квадратів та ентропійного аналізу часових вікон. Оптимізація моделі дозволяє досягати розрідженості та зменшити перенавчання. Система визначає джерело аномалії через зворотній аналіз поведінки. Вона показала хороші результати, хоч і потребує значних ресурсів.

Метод [15] використовує адаптивне прогнозування для аналізу поведінки мережевого трафіку. Комбінація згладжувальних методів дозволяє реагувати на сезонні зміни. Система ефективна для IoT-пристроїв завдяки низьким вимогам до ресурсів. Потрібне точне налаштування, що вимагає додаткових зусиль.

Шпінарева та співавтори [16] створили каскадну модель глибоких нейромереж для виявлення та класифікації атак. Використовується гібрид CNN-LSTM для виявлення, а далі CNN для визначення типу атаки. Метод протестовано на реальних даних, що доводить його ефективність. Проте аналіз великих обсягів даних у реальному часі є складним завданням.

У [17] описується гібридна система для боротьби із Zero-Day загрозами, яка поєднує мультисканер, sandbox та модуль автоматичного аналізу. Система інтегрується з антивірусами та створює унікальні правила для виявлення аномалій. Вона вимагає значних ресурсів і складна в налаштуванні. Обмеження Yara-правил також впливають на її загальну ефективність.

У роботі [18] пропонується централізована розподілена система на базі мультифрактального аналізу. Вона використовує вейвлет-перетворення та коефіцієнт Херста для виявлення самоподібності трафіку. Такий підхід дозволяє відрізнити нормальний трафік від шкідливого навіть за їх схожості. Основні обмеження пов'язані з кількістю даних та необхідністю повторного налаштування параметрів

Попри високі показники точності, сучасні системи виявлення мережевих загроз мають низку обмежень, зокрема значні обчислювальні витрати та складність налаштування. Обмежена здатність деяких методів до виявлення нових атак, а також високий рівень хибнопозитивних спрацювань створюють додаткові виклики для адміністраторів. Це підкреслює необхідність подальшого пошуку інноваційних, масштабованих і ресурсоефективних рішень, здатних адаптуватися до динаміки сучасного кіберпростору.

Формулювання цілей статті

Метою роботи є: реалізація та експериментальна перевірка достовірності гібридного методу виявлення аномального трафіку в ІКС, що поєднує сигнатурний аналіз, поведінкові підходи на основі самоподібності та механізми нечіткої логіки, з метою підвищення точності і достовірності виявлення мережевих загроз в умовах динамічного середовища при одночасній оптимізації ресурсного навантаження на інфраструктуру.

Виклад основного матеріалу

Одним із ефективних підходів у цьому напрямку є розробка гібридних методів виявлення, які поєднують у собі переваги різних методів для оцінювання рівня загроз. Запропонований метод базується на інтеграції сигнатурного аналізу, методів поведінкової аналітики, зокрема аналізу самоподібності, а також нечіткої логіки у єдину архітектуру, реалізовану за допомогою системи виявлення та запобігання вторгненням Snort 3 — популярної системи виявлення та запобігання вторгнень з відкритим кодом, що підтримує модульну архітектуру і багатопотокову обробку трафіку.

Snort 3 обрано як основу для реалізації, з огляду на його гнучкість, можливість розширення функціоналу через власні модулі та широке ком’юніті підтримки. На відміну від попередніх версій, Snort 3 дозволяє ефективно масштабувати систему, реалізовувати складні алгоритми аналізу безпосередньо у структурі препроцесорів, а також інтегрувати сторонні бібліотеки. Архітектура Snort включає чотири основні компоненти: модуль захоплення трафіку (сніфер), препроцесор, механізм виявлення загроз та модуль виводу (логування та реагування). Кожен із них виконує окрему, але тісно взаємопов’язану функцію в загальному процесі виявлення загроз. Потік трафіку між компонентами оптимізовано для обробки в реальному часі та забезпечення мінімальної затримки при ухваленні рішень щодо безпечності трафіку.

На етапі реалізації запропонованого гібридного методу було створено окремий модуль на основі API Snort 3, який виконує обробку трафіку з використанням внутрішніх механізмів системи та зовнішньої спеціалізованої бібліотеки. Цей модуль реалізує повний цикл аналізу – від ініціалізації параметрів обробки до прийняття рішень та генерації сповіщень. Основним завданням модуля є інтеграція даних, отриманих у результаті сигнатурного аналізу, з результатами поведінкового аналізу та нечіткого оцінювання ризиків. Зокрема, при захопленні трафіку за допомогою бібліотеки libpcap виконується перехоплення всіх пакетів, що проходять через обраний мережевий інтерфейс у режимі перехоплення (promiscuous mode). Далі, препроцесори Snort, зокрема frag3, stream5, http_inspect, здійснюють попередню обробку трафіку: дефрагментацію, рекомпозицію сесій, нормалізацію заголовків протоколів, що значно знижує ризик обходу системи зловмисними фрагментами.

У рамках реалізації гібридного методу в модулі передбачено окрему підсистему класифікації трафіку на основі самоподібності. Цей підхід полягає у створенні моделей нормальної поведінки користувачів, пристроїв або підсистем, та порівнянні поточних характеристик трафіку з цими моделями. У випадку виявлення значущих відхилень, що не відповідають типовим патернам, трафік маркується як потенційно аномальний. Даний метод є надзвичайно ефективним для виявлення атак нульового дня, які

не мають відомих сигнатур, але порушують правила поведінки в мережевому середовищі. Для підвищення точності класифікації застосовано функціонал динамічного оновлення моделей на основі постійного зворотного зв'язку з підсистемами логування.

Рис. 1. Алгоритм роботи Snort із використанням гібридного методу виявлення аномального трафіку в ІКС

Наступним елементом запропонованого методу є використання нечіткої логіки (НЛ) для інтегрованої оцінки ризику. Нечітка логіка дозволяє враховувати множину факторів, які не мають чітких порогових значень, проте мають суттєвий вплив на оцінку небезпеки. У рамках розробленої системи було сформовано базу правил нечіткої логіки, яка охоплює такі параметри, як швидкість передачі пакетів, частота спроб встановлення з'єднань, кількість одночасно активних сесій, співвідношення між вхідним та вихідним трафіком, відповідність сигнатурам тощо. Результатом обчислення є інтегрований ризиковий індекс, який використовується підсистемою логічного виведення для остаточного рішення: допустити трафік, згенерувати попередження або активувати механізм блокування.

Система логічного виведення функціонує на основі узагальненої оцінки, що поєднує результати сигнатурного аналізу, класифікації за самоподібністю та НЛ-оцінки. Особливу увагу приділено аналізу вихідного трафіку, як джерела потенційного витоку конфіденційної інформації або ознаки компрометації внутрішніх вузлів ІКС. Впроваджено механізми виявлення підозрілої активності, зокрема нестандартних портів, зовнішніх з'єднань у неробочий час, нетипових протоколів тощо.

Оцінка достовірності розробленого гібридного методу виявлення аномального трафіку є етапом верифікації його достовірності в умовах як лабораторного, так і реального мережевого середовища. Для забезпечення об'єктивності дослідження було сформовано тестове середовище з двома ізольованими локальними мережами, в яких імітувався як типовий дозволений трафік, так і аномальна поведінка, зокрема сканування, активна розвідка, спроби атак та несанкціоновані з'єднання. Збір даних виконувався за допомогою Snort. У результаті попереднього етапу було сформовано вибірку обсягом понад 1,48 млн записів, кожен з яких маркувався як нормальний або аномальний, відповідно до попередньо визначених правил класифікації.

Було застосовано загальновизнані метрики, а саме: True Positive (TP) — кількість коректно ідентифікованих аномальних записів, False Positive (FP) — хибнопозитивні результати, коли нормальний трафік помилково класифікується як аномальний, True Negative (TN) — кількість коректно ідентифікованих нормальних записів, False Negative (FN) — аномалії, які система не змогла виявити. Для оцінки якості класифікації додатково обчислювалися такі метрики: точність (Precision), повнота (Recall), акуратність (Accuracy), специфічність (Specificity) та F1-міра (F1-score) — збалансований показник, що враховує як Precision, так і Recall.

$$Recall = \frac{TP}{TP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (3)$$

$$Specificity = \frac{FP+FN}{TP+FP+TN+FN} \quad (4)$$

$$F1\ score = \frac{Recall+Precision}{2} \quad (5)$$

Тестування здійснювалося в два етапи: в умовах ізольованого лабораторного середовища та в умовах функціонування реального мережевого трафіку. У першому випадку використовувався попередньо сформований датасет обсягом понад 5,4 млн записів, з яких близько 307 тис. становили аномальні події. Гібридна система показала високу продуктивність: TP — 5141567, FN — 19418, FP — 28739, TN — 278933. Для порівняння, оригінальний Snort 3 мав значно гірші показники: TP — 5027861, FN — 133124, FP — 46235, TN — 261437. Система Suricata, яка часто застосовується як альтернатива, показала проміжні результати між гібридним Snort та його базовою версією.

Розрахунок підтверджує перевагу запропонованого підходу. Так, у лабораторному середовищі Accuracy гібридної системи становила 99.12%, що вищий за 96.72% у базового Snort і 97.53% у Suricata. Precision для гібридного модуля дорівнював 99.44%, що також є найвищим серед усіх систем. Показник Recall — 99.62%, вказує на здатність системи виявляти більшість аномальних подій. У свою чергу, F1-score, що об'єднує точність і повноту, становив 99.53%, проти 98.25% у Snort та 98.68% у Suricata. Отримані результати засвідчують не лише підвищену достовірність виявлення, а й значне зниження

кількості хибнопозитивних спрацювань, що є критично важливим для зменшення навантаження на аналітиків безпеки.

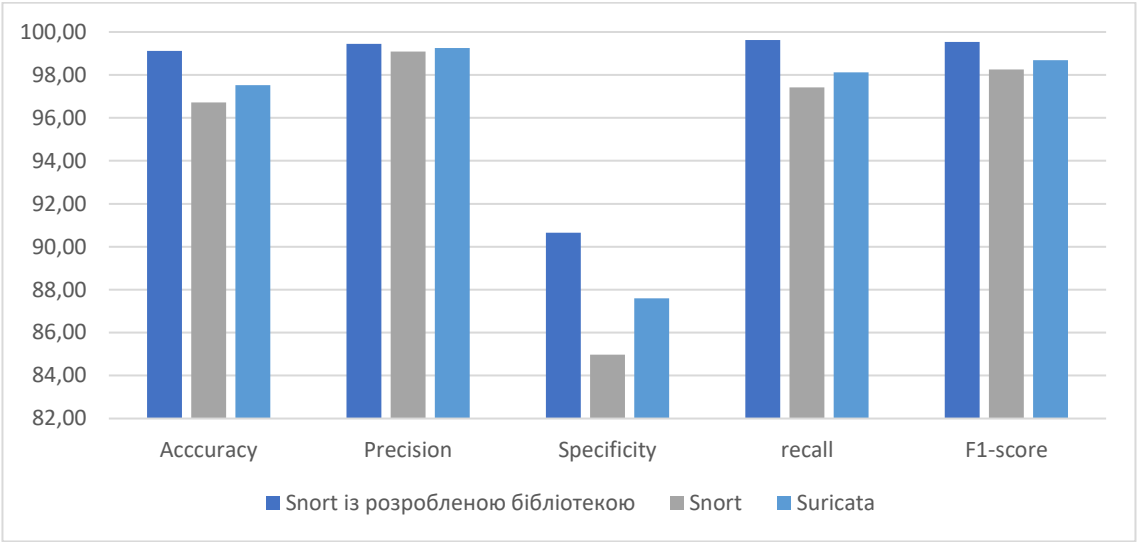

Рис. 2. Діаграма характеристик оцінки достовірності при використанні набору даних

У другому етапі було проведено тестування в умовах реального мережевого середовища, де спостерігалася природна варіативність трафіку, фоновий шум та вплив сторонніх процесів. Тут сукупна вибірка становила 1487888 записів, із яких понад 181 тис. — аномальні. За цих умов гібридний Snort продемонстрував наступні результати: TP — 1284963, FN — 21786, FP — 17514, TN — 163625. Значення Accuracy склало 97.36%, Precision — 98.66%, Recall — 98.33%, Specificity — 90.33%, а F1-score — 98.49%. У цьому тесті було зафіксовано зниження результатів у всіх системах, що є очікуваним через більшу складність аналізу реального трафіку, однак гібридний метод показав кращий результат.

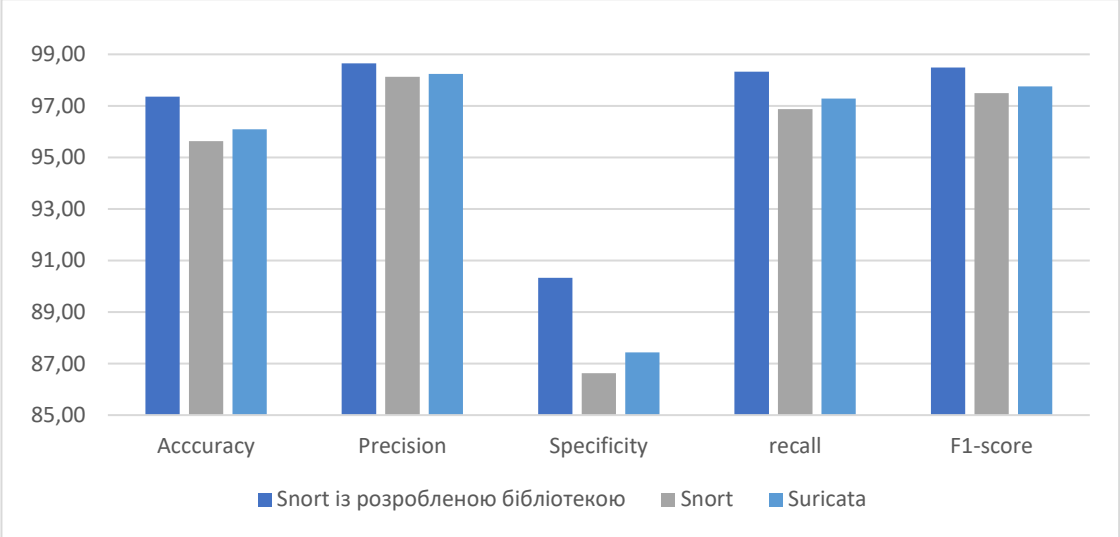

Рис. 3. Діаграма характеристик оцінки достовірності в режимі реального часу

Порівняльний аналіз із іншими системами підтверджує, що в умовах реального трафіку гібридна система переважає за всіма метриками. Так, для оригінального Snort Accuracy становила 95.63%, Precision — 98.12%, Recall — 96.88%, а F1-score — 97.50%. У Suricata ці ж показники склали відповідно 96.09%, 98.24%, 97.29% і 97.76%. Специфічність у всіх систем залишалася на рівні понад 86%, однак саме гібридний модуль демонстрував стабільно вищу здатність розрізняти нормальний і аномальний трафік, що свідчить про зниження кількості помилок другого роду (FN).

Важливо відзначити, що покращення якості виявлення забезпечується саме завдяки поєднанню методів сигнатурного аналізу, аналізу самоподібності та нечіткої оцінки параметрів трафіку. Така синергія дозволяє не лише фіксувати вже відомі шаблони атак, а й динамічно ідентифікувати невідомі загрози, які виходять за межі звичних профілів поведінки. Використання міри Херста як одного з параметрів дозволяє виявляти персистентні тенденції у зміні трафіку, що може вказувати на тривалі або приховані атаки, які не викликають спрацювань у традиційних сигнатурних системах.

Таким чином, результати тестування демонструють високу достовірність, точність та стійкість гібридного методу до флуктуацій реального мережевого трафіку. Запропонований підхід дозволяє

досягти кращої збалансованості між високою чутливістю (виявлення аномалій) і специфічністю (розпізнавання нормального трафіку), що є важливим для практичного впровадження в умовах ІКС. Отже, гібридна модель не лише розширює можливості традиційних систем виявлення, але й може бути основою для побудови адаптивних кіберзахисних комплексів нового покоління, здатних ефективно протидіяти сучасним загрозам у динамічному мережевому середовищі.

Оцінка впливу гібридного методу виявлення аномального трафіку в ІКС є важливим аспектом для визначення його практичної цінності, рівня ресурсної ефективності та здатності до інтеграції у складні мережеві архітектури. Для цього було реалізовано тестове середовище, що моделює типовий сегмент корпоративної мережі, до складу якого увійшли сервери (використані як платформи аналізу і жертви атак), маршрутизатор із функцією дзеркалювання порту (порт SPAN), а також вузли генерації трафіку. Вся система функціонувала у контрольованих умовах із навантаженням, близьким до реального — близько 200 Мб/с штатного трафіку, з імітацією кількох типів атак.

У ході експериментів проводилося покрокове тестування роботи трьох систем — базової Snort, системи Suricata та розробленого гібридного методу — з фіксацією як показників продуктивності (CPU-навантаження), так і факту виявлення або пропуску атак. Структура тестування передбачала чотири окремі сценарії: (1) вивантаження великих файлів на зовнішні ресурси на швидкості до 1 Гб/с тривалістю 1,5 с, (2) атака типу "підбір паролю" на зовнішній ресурс із трафіком 0,5 Гб/с протягом 1 с, (3) сканування портів із трафіком 0,7 Гб/с протягом 1,3 с, і (4) розсилка повідомлень через месенджери з інтенсивністю 0,3 Гб/с на 2,6 с. Кожен експеримент дозволяв оцінити не лише якість виявлення, а й реакцію системи на зміну навантаження.

$$\overline{CPU} = \frac{\sum_{i=1}^{n-1} CPU_i * (t_{i+1} - t_i)}{\sum_{i=1}^{n-1} (t_{i+1} - t_i)}, \quad (6)$$

де CPU_i - завантаження процесора на часовому інтервалі; $\overline{CPU}$ - середнє значення завантаження процесора за обраний проміжок часу. Воно не є простою арифметичною середньою, а зваженою середньою, яка враховує тривалість кожного інтервалу; t_i та t_{i+1} - послідовні моменти часу, в які проводились вимірювання; $t_{i+1} - t_i$ - це тривалість інтервалу, протягом якого фіксувалося певне навантаження.

У першому етапі тестування результати було отримано за допомогою системи Snort без додаткових модулів. Як видно з часових діаграм трафіку та графіка навантаження на процесор, система зафіксувала лише одну з трьох атак. При цьому навантаження на процесор залишалося стабільно високим і не знижувалося навіть після успішного виявлення загрози. Середнє значення CPU-завантаження становило 42,5%, що є помірним показником, однак з огляду на невисоку ефективність виявлення атак, свідчить про нераціональне використання обчислювальних ресурсів. Це особливо важливо в умовах інтенсивного трафіку, де кожен відсоток продуктивності має критичне значення для швидкого реагування.

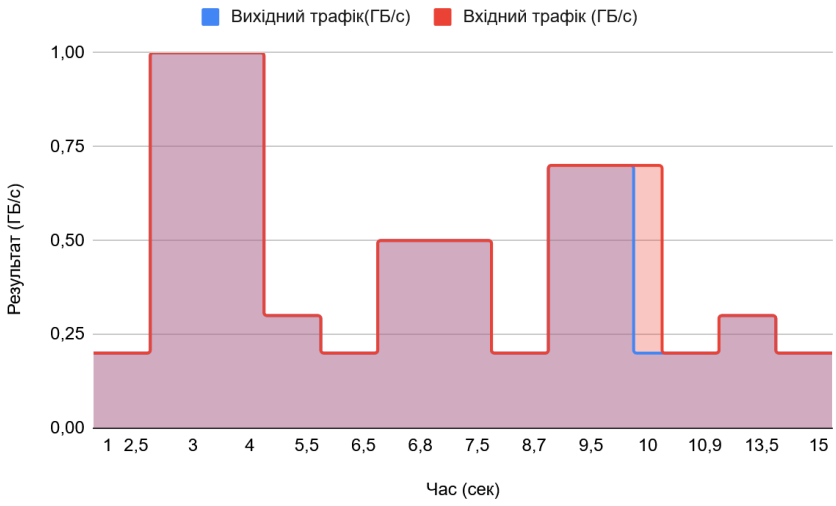

Рис. 4. Вихідний трафік з використанням SNORT

Аналіз із використанням системи Suricata продемонстрував дещо кращі результати. Було успішно виявлено дві з трьох атак, при цьому після виявлення другої атаки частково знизилося навантаження на процесор. Середнє значення CPU-навантаження склало 50,5%, що свідчить про відносно високу інтенсивність споживання ресурсів. Попри підвищену достовірність виявлення у порівнянні зі Snort, система Suricata вимагала більше обчислювальних потужностей, що може бути обмеженням у розподілених або ресурсно обмежених мережах.

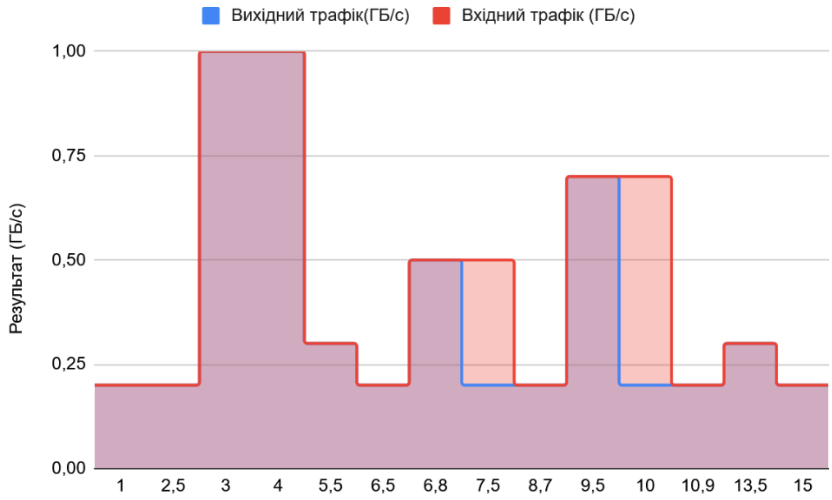

Рис. 5. Вихідний трафік з використанням Suricata

Третій варіант експерименту — використання розробленої гібридної системи — продемонстрував найкращі результати за співвідношенням між виявленими атаками та використаними ресурсами. Було виявлено дві з трьох атак, аналогічно до Suricata, однак після виявлення аномальної активності система автоматично знижувала навантаження на процесор, навіть при збереженні високої пропускної здатності трафіку. Середнє завантаження CPU становило 40,5%, що є найнижчим серед усіх досліджуваних систем. Така поведінка свідчить про ефективне керування потоками даних та адаптивне балансування навантаження відповідно до поточного стану трафіку.

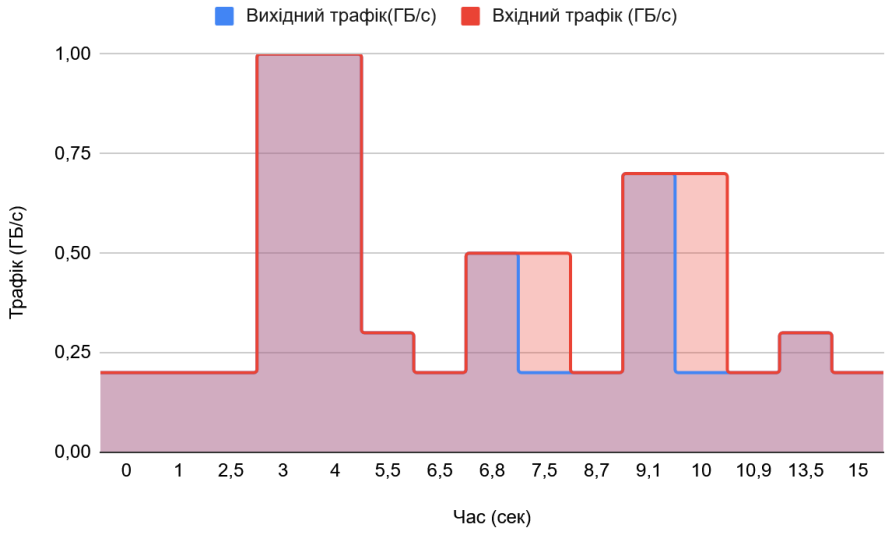

Рис. 6. Вихідний трафік з використанням власної системи

Загалом, згідно з результатами аналізу, можна зробити висновок, що застосування гібридного методу має низку переваг. По-перше, розроблена система не тільки дозволяє виявляти широкий спектр атак, а й робить це з меншими витратами ресурсів, у порівнянні з аналогами. По-друге, вона демонструє адаптивність до змін у трафіку, що підтверджується зниженням CPU-навантаження після успішної ідентифікації загроз. По-третє, система здатна працювати в реальному часі навіть у складних мережевих умовах без втрати продуктивності, що є критичним для ІКС із високим рівнем навантаження або з обмеженою доступністю до обчислювальних потужностей.

Особливо важливою є здатність системи реагувати на навантаження залежно від виявлених подій. Завдяки зваженому розрахунку середнього навантаження процесора (формула 6), система враховує часові інтервали та динаміку зміни інтенсивності навантаження. Це забезпечує реалістичну оцінку ефективності в різні моменти роботи, на відміну від традиційного обчислення простої середньої. У цьому контексті доцільним є висновок про інтелектуальний розподіл навантаження — після ідентифікації певного типу аномалії система переорієнтовує ресурси, зменшуючи пріоритет на потік, що вже класифіковано, та підвищуючи контроль за новими потенційними джерелами загроз.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

У контексті загального впливу на ІКС можна стверджувати, що гібридний метод забезпечує не лише високу точність виявлення, а й сприятливий вплив на стабільність функціонування всієї системи. Зниження навантаження після виявлення загроз дозволяє зменшити ризик перевантаження центрального вузла обробки даних або серверного обладнання. У перспективі це відкриває можливості масштабування системи без необхідності суттєвого розширення апаратної бази, що є вагомим аргументом на користь її впровадження у корпоративних мережах, а також у критично важливих інфраструктурах, де надійність і стабільність роботи систем безпеки є пріоритетом.

Література

1. Kiflay A., Tsokanos A., Fazlali M., Kirner R. (2024). Network intrusion detection leveraging multimodal features. Array, 22, 100349. doi: 10.1016/j.array.2024.100349.
2. Gu X., Howells G., Yuan H. (2024). A soft prototype-based autonomous fuzzy inference system for network intrusion detection. Information Sciences, 677, 120964. doi: 10.1016/j.ins.2024.120964.
3. S. Kushal, B. Shanmugam, J. Sundaram et al. (2024). Self-healing hybrid intrusion detection system: an ensemble machine learning approach. Discover Artificial Intelligence 4, 28. doi: 10.1007/s44163-024-00120-9.
4. I. Mbona, J. H. P. Eloff. (2022). Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches. IEEE Access, 10, 69822-69838. doi: 10.1109/ACCESS.2022.3187116.
5. M. S. E. Sayed, N. -A. Le-Khac, M. A. Azer and A. D. Jurcut. (2022). A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs. IEEE Transactions on Cognitive Communications and Networking, 8, 4, 1862-1880. doi: 10.1109/TCCN.2022.3186331.
6. Shaikh A., Gupta P. (2023). Advanced Signature-Based Intrusion Detection System. In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, 131. Springer, Singapore. doi: 10.1007/978-981-19-1844-5_24.
7. N. Sivasankari and S. Kamalakkannan. (2022). Detection and prevention of man-in-the-middle attack in iot network using regression modeling, Advances in Engineering Software, 169, 103126. doi: 10.1016/j.advengsoft.2022.103126.
8. Mohammed Ishaque, Md Gapar Md Johar, Ali Khatibi, Muhammed Yamin. (2023). A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system, Measurement: Sensors, 30, 100933. doi: 10.1016/j.measen.2023.100933.
9. Radivilova T., Kirichenko L., Tawalbeh M., Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 183–194. doi: 10.28925/2663-4023.2021.11.183194.
10. M. P. Novaes, L. F. Carvalho, J. Lloret and M. L. Proença. (2020). Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment. IEEE Access, 8, 83765-83781. doi: 10.1109/ACCESS.2020.2992044.
11. Daniele Canavese, Leonardo Regano, Cataldo Basile, Gabriele Ciravegna, Antonio Lioy. (2022). Encryption-agnostic classifiers of traffic originators and their application to anomaly detection. Computers & Electrical Engineering, 97, 107621, doi: 10.1016/j.compeleceng.2021.107621.
12. N. Berjab, H. H. Le and H. Yokota. (2022). Recovering Missing Data via Top-k Repeated Patterns for Fuzzy-Based Abnormal Node Detection in Sensor Networks. IEEE Access, 10, 61046-61064, doi: 10.1109/ACCESS.2022.3181742.
13. Chen L., Gao S., Liu, B. (2022). An improved density peaks clustering algorithm based on grid screening and mutual neighborhood degree for network anomaly detection. Scientific Reports 12, 1409. doi: 10.1038/s41598-021-02038-z.
14. Jing Zhang, Yige Yuan, Jiahong Zhang, Yang Yang, Wenjin Xie. (2023). Anomaly detection method based on penalty least squares algorithm and time window entropy for Cyber–Physical Systems. Journal of King Saud University - Computer and Information Sciences, 35(10), 101860, doi: 10.1016/j.jksuci.2023.101860.
15. Mariusz Pelc, Dawid Galus, Magda Zolubak, Stepan Ozana, Wojciech Chlewicki, Katarzyna Cichon, Michal Podpora, Aleksandra Kawala-Sterniuk. (2019). Behavioural Approach to Network Anomaly Detection for Resource-Constrained System – Presentation of the Novel Solution – Preliminary Study. IFAC-PapersOnLine, 52(27), 121-126. doi: 10.1016/j.ifacol.2019.12.743.
16. Шпінарева І. М., Якушина А. О., Волощук Л. А., Рудніченко М. Д. (2021). Використання методів поглиблених навчання для виявлення і класифікації мережевих атак. Вісник сучасних інформаційних технологій, 4(3), 244-254. doi: 10.15276/hait.03.2021.4.
17. Саприкін О.С. (2021). Моделі і методи діагностування Zero-Day загроз в кіберпросторі. Вісник сучасних інформаційних технологій, 4(2), 155-167. doi: 10.15276/hait.02.2021.5.
18. Шагін В., Нічепорук А., Каштальян А. (2021). Централізована розподілена система виявлення атак у корпоративних комп'ютерних мережах на основі мультифрактального аналізу. Measuring and

computing devices in technological processes, (1), 50–55. doi: 10.31891/2219-9365-2021-67-1-7.

References

1. Kiflay A., Tsokanos A., Fazlali M., Kirner R. (2024). Network intrusion detection leveraging multimodal features. Array, 22, 100349. doi: 10.1016/j.array.2024.100349.

2. Gu X., Howells G., Yuan H. (2024). A soft prototype-based autonomous fuzzy inference system for network intrusion detection. Information Sciences, 677, 120964. doi: 10.1016/j.ins.2024.120964.

3. S. Kushal, B. Shanmugam, J. Sundaram et al. (2024). Self-healing hybrid intrusion detection system: an ensemble machine learning approach. Discover Artificial Intelligence 4, 28. doi: 10.1007/s44163-024-00120-9.

4. I. Mbona, J. H. P. Eloff. (2022). Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches. IEEE Access, 10, 69822-69838. doi: 10.1109/ACCESS.2022.3187116.

5. M. S. E. Sayed, N. -A. Le-Khac, M. A. Azer and A. D. Jurcut. (2022). A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs. IEEE Transactions on Cognitive Communications and Networking, 8, 4, 1862-1880. doi: 10.1109/TCCN.2022.3186331.

6. Shaikh A., Gupta P. (2023). Advanced Signature-Based Intrusion Detection System. In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, 131. Springer, Singapore. doi: 10.1007/978-981-19-1844-5_24.

7. N. Sivasankari and S. Kamalakkannan. (2022). Detection and prevention of man-in-the-middle attack in iot network using regression modeling, Advances in Engineering Software, 169, 103126. doi: 10.1016/j.advengsoft.2022.103126.

8. Mohammed Ishaque, Md Gapar Md Johar, Ali Khatibi, Muhammed Yamin. (2023). A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system, Measurement: Sensors, 30, 100933. doi: 10.1016/j.measen.2023.100933.

9. Radivilova T., Kirichenko L., Tawalbeh M., Ilkov, A. (2021). Detection of anomalies in telecommunication traffic using statistical methods. Electronic professional scientific publication "Cybersecurity: education, science, technology", 3(11), 183–194. doi: 10.28925/2663-4023.2021.11.183194.

10. M. P. Novaes, L. F. Carvalho, J. Lloret and M. L. Proença. (2020). Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment. IEEE Access, 8, 83765-83781. doi: 10.1109/ACCESS.2020.2992044.

11. Daniele Canavese, Leonardo Regano, Cataldo Basile, Gabriele Ciravegna, Antonio Lioy. (2022). Encryption-agnostic classifiers of traffic originators and their application to anomaly detection. Computers & Electrical Engineering, 97, 107621, doi: 10.1016/j.compeleceng.2021.107621.

12. N. Berjab, H. H. Le and H. Yokota. (2022). Recovering Missing Data via Top-k Repeated Patterns for Fuzzy-Based Abnormal Node Detection in Sensor Networks. IEEE Access, 10, 61046-61064, doi: 10.1109/ACCESS.2022.3181742.

13. Chen L., Gao S., Liu, B. (2022). An improved density peaks clustering algorithm based on grid screening and mutual neighborhood degree for network anomaly detection. Scientific Reports 12, 1409. doi: 10.1038/s41598-021-02038-z.

14. Jing Zhang, Yige Yuan, Jiahong Zhang, Yang Yang, Wenjin Xie. (2023). Anomaly detection method based on penalty least squares algorithm and time window entropy for Cyber–Physical Systems. Journal of King Saud University - Computer and Information Sciences, 35(10), 101860, doi: 10.1016/j.jksuci.2023.101860.

15. Mariusz Pelc, Dawid Galus, Magda Zolubak, Stepan Ozana, Wojciech Chlewicki, Katarzyna Cichon, Michal Podpora, Aleksandra Kawala-Sterniuk. (2019). Behavioural Approach to Network Anomaly Detection for Resource-Constrained System – Presentation of the Novel Solution – Preliminary Study. IFAC-PapersOnLine, 52(27), 121-126. doi: 10.1016/j.ifacol.2019.12.743.

16. Shpinareva I. M., Yakushina A. O., Voloshchuk L. A., Rudnichenko M. D. (2021). Using deep learning methods to detect and classify network attacks. Bulletin of Modern Information Technologies, 4(3), 244-254. doi: 10.15276/hait.03.2021.4.

17. Saprykin O. S. (2021). Models and methods for diagnosing Zero-Day threats in cyberspace. Bulletin of Modern Information Technologies, 4(2), 155-167. doi: 10.15276/hait.02.2021.5.

18. Shagin V., Nicheporuk A., Kashtalyan A. (2021). Centralized distributed attack detection system in corporate computer networks based on multifractal analysis. Measuring and computing devices in technological processes, (1), 50–55. doi: 10.31891/2219-9365-2021-67-1-7.