УДК 004.732.056
DOI https://doi.org/10.32782/IT/2024-2-4

Павло ГРИНЧЕНКО
аспірант кафедри системного аналізу та обчислювальної математики, Національний університет «Запорізька політехніка», вул. Жуковського 64, м. Запоріжжя, Україна, 69063
***ORCID:** 0000-0002-0347-0265*

Бібліографічний опис статті: Гринченко, П. (2024). Дослідження розроблюваної системи виявлення мережевих атак (СВМА) із використанням МАІ. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 25–33, doi: https://doi.org/10.32782/IT/2024-2-4

ДОСЛІДЖЕННЯ РОЗРОБЛЮВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК (СВМА) ІЗ ВИКОРИСТАННЯМ МАІ

Розвиток комп'ютерних мереж впливає на більшість сфер діяльності людини. Функціонування мереж та інформаційних систем всередині них залежить не лише від надійності використовуваного обладнання, але й від здатності мережі протистояти будь-яким спробам порушити її роботу. З кожним роком мережі стають все більш складними та масштабними. Як наслідок, потреба у вдосконаленні систем виявлення вторгнень, які в першу чергу відповідають за виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів, набуває все більшої актуальності. Постійний стрімкий розвиток методів та засобів деструктивного програмного впливу на інформаційні системи зумовлює необхідність підвищення рівню захисту інформації. Найбільш ефективний спосіб досягнення цієї мети – проведення порівняльного аналізу систем виявлення атак та запобігання вторгненням.

***Наукова новизна** дослідження полягає в визначенні ефективності розроблюваної системи шляхом вирішення задачі багатокритеріального прийняття рішень.*

***Основною метою роботи** є дослідження більш ефективної розроблюваної системи виявлення мережевих атак (надалі СВМА) відносно вже існуючих відкритих систем.*

У роботі виконується декомпозиція задачі прийняття рішень із виділенням головної цілі та альтернатив з використанням методу Саати. Елементи однакових рівнів співставні один з одним з точки зору встановлення пріоритетів. На основі цього будується схема поточного дослідження, основною метою якого є перевірка та підтвердження ефективності розроблюваної системи виявлення мережевих атак серед трьох існуючих альтернатив за шістьма критеріями.

***Результати** проведеного аналізу підтверджують, що розроблювана система є ефективною та актуальною. Вона демонструє переваги у виявленні та реагуванні на мережеві загрози порівняно з розглянутими аналогами.*

***Ключові слова:** система виявлення мережевих атак, безпека мереж, інформаційна безпека.*

Pavlo HRYNCHENKO
Postgraduate Student of the Department of System Analysis and Computational Mathematics, National University «Zaporizhzhia Polytechnic»,64, Zhukovsky Str., Zaporizhzhya, Ukraine, 69063, phrynchenko@ukr.net
***ORCID:** 0000-0002-0347-0265*

To cite this article: Hrynchenko, P. (2024). Doslidzhennia rozrobliuvanoi systemy vyiavlennia merezhevykh atak (SVMA) iz vykorystanniam MAI [Research of the network attacks detection system (NADS) under development using MAI]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2, 25–33, doi: https://doi.org/10.32782/IT/2024-2-4

RESEARCH OF THE NETWORK ATTACKS DETECTION SYSTEM (NADS) UNDER DEVELOPMENT USING MAI

The development of computer networks affects most areas of human activity. The functioning of networks and information systems within them depends not only on the reliability of the equipment used, but also on the ability of the network to withstand any attempts to disrupt its operation. Every year, networks are becoming more complex and large-scale. As a result, the need to improve intrusion detection systems, which are primarily responsible for detecting network attacks, unauthorised access attempts and resource use, is becoming increasingly important. The constant rapid development of methods and influence of destructive software on information systems makes it necessary to increase the level of information protection. The most effective way to achieve this goal is to conduct a comprehensive analysis of attack detection and intrusion prevention systems.

The scientific novelty *of the research consists in determining the efficiency of the developed system by solving the problem of multi-criteria decision-making.*

The main *goal of the work is the study of a more effective network attack detection system under development (hereafter NADS) in comparison with already existing open systems.*

The work decomposes the decision-making task with the selection of the main goal and alternatives. Elements of the same levels are comparable to each other in terms of prioritization.

According to Saati's method, a hierarchy of goals is determined in order to achieve the given task. Based on this, the scheme of the current study is being built, the main purpose of which is to verify and confirm the effectiveness of the developed network attack detection system among three existing alternatives according to six criteria.

The results *of the analysis confirm that the developed system is effective and relevant. It demonstrates advantages in detecting and responding to network threats compared to the considered analogues.*

Key words: *network attack detection system, network security, information security.*

Актуальність поставленої задачі та аналіз останніх досліджень і публікацій. Сьогодні розвиток комп'ютерних мереж впливає на більшість сфер економічної діяльності. Безліч підприємств і організацій у всьому світі покладаються на мережі для оптимізації виробництва, координації персоналу, розподілу ресурсів і надання доступу до інтернету користувачам у віддалених місцях.

Це надає ряд суттєвих переваг – прискорення виробничих процесів, підвищення мобільності і оперативності доступу до інформації та послуг, можливість віддаленого управління рахунками, замовленням і сплатою товарів та послуг. Все це разом зумовлює значне зростання вартості інформації, що циркулює в комп'ютерних мережах.

Функціонування мереж та інформаційних систем всередині них залежить не лише від надійності використовуваного обладнання, але й від здатності мережі протистояти будь-яким спробам порушити її роботу.

На сьогодні інтернет речей (IoT) стає все більш розповсюдженим, він привернув увагу людей і організацій з багатьох галузей, надавши їм різноманітні переваги. Проте поряд з його зростанням, виникли питання підвищення безпеки інформації, та оскільки IoT – це взаємопов'язані системи пристроїв, які забезпечують безперешкодний обмін інформацією між фізичними пристроями, то кількість конфіденційної інформації в мережі буде збільшуватись, а це, в свою чергу, призведе до збільшення площини і ймовірності атак (Khraistan, 2021, p. 1).

Відсутність достатнього рівня захисту мереж має суттєвий вплив на світову економіку. В результаті кібер-атак на Colonial Pipeline близько 45% території Східного узбережжя США тимчасово втратили постачання дизельного палива, бензину та авіакеросину, що призвело до того, що середня ціна в США зросла з 7 центів до $3,04 за галон, що стало найвищим показником за останні сім років. Крім того, компанія Colonial Pipeline підтвердила, що після атаки заплатила зловмисникам викуп у розмірі 4,4 мільйона доларів США (Cremer, 2022 p. 716–717).

Слід зазначити, що атаки на інформаційні системи з кожним роком стають усе досконалішими, масштабнішими. Поточний ландшафт загроз вимагає нового підходу до систем виявлення, що спирається на традиційну складність тонкого налаштування початкових правил, порогових значень, базових показників. Боротьба з множиною хибних спрацьовувань стає неприйнятною для багатьох організацій. При підготовці до захисту від зловмисників використовується кореляція даних з декількох джерел, профілізація, поведінкова аналітика, засоби виявлення аномалій, оцінка активності та машинне навчання. Важливо підкреслити, що деякі традиційні засоби управління безпекою, такі як аналіз протоколів та антивірусне ПЗ на основі сигнатур, все ще займають свою нішу на лінії захисту, але призначені для боротьби із застарілими загрозами (Янко, 2022, с. 59).

Як наслідок, потреба у вдосконаленні систем виявлення вторгнень, які в першу чергу відповідають за виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів, стає дедалі гострішою.

Мета дослідження – дослідження більш ефективної розроблюваної СВМА що ввібрала переваги та виправила недоліки вже існуючих відкритих систем. Основними завданнями цього дослідження є:

– аналіз існуючих рішень задля виявлення атак наведених у таблиці 1;

– використання методу Сааті для декомпозиції цілі;

– дослідження розроблюваної СВМА;

– проведення порівняльного аналізу розроблюваної системи з вже існуючими за для підтвердження її ефективності та актуальності;

– висновки, узагальнення результатів дослідження, виявлення переваг та обмежень розроблюваної системи, та перспективи подальших досліджень.

Таблиця 1

Існуючі рішення задля виявлення атак

Назва системи	Виробник
OSSEC	Daniel B. Sid, OSSEC.net
NETSTAT	University of California at Santa Barbara
Prelude	Yoann Vandoorselaere, Laurent Oudot

Основна частина. Основним засобом захисту інформаційних систем та мереж від вторгнень є системи виявлення та/або запобігання вторгненням, основне завдання яких зводиться до оперативної їх ідентифікації та ініціюванні ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів (Толюпа, 2021, с. 21).

Процес моніторингу мережевого трафіку у СВА – це складний процес, що передбачає збір, аналіз та інтерпретацію великої кількості даних, що надходять з мережі. Процес моніторингу мережевого трафіку всередині СВА складається з послідовних етапів: збір даних, фільтрація трафіку та його наступний аналіз, виявлення вразливостей і атак, попередження для користувача, реагування та створення аудиту (Мєшков, 2023, с. 88–89).

Всі системи що розглядаються й наведені у таблиці 1, використовують в якості основного методу виявлення атак сигнатурний метод (порівняння рядків, шаблонів).

Система OSSEC є монолітною – в сенсори і аналізатори «зашиті» знання розробників системи виявлення атак про те, які послідовності повідомлень в журналах можуть бути ознаками атаки. Основним компонентом OSSEC IDS є менеджер, що аналізує журнали подій групи агентів та порівнює їх із конкретними шаблонами, встановленими в налаштованих правилах. Якщо події агентів OSSEC відповідають певному шаблону встановленого правила, диспетчер OSSEC виконує для агентів визначені дії, які повинні застосовуватися протягом певного періоду часу. Прикладом таких дій може бути блокування потенційно небезпечної IP-адреси або додавання її до списку пристроїв з обмеженим доступом на певний час. Така архітектура системи є важко розширюваною з точки зору бази знань про атаки (Diogo, 2019, p. 1–2).

Система NetSTAT (Network-based State Transition Analysis Tool) розроблена кафедрою комп'ютерних наук університету Каліфорнії, Санта-Барбара, США. Вона базується на розширюваній мові опису атак та їх шаблонів (STATL). Ця система має два режими функціонування: один заснований на характеристиках захищеності станів системи та послідовностях переходів, інший на сигнатурному підході, що використовує порівняння зі сценаріями атак для виявлення вторгнень в реальному часі. Система використовує абстрактні об'єкти та події для виявлення аномалій та зловживань у мережі. Управління розподілене, а архітектура дозволяє будувати агентів для виявлення атак на різних рівнях мережі (Корченко, 2019, с. 26–27).

Система Prelude використовує різні компоненти, що аналізуються, для мережевих даних і журналів реєстрації. Також використовується набір спеціалізованих модулів для виявлення специфічних атак, таких як сканування портів, некоректні ARP пакети і т.п. Спеціальні модулі виробляють дефрагментацію IP, складання TCP-потоку, декодування HTTP-запитів. Система Prelude, як і NETSTAT, є гібридною, тобто здатна виявляти атаки як на рівні системи, так і на рівні мережі. Дана система спочатку розроблялася як самостійна СВА, але в даний час є високорівневою надбудовою над відкритими СВА і системами контролю цілісності (AIDE, Osiris). Вузлова частина Prelude має достатньо широкий набір описів атак товує журнали реєстрації у якості основного джерела інформації (Голубничий, 2020, с. 1061–1070).

Система, що розробляється, порівнюється з існуючими системами та пропонує підхід до виявлення аномалій у мережах, що використовує вейвлет-перетворення та теорію ідентифікації системи. Вхідний сигнал складається з 15-вимірного вектора ознак, який описує поведінку мережевих потоків. Введено модель прогнозування для звичайного трафіку, в якому вейвлет-коефіцієнти відіграють важливу роль як зовнішні вхідні дані для моделі ARX, яка прогнозує коефіцієнт апроксимації сигналу. Порівнюючи вихідні дані моделі прогнозування трафіку, система може виміряти різницю між нормальною та ненормальною активністю. Щоб виявити піки з набору залишків, система використовує заснований на GMM алгоритм виявлення викидів. Рішення приймаються на основі результатів запропонованого алгоритму виявлення викидів.

Система використовує дискретне вейвлет-перетворення, оскільки мережеві сигнали, що аналізуються, мають певну частоту зрізу. Це дозволяє використовувати базисні функції для перетворення вхідних сигналів в набір коефіцієнтів апроксимації та деталізації, які можуть бути використані для реконструкції вхідного сигналу. Процес моделювання нормального мережевого трафіку складається з двох окремих етапів: вейвлет-декомпозиції/реконструкції та генерації авторегресійної моделі. Під час

практичної реалізації сигнали проходять через фільтри низьких і високих частот на кожному етапі. Після того, як дані низького рівня відфільтровані, коефіцієнти, що залишилися, є зведенням високого рівня про поведінку сигналів. Отже, ці коефіцієнти можна використовувати для створення профілю сигналу, що характеризує очікувану поведінку мережевого трафіку. У процесі вейвлет-розкладання/реконструкції вихідні сигнали перетворюються на набір коефіцієнтів вейвлет-апроксимації, які представляють приблизне зведення сигналу, оскільки під час фільтрації дані видаляються. Щоб оцінити параметри ARX і згенерувати модель прогнозування, використовуються вейвлет-коефіцієнти різних частин навчальних даних в якості вхідних даних та даних для підбору моделі. Процес підгонки ARX використовується для оцінки оптимальних параметрів на основі методу найменших квадратів.

Після отримання моделі прогнозування для типового мережевого трафіку, її можна застосувати для ідентифікації аномальних сигналів. Коли модель отримує виключно звичайний трафік як вхідні дані, результуючі дані, звані залишками, будуть близькі до нуля. Це означає, що прогнозоване значення, згенероване моделлю, близьке до фактичних вхідних нормальної поведінки. І навпаки, якщо в якості вхідних даних для моделі надається суміш нормального та ненормального трафіку, залишки демонструватимуть численні піки, які відповідають аномаліям. Потім ці залишки спрямовуються до механізму прийняття рішень про вторгнення, де працює алгоритм виявлення викидів, що приймає рішення про можливе вторгнення (Hrynchenko, 2023, p. 46).

Тепер виконаємо декомпозицію питання прийняття рішень з виділенням головної цілі та альтернатив. Елементи однакових рівнів співставні один з одним з точки зору встановлення пріоритетів.

Метод аналізу мережі – відносно нова методологія прийняття рішень авторства Томаса Сааті, яка побачила світ приблизно через 20 років після винайдення ним методу аналізу ієрархій. Сааті вважав, що кожну проблему прийняття рішень можна представити у формі мережі. Цей підхід став логічним послідовником MAI і уможливив вирішення найскладніших проблем. В методі аналізу мереж застосовують системний підхід до вирішення мультикритеріальних проблем. При прийнятті рішень, що залежать від багатьох критеріїв, особа, яка приймає рішення, має порівнювати альтернативи відносно критеріїв, підкритеріїв, цілей, спираючись на власні знання, досвід та інтуїцію (Бєлов, 2020, с. 31–32).

Скориставшись методом Сааті задля вирішення цієї задачі, визначається наступна ієрархія цілей (рис. 1).

Рис. 1. Загальна ієрархія проблеми прийняття рішень

На основі цього будується схема поточного дослідження на рис. 1, основною метою якого є доведення ефективності розроблюваної системи виявлення мережевих атак серед трьох існуючих альтернатив за шістьма критеріями (рис. 2).

Щоб встановити пріоритети критеріїв, отримати оцінки для альтернативних рішень, будуються матриці парних порівнянь $A = a_{ij}$.

При побудові матриці парних порівнянь використовується фундаментальна шкала переваг.

Розрахунок локальних векторів пріоритетів. Для кожної матриці розраховуються локальні пріоритети елементів, що порівнюються.

На цьому етапі можна, зокрема, зробити висновок про те, що найбільш значущим критерієм є класи атак, що можуть бути визначені, а найменш значущим – масштабованість.

Перевірка обмеженості оцінки пріоритетів. На цьому етапі обчислюється індекс узгодженості (ІУ) суджень щодо кожної матриці:

$$ІУ = \frac{\lambda_{max} - n}{n - 1}, \quad (1)$$

де n – розмірність матриці, а λ_{max} розраховується за наступними кроками:

1) підсумовується кожний стовпець матриці парних порівнянь;

2) сума першого стовпця множиться на першу компоненту локального вектора пріоритетів, сума другого стовпця на другу компоненту і т. д.;

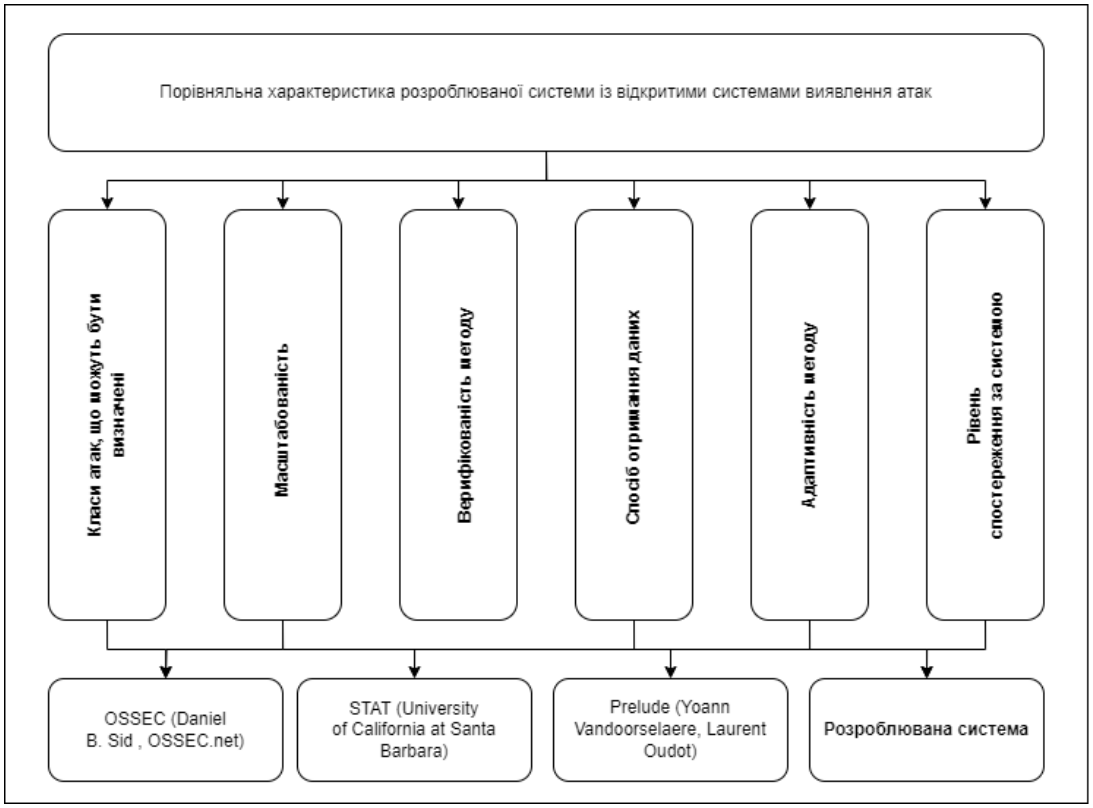

Рис. 2. Ієрархія вибору системи виявлення атак з визначеної множини альтернатив

Таблиця 2

Оцінка важливості критеріїв

Критерій	**Класи атак, що можуть бути визначені**	**Масштабованість**	**Верифікованість методу**	**Спосіб отримання даних**	**Адаптивність методу**	**Рівень спостереження за системою**	$\prod_{i=1}^{6}$	$\sqrt[6]{\prod_{i=1}^{6}}$	**локальний вектор пріоритетів** $\frac{\sqrt[6]{\prod_{i=n}^{6}}}{\sum\sqrt[6]{\prod_{i=1..n}^{6}}}$
	i=1	*i=2*	*i=3*	*i=4*	*i=5*	*i=6*			
Класи атак, що можуть бути визначені	1	9	5	7	4	3	3780	3.947	**0.444**
Масштабованість	0.(1)	1	0.2	0.(3)	0.1(6)	0.143	0.0002	0.237	**0.027**
Верифікованість методу	0.2	5	1	3	0.5	0.(3)	0.495	0.891	**0.1**
Спосіб отримання даних	0.143	3	0.(3)	1	0.25	0.2	0.007	0.439	**0.049**
Адаптивність методу	0.25	6	2	4	1	0.5	6	1.348	**0.152**
Рівень спостереження за системою	0.(3)	7	3	5	2	1	69.3	2.030	**0.228**
Загалом	2.04	31	11.53	20.33	7.92	5.18	1	8.886	1

3) отримані додатки підсумовуються.

Після чого ІС порівнюється з випадковою узгодженістю (ВУ), величиною, яка б вийшла при випадковому виборі суджень за фундаментальною шкалою для заданого значення.

Після визначення ІС і ВУ визначається відношення узгодженості (для матриць розмірністю більше за 2)

$$\text{Відношення узгодженості} = \frac{\text{індекс узгодженості}}{\text{випадкова узгодженість}}$$

$$\text{Випадкова узгодженість}_{n=4} = 0.9$$

$$\text{Випадкова узгодженість}_{n=6} = 1.24 \quad (2)$$

Якщо для конкретної матриці виявиться, що відношення узгодженості > 0.1, то можна стверджувати, що судження експерта, на основі яких заповнена досліджувана матриця, сильно неузгоджені, і йому слід заповнити матрицю знову, більш уважно використовуючи при цьому шкалу парних порівнянь. В іншому випадку судження експерта приймаються.

Розраховується відношення узгодженості за матрицею парних порівнянь критеріїв

$$\lambda_{max} = \frac{\textit{Сума значень вектора вагів}}{\textit{Кількість критеріїв}} \quad (3)$$

$$\begin{aligned}\lambda_{max} &= (2.04 \cdot 0.444) + (31 \cdot 0.027) + \\ &+ (11.53 \cdot 0.1) + (20.33 \cdot 0.049) + \\ &+ (7.92 \cdot 0.0152) + (5.18 \cdot 0.228) = 6.277\end{aligned} \quad (4)$$

$$\text{Індекс узгодженості} = \frac{\lambda_{max} - n}{n-1} = \frac{6.277 - 6}{6-1} = 0.055 \quad (5)$$

$$\textit{Відношення узгодженості} = \frac{\text{індекс узгодженості}}{\text{випадкова узгодженість}} = \frac{0.055}{1.24} = 0.045 \le 0.1 \quad (6)$$

Отримане значення відношення узгодженості не перевищує 0.1, що свідчить про те що оцінки експерту є узгодженими.

На цьому етапі послідовно обчислюються локальні вектори пріоритетів та перевіряється узгодженість результатів кожного елемента ієрархії.

Оцінка узгодженості думки експерта:

$$\begin{aligned}\lambda_{max} &= (3.27 \cdot 0.355) + (16.50 \cdot 0.067) + \\ &+ (1.74 \cdot 0.534) + (20 \cdot 0.044) = 4.076\end{aligned} \quad (7)$$

$$\text{ІУ} = \frac{(4.076 - 4)}{(4-1)} = 0.025 \quad (8)$$

$$\text{Відношення узгодженості} = \frac{0.025}{0.9} = 0.028 \le 0.1 \quad (9)$$

За класами атак, що можуть бути визначені найбільш пріоритетним є альтернатива PRELUDE.

За тим самим принципом перевіряється узгодженість результатів усіх інших елемента ієрархії.

Оцінка узгодженості думки експерта для масштабованості методів:

$$\begin{aligned}\lambda_{max} &= (8.25 \cdot 0.143) + (18 \cdot 0.046) + \\ &+ (1.44 \cdot 0.669) + (8.25 \cdot 0.143) = 4.151\end{aligned} \quad (10)$$

$$\text{ІУ} = \frac{(4.151 - 4)}{(4-1)} = 0.050 \quad (11)$$

$$\text{Відношення узгодженості} = \frac{0.050}{0.9} = 0.056 \le 0.1 \quad (12)$$

За масштабованістю найбільш пріоритетним є PRELUDE.

Оцінка узгодженості думки експерта для верифікованості:

$$\begin{aligned}\lambda_{max} &= (13.33 \cdot 0.085) + (4.34 \cdot 0.290) + \\ &+ (20 \cdot 0.042) + (1.59 \cdot 0.582) = 4.157\end{aligned} \quad (13)$$

$$\text{ІУ} = \frac{(4.157 - 4)}{(4-1)} = 0.052 \quad (14)$$

$$\text{Відношення узгодженості} = \frac{0.052}{0.9} = 0.058 \le 0.1 \quad (15)$$

Таблиця 3

Класи атак, що можуть бути визначені

Класи атак, що можуть бути визначені	**OSSEC**	**NETSTAT**	**PRELUDE**	**Розроблювана СВМА**	$\prod_{i=1}^{4}$	$\sqrt[4]{\prod_{i=1}^{4}}$	**вектор пріоритетів**
OSSEC	1	7	0.5	8	28	2.3	**0.355**
NETSTAT	0.143	1	0.125	2	0.36	0.435	**0.067**
PRELUDE	2	8	1	9	144	3.464	**0.534**
Розроблювана СВМА	0.125	0.5	0.(1)	1	0.007	0.289	**0.044**
Загалом	3.27	16.50	1.74	20		6.488	**1**

Таблиця 4

Розрахунок глобальних пріоритетів

	Класи атак, що можуть бути визначені	Масштабованість	Верифікованість методу	Спосіб отримання даних	Адаптивність методу	Рівень спостереження за системою	Глобальний пріорітет (ГП)
Приорітети	0.444	0.027	0.1	0.049	0.152	0.228	
OSSEC	0.355	0.143	0.085	0.11	0.424	0.085	**0.259**
NETSTAT	0.067	0.046	0.291	0.037	0.103	0.29	**0.144**
PRELUDE	0.534	0.669	0.042	0.427	0.05	0.042	**0.297**
Розроблювана СВМА	0.044	0.143	0.582	0.427	0.424	0.582	**0.3**
Загалом							1

За верифікованістю методу найбільш пріоритетним є розроблювана СВМА.

Оцінка узгодженості думки експерта для способів отримання даних методами:

$$\lambda_{max} = (11.5 \cdot 0.11) + (24 \cdot 0.037) + \\ + (2.31 \cdot 0.427) + (2.31 \cdot 0.427) = 4.09 \quad (16)$$

$$\text{ІУ} = \frac{(4.09 - 4)}{(4 - 1)} = 0.03 \quad (17)$$

$$\text{Відношення узгодженості} = \frac{0.03}{0.9} = 0.032 \le 0.1 \quad (18)$$

За способом отримання даних найбільш пріоритетним є PRELUDE та розроблювана СВМА.

Оцінка узгодженості думки експерта для адаптивності методів:

$$\lambda_{max} = (2.34 \cdot 0.424) + (11.33 \cdot 0.103) + \\ + (18 \cdot 0.05) + (2.34 \cdot 0.424) = 4.051 \quad (19)$$

$$\text{ІУ} = \frac{(4.051 - 4)}{(4 - 1)} = 0.017 \quad (20)$$

$$\textit{Відношення узгодженості} = \frac{0.017}{0.9} = 0.019 \le 0.1 \quad (21)$$

За адаптивності найбільш пріоритетним є OSSEC та розроблювана СВМА.

Оцінка узгодженості думки експерта для рівня спостереження за системою:

$$\lambda_{max} = (13.33 \cdot 0.085) + (4.34 \cdot 0.29) + \\ + (20 \cdot 0.0.042) + (1.59 \cdot 0.582) = 4.157 \quad (22)$$

$$\textit{ІУ} = \frac{(4.157 - 4)}{(4 - 1)} = 0.052 \quad (23)$$

$$\textit{Відношення узгодженості} = \frac{0.052}{0.9} = 0.058 \le 0.1 \quad (24)$$

За рівнем спостереження за системою найбільш пріоритетним є розроблювана СВМА.

Для підведення підсумку розраховуються пріоритети для всієї ієрархії в сукупності. Відбувається перехід безпосередньо до принципу синтезу пріоритетів. Локальні пріоритети альтернатив множаться на пріоритети відповідних критеріїв рівня та підсумовуються по кожному елементу відповідно до критеріїв. Внаслідок цього визначаються глобальні пріоритети альтернатив з урахуванням пріоритетів критеріїв. Найбільш високий рейтинг буде відповідати альтернативі з найбільшим значенням глобального пріоритету (ГП).

$$\textit{ГП} = \sum_{i,j=1}^{n} v_i v_j, \quad (25)$$

де v_i – локальний пріоритет альтернативи;
v_j – пріоритет відповідного критерія рівня.

$$\textit{ГП}_{\text{OSSEC}} = (0.444 \cdot 0.355) + (0.027 \cdot 0.143) + \\ + (0.1 \cdot 0.085) + (0.049 \cdot 0.11) + \\ + (0.152 \cdot 0.424) + (0.228 \cdot 0.085) = 0.259 \quad (26)$$

$$\textit{ГП}_{\text{NETSTAT}} = (0.444 \cdot 0.067) + (0.027 \cdot 0.046) + \\ + (0.1 \cdot 0.291) + (0.049 \cdot 0.037) + \\ + (0.152 \cdot 0.103) + (0.228 \cdot 0.290) = 0.144 \quad (27)$$

$$\textit{ГП}_{\text{PRELUDE}} = (0.444 \cdot 0.534) + (0.027 \cdot 0.669) + \\ + (0.1 \cdot 0.042) + (0.049 \cdot 0.427) + \\ + (0.152 \cdot 0.050) + (0.228 \cdot 0.042) = 0.297 \quad (28)$$

$$\textit{ГП}_{\text{СВМА}} = (0.444 \cdot 0.044) + (0.027 \cdot 0.143) + \\ + (0.1 \cdot 0.582) + (0.049 \cdot 0.427) + \\ + (0.152 \cdot 0.424) + (0.228 \cdot 0.085825) = 0.3 \quad (29)$$

Порівнюючи отримані значення глобальних пріоритетів, визначаються рейтинги альтернатив. У поточному дослідженні найбільший

пріоритет 0,3 має розроблювана система виявлення мережевих атак, що свідчить про її переваги за визначеними критеріями у загальному заліку систем, що порівнювалися, а отже, робить доцільним її подальший розвиток та вдосконалення.

Висновки. У роботі проведено аналіз та розглянуто низку систем виявлення атак (табл. 1), чиї основні особливості порівнюються із створюваною задля дослідження її актуальності.

Використання методу Сааті для декомпозиції цілі сприяло чіткому формулюванню завдань дослідження та підвищило структурованість аналізу. Проведений порівняльний аналіз підтвердив ефективність та актуальність розроблюваної системи, виявивши її переваги у виявленні й реагуванні на мережеві загрози відносно вже існуючих аналогів. Це свідчить про те, що досліджувана СВМА відповідає вимогам сучасного інформаційного середовища та може бути успішно впроваджена для забезпечення безпеки мережевих систем.

Додаткові перспективи досліджень у цьому напрямку можуть включати розширення функціональності системи, її адаптацію до нових типів загроз та пошук способів оптимізації процесу виявлення атак.

ЛІТЕРАТУРА:

1. Khraisat A., Alazab A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity.* 2021. P. 1.

2. Cremer F., Sheehan B., Fortmann M. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice.* 2022. P. 716–717.

3. Янко А.С., Макаренко О.І. Концепція системи виявлення та запобігання вторгнень до мережі. *Національний університет «Полтавська політехніка імені Юрія Кондратюка».* 2022. № 2. С. 59.

4. Толюпа С., Лукова-Чуйко Н., Шестак Я. Засоби виявлення кібернетичних атак на інформаційні системи. *Київський національний університет імені Тараса Шевченка.* 2021. № 2 (2). С. 21.

5. Мєшков В. Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2023. Вип. 1. С. 88–89.

6. Teixeira D., Assunção L., Pereira T. OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections. *Journal of Sensor and Actuator Networks.* 2019. 8, 46. P. 1–2.

7. Корченко А. Методи ідентифікації аномальних станів для систем виявлення вторгнень. *ЦП «Компринт»*: монографія / А. Корченко. Київ, 2019. С. 26–27.

8. Голубничий Д. Ю. Оцінка складності методів виявлення атак. *Scientific Collection «InterConf», (37): with the Proceedings of the 1 st International Scientific and Practical Conference «Recent Scientific Investigation».* Oslo, Norway, december 6-8 2020 y. Oslo, 2020. P. 1061–1070.

9. Hrynchenko P. Detection of Unauthorized Actions in Networks Using Wavelet Analysis. *Theoretical and Applied Cyber Security*. 2023. Vol. 5. № 2. P. 40–46.

10. Бєлов М. Л. Переваги та недоліки методу аналізу ієрархій в задачах прийняття рішень [https://ekmair.ukma.edu.ua/handle/123456789/18277] / Національний університет «Києво-Могилянська академія». Київ, 2020. С. 31–32.

REFERENCES:

1. Khraisat, A., Alazab. A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity,* 1.

2. Cremer, F., Sheehan, B., Fortmann, M. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice,* 716–717.

3. Yanko, A. S., Makarenko, O. I. (2022). Kontseptsiia systemy vyiavlennia ta zapobihannia vtorhnen do merezhi [Network intrusion detection and prevention system concept]. *Natsionalnyi universytet «Poltavska politekhnika imeni Yuriia Kondratiuka» – National University «Yuriy Kondratyuk Poltava Polytechnic»*, 2, 59 [in Ukrainian].

4. Toliupa, S., Lukova-Chuiko. N., Shestak. Ya. (2021). Zasoby vyiavlennia kibernetychnykh atak na informatsiini systemy [Tools of detection of cybernetic attacks on information systems]. *Kyivskyi natsionalnyi universytet imeni Tarasa Shevchenka – Taras Shevchenko National University of Kyiv*, 2 (2), 21[in Ukrainian].

5. Mieshkov, V. (2023). Analiz system intelektualnoho monitorynhu trafiku kompiuternoi merezhi dlia system vyiavlennia atak [Analysis of intelligent computer network traffic monitoring systems for attack detection systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security, 1, 88–89* [in Ukrainian].

6. Teixeira, D., Assunção, L., Pereira, T. (2019). OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections. *Journal of Sensor and Actuator Networks,* 8, 46, 1–2.

7. Korchenko. A. (2019). *Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen [Methods of identifying abnormal states for intrusion detection systems].* Kyiv: TsP «Komprynt» [in Ukrainian].

8. Holubnychyi, D. Iu. (2020). Otsinka skladnosti metodiv vyiavlennia atak [Assessment of the complexity of attack detection methods]. *Scientific Collection «InterConf», (37): with the Proceedings of the 1 st International Scientific and Practical Conference «Recent Scientific Investigation»,* Norway: Oslo, 1061–1070.

9. Hrynchenko, P. (2023). Detection of Unauthorized Actions in Networks Using Wavelet Analysis. *Theoretical and Applied Cyber Security*, 5, 2, 40–46.

10. Bielov, M. L. (2020). Perevahy ta nedoliky metodu analizu iierarkhii v zadachakh pryiniattia rishen: mahisterska robota [Advantages and disadvantages of the method of analyzing hierarchies in decision-making tasks]. *ekmair.ukma.edu.ua/handle/123456789/18277*. Retrieved from https://ekmair.ukma.edu.ua/handle/123456789/18277 [in Ukrainian].