https://doi.org/10.31891/2219-9365-2025-81-21
УДК 004.7

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

АНАЛІЗ МОДЕЛЕЙ ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Метою дослідження є аналіз моделей виявлення аномалій мережевого трафіку в інформаційно-комунікаційних системах (ІКС), а також оцінка їхніх переваг і недоліків. У роботі розглянуто критерії оцінки ефективності таких моделей, зокрема точність, складність налаштування, вплив на мережу та здатність до аналізу вхідного та вихідного трафіку. В результаті отримано порівняння найбільш перспективних підходів, що дозволяє визначити оптимальні рішення для забезпечення високої точності виявлення загроз при мінімальних ресурсних витратах.
Ключові слова: моделі виявлення аномалій, мережевий трафік, кіберзагрози.

PETLIAK Nataliia
Khmelnytskyi National University

ANALYSIS OF TRAFFIC ANOMALY DETECTION MODELS IN MODERN INFORMATION AND COMMUNICATION SYSTEMS AND NETWORKS

The aim of the study is to analyze existing models for detecting anomalies in network traffic to assess their advantages and disadvantages, as well as to develop criteria for determining the feasibility of using these models in information and communication systems (ICS). This allows for a deeper understanding of the capabilities and limitations of different approaches to detecting threats in networks and assessing the effectiveness of the methods used to ensure system security. This paper provides a detailed analysis of current research in this area, which collects various approaches to detecting attacks such as SQL injections, DoS attacks, botnets, man-in-the-middle attacks, and other network traffic anomalies. The work focuses on comparing models such as machine learning, fuzzy logic, hybrid models, the use of neural networks, genetic algorithms, autoencoders, as well as traditional methods, including signature analysis and data classification. One of the main tasks is to develop criteria by which to compare models, including the type of attack, the approach used, the complexity of the configuration, the load on the network, the analysis of incoming and outgoing traffic, and the accuracy of the model. These criteria help determine which model is the best for a particular type of attack, which is most suitable for working in resource-limited environments or for use in scalable systems. The study collected data on the effectiveness of various models based on real-world examples, demonstrating their accuracy, ability to adapt in real time, and efficiency in processing large volumes of network traffic. Hybrid models that combine different methods to increase the efficiency of anomaly detection were also considered. Despite the high accuracy results, there are limitations for some models, such as high setup complexity or computational costs. In particular, the use of methods based on genetic algorithms requires significant computing resources, while simpler models based on machine learning can be quickly set up and work effectively with limited resources. In other words, the accuracy and speed of models are directly related to their ability to integrate into existing ICS, where computing limitations and data processing speed requirements are also important. In addition, the impact of network load on the effectiveness of an anomaly detection system is considered, where it was found that for large volumes of traffic, the choice of low-load methods is critical. Models with a high level of computational costs can adversely affect network performance, which is an important aspect when implementing them in real-world conditions.
Keywords: anomaly detection models, network traffic, cyber threats.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних інформаційно-комунікаційних системах кіберзагрози стали одним із складних викликів для організацій, урядів і користувачів, що пояснюється збільшенням кількості атак [1-3]. Поширення цифрових технологій, мобільних пристроїв і хмарних сервісів значно розширило можливості для зловмисників [4], які використовують вразливості програмного забезпечення, методи соціальної інженерії та недостатній рівень захисту мереж для досягнення своїх цілей. Зростання кількості підключених пристроїв Інтернету речей (IoT) створює нові вектори атак і розширює атакуючу поверхню. Зловмисники постійно розробляють нові тактики, техніки та процедури, ускладнюючи виявлення та протидію атакам. Атаки, такі як SQL-ін'єкції, DoS, DDoS, ботнети, програми-вимагачі та експлойти, призводять до серйозних наслідків, включаючи фінансові втрати, витоки даних і загрози національній безпеці [5]. Особливо вразливими до кібератак є критична інфраструктура, охорона здоров'я, фінанси та енергетика, де порушення можуть мати катастрофічні наслідки.

Аналіз існуючих моделей виявлення аномалій є необхідним для глибшого розуміння ефективності сучасних підходів та визначення їхніх сильних і слабких сторін, що дозволить ідентифікувати найбільш перспективні методи, які забезпечать високу точність виявлення загроз за мінімальних ресурсних витрат і простоти впровадження. Оскільки кібератаки стають дедалі складнішими, то аналіз наявних моделей дозволить адаптувати існуючі підходи до нових умов, розробивши гнучкіші і масштабовані рішення,

покращуючи їхню інтеграцію в інформаційно-комунікаційні системи. Крім того, це сприяє зменшенню ризиків, пов'язаних із вибором неефективних або застарілих технологій, та підвищить загальний рівень кібербезпеки в організаціях різного масштабу.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

У роботі [6] досліджується модель аналізу мережевого трафіку для виявлення атак SQL-ін'єкцій за допомогою протоколу NetFlow V5. Застосування NetFlow обумовлено його здатністю ефективно збирати дані про трафік, що мінімізує обчислювальні витрати під час роботи з великими обсягами трафіку. Для аналізу використовувалися алгоритми машинного навчання та ансамблева модель. Найкращих результатів досягли моделі демонструючи точність понад 96% із низьким рівнем помилкових спрацювань.

У дослідженні [7] розроблено модель для виявлення шкідливого програмного забезпечення в операційній системі Android, яка поєднує нечітку логіку та методи машинного навчання. Основною метою є інтеграція результатів роботи класифікаторів через нечітку систему виведення для точного та ефективного виявлення шкідливих програм. Дослідження зосереджене на статичному аналізі APK-файлів, при цьому модель використовує адаптивний підхід, де процеси відбору ознак та навчання автоматизовані, що спрощує її інтеграцію. Нечітка логіка дозволяє налаштовувати правила за допомогою наборів функцій, і система може бути адаптована до різних наборів даних. Хоча використання кількох моделей збільшує обчислювальне навантаження, експериментальні результати підтверджують високу ефективність цієї моделі.

У роботі [8] розглядається розробка та тестування гібридної моделі Weighted k-Nearest Neighbor and Feedforward Neural Network (WK-FNN) для виявлення аномалій у мережевому трафіку. Модель базується на двох класифікаторах — зваженому алгоритмі k-найближчих сусідів і прямому нейронному шарі, що дозволяє поєднати переваги обох підходів та вирішувати протиріччя у їхніх результатах. У моделі WK-FNN два класифікатори оцінюють трафік паралельно, а їх результати обробляються через XOR-блок для досягнення більш точної ідентифікації аномалій. Дослідження показує високу ефективність цієї моделі на реальних даних, з точністю, що перевищує 99%.

Робота [9] описує розробку системи виявлення атак Multi-Channel Man-in-the-Middle (MC-MitM) для забезпечення безпеки Wi-Fi мереж, особливо у контексті IoT. Запропонована система використовує пасивний аналіз мережевого трафіку і сигнатурний підхід для виявлення таких атак. Система легко інтегрується і працює без змін у налаштуваннях мережі, при цьому мінімізує вплив на продуктивність. Вона підтримує інтеграцію з іншими системами безпеки.

Робота [10] присвячена використанню рекурентних нейронних мереж для виявлення аномалій у мережах IoT. Модель використовує три типи рекурентних мереж, що дозволяє ефективно працювати з послідовними даними. Вона включає кілька шарів для нормалізації та регуляризації, що покращує стабільність навчання. Модель застосовує оптимізовану архітектуру для багатокласової та бінарної класифікації, ефективно обробляючи потоки мережевого трафіку з 64 ознаками.

Робота [11] зосереджена на моделях самоподібності мережевого трафіку для виявлення аномалій у системах захисту. Дослідники пропонують моделі, які враховують хаотичну та фрактальну природу мережевого трафіку, і використовують методи штучного інтелекту, зокрема нейронні мережі та генетичні алгоритми. Моделі базуються на структурно-параметричній ідентифікації трафіку і використовують критерії мінімуму зсуву та регулярності для забезпечення точності виявлення аномалій у реальному часі.

Робота Гайдур та ін. [12] описує модель виявлення шкідливої активності в ІКС організацій, що використовує гібридний підхід на основі ансамблевого навчання. Модель комбінує кілька алгоритмів машинного навчання, таких як метод опорних векторів, дерева рішень і алгоритм k-найближчих сусідів, для покращення точності виявлення ботнетів через аналіз мережевого трафіку, моніторинг DNS-запитів та використання honeypots. Такий підхід дозволяє знижувати недоліки окремих алгоритмів і забезпечує високу адаптивність до нових сценаріїв атак.

Робота [13] пропонує модель нечіткої нейронної мережі для виявлення аномалій у даних, поєднуючи нейронні мережі та нечітку логіку. Модель має три рівні: фазифікацію даних, агрегацію через нечіткі логічні нейрони і вихідний шар з функцією активації. Вона створює нечіткі правила "якщо-тоді" для обробки складних взаємозв'язків і є ефективною для розробки експертних систем. Попри більший час навчання, модель демонструє високу точність і здатність інтегрувати отримані знання для покращення їх захисту.

В статті [14] запропоновано модель для виявлення аномалій на основі гібридного підходу з використанням кластеризації k-середніх. Спочатку відбувається попередня обробка даних для видалення нерелевантної інформації, що знижує складність і час навчання. Кластеризація формує стабільні кластери, а далі відбувається поділ трафіку на нормальний і аномальний. Така модель ефективно працює з великими обсягами даних, що характерно для мереж IoT.

Робота [15] пропонує модель виявлення мережевих аномалій на основі п'ятишарового автокодера. Модель використовує механізм реконструкції даних для виявлення аномальних шаблонів трафіку з

застосуванням порогу помилки реконструкції для ідентифікації аномалій. Її 5-рівнева структура дозволяє ефективно зменшувати розмірність даних і відновлювати їх із мінімальною втратою інформації. Попередня обробка даних, включаючи кодування та нормалізацію, покращує продуктивність і зменшує дисбаланс у наборі функцій.

Автори [16] пропонують модель виявлення аномалій на основі ансамблю механізмів навчання та прогнозування. Вона поєднує автоматизоване машинне навчання з алгоритмами фільтра Калмана для оптимізації прогнозів. Модель використовує автоматизований пошук архітектури нейронної мережі для створення оптимальних моделей глибокого навчання. Завдяки комбінації методів, модель здатна адаптуватися до змін у мережевих середовищах і виявляти нові типи атак у реальному часі.

Робота [17] націлена на покращення виявлення атак на цілісність даних, застосовуючи метод зворотного аналізу в часі (backward-in-time detection). Цей підхід дозволяє виявляти аномалії шляхом аналізу стану системи до початку атаки, використовуючи віртуальні значення стану, які оцінюються через H∞-фільтрацію. Основним елементом моделі є генерація залишкових величин та порогових значень, що допомагають визначити, чи є зміни результатом атаки. Проте модель залежить від точності математичного моделювання ІКС, що може бути складним у реальних умовах через динамічні зміни середовища та присутність шуму. Також застосування H∞-фільтра може бути обчислювально затратним, що обмежує масштабованість і застосування в реальному часі.

У [18] описано модель, яка поєднує методи виявлення вторгнень на основі аномалій та сигнатур, разом з гібридним підходом до аналізу, використовуючи нейронні мережі та нечітку логіку для виявлення кіберзагроз. Система успішно виявляє відомі атаки, зберігаючи точність на рівні 96.11%, однак її ефективність у реальних мережах із великими обсягами трафіку потребує додаткових досліджень.

STEP-GAN — це модель на основі генеративних змагальних мереж для виявлення аномалій, яка має перевагу у роботі з незбалансованими даними, проте її ефективність залежить від припущення, що нормальні дані в майбутньому будуть подібні до навчальних [19].

У [20] пропонують модель виявлення аномалій мережевого трафіку за допомогою хаотичних нейронних мереж, яка покращує класифікацію завдяки адаптивній вибірці та методам зменшення розмірності. Однак її складність і потреба в значних обчислювальних ресурсах для навчання є суттєвими недоліками.

Модель згорткової нейронної мережі для виявлення атак типу Bruteforce-SSH та Bruteforce-FTP, представлена в [21], включає різні типи шарів для обробки даних, але залежить від якості попередньої обробки, що обмежує точність.

У роботі [22] представлена модель виявлення аномалій на основі порівняння з заданими властивостями, що має адаптивність до різних типів даних. Проте процес створення і перевірки властивостей є складним, особливо для великих баз даних.

Модель для виявлення низькошвидкісних DDoS-атак, представлена в [23], використовує алгоритм класифікації Passive-Aggressive для адаптації до змін у трафіку в реальному часі, хоча потребує подальших досліджень для забезпечення ефективності в реальних сценаріях.

Автори [24] пропонують дві моделі для виявлення аномалій у мережевому трафіку: U-Net і Temporal Convolutional Network з Long Short-Term Memory, що мають високу точність, але складність реалізації та навчання є їхнім обмеженням.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: аналіз моделей виявлення аномалій трафіку в ІКС для оцінки їх переваг та недоліків, формування критеріїв оцінки доцільності їх застосування.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Аналіз досліджень та публікацій дозволяє визначити основні критерії за якими доцільно проводити порівняння. А саме: тип атаки, підхід, складність налаштування, навантаження на мережу, аналіз вхідного трафіку, аналіз вихідного трафіку та точність. Критерії, представлені в таблиці 1, ілюструють аспекти які впливають на доцільність застосування моделей виявлення аномалій у мережевому трафіку.

1. Тип атаки визначає здатність моделі виявляти різноманітні загрози, такі як SQL-ін'єкції, DoS-атаки, ботнети, атаки "людина посередині" або загальні аномалії, що підкреслює спеціалізацію моделі для конкретних загроз.

2. Застосований підхід відображає базову технологію, яка використовується в моделі, наприклад, машинне навчання, нейронні мережі, сигнатурний аналіз, генетичні алгоритми, автокодери або ансамблі моделей, що вказує на рівень гнучкості методів.

3. Складність налаштування оцінює, наскільки впровадження моделі потребує участі висококваліфікованих спеціалістів. Позначка «+» вказує на необхідність спеціалізованих знань для інтеграції, тоді як «-» означає простоту налаштування для звичайних користувачів.

4. Навантаження на мережу характеризує вплив моделі на продуктивність мережі. Низьке

навантаження «-» є перевагою для масштабованих або обмежених у ресурсах систем.

5. Аналіз вхідного трафіку демонструє здатність моделі обробляти мережеві дані для виявлення аномалій. Наявність такої функції позначається «+», а її відсутність «-».

6. Аналіз вихідного трафіку аналогічно оцінює здатність моделі працювати з даними, які надходять з мережі. Позначення аналогічні: «+» — функція доступна, «-» — відсутня.

7. Точність оцінки відображає ефективність моделі у виявленні загроз і вимірюється у відсотках, що є важливим показником для забезпечення безпеки мережі.

Таблиця 1

Порівняння моделей відповідно до заданих критеріїв

Критерій / Джерело	Критерії						
№	**1**	**2**	**3**	**4**	**5**	**6**	**7**
[6]	SQL-ін’єкції	машинне навчання, ансамблева модель	+	+	+	-	96
[7]	ШПЗ	нечітка логіка, машинне навчання	+	+	+	-	99.33
[8]	DoS, SQL-ін’єкції, людина по середині	машинне навчання	+	+	+	-	99.5
[9]	людина по середині	сигнатурний аналіз	-	+	+	-	99
[10]	аномалії	машинне навчання	+	+	+	-	99.67
[11]	аномалії	генетичний алгоритм	+	+	+	-	-
[12]	ботнет	машинне навчання	+	+	+	-	-
[13]	DoS, неавторизований доступ	нечітка логіка, машинне навчання	+	+	+	-	99
[14]	аномалії	машинне навчання	+	+	+	-	97.3
[15]	аномалії	автоенкодер	+	+	+	-	92.26
[16]	виявлення вторгнень	ансамблева модель	+	+	+	-	98.8
[17]	аномалії	зворотній аналіз в часі	+	+	+	-	98.1
[18]	QL-ін’єкції, міжсайтовий скриптинг та експлойти операційних систем	нечітка логіка, машинне навчання	+	+	+	-	96.11
[19]	аномалії	машинне навчання	+	+	+	-	99.51
[20]	аномалії	машинне навчання	+	+	+	-	98
[21]	Bruteforce-SSH, Bruteforce-FTP	машинне навчання	+	+	+	-	99.96
[22]	аномалії	машинне навчання	+	-	-	-	-
[23]	DDoS атаки	машинне навчання	+	-	+	-	99.7
[24]	аномалії	машинне навчання	+	+	+	+	97

Більшість досліджених моделей фокусуються на виявленні загальних аномалій, що свідчить про актуальність розробки універсальних рішень, здатних виявляти аномальну поведінку без прив’язки до конкретної загрози. Окрім загальних аномалій, моделі також спроможні виявляти різні типи атак, зокрема SQL-ін’єкції, DoS та DDoS-атаки. Однак, виявлення інших типів загроз, таких як атаки "людина посередині" чи ботнети, є значно меншим, що вказує на потребу в більш спеціалізованих рішеннях. Машинне навчання є найпоширенішим методом, який використовується в більшості моделей завдяки своїй високій точності та гнучкості. Хоча машинне навчання часто поєднується з іншими підходами, такими як нечітка логіка, сигнатурний аналіз, генетичні алгоритми та автокодери, саме машинне навчання залишається основним рушієм у цій галузі. Однак такі моделі вимагають високої кваліфікації для впровадження, що може ускладнити їх використання для малих організацій. Лише деякі моделі є простими в налаштуванні, що вказує на потребу в спрощенні процесу інтеграції. Щодо навантаження на мережу, всі розглянуті моделі демонструють низький рівень, що є важливою перевагою для масштабованих систем. Більшість моделей ефективно аналізують вхідний трафік, однак аналіз вихідного трафіку залишається менш розвиненим, що є перспективним напрямком для майбутніх досліджень.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Проаналізовані моделі мають як переваги, так і недоліки. Більшість моделей успішно аналізують вхідний трафік, однак їхнє впровадження нерідко потребує висококваліфікованих фахівців, що створює труднощі для ряду організацій. Крім того, деякі моделі зосереджені лише на окремих видах атак, що обмежує їхню здатність протидіяти складним загрозам.

Подальші дослідження у сфері виявлення аномалій у мережевому трафіку доцільно спрямувати на розробку адаптивних моделей, здатних реагувати на нові, раніше невідомі загрози. Перспективним є створення гібридних рішень, що поєднують переваги машинного навчання з нечіткою логікою, що дозволить підвищити точність і гнучкість систем. Важливим напрямом є також зниження навантаження на мережеву інфраструктуру, що може бути досягнуто шляхом оптимізації алгоритмів. Таким чином, майбутні розробки повинні бути спрямовані на створення адаптивних, масштабованих і високоточних моделей, здатних ефективно функціонувати в умовах реального часу та динамічного мережевого середовища.

Література

1. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки – 2021 [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf (дата звернення 14.07.2024)
2. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки – 2022 [Електронний ресурс]. – Режим доступу: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf (дата звернення 14.07.2024)
3. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки - 2023. https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення 14.07.2024)
4. Стратегія кібербезпеки України [Електронний ресурс]: Затверджено Указом Президента України від 26 серпня 2021 року №447/2021. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 27.08.2024) - Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України".
5. Cost of a Data Breach Report 2024 [Електронний ресурс]. – Режим доступу: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec (дата звернення 15.07.2024).
6. Crespo-Martínez I. S., Campazas-Vega A., Guerrero-Higueras A. M., Riego-DelCastillo V., Álvarez-Aparicio C., Fernández-Llamas C. SQL injection attack detection in network flow data / Crespo-Martínez I. S. [et al.] // Computers & Security. — 2023. — Vol. 127. DOI: 10.1016/j.cose.2023.103093.
7. Atacak İ.. An ensemble approach based on fuzzy logic using machine learning classifiers for Android malware detection / İ. Atacak // Applied Sciences. — 2023. — Vol. 13, no 13. DOI: 10.3390/app13031484.
8. Protic D., Stanković M., Antić V.. WK-FNN design for detection of anomalies in the computer network traffic / D. Protic, M. Stanković, V. Antić // Facta Universitatis - Series: Electronics and Energetics. — 2022. — Vol. 35, no. 2. — P. 269—282. DOI: 10.2298/FUEE2202269P.
9. Thankappan M., Rifà-Pous H., Garrigues C.. A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks / M. Thankappan, H. Rifà-Pous, C. Garrigues // IEEE Access. — 2024. — Vol. 12. — P. 23096—23121. DOI: 10.1109/ACCESS.2024.3362803.
10. Ullah I., Mahmoud Q. H. Design and development of RNN anomaly detection model for IoT networks / I. Ullah, Q. H. Mahmoud // IEEE Access. — 2022. — Vol. 10. — P. 62722—62750. DOI: 10.1109/ACCESS.2022.3176317.
11. Корнієнко В., Герасіна О., Тимофєєв Д., Сафаров О., Ковальова Ю.. Ідентифікація та прогнозування самоподібного трафіку інформаційно-комунікаційних мереж для систем виявлення атак / В. Корнієнко [та ін.] // Information Technology: Computer Science, Software Engineering and Cyber Security. — 2022. — № 1. — С. 20—29. DOI: https://doi.org/10.32782/IT/2022-1-4.
12. Гайдур Г. І., Гахов С. О., Гамза Д. Є.. Модель виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації / Г. І. Гайдур, С. О. Гахов, Д. Є. Гамза // Сучасний захист інформації. — 2024. — № 4 (60). — С. 30—38.
13. de Campos Souza P. V., Guimarães A. J., Rezende T. S., Silva Araujo V. J., Araujo V. S.. Detection of anomalies in large-scale cyberattacks using fuzzy neural networks / P. V. de Campos Souza [et al.] // AI. — 2020. — Vol. 1. — P. 92—116. DOI: https://doi.org/10.3390/ai1010005.
14. Gadal S., Mokhtar R., Abdelhaq M., Alsaqour R., Ali E. S., Saeed R.. Machine learning-based anomaly detection using K-Mean array and sequential minimal optimization / S. Gadal [et al.] // Electronics. — 2022. — Vol. 11, no. 2158. DOI: https://doi.org/10.3390/electronics11142158.
15. Xu W., Jang-Jaccard J., Singh A., Wei Y., Sabrina F.. Improving performance of autoencoder-based network anomaly detection on NSL-KDD dataset / W. Xu [et al.] // IEEE Access. — 2021. — Vol. 9. — P. 140136—140146. DOI: 10.1109/ACCESS.2021.3116612.
16. Imran, Jamil F., Kim D.. An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments / Imran, F. Jamil, D. Kim // Sustainability. — 2021. — Vol. 13, no. 10057. DOI: https://doi.org/10.3390/su131810057.
17. Zhang K., Polycarpou M. M., Parisini T.. Enhanced anomaly detector for nonlinear cyber-physical systems against stealthy integrity attacks / K. Zhang, M. M. Polycarpou, T. Parisini // IFAC-PapersOnLine. — 2020. — Vol. 53, no. 2. — P. 13682—13687. DOI: https://doi.org/10.1016/j.ifacol.2020.12.870.

18. Einy S., Oz C., Navaei Y.. Dorostkar The anomaly- and signature-based IDS for network security using hybrid inference systems / S. Einy [et al.] // Mathematical Problems in Engineering. — 2021. — P. 6639714. DOI: https://doi.org/10.1155/2021/6639714.

19. Adiban M., Siniscalchi S. M., Salvi G.. A step-by-step training method for multi-generator GANs with application to anomaly detection and cybersecurity / M. Adiban [et al.] // Neurocomputing. — 2023. — Vol. 537. — P. 296—308. DOI: https://doi.org/10.1016/j.neucom.2023.03.056.

20. Sheng S., Wang X.. Network traffic anomaly detection method based on chaotic neural network / S. Sheng, X. Wang // Alexandria Engineering Journal. — 2023. — Vol. 77. — P. 567—579. DOI: https://doi.org/10.1016/j.aej.2023.07.019.

21. Волокита А., Меленчуков М.. Дослідження моделей виявлення атак на розподілені системи за допомогою згорткових нейронних мереж / А. Волокита, М. Меленчуков // Measuring and Computing Devices in Technological Processes. — 2024. — № 3. — С. 224—229. DOI: https://doi.org/10.31891/2219-9365-2024-79-29.

22. Ciobanu M. G., Fasano F., Martinelli F., Mercaldo F., Santone A.. Model checking for data anomaly detection / M. G. Ciobanu [et al.] // Procedia Computer Science. — 2019. — Vol. 159. — P. 1277—1286. DOI: https://doi.org/10.1016/j.procs.2019.09.297.

23. Янко А., Прокудін А., Філь І., Крук О.. Виявлення атак типу LDDOS за допомогою SDN мереж з елементами машинного навчання / А. Янко [та ін.] // Measuring and Computing Devices in Technological Processes. — 2024. — № 4. — С. 287—296. DOI: https://doi.org/10.31891/2219-9365-2024-80-36.

24. Mezina A., Burget R., Travieso-González C. M.. Network anomaly detection with temporal convolutional network and U-Net model / A. Mezina [et al.] // IEEE Access. — 2021. — Vol. 9. — P. 143608—143622. DOI: 10.1109/ACCESS.2021.3121998.

References

1. Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks - 2021 [Electronic resource]: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf (accessed 07/14/2024).

2. Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks - 2022 [Electronic resource]: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf (дата звернення 14.07.2024)

3. Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks - 2023. https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення 14.07.2024)

4. Cybersecurity Strategy of Ukraine [Electronic resource]: Approved by the Decree of the President of Ukraine of August 26, 2021 №447/2021: https://zakon.rada.gov.ua/laws/show/447/2021#Text (accessed on 27.08.2024) - Decree of the President of Ukraine on the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine".

5. Cost of a Data Breach Report 2024 [Electronic resource]: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec (accessed on July 15, 2024).

6. Crespo-Martínez I. S., Campazas-Vega A., Guerrero-Higueras A. M., Riego-DelCastillo V., Álvarez-Aparicio C., Fernández-Llamas C. SQL injection attack detection in network flow data / Crespo-Martínez I. S. [et al.] // Computers & Security. — 2023. — Vol. 127. DOI: 10.1016/j.cose.2023.103093.

7. Atacak İ.. An ensemble approach based on fuzzy logic using machine learning classifiers for Android malware detection / İ. Atacak // Applied Sciences. — 2023. — Vol. 13, no 13. DOI: 10.3390/app13031484.

8. Protic D., Stanković M., Antić V.. WK-FNN design for detection of anomalies in the computer network traffic / D. Protic, M. Stanković, V. Antić // Facta Universitatis - Series: Electronics and Energetics. — 2022. — Vol. 35, no. 2. — P. 269—282. DOI: 10.2298/FUEE2202269P.

9. Thankappan M., Rifà-Pous H., Garrigues C.. A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks / M. Thankappan, H. Rifà-Pous, C. Garrigues // IEEE Access. — 2024. — Vol. 12. — P. 23096—23121. DOI: 10.1109/ACCESS.2024.3362803.

10. Ullah I., Mahmoud Q. H. Design and development of RNN anomaly detection model for IoT networks / I. Ullah, Q. H. Mahmoud // IEEE Access. — 2022. — Vol. 10. — P. 62722—62750. DOI: 10.1109/ACCESS.2022.3176317.

11. Kornienko V., Gerasina O., Timofeev D., Safarov O., Kovaleva Yu. Identification and prediction of self-similar traffic of information and communication networks for attack detection systems / V. Kornienko [et al: Computer Science, Software Engineering and Cyber Security. - 2022. - No. 1. - pp. 20-29. DOI: https://doi.org/10.32782/IT/2022-1-4.

12. Gaidur G. I., Gakhov S. O., Gamza D. E.. A model for detecting malicious activity in an organization's information system based on hybrid classification / G. I. Gaidur, S. O. Gakhov, D. E. Gamza. Gaidur, S.O. Gakhov, D.E. Gamza // Modern Information Protection. - 2024. - No. 4 (60). - P. 30-38.

13. de Campos Souza P. V., Guimarães A. J., Rezende T. S., Silva Araujo V. J., Araujo V. S.. Detection of anomalies in large-scale cyberattacks using fuzzy neural networks / P. V. de Campos Souza [et al.] // AI. — 2020. — Vol. 1. — P. 92—116. DOI: https://doi.org/10.3390/ai1010005.

14. Gadal S., Mokhtar R., Abdelhaq M., Alsaqour R., Ali E. S., Saeed R.. Machine learning-based anomaly detection using K-Mean array and sequential minimal optimization / S. Gadal [et al.] // Electronics. — 2022. — Vol. 11, no. 2158. DOI: https://doi.org/10.3390/electronics11142158.

15. Xu W., Jang-Jaccard J., Singh A., Wei Y., Sabrina F.. Improving performance of autoencoder-based network anomaly detection on NSL-KDD dataset / W. Xu [et al.] // IEEE Access. — 2021. — Vol. 9. — P. 140136—140146. DOI: 10.1109/ACCESS.2021.3116612.

16. Imran, Jamil F., Kim D.. An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments / Imran, F. Jamil, D. Kim // Sustainability. — 2021. — Vol. 13, no. 10057. DOI: https://doi.org/10.3390/su131810057.

17. Zhang K., Polycarpou M. M., Parisini T.. Enhanced anomaly detector for nonlinear cyber-physical systems against stealthy integrity attacks / K. Zhang, M. M. Polycarpou, T. Parisini // IFAC-PapersOnLine. — 2020. — Vol. 53, no. 2. — P. 13682—13687. DOI: https://doi.org/10.1016/j.ifacol.2020.12.870.

18. Einy S., Oz C., Navaei Y.. Dorostkar The anomaly- and signature-based IDS for network security using hybrid inference systems / S. Einy [et al.] // Mathematical Problems in Engineering. — 2021. — P. 6639714. DOI: https://doi.org/10.1155/2021/6639714.

19. Adiban M., Siniscalchi S. M., Salvi G.. A step-by-step training method for multi-generator GANs with application to anomaly detection and cybersecurity / M. Adiban [et al.] // Neurocomputing. — 2023. — Vol. 537. — P. 296—308. DOI: https://doi.org/10.1016/j.neucom.2023.03.056.

20. Sheng S., Wang X.. Network traffic anomaly detection method based on chaotic neural network / S. Sheng, X. Wang // Alexandria Engineering Journal. — 2023. — Vol. 77. — P. 567—579. DOI: https://doi.org/10.1016/j.aej.2023.07.019.

21. Volokita A., Melenchukov M.. Research of models for detecting attacks on distributed systems using convolutional neural networks / A. Volokita, M. Melenchukov // Measuring and Computing Devices in Technological Processes. - 2024. - No. 3. - P. 224-229. DOI: https://doi.org/10.31891/2219-9365-2024-79-29.

22. Ciobanu M. G., Fasano F., Martinelli F., Mercaldo F., Santone A.. Model checking for data anomaly detection / M. G. Ciobanu [et al.] // Procedia Computer Science. — 2019. — Vol. 159. — P. 1277—1286. DOI: https://doi.org/10.1016/j.procs.2019.09.297.

23. Yanko A., Prokudin A., Fil I., Kruk O.. Detection of LDDOS-type attacks using SDN networks with machine learning elements / A. Yanko [et al. Measuring and Computing Devices in Technological Processes. - 2024. - No. 4. - P. 287-296. DOI: https://doi.org/10.31891/2219-9365-2024-80-36.

24. Mezina A., Burget R., Travieso-González C. M.. Network anomaly detection with temporal convolutional network and U-Net model / A. Mezina [et al.] // IEEE Access. — 2021. — Vol. 9. — P. 143608—143622. DOI: 10.1109/ACCESS.2021.3121998.