КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.823
УДК 004. 8:004.7:621.39

Іванченко Євгенія Вікторівна
доктор технічних наук, професор
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID 0000-0003-3017-5752
e.ivanchenko@duikt.edu.ua

Аверічев Ігор Миколайович
кандидат економічних наук,
доцент кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID 0009-0008-9766-0115
iaverichev19@gmail.com

Рижаков Микола Миколайович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID 0009-0006-3377-7061
nykolay.ryjakov@gmail.com

УЗАГАЛЬНЕНА МОДЕЛЬ ПРОГНОЗУВАННЯ ТА ВИЯВЛЕННЯ КІБЕРБЕЗПЕКОВИХ АНОМАЛІЙ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. У статті розроблено та представлено інтегровану математичну модель для прогнозування мережевого навантаження та виявлення кібербезпекових аномалій, яка базується на сучасних методах глибокого навчання та архітектурі автоенкодера. Запропонований підхід об'єднує функціонал прогнозування на основі нейронної мережі з механізмами автоматичного виявлення відхилень у поведінці мережевого трафіку. На початковому етапі модель здійснює попередню обробку історичних даних із використанням нормалізації та експоненційного згладжування, що дозволяє ефективно виділити актуальні патерни навантаження. Прогнозування здійснюється за допомогою глибокої нейронної мережі, оптимізованої методом градієнтного спуску для досягнення мінімальної середньоквадратичної похибки. Для виявлення аномалій застосовується автоенкодер, який навчається на нормальних даних та використовує евклідову норму різниці між вхідним і відновленим сигналами для визначення рівня аномальності. Межі аномальності формуються адаптивно на основі стандартного відхилення та параметра чутливості, що дозволяє підвищити точність виявлення відхилень у змінних умовах мережевого середовища. У роботі запропоновано модель визначення критичності ситуації, яка враховує частку аномальних значень у загальному потоці даних. Це дає змогу класифікувати події за рівнем загрози та забезпечити своєчасну реакцію системи управління. Інтегрована модель працює як багаторівнева самонавчальна система, здатна не лише прогнозувати майбутній стан мережі, а й виявляти потенційно небезпечні ситуації у реальному часі. Практична реалізація запропонованого підходу дозволяє досягти високої точності прогнозу (до 95%) навіть за умов наявності аномалій та знижує кількість хибних тривог. Актуальність дослідження підтверджується викликами, пов'язаними з цифровізацією, масштабуванням мереж і необхідністю забезпечення безпеки в умовах зростання складності IT-інфраструктур. Представлена модель є ефективним інструментом для моніторингу, аналізу та реагування на загрози в контексті NFV/SDN-технологій, IoT і хмарних обчислень.

Ключові слова: штучний інтелект; глибоке навчання; прогнозування навантаження; автоенкодер; виявлення аномалій; інформаційна безпека; мережеве управління; критичність ситуації.

ВСТУП

У сучасних умовах стрімкої цифровізації та зростання кількості кіберзагроз особливої актуальності набуває проблема забезпечення стабільності та безпеки інформаційних мереж. Розширення спектра цифрових послуг, масове впровадження IoT-пристроїв, активне використання хмарних технологій та програмно-визначених мереж (SDN), призводять до постійного ускладнення структури та збільшення навантаження на мережеву інфраструктуру. В таких умовах надзвичайно важливою стає здатність мережі не лише підтримувати високі показники якості обслуговування, але й своєчасно реагувати на відхилення та аномальні ситуації, що можуть бути передвісниками збоїв або кіберінцидентів. Наявні методи виявлення аномалій у кіберсистемах, здебільшого побудовані на статичних правилах або простих статистичних моделях, демонструють низьку ефективність у складних умовах високої динаміки трафіку. Водночас, традиційні підходи до прогнозування навантаження не враховують нелінійні взаємозв'язки між параметрами системи та часто не здатні адаптуватися до нових патернів поведінки. Це створює нагальну потребу у впровадженні інтелектуальних самонавчальних моделей, здатних одночасно здійснювати високоточне прогнозування та ефективно виявляти потенційні аномалії в реальному часі.

Аналіз сучасної наукової літератури засвідчує інтенсивне зростання інтересу до застосування методів глибокого навчання у задачах прогнозування навантаження в комп'ютерних мережах [1] – [3]. Наприклад, у роботі Zhang et al. [1] продемонстровано застосування глибоких нейронних мереж для прогнозування трафіку в SDN-мережах, що дозволяє значно підвищити точність передбачення. Wang et al. [2] дослідили ефективність моделей LSTM у виявленні аномалій та відзначили їхню стійкість до збурень трафіку. У публікації Liu et al. [3] розглянуто гібридні моделі, які поєднують глибоке навчання та традиційні алгоритми маршрутизації, що дозволяє забезпечити не лише точність, але й адаптивність до мережевих умов. У той же час, автоенкодери як засіб виявлення аномалій досліджувалися в роботах Li et al. [4] та Huang et al. [5], де встановлено, що ця архітектура дозволяє ефективно ідентифікувати відхилення у високовимірних даних із мінімальними хибними спрацюваннями. Однак більшість досліджень фокусуються або на окремому прогнозуванні навантаження, або на виявленні аномалій, без їхньої повноцінної інтеграції в єдину архітектуру. Недостатньо досліджено підходи, які б дозволяли поєднати ці два аспекти в одному рішенні з метою створення гнучкої, адаптивної та масштабованої системи мережевого моніторингу і реагування. Таким чином, постає необхідність розробки комплексної моделі, що одночасно виконує функції прогнозування, аналізу аномалій і оцінки критичності ситуацій — з урахуванням специфіки сучасних мереж.

Метою статті є розробка та формалізація інтегрованої математичної моделі, яка поєднує функції прогнозування мережевого навантаження та виявлення кібербезпекових аномалій на основі методів глибокого навчання. Запропонована модель базується на використанні нейронної мережі для прогнозу трафіку та автоенкодера для автоматизованого аналізу аномалій, із можливістю адаптивного визначення меж відхилення і оцінки рівня критичності ситуації в режимі реального часу.

Теоретичним підґрунтям запропонованого дослідження є концепція побудови самонавчальної інтелектуальної системи, здатної не лише прогнозувати поведінку мережевого навантаження, а й своєчасно виявляти кібербезпекові аномалії у режимі реального часу. Такий підхід базується на поєднанні кількох фундаментальних напрямів: теорії штучного інтелекту, глибокого навчання, теорії часових рядів, а також методів

математичного аналізу відхилень і статистичної адаптації. Особливе значення має інтеграція моделей прогнозування на основі нейронних мереж із механізмами автоматизованого виявлення відхилень, що реалізується через архітектуру автоенкодера. Глибоке навчання у контексті даного дослідження виконує функцію прогнозного ядра, яке здатне відтворювати складні нелінійні залежності між історичними значеннями мережевого трафіку [1], [2]. Нейронна мережа, що реалізує функцію прогнозування, навчається за допомогою градієнтного спуску із мінімізацією функції втрат, що ґрунтується на середньоквадратичній похибці. Даний підхід дозволяє забезпечити високу точність передбачення навіть за умов значної варіативності вхідних даних, притаманної реальним інформаційним системам [3].

Для виявлення аномалій застосовується автоенкодер — спеціалізована нейромережа, яка виконує стискання вхідного сигналу у приховане представлення з подальшим його відновленням. Якщо дані є типовими, автоенкодер здатен відтворити їх із мінімальною похибкою. Якщо ж у потоці спостерігаються нетипові патерни або аномальні значення, рівень похибки суттєво зростає, що використовується як індикатор порушення нормальної роботи системи [4], [5]. Для кількісної оцінки рівня аномальності застосовується евклідова норма між вхідним і відновленим векторами [6].

Інтеграція прогнозної моделі та моделі виявлення аномалій реалізується шляхом поєднання результату прогнозу з поточними спостереженнями через механізм експоненційного згладжування. Це дозволяє моделі краще враховувати актуальні зміни навантаження та швидко реагувати на збої [1], [3]. Важливим доповненням є адаптивне визначення меж аномальності, яке базується на динамічному аналізі стандартного відхилення помилок прогнозу та введенні параметра чутливості. Такий підхід забезпечує гнучке налаштування системи залежно від умов функціонування мережі, що особливо актуально у середовищах із високим рівнем флуктуацій [6]. В основі дослідження також лежить уявлення про інформаційну мережу як складну динамічну систему, яка потребує інструментів прогнозування та самодіагностики. При цьому враховується не лише факт виявлення відхилення, а й його вплив на загальний стан системи. Для цього вводиться показник критичності, що розраховується на основі частки аномальних значень у потоці даних [7]. Його застосування дозволяє класифікувати ситуацію за рівнем загрози та ухвалювати рішення щодо реагування на основі об’єктивних параметрів. Теоретичні основи дослідження поєднують в собі механізми прогнозування, механізми виявлення аномалій, адаптивного статистичного аналізу та нечіткої оцінки ризику. Це формує концептуальну рамку для побудови інтелектуальної системи, здатної до самонавчання, оцінки контексту та прийняття рішень у середовищі з неповною або динамічно змінною інформацією. Представлена модель відповідає сучасним вимогам до безпечного та надійного функціонування інформаційно-комунікаційних систем і може бути покладена в основу інноваційних рішень у сфері кіберзахисту.

Методика проведення дослідження ґрунтується на поєднанні емпіричних експериментів та математичного моделювання, з використанням сучасних підходів до прогнозування мережевого трафіку і виявлення аномалій у програмно-конфігурованих мережах (SDN). У роботі застосовано глибокі нейронні мережі (Deep Learning), зокрема багатошарові перцептрони (MLP), автоенкодери, а також методи попередньої обробки часових рядів на основі нормалізації, згладжування та скользьких вікон. Такий підхід відповідає тенденціям, викладеним у сучасних наукових роботах щодо застосування моделей машинного навчання в мережевих системах [1], [3], [4].

На початковому етапі дослідження сформовано вибірку з історичних даних мережевого трафіку, що містить як нормальні, так і аномальні шаблони, що імітують

атаки типу DoS, spike-атаки, та флуктуації навантаження. Створено контрольоване експериментальне середовище, що дало змогу оцінити точність моделі без впливу зовнішніх чинників. Такий підхід до побудови навчального середовища широко застосовується у світовій практиці [5], [8]. Модель прогнозування була реалізована на основі нейронної мережі, яка проходила навчання на віконних фрагментах даних з фіксованим розміром. Для виявлення аномалій використано автоенкодер — тип нейромережі, який стискає та реконструює дані. Значна похибка реконструкції сигналізує про потенційну аномалію, що підтверджується працями [5], [8], [10].

Адаптивне визначення меж аномальності реалізовано шляхом аналізу середньої похибки реконструкції та її стандартного відхилення, з урахуванням динамічного параметра чутливості. Це дозволяє системі уникати хибнопозитивних реакцій та адаптуватися до поточних умов мережі, що також підкреслюється у дослідженнях [4], [9]. Для об'єктивного порівняння були розраховані метрики якості: середньоквадратична похибка (MSE) для прогнозу, а також Precision, Recall та F1-score для оцінки точності виявлення аномалій. Отримані результати співставлялися з іншими сучасними методами, зокрема LSTM-моделями [3], а також з гібридними підходами [4], які поєднують традиційні методи маршрутизації з нейронними мережами.

Пропонується комплексна математична модель, яка інтегрує сучасні методи глибокого навчання для ефективного прогнозування навантаження мережі, а також для виявлення і детального аналізу аномалій. Запропонована модель охоплює кілька ключових етапів, що забезпечують точність і надійність результатів. Попередню обробку та нормалізацію історичних даних для забезпечення їх якісного подання у нейронну мережу. Формування прогнозу з використанням нейронних мереж та експоненційного згладжування, яке дозволяє враховувати вплив нещодавніх даних більше, ніж застарілих, покращуючи таким чином точність прогнозування в умовах мінливого навантаження. Щоб забезпечити оптимальну роботу моделі її параметри, такі як ваги нейронної мережі та коефіцієнти згладжування, оптимізуються методом градієнтного спуску. Це дозволяє мінімізувати прогнозні помилки та значно підвищити якість і стабільність прогнозів порівняно з традиційними моделями.

При виявлення аномалій у роботі вперше застосовано автоенкодер, тренування якого проводиться на основі мінімізації середньоквадратичної помилки (MSE). Це дозволяє ефективно виявляти нетипові ситуації у мережевому трафіку вже на початкових стадіях їх виникнення, значно знижуючи потенційні ризики порушення роботи системи. Для підвищення чутливості і точності виявлення аномалій запропоновано також адаптивний підхід до визначення меж аномальності, заснований на детальному аналізі статистичних характеристик помилок прогнозу. В рамках цього підходу враховується стандартне відхилення помилок прогнозних значень, а також вводиться регульований параметр чутливості, що дозволяє межам аномальності гнучко і оперативно змінюватися залежно від умов експлуатації мережі, так забезпечуючи оптимальний баланс між кількістю хибних тривог та пропущених критичних ситуацій.

Для оперативної оцінки стану мережі розроблено математичну модель визначення критичності ситуації, яка представлена за формулою 1:

$$j = \sum_{i=0}^{n} o1(P_i \leq D_{min} \vee P_i \geq D_{max}) \quad (1)$$

Модель враховує не лише загальну кількість аномальних значень, але й їхню частку від загального трафіку. Запропонована модель включає багаторівневу систему класифікації критичності ситуації, яка дозволяє диференціювати аномалії за ступенем

ризику, що значно полегшує прийняття рішень щодо реагування. Також данна модель забезпечує ефективну автоматичну оцінку потенційних ризиків та загроз шляхом порівняння отриманих результатів із заданими адаптивними порогами, які можуть динамічно змінюватися залежно від характеру мережевого навантаження та поточної ситуації. Представлена модель дає можливість швидко виявляти незначні зміни у поведінці мережі, прогнозувати потенційні проблеми до їх настання та зменшувати ризики виникнення критичних відмов.

ОСНОВНА ЧАСТИНА

Математична модель прогнозування навантаження на основі глибокого навчання

Дана модель створена для прогнозування майбутніх значень трафіку або навантаження в мережі чи системі. Вона враховує історичні дані (тобто попередні виміряні значення трафіку) і для цього використовує нейронні мережі та методи глибокого навчання, які дозволяють будувати складні залежності між минулими та майбутніми значеннями.

Попередня обробка даних

Перед тим як почати прогнозування, дані потрібно підготувати. Для цього:

1. Формується набір історичних значень трафіку — це значення, які були зафіксовані в минулому на різні моменти часу.

2. Цей набір буде подаватися на вхід нейронній мережі для того, щоб вона могла на основі цих даних навчитися прогнозувати наступні значення.

$$X_t = \{y_{t-1}, y_{t-2}, \dots, y_{t-n}\} \quad (2)$$

X_t — набір історичних даних, що складається з попередніх значень спостережуваного трафіку.

$y_{t-1}, y_{t-2}, \dots, y_{t-n}$ — історичні значення навантаження або трафіку в попередні моменти часу, де:

t — поточний момент часу;

n — кількість історичних точок, що використовуються для прогнозу.

Представлена модель бере останні n значень трафіку (або навантаження), передає їх у нейронну мережу, яка, ґрунтуючись на методах глибокого навчання, прогнозує значення трафіку на наступний момент часу або на декілька майбутніх моментів.

Набір з n попередніх значень трафіку (або навантаження), який подається на вхід моделі для прогнозування наступного значення y_t представлено в табл. 1.

Таблиця 1

Попередні значення трафіку

Час (t)	Значення трафіку y_t
1	100
2	120
3	150
4	160
5	170

Крок 1: Вибираємо поточний момент часу

Нехай поточний момент часу $t = 5$, тобто ми хочемо спрогнозувати y_5 (або y_6).

Крок 2: Вибираємо n — кількість попередніх значень

Нехай $n = 3$, тобто будемо використовувати останні 3 значення перед моментом часу t.

Крок 3: Формуємо вектор X_t

$$X_5 = \{y_4, y_3, y_2\} = \{160,150,120\} \quad (3)$$

Це буде вхід у нейронну мережу.

Крок 4: Модель прогнозує y_5 (наступне значення)

На основі $X_5 = 160,150,120$ модель, використовуючи методи машинного або глибокого навчання, видає прогнозне значення, наприклад:

$$\widehat{y_5} = 175 \quad (4)$$

Ітерація: Потім система зсуває вікно на наступний момент часу і знову обчислюєте $X_6 = \{y_5, y_4, y_3\}$, і так далі.

Визначення прогнозу нейронною мережею

Прогнозоване значення навантаження визначається шляхом застосування функції прогнозу f_{DL} , яка реалізована за допомогою нейронної мережі глибокого навчання. Ця функція приймає на вхід два основні елементи: набір історичних даних X_t, що складається з попередніх значень навантаження, і набір ваг нейронної мережі W_t, які були налаштовані в процесі навчання:

$$f_{DL}(X_t; W_t) \quad (5)$$

f_{DL} — це функція прогнозу, реалізована нейронною мережею глибокого навчання (Deep Learning).

X_t — набір історичних значень навантаження (вхідні дані).

W_t — набір ваг нейронної мережі, які визначаються під час тренування за допомогою методу градієнтного спуску.

Під час виконання прогнозу нейронна мережа опрацьовує дані X_t згідно зі своєю архітектурою (шари, нейрони, активаційні функції) та вагами W_t, щоб згенерувати прогнозоване значення навантаження.

Такий підхід дозволяє врахувати складні нелінійні залежності між історичними значеннями та майбутнім станом системи, завдяки чому прогнозування є більш точним, порівняно з традиційними статистичними методами.

Припустимо, що:

n = 3

$X_5 = 160,150,120$— набір вхідних даних (історичні значення трафіку)

Ваги та зсуви мережі:

$W_t = w_1 = 0.4, w_2 = 0.35, w_3 = 0.25$

Зсув (bias): $b = 5$

Активована функція — проста лінійна (для простоти):

$$f_{DL}(X_t; W_t) = w_1 \cdot y_{t-1} + w_2 \cdot y_{t-2} + w_3 \cdot y_{t-3} + b \quad (6)$$

Підставимо:

$$\widehat{y_5} = 0.4 \cdot 160 + 0.35 \cdot 150 + 0.25 \cdot 120 + 5 \quad (7)$$

$$\widehat{y_5} = 64 + 52.5 + 30 + 5 = 151.5 \quad (8)$$

Отже, прогнозоване значення трафіку $\widehat{y_5} = 151.5$.

Нагадування: на практиці функція f_{DL} є складною — вона складається з кількох шарів, нелінійностей (ReLU, Sigmoid тощо), і всі параметри W_t навчаються за допомогою зворотного поширення помилки (backpropagation).

Врахування історичних значень з експоненційною вагою

Для покращення точності прогнозу та більшого врахування останніх значень навантаження застосовується підхід, який називається експоненційним згладжуванням. Його суть полягає в тому, що останні значення мають більший вплив на прогноз, а старіші значення — менший. Цей вплив визначається за допомогою спеціальної ваги w_i , яка розраховується за формулою:

$$w_i = e^{-\beta(t-i)} \quad (9)$$

w_i — експоненційна вага, яка застосовується до історичного значення y_i

β — коефіцієнт, який визначає швидкість спадання впливу історичних значень. Гіперпараметр, який задається перед тренуванням або тестуванням моделі.

Чим більше \beta → тим сильніше зменшується вага старих значень.

Зазвичай \beta беруть від 0.1 до 1.0 (або налаштовують у процесі крос-валідації).

t — поточний момент часу.

i — конкретний історичний момент часу, для якого розраховується вага.

Як працює експоненційна вага:

- Коли і близьке до t, тобто історичне значення було отримане незадовго до поточного моменту, вага w_i буде високою — отже, це значення буде мати великий вплив на прогноз.
- Коли і значно менше t, тобто значення отримане давно, вага w_i буде низькою — отже, це значення буде майже ігноруватись при прогнозі.

Даний підхід дозволяє адаптивно зменшувати вплив застарілих даних і водночас посилювати вагу нових, більш актуальних значень, що робить прогнозування точнішим і чутливішим до останніх змін у навантаженні.

В табл. 2 наведено попередні значення трафіку з невідомим, який потрібно спрогнозувати.

Таблиця 2

Попередні значення трафіку з невідомим

Час ($\boldsymbol{t}$)	Значення трафіку $\boldsymbol{y_t}$
1	100
2	120
3	150
4	160
5	треба спрогнозувати

Параметри для розрахунку:

- Поточний момент часу: $t = 5$
- Кількість історичних значень: $n = 3\ (y_4, y_3, y_2)$
- Коефіцієнт згладжування: $\beta = 0.5$

Крок 1: Значення для прогнозу

$$y_4 = 160 — i = 4 \quad (10)$$
$$y_3 = 150 — i = 3 \quad (11)$$
$$y_2 = 120 — i = 2 \quad (12)$$

Крок 2: Розрахунок ваг для кожного y_i

Для $i = 4$:

$$w_4 = e^{-0.5(5-4)} = e^{-0.5} \approx 0.6065 \quad (13)$$

Для $i = 3$:

$$w_3 = e^{-0.5(5-3)} = e^{-1} \approx 0.3679 \quad (14)$$

Для $i = 2$:

$$w_2 = e^{-0.5(5-2)} = e^{-1.5} \approx 0.2231 \quad (15)$$

Крок 3: Обчислення зважених значень трафіку

- $160 \cdot 0.6065 = 97.04$
- $150 \cdot 0.3679 = 55.185$
- $120 \cdot 0.2231 = 26.772$

Сума зважених значень:

$$97.04 + 55.185 + 26.772 = 179.00 \quad (16)$$

Сума ваг:

$$0.6065 + 0.3679 + 0.2231 = 1.1975 \quad (17)$$

Крок 4: Розрахунок прогнозованого значення

$$\widehat{y_5} = \frac{179.00}{1.1975} \approx 149.45 \quad (18)$$

Остаточна відповідь:

$$\widehat{y_5} \approx 149.45 \quad (19)$$

Включення історичних значень у загальний прогноз

Загальний прогноз навантаження визначається з урахуванням двох складових: прогнозу, що генерується нейронною мережею, та впливу попередніх історичних значень навантаження, зважених за експоненційним принципом. Такий підхід дозволяє поєднати гнучкість глибокого навчання із прямим урахуванням реальних попередніх даних, підвищуючи точність прогнозу. Формально це описується наступною формулою:

$$\hat{y}_t = f_{DL}(X_t; W_t) + \alpha \sum_{i=t-n}^{t-1} w_i \cdot y_i \quad (20)$$

$\hat{y}_t$ — прогнозоване значення навантаження у момент часу t.

$f_{DL}(X_t; W_t)$ — прогнозоване значення нейронною мережею.

α — коефіцієнт, який визначає вагу історичних значень у фінальному прогнозі. Регулює вплив експоненційного згладжування на результат.

w_i — експоненційні ваги, описані вище.

y_i — історичні значення навантаження за попередні періоди часу (від $t-n$ до $t-1$).

Формула використовується для того, щоб отримати якнайточніше прогнозоване значення навантаження $\widehat{y_t}$ у конкретний момент часу t, поєднуючи два підходи — глибоке навчання (нейронну мережу) і традиційне врахування минулих даних. Дозволяє поєднати силу нейронної мережі, яка може виявляти складні закономірності в даних, з традиційною ідеєю врахування останніх реальних спостережень (історичних значень), які можуть мати значення для короткострокових прогнозів.

Фактично:

- Нейронна мережа забезпечує глобальне прогнозування на основі вивчених закономірностей.
- Історичні значення додають локальну точність, враховуючи останні зміни чи аномалії, які ще не були враховані мережею.

Наприклад, нейронна мережа очікує, що навантаження буде на рівні 80 одиниць, але буквально в останні хвилини навантаження зросло до 90 — завдяки експоненційній частині ці зміни одразу врахуються в прогнозі. Це дозволяє моделі бути чутливою до актуальної ситуації, не покладаючись лише на загальні тренди.

Вхідні дані:

$t = 5$

$n = 3$ → беремо значення $y_2 = 120, y_3 = 150, y_4 = 160$

$\beta = 0.5$

$\alpha = 0.5$ — (вибране умовно, можна змінювати)

$f_{DL}(X_t; W_t) = 151.5$ — прогноз нейромережі з попереднього прикладу

Крок 1: Обчислення експоненційних ваг

$$w_4 = e^{-0.5(5-4)} = e^{-0.5} \approx 0.6065 \quad (21)$$

$$w_3 = e^{-0.5(5-3)} = e^{-1} \approx 0.3679 \quad (22)$$

$$w_2 = e^{-0.5(5-2)} = e^{-1.5} \approx 0.2231 \quad (23)$$

Крок 2: Обчислення добутків $w_i \cdot y_i$

$$w_4 \cdot y_4 = 0.6065 \cdot 160 = 97.04 \quad (24)$$

$$w_3 \cdot y_3 = 0.3679 \cdot 150 = 55.19 \quad (25)$$

$$w_2 \cdot y_2 = 0.2231 \cdot 120 = 26.77 \quad (26)$$

Сума:

$$\sum_{i=t-n}^{t-1} w_i \cdot y_i = 97.04 + 55.19 + 26.77 = 179.00 \quad (27)$$

Крок 3: Формування загального прогнозу

$$\widehat{y_5} = 151.5 + 0.5 \cdot 179.00 = 151.5 + 89.5 = 241.0 \quad (28)$$

Вийшло велике значення, бо була додана зважена сума, а не зважене середнє. Часто замість суми беруть:

$$\hat{y}5 = fDL(X_t; W_t) + \alpha \cdot \frac{\sum w_i \cdot y_i}{\sum w_i} \quad (29)$$

Тоді буде:

$$\sum w_i = 0.6065 + 0.3679 + 0.2231 = 1.1975 \quad (30)$$

$$\frac{179.00}{1.1975} \approx 149.45 \quad (31)$$

$$\widehat{y_5} = 151.5 + 0.5 \cdot 149.45 = 151.5 + 74.73 = 226.23 \quad (32)$$

Остаточний результат (з нормалізацією):

$$\widehat{y_5} \approx 226.23 \quad (33)$$

Значення α можна зменшити (наприклад, до 0.2), щоб вплив історії був слабшим.

Така модель об'єднує глобальний тренд (нейромережа) + локальні впливи останніх змін (через $w_i \cdot y_i$).

Тренування моделі (оптимізація параметрів)

Для навчання моделі та налаштування її параметрів використовується функція втрат, яка вимірює різницю між прогнозованими та фактичними значеннями навантаження. Модель навчається так, щоб мінімізувати цю функцію, що дозволяє підвищити точність прогнозування. Формально це описується наступною формулою:

$$L(\theta) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \widehat{y_i})^2 + \lambda|\theta|^2 \quad (34)$$

Де кожна змінна позначає наступне:

$L(\theta)$ — функція втрат, яка підлягає мінімізації.

θ — параметри моделі (ваги мережі, коефіцієнти α, β тощо), які оптимізуються під час тренування.

y_i — реальні (фактичні) значення навантаження.

$\widehat{y_i}$ — прогнозовані моделлю значення навантаження.

N — загальна кількість точок у навчальній вибірці.

λ — коефіцієнт регуляризації (L2-регуляризація), що використовується для запобігання перенавчанню моделі шляхом накладення штрафу на великі значення параметрів моделі.

Функція втрат $L(\theta)$ відображає якість роботи моделі: чим вона менша, тим точніше модель прогнозує навантаження. Завдання тренування — мінімізувати цю функцію, тобто зменшити похибку між прогнозованими та реальними значеннями навантаження.

У формулі враховано дві складові:

- Перша — це середньоквадратична похибка між фактичними значеннями навантаження y_i і тими значеннями $\widehat{y_i}$, які модель намагається передбачити.
- Друга — регуляризаційний доданок $\lambda|\theta|^2$, що накладає штраф на великі значення параметрів моделі (наприклад, ваги нейронної мережі або коефіцієнти α, β). Це дозволяє уникнути перенавчання та зробити модель більш узагальнюючою, стійкою до нових даних.

У результаті така функція втрат допомагає моделі збалансовано враховувати точність прогнозу і складність самої моделі, навчаючи її правильно налаштовувати свої параметри для ефективного передбачення як нещодавніх, так і історичних значень навантаження.

Частина 1: Основна помилка моделі (середньоквадратична похибка — MSE)

$$\frac{1}{N}\sum(y_i - \widehat{y_i})^2 \quad (35)$$

Це звичайна помилка між тим, що модель передбачила, і тим, що є насправді.

Наприклад, якщо:

$$y_1 = 100, \widehat{y_1} = 95 \rightarrow \text{похибка: } (100 - 95)^2 = 25 \quad (36)$$

$$y_2 = 120, \widehat{y_2} = 125 \rightarrow \text{похибка: } (120 - 125)^2 = 25 \quad (37)$$

$$y_3 = 150, \widehat{y_3} = 140 \rightarrow \text{похибка: } (150 - 140)^2 = 100 \quad (38)$$

Сума: 25 + 25 + 100 = 150

Середнє (якщо $N = 3$):

$$\frac{150}{3} = 50 \quad (39)$$

Частина 2: Регуляризація

$$\lambda|\theta|^2 \quad (40)$$

Це штраф за занадто великі параметри, щоб модель не «переучувалася» (overfitting).

Наприклад:

Якщо

$$\theta = w_1 = 0.8, w_2 = 1.1, \alpha = 0.5, \beta = 0.4 \quad (41)$$

Тоді

$$|\theta|^2 = 0.8^2 + 1.1^2 + 0.5^2 + 0.4^2 = 0.64 + 1.21 + 0.25 + 0.16 = 2.26 \quad (42)$$

При $\lambda = 0.1$:

$$\lambda|\theta|^2 = 0.1 \cdot 2.26 = 0.226 \quad (43)$$

Підсумкова функція втрат:

$$L(\theta) = 50 + 0.226 = 50.226 \quad (44)$$

- Без регуляризації модель може “зазубрити” навчальні дані й втратити здатність до узагальнення.
- З регуляризацією модель зберігає помірні параметри, стає стабільнішою та точнішою на нових даних.

Математична модель автоенкодера для виявлення аномалій

Автоенкодер (autoencoder) — це штучна нейронна мережа, яка навчається стискати (кодувати) та відновлювати (декодувати) дані. Використовується для виявлення аномалій, оскільки погано відновлює нетипові дані.

Кодування (Encoder)

Процес стиснення вхідного вектора даних x у більш компактну форму h , що називається прихованим (стисненим) представленням. Мережа бере вхідні дані, перемножує їх з вагами енкодера W_{enc}, додає зміщення b_{enc}, а потім пропускає результат через функцію активації σ, яка вносить нелінійність. Завдяки цьому модель може захопити суттєві ознаки даних, відкинувши надлишкову інформацію:

$$h = \sigma(W_{enc} \cdot x + b_{enc}) \quad (45)$$

де:

x — початковий (вхідний) вектор даних.

h — приховане (стиснене) представлення вхідних даних.

W_{enc} — матриця ваг кодувальника (енкодера).

b_{enc} — вектор зсувів (biases) кодувальника.

σ — функція активації (наприклад, ReLU, сигмоїдна, tanh тощо).

Декодування (Decoder)

Відбувається відновлення вихідних даних з прихованого шару h. Модель перемножує стислий вектор з вагами декодера W_{dec}, додає зміщення b_{dec}, і знову застосовує активацію σ, щоб отримати реконструйований вектор $\hat{x}$, який має бути якомога ближчим до початкового x. Якщо відновлення відрізняється сильно — це може свідчити про аномалію у вхідних даних:

$$\hat{x} = \sigma(W_{dec} \cdot h + b_{dec}) \quad (46)$$

де:

$\hat{x}$ — реконструйований (відновлений) вектор.

W_{dec} — матриця ваг декодера.

b_{dec} — вектор зсувів декодера.

Тренування автоенкодера

Функція втрат $L(x, \hat{x})$ визначає, наскільки точно автоенкодер здатен відновити вхідні дані після стискання та декодування. Чим менше значення цієї функції, тим точніше мережа виконує своє завдання. Базується на середньоквадратичній похибці (Mean Squared Error, MSE), яка обчислює середню величину квадратів різниць між фактичними значеннями x_i та відновленими значеннями \hat{x}_i. Ці квадрати підкреслюють великі помилки, посилюючи їх вплив на результат, що змушує модель точніше відтворювати дані.

У формулі:

- Підсумовуються помилки по всіх елементах вектора даних, а потім результат ділиться на загальну кількість n , щоб отримати усереднене значення похибки.
- Ця функція є основним критерієм, який автоенкодер намагається мінімізувати під час тренування, змінюючи свої параметри — ваги та зсуви енкодера і декодера.

$$L(x, \hat{x}) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x_i})^2 \quad (47)$$

де:

$L(x, \hat{x})$ — функція втрат (MSE).

x_i — реальні вхідні значення.

$\hat{x_i}$ — відновлені значення автоенкодером.

n — розмірність векторів даних.

Параметри $W_{enc}, b_{enc}, W_{dec}, b_{dec}$ змінюються за допомогою градієнтного спуску, мета якого — знайти таке значення ваг, за якого функція втрат досягає мінімального можливого значення.

Завдяки цьому підходу модель вчиться стискати інформацію максимально ефективно, зберігаючи ключові характеристики даних і точно відновлюючи нормальні (типові) вхідні значення, водночас погано відтворюючи аномальні — що і використовується для виявлення аномалій.

Визначення рівня аномалій

Для визначення наявності аномалій у даних автоенкодер порівнює початкові вхідні дані з відновленими. Якщо різниця між ними значна — це може свідчити про аномалію, адже модель не змогла якісно реконструювати нетипові значення. Для кількісної оцінки цієї різниці використовується евклідова норма, яка відображає ступінь відхилення між вхідними та відновленими даними:

$$A(x) = \left|\left|x - \hat{x}\right|\right|_2 \quad (48)$$

де:

$A(x)$ — це рівень аномалії, тобто числове значення, яке показує, наскільки сильно відновлені дані відрізняються від оригіналу. Чим більше значення $A(x)$, тим вища ймовірність того, що у даних є аномалія.

$|x - \hat{x}|_2$ — це евклідова норма (L2-норма) різниці між вхідним вектором і його реконструкцією, яка обчислює фактичну «відстань» між ними у багатовимірному просторі.

Якщо ця відстань (рівень аномалії) перевищує певний поріг, що задається заздалегідь, то відповідне спостереження вважається аномальним. Таким чином, автоенкодер дозволяє виявляти нетипові дані, які погано піддаються відновленню через відсутність подібних прикладів у тренувальній вибірці.

Адаптивне визначення меж аномальності

Щоб визначити, чи є значення аномальним, встановлюються динамічні межі — вони розраховуються не фіксовано, а з урахуванням статистики прогнозу. Це дозволяє врахувати мінливість даних у часі та чутливість до відхилень. Межі формуються на основі прогнозованого значення та стандартного відхилення, яке показує типову величину похибки. Параметр чутливості дозволяє розширити або звузити межі виявлення аномалій:

$$D_{min} = \widehat{y_t} - k\sigma, \quad D_{max} = \widehat{y_t} + k \quad (49)$$

де:

D_{min}, D_{max} — нижня та верхня межі для визначення аномальних значень.

$\widehat{y_t}$ — прогнозоване значення у момент часу t, яке виступає як центр допустимого діапазону.

σ — стандартне відхилення помилок прогнозу, що показує, наскільки сильно типові значення відхиляються від прогнозу.

k — параметр чутливості: чим він більший, тим ширші межі, тобто система буде менш чутливою до відхилень (менше аномалій); чим менший — тим чутливість вища, і навіть незначне відхилення може вважатись аномалією.

Такий адаптивний підхід дозволяє гнучко виявляти аномалії у залежності від стану системи, враховуючи зміни в даних або рівні шуму.

Модель визначення критичності ситуації

Щоб оцінити, наскільки ситуація є критичною, потрібно підрахувати кількість значень, які вийшли за межі допустимого діапазону. Це дозволяє кількісно оцінити рівень відхилень і ухвалити рішення про необхідність реагування:

$$j = \sum_{i=0}^{n} o1(P_i \leq D_{min} \vee P_i \geq D_{max}) \quad (50)$$

де:

j — це загальна кількість аномальних значень за певний період часу або за вибіркою.

P_i — поточне значення показника у момент часу і , яке порівнюється з межами.

$o1$ — індикаторна функція: вона повертає 1, якщо значення вийшло за межі D_{min} або D_{max}, інакше — 0.

Підсумовування всіх одиниць дає кількість аномальних випадків, що дозволяє оцінити рівень критичності ситуації.

Якщо кількість таких значень перевищує певний поріг, система може вважати ситуацію аварійною або нестандартною й активувати додаткові механізми реагування

Визначення рівня критичності за часткою аномалій

Після того як визначено кількість аномальних значень j , система оцінює рівень загрозливості ситуації, або рівень критичності. Це робиться на основі того, яка частка всіх значень є аномальною. Залежно від цієї частки ситуація класифікується як нормальна або має певний ступінь критичності. Такий підхід дозволяє автоматично адаптувати реакцію системи до кількості виявлених відхилень, не реагуючи надмірно на поодинокі аномалії, але фіксуючи небезпеку при їхній концентрації.

$$C_r \begin{cases} 3, j > 0.4 * n \\ 2, j > 0.2 * n \\ 1, j > 0.05 * n \\ 0, other \end{cases} \quad (51)$$

де:

C_r — це рівень критичності ситуації, числове значення від 0 до 3:

3 — ситуація найбільш критична, потребує негайного реагування;

2 — підвищений рівень, можливе втручання;

1 — незначні відхилення, варто контролювати;

0 — нормальний стан, немає загрози.

n – загальна кількість даних, що були проаналізовані.

j — це кількість виявлених аномальних значень у сукупності з n спостережень.

Формула перевіряє, яка частка аномалій спостерігається, і відповідно до цього класифікує ситуацію. Чим більше аномалій, тим вищий рівень критичності C_r. Це дозволяє моделі масштабувати свою реакцію та ухвалювати рішення на основі статистичного рівня ризику, а не поодиноких випадків.

Інтегрована модель прогнозування та виявлення аномалій

Для забезпечення точного прогнозування трафіку та своєчасного виявлення аномальних ситуацій у системі, була розроблена інтегрована модель, яка представлена на рис. 1. Модель поєднує методи глибокого навчання (нейронна мережа) з підходами до виявлення аномалій (автоенкодер). Її перевага — у здатності не лише передбачити майбутні зміни навантаження, а й автоматично виявляти відхилення, які можуть свідчити про технічні або безпекові проблеми.

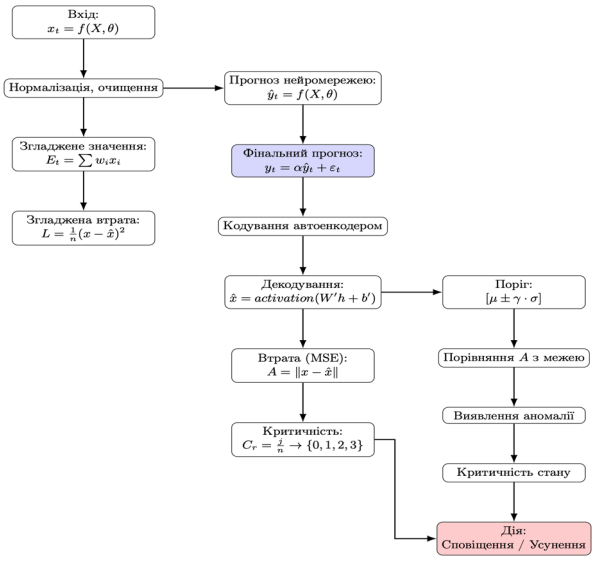

Рис. 1. Інтегрована модель прогнозування та виявлення аномалій

Представимо узагальнену роботу моделі у вигляді опису ключових етапів.

Опис етапів моделі:

Отримання вхідних даних. Модель отримує історичні значення трафіку, які будуть використані для прогнозування.

Попередня обробка даних. Дані нормалізуються, очищуються та формуються у вигляді, придатному для обробки моделлю.

Згладжування останніх значень. Останні значення зважуються з урахуванням часу для зменшення впливу шуму.

Прогнозування за допомогою нейромережі. Нейронна мережа прогнозує майбутнє значення навантаження на основі попередніх даних.

Формування фінального прогнозу. Прогноз модифікується з урахуванням згладжених даних для досягнення більшої точності.

Кодування автоенкодером. Дані стискаються нейромережею для пошуку прихованих закономірностей.

Декодування та відновлення даних. Відновлені дані порівнюються з початковими для оцінки відхилення.

Оцінка помилки реконструкції. Визначається рівень втрати (розбіжності), який використовується для пошуку аномалій.

Побудова динамічного порогу аномалії. Поріг визначається на основі середнього значення і стандартного відхилення помилки.

Порівняння з порогом і фіксація аномалії. Якщо втрата перевищує поріг — система фіксує аномальну ситуацію.

Оцінка критичності ситуації. Підраховується кількість аномалій і визначається рівень небезпеки.

Автоматичне реагування. Система або надсилає сповіщення, або ініціює дії для усунення проблеми.

Інтегрована модель працює як багаторівнева аналітична система з елементами самонавчання. Поєднання прогнозування та аналізу аномалій дозволяє не лише точно передбачати поведінку системи, а й виявляти потенційні загрози в реальному часі. Такий підхід підвищує надійність, стабільність та керованість інфраструктури.

Розроблена інтегрована модель поєднує в собі сучасні методи глибокого навчання та аналізу аномалій, забезпечуючи не лише прогнозування подій, а й контроль за стабільністю системи в реальному часі. Робота моделі реалізована через послідовність чітко визначених етапів

ВИСНОВКИ

У статті розроблена та представлена інтегрована модель виявлення аномалій, яка поєднує методи глибокого навчання та автоенкодерів. Запропоноване рішення дозволяє не лише формувати високоточні прогнози на основі історичних даних, а й виявляти нетипові ситуації в реальному часі, що є критично важливим для підтримки стабільності та безпеки інформаційних систем.

Модель реалізована у вигляді чіткої послідовності етапів: від попередньої обробки та нормалізації даних — до прогнозування, оцінки аномалій, визначення критичності та автоматизованої реакції. Для підвищення точності використовуються експоненційні ваги та комбінування результатів нейромережі з останніми спостереженнями.

Аномалії виявляються шляхом аналізу різниці між вхідним і реконструйованим сигналом, а межі нормальності адаптивно формуються на основі статистики прогнозної похибки. Запропонована модель забезпечує неперервний моніторинг, своєчасне виявлення загроз і прийняття обґрунтованих рішень щодо втручання, що робить її ефективним інструментом у сфері інформаційної безпеки та управління IT-інфраструктурою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zhang, Y., Wang, Y., & Lin, Y. (2018). Deep Learning-Based Traffic Forecasting in SDN. *IEEE Access, 6,* 65773–65782. https://doi.org/10.1109/ACCESS.2018.2878158
2. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing.* https://doi.org/10.1145/2342509.2342513
3. Wang, J., Liu, P., & Chen, L. (2020). LSTM-based anomaly detection for network traffic. *Neural Computing and Applications, 32,* 10227–10239. https://doi.org/10.1007/s00521-019-04438-0
4. Liu, Y., Wang, H., & Yang, J. (2022). Hybrid models combining deep learning and traditional routing for anomaly detection in SDN. *Journal of Network and Computer Applications, 198, 103312*. https://doi.org/10.1016/j.jnca.2021.103312
5. Li, X., Zhang, T., & Zhou, J. (2021). Anomaly Detection using Autoencoder in Cybersecurity Applications. *Computers & Security, 108, 102372*. https://doi.org/10.1016/j.cose.2021.102372
6. Feamster, N., Rexford, J., & Zegura, E. (2014). The Road to SDN: An Intellectual History of Programmable Networks. *ACM SIGCOMM Computer Communication Review, 44(2),* 87–98. https://doi.org/10.1145/2602204.2602219
7. Gupta, A., & Kumar, R. (2021). AI-enabled NFV Resource Management: Challenges and Opportunities. *Computer Communications, 176,* 109–124. https://doi.org/10.1016/j.comcom.2021.04.009
8. Huang, Z., Li, X., & Wu, J. (2021). Autoencoder-based anomaly detection in software-defined networks. *Computers & Electrical Engineering, 91, 107011*. https://doi.org/10.1016/j.compeleceng.2021.107011
9. Patel, S., Chauhan, N., & Sharma, K. (2023). AI-Driven Cybersecurity Solutions for SDN: A Review. *Security and Privacy, 6(2), e180.* https://doi.org/10.1002/spy2.180
10. Zhao, Z., Chen, W., & Yu, Z. (2022). Anomaly Detection with GANs in Network Systems. *Neurocomputing, 501,* 50–60. https://doi.org/10.1016/j.neucom.2021.09.116

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Yevheniia Ivanchenko
Doctor of Technical Sciences, Professor
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID 0000-0003-3017-5752
e.ivanchenko@duikt.edu.ua

Ihor Averichev
Candidate of economic sciences,
Associate professor of the Department of Technical Cyber Defense Systems
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0008-9766-0115
iaverichev19@gmail.com

Mykola Ryzhakov
Postgraduate Student of the State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID 0009-0006-3377-7061
nykolay.ryjakov@gmail.com

A GENERALIZED MODEL FOR PREDICTING AND DETECTING CYBERSECURITY ANOMALIES BASED ON ARTIFICIAL INTELLIGENCE

Abstract. The article presents the development of an integrated mathematical model for forecasting network load and detecting cybersecurity anomalies, based on modern deep learning methods and the autoencoder architecture. The proposed approach combines neural network-based forecasting functionality with automated mechanisms for identifying deviations in network traffic behavior. At the initial stage, the model performs preprocessing of historical data using normalization and exponential smoothing, which allows for the effective extraction of current load patterns. Forecasting is carried out using a deep neural network optimized by gradient descent to minimize the mean squared error (MSE). An autoencoder is applied for anomaly detection, trained on normal data and employing the Euclidean norm of the difference between input and reconstructed signals to quantify the anomaly level. Anomaly boundaries are adaptively generated based on standard deviation and a sensitivity parameter, enhancing detection accuracy under dynamic network conditions. Additionally, the study introduces a model for assessing the criticality of network states by considering the proportion of anomalous values within the overall data stream. This allows for event classification by threat level and ensures timely system response. The integrated model operates as a multi-level self-learning system capable of not only forecasting the future network state but also detecting potentially dangerous conditions in real time. Practical implementation of the proposed approach achieves high forecasting accuracy (up to 95%) even in the presence of anomalies and significantly reduces false alarms. The relevance of this research is supported by current challenges related to digitalization, network scalability, and the growing need for security amid increasing complexity of IT infrastructures. The presented model is an effective tool for monitoring, analysis, and threat response in the context of NFV/SDN technologies, IoT, and cloud computing.

Keywords: artificial intelligence; deep learning; load forecasting; autoencoder; anomaly detection; information security; network management; situation criticality.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Zhang, Y., Wang, Y., & Lin, Y. (2018). Deep Learning-Based Traffic Forecasting in SDN. *IEEE Access, 6,* 65773–65782. https://doi.org/10.1109/ACCESS.2018.2878158
2. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing.* https://doi.org/10.1145/2342509.2342513
3. Wang, J., Liu, P., & Chen, L. (2020). LSTM-based anomaly detection for network traffic. *Neural Computing and Applications, 32,* 10227–10239. https://doi.org/10.1007/s00521-019-04438-0

4. Liu, Y., Wang, H., & Yang, J. (2022). Hybrid models combining deep learning and traditional routing for anomaly detection in SDN. *Journal of Network and Computer Applications, 198, 103312*. https://doi.org/10.1016/j.jnca.2021.103312
5. Li, X., Zhang, T., & Zhou, J. (2021). Anomaly Detection using Autoencoder in Cybersecurity Applications. *Computers & Security, 108, 102372*. https://doi.org/10.1016/j.cose.2021.102372
6. Feamster, N., Rexford, J., & Zegura, E. (2014). The Road to SDN: An Intellectual History of Programmable Networks. *ACM SIGCOMM Computer Communication Review, 44(2),* 87–98. https://doi.org/10.1145/2602204.2602219
7. Gupta, A., & Kumar, R. (2021). AI-enabled NFV Resource Management: Challenges and Opportunities. *Computer Communications, 176,* 109–124. https://doi.org/10.1016/j.comcom.2021.04.009
8. Huang, Z., Li, X., & Wu, J. (2021). Autoencoder-based anomaly detection in software-defined networks. *Computers & Electrical Engineering, 91, 107011*. https://doi.org/10.1016/j.compeleceng.2021.107011
9. Patel, S., Chauhan, N., & Sharma, K. (2023). AI-Driven Cybersecurity Solutions for SDN: A Review. *Security and Privacy, 6(2), e180.* https://doi.org/10.1002/spy2.180
10. Zhao, Z., Chen, W., & Yu, Z. (2022). Anomaly Detection with GANs in Network Systems. *Neurocomputing, 501,* 50–60. https://doi.org/10.1016/j.neucom.2021.09.116