Кафедра **інформаційно-комунікаційних технологій**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до бакалаврської кваліфікаційної роботи на тему:

Дослідження нейронних мереж для прогнозування аномалій у великих масивах телекомунікаційних даних

Студентка групи ТР-42 Ващук А.А.
(шифр, прізвище та ініціали)

Керівник роботи **(Пелех Н.В.)**

Консультант **(Корж Г.І.)**

Завідувач кафедри **Климаш М. М.**

“____”_____ 2025 р.

Форма № У-9.01

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

(назва ВЗО)

Інститут **ІКТЕ** Кафедра **ІКТ**

Напрямок підготовки **172 «Телекомунікації та радіотехніка»**

ЗАТВЕРДЖУЮ:

Зав. кафедри інформаційно-комунікаційних технологій

д.т.н., проф. Климаш М.М.

«_____» _____ 2025 р.

З А В Д А Н Н Я

на бакалаврську кваліфікаційну роботу студентці

Ващук Анастасії Анатоліївні

(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження нейронних мереж для прогнозування аномалій у великих масивах телекомунікаційних даних затверджена наказом по інституту від « 17» квітня 2025 р. № 1395-4-08

2. Термін здачі студентом закінченої роботи _____

3. Вихідні дані до роботи *нейронні мережі, метрики оцінки моделей, особливості телекомунікаційних даних, прогнозування аномалій LSTM, заходи охорони праці при роботі за КТ*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1. Дослідження архітектур нейронних мереж для задач виявлення аномалій

2. Дослідження ефективності моделей нейронних мереж

3. Аналіз методів оброблення великих телекомунікаційних даних

4. Розробка моделі прогнозування аномалій на основі LSTM-мережі

5. Реалізація моделі виявлення аномалій та оцінка її ефективності

6. Розробка заходів по охороні праці

5. Перелік графічного матеріалу (з точним зазначенням назв слайдів)

1. Архітектура нейронних мереж

2. Телекомунікаційна система передавання даних

3. Аналіз великих даних

4. Структура нейрона моделі

5. Перелік параметрів традиційної моделі

6. Зміни втрат під час навчання та тестування

7. Порівняння передбачень моделей LTSM та ARIMA

8. Виявлення аномалій користувацького енергоспоживання

6. Консультанти по проекту (роботи), із зазначенням розділів проекту, що стосуються їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Технічний	***Пелех Н.В.***		
Охорона праці	***Корж Г.І.***		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів роботи	Термін виконання етапів роботи	Прим.
1.	Аналіз літературних джерел	30.03.2025-05.04.2025	
2.	Дослідження архітектур нейронних мереж для задач виявлення аномалій	06.04.2025-10.04.2025	
3.	Дослідження ефективності моделей нейронних мереж	11.04.2025-15.04.2025	
4.	Аналіз методів оброблення великих телекомунікаційних даних	16.04.2025-20.04.2025	
5.	Розробка моделі прогнозування аномалій на основі LSTM-мережі	21.04.2025-25.04.2025	
6.	Реалізація моделі виявлення аномалій та оцінка її ефективності	26.04.2025-30.04.2025	
7.	Аналіз отриманих результатів та корекція моделі	1.05.2025-3.05.2025	
8.	Розробка заходів з охорони праці	4.05.2025 – 6.05.2025	
9.	Оформлення графічного матеріалу	10.05.2025	
10.	Оформлення пояснювальної записки	15.05.2025	

Студент-дипломник _____
(підпис)

Керівник роботи _____
(підпис)

Anastasia Vashchuk, Nazar Pelekh (supervisor). Investigation of Neural Networks for Anomaly Prediction in Large-Scale Telecommunication Data Sets. Bachelor's thesis. - Lviv Polytechnic National University, Lviv, 2025.

Extended abstract

In today's world, communication infrastructure is a vital component of the digital society, ensuring continuous exchange of information between millions of devices. Against the backdrop of rapidly growing volumes of transmitted data and complex network structures, the likelihood of anomalies that may indicate system failures, cyberattacks, or unauthorized use of resources is increasing. Traditional methods for detecting such anomalies often cannot process large volumes of data in real-time and do not adapt to new types of anomalies. In this regard, the application of artificial intelligence, particularly neural networks, is gaining particular relevance.

Since deep neural models can learn from large volumes of data, they can detect complex nonlinear dependencies and unusual patterns that classical algorithms cannot detect. The implementation of such approaches in the telecommunications sector can not only increase the accuracy of anomaly detection but also provide early prediction, which is extremely important for preventing failures and ensuring network stability. Thus, the study of neural networks in the context of communication data processing is an important step toward creating a new generation of intelligent network surveillance and protection systems.

Against the backdrop of increasing demands for security and efficiency of communication systems, methods capable of operating in conditions of high dynamics and data changes require special attention. Neural networks, especially recurrent and convolutional networks, demonstrate great potential for adaptation to new models of network behavior, which allows them to automatically adapt to changing conditions and detect previously unknown threats. Their implementation contributes to the creation of a more flexible and resilient analytical infrastructure capable of detecting complex scenarios of anomalous activity at an early stage. In combination with data preprocessing methods such as normalization, clustering, and dimensionality reduction, neural networks can not only improve anomaly detection but also reduce the number of false positives. This makes them a key tool for building modern systems for intelligent analysis of telecommunications traffic [1-5].

The purpose of the bachelor's qualification work is to develop and research effective methods for detecting and predicting anomalies in large volumes of telecommunication data using neural networks.

Achieving the set goal is carried out by solving the following tasks:

1) analysis of the effectiveness of neural network models;
2) analysis of methods for processing large telecommunication data;
3) research of neural network architectures for anomaly detection tasks;
4) development of an anomaly prediction model based on the LSTM network;
5) research and analysis of modeling results.

Study object - processing of telecommunication data using artificial intelligence.

Study subject – The neural network models and methods for their training for detecting and predicting anomalous events in big telecommunication data.

Study methods - The methods of statistical and intellectual data analysis.

The first chapter presents the theoretical foundations, architecture, operating principles, and performance metrics of neural networks in anomaly detection tasks.

The second chapter examines the sources, structure, and processing characteristics of telecommunication data, and demonstrates the relevance of using neural networks for analyzing such data.

In the third chapter, an LSTM-based model for forecasting abnormal consumption was implemented and tested, and the results were analyzed and compared with traditional methods.

The fourth chapter analyzes potential hazards and harmful factors in computer work, and proposes protection methods, preventive measures, and occupational safety practices.

Keywords: neural networks, anomalies, telecommunication data, forecasting, artificial intelligence.

References

1. M. Hou and X. Han, "Constructive Approximation to Multivariate Function by Decay RBF Neural Network," in *IEEE Transactions on Neural Networks*, vol. 21, no. 9, pp. 1517-1523, Sept. 2010, doi: 10.1109/TNN.2010.2055888.

2. J. Suárez-Varela *et al*., "Graph Neural Networks for Communication Networks: Context, Use Cases and Opportunities," in *IEEE Network*, vol. 37, no. 3, pp. 146-153, May/June 2023, doi: 10.1109/MNET.123.2100773.

3. M. Hao *et al*., "Artificial Neural Network-Based Approach to Modeling Energy Bands of GaN-Based Heterojunction Materials," *2023 International Conference on High Performance Big Data and Intelligent Systems (HDIS)*, Macau, China, 2023, pp. 71-76, doi: 10.1109/HDIS60872.2023.10499489.

4. J. B. P. Matos, E. B. de Lima Filho, I. Bessa, E. Manino, X. Song and L. C. Cordeiro, "Counterexample Guided Neural Network Quantization Refinement," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 4, pp. 1121-1134, April 2024, doi: 10.1109/TCAD.2023.3335313.

5. C. H. Park, "Anomaly Pattern Detection on Data Streams," *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Shanghai, China, 2018, pp. 689-692, doi: 10.1109/BigComp.2018.00127.

Ващук А.А., Пелех Н.В. (керівник). Дослідження нейронних мереж для прогнозування аномалій у великих масивах телекомунікаційних даних. Бакалаврська робота. - Національний університет "Львівська політехніка", Львів, 2025.

Анотація

У сучасному світі комунікаційна інфраструктура є життєво важливим компонентом цифрового суспільства, що забезпечує безперервний обмін інформацією між мільйонами пристроїв. На тлі стрімко зростаючих обсягів переданих даних та складних мережевих структур зростає ймовірність аномалій, які можуть свідчити про системні збої, кібератаки або несанкціоноване використання ресурсів. Традиційні методи виявлення таких аномалій часто не здатні обробляти великі обсяги даних у режимі реального часу та не адаптуються до нових типів аномалій. У зв'язку з цим застосування штучного інтелекту, зокрема нейронних мереж, набуває особливої актуальності. Оскільки глибокі нейронні моделі здатні навчатися на великих обсягах даних, вони здатні виявляти складні нелінійні залежності та незвичайні закономірності, які класичні алгоритми не можуть виявити. Впровадження таких підходів у телекомунікаційному секторі може не лише підвищити точність виявлення аномалій, але й забезпечити раннє прогнозування, що надзвичайно важливо для запобігання збоям та забезпечення стабільності мережі. Таким чином, вивчення нейронних мереж у контексті обробки комунікаційних даних є важливим кроком до створення нового покоління інтелектуальних систем мережевого спостереження та захисту.

На тлі зростаючих вимог до безпеки та ефективності систем зв'язку, методи, здатні працювати в умовах високої динаміки та змін даних, потребують особливої уваги. Нейронні мережі, особливо рекурентні та згорткові мережі, демонструють великий потенціал для адаптації до нових моделей поведінки мережі, що дозволяє їм автоматично адаптуватися до змінних умов та виявляти раніше невідомі загрози. Їх впровадження сприяє створенню більш гнучкої та стійкої аналітичної інфраструктури, здатної виявляти складні сценарії аномальної активності на ранній стадії. У поєднанні з методами попередньої обробки даних, такими як нормалізація, кластеризація та зменшення розмірності, нейронні мережі можуть не тільки покращити виявлення аномалій, але й зменшити кількість хибнопозитивних результатів. Це робить їх ключовим інструментом для побудови сучасних систем інтелектуального аналізу телекомунікаційного трафіку [1-5].

Метою бакалаврської кваліфікаційної роботи є розроблення та дослідження ефективних методів виявлення та прогнозування аномалій у великих обсягах телекомунікаційних даних за допомогою нейронних мереж.

Досягнення поставленої мети здійснюється розв’язанням таких завдань:

1) аналіз ефективності моделей нейронних мереж;

2) аналіз методів оброблення великих телекомунікаційних даних;

3) дослідження архітектур нейронних мереж для задач виявлення аномалій ;

4) розроблення моделі прогнозування аномалій на основі LSTM-мережі;

5) дослідження та аналіз результатів моделювання.

Об'єкт дослідження – оброблення телекомунікаційних даних з використанням штучного інтелекту.

Предмет дослідження – моделі нейронних мереж та методи їх навчання для виявлення і прогнозування аномальних подій у великих телекомунікаційних даних.

Методи дослідження. У роботі використовувалися методи статистичного та інтелектуального аналізу даних.

У першому розділі представлені теоретичні основи, архітектуру, принцип роботи та показники ефективності нейронних мереж у задачах виявлення аномалій.

У другому розділі розглядаються джерела, структура та характеристики обробки телекомунікаційних даних, а також демонструється доцільність використання нейронних мереж для аналізу таких даних.

У третьому розділі було реалізовано та протестовано модель прогнозування аномального споживання на основі LSTM, а результати проаналізовано та порівняно з традиційними методами.

У четвертому розділі аналізуються можливі небезпеки та шкідливі фактори в роботі комп'ютера, а також пропонуються методи захисту, профілактики та заходи охорони праці.

Ключові слова: нейронні мережі, аномалії, телекомунікаційні дані, прогнозування, штучний інтелект.

Література

1. M. Hou and X. Han, "Constructive Approximation to Multivariate Function by Decay RBF Neural Network," in *IEEE Transactions on Neural Networks*, vol. 21, no. 9, pp. 1517-1523, Sept. 2010, doi: 10.1109/TNN.2010.2055888.

2. J. Suárez-Varela *et al.*, "Graph Neural Networks for Communication Networks: Context, Use Cases and Opportunities," in *IEEE Network*, vol. 37, no. 3, pp. 146-153, May/June 2023, doi: 10.1109/MNET.123.2100773.

3. M. Hao *et al.*, "Artificial Neural Network-Based Approach to Modeling Energy Bands of GaN-Based Heterojunction Materials," *2023 International Conference on High Performance Big Data and Intelligent Systems (HDIS)*, Macau, China, 2023, pp. 71-76, doi: 10.1109/HDIS60872.2023.10499489.

4. J. B. P. Matos, E. B. de Lima Filho, I. Bessa, E. Manino, X. Song and L. C. Cordeiro, "Counterexample Guided Neural Network Quantization Refinement," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 4, pp. 1121-1134, April 2024, doi: 10.1109/TCAD.2023.3335313.

5. C. H. Park, "Anomaly Pattern Detection on Data Streams," *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Shanghai, China, 2018, pp. 689-692, doi: 10.1109/BigComp.2018.00127.

ЗМІСТ

ВСТУП

У сучасному світі цифрові технології охоплюють усі сфери людської діяльності, а системи зв'язку відіграють ключову роль у забезпеченні безперервного обміну інформацією. Стрімке зростання кількості користувачів, пристроїв та обсягів переданих даних призвело до складності комунікаційної інфраструктури, що, у свою чергу, збільшує ризик збоїв, аномалій та кібератак. Забезпечення стабільної та безпечної роботи таких систем вимагає нового інтелектуального підходу до аналізу великих обсягів даних у режимі реального часу.

Традиційні методи обробки та аналізу комунікаційного трафіку, хоча й залишаються корисними, дедалі частіше демонструють обмеження у виявленні складних та нечітко визначених аномалій. З огляду на зростаючу складність даних, потрібні системи, які можуть адаптуватися до нових типів інформації, виявляти приховані закономірності та своєчасно позначати потенційні загрози.

Одним із найперспективніших підходів у цій галузі є використання нейронних мереж, інструменту штучного інтелекту, які довели свою ефективність у багатьох галузях промисловості. Нейронні мережі, особливо глибокі моделі, продемонстрували здатність автоматично навчатися на великих обсягах вхідних даних, що робить їх ідеальними для виявлення складних аномалій. Це дозволяє створювати високоточні системи прогнозування, які не тільки виявляють існуючі відхилення, але й передбачають їх виникнення. Це дозволяє операторам телекомунікаційних мереж своєчасно вживати заходів для зменшення ризику простоїв, втрати даних або порушень безпеки.

Особлива увага приділяється вибору архітектури нейронної мережі, оскільки різні типи моделей (згорткові, рекурентні та автокодерні) мають різні переваги залежно від специфіки завдання та типу даних. Наприклад, для обробки часових рядів трафіку рекомендується використовувати LSTM-мережі, які можуть ефективно моделювати часові залежності. Отже, правильний вибір моделі є ключовим фактором успішного впровадження інтелектуальних систем у телекомунікаційній галузі [1].

РОЗДІЛ 1. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ НЕЙРОННИХ МЕРЕЖ

1.1 Основи нейронних мереж

1.1.1 Визначення та принципи роботи нейронних мереж

Нейронні мережі є одним з основних інструментів обробки даних у сучасному штучному інтелекті. Натхненні тим, як працює людський мозок, вони створюють математичні моделі та здатні вирішувати численні складні завдання, такі як розпізнавання образів, класифікація, прогнозування тощо. Основними компонентами нейронної мережі є нейрони, які отримують вхідні дані, обробляють їх та передають результати. Це дозволяє нейронним мережам імітувати певні особливості людського інтелекту, виконувати обчислення паралельно та коригувати параметри шляхом навчання. Принцип роботи нейронної мережі полягає в тому, що кожен нейрон отримує вхідний сигнал та обробляє його за допомогою певної математичної функції. Ця функція може бути лінійною або нелінійною, залежно від завдання, яке потрібно вирішити. Вхідні дані множаться на ваги, які визначають важливість кожного елемента вхідної інформації. Потім нейрон передає результат до функції активації, яка може відрізнятися від мережі до мережі.

Навчання є важливим аспектом нейронних мереж. Під час цього процесу мережа коригує свої ваги на основі помилки, що генерується при порівнянні виходу мережі з фактичним результатом. Одним з найпоширеніших методів навчання є алгоритм зворотного поширення помилки, який дозволяє оптимізувати ваги за допомогою градієнтного спуску. Це дозволяє мережі поступово покращувати свої можливості прогнозування та класифікації. Існує багато різних архітектур нейронних мереж. Деякі складаються з одного шару нейронів, а інші - з кількох шарів нейронів. Вони називаються багатошаровими мережами і зазвичай досягають найкращих результатів під час вирішення складних задач. Характерною рисою цих мереж є те, що вони можуть виявляти складні закономірності та зв'язки між даними, що робить їх ефективним інструментом для аналізу великих обсягів інформації. Основні типи нейронних мереж включають перцептрони, згорткові нейронні мережі та рекурентні нейронні мережі.

Перцептрони - це найпростіші моделі, що складаються з одного шару нейронів, і можуть вирішувати задачі, які потребують лінійного розділення даних. З іншого боку, згорткові мережі дуже ефективні в обробці зображень та інших двовимірних даних, оскільки вони здатні виявляти локальні залежності в даних, застосовуючи операції згортки. Рекурентні нейронні мережі (Recurrent Neural Networks, RNN) характеризуються своєю здатністю розглядати послідовності вхідних даних. Вони широко використовуються в завданнях, де контекст або залежність від минулого значення є критично важливою, таких як обробка природної мови або прогнозування часових рядів. Рекурентні нейронні мережі можуть “запам’ятовувати” інформацію про минулі стани та використовувати цю інформацію для прийняття майбутніх рішень.

Нейронні мережі мають широкий спектр застосування в різних галузях промисловості завдяки своїй гнучкості та адаптивності. Вони використовуються в медицині для діагностики захворювань, в автомобільній промисловості для створення систем автономного водіння, у фінансовій сфері для прогнозування ринків тощо. Це відкриває широкі перспективи для розвитку штучного інтелекту, дозволяючи створювати точніші та ефективніші моделі для вирішення реальних проблем. Однак, незважаючи на свої численні переваги, нейронні мережі також стикаються з деякими обмеженнями. Найважливіше з них полягає в тому, що вони вимагають великої кількості даних для ефективного навчання та потребують багато обчислювальних ресурсів, що в деяких випадках обмежує їх застосування. Крім того, нейронні мережі можуть діяти як “чорна скринька”, а це означає, що часто важко зрозуміти, чому мережа приймає певне рішення. Питання інтерпретованості та прозорості моделі є важливим напрямком для майбутніх досліджень у галузі штучного інтелекту. Інтерпретованість та прозорість моделей нейронних мереж є важливими темами для реальних застосувань штучного інтелекту. Після навчання важко точно зрозуміти, як мережа прийшла до певного рішення. Оскільки нейронні мережі містять велику кількість параметрів і складних структур, зрозуміти причини певного результату може бути надзвичайно складно. Ця відсутність прозорості може

бути небажаною або навіть небезпечною в багатьох застосуваннях, де точність і надійність рішень мають вирішальне значення.

Особливо в таких галузях, як медицина чи фінанси, де рішення нейронних мереж можуть мати значний вплив на життя людей чи економіку, вкрай важливо мати змогу пояснити, чому модель прийняла певне рішення. У таких випадках нездатність зрозуміти процес прийняття рішень може призвести до недовіри серед користувачів і навіть до юридичних наслідків. Тому інтерпретованість моделі є важливим питанням для розробників, які працюють над створенням більш зручних для користувача та надійних систем штучного інтелекту. Одним із способів підвищення прозорості є розробка спеціалізованих методів для "розкриття" внутрішніх процесів нейронних мереж. Наприклад, методи візуалізації можна використовувати для розуміння того, які дані або вхідні шаблони мають найбільший вплив на рішення мережі. Одним із таких методів є теплова карта, яка може показати, які частини зображення або тексту мережа вважає найважливішими для класифікації. Інший підхід полягає у використанні простих моделей, щоб спробувати наближено представити складні мережеві рішення до структур, які легше зрозуміти. Наприклад, методи інтерпретації, засновані на лінійних моделях або деревах рішень, можуть забезпечити інтерпретовані рішення для складніших мереж. Хоча ці методи не можуть забезпечити таку ж точність, як складні нейронні мережі, вони допомагають досягти балансу між точністю та прозорістю.

Крім того, існують спеціалізовані методи, які можуть покращити інтерпретацію без шкоди для ефективності. Одна зі стратегій полягає в розробці гнучких та легких для розуміння архітектур нейронних мереж, таких як інтерпретовані багатошарові архітектури або нейронні мережі, що включають механізми самоаналізу. Ці архітектури дозволяють моделям надавати додаткову інформацію про те, чому і як були прийняті певні рішення.

1.1.2 Архітектура нейронних мереж

Архітектура нейронної мережі має вирішальне значення для її здатності вирішувати широкий спектр проблем. Одношарова нейронна мережа є

найпростішою архітектурою та складається лише з одного шару нейронів, через який передається вся інформація. Така структура дозволяє виконувати лінійні операції над вхідними даними. Такі мережі в основному використовуються для простих задач класифікації або регресії, які потребують розподілу за одним або кількома атрибутами. Однак одношарові мережі обмежені у своїй здатності моделювати складні залежності та зв'язки в даних і не можуть ефективно вирішувати нелінійні проблеми. Для складніших проблем, таких як ті, що потребують складнішого контексту або багатогранних зв'язків у даних, використовуються багатошарові нейронні мережі. Ці мережі містять кілька шарів нейронів, причому кожен наступний шар містить більш складні та абстрактні ознаки з вхідних даних. Наприклад, перший шар може виявляти прості ознаки, такі як краї, кольори або текстури, тоді як наступні шари можуть інтегрувати ці ознаки в більш складні елементи, такі як форми або об'єкти [1-5].

Багатошарові мережі дозволяють виконувати складніші завдання, такі як розпізнавання зображень, природне мовлення та складна класифікація, які потребують поглибленого аналізу даних. Згорткові нейронні мережі (CNN, Convolutional Neural Networks) є однією з найпоширеніших архітектур сучасного штучного інтелекту. Вони спеціалізуються на обробці даних зі структурованими просторовими або часовими залежностями, таких як зображення чи відео. Головною перевагою згорткових мереж є використання згорток, які дозволяють їм ефективно виявляти локальні закономірності в даних. Як результат, вони добре підходять для розпізнавання об'єктів на зображеннях, сегментації зображень та завдань, де важлива локальна інформація в даних, таких як аналіз аудіо- чи відеофайлів.

Рекурентні нейронні мережі (RNN) - це ще одна важлива архітектура, яка відрізняється від традиційних мереж тим, що вони можуть обробляти послідовні дані. Це критично важливо для завдань, де інформація залежить від попередніх етапів, таких як прогнозування часових рядів, обробка тексту та машинний переклад. У RNN нейрони мають внутрішній зворотний зв'язок, що дозволяє їм зберігати інформацію про попередні стани та використовувати цю інформацію для

прийняття рішень на наступних етапах. Це дозволяє ефективно обробляти дані, де важливий порядок елементів, наприклад, слова в реченні або події в часовому ряді. Однак, класичні RNN обмежені у своїй здатності зберігати інформацію про довгострокові залежності, оскільки ці залежності з часом згасають або стають недійсними. Для вирішення цієї проблеми були розроблені вдосконалені форми RNN, такі як мережі з довгою короткостроковою пам'яттю (Long Short-Term Memory, LSTM) та GRU (Gated Recurrent Unit). Ці моделі використовують спеціальні механізми, які дозволяють їм зберігати важливу інформацію протягом тривалого часу, таким чином уникаючи проблем, що виникають у класичних RNN, та покращуючи здатність моделі обробляти довгі послідовності (Рис.1.1).

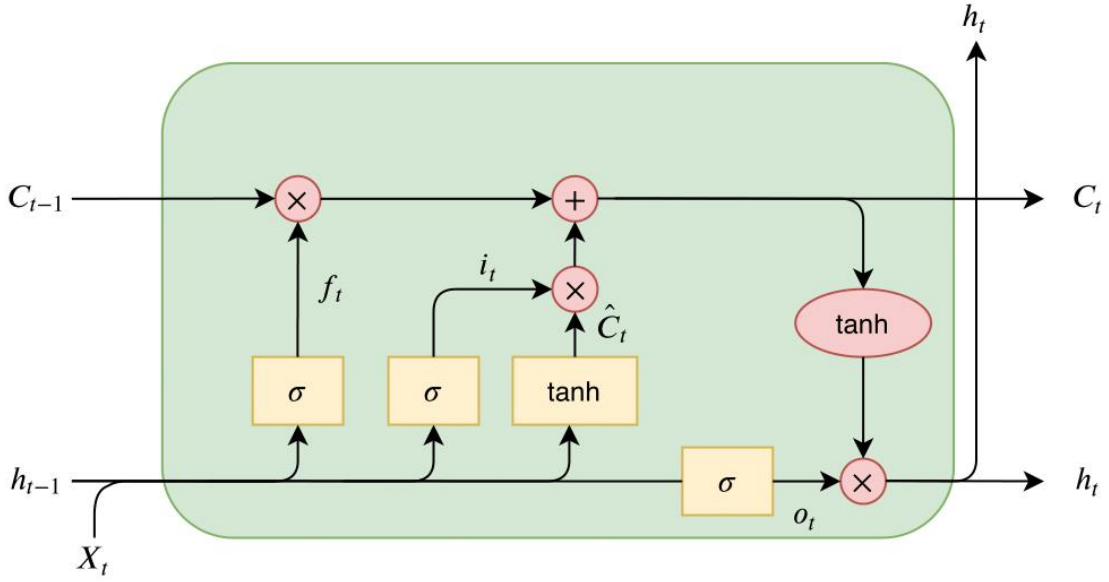


Рис.1.1. Архітектура LTSM

Багатошарові нейронні мережі можуть поєднувати різні архітектури для досягнення кращих результатів залежно від завдання. Наприклад, у багатьох випадках рекурентні нейронні мережі в поєднанні зі згортковими мережами можуть створювати потужні системи обробки відео або тексту, де локальна інформація важлива не лише в контексті. Це поєднання дозволяє нейронним мережам обробляти складніші дані та враховувати просторові та часові залежності. Ще однією цікавою архітектурою, яка часто використовується для генерації нових даних або створення завдань, що залежать від змінних, є генеративно-змагальні мережі, що складаються з двох конкуруючих моделей - генератора та

дискримінатора. Генератор намагається генерувати реалістичні дані, тоді як дискримінатор оцінює їхню надійність. Цей процес дозволяє створювати нові, реалістичні зображення, тексти або інші типи даних. Змагальні генеративні мережі часто використовуються в таких галузях, як генерація зображень, покращення якості зображень, а також у креативних індустріях, таких як музика та створення мистецтва.

Вибір архітектури нейронної мережі завжди залежить від конкретного завдання та типу даних. Одношарової мережі може бути достатньо для простих завдань, але для складніших завдань, таких як обробка зображень або послідовних даних, більше підходять багатошарові, рекурентні або згорткові мережі. Змагальна розробка та інтеграція нових архітектур досягають вражаючих результатів у широкому спектрі застосувань, від медицини до креативних індустрій, відкриваючи нові шляхи для розвитку штучного інтелекту.

Досягнення в розробці нових архітектур нейронних мереж значно розширили можливості штучного інтелекту, дозволяючи йому вирішувати дедалі складніші проблеми з більшою ефективністю та точністю. Від традиційних одношарових або багатошарових моделей до новіших, більш спеціалізованих архітектур, кожен крок в еволюції мереж відкривав нові шляхи для практичного застосування. Завдяки постійному вдосконаленню математичних методів, алгоритмів навчання та обчислювальної потужності стало можливим створювати нейронні мережі, які можуть досягати дивовижної точності та гнучкості в широкому спектрі завдань. Однією з найважливіших нових архітектур, яка суттєво змінила спосіб обробки послідовних даних, є трансформер. Зокрема, трансформер широко використовувався в галузі обробки природної мови та показав кращі результати, ніж попередні моделі, такі як рекурентні нейронні мережі. Ці мережі спираються на механізми уваги, які дозволяють їм ефективно обробляти великі обсяги даних, зосереджуючись на важливих частинах вхідної інформації, уникаючи при цьому впорядкування даних. Це дає Трансформеру значну перевагу в швидкості та гнучкості, дозволяючи йому ефективно обробляти великі текстові колекції, такі як моделі GPT, BERT або T5.

Поява глибоких генеративних моделей, таких як автокодери та генеративно-змагальні мережі, є важливим досягненням. Автокодери використовуються для стиснення та реконструкції даних у латентному просторі, що дозволяє створювати нові варіанти даних, такі як зображення, відео та навіть текст. Ці мережі здатні навчатися на масивних наборах даних, відновлювати відсутню інформацію та генерувати нові варіанти. Як згадувалося раніше, механізм роботи генеративно-змагальних мереж базується на конкуренції між генератором (який створює нові дані) та дискримінатором (який оцінює їхню автентичність). Ці моделі досягли вражаючих результатів у створенні реалістичних зображень, відео та навіть музики, відкриваючи нові можливості для творчих та медіа-застосунків.

Крім того, дослідники активно розробляють архітектури, які можуть краще обробляти масивні, складні та високопов'язані дані. Одним із таких підходів є графові нейронні мережі, які здатні обробляти дані у вигляді графів, де кожен елемент може бути пов'язаний з іншими елементами. Цей підхід особливо корисний для завдань, де структура зв'язків між об'єктами є критично важливою, таких як соціальні мережі, біоінформатика, рекомендаційні системи та логістика. Графові мережі дозволяють нам виявляти складні зв'язки між даними, які неможливо адекватно змоделювати традиційними методами. Ще одним важливим напрямком є розробка фреймворків для обробки мультимодальних даних – даних, що містять різні типи інформації, таку як текст, зображення та аудіо. Мультимодальні нейронні мережі дозволяють нам поєднувати різні типи даних та використовувати їх для вирішення складних завдань, таких як розпізнавання об'єктів на зображеннях за допомогою описів природною мовою або аналіз відео з одночасним перекладом тексту. Це вимагає поєднання різних фреймворків, таких як згорткові мережі для зображень та трансформатори для тексту, щоб нейронні мережі могли ефективно обробляти різноманітні джерела інформації.

Важливим кроком є розробка моделей, які можуть працювати на обмежених обчислювальних ресурсах, таких як вбудовані системи або мобільні пристрої. Такі фреймворки є прикладами ефективних нейронних мереж, які підтримують високу

точність, будучи оптимізованими для пристроїв з низьким енергоспоживанням. Методи, що використовуються в цих мережах, можуть значно зменшити кількість параметрів та обчислювальних ресурсів без суттєвого зниження ефективності, що робить їх ідеальними для обробки даних у режимі реального часу.

Розробка нових архітектур також спрямована на покращення навчання нейронних мереж, особливо шляхом використання нових методів регуляризації, адаптивних оптимізаторів та методів навчання для зменшення перенавчання та покращення стійкості моделі до шуму даних. Досягнення в розробці нових архітектур нейронних мереж відкривають багато нових можливостей, дозволяючи нам створювати потужніші та гнучкіші моделі для вирішення складних проблем. Застосування цих нових архітектур у різних галузях, таких як медицина, автомобілі та фінанси, досягло практичних результатів, змінивши спосіб обробки даних та автоматизації процесів.

1.1.3 Функції активації та оптимізації в нейронних мережах

Функції активації та функції оптимізації є одними з найважливіших компонентів нейронних мереж. Вони визначають, як мережа обробляє та адаптується до вхідних даних, а також як вона навчається та налаштовує параметри під час навчання. Функції активації визначають, чи буде сигнал, що надходить на нейрон, передаватися в мережі. Ці функції вносять нелінійність у нейронну обробку, дозволяючи мережі моделювати складні залежності в даних. Без нелінійних функцій активації нейронні мережі були б лінійними, і навіть багатошарові архітектури не змогли б обробляти складні завдання, такі як розпізнавання зображень або обробка мови. Однією з найбільш широко використовуваних функцій активації є функція S-типу, вихідні значення якої коливаються від 0 до 1. Вона широко використовувалася в минулому, але з розвитком технологій стали очевидними деякі її обмеження, особливо під час навчання глибоких мереж, де виникали проблеми градієнтного спуску. Тому функція ReLU (Rectified Linear Unit) стала популярною завдяки своїй простоті та ефективності. ReLU дозволяє значенням, більшим за нуль, проходити через нейрони без змін, тоді як значенням, меншим за нуль, присвоюється нуль. Це

дозволяє уникнути проблеми градієнтного спуску та пришвидшує процес навчання. Однак, ReLU також має свої недоліки, особливо проблему “мертвих нейронів”, коли деякі нейрони ніколи не активуються.

Для подолання цих проблем було запропоновано різні типи ReLU, такі як Leaky ReLU та Parametric ReLU. Вони дозволяють значенням меншим за нуль мати невеликі негативні градієнти, що допомагає запобігти “мертвим нейронам”. Ще однією поширеною функцією активації є tanh, яка є гіперболічною тангенсною функцією з діапазоном виходу від -1 до 1 і є більш ефективною в деяких випадках. Вибір функції активації залежить від конкретної проблеми, характеристик мережі та вимог до швидкості та точності навчання.

Оптимізація - ще один важливий аспект нейронних мереж, який відповідає за коригування ваг мережі під час навчання для мінімізації функції помилки або втрат. Процес оптимізації включає використання алгоритмів, які поступово змінюють параметри мережі для отримання найкращих результатів на тестових даних. Одним з найпоширеніших методів оптимізації є градієнтний спуск, який використовує похідну функції втрат для визначення напрямку коригування ваг для мінімізації помилки. Існує багато форм градієнтного спуску, включаючи стохастичний градієнтний спуск та мінімальний градієнтний спуск. На відміну від стандартного градієнтного спуску, який використовує всі дані для кожної ітерації, стохастичний градієнтний спуск оновлює ваги після обробки кожного зразка в навчальному наборі даних. Це може значно пришвидшити процес навчання, особливо під час роботи з великими наборами даних. Однак цей підхід може внести значну мінливість у процес навчання через часті зміни параметрів. Для вирішення цієї проблеми були розроблені вдосконалення, такі як мінімальний градієнтний спуск, який використовує частину даних на кожному кроці [6-14].

Більш просунуті методи оптимізації включають алгоритми, які автоматично регулюють швидкість навчання кожного параметра. Одним з таких алгоритмів є алгоритм Adam, який поєднує сильні сторони двох інших методів, Adagrad та RMSProp. Adam використовує середньоквадратичні градієнти для адаптивного

регулювання швидкості навчання кожного параметра мережі. Це дозволяє Adam працювати швидко та ефективно під час оптимізації складних завдань, таких як навчання глибоких нейронних мереж. Ще одним важливим аспектом є точне налаштування, техніка, яка допомагає запобігти перенавчанню моделі, особливо коли модель добре працює на навчальних даних, але погано на нових, невідомих даних. Одним з найпоширеніших методів точного налаштування є алгоритм Dropout, який випадковим чином вимикає деякі нейрони на кожній ітерації навчання, щоб мережа не надто покладалася на певні ознаки. Це покращує здатність мережі до узагальнення, дозволяючи їй краще працювати з новими даними. Незважаючи на значний прогрес в оптимізації нейронних мереж, процес залишається складним і залежить від багатьох факторів, таких як вибір функції активації, алгоритму оптимізації, розміру даних та конфігурації мережі. Різні методи активації та оптимізації можуть суттєво змінити продуктивність моделі, тому вкрай важливо ретельно вибрати найбільш підходящий метод для конкретної проблеми.

1.2 Типи нейронних мереж для аналізу даних

1.2.1 Перцептрони та їх застосування в задачах класифікації

Персептрон є однією з найстаріших моделей нейронних мереж і є основою багатьох сучасних методів штучного інтелекту та машинного навчання. Це простий алгоритм, що складається з шару нейронів, здатних до лінійної класифікації. Принцип полягає в тому, що кожен вхідний сигнал обробляється набором вагових коефіцієнтів, а вихідний визначається функцією активації. Персептрон здатний класифікувати вхідні дані на дві категорії на основі надлінійної площини, яка розділяє простір вхідних даних. Таким чином, він здатний вирішувати задачі, де дані можуть бути розділені лише лінійною межею. Основною перевагою персептрона є його здатність навчатися на вибірках, що дозволяє коригувати ваги відповідно до нових даних на кожному кроці. Для цього використовуються методи корекції ваг, зокрема алгоритм зворотного поширення помилки, щоб зменшити різницю між прогнозованими результатами та фактичними результатами. Після належного навчання персептрон здатний оптимізувати свої параметри і таким чином

розпізнавати закономірності в нових даних, подібні до його навчальних даних. Однак на ранніх етапах розвитку нейронних мереж стало зрозуміло, що класичні персептрони мають очевидні обмеження. Найбільшою проблемою було те, що вони не могли вирішувати задачі, які не можна було класифікувати за допомогою надлінійної площини. Це відкриття було зроблено під час спроби навчити перцептрони розпізнавати прості функції, такі як булева функція або оператор.

Нездатність стандартних перцептронів вирішувати задачі без лінійних меж, такі як операція XOR, призвела до розробки багатошарових архітектур. Тим не менш, перцептрони все ще відіграють важливу роль у задачах класифікації, де категорії можна чітко розділити за допомогою лінійної межі. Наприклад, перцептрони ефективно використовуються в таких галузях, як розпізнавання образів, або в задачах, де потрібно розрізнити два набори даних з чітко різними структурами. Вони також використовуються у фінансах (для класифікації заявок на кредити), медицині (для діагностики захворювань на основі простих критеріїв) та інших галузях, де потрібна швидка лінійна класифікація. Важливо, що нейронні перцептрони формують основу для розробки складніших і потужніших моделей нейронних мереж. Багатошарові перцептрони, які складаються з кількох шарів нейронів, здатні вирішувати складніші задачі за допомогою нелінійних функцій активації. Ці перцептрони також розширюють свої можливості, дозволяючи мережі моделювати складніші, нелінійні зв'язки в даних, що призводить до точнішої класифікації в складніших ситуаціях.

Примітно, що нейронні перцептрони також ефективно працюють з невеликими обсягами даних. Вони відносно прості та швидкі в навчанні, що робить їх добре придатними для застосувань реального часу, які потребують швидкої класифікації даних. Вони ідеально підходять для завдань, де вхідні дані не є надто складними або багатими на функції, а головним завданням є швидка та ефективна обробка інформації. Нейронні перцептрони можуть бути недостатніми для складних завдань класифікації, які потребують високої точності та великої кількості ознак. У таких випадках часто використовуються складніші моделі, такі як багатошарові

нейронні мережі, згорткові мережі та рекурентні моделі, які здатні обробляти складніші, багатовимірні дані. Тому перцептрони залишаються важливим інструментом у машинному навчанні та нейронних мережах. Їхня простота та ефективність роблять їх дуже корисними для вирішення базових завдань класифікації, але вони також відкривають двері до більш просунутих методів для складніших завдань. Тим не менш, перцептрони незамінні в навчальних курсах, оскільки вони складають основу для вивчення структури та принципів роботи складніших нейронних мереж.

1.2.2 Рекурентні нейронні мережі і їх роль у обробці послідовних даних

Рекурентні нейронні мережі (RNN) є значним прогресом у машинному навчанні, особливо в завданнях, що включають послідовну обробку даних. Ключовою перевагою RNN є їхня здатність зберігати інформацію з попередніх кроків обробки та використовувати її для обробки поточних даних. Це досягається завдяки рекурентним зв'язкам, які дозволяють нейронам передавати свій вихід на наступні часові кроки. Це робить RNN особливо корисними для завдань, де зв'язки між елементами послідовності є критично важливими, таких як обробка природної мови або часові ряди. Однією з головних проблем, з якими стикаються стандартні RNN, є градієнтний спад або вибух. Під час навчання мережі на довгих послідовностях градієнти, що використовуються для коригування ваг, можуть бути занадто малими або занадто великими. Це ускладнює навчання та знижує ефективність мережі в обробці довгострокових залежностей (Рис.1.2).

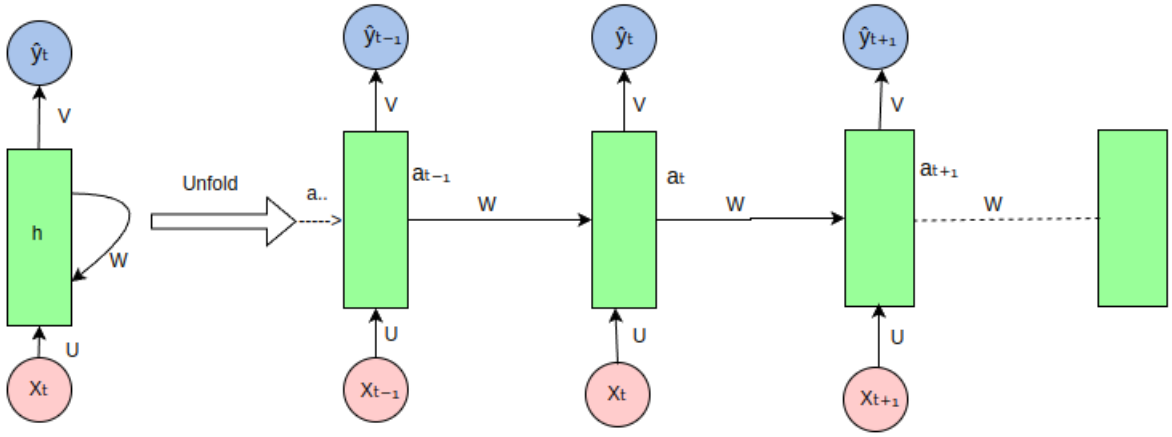


Рис.1.2. Архітектура RNN

Мережі LSTM та GRU є одними з найпоширеніших типів рекурентних мереж. Вони значно покращують здатність мережі вивчати довгі послідовності, дозволяючи їй краще зберігати важливу інформацію. LSTM використовують комірки пам'яті, які дозволяють їм зберігати інформацію протягом тривалого часу та контролювати, яку інформацію слід зберігати, а яку забувати. Це робить мережі LSTM дуже ефективними в завданнях, де існують значні залежності від часової затримки між елементами послідовності, таких як машинний переклад або генерація тексту. RNN стали стандартом в обробці природної мови, де послідовності слів або символів мають вирішальне значення для розуміння значення. Рекурентні нейронні мережі дозволяють моделювати контекст, що є важливим для багатьох завдань, таких як переклад тексту, аналіз настроїв, розпізнавання мовлення тощо.

Оскільки мова має послідовну природу, RNN здатні обробляти послідовні текстові елементи та зберігати контекст на кожному етапі обробки, що є ключовою особливістю для досягнення високої точності в цих завданнях. На додаток до природної мови, RNN широко використовуються для обробки часових рядів, таких як фінансові дані або прогнози погоди. У цих випадках мережа повинна враховувати минулі значення, щоб передбачити майбутні значення. Наприклад, на фінансових ринках рекурентні мережі можна використовувати для прогнозування цін на акції з урахуванням історичних змін. Це робить прогнози, засновані на минулому досвіді, точнішими. Рекурентні мережі також використовуються в обробці відео, де вони не тільки обробляють окремі кадри, але й виявляють безперервні зміни між кадрами. Вони можуть допомогти ідентифікувати об'єкти у відео, виявляти події та навіть генерувати відео з текстових описів. Рекурентні мережі можуть враховувати час та зміни між кадрами, що призводить до кращого розуміння динаміки подій у відео. RNN можна використовувати для завдань, які потребують моделювання та прогнозування безперервних дій. Це можна застосувати до робототехніки, де рекурентні мережі можуть допомогти планувати траєкторію руху робота, прогнозувати майбутні дії або навчати робота виконувати складні дії на основі минулого досвіду.

Незважаючи на свої численні переваги, рекурентні нейронні мережі також мають деякі обмеження. Одним з їхніх головних недоліків є те, що їх важко навчати на великих наборах даних через високі вимоги до обчислювальних ресурсів та часу навчання. Крім того, навіть просунуті версії рекурентних нейронних мереж, такі як LSTM та GRU, не завжди можуть ефективно обробляти дуже довгі послідовності або дані, що містять складні залежності та охоплюють тривалі часові масштаби. Це призвело до розробки нових архітектур та методів для підвищення ефективності обробки послідовних даних, таких як Transformer, який може обробляти послідовності паралельно та не схильний до проблеми зниклого градієнта. Рекурентні нейронні мережі відіграють важливу роль у вирішенні задач, що потребують обробки послідовних даних, та заклали основу для розробки нових методів у галузі глибокого навчання. Їхня здатність моделювати складні часові залежності робить їх незамінним інструментом у таких галузях, як обробка мови, прогнозування, робототехніка та аналіз даних. Незважаючи на обмеження, їх постійний розвиток та нові вдосконалення відкривають нові шляхи для їхнього майбутнього застосування.

1.2.3 Згорткові нейронні мережі для виявлення структурних аномалій у даних

Згорткові нейронні мережі (CNN) є одним з провідних інструментів для вирішення проблем, пов'язаних з аналізом зображень, але їх застосування цим не обмежується. Одним з їхніх найважливіших застосувань є виявлення аномалій структури даних, що полягає в здатності мережі виявляти аномалії, що відхиляються від нормальних шаблонів або структур у складних наборах даних. Завдяки своїй архітектурі, яка складається з кількох згорткових шарів, мережа здатна навчитися розпізнавати навіть найменші аномалії в структурі даних, що особливо корисно для завдань, де аналітична точність є критично важливою. Однією з ключових переваг згорткових нейронних мереж є їхня здатність обробляти локальні залежності в даних. Згорткові шари використовують фільтри для перевірки вхідних даних у пошуках певних ознак або шаблонів, таких як краї зображення, текстури або

повторювані шаблони. У задачах виявлення аномалій ці шаблони можуть включати очікувані структури або природні варіації в даних, і будь-яке відхилення від цих шаблонів може свідчити про наявність аномалії (Рис.1.3).

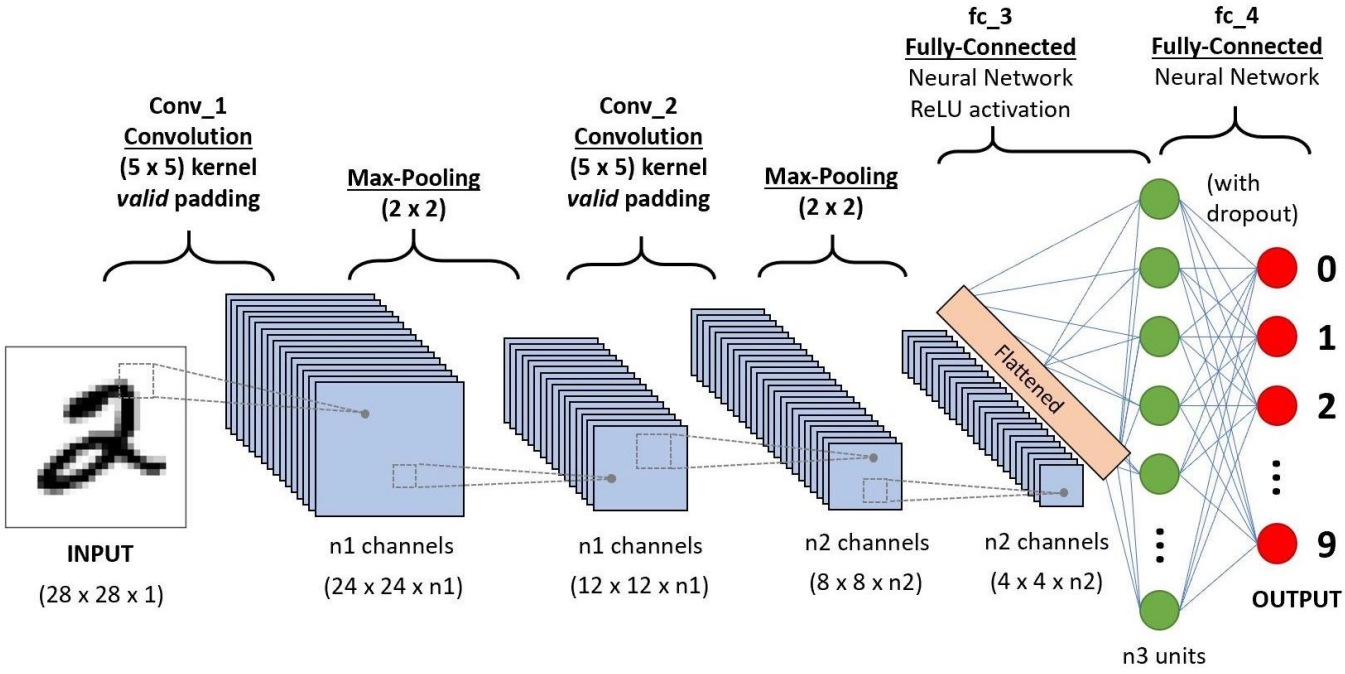


Рис.1.3. Архітектура CNN

Тому CNN можна використовувати для аналізу медичних зображень, фінансових даних або будь-яких інших структурованих даних, що містять очікувані стандарти або шаблони. У завданнях виявлення аномалій здатність мережі навчатися без явних міток (тобто неструктурованих або частково позначених даних) є вирішальною. Згорткові нейронні мережі можуть виявляти приховані зв'язки в даних, навіть коли аномалії неможливо чітко визначити або описати. Наприклад, у медичних дослідженнях згорткові нейронні мережі використовуються для виявлення аномалій у медичних скануваннях (таких як МРТ або рентген), а деякі захворювання можуть проявлятися як ледь помітні або дуже складні структурні аномалії.

Важливим аспектом використання згорткових нейронних мереж для виявлення аномалій є те, що мережа здатна автоматично виділяти ключові особливості та структури без необхідності попереднього детального аналізу даних. Це може значно скоротити час, необхідний для підготовки даних до моделювання,

та зменшити ризик людської помилки при виявленні потенційних аномалій. Згорткові нейронні мережі можуть автоматично знаходити найважливіші особливості та виконувати ефективний аналіз навіть у дуже складних та різноманітних наборах даних. Ці мережі дуже ефективні у виявленні складних аномалій, таких як структурні дефекти у виробництві або виявлення шахрайства у фінансовій звітності. У цих застосуваннях згорткові мережі можуть обробляти величезні обсяги даних та виявляти аномалії, з якими важко впоратися традиційними аналітичними методами. Наприклад, у промисловій сфері згорткові мережі використовуються для аналізу зображень виробничих процесів, що дозволяє виявляти дефекти або аномалії у продуктах на ранній стадії, тим самим знижуючи витрати та покращуючи якість.

Згорткові мережі особливо ефективні у виявленні аномалій у багатофункціональних даних, таких як відео або багатовимірні сигнали. Наприклад, у відеоаналізі згорткові мережі можуть використовуватися для виявлення аномальних або неочікуваних змін у поведінці об'єктів, що може бути застосовано в сферах безпеки та моніторингу. Ці мережі можуть аналізувати зміни з часом та виявляти структурні аномалії, навіть коли ці зміни невеликі або приховані у великій кількості звичайних даних. CNN також ефективні при обробленні різноманітних типів даних, включаючи багатоканальні зображення або цифрові часові ряди, де кожен канал може містити незалежні ознаки або характеристики, які є критично важливими для виявлення аномалій. Ця здатність дозволяє застосовувати згорткові нейронні мережі в багатьох галузях, де дані необхідно ретельно аналізувати для виявлення відхилень від нормальних закономірностей. Наприклад, у фінансових системах вони можуть допомогти виявляти підозрілі транзакції або аномальну поведінку користувачів. Загалом, згорткові нейронні мережі чудово виявляють структурні аномалії в даних завдяки своїй здатності автоматично виявляти закономірності та аномалії. Завдяки своїй універсальності, здатності обробляти величезні обсяги даних та високій точності, ці мережі стають дедалі популярнішими в широкому спектрі галузей, від медицини до виробництва. Ці мережі не тільки

ефективно виявляють аномалії, але й можуть працювати на високих швидкостях, що є важливим для реальних застосувань, де час відгуку є критичним.

1.3. Моделювання аномалій за допомогою нейронних мереж

1.3.1 Методи виявлення аномалій в різних типах даних

Виявлення аномалій є критично важливим завданням в аналізі даних, і для досягнення цієї мети використовуються різні методи, залежно від типу та структури даних. Аномалії даних - це відхилення від нормальних або очікуваних закономірностей, які можуть свідчити про помилки, несправності або незвичайні явища, що потребують уваги. Одним з найважливіших методів виявлення аномалій є використання статистичних методів, які допомагають ідентифікувати спостереження, що суттєво відрізняються від середнього значення або його розподілу. Ці методи можна застосовувати до числових даних, що дозволяє нам виявляти великі відхилення від середнього значення, наприклад, ідентифікуючи аномалії. Для категоріальних або дискретних даних, значення яких можуть не бути числовими, можна використовувати інші методи, такі як методи на основі моделей або методи класифікації.

Поширеним підходом є використання моделей класифікації, таких як дерева рішень або методи опорних векторів (SVM), для розрізнення нормальних та аномальних класів на основі навчальних даних. У таких завданнях важливо знати, які класи можуть бути аномальними та чи можна їх ідентифікувати як аномалії. Для часових рядів часто використовуються методи, що враховують залежність даних від часу. Наприклад, у фінансовому аналізі або моніторингу обладнання часто необхідно виявляти аномалії в ряді даних, які змінюються з часом. Один із цих методів базується на методах згладжування, таких як ковзні середні або експоненціальне згладжування, які допомагають виявляти неочікувані зміни в тенденціях. Більш просунуті підходи включають використання RNN, які можуть виявляти складні закономірності в послідовностях та виявляти аномалії, що виникають протягом триваліших періодів часу.

Інші спеціалізовані підходи до виявлення аномалій на зображеннях, такі як CNN, добре підходять для обробки візуальних даних. Ці підходи можуть автоматично виявляти аномалії на зображеннях, такі як дефекти продукції або захворювання на медичних зображеннях. Згорткові нейронні мережі можуть виявляти навіть дуже тонкі зміни в структурі зображення, які можуть бути непомітними для людського ока. Цей підхід широко використовується в таких галузях, як медицина, де точне виявлення аномалій на зображеннях є критично важливим, наприклад, під час діагностики раку чи інших захворювань.

Виявлення аномалій також є критично важливим для текстових даних, таких як документи або соціальні мережі. У цьому випадку методи обробки природної мови часто використовуються для виявлення незвичайних закономірностей у тексті, які можуть свідчити про аномалії або маніпуляції. Один із підходів полягає у використанні моделей на основі глибоких нейронних мереж для виявлення відхилень у мовних шаблонах, таких як зловживання в соціальних мережах або шахрайська інформація в тексті. Алгоритми машинного навчання можуть аналізувати великі обсяги текстових даних для виявлення ненормативної лексики або інших відхилень від шаблонів природної мови.

Для багатовимірних даних з кількома змінними часто використовуються методи кластеризації, щоб допомогти виявити аномалії шляхом групування подібних спостережень. У цьому контексті аномалії визначаються як дані, які не належать до жодного кластера або суттєво відрізняються від найближчої точки. Цей підхід широко використовується в таких галузях, як маркетинг (для аналізу моделей поведінки споживачів) або в кібербезпеці для виявлення аномальних дій або звернень. Методи глибокого навчання, такі як автокодери, також використовуються для виявлення аномалій у різних типах даних. Автокодер - це нейронна мережа, яка навчається реконструювати дані, спочатку стискаючи вхідні дані в менший простір. Вони використовуються для виявлення аномалій, оскільки, коли модель стикається з аномальними даними, вона не може ефективно відновити їх, що призводить до значних помилок відновлення. Цей підхід добре працює для числових, текстових та

графічних даних, які важко виявити безпосередньо за допомогою традиційних статистичних методів.Загалом, виявлення аномалій є важливим інструментом для аналізу даних у багатьох різних галузях. Використовувані методи можуть відрізнятися залежно від типу даних та конкретного завдання. Завдяки досягненням у методах машинного навчання, виявлення аномалій стало ефективнішим, що дозволяє знизити ризики, покращити якість продуктів та послуг, а також безпеку в усіх сферах життя.

1.3.2 Використання автокодерів для виявлення аномалій

Автокодери є одним із найефективніших методів виявлення аномалій у всіх типах даних. Вони являють собою тип нейронної мережі, яка здатна навчитися реконструювати стиснуті вхідні дані в компактне представлення. Процес навчання автокодера включає спробу мінімізувати різницю між вхідними даними та їх реконструйованим виходом. У сфері виявлення аномалій автокодери використовуються для навчання реконструкції нормальних даних, а потім виявлення аномалій у даних, які не відповідають навчальному шаблону. Їх перевагою є те, що вони не потребують міток для навчання, що робить їх добре придатними для обробки неструктурованих або частково позначених даних. Автокодери можуть автоматично витягувати важливі ознаки з даних, стискати їх до меншого розміру та витягувати найважливішу інформацію. Це дозволяє виявляти аномалії, оскільки вони не здатні ефективно відновлювати дані, які суттєво відрізняються від нормального шаблону, на якому навчалася модель.

У завданні виявлення аномалій автокодери використовуються таким чином, що після навчання на “нормальних” даних вони стають менш ефективними у відновленні аномалій або нових даних. Це означає, що коли автокодувальник виявляє аномалії, він не може відновити їх з такою ж точністю, як звичайні дані. У випадку аномалій різниця між вхідними даними та їх відновленим значенням (помилка відновлення) набагато більша, що дозволяє ефективно розпізнавати. Цей підхід широко використовується в таких галузях, як виявлення дефектів у виробництві, де виявлення нетипових закономірностей у продуктах є критично

важливим. Наприклад, виявлення дефектів на зображеннях товарів або перевірка якості продукції на складальній лінії. Оскільки автокодувальники здатні зменшувати розмірність даних і зберігати лише найважливішу інформацію, вони ефективні у виявленні аномалій, навіть якщо ці аномалії дуже рідкісні або незвичайні.

Автокодери також використовуються для виявлення аномалій у фінансових даних, таких як транзакції. Вони можуть вивчати нормальну поведінку (наприклад, банківські транзакції) з історичних даних, а потім ідентифікувати транзакції, які суттєво відрізняються від звичайних закономірностей. Це дозволяє їм автоматично виявляти підозрілі або шахрайські транзакції, які традиційні методи моніторингу можуть пропустити. У сфері кібербезпеки автокодери використовуються для виявлення аномалій у мережевих даних. Вони можуть допомогти виявляти несанкціоновані операції або мережеві атаки, що проявляються аномальною поведінкою трафіку, такою як нестандартні запити або підозрілі шаблони доступу. Автокодери навчаються на звичайному мережевому трафіку та можуть негайно виявляти аномалії, значно підвищуючи безпеку. У медичних застосуваннях автоенкодери використовуються для аналізу зображень. Вони здатні виявляти аномалії, які можуть свідчити про захворювання, невидимі людському оку. Наприклад, автоенкодери можуть допомогти виявити ранні стадії раку або інших захворювань, значно полегшуючи діагностику та дозволяючи лікарям виявляти потенційні проблеми, які в іншому випадку могли б залишитися непоміченими.

Є ще одна важлива перевага використання автокодерів для виявлення аномалій: вони можуть обробляти великі обсяги даних без необхідності ручного аналізу або попередньої обробки. Вони також здатні автоматично адаптуватися до нових типів аномалій, що робить їх ідеальними для динамічних середовищ, де шаблони аномалій змінюються з часом. Це дозволяє автоенкодерам пропонувати виняткову гнучкість та ефективність у таких сферах, як спостереження в режимі реального часу або автоматизовані системи виявлення аномалій.

Таким чином, автокодерами можна назвати потужний інструмент для виявлення аномалій, оскільки вони здатні навчатися на основі звичайних даних та

ефективно виявляти аномалії в нових або незвичайних спостереженнях. Вони здатні автоматично виявляти різні типи даних, від зображень до фінансових та мережевих даних, значно підвищуючи ефективність та безпеку спостереження в різних сферах.

1.3.3 Оцінка ефективності нейронних мереж при прогнозуванні аномалій

Оцінка продуктивності нейронних мереж у прогнозуванні аномалій є ключовим кроком у розробці та застосуванні цих моделей. Враховуючи рідкість та незвичайність аномалій, надзвичайно важливо точно оцінити ефективність моделі у виявленні відхилень від знайомих закономірностей. Для цього використовуються різні метрики для визначення точності, чутливості та специфічності моделі. Точність є однією з найважливіших метрик, яка представляє частку аномалій до нормальних спостережень, які модель правильно класифікує. Однак точність не завжди є достатньою метрикою, особливо у випадку дисбалансу класів. Ще однією важливою метрикою є чутливість або повнота, яка вимірює здатність моделі виявляти аномалії серед усіх справжніх аномалій. Ця чутливість є критично важливою, оскільки пропущені аномалії можуть мати серйозні наслідки, наприклад, у фінансових або медичних системах.

Вища чутливість означає, що модель здатна виявляти більшу частку аномалій, тим самим зменшуючи ризик пропуску важливих аномалій. Однак це також може призвести до збільшення кількості хибнопозитивних результатів, тому необхідно знайти баланс між чутливістю та специфічністю. Такі метрики, як точність та метрика F1 (середнє гармонійне точності та чутливості), використовуються для оцінки продуктивності нейронних мереж. Метрика F1 допомагає знайти найкращий баланс між двома метриками, що дуже важливо при прогнозуванні аномалій, оскільки вона може враховувати як пропущені аномалії, так і хибнопозитивні результати. Метрика F1 особливо корисна в завданнях, де виявлення аномалій – це більше, ніж просто зменшення кількості хибнопозитивних результатів.

Використання кривих ROC та AUC може допомогти вам краще зрозуміти здатність нейронної мережі розрізняти аномальні та нормальні дані при різних порогах. Крива ROC (Receiver Operating Characteristic) показує зв'язок між

чутливістю та специфічністю, тоді як AUC (Area Under the Curve) вимірює площу під кривою. Чим більша AUC, тим краща модель загалом, що вказує на її здатність правильно класифікувати нормальні та аномальні спостереження при різних порогових рівнях.

Тестування моделі з реальними даними є важливою частиною оцінки ефективності нейронних мереж у прогнозуванні аномалій. З огляду на рідкість аномалій, критично важливо точно оцінити ефективність моделі, оцінивши її стійкість та здатність до узагальнення шляхом перевірки на різних підмножинах даних. Тестування з реальними даними дозволяє нам зрозуміти, як модель поводиться за наявності шуму, нестандартних змін та змінних у часі шаблонів, що є критично важливим для забезпечення її практичної ефективності. Враховуючи здатність нейронних мереж адаптуватися до нових даних, також важливо враховувати метрики, які оцінюють зміни ефективності моделі в динамічних умовах. Прогнозування аномалій часто вимагає від моделей постійної адаптації до нових умов або типів аномалій, тому критично важливо оцінити здатність моделі оновлювати параметри або навчатися на нових, невідомих даних без суттєвого погіршення продуктивності. У випадках, коли необхідно враховувати складність моделі, таких як великі нейронні мережі або глибоке навчання, також важливо контролювати час навчання та швидкість моделі.

Моделі, які потребують великих обчислювальних ресурсів або займають багато часу для навчання, можуть погано працювати в реальних додатках, які потребують прогнозів у реальному часі. Тому при оцінці продуктивності слід враховувати такі аспекти, як швидкість обчислень та ефективність. Зрештою, оцінка продуктивності нейронних мереж у прогнозуванні аномалій - це складний процес, який охоплює традиційні показники точності та специфічні для застосування показники, такі як чутливість, специфічність, прецизійність та час відгуку. Оцінка на основі реальних даних та безперервна оптимізація моделі можуть допомогти забезпечити її практичність та максимальну ефективність у вирішенні задач прогнозування аномалій [15-21].

Висновок до розділу 1

У розділі 1 розглянуто основи нейронних мереж, їхня архітектура та ключові характеристики, які роблять їх ефективними у виконанні різноманітних завдань. Були визначені різні архітектури нейронних мереж, такі як одношарова, багатошарова, рекурентна та згорткова, кожна з яких має свої переваги залежно від завдання та типу вхідних даних. Тип нейронної мережі, що використовується для аналізу даних, має вирішальне значення для ефективного вирішення задач класифікації, обробки послідовних даних та виявлення аномалій.

Оцінка ефективності нейронних мереж у прогнозуванні аномалій включає аналіз таких показників, як точність, чутливість та специфічність, що дозволяє нам точно визначити продуктивність моделі в реальних умовах. Загалом, нейронні мережі з їх багатими архітектурами та методами мають великий потенціал для аналізу складних даних та виявлення аномалій у різних галузях. Їхня здатність адаптуватися до нових типів даних та автоматично виявляти неочевидні шаблони робить їх незамінним інструментом у сучасних завданнях машинного навчання та штучного інтелекту.

РОЗДІЛ 2. ОБРОБЛЕННЯ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1 Характеристика великих масивів телекомунікаційних даних

2.1.1 Структура та формат телекомунікаційних даних

Структури та формати телекомунікаційних даних є фундаментальними концепціями для обміну інформацією на великих відстанях. Вони визначають, як інформація електронно кодується, передається, отримується та декодується між різними пристроями. Успішна комунікація вимагає узгоджених стандартів, щоб різні системи могли розуміти одна одну, навіть якщо вони походять від різних виробників або використовують різні протоколи. Телекомунікаційні дані мають багаторівневу структуру, організовану відповідно до принципів моделі OSI або TCP/IP. У цій структурі кожен рівень виконує певну функцію, від фізичної передачі бітів до забезпечення взаємодії користувацьких програм. Наприклад, на фізичному рівні дані існують у формі електричних імпульсів або оптичних сигналів; тоді як на канальному рівні дані попередньо організовані в кадри, що містять службову інформацію. Компоненти телекомунікаційної системи передаваня даних зображено на Рис.2.1.

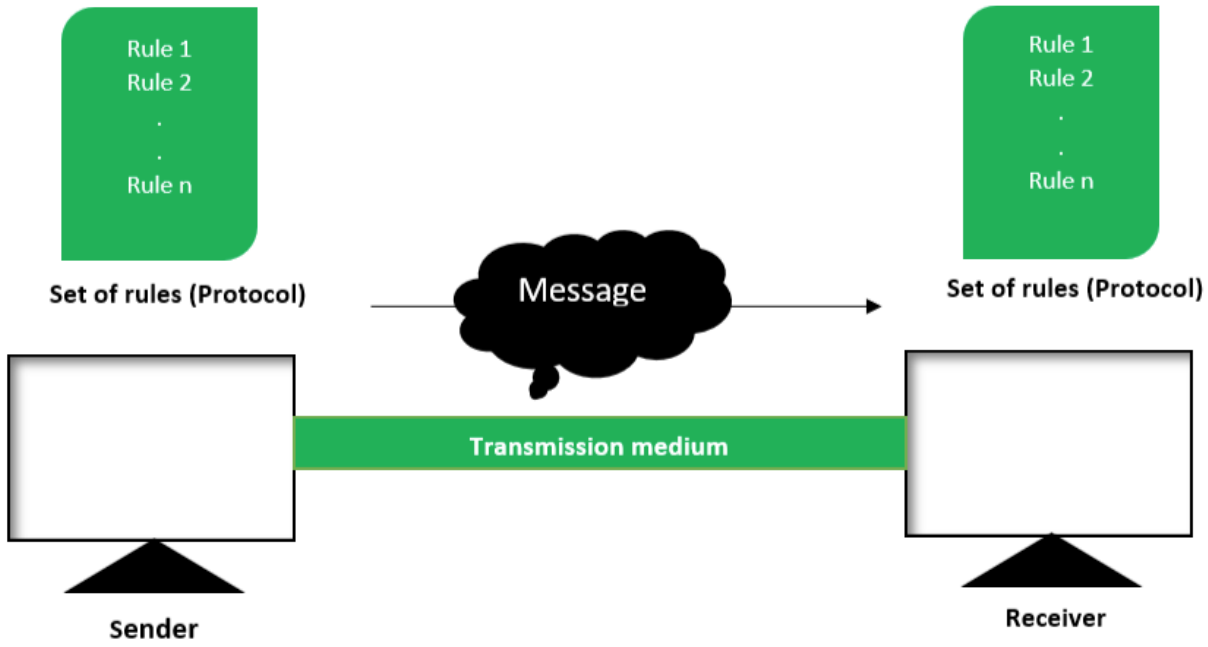


Рис.2.1. Телекомунікаційна система передаваня даних

Ключовим компонентом структури телекомунікаційних даних є заголовок. Заголовок - це частина пакета або кадру, яка містить службову інформацію про адреси джерела та призначення, тип даних та інші параметри. Заголовок дозволяє системі маршрутизувати, автентифікувати та групувати дані в правильному порядку. Окрім заголовка, телекомунікаційні дані також містять фактичне корисне навантаження та набір валідацій для виявлення помилок під час передачі. Формат передачі визначає порядок та розмір кожного елемента в пакеті, що є критично важливим для сумісності апаратного та програмного забезпечення. Формати даних різняться залежно від типу мережі, протоколу та застосування. Наприклад, Ethernet використовує чітко структурований формат кадру з полем MAC-адреси, ідентифікатором типу протоколу та полем CRC для перевірки цілісності. Мобільні мережі або VoIP-сервіси використовують інші формати, адаптовані до характеристик передачі голосу або відео. Різноманітність форматів та структур випливає з необхідності підвищення швидкості передачі даних, надійності та ефективності в різних середовищах.

Наприклад, для потокової передачі даних зменшення затримки є критично важливим, тоді як для фінансових транзакцій важливо підтримувати цілісність кожного байта. Варто також зазначити, що сучасні засоби зв'язку часто використовують технологію інкапсуляції, яка інкапсулює дані одного протоколу в структуру іншого протоколу. Це забезпечує прозору передачу між різними типами мереж та допомагає реалізувати складні мережеві архітектури, такі як віртуальні приватні мережі або хмарні обчислювальні рішення. Загалом, структура та формат комунікаційних даних – це складна та динамічна система, яка постійно розвивається. Нові технології, такі як 5G, Інтернет речей та квантовий зв'язок, вимагають нових форматів, які можуть забезпечити швидший, безпечніший та ефективніший обмін інформацією.

2.1.2 Джерела телекомунікаційних даних

Джерела телекомунікаційних даних охоплюють широкий спектр інформації, що генерується та обробляється в процесі використання телекомунікаційних послуг.

Ці дані включають як технічні, так і персональні дані, що відображають характеристики мережевого трафіку та поведінку окремих користувачів. Збір, обробка та аналіз цих даних відіграють важливу роль у забезпеченні ефективності телекомунікаційних систем, а також безпеки, маркетингу та обслуговування клієнтів. Трафік є одним з основних джерел телекомунікаційних даних. Трафік містить інформацію про дані, що передаються через мережу: обсяг, напрямок, час, тривалість, IP-адреси джерела та призначення, а також використані протоколи. Ці дані дозволяють операторам контролювати навантаження мережі, виявляти будь-які збої, планувати оновлення інфраструктури та надавати послуги клієнтам на основі фактичного використання. Ще одним важливим джерелом є журнали викликів (Call Detail Records, або CDR), які записують ідентифікаційні дані голосових викликів.

Ці журнали включають номер абонента, номер абонента, що приймає, дату та час виклику, тривалість виклику, тип виклику (місцевий, міжнародний, вхідний чи вихідний) та інші технічні параметри. Хоча сам вміст розмови не зберігається, ці метадані надзвичайно цінні для аналізу соціальних мереж, опитувань та бізнес-аналізу. Окрім журналів трафіку та викликів, дані користувачів також є одним із джерел комунікаційних даних. Це включає реєстраційну інформацію, таку як ім'я, адреса та паспортні дані, а також тарифні плани, записи про платежі та інформацію про налаштування технічного обладнання. Ці дані необхідні для ведення обліку користувачів, надання технічної підтримки та дотримання вимог законодавства, пов'язаних з ідентифікацією користувачів.

У сучасних мережах до джерел комунікаційних даних також додаються різні типи лог-файлів, що генеруються мережевим обладнанням та програмним забезпеченням. Ці файли можуть містити інформацію про помилки, спроби доступу, стан підключення, завантаження каналу та сповіщення про події. Ці дані є важливими для моніторингу безпеки, обслуговування та автоматизованого реагування на інциденти. Дані геолокації, зібрані через вежі стільникового зв'язку, GPS-пристрої або Wi-Fi-з'єднання, також відіграють важливу роль. Ці дані використовуються для визначення місцезнаходження користувачів, аналізу їхнього

місцезнаходження, налаштування послуг та ввімкнення систем навігації, безпеки та розслідування. У сфері мобільного Інтернету джерела телекомунікаційних даних також включають дані про використання мобільних додатків, тип пристрою, операційну систему, версію програмного забезпечення та час використання. Ці джерела даних є важливими для розробників, маркетологів та аналітиків, оскільки вони допомагають зрозуміти поведінку користувачів та покращити послуги. Усі ці джерела даних представляють величезну кількість інформації, яку потрібно впорядкувати та захистити. Великі дані та штучний інтелект відіграють дедалі більшу роль в обробці телекомунікаційних даних не лише для покращення роботи мережі, але й для прогнозування потреб користувачів, виявлення шахрайства або створення нових цифрових послуг.

2.1.3 Важливість обробки великих даних для прогнозування та виявлення аномалій

Обробка великих даних відіграє ключову роль у сучасних інформаційних системах, охоплюючи багато галузей, таких як зв'язок, фінанси, охорона здоров'я, транспорт тощо. Технологія великих даних, завдяки своїй здатності аналізувати величезні обсяги інформації в режимі реального часу, може не тільки фіксувати події, але й прогнозувати їх розвиток, виявляючи закономірності та аномалії, які традиційні аналітичні методи не можуть виявити [22-24].

Прогнозування є однією з найважливіших функцій обробки великих даних. У швидкозмінному середовищі, де обсяг інформації зростає щосекунди, здатність прогнозувати майбутні події або поведінку користувачів на основі історичних даних має вирішальне значення. Наприклад, у телекомунікаційних компаніях прогностичні можливості допомагають прогнозувати навантаження мережі, планувати розширення мережі, уникати перевантажень та забезпечувати стабільну якість з'єднання. Не менш важливою є здатність великих даних виявляти аномалії (події, що відхиляються від звичайної схеми). У багатьох випадках ці аномалії вказують на системні помилки, спроби зловмисного доступу, технічні збої або шахрайство.

Своєчасне виявлення аномалій може запобігти серйозним наслідкам, таким як витоки даних, фінансові втрати або перебої в обслуговуванні.

Моделі машинного навчання, що використовуються в аналізі великих даних, здатні навчатися на мільйонах прикладів та самостійно виявляти нові закономірності, не будучи явно запрограмованими. Це особливо важливо при роботі з неструктурованими або менш структурованими даними, де традиційні методи не працюють належним чином. Наприклад, текст, зображення та неструктуровані журнали подій можна точно аналізувати за допомогою цих методів. У сфері кібербезпеки аналітика великих даних дозволяє створювати адаптивні системи захисту, які можуть негайно реагувати на зміни в поведінці користувачів або появу нових загроз. Ці системи можуть виявляти підозрілу активність на основі профілів користувачів або мережевого трафіку, тим самим знижуючи ризики до того, як атаки завдадуть шкоди. Окрім сфери безпеки, прогнозна аналітика також широко використовується в сфері обслуговування клієнтів. За допомогою обробки великих даних можна прогнозувати потреби користувачів, надавати персоналізовані послуги, а також автоматично реагувати на зміни в емоціях чи інтересах користувачів. Це може покращити якість обслуговування, підвищити лояльність клієнтів та сприяти зростанню прибутку компанії (Рис.2.2).

Рис.2.2. Аналіз великих даних

Особливістю обробки великих даних є те, що вона вимагає потужної обчислювальної потужності та складних алгоритмів обробки. Водночас, з розвитком хмарних обчислень та технологій розподілених обчислень, аналіз у режимі

реального часу стає все більш доступним навіть для середніх підприємств. Це створює можливості для широкого застосування прогнозної аналітики в різних сферах. Таким чином, важливість обробки великих даних для прогнозування та виявлення аномалій стає дедалі помітнішою. Це вже не просто інструмент підтримки рішень, а важлива частина конкурентоспроможності, цифрової трансформації та стратегічного управління в епоху даних.

2.2 Аномалії у телекомунікаційних даних

2.2.1 Типи аномалій, які можуть виникати в телекомунікаційних системах

У телекомунікаційних системах може виникнути багато типів збоїв, які можуть негативно вплинути на якість зв'язку, безпеку даних та стабільність мережі. Найпоширенішими збоями є помилки зв'язку, спричинені фізичним пошкодженням лінії, втратою сигналу, поганою якістю каналу або відмовою обладнання.

Ці збої можуть призвести до втрати пакетів, обриву дзвінків, зниження швидкості мережі та інших збоїв у роботі мережі. До збоїв також належать нецільове використання телекомунікаційних ресурсів, таке як спам, атаки типу «відмова в обслуговуванні» або використання мережі для поширення шкідливого програмного забезпечення. У цьому випадку зловмисники навмисно перевантажують систему, порушують нормальну роботу або намагаються отримати доступ до конфіденційної інформації. Це створює серйозну загрозу як для користувачів, так і для операторів телекомунікацій.

Збої також можуть проявлятися в поведінці користувачів, що вказує на можливість шахрайства. Наприклад, раптове збільшення кількості дзвінків або повідомлень, зміна місцезнаходження користувачами на незвичне, використання нетипових послуг або підозріла комбінація послуг - все це може бути ознаками несанкціонованого доступу або зловживання. Несподівані зміни в трафіку даних у телекомунікаційних мережах також можуть виглядати ненормальними. Навантаження можуть раптово зростати через технічні проблеми та зовнішні події (наприклад, під час масових заходів або надзвичайних ситуацій). Якщо система не справляється з такими коливаннями, це може призвести до перевантажень або

перебоїв у наданні послуг. Помилки конфігурації часто спричинені людським фактором або автоматичними оновленнями. Неправильна конфігурація мережевого пристрою, зміни маршрутизації або неправильне застосування політик безпеки можуть порушити логіку обміну даними, що призводить до серйозних вразливостей безпеки.

Ще одним типом аномалії є проблема якості обслуговування, яка виникає, коли система не відповідає очікуваним стандартам, наприклад, коли швидкість мережі нижча за тарифний стандарт, або затримка голосового виклику перевищує дозволену межу. Такі ситуації зазвичай вимагають детального аналізу на основі історичних даних та постійного моніторингу. Аномалії можуть бути пов'язані з помилками системи виставлення рахунків, або коли з користувачів неправильно стягується плата за послуги, які не були надані, або навпаки - тобто фактична вартість не враховується. Це може спричинити конфлікти, підірвати довіру до операторів та вимагати складних процесів відновлення або перевірки. Також класифікуються аномалії, спричинені оновленнями програмного забезпечення або змінами в мережевій інфраструктурі. Після впровадження нового рішення можуть виникнути неочікувані збої, які раніше не помічалися. Використання автоматизованої системи моніторингу для виявлення цих помилок може швидко реагувати та зменшувати ризики для користувачів і всієї мережі.

2.2.2 Методи класифікації аномалій в телекомунікаційних системах

Методи класифікації аномалій у телекомунікаційних системах спираються на поєднання традиційних статистичних методів та сучасних методів штучного інтелекту. Класифікація спрямована на визначення типу, джерела, характеру аномалій та їхнього потенційного впливу на систему. Це допомагає ефективно реагувати, автоматично діагностувати проблеми та запобігати майбутнім збоям. Одним з основних методів є спостережна класифікація. Аномалії можуть бути точковими аномаліями (окрема подія або значення поза межами нормального діапазону) або контекстними аномаліями (на перший погляд нормальні в окремому контексті, але не відповідають іншим умовам). Існують також колективні аномалії

(група подій разом демонструє підозрілість, навіть якщо вони виглядають типовими окремо). За джерелом аномалій аномалії можна розділити на мережеві аномалії, аномалії користувачів та системні аномалії.

Мережеві аномалії включають порушення маршрутизації, перевантаження каналу або втрату з'єднання. Користувацькі аномалії стосуються поведінки користувача, яка виходить за межі нормального діапазону: надмірна активність, повторний набір підозрілих номерів та зміни географічного розташування. Системні аномалії пов'язані з внутрішньою роботою телекомунікаційного обладнання або програмного забезпечення, такими як збої, апаратні збої та помилки журналу.

Інший метод - класифікація за наслідками. Цей метод розрізняє нешкідливі аномалії, які не впливають на роботу мережі, потенційно небезпечні аномалії, які потребують моніторингу, та серйозні аномалії, які потребують негайного втручання. Ця ієрархія є критично важливою для автоматизованих систем реагування, оскільки система надає пріоритет серйозним загрозам. Класифікація на основі методів виявлення також широко використовується: детерміновані методи використовують заздалегідь визначені правила або пороги, статистичні моделі аналізують розподіли та ймовірності, а методи машинного навчання навчаються на історичних даних для виявлення складних закономірностей. До останніх належать дерева рішень, нейронні мережі, алгоритми кластеризації та алгоритми ізоляції. У сфері телекомунікацій також важлива класифікація за часом виявлення. Аномалії можна виявляти в режимі реального часу (онлайн-аналіз) або після того, як подія сталася (офлайн-аналіз). Онлайн-методи швидко реагують, але вимагають потужних обчислювальних ресурсів та високої точності.

Інший підхід полягає в класифікації аномалій на основі їхнього впливу на бізнес-операції. Аномалії можуть впливати на якість обслуговування клієнтів, безпеку даних, витрати оператора та навіть репутацію компанії. Тому класифікація зазвичай включає ключові бізнес-індикатори для визначення пріоритетів реагування. Ефективна класифікація аномалій у телекомунікаційних системах є багатогранним завданням, яке вимагає врахування технічних, поведінкових, часових

та бізнес-характеристик. Її впровадження допомагає розробляти інтелектуальні та адаптивні системи виявлення та управління подіями, які є важливими для операційної стабільності сучасних мереж.

2.2.3 Проблеми, що виникають при виявленні аномалій у реальних даних

Виявлення аномалій у даних зв'язку в реальному часі стикається з багатьма серйозними проблемами, які впливають на точну діагностику та ефективне реагування. Найсерйознішою проблемою є висока мінливість та неоднорідність даних. У системах зв'язку дані надходять з багатьох джерел – журналів подій, датчиків, систем виставлення рахунків та користувацьких пристроїв – і відрізняються за структурою, обсягом, точністю та частотою оновлення, що ускладнює інтеграцію та аналіз даних. Ще однією важливою проблемою є велика кількість шуму даних. Дані зв'язку в реальному часі часто містять неправильні або частково пошкоджені записи, дублікати значень та відсутні значення, що може призвести до неправильної роботи систем виявлення аномалій.

Крім того, оскільки умови мережі або поведінка користувачів постійно змінюються, система може інтерпретувати нові та навіть дійсні шаблони як підозрілі. Дисбаланс даних також є дуже поширеним явищем. У більшості випадків аномалії становлять лише невелику частину загальної кількості даних. Це створює проблеми для моделей машинного навчання, які можуть ігнорувати ці окремі випадки на користь виявлення ширших шаблонів, тим самим пропускаючи ключові відхилення.

Ще однією серйозною перешкодою є складність точного визначення аномалій. У реальному світі не існує єдиного або суворого стандарту для виявлення аномалій. Поведінка, яка вважається аномальною в одному контексті, може бути цілком нормальною в іншому. Наприклад, раптове збільшення трафіку може бути спричинене атакою, підвищенням на посаді або святом. Ще однією проблемою є необхідність обробки даних у режимі реального часу. Своєчасне виявлення аномалій часто є критично важливим для уникнення втрат або збоїв, але обробка

високошвидкісних потоків даних вимагає потужних апаратних ресурсів, оптимізованих алгоритмів та складних архітектур систем моніторингу.

Поширеною проблемою є відсутність добре маркованих навчальних даних для побудови моделей. У багатьох випадках компанії не мають детальних історичних записів аномалій, або ці дані є конфіденційними і тому їх важко використовувати для навчання. Це ускладнює застосування моделей машинного навчання, особливо в завданнях навчання з учителем. Інтерпретація результатів також є проблемою. Навіть якщо система виявляє аномалію, важливо пояснити, чому вона була класифікована як підозріла. Багато сучасних алгоритмів, включаючи глибокі нейронні мережі, схожі на «чорні скриньки» і не можуть надати чітких пояснень своїх рішень, що ускладнює їх використання в критично важливих системах. Поведінка користувачів, конфігурація мережі або типові моделі трафіку змінюються з часом. Якщо модель не оновлюється або їй бракує адаптивних можливостей, її ефективність у виявленні поточних аномалій швидко знизиться. Це вимагає постійного обслуговування, перенавчання моделі та гнучких алгоритмів.

2.3 Особливості використання нейронних мереж для прогнозування аномалій в телекомунікаційних даних

2.3.1 Переваги застосування нейронних мереж для роботи з великими даними

Використання нейронних мереж для обробки великих даних відкриває величезні можливості для аналізу, прогнозування та автоматизації процесів у всіх галузях промисловості. Однією з найважливіших переваг нейронних мереж є їхня здатність виявляти складні та приховані залежності від величезних обсягів інформації, з якими традиційні алгоритми можуть бути не в змозі обробити. Завдяки глибокому навчанню моделі здатні розпізнавати багатовимірні закономірності та отримувати точніші результати навіть під час обробки неструктурованих або частково заповнених даних.

Ще однією важливою перевагою нейронних мереж є їхня висока адаптивність, оскільки вони можуть навчатися на нових даних, що дозволяє постійно оновлювати

моделі без необхідності переписувати алгоритм. Такий підхід особливо ефективний у динамічних середовищах, де дані швидко змінюються, наприклад, у фінансовій сфері або в системах моніторингу безпеки мережі. Нейронні мережі також мають чудову масштабованість і здатні одночасно обробляти величезні обсяги даних, що робить їх незамінною частиною великих центрів обробки даних та хмарних середовищ. Ця продуктивність скорочує час обробки та підвищує ефективність аналізу даних, що є важливим для компаній, які щодня генерують великі обсяги інформації. Перевагою нейронних мереж є також їхня універсальність. Вони успішно застосовуються для класифікації, регресії, кластеризації, обробки природної мови, обробки зображень, обробки аудіо та інших типів даних. Це дозволяє створювати складні аналітичні системи, що об'єднують різні джерела інформації в єдину модель.

Нейронні мережі демонструють надзвичайно високу точність прогнозування результатів. Завдяки своїй здатності враховувати мільйони параметрів одночасно, вони можуть забезпечити глибший аналіз, ніж традиційні статистичні методи. Наприклад, у сфері охорони здоров'я це дозволяє раннє виявлення захворювань або високонадійні прогнози ефектів лікування. Також варто відзначити здатність нейронних мереж до автономного навчання. Завдяки методам глибокого навчання та зворотного поширення помилок моделі покращують прогнози без втручання людини. Це значно спрощує обслуговування аналітичних систем, зменшує витрати на людські ресурси та скорочує час, необхідний для впровадження нових рішень.

У багатьох випадках нейронні мережі мають кращу толерантність до шуму даних. Вони ефективно працюють навіть з неповними, зашумленими або неправильними записами, які є поширеними у великих наборах даних. Це значно зменшує ймовірність помилок та підвищує надійність моделей. Нарешті, застосування нейронних мереж сприяє інноваціям та розвитку нових технологій. Вони складають основу штучного інтелекту, машинного навчання, автономних систем та численних сучасних додатків, які постійно змінюють спосіб роботи з великими даними. Їхнє застосування не лише сприяє технологічному прогресу, але й

сприяє стратегічному зростанню компаній, які активно використовують ці інструменти для своєї діяльності.

2.3.2 Використання нейронних мереж для передбачення проблем в мережах зв'язку

Використання нейронних мереж для прогнозування проблем телекомунікаційних мереж може ефективно виявляти потенційні збої до їх виникнення. Завдяки можливості аналізу великих обсягів телеметричних даних, моделі штучного інтелекту можуть виявляти будь-які аномалії в трафіку даних, навантаженні або поведінці окремих компонентів мережі. Це значно знижує ризик раптових перебоїв та дозволяє операторам зв'язку вживати проактивних заходів для забезпечення безперебійної роботи інфраструктури. Нейронні мережі здатні ефективно обробляти потоки даних у режимі реального часу з різних джерел, таких як маршрутизатори, комутатори, базові станції або користувацьке обладнання. Це дає змогу створювати системи моніторингу, які не тільки фіксують поточний стан, але й прогнозують майбутні проблеми, такі як перевантаження каналу, зниження пропускної здатності або погіршення якості обслуговування.

Моделі глибокого навчання можуть виявляти закономірності, які важко виявити людям або традиційним аналітичним методам. Наприклад, вони можуть навчитися виявляти ознаки деградації обладнання на основі незначних змін параметрів, що дозволяє своєчасно проводити технічне обслуговування. Це допомагає знизити витрати на ремонт і покращити обслуговування клієнтів. У телекомунікаційних системах затримка реагування на події є критично важливою, і нейронні мережі можуть забезпечувати аналіз майже в режимі реального часу. Вони можуть автоматично генерувати попередження про потенційні збої, дозволяючи технікам швидше реагувати на загрози. Такий підхід не лише зменшує час простою мережі, але й підвищує загальну надійність обслуговування. Оскільки нейронні мережі можуть враховувати кілька факторів одночасно, вони допомагають точно визначити першопричину проблеми. Це не лише виявляє несправності, але й дозволяє розробляти довгострокові стратегії для покращення мережевої

інфраструктури. Це зменшує кількість повторюваних проблем і підвищує ефективність використання ресурсів.

Інтеграція нейронних мереж у системи управління мережею дозволяє автоматизувати рутинні завдання. Замість постійного ручного моніторингу та аналізу даних, оператори можуть покладатися на інтелектуальні моделі, щоб автономно вирішувати, як маршрутизувати, визначати пріоритети або перенаправляти трафік, коли навантаження зростає. Це особливо важливо для великих мереж з тисячами вузлів. Завдяки своїм можливостям самонавчання нейронні мережі можуть постійно покращувати точність своїх прогнозів.

Моделі можуть адаптуватися до змін в архітектурі мережі, нових типів трафіку або атак, забезпечуючи стабільну аналітичну точність. Це дозволяє мережі залишатися стійкою перед обличчям нових викликів, включаючи зростання обсягів даних та кіберзагроз. Загалом, використання нейронних мереж для прогнозування проблем телекомунікаційних мереж допомагає створювати розумніші, більш адаптивні та надійніші телекомунікаційні системи. Такий підхід змінює традиційну модель управління мережею та дозволяє перейти від реактивного до проактивного обслуговування, що є критично важливим для забезпечення стабільної роботи послуг та задоволення потреб користувачів у сучасній цифровій економіці.

2.3.3 Моделі для автоматичного виявлення аномалій у телекомунікаційних системах

Моделі автоматичного виявлення аномалій у телекомунікаційних системах є важливим інструментом для підтримки надійності та стабільності мережі. Сучасна телекомунікаційна інфраструктура генерує величезні обсяги даних у режимі реального часу, і виявлення аномалій у цих потоках даних надзвичайно складне без використання інтелектуальних алгоритмів.

Методи машинного навчання та нейронних мереж можуть ефективно виявляти аномалії в роботі системи до того, як виникнуть серйозні проблеми або збої в роботі. Одним із найпоширеніших методів виявлення аномалій є використання автокодерів. Ці нейронні мережі навчаються стискати та відновлювати вхідні дані, що дозволяє

їм розпізнавати знайомі системні шаблони. Коли автокодер зустрічає нову або незвичайну інформацію, його помилка відновлення збільшується – ця помилка вказує на наявність аномалії. Це робить автокодери дуже ефективними у виявленні аномальної поведінки у складних багатовимірних наборах даних.

Ще одним поширеним методом є використання рекурентних нейронних мереж, особливо LSTM. Ці мережі здатні ефективно обробляти часові ряди, такі як метрики трафіку, затримка сигналу або активність користувачів у мережі. Системи LSTM навчаються прогнозувати наступне значення на основі попередніх значень. Якщо фактичне значення значно відрізняється від прогнозованого, це може свідчити про завантаження або збій мережі. Також широко використовуються моделі кластеризації, які здатні групувати подібні дані в групи та виявляти елементи даних, що не належать до жодної групи. Ці елементи даних можуть свідчити про збої в мережі, атакуючу активність або неочікувані зміни в конфігурації пристрою. Кластеризація особливо ефективна при аналізі великих обсягів неструктурованої або частково структурованої інформації. У складних системах зв'язку все частіше використовуються гібридні моделі, які поєднують сильні сторони кількох підходів. Наприклад, автокодери можна поєднувати з класифікаторами або правилами, заснованими на експертних знаннях, для точнішого виявлення аномалій. Ці системи не тільки здатні виявляти аномалії, але й автоматично приймати рішення щодо інших дій, таких як перенаправлення трафіку або надсилання сповіщень адміністраторам. Ще однією перспективною тенденцією є використання байєсівських мереж, які здатні оцінювати ймовірність аномалій на основі статистичного аналізу. Вони будують ймовірнісні моделі типової роботи системи, а потім порівнюють нові спостереження з цими моделями.

Якщо ймовірність спостережуваної закономірності занадто низька, система ідентифікує її як аномалію. У випадках, пов'язаних з поведінкою користувача або пристрою, поведінкові моделі використовуються для створення профілів типової діяльності. Відхилення від типових закономірностей, такі як різке збільшення обсягу переданих даних, часті підключення до невідомих адрес або незвичайне географічне

розташування підключень, можуть свідчити про зловмисну активність або технічні збої. Ці моделі особливо важливі в галузі мережевої безпеки. Сучасні оператори зв'язку все частіше інтегрують системи виявлення аномалій безпосередньо у свою інфраструктуру, включаючи хмарні сервіси та периферійні пристрої. Це дозволяє їм реагувати на проблеми в режимі реального часу та зменшувати навантаження на центральні сервери. Тому автоматичне виявлення аномалій стало важливою частиною сучасних систем управління зв'язком, забезпечуючи надійність, адаптивність та безпеку системи.

Автоматичне виявлення аномалій стало невід'ємною частиною сучасних систем управління зв'язком. Процес передбачає використання власних алгоритмів для виявлення будь-яких відхилень від нормальних робочих характеристик системи. Такий підхід дозволяє своєчасно реагувати на потенційно небезпечні ситуації, тим самим підвищуючи надійність та безпеку зв'язку. Складність мереж та зростаючий обсяг даних щороку вимагають більш ефективних засобів моніторингу. У системах зв'язку автоматичне виявлення аномалій дозволяє швидко реагувати на порушення, які можуть виникати під час передачі інформації, що може включати збої мережевого обладнання, атаки на інфраструктуру або проблеми з обробкою даних.

Завдяки вбудованим алгоритмам система здатна негайно виявляти аномалії, тим самим знижуючи ризики та значно пришвидшуючи вирішення потенційних проблем. Системи автоматичного виявлення аномалій здатні адаптуватися до змін у мережі та оптимізувати операції без постійного втручання людини. Вони збирають інформацію про нормальну роботу, а потім порівнюють її з фактичними умовами. Якщо дані відхиляються від нормальних значень, система вказує на потенційні проблеми, тим самим запобігаючи серйозним збоям або витокам даних.

Однією з найважливіших переваг використання автоматичного виявлення аномалій є зменшення робочого навантаження на співробітників. Технічні експерти можуть зосередитися на вирішенні критичних проблем, поки система автоматично контролює та аналізує величезні обсяги даних. Це підвищує ефективність роботи та зменшує можливість людської помилки. Зі швидким розвитком технологій та

постійним зростанням обсягу інформації безпека систем зв'язку стала головним пріоритетом. Аномалії можуть свідчити не лише про технічну проблему, але й про кібератаку, таку як спроби несанкціонованого доступу або надсилання шкідливих повідомлень. Автоматичне виявлення цих вразливостей дозволяє негайно вжити заходів для захисту інформації та підтримки безпеки мережі.

Покращення адаптивності системи є ще одним важливим компонентом автоматичного виявлення аномалій. Мережі зв'язку швидко змінюються, постійно з'являються нові пристрої, послуги та дані. Системи, які можуть виявляти аномалії, повинні не лише реагувати на поточні вразливості, але й передбачати потенційні загрози в майбутньому. Це може скоротити час реагування та мінімізувати вплив на продуктивність мережі. Технологія автоматичного виявлення аномалій також може покращити здатність системи до самовідновлення, дозволяючи їй швидко виявляти несправності, які можуть спричинити перебої в роботі мережі, та вживати необхідних заходів для вирішення проблеми без зовнішнього втручання. Це означає, що мережа буде більш стійкою та менш схильною до тривалих перебоїв або технічних збоїв.

Завдяки цим технологіям сучасні телекомунікаційні системи працюють ефективніше, надійніше та безпечніше. Можливості автоматичного виявлення аномалій гарантують негайне реагування на будь-які відхилення, що зрештою покращує загальний рівень обслуговування та зменшує ризики для користувачів. В результаті сучасні телекомунікаційні мережі будуть стабільнішими та зможуть справлятися з будь-якими викликами.

Технології автоматичного виявлення аномалій стали основними технологіями в багатьох галузях, таких як інформаційні системи та мережева безпека. Вони здатні виявляти нерівності або аномалії в даних або поведінці системи без прямого втручання людини. Ці технології спираються на алгоритми машинного навчання, які можуть навчитися визначати нормальні закономірності в даних та оперативно виявляти будь-які відхилення від нормальних закономірностей. Це дозволяє негайно реагувати на потенційно небезпечні або неочікувані ситуації, значно знижуючи

ризики. Однією з найважливіших переваг цих технологій є їхня здатність працювати в режимі реального часу, постійно аналізуючи потоки даних та виявляючи будь-які аномалії. Це особливо важливо в таких галузях, як мережева безпека, де навіть найменше відхилення може свідчити про хакерську атаку або іншу загрозу. Такий підхід дозволяє негайно реагувати на загрози, значно скорочуючи час, необхідний для захисту від атак. Використання технологій автоматичного виявлення аномалій також допомагає зменшити навантаження на людські ресурси. Ці системи можуть автоматично виявляти нерівності без ручної перевірки всіх даних або процесів, дозволяючи експертам зосередитися на складніших завданнях. Це підвищує ефективність та швидкість реагування на системні проблеми. Технології автоматичного виявлення аномалій використовуються не лише для виявлення проблем, але й для підвищення загальної ефективності системи. Наприклад, у фінансовій сфері ці технології допомагають виявляти шахрайські операції або аномальні транзакції, що дозволяє негайно запобігати підозрілій поведінці. У виробничому процесі ці системи можуть виявляти нестандартні робочі параметри обладнання, що дозволяє своєчасно проводити технічне обслуговування та запобігати збоям.

Удосконалені алгоритми машинного навчання є одним з ключових досягнень у технологіях автоматичного виявлення аномалій. Завдяки останнім досягненням у цій галузі ці системи стали більш аналітично складними. Вони можуть не тільки виявляти порушення, але й прогнозувати майбутні аномалії, аналізуючи історичні дані та тенденції. Це дозволяє розробляти ефективніші плани дій та профілактичні заходи, перш ніж проблеми стануть серйозними. Ще одним важливим аспектом є адаптивність цих технологій до змін у системі. Зі зміною умов або появою нових стандартів алгоритми можуть коригувати свої моделі, щоб зберегти їхню актуальність та точність. Це робить системи автоматичного виявлення аномалій ефективними не лише за стабільних умов експлуатації, але й у періоди змін або нестандартних ситуацій. Технології автоматичного виявлення аномалій є важливими для забезпечення безпеки сучасної інфраструктури. Вони допомагають виявляти

мережеві вторгнення, атаки на інформаційні системи або зловмисні зміни даних. Це дозволяє виявляти кібератаки негайно, перш ніж вони можуть завдати значної шкоди. Як наслідок, ці технології формують основу для підтримки цілісності та конфіденційності даних у сучасному цифровому світі. Нарешті, технології автоматичного виявлення аномалій стають важливим фактором у забезпеченні стабільності та надійності різних систем. Вони не тільки знижують ризики та роблять процеси управління ефективнішими, але й сприяють розробці нових та розумніших рішень у різних галузях. Популярність цих технологій зростає з року в рік, а їх застосування постійно розширює можливості автоматизації та вдосконалення процесів у багатьох галузях.

Загалом, використання нейронних мереж для прогнозування проблем комунікаційних мереж є одним із ключових напрямків розвитку сучасних інтелектуальних технологій. Завдяки своїй здатності навчатися на величезних наборах даних, нейронні мережі здатні виявляти приховані закономірності та складні взаємозв'язки, які важко або навіть неможливо виявити традиційними методами. Це відкриває нові можливості для запобігання технічним збоям, оптимізації ресурсів та забезпечення стабільної роботи мережі. У сфері комунікацій нейронні мережі здатні миттєво виявляти потенційні загрози, такі як перевантаження каналів, відмова обладнання або аномалії трафіку.

Ці системи можуть аналізувати історичні та поточні дані, визначати сценарії ризику та автоматично генерувати прогнози для подальшого розвитку. Це дозволяє операторам не тільки швидко реагувати на проблеми, але й запобігати їм до їх виникнення. Однією з переваг нейронних мереж є їхня здатність до самонавчання. У міру накопичення нових даних мережа покращує точність своїх прогнозів, роблячи систему більш гнучкою та здатною адаптуватися до змін у середовищі. Це особливо важливо в контексті динамічної еволюції комунікаційної інфраструктури, з появою нових форматів передачі даних, зміною протоколів зв'язку та новими типами навантажень. Інтеграція нейронних мереж у системи моніторингу може забезпечити автоматичне виявлення несправностей та підвищити ефективність обслуговування.

Наприклад, система може передбачати, коли певний пристрій потрібно замінити або оновити, тим самим знижуючи ризик аварій та зменшуючи витрати на ремонт. Це особливо важливо для великих операторів, які керують масштабними мережами та мають обмежені ресурси для постійного ручного моніторингу. Нейронні мережі також можуть допомогти покращити якість обслуговування користувачів. Прогнозування пікових навантажень та потенційних затримок може заздалегідь скоригувати маршрутизацію даних та забезпечити стабільну швидкість з'єднання. Кінцеві користувачі отримають надійніші з'єднання з меншою кількістю затримок та перерв, що є важливим для таких послуг, як відеозв'язок, прямі трансляції та онлайн-ігри.

Завдяки гнучкості архітектур нейронних мереж їх можна адаптувати до конкретних завдань у системах зв'язку, таких як прогнозування навантажень у певних зонах та виявлення індикаторів мережевих загроз. Такий підхід дозволяє створювати спеціалізовані інтелектуальні моделі, що враховують характеристики інфраструктури, поведінку користувачів та бізнес-цілі оператора. Нейронні мережі також є ефективним інструментом для аналізу великих обсягів неструктурованих даних, які часто виникають під час роботи систем зв'язку. Наприклад, вони можуть обробляти журнали подій, повідомлення пристроїв або запити клієнтів і перетворювати ці дані на корисну інформацію, яка допомагає керівництву приймати рішення. Це допомагає глибше зрозуміти операції та покращити координацію між технічними та бізнес-відділами. Тому використання нейронних мереж для прогнозування проблем комунікаційної мережі може не тільки запобігти інцидентам та знизити витрати, але й створити умови для побудови розумніших, адаптивніших та надійніших систем зв'язку. У майбутньому ці технології відіграватимуть дедалі важливішу роль у забезпеченні стабільності цифрової інфраструктури, що є важливим для нормального функціонування сучасного суспільства.

Розвиток нейронних мереж у сфері комунікацій тісно пов'язаний із застосуванням штучного інтелекту та концепцій великих даних. Зі збільшенням кількості підключених пристроїв зростає також обсяг інформації, яку необхідно

аналізувати в режимі реального часу. Оскільки нейронні мережі можуть обробляти величезні набори даних, вони здатні ефективно обробляти ці потоки даних та витягувати ключову інформацію для швидкого прийняття рішень. Це дозволяє мережам не лише реагувати пасивно, але й проактивно – прогнозувати та уникати більшості проблем до їх виникнення. Ще одним важливим аспектом є можливість інтеграції нейронних мереж з іншими технологіями, особливо з хмарними обчисленнями та обробкою даних на периферії. Це дозволяє масштабувати рішення до різних масштабів – від центральних центрів обробки даних до окремих вузлів мережі. Це також дозволяє створити єдину розподілену систему прогнозування, яка може швидко реагувати на локальні зміни, не впливаючи на загальну ситуацію всієї мережі.

Використання глибоких нейронних мереж відкриває нові способи розпізнавання складних закономірностей та виявлення нетипових сценаріїв, які раніше не помічали. Наприклад, вони можуть виявляти потенційні загрози, які розвиваються повільно та проявляються як очевидні помилки лише тоді, коли трапляється серйозний інцидент. Отже, штучний інтелект не лише розширює аналітичні можливості системи, але й покращує її прогностичні можливості в складних та динамічних середовищах. У 5G та майбутніх поколіннях мобільного зв'язку перспективи застосування нейронних мереж є багатообіцяючими. Ці мережі мають дедалі вищі вимоги до швидкості, стабільності та обробки величезних обсягів даних у режимі реального часу. Використання інтелектуальних моделей на основі нейронних мереж дозволяє ефективніше керувати ресурсами, зменшує затримку, забезпечує балансування навантаження та забезпечує найвищий рівень обслуговування навіть у години пік.

Окрім технічного аспекту, нейронні мережі також впливають на стратегічне планування телекомунікаційних компаній. Аналіз на основі прогностичних моделей допомагає приймати бізнес-рішення, пов'язані з розширенням інфраструктури, впровадженням нових послуг або покращенням існуючих операцій. Це допомагає знизити витрати, підвищити конкурентоспроможність та швидше та ефективніше

адаптуватися до потреб ринку. У майбутньому, з розвитком квантових обчислень та нових архітектур глибокого навчання, можливості нейронних мереж у сфері телекомунікацій будуть ще більше розширені. Вони зможуть не тільки прогнозувати проблеми, але й навчатися автономно коригувати стратегії управління мережею на основі змін у зовнішньому середовищі або внутрішніх факторах. Це прокладе шлях для створення повністю автономних та самокерованих мереж наступного покоління [24-26].

Висновок до розділу 2

У розділі розглянуто структуру та формат даних, що використовуються в сучасних системах зв'язку. Масові джерела даних, такі як трафік, журнали викликів та дані користувачів, вимагають спеціалізованих методів обробки. Ці джерела даних містять величезну кількість інформації, яка дозволяє операторам точно аналізувати поточний стан мережі та прогнозувати її поведінку. Обробка великих даних є основоположною для прогнозування та виявлення аномалій, що може підвищити ефективність та надійність систем зв'язку.

Використання нейронних мереж для прогнозування аномалій у даних зв'язку має значні переваги. Вони здатні аналізувати великі обсяги інформації та виявляти складні закономірності, які можуть бути не виявлені традиційними методами. Це особливо важливо для великих телекомунікаційних операторів, які обробляють величезні обсяги даних у режимі реального часу.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПРОГНОЗУВАННЯ АНОМАЛІЙ

3.1 Ключові проблеми при виявленні аномалій

Виявлення аномалій є критично важливим завданням у багатьох галузях, таких як кібербезпека, медицина та фінансове регулювання. Однак цей процес пов'язаний з багатьма труднощами, які ускладнюють створення ефективних та точних систем. Однією з найголовніших проблем є брак високоякісних, збалансованих даних. Аномалії трапляються рідко, що призводить до сильно незбалансованих наборів даних, що ускладнює навчання моделей машинного навчання. Ще однією проблемою є висока мінливість аномалій. Одна й та сама поведінка може вважатися нормальною або підозрілою в різних контекстах. Це перешкоджає розробці комплексних методів виявлення аномалій, які повинні враховувати контекст та характеристики конкретного завдання чи галузі.

Варто також зазначити, що важко визначити чіткі критерії класифікації аномальних даних. У багатьох випадках немає попередньо визначених правил, що ускладнює створення базової моделі. Це призводить до використання евристик або методів без нагляду, які не завжди забезпечують необхідну точність. Проблема шуму даних також є важливим фактором. Високий рівень шуму може маскувати реальні аномалії або створювати хибні сигнали, які система розглядає як відхилення. В результаті, кількість хибнопозитивних результатів збільшується, що знижує достовірність моделі та вимагає додаткової ручної перевірки. Питання масштабованості також є критично важливим. Під час роботи з великими обсягами даних системи виявлення аномалій повинні демонструвати високу продуктивність без шкоди для точності. Це вимагає вдосконалення алгоритмів та використання розподілених обчислень, що збільшує складність впровадження.

Поведінка даних змінюється з часом, і модель, яка була точною вчора, сьогодні може бути застарілою. Тому система повинна мати можливість автономно адаптуватися до змін у середовищі, зберігаючи при цьому здатність виявляти нові, раніше невідомі аномалії.

Особливу увагу необхідно приділяти інтерпретації результатів. У багатьох галузях, таких як медицина чи фінанси, важливо не лише виявляти аномалії, а й пояснювати їх причини. Багато сучасних моделей, особливо глибокі нейронні мережі, працюють як «чорні скриньки», що ускладнює пояснення рішень. Нарешті, етичні та правові міркування також можуть створювати перешкоди. Автоматичне виявлення аномалій у персональних або конфіденційних даних може призвести до порушень конфіденційності або дискримінації. Це вимагає ретельного збору даних, налаштування моделі та дотримання нормативних вимог. Окрім вищезазначених аспектів, вирішальним є також складність інтеграції систем виявлення аномалій у реальні бізнес-процеси. Існуючі організаційні структури та IT-інфраструктура часто не підходять для впровадження цих рішень, що створює технічні та управлінські труднощі. Ефективна інтеграція вимагає не лише технічної підтримки, але й удосконалення внутрішніх процесів, навчання співробітників та постійного моніторингу продуктивності системи. Варто також зазначити, що покладатися на ознаки чи характеристики, що використовуються для навчання моделі, є проблематичним. Вибір нерелевантних або надто загальних ознак значно знижує здатність системи виявляти аномальну поведінку. Цей процес часто вимагає глибоких знань предметної області, а автоматичний вибір ознак не завжди дає очікувані результати, особливо у складних або динамічних середовищах.

Відсутність чітко визначених аномалій у даних ускладнює об'єктивну оцінку точності моделі. У цьому випадку необхідно вручну перевіряти результати або створювати штучні аномалії для тестування, які можуть не повністю відповідати фактичній ситуації. Крім того, у багатьох випадках аномалії є не окремими точками, а послідовностями або часовими закономірностями. Це ускладнює завдання та вимагає використання спеціалізованих методів, таких як рекурентні нейронні мережі або моделі, що враховують часові ряди. У цьому випадку простих статистичних методів недостатньо для досягнення необхідної точності та надійності.

Не слід також ігнорувати проблему узагальнення моделей. Моделі, навчені на одному джерелі даних, можуть погано працювати на інших наборах даних (навіть

схожих). Це обмежує можливості масштабування рішень або повторного використання моделей у різних середовищах без додаткового налаштування чи перенавчання. Насправді, важливо також реагувати на виявлені аномалії. Виявлення без відповідного механізму реагування втрачає свій сенс. Багато систем просто позначають аномалії, але не надають інструментів для автоматичного аналізу, ізоляції проблем або прийняття рішень. Це відкриває нові шляхи для розробки інтегрованих рішень, що поєднують виявлення та реагування. Проблеми також виникають у випадках, коли потрібно враховувати зв'язки між об'єктами. Наприклад, у сфері соціальних мереж або кібербезпеки аномалії можуть бути пов'язані з колективною поведінкою, яка не є очевидною на рівні окремих даних. У цьому випадку нам потрібні графові моделі та методи, які можуть виявляти складні залежності між об'єктами. Успішна система повинна не лише точно та швидко виявляти аномалії, але й бути прозорою, адаптивною, масштабованою та здатною підтримувати прийняття рішень у складних та мінливих умовах.

Це вимагає складніших систем, що поєднують машинне навчання, аналіз графів, інтерфейси зворотного зв'язку та автоматизовані механізми реагування. Такий підхід не лише виявляє аномалії, але й розуміє контекст, у якому вони виникають - як вони пов'язані з іншими елементами системи, які наслідки вони можуть мати та які дії слід вжити. Це критично важливо для виявлення прихованих загроз, що маскуються під нормальну поведінку, що дозволяє враховувати структуру взаємодій у всій системі. Крім того, важливо зазначити, що дані, на яких працює система, часто є неповними, зашумленими або містять суперечливу інформацію. Це створює додаткову проблему для забезпечення стабільності моделі, оскільки модель повинна бути здатною відрізняти справді важливі сигнали від випадкових коливань. Для цього потрібна попередня обробка, очищення даних та більш стійкі до шуму алгоритми виявлення. Здатність системи ефективно працювати в таких умовах є ще одним важливим показником її практичної цінності.

Взаємодія людини з машиною не менш важлива. Повна автоматизація не завжди бажана, тому ефективна система повинна підтримувати гібридну модель

взаємодії, яка дозволяє людям перевіряти, пояснювати або виправляти рішення. Це може поєднувати машинну швидкість, інтуїцію та людський досвід, що особливо корисно в складних або неоднозначних ситуаціях. В останні роки етичне використання систем виявлення аномалій отримало значну увагу, особливо з точки зору конфіденційності даних, упередженості моделі та прозорості рішень. З одного боку, система повинна бути максимально ефективною, водночас гарантуючи, що права користувачів не порушуються. Це вимагає впровадження певних політик, механізмів валідації та регулярних системних аудитів незалежними експертами.

3.1.1 Прозорість системи

Прозорість є однією з найважливіших характеристик систем виявлення аномалій, особливо в таких критично важливих секторах, як охорона здоров'я, банківська справа, енергетика та державне управління. Це означає здатність розуміти, як і чому система прийняла певне рішення, тобто ідентифікувала конкретний випадок як аномалію. Без цієї прозорості користувачам важко довіряти результатам системи, а розробникам – виправляти або покращувати їх. Однією з найбільших перешкод для прозорості є використання складних моделей, таких як глибокі нейронні мережі, які часто діють як «чорні скриньки». Вони здатні досягати високої точності, але не надають чітких пояснень своїх рішень. Це створює ризики, особливо коли системні помилки мають серйозні наслідки, такі як відмови у видачі кредитів, неправильні діагнози або хибні звинувачення у шахрайстві.

Ще один спосіб забезпечення прозорості – це використання простіших, більш інтерпретованих моделей, таких як дерева рішень, правила асоціації або статистичні методи, де логіка прийняття рішень є чіткою та явною. Хоча ці моделі можуть бути не такими точними, як складні моделі нейронних мереж, їх легше тестувати, перевіряти та адаптувати до змін у середовищі. Прозорість також допомагає посилити підзвітність. Коли кожна аномалія пояснюється, відповідальність можна чітко розподілити між системами, розробниками, користувачами та керівництвом. Це особливо важливо для дотримання таких нормативних актів, як Загальний регламент про захист даних, який вимагає можливості пояснювати рішення,

прийняті автоматизованими системами. Варто також зазначити, що прозорість має освітнє значення – вона дозволяє операторам та аналітикам краще розуміти природу аномалій, покращувати свої аналітичні навички, виявляти нові закономірності та накопичувати знання, які згодом можна використовувати для оновлення правил або створення нових моделей.

Зрештою, прозорість - це місток між алгоритмами та людьми. Це допомагає подолати недовіру людей до штучного інтелекту та створює умови для тіснішої співпраці між автоматизованими аналітичними системами та людським досвідом. У майбутньому прозорі системи виявлення аномалій стануть не лише інструментом контролю, але й ефективним партнером у прийнятті складних рішень.

3.1.2 Адаптивність системи

Адаптивність системи виявлення аномалій стосується її здатності реагувати на зміни в середовищі, даних або поведінці користувача без повного перенавчання чи втручання людини. У реальному світі дані не є статичними: змінюються умови роботи, виникають нові типи поведінки, а також нові загрози або сценарії використання. Якщо система не може адаптуватися до цих змін, вона швидко втратить свою ефективність і або ігноруватиме аномалії, або фіксуватиме їх, коли їх немає. Ключовим елементом адаптивності є здатність системи до самонавчання. Це означає, що вона може оновлювати своє розуміння норм у режимі реального часу на основі нових даних. Такий підхід особливо важливий у високодинамічних областях, таких як фінансові операції, інтернет-трафік або поведінка користувачів в онлайн-сервісах. Використання алгоритмів онлайн-навчання дозволяє системі поступово перебудовувати модель, зберігаючи при цьому здатність виявляти невідомі аномалії.

Ще однією важливою особливістю адаптивності є здатність виявляти концептуальні аномалії, які є явищами, коли структура або природа “нормальних” даних змінюється з часом. Наприклад, поведінка клієнтів може змінюватися під час свят, або логіка обробки даних може змінюватися в нових версіях програмного забезпечення. Якщо система не враховує ці зміни, вона почне генерувати велику кількість хибних спрацьовувань. Для вирішення цієї проблеми використовуються

методи відстеження змін у розподілі даних та автоматичного оновлення припущень щодо нормальної поведінки. Адаптивна система повинна включати механізми зворотного зв'язку з користувачем. Наприклад, якщо оператор класифікує подію як хибну тривогу, система повинна враховувати цю інформацію в майбутньому, тим самим підвищуючи точність та зменшуючи кількість хибних спрацьовувань. Це не тільки зменшує навантаження на співробітників, але й дозволяє ефективніше адаптувати модель до характеристик конкретної організації чи процесу.

Однак адаптивність - це не лише технічна особливість; вона також пов'язана із загальною архітектурою системи. Гнучка та модульна система дозволяє швидко інтегрувати нові джерела даних, змінювати типи алгоритмів, налаштовувати правила або інтегрувати зовнішні сервіси. Це робить систему гнучкою до зовнішніх змін та придатною для довгострокового використання без великих витрат на реструктуризацію. Звичайно, адаптивність не означає повну автоматизацію без контролю. Існує ризик того, що при швидкій адаптації система може почати розглядати небезпечну та повторювану поведінку як “норму”. Тому вкрай важливо встановити обмеження, наприклад, вимагати ручного схвалення під час зміни моделі або зберігати попередні версії моделі для порівняння. Таким чином, адаптивність системи виявлення аномалій не обмежується здатністю виявляти поточні загрози, а й здатністю справлятися з майбутніми викликами. Це необхідна умова для того, щоб система працювала в постійно невизначеному та мінливому середовищі в довгостроковій перспективі [25-30].

3.2 Здатність до швидкого прийняття рішень

3.2.1 Масштабованість системи

Масштабованість системи виявлення аномалій – це її здатність ефективно працювати, незважаючи на зростання обсягу даних, кількості джерел даних та складності процесів обробки. У сучасну цифрову епоху величезні обсяги інформації генеруються майже в кожній галузі – від інтернет-сервісів та виробництва до медичних установ та систем моніторингу. Якщо система не може масштабуватися, її

продуктивність та точність різко знижуються зі збільшенням навантаження, що робить її непридатною для використання.

Першим важливим аспектом масштабованості є обчислювальна ефективність алгоритму. Деякі традиційні методи, особливо ті, що мають високу складність, просто не можуть обробляти мільйони записів у режимі реального часу. Тому все частіше використовуються легкі моделі, спеціалізовані індекси, методи поступового навчання або методи, засновані на потоковій обробці даних, щоб система реагувала майже миттєво навіть під високим навантаженням. Крім того, масштабованість також стосується можливості горизонтального масштабування – тобто додавання нових вузлів або серверів без повного перезапуску або зміни архітектури. Це особливо актуально в хмарних обчисленнях, які можуть динамічно розподіляти ресурси на основі навантаження. Добре спроектована, масштабована система повинна підтримувати розподілену обробку, кешування, паралельне виконання завдань та ефективне балансування навантаження. Здатність системи обробляти різні типи даних (структуровані, неструктуровані, потокові, історичні та з різних джерел (датчики, журнали подій, API тощо)) також є критично важливою. У цьому контексті масштабованість включає не лише кількісне розширення, але й функціональну гнучкість, здатність обробляти різнорідні дані та здатність підтримувати зростаючу кількість джерел інформації.

Ще одним важливим фактором є масштабованість з точки зору управління та моніторингу. У великих системах необхідно не лише виявляти аномалії, але й мати можливість відстежувати, реєструвати, аналізувати та ефективно реагувати на кожну аномалію. Це вимагає побудови простого у використанні інтерфейсу управління, системи сповіщень, аналітичних панелей та автоматизованих інструментів аудиту, які можуть працювати без затримки навіть при обробці десятків тисяч подій за хвилину.

Забезпечення масштабованих систем безпеки та доступу також є критично важливим. У великих організаціях часто необхідно обмежувати доступ до різних частин системи, дозволяти або блокувати певні дії для різних груп користувачів та

контролювати всі зміни в режимі реального часу. Це ставить додаткові вимоги до архітектури системи та вимагає впровадження політик безпеки, які не уповільнюють роботу системи. Зрештою, масштабованість означає не лише швидшу роботу, а й загальну здатність системи зростати разом з організацією та адаптуватися до її потреб, обсягу даних та складності. Без масштабованості навіть найточніші та найінтелектуальніші моделі виявлення аномалій залишаться лише теоретичними інструментами та не можуть бути застосовані в реальних сценаріях.

Також важливо розуміти, що масштабована система безпеки повинна бути не лише технічно надійною, але й організаційно гнучкою. Це означає підтримку ієрархічної структури доступу, інтеграцію з системами управління ідентифікацією та забезпечення централізованого управління в багатокористувацькому середовищі. У великих організаціях кожен відділ може мати свої власні потреби в безпеці, і система повинна забезпечувати локальне налаштування правил без шкоди для загальної безпеки. Окрім контролю доступу, ключовою можливістю є аудит – здатність реєструвати всі дії, пов’язані з доступом, зміни конфігурації або обробку винятків. Це не тільки дозволяє швидко реагувати на інциденти, але й відповідає нормативним вимогам щодо підзвітності та прозорості. Масштабована система повинна автоматично забезпечувати ці можливості, не спричиняючи додаткового навантаження на ресурси або операційних затримок. У цьому контексті спеціальні журнали подій (журнали аудиту), шифрування журналів та інструменти автоматизованого аналізу поведінки користувачів (UEBA) не рекомендуються, але повинні бути невід’ємною частиною архітектури системи.

Зі зростанням розміру системи зростає потреба в постійному управлінні конфліктами доступу та ескалацією привілеїв. Система повинна мати можливість динамічно реагувати на зміни: наприклад, тимчасово обмежувати дії користувачів при виявленні підозрілої активності або автоматично переміщувати події на вищий рівень безпеки для перевірки. У складних середовищах такої динамічної поведінки можна досягти лише завдяки тісній інтеграції систем виявлення, автентифікації, контролю доступу та моніторингу. Така інтеграція не лише забезпечує надійність,

але й створює умови для гнучкого коригування політик на основі змін у бізнес-процесах.

3.2.2 Здатність швидко приймати рішення

Здатність систем виявлення аномалій швидко приймати рішення є важливою в тих сферах, де час реагування є критично важливим. Це особливо актуально в кібербезпеці, фінансовій торгівлі, охороні здоров'я, моніторингу промислових процесів та системах відеоспостереження. У цих випадках кожна секунда затримки може мати серйозні наслідки – втрату даних, фінансові втрати, шкоду здоров'ю або простої виробництва. Тому швидкість прийняття рішень є не лише перевагою, але й основною вимогою до системи. Для досягнення високошвидкісного прийняття рішень система повинна працювати в режимі реального часу або майже в реальному часі.

Це означає, що вона повинна обробляти вхідні дані в міру їх надходження, не ставлячи їх у чергу та не чекаючи завершення всього циклу аналізу. Для цієї мети часто використовується потокова обробка, що дозволяє системі працювати негайно - аналізуючи кожен новий запис. Однак швидкість не повинна жертвувати якістю. Надмірна оптимізація реального часу може призвести до великої кількості хибнопозитивних або хибнонегативних результатів. Тому вкрай важливо знайти баланс між точністю моделі та швидкістю. Це досягається за допомогою попередньо навчених моделей, оптимізованих алгоритмів, індексації даних та використання апаратних прискорювачів, таких як графічні процесори або програмовані польовими логічними матрицями, які можуть швидше виконувати складні обчислення.

Ще одним фактором, що впливає на швидкість прийняття рішень, є оптимізація внутрішньої логіки реагування. Це означає, що система повинна не тільки виявляти будь-які аномалії, але й автоматично активувати відповідні сценарії: надсилати сповіщення, обмежувати доступ, блокувати транзакції або зв'язуватися з технічними фахівцями. Ці механізми повинні бути максимально простими та надійними, щоб не ускладнювати процес і не створювати додаткових точок збою. Варто також зазначити, що швидкість реагування також залежить від структури

зберігання даних. Традиційні реляційні бази даних не завжди підходять для високочастотних аналітичних завдань. Натомість часто використовуються спеціалізовані бази даних часових рядів, сховища в пам'яті або NoSQL-технології, які забезпечують високу продуктивність навіть при високому навантаженні.

Не менш важливим є людський фактор. Якщо система вимагає підтвердження або втручання оператора, процес має бути інтуїтивно зрозумілим, швидким і не порушуватися зайвою інформацією. Успішне впровадження вимагає створення зручних інтерфейсів, які дозволяють негайно оцінювати ситуацію та приймати рішення без тривалого аналізу. Тому здатність системи приймати швидкі рішення випливає з її комплексного підходу: оптимізованих алгоритмів, ефективної архітектури, продуманих інтерфейсів та гнучких механізмів реагування.

3.3 Алгоритм на основі нейронних мереж для прогнозування аномалій

У роботі досліджено одна з ключових проблем, з якою стикається сучасна енергетика: виявлення ненормального споживання електроенергії, що є важливим для надійності та ефективності “розумних” мереж. Основна мета дослідження — підвищити точність прогнозів енергоспоживання та виявити аномалії, такі як крадіжка електроенергії або вихід з ладу лічильників, за допомогою моделей штучного інтелекту. В дослідженні використано рекурентну нейронну мережу - LSTM (Long Short-Term Memory Network), яка може враховувати часові залежності, сезонні тенденції та зовнішні фактори, такі як погода та свята. У порівнянні з традиційним методом - алгоритмом ARIMA (Autoregressive Integrated Moving Average), ця модель може робити прогноз споживання електроенергії з меншою похибкою.

3.3.1 Особливості запропонованого методу

Особливість методу полягає в його тривалому аналізі: використано дані за тривалий період часу, а не звичайні щоденні чи погодинні дані, що дозволяє точніше виявляти закономірності. Цей метод виявлення також може виявити ненормальні моделі, які можуть бути пропущені за коротші періоди часу. Модель тренувалась на аналітиці даних, зібраних протягом року на основі даних понад 21

000 користувачів. Дані містять таку інформацію, як споживання енергії, температура, швидкість вітру, погодні умови, день тижня та державні свята.

Метод передбачає перетворення необроблених даних у формат, придатний для машинного навчання: стандартизацію, кодування категоріальних змінних, усунення відсутніх даних і побудову контрольованої навчальної проблеми, де прогноз на кожен день базується на даних за попередні дні. Крім прогнозування, модель також використовується для виявлення аномалій. Якщо фактичне значення значно відрізняється від прогнозованого значення, точка вважається підозрілою. Сума цих точок за певний період часу дозволяє нам виявити систематичні аномалії. Результати показують, що модель LSTM демонструє вищу точність прогнозування (RMSE зменшено на 22% порівняно з моделлю ARIMA) і покращує здатність виявляти крадіжки електроенергії.

Можна визначити, що запропонований підхід принесе практичну користь енергетичним компаніям і підвищить безпеку мережі. Порівняння з іншими методами, включаючи алгоритми кластеризації, такі як K-means, показують, що LSTM забезпечує вищу повноту та помірну точність – 71% точності та 58% повноти, тоді як K-means має 82% та 26% відповідно. Те, що LSTM забезпечує вищу повноту означає, що модель на основі LSTM виявила більше реальних випадків аномального споживання (електроенергії) з усіх, що насправді є в наявності. Це стосується метрики “recall” (повнота) у задачах класифікації.

3.3.3 Результати експериментальних досліджень

Рис.3.1 показує, як різні змінні погоди, такі як температура, швидкість і напрямок вітру, представлені як нормалізовані значення. Ці змінні були нормалізовані до однієї шкали, щоб полегшити їх обробку для нейронної мережі. Це дозволяє моделі LSTM рівномірно обробляти різнорідні дані без домінування однієї функції над іншою. Нормалізація покращує стабільність і якість навчання моделі за рахунок уникнення впливу “зашумлених” значень.

На Рис.3.2 показано внутрішню структуру одного нейрона в моделі LSTM. Модель має три “вікна” - забуття, введення та виведення, — які контролюють потік

інформації через нейрон. Ці механізми дозволяють нейронам запам’ятовувати довгострокові стосунки та забувати непотрібну інформацію. Саме ця структура робить модель довгострокової пам’яті ефективною для аналізу часових рядів.

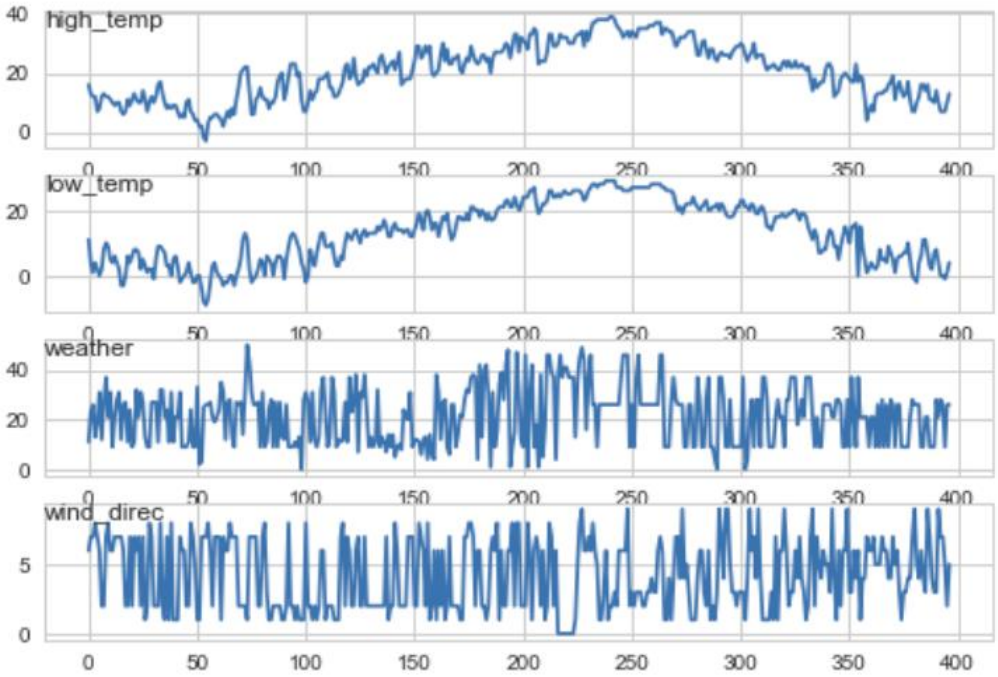


Рис.3.1. Відображення змінних у вигляді нормалізованих значень

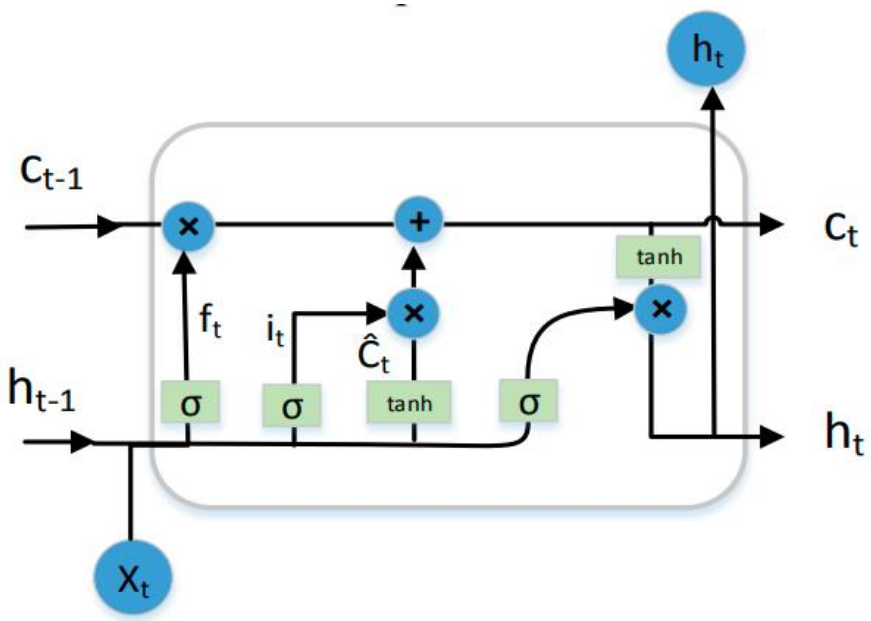


Рис.3.2. Структура нейрона моделі

Таблиця 3.1

Результати AR-моделі. Коефіцієнти

Змінна	coef	std err	z	P>|z|	[0.025	0.975]
Const	11.0497	3.349	3.299	0.001	4.486	17.614
ar.L1.D.3317000550	0.8213	0.048	17.001	0.000	0.727	0.916
ar.L2.D.3317000550	-0.1156	0.064	-1.815	0.070	-0.240	0.009
ar.L3.D.3317000550	0.0484	0.064	0.756	0.450	-0.077	0.174
ar.L4.D.3317000550	-0.0857	0.064	-1.346	0.179	-0.210	0.039
ar.L5.D.3317000550	0.2765	0.048	5.727	0.000	0.182	0.371

Таблиця 3.2

Корені характеристичного полінома

AR	Real	Imaginary	Modulus	Frequency
AR.1	1.0298	-0.0000j	1.0298	-0.0000
AR.2	0.6849	-1.0859j	1.2839	-0.1604
AR.3	0.6849	+1.0859j	1.2839	0.1604
AR.4	-1.0449	-1.0193j	1.4597	-0.3770
AR.5	-1.0449	+1.0193j	1.4597	0.3770

Таблиця.3.1 та Таблиця 3.2 показують короткий перелік параметрів традиційної моделі ARIMA для порівняння, а також містять коефіцієнти та статистичні дані, що описують модель на основі даних навчання. Цей підхід дозволяє нам зрозуміти, як працюють традиційні часові моделі, але він також підкреслює їх обмеження в складних ситуаціях, що стає очевидним при порівнянні з результатами LSTM.

На Рис.3.3 показано, як змінюються помилки (втрати) на тренувальних і тестових наборах протягом 300 епох навчання. Спочатку помітно перенавчання, але поступово модель стабілізується. Це вказує на те, що модель добре узагальнюється і що з часом навчиться розрізняти реальні шаблони та шум у даних.

На Рис.3.4 показано розподіл помилок прогнозування при роботі моделі ARIMA. Хоча форма розподілу похибок близька до нормального розподілу, центр ваги зміщений, що вказує на наявність систематичних похибок. Цей факт ще раз підтверджує, що ARIMA працює не так добре, як нейронні мережі, особливо за наявності складних зовнішніх факторів.

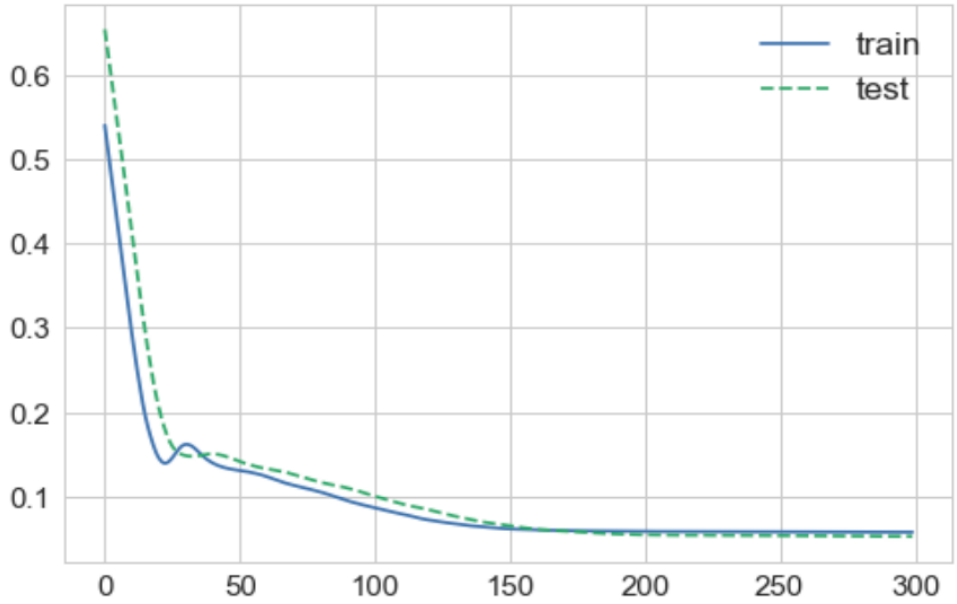


Рис.3.3. Зміни втрат під час навчання та тестування

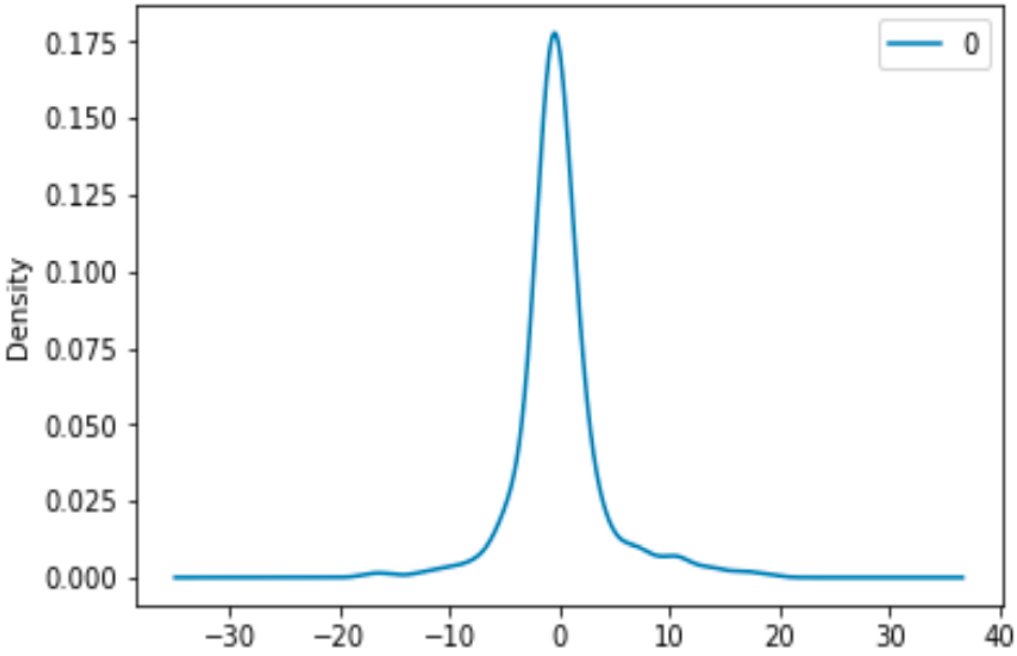
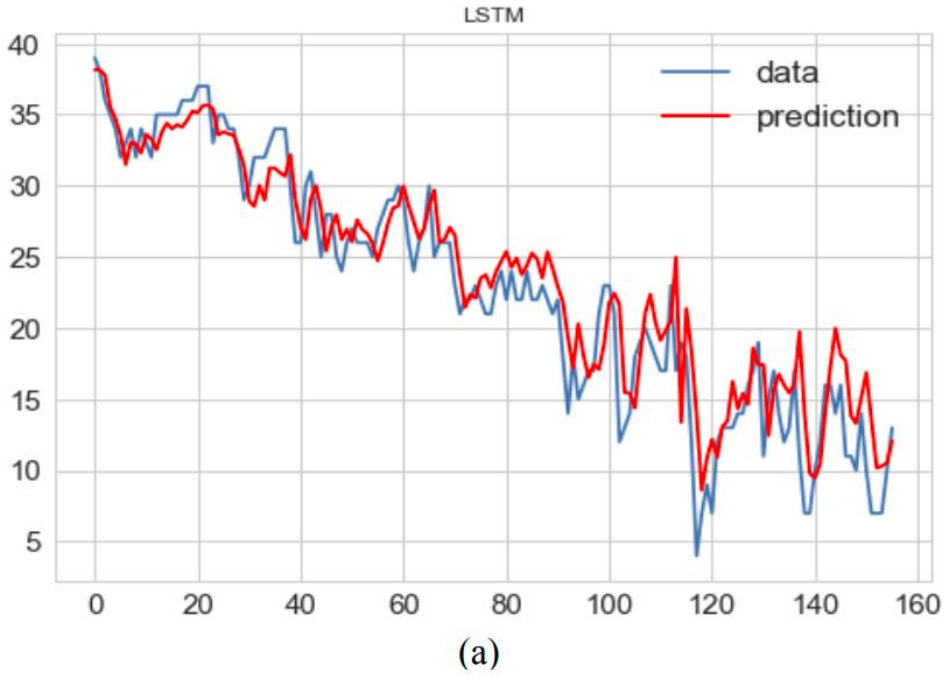
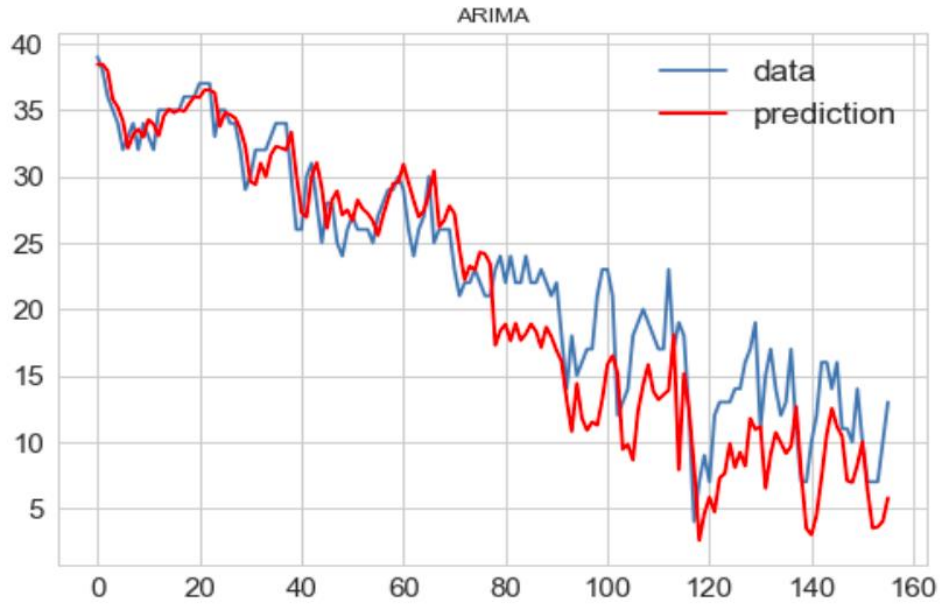


Рис.3.4. Розподіл помилок стандартного алгоритму

На Рис.3.5 показано два графіки: фактичне споживання (червона лінія) і прогнозоване споживання (синя лінія), один для моделі LSTM, а інший для моделі ARIMA. Примітно, що модель LSTM більш точно відтворює реальність. Використовуючи погодні та календарні змінні, нейронна мережа може передбачати поведінку користувачів краще, ніж традиційна модель.



(a)



(b)

Рис.3.5. Порівняння передбачень моделей LTSM (a) та ARIMA (b)

Рис.3.6 показує результати аналізу відхилень для одного користувача. Синя лінія позначає споживання, червона лінія позначає порогове значення, а зелена позначає вікно аномалії. Цей підхід може не тільки визначити конкретні підозрілі моменти, але й визначити весь цикл ненормальної поведінки споживання - показник потенційного шахрайства. В дослідженні використано LSTM щоб розробити точну та ефективну модель для прогнозування та виявлення аномалій у споживанні

електроенергії. На відміну від традиційних методів, модель враховує сезонні та зовнішні фактори та є адаптивною. Результати показують, що глибоке навчання перевершує традиційні статистичні методи в складних середовищах великих даних. Похибка прогнозу зменшилася на 22%, що є вагомим показником.

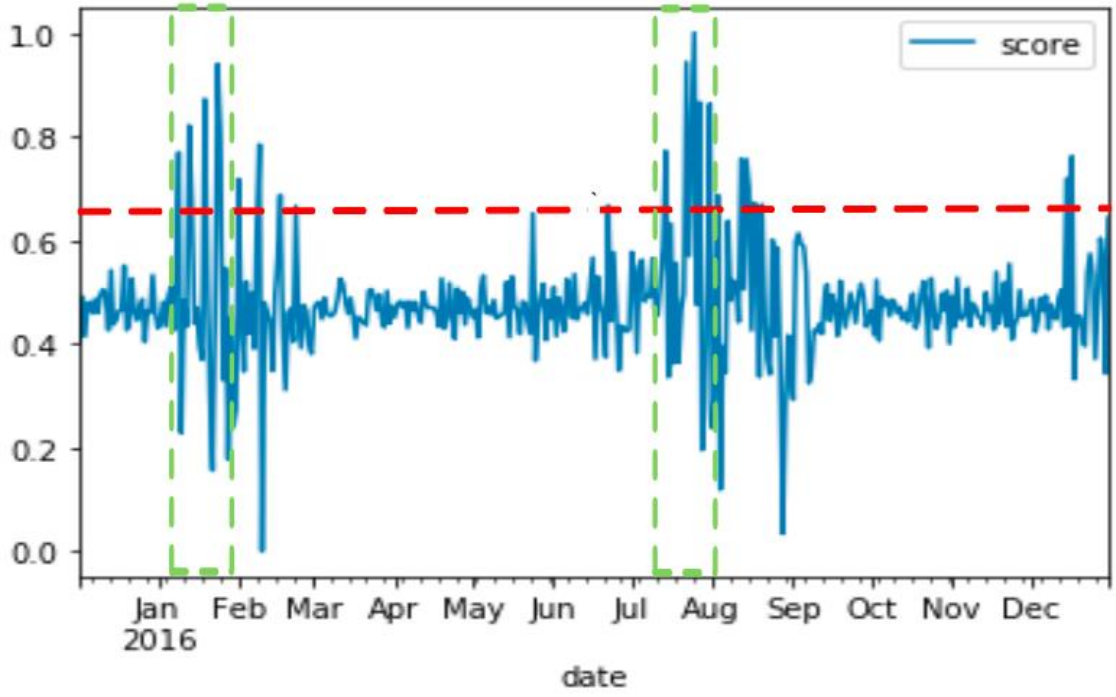


Рис.3.6. Виявлення аномалій користувацького енергоспоживання

З точки зору виявлення аномалій, LSTM має високу точність і прийнятну повноту, а також здатний виявляти відомі та невідомі моделі споживання електроенергії. Практичні застосування включають виявлення крадіжок електроенергії, збоїв лічильників та оптимізацію споживання енергії користувачами. Це створює великий потенціал для енергетичних компаній. У майбутньому варто далі вдосконалювати алгоритм, включаючи його поєднання з іншими методами машинного навчання для підвищення точності та адаптивності системи.

Крім того, перспективним напрямком досліджень є розробка багатоагентних систем, де LSTM може бути однією з підсистем, що взаємодіють з іншими алгоритмами в режимі реального часу. Такий підхід може не тільки виявляти аномалії, але й негайно реагувати, автоматично повідомляючи операторів, перевіряючи лічильники або змінюючи режими живлення. Інтеграція моделей у

хмарну інфраструктуру також є перспективною, забезпечуючи масштабованість, централізовану обробку даних та знижуючи витрати на обслуговування [30-35].

Висновок до розділу 3

У розділі представлено ефективний метод прогнозування та виявлення аномального споживання електроенергії за допомогою LSTM. Дослідження показало, що глибоке навчання може значно покращити результати порівняно з традиційними статистичними методами, такими як ARIMA. Метод демонструє високу точність прогнозування, значно зменшує помилки (на 22%) та здатний виявляти як систематичні, так і індивідуальні аномалії, пов'язані з аномальним споживанням електроенергії. Метод враховує фактори часу, погоди та календаря, що дозволяє більш реалістично моделювати поведінку користувачів. Нормалізація, попередня обробка даних та побудова завдань навчання з учителем покращують стабільність та здатність моделі до узагальнення. Модель демонструє високу точність та повноту, що означає, що вона може виявляти більшість реальних випадків аномального споживання електроенергії, що має вирішальне значення для практичного застосування.

Візуалізація експериментальних результатів підтверджує переваги LSTM в обробці масивних даних та складних залежностей. Крім того, модель здатна виявляти весь цикл підозрілої поведінки, що робить її ефективним інструментом для виявлення шахрайства та технічних збоїв. Запропонований метод має великий потенціал для практичного застосування в енергетичній галузі, особливо в завданнях моніторингу, безпеки, планування навантаження та оптимізації ефективності. Отже, алгоритми на основі LSTM є перспективними інструментами для побудови інтелектуальних систем у сфері енергетики.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ

В даному дипломному проекті необхідно побудувати програмну модель дослідження нейронних мереж для прогнозування аномалій у великих масивах телекомунікаційних даних.

Робота над дипломом виконувалась в приміщенні, в якому знаходиться 2 робочих місць з комп'ютерною технікою.

В цьому розділі потрібно розглянути вимоги, стандарти для комфортної та безпечної роботи працівників за комп'ютерними місцями. Наведемо дослідження та розрахунки безпеки роботи за комп'ютерами у робочому приміщенні.

4.1 Аналіз шкідливих та небезпечних виробничих чинників при роботі з комп'ютером

Розробка дипломного проекту виконувалась в приміщенні, з робочим місцем яке обладнане комп'ютером. Важливим фактором являється аналіз усіх чинників при роботі за комп'ютером. Згідно ГОСТ 12.0.003-74 «Небезпечні та шкідливі виробничі фактори» всі умови роботи за фактором небезпеки поділяються на певні фактори. Було проаналізовано такі фактори, як: фізичні, психофізіологічні, та хімічні. Розглянемо їх детальніше:

Фізичні:

- підвищене значення напруги електричного кола
- підвищений рівень електромагнітного випромінювання
- підвищений рівень статичної електрики
- підвищений рівень іонізації повітря

Психофізіологічні:

- статичні та динамічні перевантаження
- розумове перенапруження
- перенапруження зору при роботі за екранами пристроїв.

Хімічні**:**

- підвищений вміст у повітрі робочої зони озон, смоли;

З цих всіх факторів, виділомо один, це довга робота за комп’ютером. Люди працюють за робочим місце годинами, забуваючи за всі норми, та потребу відпочити від такого навантаження, адже при такій робочі сильно втомлюються очі, втомлюються і інші частини тіла, через втому падає продуктивність людини, робота виконується не так швидко і успішно. Тому, щоб уникнути небажаних проблем зі здоров’ям, та зменшити втому від такого навантаження потрібно виконувати наступні вказівки:

- Проводити обов’язкові перерви на 5 – 10 хв, через кожну годину роботи за комп’ютером. Також не працювати довше ніж 6 годин на добу
- у робочому приміщенні варто збільшувати вологість (оптимальна вологість — 60% при температурі 21° С), розмістити квіти, акваріум у радіусі 1,5 м від комп'ютера
- Протирати пил з робочих поверхонь

4.2 Заходи з охорони праці під час роботи з комп’ютером

Вся робота як проводиться за комп’ютером нормується нормативними документами НПАОП 0.00-7.-18 «Вимоги до безпеки та захисту працівників під час роботи з екранними пристроями.», та ДСанПіН 3.3.2.007-98 «Державними санітарними правилами і нормами роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»

Організація робочого місця

Для комфортної роботи працівників за комп’ютерами потрібно дотримуватись таких норм:

- Положення тіла повинно відповідати напрямку погляду, неправильна поза призводить до виникнення згорблення;
- Нижній край екрана повинен бути на 20 см нижче рівня очей;
- Рівень верхньої кромки екрана повинен бути на висоті чола;
- Екран комп'ютера — на відстані 75—120 см від очей;
- Висота клавіатури повинна бути встановлена таким чином, щоб кисті рук користувача розміщувались прямо

- Спинка стільця повинна підтримувати спину користувача
- Кут між стегнами і хребтом має становити 90°
- Крісло та клавіатуру розміщують таким чином, щоб не було потреби далеко витягуватись
- відстань між столами з комп'ютерами повинна бути не менша 1,5 м, між моніторами 2,2 м;
- якщо під час роботи доводиться дивитись на документи, то підставку з оригіналом документа слід встановлювати в одній площині з екраном і на одній з ним висоті
- треба уникати яскравого освітлення, не втомлювати очі різкою зміною потужності світлових потоків
- екран комп'ютера треба розміщувати під прямим кутом до вікон, самі вікна під час роботи доцільно завішувати або закривати жалюзями

Допустимі умови та мікроклімат при виконанні роботи за комп'ютером

За ДСН 3.3.6.042-99, робота за комп'ютером відноситься до категорії легких робіт Іа – це легкі фізичні роботи, при яких витрата енергії дорівнює 105-140 Вт (90-120 ккал/год). Тому для оптимальної роботи можна виділити такі величини температур, відносної вологості та швидкості руху повітря:

Таблиця 4.1

Оптимальні величини температура, вологості та швидкості руху

Період	Категорія	Температура	Відносна вологість	Швидкість руху
Холодний	Іа	22 – 24	60 – 40	0,1
Теплий	Іа	23 – 25	60 – 40	0,1

Також важливим є параметр площі, яка відповідає одному робочому місцю, якщо їх кількість перевищує одне робоче місце, мінімальна площа для одного робочого місця повинна складати 6 м2, тобто на 2 робочих місця це мінімум 12 м2, та об'єм не менше 20 м3.

Освітлення в робочому приміщенні

Серед чинників зовнішнього середовища, що впливають на організм людини в процесі праці, світло посідає одне з перших місць. Відомо, що 90 % усієї інформації про довкілля людина одержує через органи зору. Під час здійснення трудової діяльності втомлюваність очей, в основному, залежить від напруженості процесів, що супроводжують зорове сприйняття. Коефіцієнт природної освітленості повинен бути близько 1,5%, згідно з документами ДБН В.2.5 – 28:2018. Робота за комп'ютером відповідно до 4 розряду середньої точності зорових робіт. Природне освітлення забезпечуються при цьому освітлення на поверхні робочого столу та в зоні розміщення документів має становити до 300 лк. -Нормативні величини освітленості робочих місць для різних видів робіт та відповідних зорових навантажень визначаються ДБН Б.2.5.-28-2006 «Природне і штучне освітлення». - Згідно ДБН Б.2.5.-28-2018 Природне і штучне освітлення - штучне освітлення має здійснюватися системою загального рівномірного освітлення, яка включає суцільні або преривчасті лінії світильників, розташованих збоку робочих місць (переважно ліворуч), паралельно лінії зору користувачів ПК. Світильники повинні мати розсіювачі світла та екрануючі сітки (світильники серії ЛПО 36 із дзеркальними сітками, укомплектовані високочастотними пускорегулювальними апаратами ВЧ ПРА).

Допускається використання світильників слідуючих класів світлорозподілу:

- - прямого світла – П;
- - переважно прямого світла – Н;
- - переважно відбитого світла – В.

При розміщенні ПК по периметру приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями.

Рівень освітленості на робочому столі користувача в зоні розташування комп'ютера має бути в межах 300-500лк.Якщо цей рівень освітленості неможливо забезпечити системою загального освітлення то допускається застосування світильників місцевого освітлення, але при цьому не повинно бути відблисків на

поверхні екрану (яскравість відблисків не повинна перевищувати 40кд/м2) та перевищення його освітленості більше ніж 300лк.

Яскравість світильників загального освітлення, а також яскравість стелі при застосуванні системи відбитого освітлення не повинна перевищувати 200кд/м2. Величина коефіцієнта пульсації освітленості не повинна перевищувати 5%, що забезпечується застосуванням газорозрядних ламп у світильниках загального і місцевого освітлення.

Електробезпека в робочому приміщенні

Приміщення із робочими місцями, оснащеними електротехнікою, зокрема комп'ютерною технікою, для захисту від ураження електричним струмом, повинні мати достатні технічні засоби захисту відповідно до «Правила улаштування електроустановок» (ПУЕ-2017). Вимикач до 5 комп'ютерів Також працівники повинні дотримуватись наступних правил при роботі з такою технікою:

- Якщо на металевих частинах обладнання виявлено напругу (відчуття струму), заземлюючий провід (опір проводу до 100 Ом) обірваний, необхідно вимкнути обладнання, негайно доповісти керівникові про несправності електрообладнання і без його вказівки до роботи не приступати.
- При припиненні подавання електроенергії, вимкнути обладнання.
- При появі незвичного звуку, запаху паленого, мимовільного відключення комп'ютера та оргтехніки, негайно припинити роботу і поставити до відома керівника.

Електроживлення робочого приміщення

У приміщенні, де одночасно експлуатуються понад п'ять персональних комп'ютерів і периферійних пристроїв, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Персональні комп'ютери і периферійні пристрої повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення. При організації робочих місць операторів електромережу штепсельних розеток для

живлення персональних комп'ютерів, периферійних пристроїв і у центрі приміщення прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах. При цьому не допускається застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, які містять сірку.

Випромінювання в приміщеннях з комп'ютерною технікою

Джерелами змінних електричних і магнітних полів у ПК є вузли, у яких присутня висока змінна напруга, і вузли, що працюють з великими струмами. Рівні напруженості електромагнітних полів за електричними складовими та густиною магнітних потоків (індукції) у цих піддіапазонах регламентуються чинним в Україні нормативним актом ДСанПіН 3.3.2.007-98 та загальноєвропейським стандартом MPR II.

Шум в приміщенні

Рівні шуму та вібрації на робочих місцях осіб, що працюють з ПК, визначаються відповідно до ДСН 3.3.6.037–99

Таблиця 4.2

Залежність допустимого рівня шуму від характеристики приміщення (ДСН 3.3.6.037–99)

Характеристика приміщення	Рівні звуку, дБ
Приміщення конструкторських бюро, програмістів обчислювальних машин,	50
Приміщення керування, робочі кімнати	60
Кабіни спостережень і дистанційного керування: без мовного зв'язку, з мовним зв'язком по телефону	80 65
Постійні робочі місця і робочі зони у виробничих приміщеннях і на території підприємств	80

Для забезпечення дотримання допустимих рівнів шуму на робочих місцях застосовуються засоби звукопоглинання, вибір яких обґрунтовується спеціальними інженерно-акустичними розрахунками (п. 3.3.3 ДСанПіН 3.3.2.007-98) державного

санітарно-епідеміологічного нагляду. Крім того, необхідно застосовувати підвісні стелі з аналогічними властивостями.

При виконанні дипломного проекту, рівень шуму в приміщенні не повинен перевищувати – 50 дБ.

Перенапруга аналізаторів зору при роботі за КТ. Заходи попередження

Тривала робота за комп'ютером робить негативний вплив на очі і зір. Останнім часом з'явилося декілька нових термінів визначають захворювання очей, спричинені довгою роботою на ПК.

Дисплейна хвороба (астенопія: від грец. Asten-втома + ops-зір), характеризується порушенням акомодації очей через тривале перенапруження війкового тіла. Війкове тіло розташоване відразу під веселковою оболонкою ока і складається з безлічі м'язових волокон. Війкове тіло являє собою своєрідне м'язове кільце усередині якого кріпиться кришталик. Скорочення або розслаблення м'язів війкового тіла приводить до зміни кривизни кришталика і, отже, змінює його заломлюючу здатність. У нормі робота війчастих тіл обох очей підтримує концентрування світлового пучка на обмежену ділянку сітківки. При хронічному перенапруженні війкового тіла воно втрачає здатність скорочуватися а, отже, втрачається здатність очей до акомодації (сприйняття об'єктів на різних відстанях).

Синдром сухого ока - збірна назва захворювання викликаного порушенням зволоження передньої поверхні ока (рогівки) слізної рідиною. У нормі людина здійснює більше 20 рухів в секунду. У результаті цього передня поверхня ока постійно зволожується і очищується слізної рідиною. Під час роботи за комп'ютером частота моргання зменшується щонайменше в три рази. При цьому поверхня рогівки «висихає». Синдром сухого ока розвивається через деякий час роботи за комп'ютером і проявляється печінням в очах, почервонінням кон'юнктиви, появою судинної сітки на бічних поверхнях очей. Якщо при виникненні цих ознак робота за комп'ютером припиняється, то симптоми регресують. Однак під час тривалої роботи за комп'ютером вищевказані симптоми стають більш стійкими і не зникають після припинення роботи на комп'ютері. Пояснюється це приєднанням

інфекції і порушенням трофіки оболонок ока, викликані недостатнім зволоженням очей слізної рідиною.

Заходи попередження

1. Щодня перед початком роботи необхідно очищати екранні пристрої від пилу та інших забруднень.

2. Після закінчення роботи екранні пристрої слід відключати від електричної мережі.

3. У разі виникнення аварійної ситуації необхідно негайно відключити екранний пристрій від електричної мережі.

4. Не допускається:

- виконувати технічне обслуговування, ремонт і налагодження екранних пристроїв безпосередньо на робочому місці працівника під час роботи з екранними пристроями;
- відключати захисні пристрої, самочинно проводити зміни у конструкції та складі екранних пристроїв або їх технічне налагодження;
- працювати з екранними пристроями, у яких під час роботи виникають нехарактерні сигнали, нестабільне зображення на екрані та інші несправності.

5. Під час виконання робіт операторського типу, пов’язаних з нервово-емоційним напруженням, у приміщеннях під час роботи з екранними пристроями, на пультах і постах керування технологічними процесами та в інших приміщеннях мають дотримуватися оптимальні умови мікроклімату відповідно до вимог ДСН 3.3.6.042-99.

Мінімальні вимоги безпеки до екранних пристроїв

1. Екранні пристрої не мають бути джерелом ризику для працівників.

2. Усе випромінювання, за винятком видимої частини електромагнітного спектра, має бути зведене до незначного рівня з погляду безпеки і охорони здоров’я працівників.

3. Символи на екранних пристроях мають бути чіткими, відповідного розміру. Між символами і рядками символів має бути належна відстань.

4. Зображення на екрані має бути стабільним, без миготінь або інших видів нестабільності.

5. Яскравість та/або контрастність символів має легко регулюватися працівником під час роботи з екранними пристроями, а також швидко адаптуватися до навколишніх умов.

6. Вибираючи екрани, слід надавати перевагу таким екранам, які легко та вільно повертаються і нахиляються відповідно до потреби працівника.

7. За необхідності може використовуватись окрема підставка або регульований стіл для розміщення екрана.

8. Екран не має відблискувати або відбивати світло, щоб не викликати дискомфорту у працівника під час роботи з екранними пристроями.

9. Вибираючи клавіатуру, слід надавати перевагу такій клавіатурі, яка відкидається і є автономною (відокремленою від екрана), щоб працівник міг вибрати зручну робочу позу й уникнути втоми рук (кисті і верхньої частини руки).

10. Поверхня клавіатури має бути матовою, щоб уникнути віддзеркалювання. Розташування клавіш і самі клавіші мають полегшувати роботу із клавіатурою. Позначення клавіш повинно бути достатньо контрастним і розбірливим.

11. Устаткування, яке входить до робочої станції, не має виділяти надлишкового тепла, що може спричинити незручності працівникам під час роботи з екранними пристроями.

12. Під час розробки, вибору, замовлення та модифікації програмного забезпечення, а також під час розробки завдань, що передбачають використання устаткування з екранними пристроями, роботодавець має керуватися таким програмним забезпеченням, яке відповідає розв’язуваним завданням і є простим у використанні, а де необхідно - адаптованим до рівня знань і досвіду працівника.

Висновок до розділу 4

В цьому розділі ми проаналізували усі можливі варіанти, які можуть перешкоджати в першу чергу безпечній, комфортній та здоровій праці людей, які працюють за робочим місцем обладнаним КТ.

В першому підрозділі проаналізували шкідливі і небезпечні чинники, які виникають при роботі за КТ. Також вказали як їх зменшити, та запобігти подібному.

У другому підрозділі розглянули усі можливі заходи охорони праці під час роботи працівників за КТ. Невиконання та недотримання таких заходів може призвести до небажаних наслідків, тому за таке грозить адміністративна, або-ж у серйознішому випадку – кримінальна відповідальність.

У третьому підрозділі ми зрозуміли що таке перенапруга аналізаторів зору та заходи їх попередження.

ВИСНОВКИ

В роботі проведено дослідження нейронних мереж для прогнозування аномалій у великих телекомунікаційних наборах даних. Робота зосереджена на структурі, характеристиках та застосуванні нейронних мереж у задачах аналізу даних. У першому розділі детально описано типи нейронних мереж, такі як одношарові мережі, багатошарові мережі, рекурентні мережі та згорткові мережі, а також окреслено їхню роль у задачах класифікації, обробки послідовностей та виявлення аномалій. Крім того, наголошується на важливості оцінки точності, чутливості та специфічності моделі, що дозволяє об'єктивно оцінити ефективність системи в реальних застосуваннях.

Другий розділ зосереджений на особливостях обробки великих телекомунікаційних даних, таких як трафік, записи дзвінків та дані користувачів, які потребують спеціалізованих методів аналізу через свій розмір та динамічний характер. У роботі наголошується на здатності нейронних мереж ефективно виявляти складні закономірності в цих інформаційних наборах, тим самим забезпечуючи покращену якість прогнозування аномалій та сприяючи надійності телекомунікаційних систем.

У третьому розділі наведено приклад практичного застосування нейронних мереж LSTM у прогнозуванні споживання електроенергії та виявленні аномалій, пов'язаних з відхиленнями у споживанні електроенергії. Результати показують, що модель LSTM перевершує традиційні статистичні методи за точністю та здатністю виявляти систематичні та індивідуальні аномалії. Врахування інших факторів, таких як погодні умови та залежність від часу, може значно покращити точність прогнозування, тим самим доводячи практичну доцільність методу в енергетичному секторі. Четвертий розділ зосереджений на захисті працівників під час роботи з комп'ютерним обладнанням. Підсумовуючи, проведене дослідження підкреслює великий потенціал використання нейронних мереж для аналізу масивних даних та виявлення аномалій у системах зв'язку, а також показує перспективи їх застосування в суміжних галузях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. M. Hou and X. Han, "Constructive Approximation to Multivariate Function by Decay RBF Neural Network," in *IEEE Transactions on Neural Networks*, vol. 21, no. 9, pp. 1517-1523, Sept. 2010, doi: 10.1109/TNN.2010.2055888.

2. M. Khalid and S. Omatu, "A neural network based control scheme with an adaptive neural model reference structure," *[Proceedings] 1991 IEEE International Joint Conference on Neural Networks*, Singapore, 1991, pp. 2128-2133 vol.3, doi: 10.1109/IJCNN.1991.170702.

3. J. Suárez-Varela *et al*., "Graph Neural Networks for Communication Networks: Context, Use Cases and Opportunities," in *IEEE Network*, vol. 37, no. 3, pp. 146-153, May/June 2023, doi: 10.1109/MNET.123.2100773.

4. M. Hao *et al*., "Artificial Neural Network-Based Approach to Modeling Energy Bands of GaN-Based Heterojunction Materials," *2023 International Conference on High Performance Big Data and Intelligent Systems (HDIS)*, Macau, China, 2023, pp. 71-76, doi: 10.1109/HDIS60872.2023.10499489.

5. J. B. P. Matos, E. B. de Lima Filho, I. Bessa, E. Manino, X. Song and L. C. Cordeiro, "Counterexample Guided Neural Network Quantization Refinement," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 4, pp. 1121-1134, April 2024, doi: 10.1109/TCAD.2023.3335313.

6. C. H. Park, "Anomaly Pattern Detection on Data Streams," *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Shanghai, China, 2018, pp. 689-692, doi: 10.1109/BigComp.2018.00127.

7. C. -I. Chang, "Target-to-Anomaly Conversion for Hyperspectral Anomaly Detection," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 60, pp. 1-28, 2022, Art no. 5540428, doi: 10.1109/TGRS.2022.3211696.

8. S. M. A. Karim, N. Ranjan and D. Shah, "A Scalable Approach to Time Series Anomaly Detection & Failure Analysis for Industrial Systems," *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020, pp. 0678-0683, doi: 10.1109/CCWC47524.2020.9031262.

9. J. Lee, C. -R. Jeon and S. -J. Kang, "Performance Comparison of Soiling Detection Using Anomaly Detection Methodology," *2022 19th International SoC Design Conference (ISOCC)*, Gangneung-si, Korea, Republic of, 2022, pp. 229-230, doi: 10.1109/ISOCC56007.2022.10031428.

10. Z. Zhao, Y. Zhang, X. Zhu and J. Zuo, "Research on Time Series Anomaly Detection Algorithm and Application," *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Chengdu, China, 2019, pp. 16-20, doi: 10.1109/IAEAC47372.2019.8997819.

11. F. Peng, H. Wang, L. Zhuang, M. Wang and C. Yang, "Methods of enterprise electronic file content information mining under big data environment," *2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE)*, Bangkok, Thailand, 2020, pp. 5-8, doi: 10.1109/ICBASE51474.2020.00008.

12. H. Liu, F. Huang, H. Li, W. Liu and T. Wang, "A Big Data Framework for Electric Power Data Quality Assessment," *2017 14th Web Information Systems and Applications Conference (WISA)*, Liuzhou, China, 2017, pp. 289-292, doi: 10.1109/WISA.2017.29.

13. D. Arruda and N. H. Madhavji, "Towards a big data requirements engineering artefact model in the context of big data software development projects: Poster extended abstract," *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, USA, 2017, pp. 4725-4726, doi: 10.1109/BigData.2017.8258521.

14. A. Cuzzocrea, "Big OLAP Data Cube Compression Algorithms in Column-Oriented Cloud/Edge Data Infrastructures," *2023 IEEE Ninth Multimedia Big Data (BigMM)*, Laguna Hills, CA, USA, 2023, pp. 1-2, doi: 10.1109/BigMM59094.2023.00020.

15. A. Cuzzocrea and E. Damiani, "Privacy-Preserving Big Data Exchange: Models, Issues, Future Research Directions," *2021 IEEE International Conference on Big Data (Big Data)*, Orlando, FL, USA, 2021, pp. 5081-5084, doi: 10.1109/BigData52589.2021.9671686.

16. M. Liu, X. Hu, L. Liu and Y. Li, "Intelligent Trend for Telecommunications Networks' Energy Equipment," *2018 IEEE International Telecommunications Energy*

Conference (INTELEC), Turino, Italy, 2018, pp. 1-5, doi: 10.1109/INTLEC.2018.8612362.

17. M. Liu, X. Hu, L. Liu and Y. Li, "Intelligent Trend for Telecommunications Networks' Energy Equipment," *2018 IEEE International Telecommunications Energy Conference (INTELEC)*, Turino, Italy, 2018, pp. 1-5, doi: 10.1109/INTLEC.2018.8612362.

18. X. Lin, T. -J. Lv and X. Chen, "The coevolutionary relationship of technology, market and government regulation in telecommunications," in *China Communications*, vol. 15, no. 8, pp. 152-173, Aug. 2018, doi: 10.1109/CC.2018.8438281.

19. H. Hirner, M. Lavicka, S. Schefer-Wenzl and I. Miladinovic, "Agile Software Integration in Telecommunications — a Case Study," *2019 27th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2019, pp. 1-4, doi: 10.1109/TELFOR48224.2019.8971239.

20. S. Lentz and B. Howe, "Scientific Monitoring And Reliable Telecommunications (SMART) Cable Systems: Integration of Sensors into Telecommunications Repeaters," *2018 OCEANS - MTS/IEEE Kobe Techno-Oceans (OTO)*, Kobe, Japan, 2018, pp. 1-7, doi: 10.1109/OCEANSKOBE.2018.8558862.

21. Y. Wei, H. Young, D. Ke, F. Wang, H. Qi and J. Rodríguez, "Model-Free Predictive Control Using Sinusoidal Generalized Universal Model for PMSM Drives," in *IEEE Transactions on Industrial Electronics*, vol. 71, no. 11, pp. 13720-13731, Nov. 2024, doi: 10.1109/TIE.2024.3379667.

22. M. Van Den Brand, L. Cleophas, R. Gunasekaran, B. Haverkort, D. A. M. Negrin and H. M. Muctadir, "Models Meet Data: Challenges to Create Virtual Entities for Digital Twins," *2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, Fukuoka, Japan, 2021, pp. 225-228, doi: 10.1109/MODELS-C53483.2021.00039.

23. S. Mi, C. He and H. Wu, "Duty-Cycle Model Predictive Current Control," *2021 IEEE International Conference on Predictive Control of Electrical Drives*

and Power Electronics (PRECEDE), Jinan, China, 2021, pp. 552-556, doi: 10.1109/PRECEDE51386.2021.9680902.

24. Y. Li, D. Liu, T. Wu, W. Guo, X. Zhang and Y. Deng, "Model Predictive Current Control for Permanent Magnet Synchronous Motor based on Neural Network," *2023 IEEE International Conference on Predictive Control of Electrical Drives and Power Electronics (PRECEDE)*, Wuhan, China, 2023, pp. 1-6, doi: 10.1109/PRECEDE57319.2023.10174503.

25. Z. Feng, W. Cao, T. Rui, C. Hu and Z. Yin, "A Model-Free Predictive Control Method for Grid-Tied Inverter Based on Discrete Space Vector," *2021 IEEE International Conference on Predictive Control of Electrical Drives and Power Electronics (PRECEDE)*, Jinan, China, 2021, pp. 634-639, doi: 10.1109/PRECEDE51386.2021.9680938.

26. A. Aryan, S. P. Sagar, N. M. K. Varma, R. Manikanta, R. Rajashekar and G. D. Arora, "Optimizing Marketing Strategies: Predicting Customer Personality using Advanced Machine Learning Models," *2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, Faridabad, India, 2024, pp. 822-827, doi: 10.1109/ICAICCIT64383.2024.10912234.

27. T. R. N and R. Gupta, "A Survey on Machine Learning Approaches and Its Techniques:," *2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS)*, Bhopal, India, 2020, pp. 1-6, doi: 10.1109/SCEECS48394.2020.190.

28. T. Jadhav *et al.*, "Predicting Urban Land Cover Using Classification: A Machine Learning Approach," *2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC)*, Rajkot, India, 2023, pp. 450-454, doi: 10.1109/R10-HTC57504.2023.10461930.

29. S. Subramanian, B. Tseng, R. Barbieri and E. N. Brown, "Unsupervised Machine Learning Methods for Artifact Removal in Electrodermal Activity," *2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, Mexico, 2021, pp. 399-402, doi: 10.1109/EMBC46164.2021.9630535.

30. V. Bobade and C. Puri, "Improving Software Defects Detection: An In-Depth Analysis of Machine Learning Methods and Static Analysis Tools for Greater Accuracy," *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, Prawet, Thailand, 2025, pp. 502-507, doi: 10.1109/ICMLAS64557.2025.10968410.

31. A. Waheed and Q. Ali, "Software emergence for need based large data processing in engineering problems," *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, Beijing, China, 2017, pp. 442-446, doi: 10.1109/ICBDA.2017.8078858.

32. Z. Dong, "Research of Big Data Information Mining and Analysis : Technology Based on Hadoop Technology," *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, Sanya, China, 2022, pp. 173-176, doi: 10.1109/BDICN55575.2022.00041.

33. J. Chen, Q. Jiang, Y. Wang and J. Tang, "Study of data analysis model based on big data technology," *2016 IEEE International Conference on Big Data Analysis (ICBDA)*, Hangzhou, China, 2016, pp. 1-6, doi: 10.1109/ICBDA.2016.7509810.

34. H. Li, "Research on Big Data Analysis Data Acquisition and Data Analysis," *2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA)*, Xi'an, China, 2021, pp. 162-165, doi: 10.1109/CAIBDA53561.2021.00041.

35. X. HongJu, W. Fei, W. FenMei and W. XiuZhen, "Some key problems of data management in army data engineering based on big data," *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, Beijing, China, 2017, pp. 149-152, doi: 10.1109/ICBDA.2017.8078796.

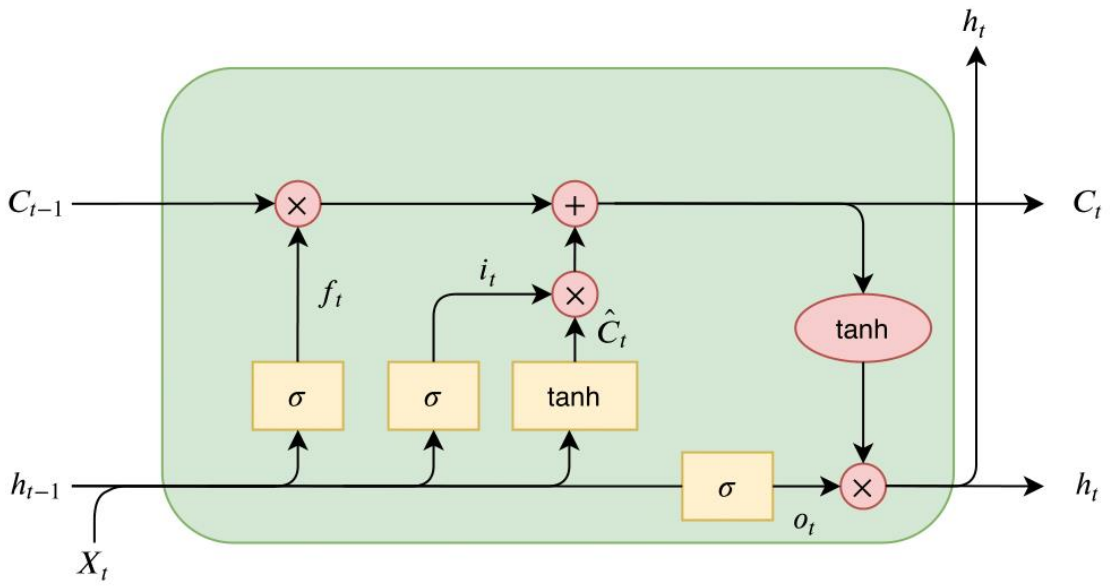


Рис.1.1. Архітектура LTSM

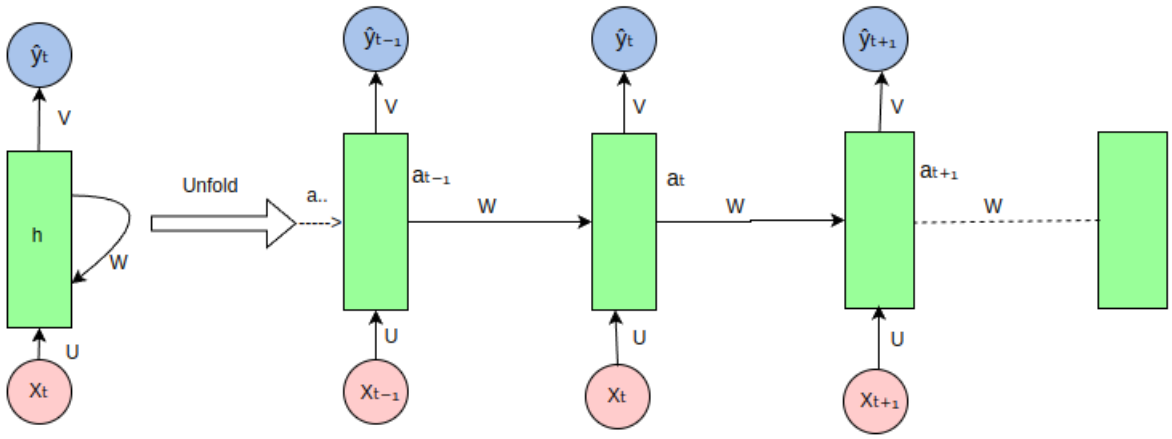


Рис.1.2. Архітектура RNN

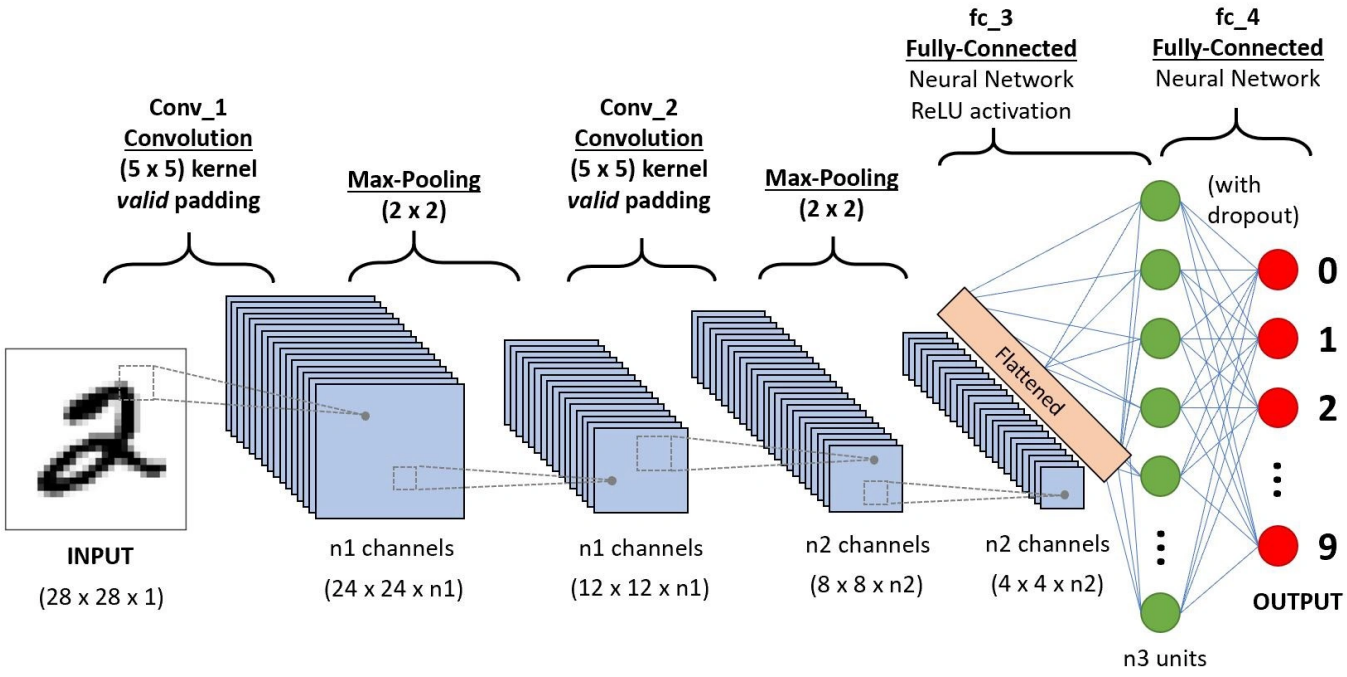


Рис.1.3. Архітектура CNN

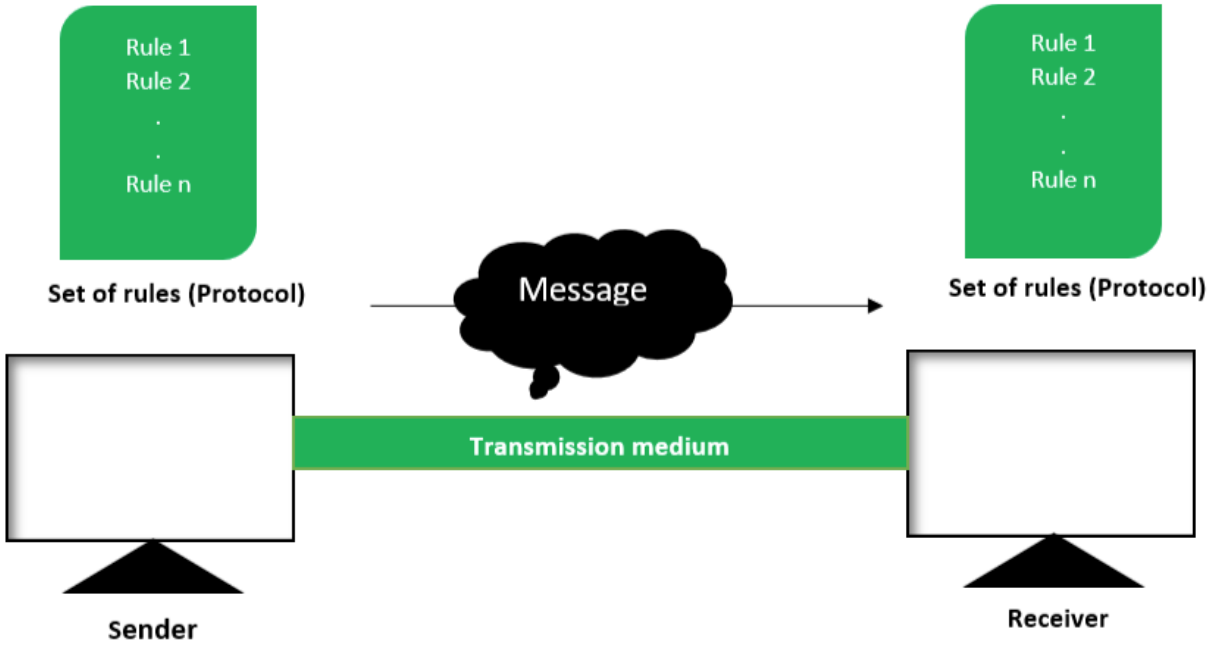


Рис.1.4. Телекомунікаційна система передаваня даних

Рис.1.5. Аналіз великих даних

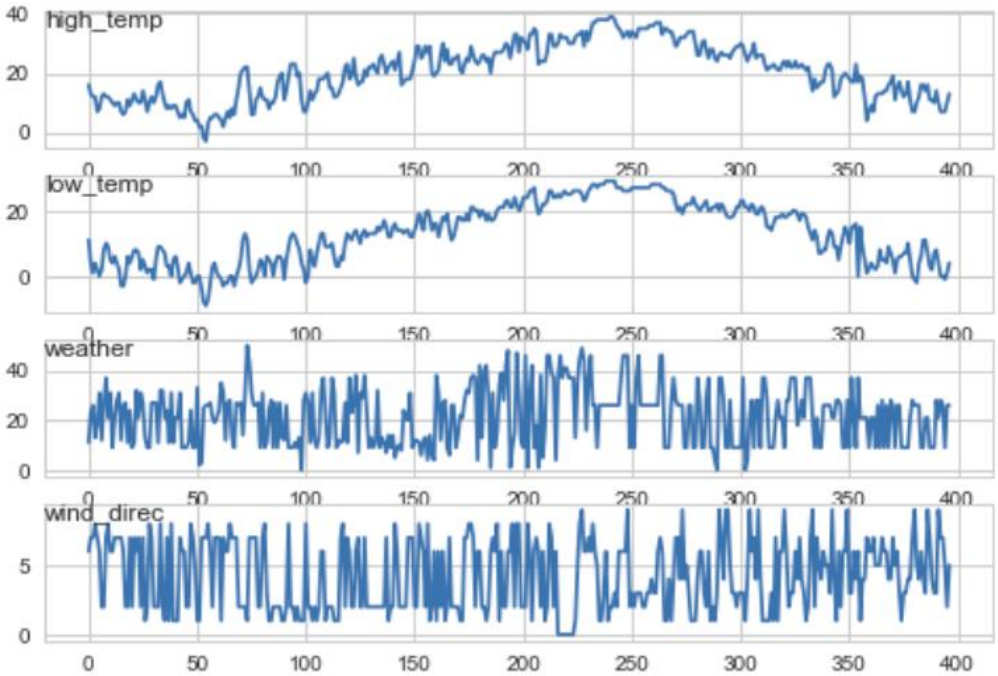


Рис.1.6. Відображення змінних у вигляді нормалізованих значень

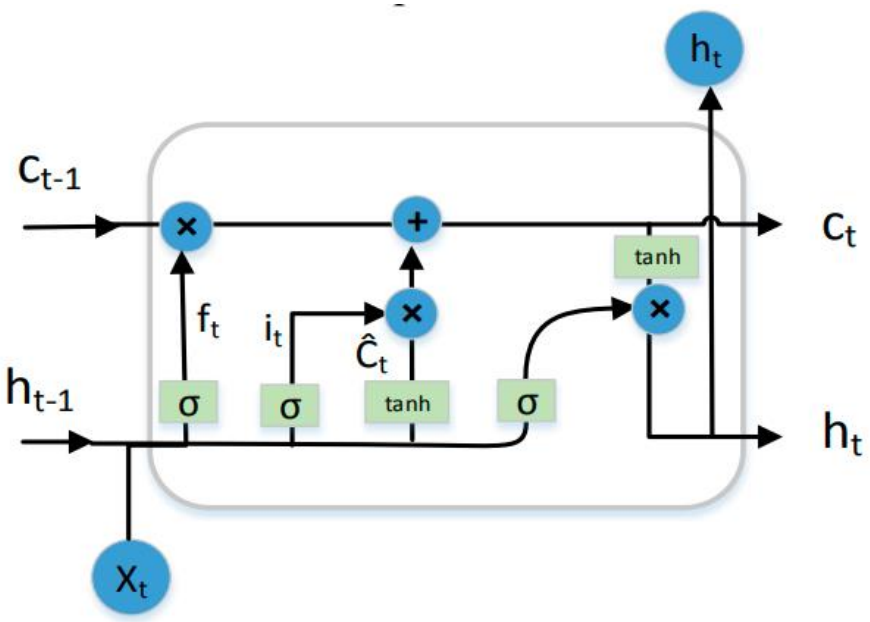


Рис.1.7. Структура нейрона моделі

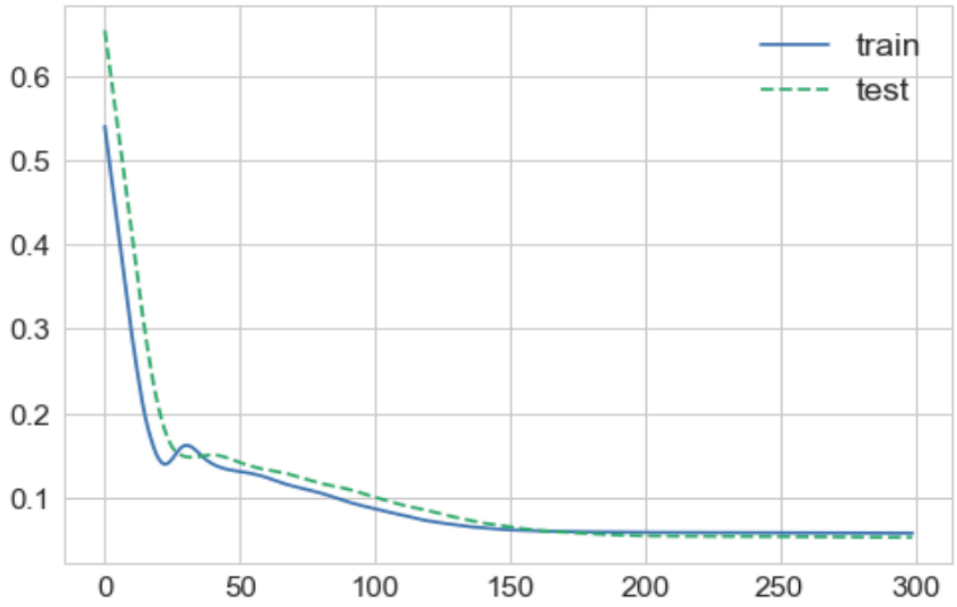


Рис.1.8. Зміни втрат під час навчання та тестування

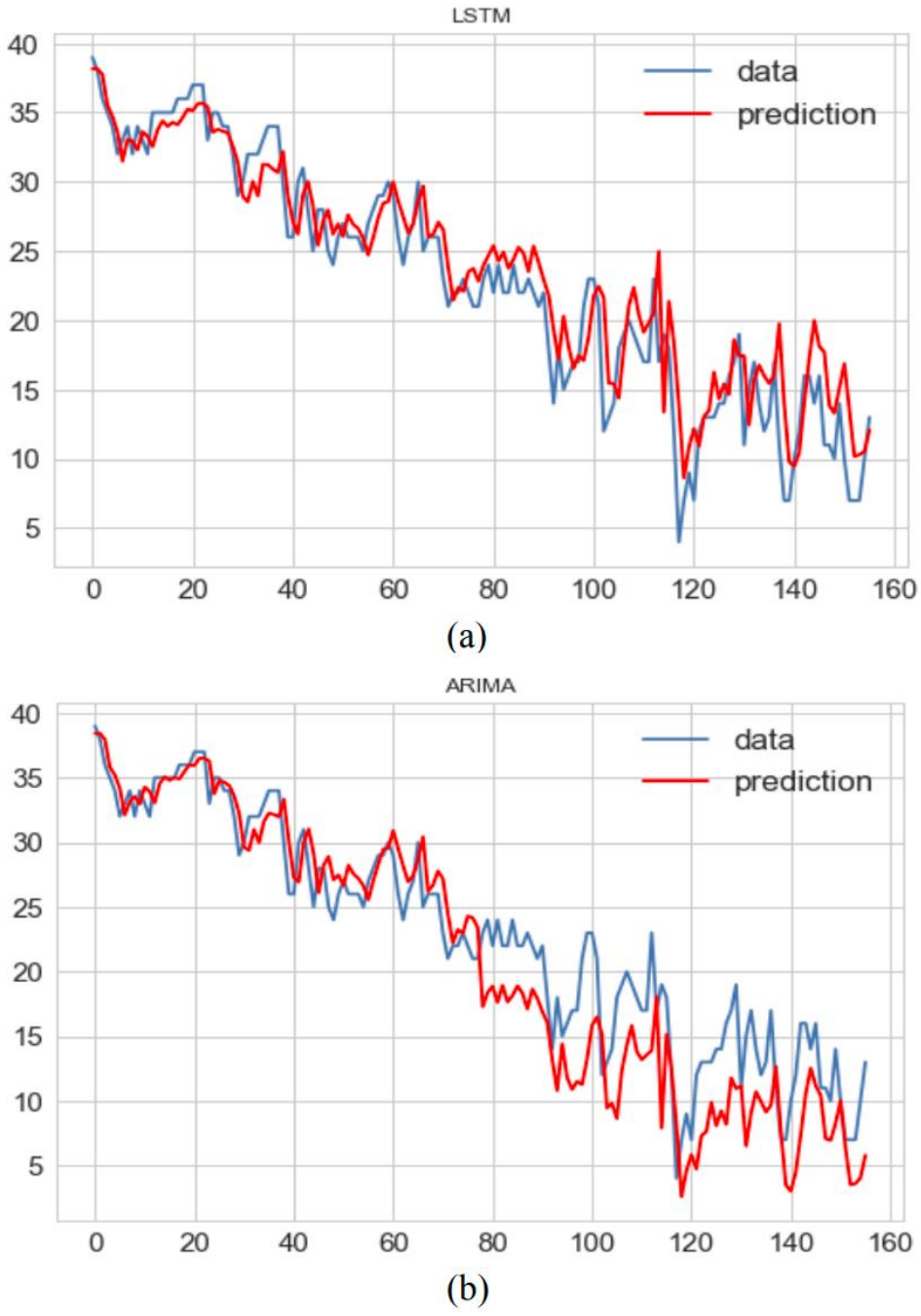


Рис.1.9. Порівняння передбачень моделей LTSM (a) та ARIMA (b)

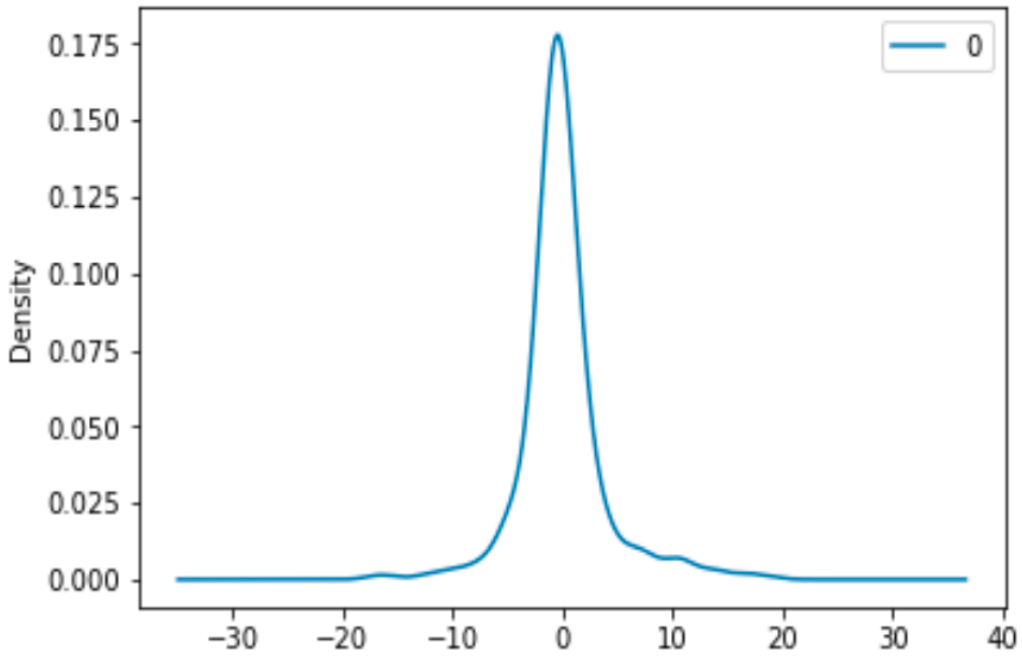


Рис.1.10. Розподіл помилок стандартного алгоритму

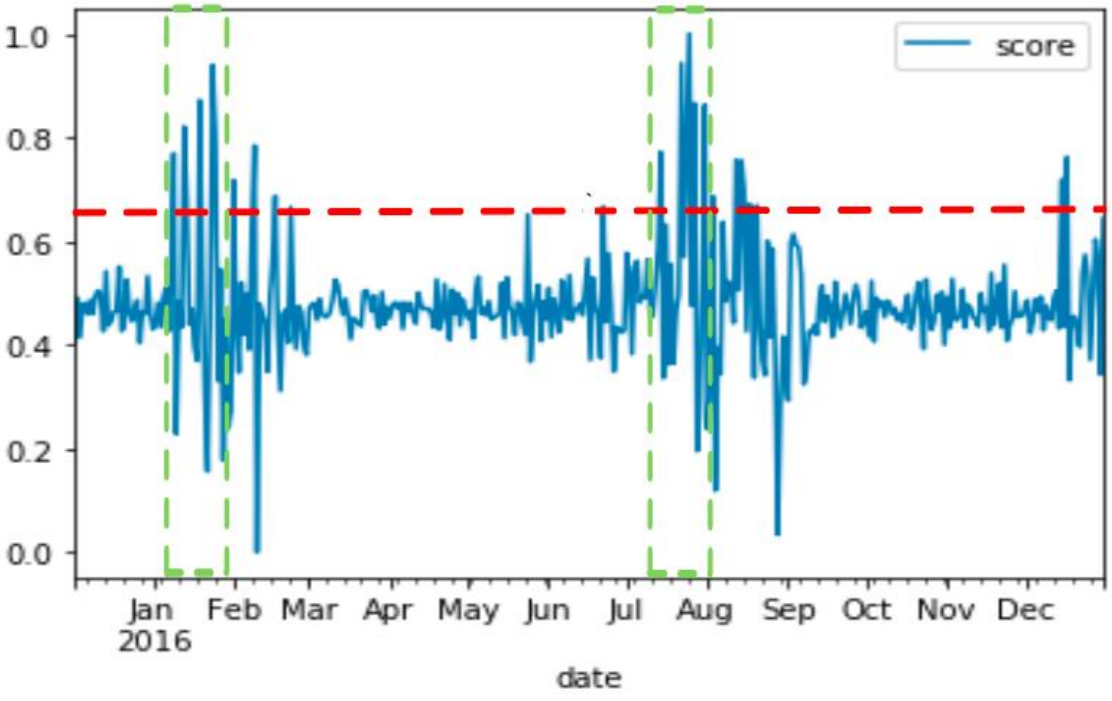


Рис.1.11. Виявлення аномалій користувацького енергоспоживання