Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Створення методу виявлення аномалій в технологічних сигналах

Виконав: студент VI курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Баранніков В.В. (прізвище та ініціали)

Керівник (підпис) Максимчук О.О. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль - 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Бараннікову Віталію Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Створення методу виявлення аномалій в технологічних сигналах

Керівник роботи Максимчук Олександр Олександрович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » 11 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 25.12.2023р.

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналіз предметної області.
2. Існуючі методи та підходи до виявлення аномалій.
3. Практична частина.
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема роботи. 2. Актуальність. 3. Мета, задачі, об'єкт, предмет дослідження.
4. Наукова новизна, практичне значення роботи. 5. Проблема виявлення аномалій
6. Практичне застосування виявлення аномалій. 7. Типи аномалій
8 -10. Вснуючі методи та підходи до виявлення аномалій.
11. Опис вихідних даних. 12. Список розрахункових ознак
13. Програмні засоби, які використані 14. Процес навчання класифікатора
15. Результати експериментів. 16 Основні висновки по роботі

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., зав. каф. КС		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з АГРБ		

7. Дата видачі завдання 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.11 – 17.11	*Виконано*
2.	Підбір джерел про способи і методи виявлення	18.11 – 26.11	*Виконано*
3.	Опрацювання джерел про способи і методи виявлення		
	аномалій в технологічних сигналах	27.11 – 30.11	*Виконано*
4.	Виконання дослідження щодо розробки методу і		
	виявлення аномалій	01.12 – 06.12	*Виконано*
5	Розробка алгоритмів	07.12 – 10.12	
6.	Оформлення розділу «Аналіз предметної області»	11.12 – 13.12	*Виконано*
7.	Оформлення розділу «Теоретична частина»	14.12 – 15.12	*Виконано*
8.	Оформлення розділу «Існуючі методи та підходи		
	до виявлення аномалій»	16.12 – 18.12	*Виконано*
9.	Виконання завдання до підрозділу «Охорона праці та		
	безпека в надзвичайних ситуаціях»	06.12 – 16.12	*Виконано*
10.	Оформлення кваліфікаційної роботи	14.12 – 19.12	*Виконано*
11.	Нормоконтроль	18.12 – 20.12	*Виконано*
12.	Перевірка на плагіат	16.12 – 19.12	*Виконано*
13.	Попередній захист кваліфікаційної роботи	17.12 – 20.12	*Виконано*
14.	Захист кваліфікаційної роботи	26.12	

Студент _____ Баранніков В.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Максимчук О.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Створення методу виявлення аномалій в технологічних сигналах // Баранніков Віталій Віталійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2023 // с. – 74, рис. – 14, табл. – 7 , слайд. – 16, бібліогр. – 42.

Ключові слова: ВИЯВЛЕННЯ АНОМАЛІЙ, ГРАДІЄНТНИЙ БУСТІНГ, КЛАСТЕРИЗАЦІЯ, МАШИННЕ НАВЧАННЯ, МЕТРИКИ, ПРОСТІР ОЗНАК, ШАХРАЙСЬКІ ТРАНЗАКЦІЇ

Кваліфікаційна робота присвячена проблемам виявлення аномалій у множині технологічних сигналів, розробці відповідних алгоритмів та моделей, для створення та побудови яких потрібна множина ресурсів, знань та інформації про предметну область.

Розглядаються три існуючі види аномалій. Як вступна частина до розробки алгоритмів виявлення аномалій у множині технологічних сигналів розкривається сутність розпізнавання аномалій і даються відповіді на питання про режими розпізнавання аномалій та які бувають методи розпізнавання викидів. Наводиться класифікація відповідно до умов та стратегій виявлення аномалій. Зокрема, розглядаються методи кластеризації та способи її застосування у галузі інформаційної безпеки.

На наявній множині технологічних сигналів з реальних об'єктів застосовано методи виявлення аномалій, розроблено алгоритм, створено схему та програмну реалізацію алгоритму для застосування в інформаційній безпеці.

Отримані результати підтверджують працездатність даного алгоритму класифікації технологічного сигналу. Рання версія даного алгоритму класифікації було впроваджено у прототип модуля виявлення аномалій у технологічному сигналі.

ANNOTATION

Creation of a method for detecting anomalies in technological signals // Barannikov Vitalii // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2023 // p. - 74, Fig. - 14, Table - 7, Slides - 16, References - 42.

Keywords: ANOMALY DETECTION, GRADIENT BOOSTING, CLUSTERIZATION, MACHINE LEARNING, METRICS, MARK SPACE, FRAUDULENT TRANSACTIONS

The qualification work deals with the problems of detecting anomalies in a set of technological signals, the development of appropriate algorithms and models, the creation and construction of which requires a set of resources, knowledge and information about the subject area.

Three existing types of anomalies are considered. As an introductory part to the development of algorithms for the detection of anomalies in a set of technological signals, the essence of anomaly recognition is revealed and answers are given to questions about the modes of anomaly recognition and what methods there are for recognizing emissions. The classification is given according to the conditions and strategies for detecting anomalies. In particular, methods of clustering and methods of its application in the field of information security are considered.

Anomaly detection methods were applied to the existing set of technological signals from real objects, an algorithm was developed, a scheme and a software implementation of the algorithm were created for use in information security.

The obtained results confirm the efficiency of this technological signal classification algorithm. An early version of this classification algorithm was implemented in the prototype module for detecting anomalies in the technological signal.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

ANN (Artificial Neural Networks) - штучні нейронні мережі.

GBM (Gradient Boosting Machine) – градієнтний бустинг.

IoT (Internet of Things) – інтернет речей.

k - NN (k-nearest neighbors algorithm) – метод *k* найближчих сусідів.

SVM (Support Vector Machine) – метод опорних векторів.

Автокодувальники (англ. Autoencoder) – нейронні мережі прямого поширення, які відновлюють вхідний сигнал на виході.

ВА – виявлення аномалій.

ЕОМ – електронно-обчислювальна машина.

ІТ – інформаційні технології.

МН – машинне навчання.

ПЗ – програмне забезпечення.

ЧР – часовий ряд.

Фрод (англ. Fraud) – шахрайські операції у сфері інформаційних технологій.

ЗМІСТ

ВСТУП 10
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ 13
1.1 Завдання пошуку аномалій 14
1.2 Види аномалій 17
1.2.1 Точкові аномалії 19
1.2.2 Контекстні аномалії 20
1.2.3 Колективні аномалії 22
1.3 Висновки до першого розділу 23
2 ІСНУЮЧІ МЕТОДИ ТА ПІДХОДИ ДО ВИЯВЛЕННЯ АНОМАЛІЙ 24
2.1 Класифікація методів пошуку аномалій 24
2.2 Ймовірнісний підхід 27
2.3 Лінійні методи 29
2.4 Метричні методи 30
2.5 Ізолюючий ліс 32
2.6 Приховані Марківські моделі 33
2.7 Класифікація градієнтним бустингом 34
2.8 Функції втрат 35
2.9 Метрики 36
2.10 Інші методи та додаткова інформація 38
2.11 Висновки до другого розділу 42
3 ПРАКТИЧНА ЧАСТИНА 43
3.1 Побудова алгоритму класифікації 43
3.1.1 Опис вихідних даних 43
3.1.2 Попередня обробка даних 44
3.1.3 Формування простору ознак 48
3.2 Експериментальні дослідження 50
3.2.1 Навчання класифікатора 50
3.2.2 Результати та обговорення 51
3.2.3 Додаткові відомості про давачі 54

3.3 Висновки до третього розділу 56
4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 58
4.1 Охорона тпраці 61
4.2 Планування та порядок проведення евакуації населення з районів наслідків впливу НС техногенного та природного характеру. 58
4.3 Висновки до четвертого розділу 61
ВИСНОВКИ 62
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 63
ДОДАТКИ
Додаток А. Тези конференції

ВСТУП

Актуальність теми. Операційні можливості ЕОМ досягли небувалих масштабів. Показники ефективності постійно зростають. За останні кілька десятків років було розроблено безліч методів та алгоритмів для обробки даних та побудови на їх основі моделей, але в сучасних умовах ці самі методи з їх сучасними модифікаціями в сукупності з можливостями ЕОМ знаходять застосування у багатьох актуальних задач. Впровадження автоматизованих систем підтримки прийняття рішення спрямоване переважно на дві групи завдань: підвищення безпеки виробництва, що включає аналіз та запобігання аваріям та економічні ефекти від оптимізації режимів споживання ресурсів [1].

Стратегія полягає у побудові моделей на основі даних, що надходять від давачів, розташованих на реальних фізичних об'єктах.

Завдання підвищення ефективності роботи технологічних ділянок досягається мінімізацією втрат. Втрати включають простій обладнання, витрати на ремонт, заміну, усунення наслідків аварій, збої, позаштатні ситуації та інше. Деякі втрати неминучі, але завжди досягається завдання мінімізації існуючих витрат виробництва з підвищенням якості, що супроводжується.

Широке застосування для завдання ВА знайшли методи МН [2-3]. До їх переваг відноситься проста параметризованість, можливість задавати різні метрики і кількість ступенів свободи моделі. До алгоритмів МН, що застосовуються для ВА, відносяться алгоритми таких типів як класифікація, кластеризація, статистичні методи.

Актуальною є потреба структурувати наявну інформацію, щоб допомогти відповісти на запитання: які бувають методи ВА у технологічних сигналах, які методи слід використовувати у конкретній ситуації, з яким типом чи типами даних.

Мета дослідження: узагальнення інформації про різні методи ВА та їх практичне застосування на технологічних сигналах.

В роботі поставлено та розв’язано наступні задачі:

– вивчити дані, на основі яких проводитимуться експерименти;

– провести класифікацію і систематизацію технологічних даних;

– розробити загальний план експериментів;

– вибрати інструменти на дослідження;

– реалізувати експерименти;

– оцінити отримані рішення.

Об’єкт дослідження: визначення аномалій в технологічних даних.

Предмет дослідження: аномалії в технологічних сигналах.

Методи дослідження: наукові праці закордонних та вітчизняних учених за тематикою дослідження, фундаментальні положення інформаційної безпеки; методи – математичного та імітаційного моделювання, проектування, машинного навчання.

Наукова новизна отриманих результатів:

– розроблено алгоритм класифікації із використанням GBM, який формує розширений простір ознак та враховує апріорну інформацію про походження технологічного сигналу;

– запропоновано застосувати створений метод BA для детектування шахрайства із банківськими транзакціями;

– розроблений програмний модуль є інваріантним до отриманих сигналів.

Практичне значення одержаних результатів. Результати проведеного дослідження можуть бути ефективно застосовані для виявлення зловмисних проникнень завдяки незвичному трафіку мережі чи нетиповим вчинкам користувачів у мережах реальних установ чи організацій. Також можливе застосування для банківських операцій з метою виявлення шахрайських транзакцій (так званий банківський фрод).

Апробація. Результати дослідження апробовано на XI науково-технічній конференції «Інформаційні моделі, системи та технології» у вигляді опублікованих тез [4].

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 4 розділів,

висновків, списку використаної літератури та додатків. Обсяг роботи: пояснювальна записка – 74 арк. формату А4, графічна частина – 16 слайдів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Усі ми іноді спостерігаємо аномалії у світі. Це і незвичайна спека, і тварини-альбіноси, і гетерохромія. Аномальні відхилення у невеликих кількостях присутні у будь-якому явищі. Важливо вміти відрізнити аномалію від шуму.

Розберемося, через що з'являються аномалії, коли їх треба враховувати під час розробки моделей МН та як їх виявити.

Припустимо, що у вас є банківська картка. І ось, одного невдалого дня її вкрали. Ваш банк відстежує вашу звичайну схему витрат, щоб повідомляти про будь-які суттєві зміни. Ці схеми включають кількість транзакцій, суми, місцезнаходження тощо. Якщо кредитну картку вкрадено, то, швидше за все, витрати на неї сильно зростуть. Саме в таких ситуаціях компанії використовують (у тому числі) пошук аномалій для виявлення незвичайних операцій на карті.

Який вигляд має шум у реальному світі? Наприклад розглянемо графік продажів продуктового магазину. Люди зазвичай купують більше продуктів на початку місяця, тому до його закінчення власник магазину починає помічати зниження продажів. Він починає робити знижки на деякі товари, щоб збільшити попит. Така схема може призвести до нерівномірного зростання продажів, але чи вписуватиметься він у звичайний графік? Звичайно ж ні. Це зростання буде створювати шуми, а точніше стохастичні шуми.

Сигналом називається такий фізичний процес, що є відображенням стану будь-якого об'єкта, за яким спостерігають, та придатний для зберігання, передачі і обробки.

Аномалії — це закономірності даних, котрі не відповідають добре визначеному поняттю нормального поведінки. Проблема виявлення цих патернів називається ВА. Важливість ВА зумовлена тим фактом, що аномалії власне даних приводять до значної і дієвої інформації в різних областях застосування [5, 6]. Наприклад, ненормальні схеми трафіку в комп'ютерних мережах можуть означати, що вкрадені комп'ютери відправляють конфіденційні дані в несанкціоновані місця призначення [7], ненормальні зображення МРТ можуть

вказувати на злоякісні пухлини, відхилення в даних транзакції по кредитній картці можуть вказувати на кредитні картки або посвідчення особи. Покази давачів космічного корабля можуть вказувати на відмову певних частин транспорту.

1.1 Завдання пошуку аномалій

На абстрактному рівні ВА здається простим завданням. Але це завдання може бути і дуже складним [8]. Нижче наведено деякі проблеми.

Визначити нормальні регіони дуже важко. У багатьох випадках межі між нормальними даними і аномаліями неможливо визначити точно. Власне в цьому випадку нормальні спостереження можуть прийматися за аномалії та може мати місце зворотнє.

Коли дія є шкідливою, як шахрайство, вона вважається аномалією. Практично завжди зловмисники пробують провести адаптацію вчиненії ними дій до нормального стану.

Те, що зараз приймається за нормальне, завтра вже може бути ненормальним. Оскільки бізнес-системи здатні змінюватися у часі, зазнаючи впливу різноманітних факторів.

Способи ВА в одній області частіше не можуть бути використані в іншій. Вони, здебільшого, будуть неефективні [9].

Доступність даних для навчання та перевірки навчання моделі є серйозним питанням, котре потребує розв’язання.

ВА було вивчено кількома дослідницькими спільнотами для вирішення проблем у різних галузях. У багатьох областях, таких як безпека польотів, виявлення вторгнень, виявлення шахрайства, охорона здоров'я - дані збираються як послідовності чи ЧР. Наприклад, в галузі авіації або безпеки польотів дані, зібрані під час польотів, подаються у вигляді послідовностей спостережень різних давачів літака під час польоту. Несправність у літаку призводить до аномальних показань у послідовностях, зібраних з одного або кількох давачів. Так само в галузі охорони здоров'я ненормальний медичний стан у серці

пацієнта може бути виявлений шляхом ВА у відповідних ЧР із записами електрокардіограми (ЕКГ) пацієнта.

При добуванні даних, ВА - це виявлення рідкісних предметів, подій чи спостережень, які викликають певні підозри, так як сильно різняться від інших даних. Часто аномальні елементи призводять до виникнення будь-яких проблем, як-от банківське шахрайство, структурні дефекти, проблеми зі здоров'ям або текстові помилки. Аномалії також називають викидами, нововведеннями, шумом, відхиленнями [10].

У процесі виявлення викидів важливу роль відіграє спосіб створення даних. Звичайні зразки з набору даних (рис.1.1) найчастіше створюються тим самим способом, але викиди можуть бути згенеровані в результаті інших процесів.

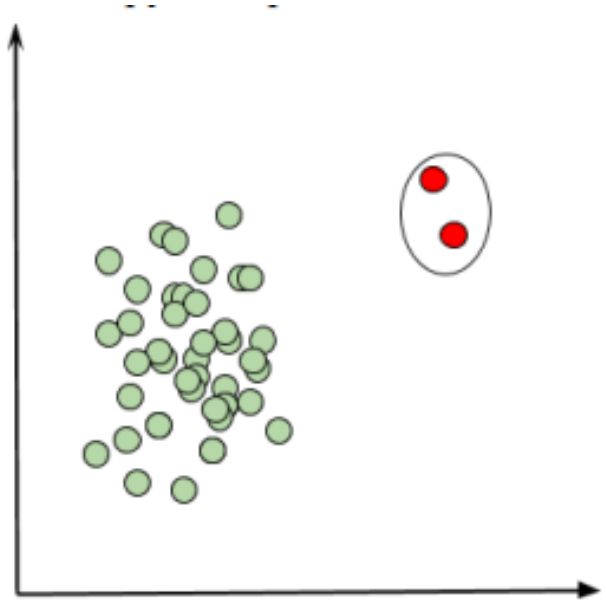

Рисунок 1.1 – Множина точок (включаючи аномалії) на двовимірному графіку

Близькість викидів у наборі даних один до одного визначається процесом, внаслідок якого вони з'явилися. Можна припустити, що дві червоні цятки згенеровані якимось іншим способом. Але як ми можемо довести, що він справді був іншим? Тільки будуючи припущення.

Аномалією чи викидом називається таке спостереження, яке не є

нормальним. Нормальність залежить від контексту.

Багатовимірні спостереження – такі, де різні точки – це різні виміри. Крапки утворюють хмари. У найпростішому випадку одна і частіше більша хмара складається з нормальних спостережень, і менша хмара – з аномалій.

Пошук викидів - той випадок, коли в нашій тренувальній вибірці вже є якісь викиди, і ми хочемо їх просто знайти, очистити, детектувати і таке інше.

Алгоритми, які працюють з такими викидами, мають знайти щільні ділянки, де зосереджені всі наші нормальні спостереження та аномалії, які значно відрізняються від нормальних [11].

Інший тип завдань – пошук новизни. Той випадок, коли наша вибірка, що навчає, не забруднена викидами. Іншими словами, ми вважаємо, що у нашій тренувальній вибірці всі дані нормальні. У такому разі необхідно побудувати такі моделі, які здатні навчитися на одному класі даних, а надалі мають відрізняти чисті дані від потенційних аномалій.

При аналізі аномалій зазвичай прийнято робити кілька припущень щодо «нормальних» даних, а потім виділяти об'єкти, що порушують їх. Дивлячись на графік, можна подумати, що аналіз аномалій та розбиття даних на кластери — майже одне й те саме. Ці процеси дійсно тісно пов'язані, але не однакові, оскільки мають різні цілі. Кластери - це групи схожих за характеристиками точок, а аномалії - об'єкти, що вибиваються із загального набору.

Навіщо взагалі шукати аномалії?

По-перше, щоб покращити якість моделі. Тобто це завдання передобробки даних.

По-друге, в даних можуть бути шуми. Таким чином, аномалії зашумлюють наші дані і через ці викиди наш алгоритм може перенавчитися та видавати невірні оцінки. Тобто, є мета уникнення подальшого перенавчання.

По-третє, вивчення викидів. Можливо, наприклад, у деякій системі з платною підпискою є кілька аномальних користувачів, які платять у десятки разів більше за всіх інших. Тоді нам потрібно вивчити, що це за користувачі і що потрібно зробити, щоб їх зберегти. На основі цього вже вирішувати, чи варто ці аномалії виключати із даних, чи ні.

По-четверте, виявлення поломок. Зазвичай цим займаються диспетчери, які сотні годин бачать графіки зміни показань тих чи інших приладів і в деяких випадках їм вдається запобігти поломці. Або після її виникнення виявити, де саме і коли вона сталася.

Якщо доручити це й аналогічні завдання алгоритму, то, можливо, поломок більше не виникатиме, оскільки відсутній людський фактор неуважності. Система точно і беззастережно визначить, чи ця подія є аномалією, чи ні. Однак навіть алгоритм може помилятися, але це вже питання правильного вибору та складання моделі.

У більшості випадків аномальні дані, що визначаються нами, відносяться до виявлення викидів. Після навчання цих даних ми шукатимемо аномальні точки в новому наборі даних.

Виявлення новизни - це метод, що дозволяє ідентифікувати нові чи невідомі шаблони та закони даних. Ці закони не виявляються у навчальному наборі існуючих систем МН. Передумова виявлення новизни у тому, що набір навчальних даних, як відомо, є «чистим» і не забруднений реальними «шумовими» даними чи реальними «викидами», та був після навчання цих даних нові дані навчаються для пошуку шаблонів даних новизни [4].

Виявлення новизни, в основному, застосовується для дослідження та розпізнавання нових шаблонів, тем і тенденцій, включаючи обробку сигналів, комп'ютерний зір, розпізнавання образів, інтелектуальних роботів та інші технічні вказівки, а також сфери застосування, такі як дослідження потенційних захворювань, відкриття нових видів, надбання нових тем спілкування тощо.

Виявлення новизни пов'язані з ВА. На початку точки новизни часто з'являються у даних стороннім чином. Цей сторонній спосіб зазвичай сприймається як сторонній. Тому шаблони виявлення та розпізнавання цих двох типів дуже схожі.

Однак через деякий період часу, коли дані новизни підтверджуються як нормальний патерн, наприклад, нове захворювання ідентифікується як поширене захворювання, патерн новизни буде об'єднаний у нормальний патерн і більше не буде ставитись до категорії аномальних точок [4].

1.2 Види аномалій

Як вже було сказано раніше, аномаліями називаються стани сигналу, які мають структуру, що відрізняє їх від передбачуваної типової поведінки системи.

Детектуванням аномалій називають процес виявлення об'єктів, подій або інших даних, які виділяються на тлі поведінки основної маси даних.

Поява аномалій у даних. Способи генерації аномалій сильно варіюються залежно від сфери застосування. Ось кілька випадків, коли виявлення викидів надзвичайно важливе:

1. Виявлення проникнень. У кібербезпеці зловмисні проникнення можна детектувати завдяки незвичному трафіку мережі чи нетиповим вчинкам юзерів. Ці вторгнення в силі пошкодити конфіденційність даних, як приватну, так і організаційну. Їх детектування веде до аналізу власне аномалій.

2. Шахрайські транзакції. Банківські операції — одна з областей, де аналіз аномалій надзвичайно потрібний. Багато хто напевно чув, що, заволодівши інформацією про кредитну картку, зловмисники можуть скористатися нею без вашого відома. Це часто призводить до незвичайної поведінки у схемі витрат, що робить пошук викидів ефективним способом виявлення шахрайства.

3. Спрацювання електронних давачів (в т.ч IoT). Електронні давачі дозволяють вивчати дані з різних джерел. Більшість мобільних пристроїв також мають давачі: акселерометр, гіроскоп, давач відстані. Аналіз одержуваних із них даних може знайти багато цікавих застосувань. Але що відбувається, коли давачі виходять із ладу? Їхні дані стають некоректними і створюють викиди.

Але причина аномалій може бути і в джерелі даних, наприклад, занадто висока частота пульсу після фізичних вправ. Це важливо враховувати під час розробки комерційних додатків.

У всіх галузях уявлення про аномалії схожі один на одного: це дані, які сильно відрізняються від «нормальних». Для пошуку ми приймаємо деякі правила, яким підпорядковуються звичайні екземпляри даних. Але й інші типи аномалій.

Аномальні спостереження відстають від генеральної сукупності. І тому, перш ніж приступити до розгляду класифікації наявних методів ВА та їх прикладів, аномалії даних можна поділити на три типи [12]:

– точкові;
– контекстуальні;
– колективні.

Розглянемо кожен із них (рис. 1.2) та його особливості.

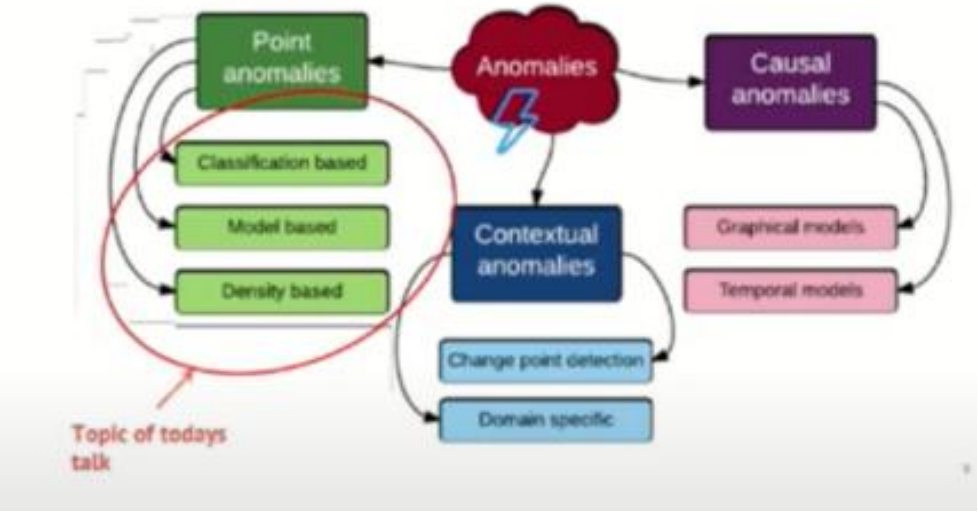

Рисунок 1.2 – Типи аномалій

1.2.1 Точкові аномалії

З’являються у випадку, якщо окремому екземпляру даних може ставитися у відповідність аномальність стосовно інших (рис. 1.3). Цей варіант аномалій є найлегше розпізнаваним, оскільки, у більшості випадків, існуючі методи розроблені для розпізнавання саме таких аномалій. Цей тип - найпоширеніший тип викидів. Якщо представити якісь дані як множину точок, тоді аномалії такого типу будуть значно виділятися із загального стану.

Головна ідея у їх детектуванні - визначити граничне значення відхилення, котре свідчить про ймовірний викид, що є власне окремою значною сферою для проведення різних досліджень. Такі аномалії досить часто застосовують у засобах контролю транзакцій для детектування шахрайства.

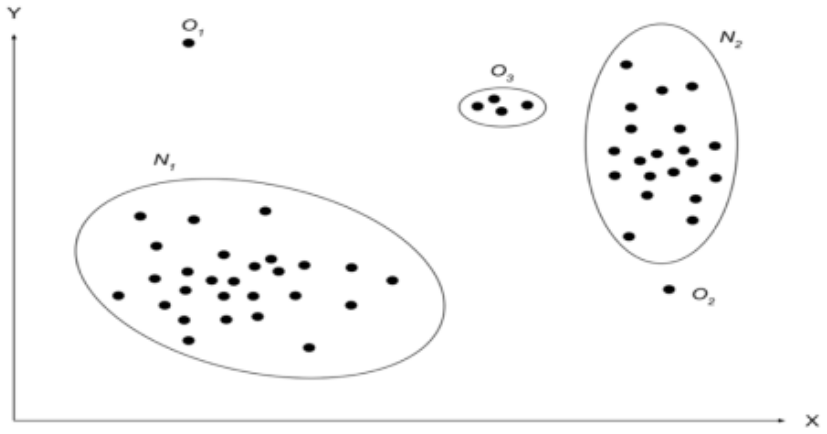

Рисунок 1.3 – Точкові аномалії

Висновок з наведеного вище – маркування точкових аномалій спрацьовуватиме правильно не у всіх випадках, оскільки в завданнях аналізу даних ймовірно наявними є зовсім різні умови та аспекти. Якщо сказати по іншому, аномалії, ймовірно, є залежними від контексту.

1.2.2 Контекстні аномалії

Це дані, які вважаються аномальними тільки для визначеного змісту (інша назва цих аномалій - умовні). Щодо дефініцій таких аномалій (рис. 1.4) – основним є виокремлення атрибутів (контекстуальних і поведінкових). Викид щодо типової поведінки спостережень.

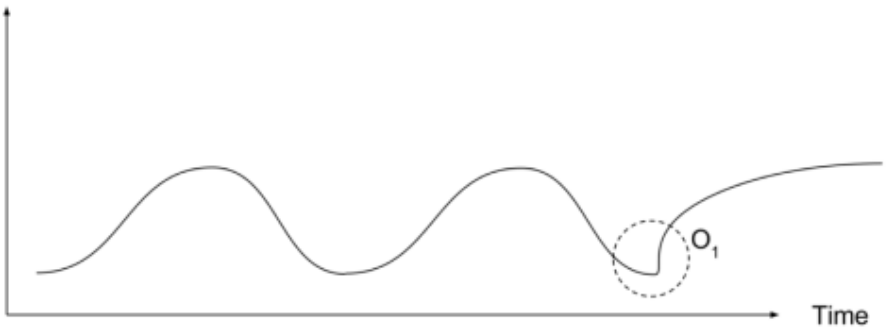

Рисунок 1.4 – Контекстні аномалії

Атрибути поділяються на:

– контекстуальні. Їх застосовують для з’ясування змісту (чи оточення)

кожного окремого екземпляру. У ЧР таким атрибутом є власне час. Саме він задає положення екземпляра всього діапазону. Таким атрибутом є, наприклад, у просторове положення або складніші поєднання властивостей;

– поведінкові. Вони визначають неконтекстуальні параметри, котрі стосуються визначеного екземпляру даних.

Поведінка, котра сприймається за аномальну, виявляється при допомозі аналізу ваг поведінкових атрибутів, зважаючи на визначений зміст даних. Отже, екземпляр може вважатися контекстуальною аномалією за цих умов, проте за тих самих поведінкових параметрів бути нормальним в іншому змісті.

Якщо, знаходячись в Українських Карпатах, температура надворі є близько +22 градусів, Чи є вона нормальною? Не володіючи певною додатковою інформацією дати відповідь на це питання складно, оскільки необхідно знати пору року, точне місцезнаходження, середню температуру доби упродовж останніх хоча б 10 років тощо. Якщо в Карпатах у даний час літо, тоді ця температура вважається нормальною. Але якщо зима, то ситуація діаметрально протилежна, оскільки зазвичай у цей час температура -20 градусів Цельсія, що становить відхилення 42 градуси і явно вибивається з контексту!

Чи розглянемо другий приклад. Всім відомі великі кліматичні зміни, котрі спричиняють глобальне потепління. Якщо переглянути новини, то можна побачити: «Березень на Алясці цього року був надзвичайно теплим, такого явища не траплялося упродовж всього періоду спостережень».

Необхідно звернути увагу на слова "незвичайно теплий". Щодо Аляски – це 15 градусів в плюс, проте для інших територій ця температура не вважатиметься аномальною.

Такі моменти носять назву контекстуальних аномалій, для них відхилення перебуває у залежності від контекстних даних, котрі регулюється атрибутами, як контекстними, так і поведінковими. Тут контекстним атрибутом властиво є місце знаходження, а поведінковим – власне температурний режим.

ВА перебуває у залежності від специфіки інформації, у різноманітних її контекстах. Саме тому, здебільшого, для їх формалізації варто отримати консультації від спеціалістів у визначеній предметній області.

1.2.3 Колективні аномалії

Є діапазоном зв’язаних екземплярів даних, котрі є аномальними щодо всього набору даних. Один екземпляр даних у такому діапазоні може бути і якимось відхиленням, хоча спільне багаторазове явище цих екземплярів власне і буде колективної аномалією (рис. 1.5).

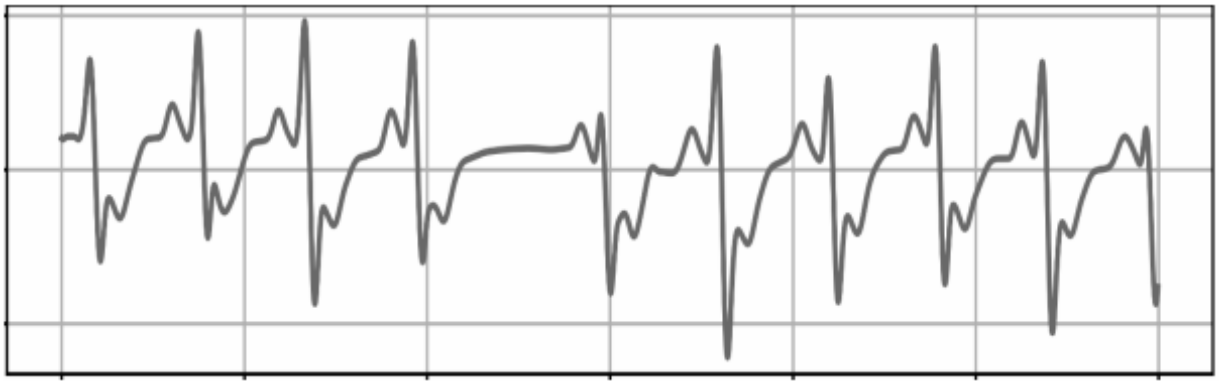

Рисунок 1.5 – Колективні аномалії

Розглянемо, наприклад, щоденні постачання фабрики текстилю. У цих сферах досить часто відбуваються затримки у доставці замовлень. Проте коли котрийсь із днів має забагато таких затримок, ось тоді ситуаціє потребує додаткового дослідження. Разова відтермінована поставка не буде важливою, проте аналіз такої картини повинен брати до уваги загальну ситуацію.

Аномалії такого типу важливі, якщо розглядати не окремі точки, а аналізувати їх поведінку в загальному. Якщо дана послідовність, то відносно одна одної такі аномалії можуть бути нормальними, проте щодо інших виникає точка зламу (англ. "change point"). Також має назву "розладка". Необхідно обчислити цей відрізок, відмінний від генеральної сукупності.

Важливе зауваження. Властиво для будь-яких даних власне точкові чи контекстуальні аномалії можуть бути наявними в будь-якій кількості.

Колективні аномалії можливі лише у тих наборах даних, в яких дані перебувають в тісному зв’язку між собою. Важливим є той факт, що точкові чи колективні аномалії разом з тим можуть бути і контекстуальними водночас. Точкова аномалія може стати контекстною, якщо ми застосуємо до неї контекст.

Або точкові аномалії можуть стати колективними, якщо ми поєднаємо кілька точкових аномалій.

1.3 Висновки до першого розділу

В цьому розділі дано основні визначення та терміни. Наведено докладний огляд, що ж таке власне аномалія, які вони бувають і чим характеризуються, а також порушені основні причини, цілі та завдання пошуку аномалій.

Коротко викладено основні підходи щодо пошуку аномалій у технологічному сигналі. Описано переваги та недоліки алгоритмів пошуку аномалій.

2 ІСНУЮЧІ МЕТОДИ ТА ПІДХОДИ ДО ВИЯВЛЕННЯ АНОМАЛІЙ

2.1 Класифікація методів пошуку аномалій

Для ВА можуть використовуватися наступні підходи:

– математичні підходи;
– методи дослідження операцій;
– кібернетичні методи;
– прогностичні методи.

У свою чергу всі підходи щодо пошуку аномалій, глобально можна розділити на три підгрупи завдань.

Завдання пошуку аномалій без вчителя має на увазі відсутність розмічених даних, а саме відсутні мітки про аномальність. Передбачається, що більшість використовуваної під час навчання вибірки є штатної, тоді екземпляри даних, які найменше відповідають більшій частині вибірки вважаються аномальними.

Під завданням пошуку аномалій з учителем мається на увазі наявність додаткової ознаки у вихідних наборах даних - мітки класу, в якій міститься інформація про те, чи є екземпляр даних штатним чи аномальним. Майже завжди такі завдання вирішуються шляхом побудови та навчання класифікаторів – алгоритмів МН, які здатні навчатися навіть на даних із незбалансованими класами.

При вирішенні задачі ВА з частковим залученням вчителя, вихідний набір даних містить інформацію лише про нормальні об'єкти та не містить аномальних.

Способи визначення аномалій можна розбити на такі підгрупи, як:

– ВА виходячи з метричних показників;
– кластерний аналіз;
– відхилення від асоціативних правил;
– застосування алгоритмів МН та нейронних мереж.

Нижче будуть докладно описані найбільш популярні способи ВА.

Існують різні підходи до розподілу методів ВА на типи. У цій роботі

розглядається класифікація методів за режимом розпізнавання та за способом реалізації.

Залежно від алгоритму, що застосовується, результатом роботи системи ідентифікації аномалій може бути або мітка екземпляра даних як аномального, або оцінка ступеня ймовірності того, що екземпляр є аномальним.

Останнім часом велика увага приділяється аналізу ЧР, що використовуються в різних галузях та описують тривалі процеси, що протікають у часі [13, 14].

У випадку ЧР - це впорядкована послідовність значень $TS=<ts_1, ts_2, ..., ts_n>$, що описує протікання будь-якого тривалого процесу. Значеннями ts_i можуть бути покази давачів, ціни на будь-який продукт, курс валюти тощо. У подальших прикладах час t вважається дискретним.

Процес ВА може проводитись для даних різного формату:

– потік даних (робота у часі);

– архів даних.

Кожному формату притаманні різні підходи ВА. Так, для потоку даних, що надходить у режимі реального часу, важливим є негайне отримання прогнозованої оцінки наявності аномалії та/або рекомендацій щодо її усунення. Робота з архівом даних, навпаки, передбачає обробку значно більших обсягів інформації та немає суворої вимоги негайного отримання результату.

Класифікація за типом навчання.

В залежності від класів даних, що застосовуються для втілення алгоритму, методи ВА можуть функціонувати в таких режимах [15].

1) Supervised anomaly detection (режим розпізнавання з учителем). Тут вимагається наявність навчальної вибірки, котра повністю повноцінно репрезентує систему і містить екземпляри визначених класів (як нормального, так і аномального). Дані позначені в наборах даних для навчання та тестування; коли простий класифікатор можна навчити та застосувати.

Цей випадок схожий на традиційне розпізнавання образів, за винятком класів, які здебільшого не збалансовані. Не всі підходи до класифікації підходять для цього завдання.

Наприклад, деякі типи дерев рішень не в змозі опрацьовувати з незбалансовані дані. SVM або ANN повинні працювати краще. Однак це налаштування не актуальне, тому що нам потрібно знати всі аномалії та правильно маркувати дані. У багатьох випадках аномалії не відомі заздалегідь або можуть виникати як новації на етапі тестування.

2) Semi-Supervised anomaly detection (режим розпізнавання частково з учителем). Спочатку, коли ми не маємо жодних знань, ми збираємо дані за результатами тренувань. У цьому налаштуванні також використовуються набори даних для навчання та тестування, де дані для навчання складаються лише з нормальних даних без будь-яких аномалій. Ідея в тому, що модель звичайного класу вже навчена і аномалії можна детектувати шляхом відхилення від вивченої моделі. Цей підхід також відомий як «однокласова» класифікація. Добре відомі підходи – це однокласова SVM та автокодувальники (автоекодери).

Автокодувальники (рис. 2.1) за архітектурою поділяються на такі:

– повнозв'язний;
– рекурентний;
– синхронний;
– seq2seq.

Загалом, будь-який підхід до оцінки густини може бути застосований для моделювання функції густини ймовірності нормальних класів. Наприклад, такі підходи, як гаусова суміш (англ. Gaussian Mixture) або оцінка щільності ядра (англ. Kernel Density Estimation).

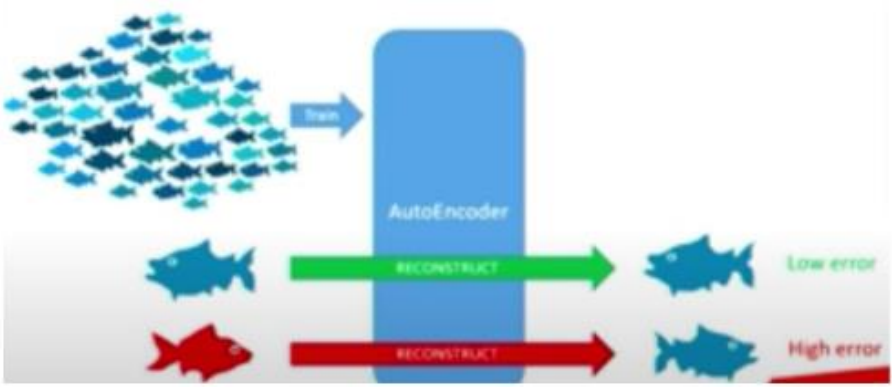

Рисунок 2.1 – Принцип автокодувальника

На рис. 2.2 наведено структуру «змагального» автоенкодера [16].

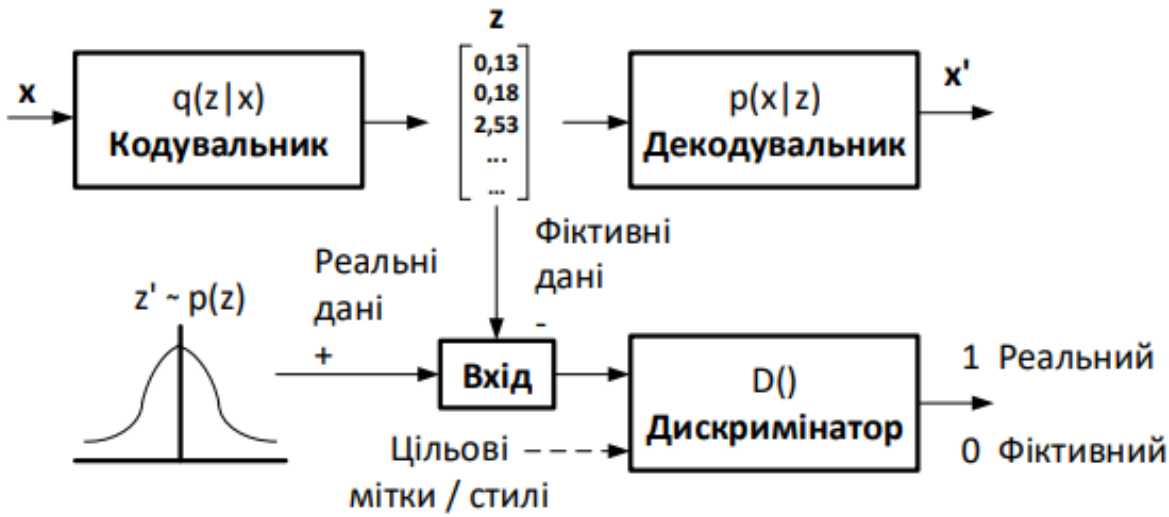

Рисунок 2.2 – Структура змагального автокодувальника

3) Unsupervised anomaly detection (режим розпізнавання без вчителя). Використовується, якщо інформації про дані відсутня апріорі. Такі алгоритми побудовані на здогадці, що аномальні екземпляри трапляються значно рідше, ніж нормальні. Ми не знаємо, що у даних нормально, а що ні. Це найбільш гнучка конфігурація, яка не потребує міток. Також немає різниці між навчальним та тестовим набором даних. Підходи до неконтрольованого ВА оцінюють дані виключно з урахуванням природних особливостей набору даних.

Зазвичай відстані або густини використовуються для оцінки того, що є нормальним, а що – викидом [17].

2.2 Ймовірнісний підхід

У генеративному підході пропонується вибрати ймовірнісну модель розподілу, з якої були відібрані нормальні дані, інакше кажучи знайти щільність розподілу $p(x)$. Тут об'єкти з низькою ймовірністю оголошуються аномаліями, тобто сама функція p діє як *anomaly score*. Такий підхід зіштовхується з принциповими труднощами. Для побудови щільності розподілу $p(x)$ потрібно

вирішити задачу виду (2.1)

$$\prod_{x \in Xnorm} \quad p(x, \theta) \rightarrow \frac{max}{\theta}, \tag{2.1}$$

де $x \in Xnorm$ - нормальні дані з вибірки, $\{p(x, \theta | \theta \in \theta)\}$ - деяке параметризоване сімейство густин розподілів

У разі відсутності міток завдання замінюється на (2.2)

$$\prod_{x \in X} \quad p(x, \theta) \rightarrow \frac{max}{\theta} \tag{2.2}$$

де X - всі доступні дані, включаючи аномалії.

Ці дві проблеми не еквівалентні і мають різні рішення, особливо при великій кількості аномалій даних. Для деяких сімейств розподілів існують методи підвищення стійкості, які теоретично можна використовувати для вирішення цієї проблеми (наприклад, замість оцінки математичного сподівання за середнім значенням, оцінюється за середнім значенням, стійким до викидів).

Однак на практиці метод недостатньо застосовний: складно перевірити отриману модель на адекватність, так і переконатися, що сімейство розподілів обрано правильно. Це з тим, що низьке значення функціоналу (2.2) може означати як невдале моделювання, і вироджене значення з малою ймовірністю появи аномальних об'єктів, що навпаки, є успіхом. Часто їх важко відрізнити один від одного. В результаті, у разі навчання без вчителя, ймовірнісне моделювання може застосовуватися тільки на основі апріорної інформації, інакше результат, отриманий за допомогою алгоритму, стає безпідставним.

Метод із використанням байєсовських мереж використовується для завдань класифікації. Основна ідея методу – перехід від апріорних ймовірностей до апостеріорних, при цьому всі ознаки та значення вважаються випадковими. Байєсовську мережу можна зобразити як ациклічний граф, вершини якого є

ознаки, а ребра - імовірнісними залежностями між них. Елементарна реалізація байєсівської мережі - це наївний класифікатор Байєса, який виявився одним з найефективніших методів обробки даних.

2.3 Лінійні методи

Основна їх ідея – створити таку лінійну модель, суттєві відхилення від якої характеризують аномалії. Нелінійний характер даних практично означає, що або необхідно побудувати ряд таких моделей і якимось чином усереднити відхилення, або застосувати ядерний перехід. Основне припущення лінійних методів у тому, що нормальні дані перебувають у підпросторі простору ознак R^d з розмірністю менше d.

Один з можливих алгоритмів наступний: оголосити i-ту ознаку вибірки цільовою змінною і вирішити задачу за допомогою лінійної регресії на основі ознак, що залишилися. Відхилення прогнозу від істини вважається аномальним значенням. Остаточна відповідь – усереднення цього результату за всіма ознаками. Такий алгоритм припускає, що між ознаками виявляється лінійна залежність, яка порушується для аномалій.

Узагальнення цього методу ґрунтується на властивостях основних компонентів $e_1, e_2, \ldots, e_d$ — нормованих власних векторів матриці XTX відповідних власним значенням $\lambda_1 \geq \lambda_2 \geq \ldots \geq . \lambda_d$.

Алгоритми, засновані на лінійних методах і, зокрема, на властивостях основних компонентів, застосовні практично лише у тому випадку, якщо дані показують лінійні залежності чи тренди. Якщо підпростір, у якому зосереджені нормальні дані, менш тривіальний, стає важко визначити вид цього підпростору.

Щоб обійти цю проблему, можна застосувати ядерний перехід і перейти в простір вищого виміру, де аномалії та нормальні дані можуть бути розділені гіперплощиною.

Найпопулярніший лінійний метод – SVM [18, 19]. Його мета – знайти гіперплощину в N-мірному просторі (N - кількість функцій), яка поділяє точки (приклади об'єктів) на окремі класи. Є множина ймовірних гіперплощин для

поділу точок на два різні класи. Мета методу – відшукати площину, котра володіє найбільшою відстанню між точками, які належать до обидвох класів. Метод належить до методів, які оцінюють щільність нормальних даних. Передбачається, що навіть розмітки немає. Є лише представники нормального класу. І ми маємо на тлі цього нормального класу виявити спостереження, які можна характеризувати як аномальні. Як сформувати таке правило? Описати, що таке нормальність та ненормальність. Геометрична інтерпретація полягала б у тому, що нормальним вважаємо все те, що щільно згруповано всередині деякої сфери радіуса *R*. Яка кількість точок випадатиме. Ми хочемо, щоб сфера була якнайменша, щоб множина була в деякому сенсі компактною. Мінімізуємо радіус цієї сфери при обмеженні на те, що у нас є всі об'єкти всередині сфери.

2.4 Метричні методи

Вони шукають точки в даних, які якимось чином перебувають і ізоляції від інших. Вважаємо, що у просторі визначена певна метрика $\rho(x_1, x_2)$, тоді можна ввести такі уявлення аномалії: це точки, що не належать ні одному з кластерів. До отриманих даних можна використати один із можливих алгоритмів кластеризації.

Найпопулярнішим метричним алгоритмом у задачах пошуку аномалій вважається метод $k - NN$ [20]. Є метричним алгоритмом класифікації об'єктів чи регресії (рис. 2.3).

Щоб класифікувати кожен об'єкт вибірки потрібно крок за кроком виконати наступне:

– обчислити дистанцію до кожного з них;

– провести відбір k об'єктів з навчальної вибірки з мінімальною відстанню до об'єкта, що класифікується.

Класом для класифікованого призначається той, який зустрівся найбільше разів з k найближчих.

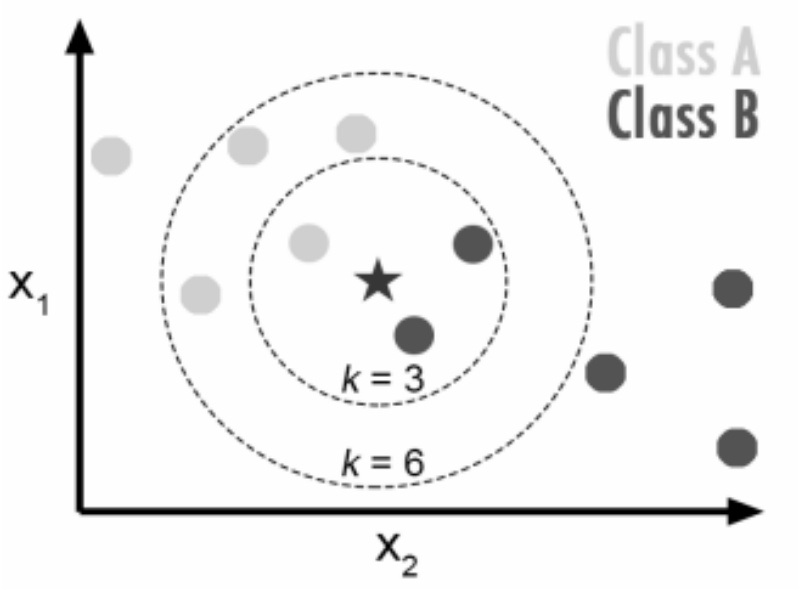

Рисунок 2.3 – Візуалізація прикладу *k - NN* з різними параметрами *k*

Аномаліями можуть бути потенційно класифіковані будь-які ізольовані об'єкти.

Такі методи відносяться так само є елементами кластерного аналізу чи кластеризації - це задача згрупування об'єктів так, щоб об'єкти одній групі (її і називають кластером) мали більшу схожість між собою (у визначеному сенсі), ніж об'єкти інших кластерів. Це основна мета інтелектуального аналізу даних і є загальним методом статистичного аналізу даних, що застосовується в різних областях, в т.ч. аналіз та розпізнавання зображень, відшукання інформації, біоінформатика, стиснення даних, комп'ютерну графіку та МН. Ідентифікація аномалій у такому угрупованні відбувається, коли виконується гіпотеза про те, що нормальні екземпляри даних знаходяться ближче до центрів кластерів, у той час як аномальні екземпляри знаходяться на відстані і можуть не входити в жоден із кластерів або утворювати власні окремі кластери. Кластеризація включена до групи навчання без учителя.

Застосування таких алгоритмів з параметрами (як варіант, *k*) вимагає присутності безсумнівної інформації про можливі розміри кластерів аномалій.

Основний позитив цих методів – їх інтерпретованість. Сміливо можна стверджувати, що людина використовує метричні методи для розв’язання задачі ВА. Проте є і негатив – необхідність вибору метрики. В реальних в даних немає

метрики, що інтерпретується. Потрібна апроксимація стандартними метриками – наприклад, манхеттенськими, евклідовими чи чебишевськими. Вибирання метрики без міток ймовірно буде сліпим вибиранням, а наближення може бути грубим навіть з урахуванням найкращої відповідності.

k -NN - це метричний метод, тобто алгоритм заснований на метриці або відстані. Використовується для автоматичної класифікації об'єктів, регресії. Для того, щоб віднести об'єкт чи точку до якогось класу застосовується наступний метод: цей предмет присвоюється тому класу, який є поширеним серед сусідів. Вибираємо *k* сусідів і дивимося, до якого класу належить більшість із них, і після цього присвоюємо наш об'єкт класу, що визначений.

2.5 Ізолюючий ліс

Ідея ізольованого лісу ґрунтується на принципі Монте-Карло: виконується випадковий поділ простору ознак так, коли ізольовані точки в середньому власне відсікаються від нормальних згрупованих даних [21]. Фінальне значення усереднюється за декілька проходів стохастичного алгоритму (рис. 2.4).

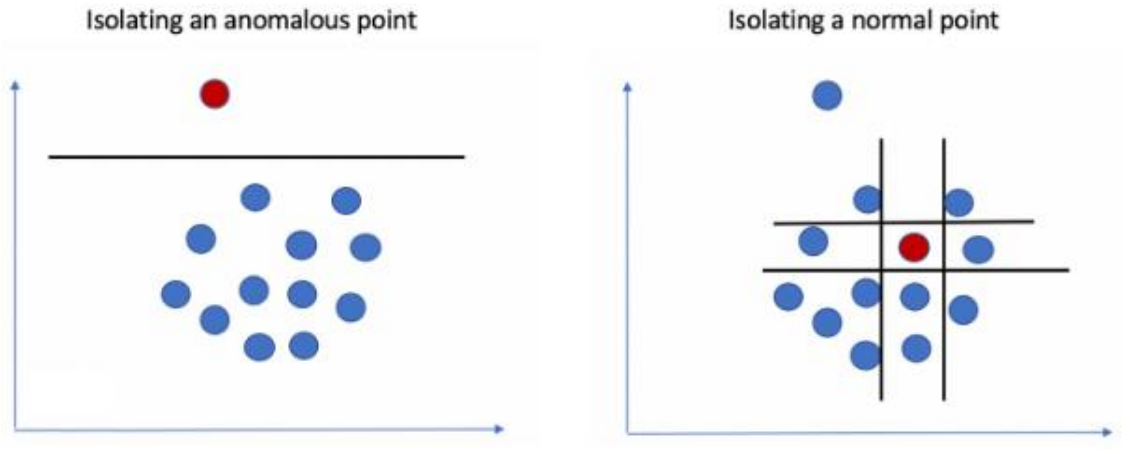

Рисунок 2.4 – Застосування ізоляційного лісу

Набір операцій ізолюючого дерева складається із створення випадкового двійкового дерева рішень. Корінь дерева – це весь простір ознак. На наступному вузлі вибираються випадкова ознака і визначається поріг випадкового поділу, які

вибираються з рівномірного розподілу в інтервалі від min до max значення визначеної ознаки. Мірилом зупинки буде збіг всіх об'єктів у визначеному вузлі, іншими словами дерево рішень повністю створено [22].

Існує твердження, що аномальні точки, як правило, знаходяться в листі невеликої глибини, який близький до кореня, якщо дереву необхідно створити ще кілька шарів, щоб розбити кластер нормальних даних на гіперплощині. Окрім того, число таких рівнів властиво перебуває у пропорційній залежності до розміру кластера. Таким чином, оцінка аномалії для зазначених у ній точок також пропорційна. Звідси випливає, що об'єкти, створені з невеликого розміру кластерів, які можуть бути аномаліями, мають значно меншу ймовірність.

Варто відмітити переваги алгоритму [22]:

– легко виявляє аномалії різного типу, як то ізольовані точки, котрі мають низьку локальну щільність, так і скупчення дрібних аномалій;

– відносно невисока складність дерева – $O(n \cdot \log \cdot n)$, що найчастіше ефективніше, ніж у інших алгоритмів;

– не потребує значних витрат на зберігання;

– відсутні гіперпараметри;

– незмінний до масштабування ознак, не вимогливий до задання метрик, не потребує особливих знань про природу даних.

2.6 Приховані Марковські моделі

Прихована марковська модель [23] заснована на ланцюзі Маркова. Ланцюги Маркова - це моделі, які інформують нас про ймовірності випадкових величин і послідовностей станів, кожна з яких може набувати значення з певного набору. Ці пропозиції можуть бути набором слів, тегів чи символів та інших станів. Ланцюги Маркова ґрунтуються на припущенні, що при прогнозуванні наступного стану поточної послідовності необхідна та важлива лише інформація про поточний стан, а будь-які попередні стани не впливають на результати.

2.7 Класифікація градієнтним бустингом

Як було зазначено, існує безліч різних алгоритмів у вирішенні завдання класифікації, проте для роботи цікаві лише ті, які вирішують завдання класифікації з допомогою “табличних” даних. Серед інших, виділяються ансамблієві моделі засновані на GBM [24, 25]. Це підтверджується численними перемогами на змаганнях з МН, як-от Kaggle[26].

Спочатку розглянемо загальну постановку завдання класифікації. Вирішуватимемо завдання відновлення вирішальної функції в контексті навчання з учителем. Нехай у нас є пари наборів ознак *x* та цільових змінних y, $\{(x_i, y_i)\}_{i=1,\dots n}=1,\dots n,$ на яких потрібно відновити вирішальну функцію $y_i = f(x_i)$. Для відновлення залежностей, використовуватимемо наближену функцію $\hat{f}(x)$. Також, для оцінки правдоподібності функції введемо функцію втрат *L(y, f(x))*, яку надалі мінімізуватимемо:

$$y \approx \hat{f}(x),$$
$$f(x) = arg\,\frac{min}{f(x)} L(y, f(x)). \qquad (2.3)$$

Але практично функцію *f(x)* досить складно оптимізувати, і набагато легше проводити оптимізацію в деякому функціональному просторі і шукати вже наближення $\hat{f}(x)$ ітеративно у вигляді кількох більш простих функцій:

$$\hat{f}(x) = \sum_{i=0}^{M} \blacksquare \hat{f}_i(x). \qquad (2.4)$$

Для вирішення поставленої задачі необхідно обмежитися сімейством функцій $f(x) = h(x,\theta)$, де θ - параметри функції. На кожному ітераційному кроці *t* знадобиться підбирати оптимальний коефіцієнт $\rho \in \mathbb{R}$. Тоді задачу з оптимізації, можна переписати таким чином:

$$\widehat{f}(x) = \sum_{i=0}^{t-1} \widehat{f}_i(x),$$
$$(\rho_t, \theta_t) = arg \min_{\rho,\theta} E_{x,y}[L(y, \widehat{f}(x) + \rho * h(x, \theta))], \quad (2.5)$$
$$f_t = \rho_t * h(x, \theta_t).$$

Вирішення подібних задач у загальному вигляді практично вкрай складний процес, тому, розумно, призвести завдання до більш простішого виду. Ми навчимо моделі так, щоб прогнози максимально корелювали з негативними градієнтами. Тобто вирішуючи завдання регресії методом найменших квадратів, уточнюючи передбачення цих залишків. Таким чином постійно мінімізувати квадрат різниці між залишками *r* і нашими прогнозами. На кроці *t* задача виглядає так:

$$\widehat{f}(x) = \sum_{i=0}^{t-1} \hat{f}_i(x),$$
$$r_{i,t} = -\left[\frac{\partial L(y_i, f(x_i))}{\partial f(x_i)}\right]_{f(x)=\widehat{f}(x)}, for\ i = 1, \ldots, n,$$
$$\theta_t = arg \min_{\rho,\theta} \sum_{i=1}^{n} (r_{i,t} - h(x_i, \theta_t))^2, \quad (2.6)$$
$$\rho_i = arg \min_{\rho} \sum_{i=0}^{t-1} L(y_i, \widehat{f}(x_i) + \rho * h(x_i, \theta_t)).$$

2.8 Функції втрат

Розглянемо варіанти того, які функції втрат можна використовувати для завдання двійкової класифікації, якщо $y \in \{-1, +1\}$. У зв'язку з принципово різним характером розподілів цільових змінних, ми прогнозуватимемо не самі класи, а логарифм їхньої ймовірності *L(y, f) = log(1 + exp(-2yf)).* Ця функція втрат відома як Logistic loss, або Bernoulli loss. Особливістю цієї функції втрат можна назвати те, що ми штрафуємо нашу модель навіть за коректні передбачення, тим самим збільшуючи межу між класами. Ця функція втрат найчастіше використовується під час бінарної класифікації.

L(y, f) = exp(-yf), також відома як Adaboost loss. Ця функція втрат схожа з

логістичною функцією втрат, але має жорсткіший штраф при помилки класифікації, як правило, використовується рідше.

При досить великій кількість параметрів можна показати, що певний параметр - це межа зверху частку об'єктів, які у нашій вибірці аномальні. Тобто. якщо хочемо, щоб 20% вибірки було поза сферою, параметр достатньо взяти 0.2.

Як вирішувати: беремо цільову функцію. Додаємо лямбда (множник Лагранжа), множимо на обмеження, отримуємо Лагранжіан. Далі оптимізуємо за подвійними змінними та виписуємо подвійне завдання оптимізації. Стандартний спосіб розв'язання задач квадратичної оптимізації. Якщо це зробити, то виходить сполучене двоїсте завдання щодо двоїстих змінних альфа.

Переваги методу в тому – дозволяє виміряти схожість двох об'єктів і можна ввести ядерну функцію.

Сила ядерних методів – був якийсь вихідний простір, в якому класи поділялися виключно нелінійним чином, але завдання все одно зводиться до лінійного поділу класів.

2.9 Метрики

Для оцінки того, як добре алгоритми розпізнавання аномалій працюють, потрібно ввести адекватну метрику оцінки моделі [27]. Як було зазначено раніше, ми шукаємо колективні аномалії, які вони своєю чергою зустрічаються дуже рідко під час аналізу реальних даних із підприємств. Значить і метрику оцінки якості моделі варто вибирати ту, що враховує класовий дисбаланс. Виходячи з цього були обрані такі метрики:

Accuracy – частка правильних відповідей. Найпоширеніша метрика в завданнях класифікації, основною її перевагою є легка інтерпретованість.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2.7}$$

Precision - частка чітко розпізнаних позитивних об'єктів (у разі аномалій) з усіх позитивно визначених.

$$precision = \frac{TP}{TP + FP} \tag{2.8}$$

Recall - частка чітко ідентифікованих об'єктів, які є позитивними.

$$recall = \frac{TP}{TP + FN} \tag{2.9}$$

F-score, або F-міра - агрегований критерій, що об'єднує за допомогою гармонійного середнього precision і recall. Найбільш популярний спосіб поєднати 2 метрики в 1.

$$F_\beta = (1 + \beta^2) \cdot \frac{precision \cdot recall}{(\beta^2 \cdot precision) + recall} \tag{2.10}$$

Як сказано, accuracy не розрізняє, помилилися ми, знаходячи нормальний елемент чи аномалію, чи ні.

Насправді ж, коли ми ставимо завдання ВА, нам куди критичніше виділити якийсь певний клас. Критично знайти помилку. Тому ми будемо використовувати метрику на основі precision / recall. Ідея наступна: під час роботи системи ми даватимемо сигнали тривоги. І ця метрика показуватиме, як часто наші сигнали виявляються вірними. Тобто, якщо ми даємо дуже мало неправдивих спрацьовувань, то у нас буде дуже високе значення метрики precision. Якщо у нас дуже багато хибних, то навпаки.

Інша метрика – це recall. Нам мало давати мало хибних. Потрібно отримати гарне покриття. При цьому ми не хочемо пропустити надто багато поломок, хвороб, атак на мережу тощо. Recall каже, яку частку всіх ключових поломок ми змогли знайти.

У україномовній термінології обидва терміни перекладаються як точність, тому надалі використовуватимемо англомовні терміни.

Оптимізувати обидва одразу – складне завдання. Простіше підібрати таке значення, яке їх комбінуватиме. Наприклад, середньогармонійне між обома метриками. Це захищає нас від великого перепаду у значеннях між метриками.

Додатково можна зважити і куди сильніше штрафувати за хибне спрацьовування, ніж за недостатньо хороше покриття. Це вже завдання аналізу задачі і того, що нам потрібно і корисніше.

Тим не менш, багато алгоритмів дають не бінарну відповідь: аномалія чи ні - а ступінь впевненості. Ось це "погане", а це - "незрозуміло". Як варіант, можна встановити поріг. Із 5% ймовірністю це значення аномалія. Оцінюємо для кожного, що вище за 5% - відкидаємо. Який у цьому випадку precision/recall? А на 10%? Для 15%? І т.д.

Таким чином, знаходимо значення та будуємо криву. Ставиться завдання, усно сформульоване приблизно так: "Ми хочемо, щоб у нас помилкових спрацьовувань було не більше 1 на 10". Для цього дивимося на графік і розуміємо, скільки ми зможемо знайти поганих елементів. спрацьовувань Зручним числом є площа під цією кривою AUC.”

Під час оцінки якості ми можемо визначити, що погано та що добре. Але ми лише навчаємо модель і не знаємо що є що. Зручним способом є створення штучної аномалії. У реальних системах, якщо ми маємо знання, як вона поводиться в аномальному стані, то такі значення і генеруємо. Якщо знаємо і можемо зробити припущення, можна брати значення з рівномірного розподілу [27].

Це зумовлено тим фактом, що рівномірний розподіл складно для детектування чогось поганого.

2.10 Інші методи та додаткова інформація

Класифікація. Втілення цього методу полягає в припущенні у тому, що для визначення «нормальності поведінки» системи достатньо одного чи кількох

класів. Отже, екземпляр, який не є у складі жодного з класів, буде відхиленням. ВА має етапи навчання і розпізнавання. Широке поширення серед алгоритмів даного методу мають нейронні мережі, байєсові мережі, SVM.

SVM використовується для ВА в системах, в яких нормальна поведінка представляється лише одним класом. Цей метод окреслює межу регіону, де містяться екземпляри нормальних даних (рис. 2.5). Властиво для кожного екземпляра потрібно з'ясувати, чи він перебуває у визначеному регіоні.

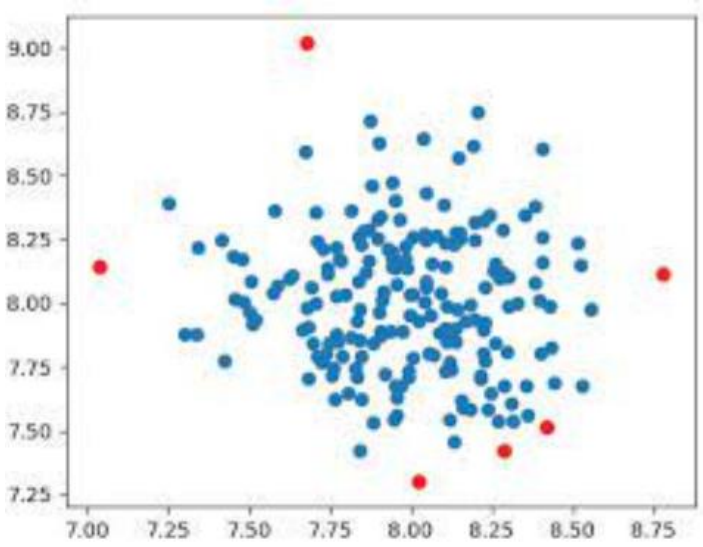

Рисунок 2.5 – ВА із застосуванням однокласового SVM

Кластеризація передбачає угруповання схожих екземплярів у кластери і потребує знань про властивості можливих відхилень. Підґрунтям ВА може слугувати припущення, що нормальні варіанти даних містяться в їх кластері, тоді як аномалії не належать жодному кластеру.

Проте за такої ситуації ймовірна поява проблеми визначення чітких кластерних меж.

Звідси можна зробити припущення, за якого нормальні дані знаходяться ближче до кластерного центру, тоді як аномальні є на значній відстані від нього.

За умови, що аномальних екземплярів є хоча б декілька, вони всі також можуть формувати кластери. Отже, їх в основі їх детектування лежить таке припущення - нормальні дані формують значні щільні кластери, тоді як аномальні – дрібні і розрізнені.

Одним із, мабуть, найпростіших втілень способу (беручи до уваги кластеризацію) вважається алгоритм k-means.

Як приклад гібридних систем ВА можна вважати операції:

– спільне використання кластеризації та k - NN;

– поєднання застосування суміщених k - NN алгоритмів Байєсових мереж та дерев рішень, а на додачу і k - NN разом із класифікацією;

– разом використати SVM та нейронної мережі глибинного навчання.

Розпізнавання аномалій у потоках даних.

Метод ковзного вікна. ВА як реального часу може вимагати додаткової модифікації методів. Найбільш простим у реалізації є алгоритм ковзного вікна.

Ця методика використовується для ЧР, які розбивається на кілька підпослідовностей - вікон.

Необхідно вибрати вікно фіксованої довжини, меншої ніж довжина ряду, для захоплення аномалії в процесі ковзання. Пошук аномальної підпослідовності здійснюється із застосуванням ковзного вікна по всьому ряду з кроком, що менший за довжину вікна.

Аугментацією називають методику збільшення даних з допомогою зміни наявних даних.

Зменшення дисперсії, як і збільшення дисперсії, вимагає декомпозиції сигналу на такі адитивні компоненти як шум $(noise)$ та тренд $(trend)$. Зазвичай для пошуку тренду в ЧР спочатку відбувається згладжування даних, а потім вже відбувається пошук функцій, що максимально точно відображають згладжену поведінка сигналу. Найчастіше для цього використовують експоненційне, логарифмічне або поліноміальне перетворення даних. Відмінність перетворення, що збільшує тренд, від того, котре зменшує тренд, полягає у виборі позитивного значення a, а саме, у першому випадку ми беремо значення $a > 1$, а в другому беремо $a <$ 1. Потім множимо її на адитивну компоненту відповідну шуму та складаємо з адитивною компонентою тренду.

Класичним підходом збільшення частки розмічених даних є алгоритм Noisy student:

– вибираємо модель teacher, яка добре класифікує розмічену ділянку

датасету;

– розмічаємо за допомогою моделі teacher нерозмічену частину датасету;

– отриманий датасет збільшуємо за допомогою аугментацій, описаних раніше, і навчаємо на ньому чисту модель student;

– повторюємо п.1 тільки тепер як модель teacher виступає модель student.

При використанні підходу Noisy student значно покращуються результати підсумкової моделі за рахунок додавання до вихідних розмічених даних, даних з латентною розміткою під час аналізу яких було отримано найвищі оцінки правдоподібності.

Такі підходи дозволяють генерувати необмежену кількість нових розмічених даних, придатних для подальшого навчання моделей.

Нетипові точки. Коли ми знаємо, що в наборі даних є нетипові точки, просто дотримуватись точності класифікації неправильно, оскільки вона показує лише відсоток правильних прогнозів моделі. Тому, перш ніж робити висновки, ми маємо переконатися, що модель здатна правильно класифікувати точки викидів. Хоча в деяких завданнях аномалії не відіграють суттєвої ролі, але брати їх до уваги хороша практика.

Ілюзія "правильності" моделі, яку дає нам описана вище точність, називається "класифікаційний парадокс". Найпростіший і наївніший спосіб вирішення цієї проблеми — видалення викидів перед відправкою даних.

Отримуємо користь від аномалій. Коли важливо, щоб модель могла правильно знаходити та оцінювати викиди, ми можемо просто навчити її на наборі даних із аномаліями. Добре відомий метод - навчання з урахуванням витрат класифікації (Cost-Sensitive Learning). Ідея в тому, щоб запровадити штраф за кожну виявлену аномалію (звичайні моделі ніяк не карають та не заохочують своїх прогнозів). Розглянемо приклад із шахрайськими транзакціями. По суті це завдання бінарної класифікації. Що відбувається, коли модель робить неправильний прогноз? Тут можливі два варіанти:

– класифікація звичайної операції як шахрайської;

– помилкова класифікація незаконної операції як звичайної.

Щоб оцінити масштаб, ми повинні взяти до уваги витрати на помилкову

класифікацію, які понесе банк. Якщо законна транзакція класифікується як шахрайська, користувач зазвичай дзвонить у службу підтримки та пояснює ситуацію. У цьому випадку витрати на вирішення питання, швидше за все, будуть незначними. Але у другому випадку можуть виникнути серйозні проблеми. Якщо вашу кредитну картку вкрали і витратили нетипово велику суму, яка не викликала банку підозр, то гроші можуть бути повернуті.

У традиційних моделях МН процес оптимізації зазвичай полягає у зменшенні вартості неправильних прогнозів. Для запобігання описаній вище проблемі ми пов'язуємо цю гіпотетичну вартість із правильно детектованою аномалією. Потім модель намагається зменшити чисті витрати (як у випадку із банком) замість штрафу за неправильну класифікацію.

Зауважимо, що всі моделі МН намагаються оптимізувати функцію витрат для підвищення ефективності. Це важливий процес, оскільки ми маємо переконатися, що класифікація працює правильно.

2.11 Висновки до другого розділу

Представлений великий ряд різних методів, а також їх комбінацій, що дозволяє вибрати потрібний для конкретної задачі і, спираючись на теоретичні відомості, перейти до практичного застосування того чи іншого методу або їх сукупності. Також розглянуто різні метрики.

3 ПРАКТИЧНА ЧАСТИНА

3.1 Побудова алгоритму класифікації

3.1.1 Опис вихідних даних

Дані, здебільшого, складаються з штучно зґенерованих сигналів з накладеними поверх аномаліями, але крім штучних, модель тестувалася і на відкритому датасеті Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation Version 1.0 [28, 29], в якому зберігаються сигнали довжини 500. Як було зазначено раніше, потрібні більш довгі сигнали, тому здійснювалося склеювання різних сигналів та аугментація даного датасета.

Склеювання сигналів неминуче спричиняє "шви", які модель може неправильно розпізнати. Тому використовувалися методи "амплітудного завмирання" (amplitude fades). Даний метод часто використовується для обробки звукових і радіо сигналів. При "амплітудному завмиранні" відбувається накладення двох сигналів один на одного за допомогою зваженої суми: один сигнал поступово збільшує амплітуду (fade in) від 0 до 1, а інший навпаки поступово зменшує (fade in) від 1 до 0 (рис. 3.1).

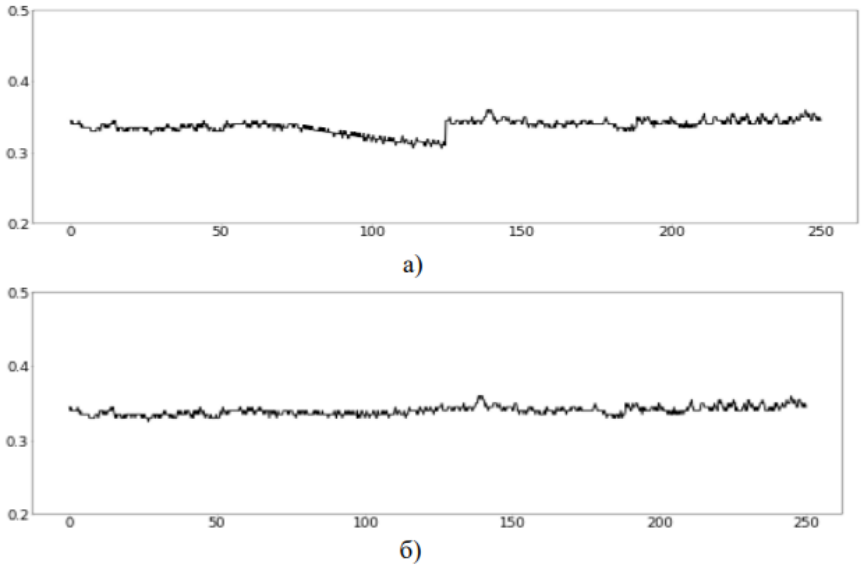

Рисунок 3.1 – Приклад амплітудного завмирання:
а) склеюванні зі швом; б) склеювання з амплітудним завмиранням

3.1.2 Попередня обробка даних

Розмітка. У деяких випадках, але не завжди, дані можуть бути розмічені. Це означає, що на навчальній вибірці ми точно знаємо, які спостереження є аномаліями, а які – ні. Наявність цього чинника сильно полегшує завдання, оскільки маємо повну інформацію у тому, які дані є аномальними. Розмітка дозволяє використовувати класичні підходи навчання з учителем (бінарна класифікація) [30].

Але, на жаль, не завжди є можливість розмітки даних, оскільки кількість спостережень може обчислюватися мільйонами рядків. Найчастіше ми маємо вміти вирішувати завдання виявлення аномалій, які не мають розмітки і лейблів англ. “label”). З цим виникає і ще одна проблема: якщо у нас відсутні лейбли, то як же нам валідувати дані? Як переконатися в тому, що та система, яку ми побудували, адекватна і те, що вона знаходить, справді аномалії?

Рішень може бути безліч, і універсального для всіх задач немає. Але певні кроки часто можуть допомогти у процесі валідації.

Перше, що може допомогти - експертна оцінка (англ. "domain knowledge") про відсоток аномальних спостережень, які можуть очікуватися в нашій вибірці. Наприклад, банківський фрод. У функціонуючого банку напевно мають бути експертні оцінки за рівнем фроду за банківськими картками. Наприклад, не більше 0.5-1%, інакше банк був би недостатньо надійним. У цьому випадку наші алгоритми можна було б налаштовувати таким чином, щоб вони відловлювали 0.5-1% спостережень як аномалії, тому що в іншому випадку, якщо такої оцінки немає, ми могли б вирішити, що аномалії складають і 10, і 20% від усієї сукупності даних, що в корінь би не відповідало дійсності.

Ще один варіант – намагатися інтерпретувати аномалії. Поставити запитання: «А чому те, що алгоритм визначив як аномалії, дійсно має бути аномалією?». Спробувати збудувати їх на графіку. Подивитися, як вони відрізняються від решти спостережень.

Визначити, в якому квантилі вони лежать, спробувати побудувати гістограми і таке інше.

Інший варіант – побудувати кілька моделей. Наприклад, не обмежуватися

прикладом, що ґрунтується на розладах, а розглянути також приклад, що ґрунтується на щільності і подивитися, які об'єкти різні моделі вважають аномаліями. Потім можна усереднити їх Score або сказати, що, наприклад, якщо більшість моделей визначили спостереження як аномальне, однозначно розглядати його як аномальне, в іншому випадку відкинути припущення про його аномальність.

І ще один варіант, який працює тільки в тому випадку, якщо очищення даних – це лише крок у підготовці даних для подальшого моделювання. Ми можемо побудувати модель на очищених даних. Але очищення повинне проводиться тільки на навчальній вибірці.

Переваги підходу в тому, що у нас залишаються в арсеналі всі можливі стандартні метрики навчання з учителем: завдання регресії, класифікація.

Наприклад, ми маємо завдання регресії. Хочемо передбачити ціну на квартиру. Якщо зібрати дані квартир по м. Тернопіль, то з'ясується, що серед них знайдеться безліч аномальних значень: як то квартири з дуже маленькою площею і ненормально високою ціною, так і з великою площею і дуже низькою ціною. Якщо спробувати побудувати модель таких даних, то, швидше за все, нічого хорошого не вийде. Модель навчиться під викиди. Тому першим кроком може бути очищення даних від таких аномальних значень. Але щоб все було зроблено акуратно, очищення слід проводити тільки на тренувальній частині даних, так як інакше ми випадково може привнести відкладену інформацію про випадкову відкладену вибірку в тренувальну частину.

Тому ми очищаємо тренувальну частину, навчаємо модель на тренувальних даних, прогнозуємо на тестових даних і дивимося, як змінюється якість моделі. Таким чином ми розуміємо, наприклад, скільки аномалій слід забрати з тренувальних даних.

Ця робота розширює область застосовності наявних підходів до класифікації сигналу, за рахунок розширення ознакового простору, у якому відображатимуться ЧС. Попередні дослідження ніяк не використовували апріорні знання про стандартну поведінку системи, що негативно позначається в конкретних робочих ситуаціях. Тим не менш, робота має обмеження на те, що

здійснює пошук тільки колективних аномалій, а це означає, що вона може працювати тільки з великими ділянками сигналу, а не з окремими мітками часу.

Виходячи з описаного вище, був розроблений і реалізований новий алгоритм, що формує ознаковий простір, що враховує апріорну інформацію про природу сигналу.

Нехай у нас є дискретизований технологічний сигнал, представлений ЧР $X(t) = \{x_i\}_{i=0}^{N}$, де $t_i = t_0 + (\mathrm{i} - 1)\tau : x_i = x(t_i), i = 1, \ldots, N$ з постійним кроком дискретизації τ та апріорна інформація про те, які значення має видавати система за кожного режиму роботи. Тоді в такому випадку аномалією можна називати такі значення фрагмента x_t для яких параметр P більший за якийсь вибраний поріг S.

Перші 80% значень нашого ЧР назвемо тренувальними, решта відповідно тестовими. Потім за допомогою методу ковзного вікна (рис. 3.2) з постійним кроком передаємо набори значень з тренувальної вибірки на вхід алгоритму попередньої обробки даних.

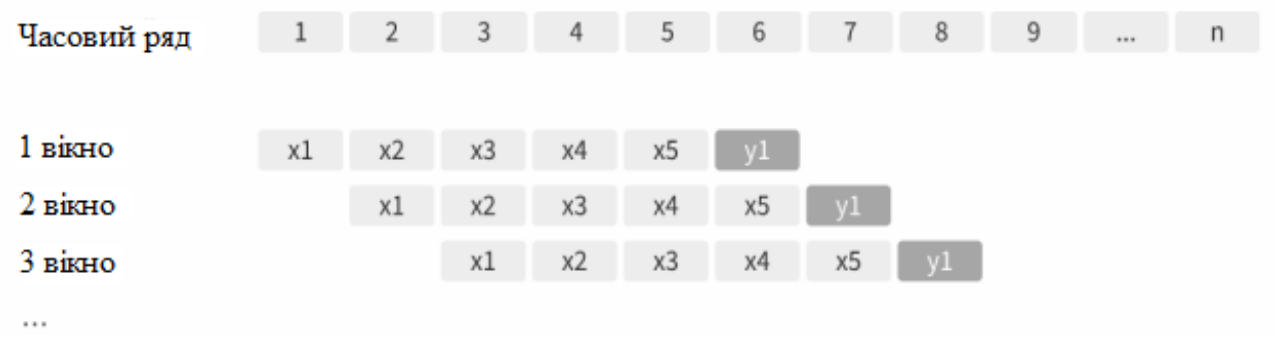

Рисунок 3.2 – Ковзне вікно

На етапі передобробки даних використовується апріорна інформація про штатну поведінку системи. В даному випадку ми знаємо кількість робочих фаз системи, що відстежується, і їх передбачувані штатні значення.

Основна ідея полягає в тому, що ми можемо знайти найближче передбачуване штатне еталонне значення для кожного елемента з поданого на передобробку фрагмента, а потім вже обчислювати статистичні ознаки.

Нехай є x- фрагмент сигналу розмірності v, отриманий на передобробку за

допомогою ковзного вікна, набір n фаз роботи системи, і для кожної фази є своє передбачувана штатна поведінка p_i де $i \in [1, N]$. Тоді ми можемо створити матрицю M_{n*v}, де кількість рядків збігається з кількістю фаз роботи системи, а кількість стовпців збігається з розмірністю x. Рядки заповнюємо відповідними значеннями p_i. Далі віднімаємо відрізок вхідного сигналу по рядках з матриці, що вийшла, і шукаємо мінімум модуля різниці по стовпцях (рис. 3.3).

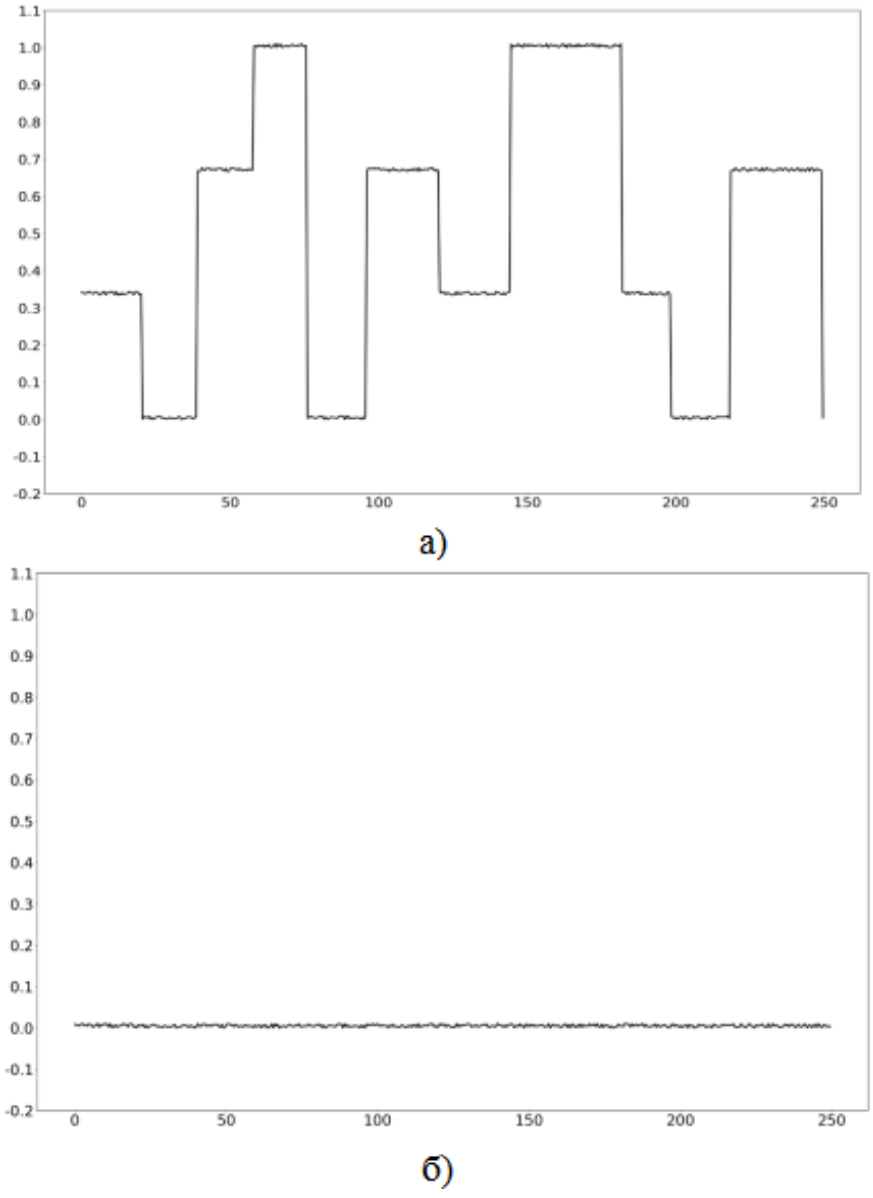

Рисунок 3.3 – Попередня обробка сигналу:
а) вихідний сигнал; б) сигнал передобробки

За допомогою цього етапу ми шукаємо для кожного значення фазу, яка найімовірніше відпрацьовувала в даний конкретний відрізок часу. У результаті

отримуємо розкладання сигналу на передбачувані щаблі та інший шум.

Також на цьому кроці отримуємо додаткову ознаку про поведінку сигналу, групуючи поряд однакові ймовірні фази, що стоять. Дана ознака, назвемо її order, допомагає при класифікації фрагмента, оскільки на підприємствах критично важливо знати, за яких умов трапляються ті чи інші аномалії.

Алгоритмічно пошуку такої ознаки можна описати так.

Нехай у нас є впорядкований набір фаз для вхідного сигналу w_i, де $i \in N$. Тоді, якщо $w_{i+1} = w_i$, то видаляємо w_{i+1} з набору. Для набору, що утворився, повторюємо цю процедуру до тих пір, поки будь-які два сусідніх значення не будуть різними.

3.1.3 Формування простору ознак

У отриманого сигналу після передобробки потрібно обчислити статистичні ознаки (табл. 3.1), на основі яких надалі і проводитиметься класифікація фрагментів сигналу.

Таблиця 3.1 – Список розрахункових ознак

Назва	Опис
difference	Різниця між найбільшим та найменшим значенням
order	Порядок зміни станів роботи
mean	Середнє значення
median	Медіана
skewness	Момент Пірсона
std	Стандартне відхилення
variance	Дисперсія
kurtosis	Коефіцієнт ексцесу
complexity	Складність
TP	Кількість пікових точок

Продовження табл. 3.1

LC	Лінійний коефіцієнт з LS
MSDC	Середня друга похідна
MAC	Середнє абсолютних змін
SAC	Сума абсолютних змін

Існує кілька підходів до передачі ознак у модель класифікації. Якби ми мали величезні масиви даних, то розумно було б ознаки з табл. 3.1 передавати безпосередньо в модель. Але оскільки в реальних завданнях даних завжди недостатньо, то вибирається один із методів зменшення розкиду можливих значень ознак - різні округлення, перевід чисел з одного формату в інший, логарифмування та інше. В даному випадку ми вдамося до способу, який для кожної статистичної ознаки $F = [f_1, f_2, \ldots, f_l]$, оцінює її попадання у розподіл із тренувальної вибірки за формулою:

$$M[\, f^i_{train}\,] - z \times D[\, f^i_{train}] \leq \; f^i_{test} \leq M[\, f^i_{train}] + z \times D[\, f^i_{train}\,] \quad (3.1)$$

де f^i - i-та ознака, $1 \leq \; i \leq N$, $M[*]$ та $D[*]$ мат. сподівання та дисперсія відповідно, z - коефіцієнт дисперсії, який при тренуванні алгоритму використовувався рівним 2, інакше кажучи, відбувається оцінка влучення в 2-дисперсійний інтервал.

Таким чином, ми отримуємо матрицю $M = [к \; x \; n]$, $m_{ij} = \{0,1\}$, де k - кількість інтервалів, котрі тестуються, n - кількість ознак, що розраховуються. Нуль означає, що обчислене значення ознаки не потрапило у 2-дисперсійний інтервал, одиниця – потрапило. Виконавши це перетворення ми отримуємо новий простір ознак, який подається на вхід класифікатора для визначення його аномальності.

У відкритому доступі є низка рішень, заснованих на GBM, всі вони, як показує практика, дають приблизно однакові результати. Найбільш популярними

з них вважаються XgBoost та CatBoost. У поточній роботі буде використовуватися XgBoost, оскільки у нього більш детальна документація [31].

3.2 Експериментальні дослідження

Для досягнення поставлених раніше завдань необхідно довести, що запропонований алгоритм перевершує аналоги, котрі використовуються при вирішенні задачі класифікації технологічного сигналу. Отже нам необхідно розробити модель $a(j(X(t)), \theta)$, де j - алгоритм попередньої обробки даних, θ - параметри моделі, яка вже зі свого боку на основі переданих у неї попередньо оброблених фрагментів визначає чи є вони аномальними, чи ні з високим рівнем достовірності.

У ході побудови описаної вище моделі використовувалася мова програмування Python 3.8 [32] та стек бібліотек [33 - 36] з табл. 3.2.

Таблиця 3.2 – Стек використовуваних бібліотек

Назва бібліотеки	Короткий опис
numpy	бібліотека призначена для ефективної роботи з багатовимірними масивами
pandas	бібліотека з необхідними інструментами для роботи з часовими рядами та
scipy	бібліотека яка включає інструментарій для знаходження статистичних ознак, які формують простір ознак для фрагментів сигналу
matplotlib	бібліотека включає основні інструменти для візуалізації
xgtboost	бібліотека для МН, що використовує GBM

3.2.1 Навчання класифікатора

Цей процес відбувався на описаних раніше розмічених сигналах з використанням усіх перерахованих аугментацій та синтетичних його генерацій. Сам датасет для кожного свого значення $x \in X_{train}$ має клас належності $y(x) \in \{0;$

1}. Процедура з підготовки та передобробки відповідає тому, що було викладено у другому розділі даної роботи. Відповідно до цього, сигнал був розбитий на фрагменти рівної довжини, на основі їх обчислена матриця ознак *F*, оцінка попадання в допустимий інтервал. Таким чином отримуємо матрицю розмірності *[k x n]* і мітку аномальності кожного фрагмента *y(x)*.

Таким чином ми отримали 153 000 фрагментів поділених щодо 80/20 на навчальну та тестову вибірку. Параметри алгоритму (табл. 3.3) були підібрані за допомогою методу (grid search) на крос валідації.

Таблиця 3.3 – Параметри класифікатора XgBoost

Параметри	Значення
iterations	1000
learning rate	0.03
random seed	0
L2	3.0
bagging temperature	1
depth	6
step	30
window size	70

Оскільки класифікатор навчався на досить великий вибірці, що включає великий спектр різних аномалій, передбачається що він може давати досить хороші результати під час використання реальних даних. Також для покращення результатів класифікації його можна донавчати.

3.2.2 Результати та обговорення

Навчена модель тестувалася на реальних даних з додаванням штучних ступенів у них. У такий спосіб можна було згенерувати необмежену кількість тренувальних значень. На рис. 3.4 представлений сигнал з однією фазою роботи

із штучно доданими ступенями.

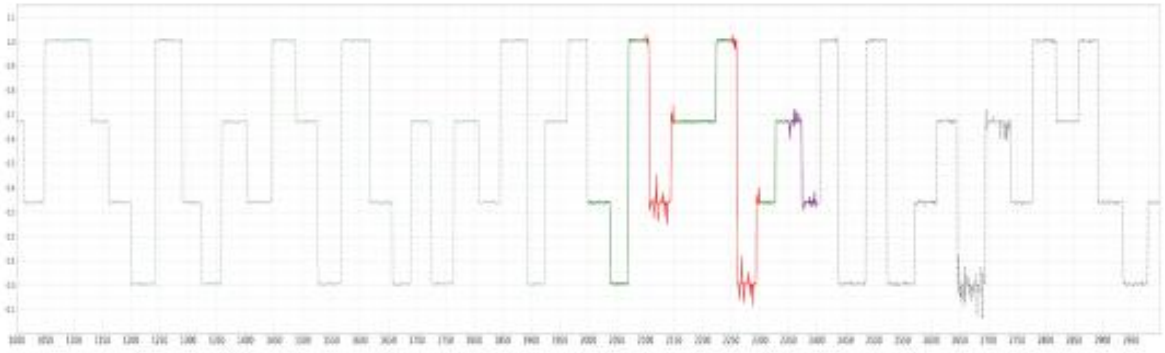

Рисунок 3.4 – Тестовий ступінчастий сигнал

Ця модель значно перевершує аналогічну модель 2019 року і значно покращує якість знаходження аномалій. Це доводять дані із наведених нижче табл. 3.4 – 3.6 з усередненими значеннями метрик з усіх видів аномальності:

Таблиця 3.4 – Результати моделі 2019 (без ступінчастих сигналів)

	Accuracy	Precision	Recall
Change trend	95.43	95.22	93.49
Increase dispersion	88.00	85.51	78.87
Decrease dispersion	81.21	62.96	56.35
Shift trend	82.80	77.17	61.71
Add noise	92.38	88.70	85.62

Таблиця 3.5 – Результати поточної моделі (без ступінчастих сигналів)

	Accuracy	Precision	Recall
Change trend	96.31	95.78	93.98
Increase dispersion	90.12	87.31	82.53
Decrease dispersion	81.30	64.73	62.14
Shift trend	83.25	80.32	65.41
Add noise	93.36	89.65	87.70

Таблиця 3.6 - Результати моделі 2019 із ступінчастим сигналом

	Accuracy	Precision	Recall
Change trend	23.12	17.26	76.32
Increase dispersion	16.26	14.43	52.56
Decrease dispersion	20.21	16.66	46.35
Shift trend	26.16	19.59	36.45
Add noise	22.47	18.75	46.54

Таблиця 3.7 - Результати поточної моделі зі ступінчастим сигналом

	Accuracy	Precision	Recall
Change trend	93.37	90.17	89.20
Increase dispersion	86.63	84.20	77.59
Decrease dispersion	77.44	59.70	56.57
Shift trend	79.06	74.70	60.76
Add noise	89.88	85.67	80.54

Якщо порівнювати випадки без ступінчастого сигналу, то неважко помітити, що якість залишилася приблизно на тому ж рівні або збільшилась досить мінорно - це можна пояснити тим, що використовувалася новіша версія реалізації GBM, і ще більш розширений простір ознак. Якщо говорити про сигнал з додаванням до нього ступенів, то, очевидно, що модель не здатна його аналізувати - більшість поданих на аналіз фрагментів сприймалися як аномалії. Таку поведінку можна пояснити тим, що модель сприймала переходи від ступеня однієї фази до іншої як аномалію зміщення тренда. Також варто відзначити, що при додаванні ступенів, поточна модель теж дещо погіршила свої показники, це зрозуміло, оскільки в процесі передобробки ми перемножуємо різницю модуля сигналу з матрицею еталонних значень кожної фази роботи, тоді існує ймовірність, що модуль різниці фактичної фази може виявитися більшим, ніж модуль різниці з якоюсь іншою фазою роботи. У такому разі у нас вийде, що ми

ще на етапі передобробки припустилися помилки, відносячи деякі значення не до тієї фази.

Але як свідчить практика, такі помилки виявляються вкрай рідко, саме рідше, ніж 0.13% від усього аналізованого сигналу.

3.2.3 Додаткові відомості про давачі

Щодня генерується величезна кількість даних із різних давачів. Ми живемо під час четвертої промислової революції, в якій вирішальну роль відіграють IoT та штучний інтелект [37]. Де є IoT, там є давачі [38]. А точніше, широка мережа давачів, яка відстежує безліч реальних проблем. Коли давачі спрацьовують неправильно, їх сигнали ведуть до хибних спрацьовувань систем усунення несправностей. Тому без виявлення аномалій не обійтись.

Джерелом може бути будь-яка складна інженерна система. Звичайним завданням для будь-якого виробництва є контроль за справністю пристроїв. Виникає потреба проводити регламентне обслуговування. Наприклад, для літака. Але обслуговувати всі вузли літака після кожного польоту надзвичайно дорого і не ефективно. Хотілося б, якщо ми маємо таку можливість, збирати параметри, виявляти зміни в системі, які спричиняють поломки. Раніше виявлення несправностей та поломок дозволить заощадити на ремонті, доки ситуація не стала критичною.

Таким чином утворюються нові сервісні моделі. Сучасні корпорації прагнуть надати подібні послуги в комплекті зі своїм товаром. Тобто продається не лише фізичний товар, а й послуга щодо його моніторингу. Такий підхід є вигідним для всіх сторін, зацікавлених в ефективній взаємодії.

Наступний крок у розвитку таких компаній – це продавати не лише пристрій, а ще й час безвідмовної роботи. Тенденція підтверджує, що саме такої стратегії дотримуються сучасні компанії. Реалізація включає велику кількість технічних завдань, у тому числі вже згадане МН. Існують різні критерії, які хочеться балансувати у кожному окремо взятому завданні. Наприклад, щоб послуга була доступна 24/7, а також збільшення часу безперебійної роботи та зменшення витрат на обслуговування. Складність у тому, що це взаємозалежно.

Зведення витрат на обслуговування до мінімуму може призвести до скорочення терміну безперебійної роботи. Потрібно знайти баланс між критеріями, залежно від цін помилок кожного критерію. Важливо також враховувати властивості технічної системи. Часто інфраструктура не готова для зберігання та збору даних.

Процес застосування системи контролю може бути розбитий на три рівні.

Перший рівень: збір даних. Найчастіше у сучасних системах це вже реалізовано. Для верстатів старого виробництва можуть знадобитися нові давачі.

Другий рівень: складування. Пропуски, зашумлення, дискретні та безперервні дані. Різна частота. Різнорідність. Проблеми технічного плану. Потрібно побудувати прогнозну модель.

Третій рівень: ухвалення рішення. На основі прогнозної моделі необхідно зробити висновки та прийняти рішення про заміну тих чи інших вузлів, що, природно, має на увазі під собою втручання у бізнес-процес.

Особливо складно впоратися із ситуацією, коли потрібна заміна деталі, заміна якої не регламентована, або за регламентом має бути ще не скоро.

Тому, незважаючи на те, що запропоноване рішення підвищить ефективність надання послуг або виробництва, зміна бізнес-процесу може виявитися дорогою і недоступною на даному етапі життя компанії.

Приклад. Літак. Декілька параметрів характеризує температуру рідини, що охолоджує. Мета: зрозуміти, чи стався витік. На даних із давачів є шум. Необхідно автоматично детектувати витік і спрогнозувати, через скільки польотів буде пробитий критичний рівень, тобто встановити своєрідний індикатор. У разі спрацьовування ймовірність витоку схоплюється і робиться прогноз, коли станеться аварія.

Інший приклад. Є силова установка. Знімається набір параметрів близько двохсот. Усі вони різноманітні. Деякі знімаються разів за політ, інші мають по десятки тисяч свідчень за політ. Є журнал збоїв. Таким чином, маємо ЧР з різною частотою.

За кілька польотів необхідно визначити і детектувати поломки. Турбіна виробляє електроенергію. Зі значень сотень параметрів необхідно виявити, що

з'явилося аномальне спостереження, яке є провісником поломки.

Кількість поломок може бути невеликою. Як припущення, можна застосувати метод класифікації. Але поломок може бути настільки мало, аж до того, що їх доводиться розмічати вручну. Або може бути багато різних помилок. Які групи властивостей потенційно відповідальні відразу визначити неможливо.

Ситуації можуть бути різні, але якийсь єдиний принцип вирішення все одно потрібний. Як практиці завдання не зводиться до того, що ми беремо якийсь відомий нам метод і застосовуємо. Доводиться будувати складний набір методів, щоб одержати пов'язану модель.

Якщо відбувається поломка і є непрямі спостереження, то даних мають бути провісники. Якщо в приладі є тріщина, то зростають показання давача вібрації. Якщо виявити подібні свідчення, можна прогнозувати події, які нас цікавлять.

Перший крок у пошуку провісників. На безлічі наявних параметрів будуємо графік зв'язків між цими параметрами. Може також зображуватись матрицею з використанням колірних виділень, де чим темніший колір осередків, тим сильніший зв'язок між параметрами. Зв'язок може бути як лінійний, так і не лінійний.

Далі ці параметри декомпонуємо. Усередині кожної групи намагаємось виділити аномалії. Якщо групи перестали бути корельованими, то незабаром поломка буде в якійсь групі.

У кожній групі підпослідовність аномалій (за історичними даними). Намагаємося зрозуміти, яка з них найбільш ймовірно призводить до тієї поломки, яку ми прогнозуємо. Якщо такі залежності виявлено на історичних даних, то можна тестувати і на реальних даних.

3.3 Висновки до третього розділу

У цьому розділі було описано новий підхід для побудови високоточного класифікатора ЧР з розширенням області застосування на ступінчастий сигнал. Виділено унікальний ознаковий простір, що адекватно відображає поведінку

сигналу. Описано новий алгоритм передобробки ЧР.

Для кожного кроку потрібно використовувати різні способи МН. Одним класом обмежуватися не можна, оскільки кожен випадок унікальний, а використання базових методів дасть грубу тривіальну модель.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою кваліфікаційної роботи магістра є узагальнення інформації про різні методи ВА та їх практичне застосування на технологічних сигналах. Оскільки, проведення робіт з розробки та використання алгоритму передбачає застосування комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки ПЗ комп'ютерних систем, в тому числі і фахівців з практичного застосування ВА в технологічних сигналах, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [39]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог [40];

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського

виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Не допускається підключати комп'ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп'ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18.

Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення

інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з дослідження інформації про різні методи ВА та їх практичне застосування на технологічних сигналах.

4.2 Планування та порядок проведення евакуації населення з районів наслідків впливу НС техногенного та природного характеру

В умовах неповного забезпечення захисними спорудами в містах та інших населених пунктах, що мають об'єкти підвищеної небезпеки, основним засобом захисту населення є евакуація і розміщення його у зонах, які є безпечними для проживання людей.

Евакуації підлягає населення, яке проживає в населених пунктах, що знаходяться у зонах можливого катастрофічного затоплення, можливого небезпечного радіоактивного забруднення, хімічного ураження, в районах виникнення стихійного лиха, аварій і катастроф (якщо виникає безпосередня загроза життю та здоров'ю людей). Залежно від обставин, які склалися на час надзвичайної ситуації, може бути проведено загальну або часткову евакуацію населення тимчасового або безповоротного характеру. Загальна евакуація проводиться за рішенням Кабінету Міністрів України для всіх категорій населення і планується на випадок [41]:

– можливого небезпечного радіоактивного забруднення територій навколо атомних електростанцій (якщо виникає безпосередня загроза життю та здоров'ю людей, які проживають в зоні ураження);

– виникнення загрози катастрофічного затоплення місцевості з чотиригодинним добіганням проривної хвилі.

Часткова евакуація проводиться за рішенням Кабінету Міністрів України у разі загрози або виникнення надзвичайної ситуації техногенного та

природного характеру.

Під час проведення часткової евакуації завчасно вивозиться не зайняте у сферах виробництва та обслуговування населення: діти, учні навчальних закладів, вихованці дитячих будинків, разом з викладачами та вихователями, студенти, пенсіонери та інваліди, які утримуються у будинках для осіб похилого віку, разом з обслуговуючим персоналом і членами їх сімей.

У сфері захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру евакуація населення планується на випадок:

– аварії на атомній електростанції з можливим забрудненням території; усіх видів аварій з викидом сильнодіючих отруйних речовин; загрози катастрофічного забруднення місцевості :

– лісових і торф'яних пожеж, землетрусів, зсувів, інших геофізичних і гідрометеорологічних явищ з тяжкими наслідкам, що загрожують населеним пунктам.

Загальна евакуація проводиться шляхом вивезення основної частини населення з міст і небезпечних районів усіма видами наявних транспортних засобів на відповідній адміністративній території та виведення найбільш витривалої його частини пішки. Часткова евакуація проводиться з використанням транспортних засобів, що експлуатуються за діючим графіком. На органи виконавчої влади, органи місцевого самоврядування та керівників об'єктів, які проводять евакуацію населення, покладається:

– планування і проведення евакуації працівників та членів їх сімей;

– подання до відповідних транспортних органів розрахунків потреби у транспортних засобах для вивезення працівників і членів їх сімей до безпечних районів;

– контроль за плануванням, підготовкою і проведенням евакуаційних заходів підвідомчими об'єктами;

– визначення та підготовка безпечного району для розміщення евакуйованих працівників і членів їх сімей.

Інші заходи та порядок проведення евакуації викладено у постанові

Кабінету Міністрів від 26 жовтня 2001р. № 1432 про затвердження Положення про порядок проведення евакуації населення у разі загрози або виникнення надзвичайних ситуацій техногенного та природного характеру.

У плані евакуації, складовою частиною якого є карта (схема), зазначаються:

– висновки з оцінки обстановки у разі виникнення надзвичайної ситуації;

– порядок оповіщення населення про початок евакуації;

– кількість населення, яке підлягає евакуації, за віковими категоріями;

– терміни проведення евакуації;

– склад евакуаційних органів і терміни приведення їх у готовність;

– кількість населення, яке вивозиться різними видами транспортних засобів окремо і виводиться пішки;

– розподілення об'єктів за збірними евакуаційними пунктами, пунктами посадки, районами (пунктами) розміщення та евакуаційними напрямками; маршрути евакуації;

– райони (пункти) розміщення евакуйованого населення; пункти посадки на транспортні засоби, пункти висадки у безпечному районі, порядок доставки населення з пунктів висадки до районів (пунктів) розміщення;

– заходи щодо організації приймання, розміщення, захисту та життєзабезпечення евакуйованого населення у безпечному районі;

– порядок організації управління і зв'язку.

Розділ плану, в якому визначаються види забезпечення евакуації, розробляється відповідними службами. До цього розділу включаються:

– основні завдання служби;

– перелік сил і засобів, які залучаються для виконання евакуаційних заходів;

– терміни виконання завдань.

Евакуаційна комісія відповідного органу виконавчої влади, на території якої планується розміщення евакуйованого населення, розробляє план його приймання і розміщення у безпечному районі з картою (схемою) [41].

У плані зазначаються:

– кількість евакуйованого населення за віковими категоріями, яке прибуває у район, місто, район у місті, селище, село;

– кількість об'єктів і їх розподіл за районами у місті, сільськими і селищними радами, населеними пунктами;

– чисельність населення, яке проживає на відповідній території;

– будівлі і споруди для розміщення об'єктів господарювання;

– пункти висадки евакуйованого населення;

– порядок і терміни доставки евакуйованого населення з приймальних евакуаційних пунктів до районів (пунктів) розміщення;

– порядок розміщення евакуйованого населення;

– порядок забезпечення евакуйованого населення продуктами харчування, водою, предметами першої необхідності, медичним та іншими видами обслуговування;

– порядок оповіщення посадових осіб, які відповідають за приймання евакуйованого населення, про початок евакуації і терміни прибуття населення.

План приймання і розміщення евакуйованого населення включає також розділ з транспортного забезпечення евакуації, в якому зазначається:

– кількість транспортних засобів кожного виду і термін їх подачі до пунктів посадки;

– кількість населення, яке підлягає евакуації;

– терміни відправлення евакуйованого населення у безпечні райони;

– терміни прибуття евакуйованого населення до пунктів посадки;

– маршрути руху транспортних засобів;

– кількість рейсів.

На всіх громадян, які підлягають евакуації, завчасно складаються списки за об'єктами і житлово-експлуатаційними організаціями у трьох примірниках, один з яких залишається на об'єкті або в житлово-експлуатаційній організації, другий (у разі одержання рішення про проведення евакуації) після уточнення списків надсилається на збірний евакуаційний пункт, третій - до евакуаційної комісії району (пункту) розміщення.

З отриманням рішення (сигналу) про проведення евакуації евакуаційні комісії уточнюють завдання керівникам об'єктів щодо проведення евакуаційних заходів, контролюють стан оповіщення населення, його збору, формування колон (через начальників маршрутів), забезпечують переміщення їх до пунктів евакуації, а також разом з транспортними службами - готовність транспортних засобів до перевезень, уточнюють порядок їх використання, підтримують постійний зв'язок з начальниками маршрутів та з органами виконавчої влади безпечних районів, інформують їх про хід евакуації.

У райони розміщення евакуаційних органів та населення, яке підлягає евакуації, направляються представники евакуаційних комісій для вирішення питань приймання, розміщення і життєзабезпечення евакуйованого населення.

Керівник органу виконавчої влади і евакуаційна комісія безпечного району, організовують підготовку пунктів висадки, розгортають приймальний евакуаційний пункт, уточнюють кількість прибулих і порядок подачі транспортних засобів для їх вивезення з пунктів висадки, а також з проміжних пунктів евакуації до пунктів розміщення, контролюють роботу керівників об'єктів безпечних районів з прийому і розміщення евакуйованого населення.

У разі оголошення евакуації громадяни самостійно на міських транспортних засобах, які у цей період працюють цілодобово, прибувають на збірні евакуаційні пункти. Працівники цих пунктів розподіляють громадян, які підлягають евакуації, за транспортними засобами, інструктують їх і забезпечують посадку на транспортні засоби.

Евакуйовані громадяни повинні мати при собі паспорт, військовий квиток, документ про освіту, трудову книжку або пенсійне посвідчення, свідоцтво про народження, гроші і цінності, продукти харчування і воду на 3 доби, постільну білизну, необхідний одяг і взуття загальною вагою не більш як 50 кілограмів на кожного члена сім'ї. Дітям дошкільного віку вкладається у кишеню або пришивається до одягу записка, де зазначається прізвище, ім'я та по батькові, домашня адреса, а також ім'я та по батькові матері і батька.

4.3 Висновки до четвертого розділу

В цьому розділі розглянуто важливі питання охорони праці та безпеки в надзвичайних ситуаціях, висвітлено питання Планування та порядок проведення евакуації населення з районів наслідків впливу НС техногенного та природного характеру.

ВИСНОВКИ

Кваліфікаційна робота присвячена виявленню аномалій у технологічному сигналі з використанням методів МН.

Основні результати проведеного дослідження:

– здійснено розширення вибірки з допомогою аугментації реальних даних. Вибірка, що вийшла, покриває великий спектр аномалій, що зустрічаються в реальних даних з підприємств;

– розроблено новий алгоритм класифікації технічних сигналів шляхом перетворення їх у набори статистичних ознак та подальшої їх класифікації методом градієнтного бустингу;

– продемонстрована працездатність алгоритму на модельних даних та на синтезованих штучно. Здійснено оцінку роботи алгоритму на них та аналіз отриманих оцінок.

Отримані результати підтверджують працездатність даного алгоритму класифікації технологічного сигналу. Рання версія даного алгоритму класифікації було впроваджено у прототип модуля виявлення аномалій у технологічному сигналі.

Передбачається, що модуль, що розробляється, інваріантний до отриманих сигналів, і повинен показувати гідний результат на широкому спектрі можливих завдань.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.

2. Басюк Т.М. Машинне навчання: Навчальний посібник. - Львів: Видавництво «Новий Світ - 2000», 2021. - 315 с.

3. Кононова К. Ю. Машинне навчання: методи та моделі. - Харків: ХНУ імені В. Н. Каразіна, 2020. - 301 с

4. Баранніков В.В. Особливості завдання виявлення аномалій // Інформаційні моделі, системи та технології: Праці XI наук.-техн. конф. (Тернопіль, ТНТУ ім. І. Пулюя, 13-14 грудня 2023 р.) – Тернопіль, 2023. – С. 17.

5. Richardson Bartley D, Radford Benjamin J, Davis Shawn E et al. Anomaly Detection in Cyber Network Data Using a Cyber Language Approach // arXiv preprint arXiv:1808.10742. — 2018.

6. Sergey Gavrin, Damir Murzagulov, Alexander Zamyatin. Anomaly Detection in Process Signals within Machine Learning and Data Augmentation Approach. 15th International Conference on Machine Learning and Data Mining MLDM 2019.

7. Damir A. Murzagulov, Alexander V. Zamyatin, Pavel M. Ostrast. Approach To Detection Of Anomalies Of Process Signals Using Classification And Wavelet Transforms. IEEE International Russian Automation Conference 2018

8. H.-S. Wu, “A survey of research on anomaly detection for time series,” 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Dec. 2016.

9. Ibidunmoye O., Metsch T., Elmroth E. Real-time detection of performance anomalies for cloud services //2016 IEEE/ACM 24th International Symposium on Quality of Service (IWQoS). – IEEE, 2016. – pp. 1-2.

10. Jolliffe I. Principal component analysis //International encyclopedia of statistical science. – Springer, Berlin, Heidelberg, 2011. – pp. 1094-1096.

11. Mehrotra G., Mohan K., Huang H., 2017. Anomaly Detection Principles

and Algorithms.

12. Рубан І.В., Мартовицький В.О., Партика С.О. / «Класифікація методів виявлення аномалій в інформаційних системах» // УДК 004.056.5 // Системи озброєння і військова техніка, 2016, № 3(47).

13. Прогнозування та аналіз часових рядів. Методичні вказівки до практичних занять та самостійної роботи студентів спеціальності 051 «Економіка» // Укл: Юрченко М. Є. – Чернігів: ЧНТУ. 2018. – с. 5-15.

14. Ceschini G. F. et al. Optimization of statistical methodologies for anomaly detection in gas turbine dynamic time series //Journal of Engineering for Gas Turbines and Power. – 2018. – vol. 140. – is. 3. – p. 032401.

15. Machine Learning for Predictive Maintenance: A Multiple Classifier Approach / Susto Gian A., Pampuri Simone and other // IEEE Transactions on Industrial Informatics. 2015. V. 11, iss. 3. pp. 812–820.

16. Improved Bidirectional GAN-Based Approach for Network Intrusion Detection Using One-Class Classifier / Wen Xu [et al.] // Computers. – 2022. – Vol. 11, no. 6. – P. 85.

17. Gavrin S., Murzagulov D., Zamyatin A. Anomaly Detection in Process Signals within Machine Learning and Data Augmentation Approach // Machine Learning and Data Mining in Pattern Recognition. MLDM 2019: 15th International Conference on Machine Learning and Data Mining, New York, 20-25 July 2019 : proceedings. Vol. 2. Leipzig: Ibai-publishing, 2019. pp. 585–598.

18. Candelieri A. Clustering and support vector regression for water demand forecasting and anomaly detection //Water. – 2017. – vol. 9. – is. 3. – pp. 224-235.

19. Shengfeng T., Jian Y., Chuanhuan Y. Anomaly Detection Using Support Vector Machines // Advances in Neural Networks. 2004. Vol. 3173. pp 592–597.

20. What is the k-nearest neighbors algorithm? [Електронний ресурс] - Режим доступу: https://www.ibm.com/topics/knn (дата звернення: 12.11.2023).

21. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // Data Mining, 2008. ICDM’08. Eighth IEEE International Conference on. – IEEE, 2008. – pp. 413-422.

22. Liu F. T., Ting K. M., Zhou Z. H. Isolation-based anomaly detection //ACM Transactions on Knowledge Discovery from Data (TKDD). – 2012. – vol. 6. –

is. 1. – pp. 3 - 12.

23. Прихована марковська модель. [Електронний ресурс] - Режим доступу: https://uk.wikipedia.org/wiki//Прихована_марковська_модель (дата звернення: 14.11.2023)

24. Jain Anil K., Dubes Richard C. Algorithms for clustering data. — Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1988.

25. Friedman J. H. Greedy function approximation: a gradient boosting machine //Annals of statistics. – 2001. – pp. 1189-1232.

26. Kaggle. [Електронний ресурс] - Режим доступу: https://www.kaggle.com/ (дата звернення: 15.11.2023).

27. Класифікаційні метрики [Електронний ресурс] - Режим доступу: http://www.andriystav.cc.ua/Downloads/MITER/Lecture_04.pdf (дата звернення: 16.11.2023).

28. Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation Version 1.0. [Електронний ресурс] - Режим доступу: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/6 C3JR1 (дата звернення: 14.11.2023).

29. Tennessee Eastman Process with cyber-attacks dataset, 2017. [Електронний ресурс] - Режим доступу: https://kas.pr/ics-research/dataset_tep_59 (дата звернення: 14.11.2023).

30. Попередня обробка даних [Електронний ресурс] - Режим доступу: http://elbib.in.ua/predvaritelnaya-obrabotka-dannyih.html (дата звернення: 24.11.2023).

31. XGBoost Documentation [Електронний ресурс] - Режим доступу: https://xgboost.readthedocs.io/en/stable/ (дата звернення: 24.11.2023).

32. Machine Learning with Python. [Електронний ресурс] - Режим доступу: https://www.freecodecamp.org/learn/ machine-learning-with-python/ (дата звертання 02.12.2023).

33. NumPy [Електронний ресурс] - Режим доступу: https://numpy.org/ (дата звертання 03.12.2023).

34. Pandas [Електронний ресурс] - Режим доступу:

https://pandas.pydata.org/ (дата звертання 03.12.2023).

35. SciPy [Електронний ресурс] - Режим доступу: https://scipy.org/ (дата звертання 03.12.2023).

36. Matplotlib — Visualization with Python [Електронний ресурс] - Режим доступу: https://matplotlib.org/ (дата звертання 03.12.2023).

37. Нічепорук А.О. Інтелектуальна система виявлення аномалій та ідентифікації пристроїв розумних будинків із застосуванням колективної комунікації // Електротехнічні та комп'ютерні системи. 2021. № 34 (110). – с.

38. Wheelus, C. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework [Text] / C. Wheelus, X. Zhu // Cyber Security and Privacy in IoT. 2020. P. 259–285

39. Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. 2011. 215 с.

40. НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації ЕОМ». Наказ Держгірпромнагляду від 26.03.2010 No 6

41. Зеркалов Д.В. Безпека життєдіяльності та основи охорони праці. Навч. посібник. К.: «Основа». 2016. 267 с.

42. Атаманчук П.С. Безпека життєдіяльності та охорона праці (Практичний курс): Навчальний посібник. Кам'янець-Подільський: "Думка". 2010. 152 с.

ДОДАТКИ

ДОДАТОК А
Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

Ю. Апостол, Р. Трембач, М. Яворська
ВИМІРЮВАЛЬНА СИСТЕМА ДЛЯ КОНТРОЛЮ ПРОФІЛЮ ВЕЛИКОГАБАРИТНИХ СУПУТНИКОВИХ АНТЕННИХ СИСТЕМ
J. Apostol, R. Trembach, M. Javorska
MEASURING SYSTEM FOR CONTROLLING THE PROFILE OF LARGE SATELLITE ANTENNA SYSTEMS 14

Базан І.В., Коваль А.А.
ВИЯВЛЕННЯ КІБЕРАТАК В «РОЗУМНОМУ МІСТІ» НА ОСНОВІ МАШИННОГО НАВЧАННЯ
I. Bazan, A. Koval
DETECTING CYBERATTACKS IN A SMART CITY BASED ON MACHINE LEARNING 16

В.В. Баранніков
ОСОБЛИВОСТІ ЗАВДАННЯ ВИЯВЛЕННЯ АНОМАЛІЙ
V.V. Barannikov
FEATURES OF ANOMALIES DETECTION TASK 17

О.Безруков, Стадник Марія
ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ З ДОПОМОГОЮ МЕТОДІВ МАШИННОГО НАВЧАННЯ
O. Bezrukov, Stadnyk Mariia 18
DETECTION OF FRAUD TRANSACTIONS USING MACHINE LEARNING METHODS

Богатирчук І.П., Дичик І.О., Патей Я.В., Яблонський Д.С.
ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПРЕДСТАВЛЕННЯ МЕДИЧНИХ ДАНИХ
I. Bohatyrchuk, I. Dychyk, Patey Ya., D. Yablonskiy
COMPARATIVE ANALYSIS OF METHODS AND MEANS OF MEDICAL DATA PRESENTATION 19

Марія Бояринцева
ОГЛЯД МОЖЛИВОСТЕЙ RUBY В КОНТЕКСТІ ПОБУДОВИ СИСТЕМ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ
Mariia Boyaryntseva
OVERVIEW OF RUBY CAPABILITIES IN THE CONTEXT OF BUILDING SYSTEMS USING ARTIFICIAL INTELLIGENCE 20

Василь Валицький; Богдана Млинко
МЕТОДИ ТА МОДЕЛІ СПЕКТРАЛЬНОГО АНАЛІЗУ БІОМЕДИЧНИХ СИГНАЛІВ
Vasyl Valytskyi; Bogdana Mlynko
METHODS AND MODELS OF BIOMEDICAL SIGNAL SPECTRUM ANALYSIS 21

В.А. Варава
ПОШУК ЛОКАЛЬНИХ ЕКСТРЕМУМІВ НА ГРАФІКАХ ЯСКРАВОСТІ
V.A.Varava
SEARCH OF LOCAL EXTREMUM ON BRIGHTNESS GRAPHS 22

А.О. Вельгош, М.В. Дуда, М.П. Далінський, І.С. Завіша
АВТОМАТИЗОВАНА СИСТЕМА КЕРУВАННЯ ПАЛИВНИМИ ЄМНОСТЯМИ
A. O. Velhov, M. V. Dynia, M. P. Dolinskyi, I. S. Zavisha
AUTOMATED FUEL TANK MANAGEMENT SYSTEM 23

Р.Р. Вербівський, О.П. Кузьмич, Я.В. Литвиненко
МЕТОДИ ОПРАЦЮВАННЯ БІОМЕДИЧНИХ СИГНАЛІВ В ЗАДАЧАХ ТЕЛЕМЕДИЦИНИ
R.R. Verbitskyi, O.P. Kuzmych, Ia.V. Lytvynenko
METHODS OF PROCESSING BIOMEDICAL SIGNALS IN THE PROBLEMS OF TELEMEDIC 25

Вертух В.І., Матчак О.М., Олійник Д.А.
ЗАСТОСУВАННЯ ФІЛЬТРОВОГО МЕТОДУ ДЛЯ ОЦІНЮВАННЯ СТАТИСТИК БІОСИГНАЛІВ
V.Vertsuch, O. Matchak, D. Oliynyk
APPLICATION OF FILTER METHOD FOR EVALUATION OF BIOSIGNAL STATISTICS 26

УДК 004.056
В.В. Баранніков
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОСОБЛИВОСТІ ЗАВДАННЯ ВИЯВЛЕННЯ АНОМАЛІЙ

V.V. Barannikov

FEATURES OF ANOMALIES DETECTION TASK

Аномалії — це закономірності даних, котрі не відповідають добре визначеному поняттю нормального поведінки. Проблема детектування цих патернів називається виявленням аномалій (ВА). Важливість ВА зумовлена тим фактом, що аномалії даних приводять до значної і дієвої інформації в різних областях застосування. Наприклад, ненормальні схеми трафіку в комп'ютерних мережах можуть означати, що комп'ютери відправляють конфіденційні дані в несанкціоновані місця призначення, відхилення в даних транзакції по кредитній картці можуть вказувати на кредитні картки або посвідчення особи і т.п.

Навіщо взагалі шукати аномалії?

По-перше, щоб покращити якість моделі. Тобто це завдання передобробки даних.

По-друге, в даних можуть бути шуми. Таким чином, аномалії зашумлюють наші дані і через ці викиди наш алгоритм може перенавчитися та видавати невірні оцінки. Тобто, є мета уникнення подальшого перенавчання.

По-третє, вивчення викидів. Можливо у деякій системі з платною підпискою є кілька аномальних користувачів, які платять у десятки разів більше за всіх інших. Тоді нам потрібно вивчити, що це за користувачі і що потрібно зробити, щоб їх зберегти. На основі цього вже вирішувати, чи варто ці аномалії виключати із даних, чи ні.

По-четверте, виявлення поломок. Зазвичай цим займаються диспетчери, які сотні годин бачать графіки зміни показів тих чи інших приладів і в деяких випадках їм вдається запобігти поломці. Або після її виникнення виявити, де саме і коли вона сталася.

Якщо доручити це й аналогічні завдання алгоритму, то, можливо, поломок більше не виникатиме, оскільки відсутній людський фактор неуважності. Система точно і безпастережно визначить, чи ця подія є аномалією, чи ні. Однак навіть алгоритм може помилятися, але це вже питання правильного вибору та складання моделі.

У більшості випадків аномальні дані, що визначаються нами, відносяться до виявлення викидів. Після навчання цих даних ми шукатимемо аномальні точки в новому наборі даних.

Виявлення новизни (ВН) - це метод, що дозволяє ідентифікувати нові чи невідомі шаблони та закони даних. Передумова виявлення новизни у тому, що набір навчальних даних, як відомо, є «чистим» і не забруднений реальними «шумовими» даними чи реальними «викидами», та був після навчання цих даних нові дані навчаються для пошуку шаблонів даних новизни. ВН, в основному, застосовується для дослідження та розпізнавання нових шаблонів, тем і тенденцій, включаючи обробку сигналів, комп'ютерний зір, розпізнавання образів, інтелектуальних роботів та інші технічні вказівки, а також сфери застосування, такі як дослідження потенційних захворювань, відкриття нових видів, надбання нових тем спілкування тощо. ВН пов'язані з ВА.

На початку точки новизни часто з'являються у даних сторонніми чином. Цей сторонній спосіб зазвичай сприймається як сторонній. Тому шаблони виявлення та розпізнавання цих двох типів дуже схожі. Однак через деякий період часу, коли дані новизни підтверджуються як нормальний патери, наприклад, нове захворювання ідентифікується як поширене захворювання, патери новизни буде об'єднаний у нормальний патери і більше не буде ставитись до категорії аномальних точок.