

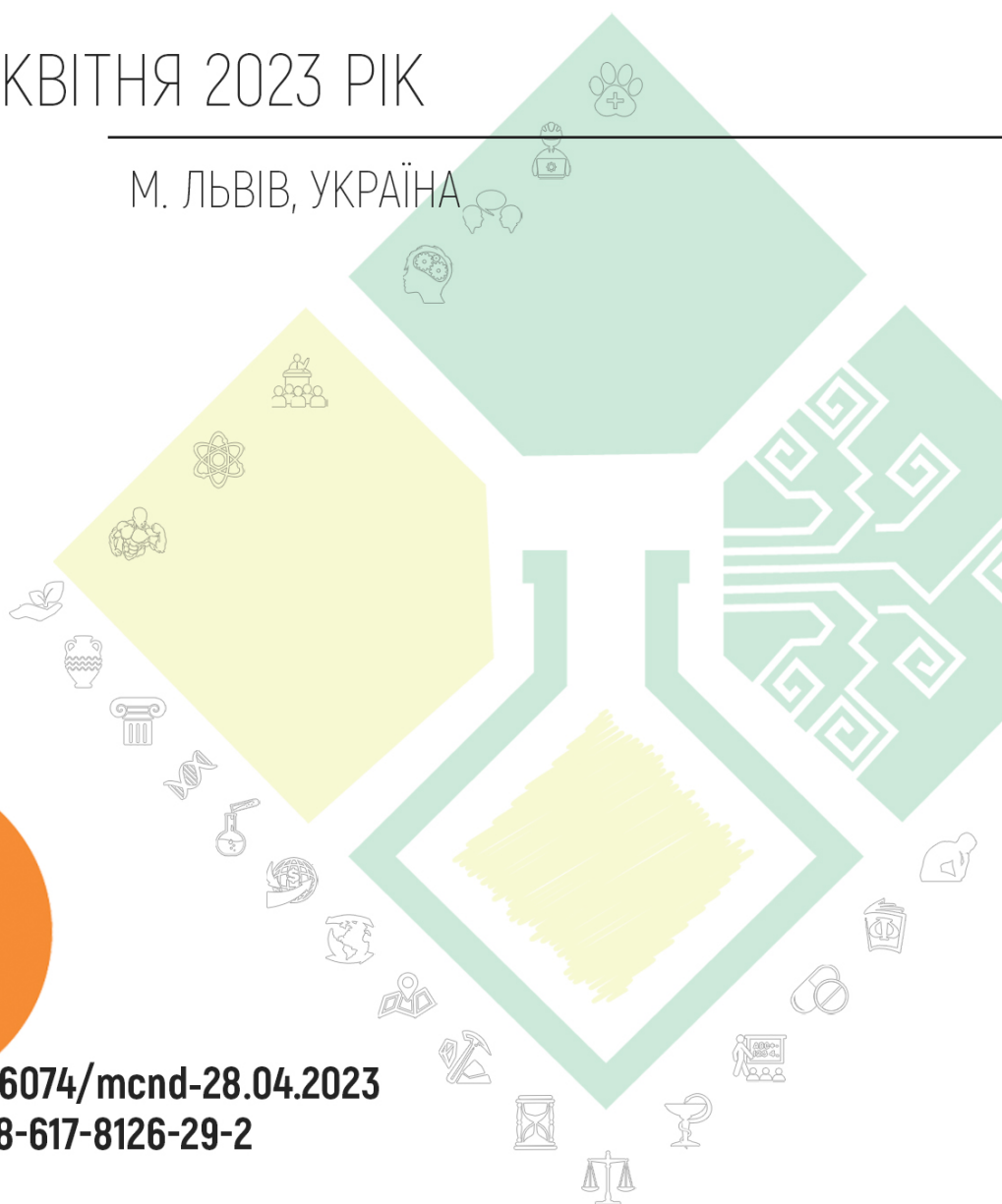
РОЗВИТОК НАУКОВОЇ ДУМКИ ПОСТІНДУСТРІАЛЬНОГО СУСПІЛЬСТВА: СУЧАСНИЙ ДИСКУРС

I 28 КВІТНЯ 2023 РІК

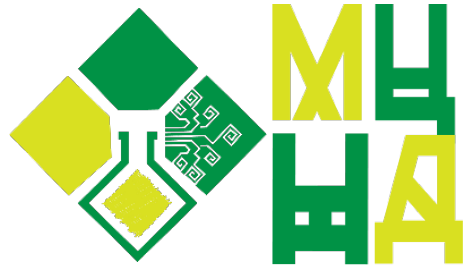
М. ЛЬВІВ, УКРАЇНА



DOI 10.36074/mcnd-28.04.2023
ISBN 978-617-8126-29-2



МАТЕРІАЛИ
ІІІ МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ



Міжнародний Центр Наукових Досліджень

РОЗВИТОК НАУКОВОЇ ДУМКИ ПОСТІНДУСТРІАЛЬНОГО СУСПІЛЬСТВА: СУЧАСНИЙ ДИСКУРС

| 28 КВІТНЯ 2023 РІК
м. Львів, Україна

Вінниця, Україна
«Європейська наукова платформа»
2023



Організація, від імені якої випущено видання:
ГО «Міжнародний центр наукових досліджень»

Голова оргкомітету: Рабей Н.Р.

Верстка: Зрада С.І.

Дизайн: Бондаренко І.В.



Конференцію зареєстровано Державною науковою установою «УкрІНТЕІ» в базі даних науково-технічних заходів України та бюлетені «План проведення наукових, науково-технічних заходів в Україні» (Посвідчення № 58 від 17.01.2023).

Матеріали конференції знаходяться у відкритому доступі на умовах ліцензії Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0).

Р 64

Розвиток наукової думки постіндустріального суспільства: сучасний дискурс: матеріали III Міжнародної наукової конференції, м. Львів, 28 квітня, 2023 р. / Міжнародний центр наукових досліджень. — Вінниця: Європейська наукова платформа, 2023. — 192 с.

ISBN 978-617-8126-29-2

DOI 10.36074/mcnd-28.04.2023

Викладено матеріали учасників III Міжнародної спеціалізованої наукової конференції «Розвиток наукової думки постіндустріального суспільства: сучасний дискурс», яка відбулася 28 квітня 2023 року у місті Львів.

УДК 001 (08)

ISBN 978-617-8126-29-2

© Колектив учасників конференції, 2023
© ГО «Європейська наукова платформа», 2023
© ГО «Міжнародний центр наукових досліджень», 2023

СПІЛЬНИЙ АВТОКОДЕР ІЗ ПОРОГОМ ВИЯВЛЕННЯ АНОМАЛІЇ СУГЛОБА НА ВИРОБНИЧИХ ЛІНІЯХ Шустрова А.Є.	120
---	-----

СЕКЦІЯ XVI. ФІЛОЛОГІЯ ТА ЖУРНАЛІСТИКА

ОСОБЛИВОСТІ ПЕРЕКЛАДУ ВЛАСНИХ НАЗВ У ХУДОЖНІЙ ЛІТЕРАТУРІ НА МАТЕРІАЛІ РОМАНУ І. НОЛЛЬ «АПТЕКАРКА» Росоха О.В.	126
---	-----

СЕКЦІЯ XVII. ФІЛОСОФІЯ ТА ПОЛІТОЛОГІЯ

ДІАЛОГ ЯК СПІЛКУВАННЯ: ПСИХОАНАЛІТИЧНИЙ ВИМІР Шморгун О.О.	128
--	-----

СПЕЦИФІКА ПОСТКОМУНІСТИЧНИХ ТРАНСФОРМАЦІЙ ТА ОСОБЛИВОСТІ ДЕМОКРАТИЧНОГО ТРАНЗИТУ В УКРАЇНІ Киристюк В.О.	131
--	-----

СЕКЦІЯ XVIII. ПЕДАГОГІКА ТА ОСВІТА

CREATIVE INITIATIVE AS A COMPONENT OF COGNITIVE ACTIVITY OF FUTURE MUSIC TEACHERS Demidova M.H.	134
---	-----

ESSENTIAL FEATURES OF COMPETENCE Li Naohuan	136
---	-----

METHODOLOGICAL FEATURES OF FORECASTING IN THE PROFESSIONAL ACTIVITY OF A PIANIST-CONCERTMASTER Demidova V.H.	138
--	-----

THE IMPORTANCE OF INTERPERSONAL INTERACTION IN THE MUSICAL ART EDUCATION OF FUTURE TEACHERS Wei Yiqian	140
--	-----

ВИКОРИСТАННЯ ЗАВДАНЬ З ЛОГІЧНИМ НАВАНТАЖЕННЯМ НА УРОКАХ МАТЕМАТИКИ ЯК ЗАСІБ ІНТЕЛЕКТУАЛЬНОГО РОЗВИТКУ ЗДОБУВАЧІВ ПОЧАТКОВОЇ ОСВІТИ Сірант Н.П., Жук Л.В.	142
--	-----

СПІЛЬНИЙ АВТОКОДЕР ІЗ ПОРОГОМ ВИЯВЛЕННЯ АНОМАЛІЇ СУГЛОБА НА ВИРОБНИЧИХ ЛІНІЯХ

Шустрова Анна Євгенівна

здобувач вищої освіти, Факультет інформаційних
радіотехнологій та технічного захисту інформації
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Кузьомін Олександр Якович

доктор технічних наук, професор, професор кафедри інформатики,
Засновник Асоціації випускників ХНУРЕ
Харківський національний університет радіоелектроніки, Україна

***Анотація.** З розвитком технологій Інтернету речей (IoT) розгортається все більше різноманітних пристроїв, які підключаються до Інтернету через шлюзи IoT або локальні маршрутизатори. Враховуючи велику кількість пристроїв у типовому смарт виробничий сценарій, наприклад розумні фабрики, може мати величезну кількість даних генерується в усі часи. Ці дані потрібно автоматично передати в сервер для подальшого аналізу. У передачі даних може бути дуже високий ризик інформаційної безпеки, якщо їх неможливо ефективно захистити. Оскільки вони зазвичай містять критичні знання про виробництво та ноу-хау в галузі промисловості, це ще більше загрожуватиме конкурентоспроможності компанії. Основною проблемою пристроїв IoT є їх відсутність безпеки.*

Виявлення аномалій

Виявлення аномалій – це процес у машинному навчанні, який визначає точки даних, події та спостереження, які відрізняються від нормальної поведінки набору даних. І виявлення аномалій на основі даних часових рядів є критичною проблемою для промислового застосування.[1]

Згідно з опитуванням IDC у квітні 2021 року, обробна промисловість, за якою слідує галузі фінансів, транспорту, зв'язку та комунальних послуг, перебувають на передньому краї використання передового машинного навчання для прогнозованого та рекомендованого технічного обслуговування.

В опитуванні стверджується, що зі зниженням вартості збору даних за допомогою датчиків, а також збільшенням зв'язком між пристроями виявлення аномалій за допомогою машинного навчання буде все більш масовим. Щоб мати ефективну програму прогнозованого технічного обслуговування, надзвичайно важливо мати можливість виявляти аномальну поведінку, щоб можна було вжити заходів, щоб уникнути втрат під час простою.

Однак ідентифікувати аномалії до події збою складно, оскільки, як правило, збої є порівняно рідкісними подіями, тому часто існує дефіцит позначених тегами даних для побудови прогнозних моделей. Спільний автокодер з порогом виявлення аномалії - це алгоритм машинного навчання, який може виявляти аномалії у даних, що створюються на виробничих лініях, де працюють роботи або люди[2].

Автокодер - це нейронна мережа, що здатна згорнути вхідні дані у меншому просторі та згодом розгорнути їх назад до вихідних даних. Ідея полягає в тому, що якщо на виробничій лінії все проходить нормально, то дані, отримані з різних сенсорів на різних робочих станціях, будуть схожими та повинні бути здатні побудувати взаємно-однозначне відображення.

Види виявлення аномалії

Загалом випадки використання виявлення аномалій можна розділити на три типи залежно від типу доступних даних. Контрольоване виявлення аномалій спрямоване на вивчення моделі за допомогою позначених даних, які представляють попередні збої або аномалії. У неконтрольованому режимі дані з мітками не надаються[3].

Третя категорія, напівконтрольоване виявлення аномалій, покладається на невелику кількість позначених даних для перевірки та вибору найкращої моделі, навченої на звичайних даних (або даних без аномалій).

Враховуючи дефіцит позначених даних про несправності, найбільш застосовними випадками використання є неконтрольоване та напівконтрольоване виявлення аномалій.

Виявлення аномалій для даних часових рядів створює свої проблеми через природну складність у відокремленні шуму від аномальної моделі. Для аналізу часових рядів важливо знати, чи є дані стаціонарними, а також враховувати тенденції та сезонність.

Крім того, аномалії можуть бути глобальними викидами (також звані точковими аномаліями) або контекстними аномаліями, що означає, що існує відхилення від набору точок даних у контексті.

Визначення та використання

Автокодер — це особливий тип архітектури глибокого навчання, який використовується для вивчення представлень даних виключно на основі описових функцій. Представлення, яке є перетворенням необроблених даних, вивчається з метою найточнішої реконструкції вихідних даних.

Цю стратегію навчання подання можна використовувати для зменшення розмірності, усунення шумів або навіть генеративних програм[4].

Автокодер можна розділити на дві частини:

- Частина кодера, яка відображає вхідні дані в представлення, також називається «кодом» або «вузьким місцем».
- Декодер, який відображає код у реконструкції вхідних даних.

Кодер і декодер можуть мати складні архітектури, такі як рекурентні нейронні мережі при роботі з послідовними даними або згорткові нейронні мережі при роботі з зображеннями. Але в своїй найпростішій формі це багатосарові нейронні мережі прямого зв'язку.

Розмірність коду, який також є входом декодера, може фіксуватися довільно. Цей розмір, як правило, вибирається нижчим за початковий вхідний розмір, щоб зменшити розмірність і дізнатися базові метазмінні. Розмір виходу декодера такий самий, як і вхід кодера, оскільки його призначення — реконструювати вхід[5].

Архітектура, як правило, навчається наскрізно шляхом оптимізації реконструкції вхідних даних, тобто шляхом мінімізації втрат, які вимірюють різницю між виходом моделі та вхідними даними. Його можна навчити з будь-якими даними без міток. коли автокодер є «глибоким», тобто є проміжні рівні, відповідно між входом і вузьким місцем і між вузьким місцем і виходом, можна навчати шари послідовно, а не одночасно Автокодери можна використовувати як техніку для неконтрольованого або напівконтрольованого виявлення аномалій, що призвело до їх багаторазового використання для виявлення шахрайства з кредитними картками.

Виявлення аномалії

Виявлення шахрайства може здійснюватися як контрольованими, так і неконтрольованими методами, оскільки це особливий випадок ширшої проблеми,

яка називається виявленням аномалій або виявленням викидів.

Останній, як правило, включає методи ідентифікації елементів, які є рідкісними або значно відрізняються від «нормальної» поведінки, спостережуваної в більшості даних і можна легко зрозуміти, як шахрайство з кредитною картою можна визначити як аномалію в транзакціях[6].

Ці аномалії можуть бути рідкісними подіями чи неочікуваними сплесками активності поведінки одного власника картки, або специфічними моделями, не обов'язково рідкісними, у поведінці глобальних споживачів.

Рідкісні події або викиди можна виявити за допомогою неконтрольованих методів, які вивчають нормальність і здатні оцінити невідповідність цій нормі. Але для виявлення інших типів аномалій можуть знадобитися методи під наглядом і належне навчання.

Таким чином, можна виділити три типи методів виявлення аномалій:

- Техніки під керівництвом, які були широко розглянуті в попередніх розділах і розділах. Ці методи вимагають анотацій даних, які складаються з двох класів, «нормальних» (або «справжніх») і «ненормальних» (або «шахрайських»), і вони навчаються розрізняти ці класи.

- Неконтрольовані методи, спрямовані на виявлення аномалій шляхом моделювання поведінки більшості та розглядання її як «нормальної». Потім вони виявляють «ненормальну» або шахрайську поведінку, шукаючи приклади, які не відповідають нормальній поведінці.

- Напівконтрольовані методи, які є проміжними між двома вищезазначеними випадками та які можуть вивчати як немарковані, так і позначені дані для виявлення шахрайських транзакцій.

Автокодер можна використовувати для моделювання нормальної поведінки даних і виявлення викидів, використовуючи помилку реконструкції як індикатор. Зокрема, один із способів зробити це — навчити його глобально реконструювати транзакції в наборі даних. Звичайна тенденція, яка спостерігається в більшості транзакцій, буде краще наближена, ніж рідкісні події[7].

Тому помилка реконструкції «нормальних» даних буде нижчою, ніж помилка реконструкції викидів. Таким чином, автокодер можна розглядати як неконтрольовану техніку для виявлення шахрайства.

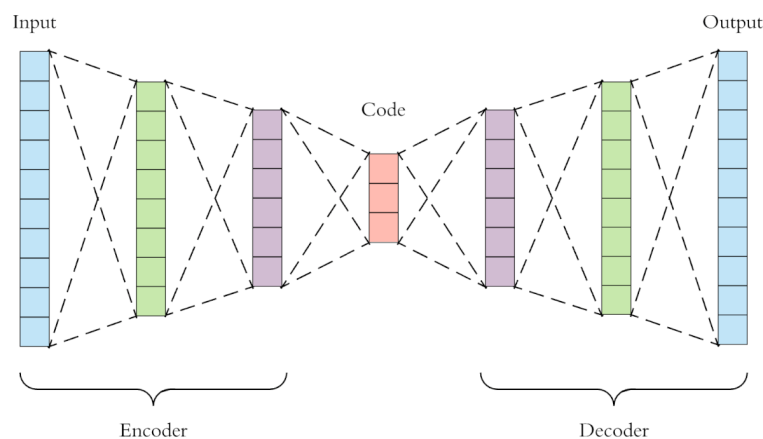


Рис. 1. Encoder and decoder

Різні типи аномалій у виявленні аномалій

Не всі аномалії однакові. Насправді їх можна розділити на три великі категорії:

- Точкові аномалії

Точкова аномалія – це те, що одна точка даних виділяється з очікуваного шаблону, діапазону або норми. Іншими словами, точка даних є неочікуваною: витрати кредитної картки як приклад[2].

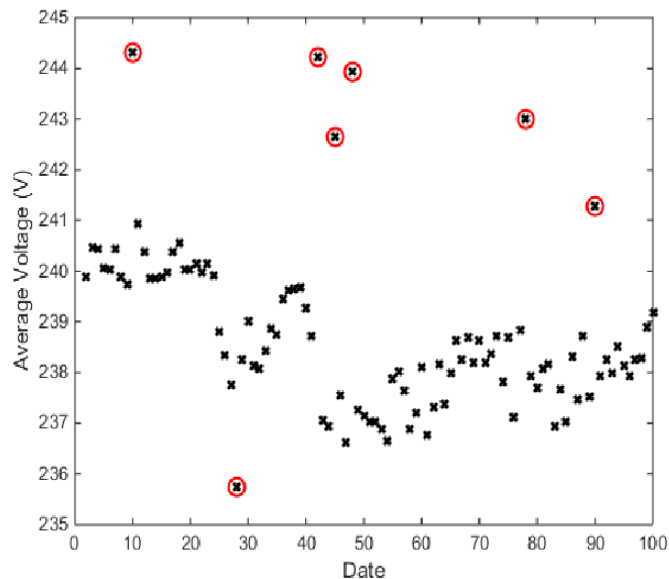


Рис. 2. Точкова аномалія

Точковою аномалією було б одноразове, велике та незвичайне витрачання на кредитну картку. Наприклад, звичайні витрати на кредитну картку можуть складати невеликі та середні суми, як правило, у межах однієї географічної області та зазвичай для придбання подібної групи продуктів.

Точковою аномалією було б, якби ця кредитна картка потім була використана для одноразової покупки великої вартості товару, який раніше не купувався та був придбаний у місці, де кредитна картка раніше не використовувалася[5]. Ця точкова аномалія може вказувати на шахрайство.

- Колективні аномалії

Колективна аномалія виникає, коли окремі точки даних, розглянуті окремо, виглядають нормально. Однак, коли ви дивитесь на групу цих точок даних, стають очевидними несподівані моделі, поведінка або результати.

Ці несподівані випадки можуть бути, наприклад, подіями, що відбуваються в порядку або в неочікуваній комбінації.

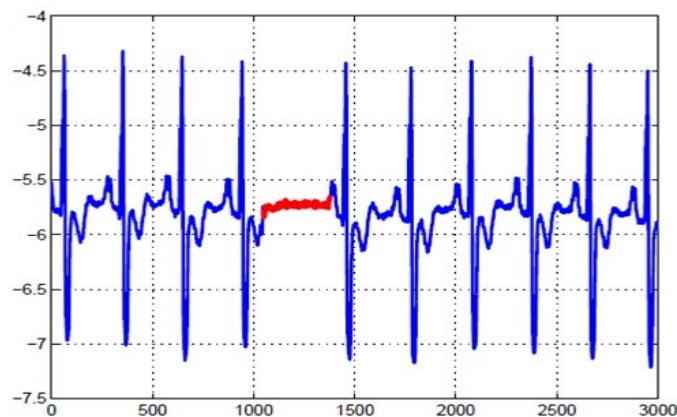


Рис. 3. Колективна аномалія

Ми можемо знову використати потенційне шахрайство з кредитними картками як наш приклад. Це може статися, якщо кілька покупок, здавалося б, відповідають нормальній витратній діяльності, якщо дивитися окремо. Однак, коли розглядати ці покупки як групу, можуть виявитися незвичайні моделі та поведінка.

- Контекстуальні аномалії

Замість того, щоб розглядати конкретні точки даних або групи даних, алгоритм, який шукає контекстуальні аномалії, буде зацікавлений у несподіваних результатах, які походять від того, що здається нормальною діяльністю. Хорошим прикладом у цьому випадку є спроба вторгнення в мережу.

Алгоритм, який шукає контекстуальні аномалії, матиме базову лінію активності, яка надає йому нормальні параметри. Це може, наприклад, показати очікуваний рівень трафіку, що отримує доступ до мережі в різний час доби. Трафік може бути найменшим рано вранці. Таким чином, сплеск трафіку о 3 годині ночі є контекстною аномалією, яка вимагає подальших дій та/або розслідування, оскільки це може вказувати на спробу вторгнення в мережу[7].

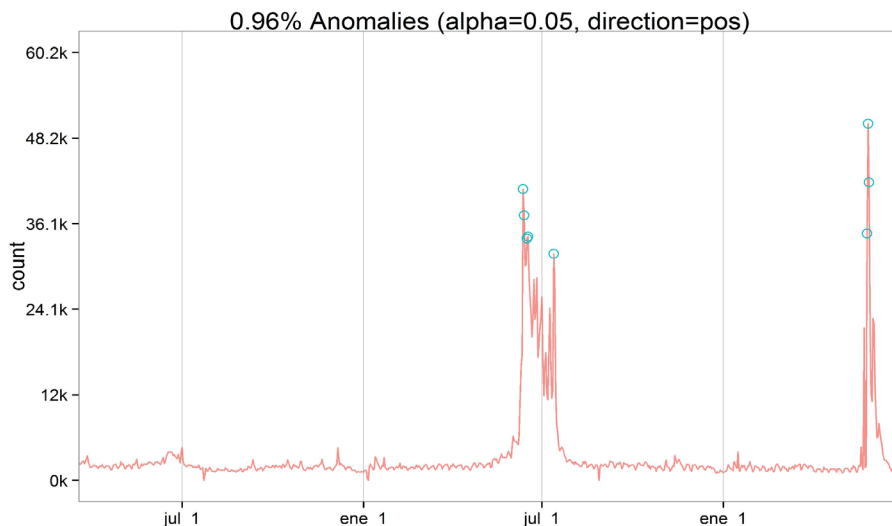


Рис. 4. Аномалія

Іншими словами, доступ до мережі сам по собі був цілком нормальною подією. Однак мати такий високий рівень трафіку о третій годині ранку було незвично; це була аномалія. Точкова аномалія – це те, що одна точка даних виділяється з очікуваного шаблону, діапазону або норми. Іншими словами, точка даних є неочікуваною.

Висновок

Отже, спільний автокодер із порогом виявлення аномалії може бути корисним інструментом для виявлення проблем зі суглобами на виробничих лініях. Ця технологія може виявляти аномальні дані та попереджати про можливі проблеми зі здоров'ям робочих на лінії. Важливо пам'ятати, що ця технологія повинна бути використовувана разом з іншими методами та процедурами безпеки на виробництві, щоб забезпечити максимальну безпеку та захист здоров'я робочих.

Список використаних джерел:

1. Keras: the Python deep learning API.
2. Anomaly Detection In Temporal Data Mining /by Mehmet Yavuz Onat.

3. Network Anomaly Detection A Machine Learning Perspective By Dhruba Kumar Bhattacharyya, Jugal Kalita.
4. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction by Ashfaqr Rahman,Jeremiah Deng, Jiuyong Li.
5. Time-based Anomaly Detection using Autoencode by Mohammad A. Salahuddin; Md. Faizul Bari; Hyame Assem Alameddine; Vahid Pourahmadi
6. Using Autoencoders for Anomaly Detection and Transfer Learning in IoT by Chin-Wei Tien 1,Tse-Yung Huang 1,Ping-Chun Chen 1 andJenq-Haur Wang.
7. Anomaly Detection with Robust Deep Autoencoders by Chong Zhou Randy C. Paffenroth.