DOI: https://doi.org/10.26642/ten-2025-1(95)-325-331
УДК 004.8:519.23

Д.В. Фуріхата, аспірант, ст. викладач
Т.А. Вакалюк, д.пед.н., проф.
Державний університет «Житомирська політехніка»

Теоретичні підходи до виявлення аномалій у показах лічильників у науковій літературі

Стаття присвячена дослідженню сучасних наукових підходів до виявлення аномалій у показах лічильників у контексті розвитку інтелектуальних енергетичних мереж. Актуальність дослідження зумовлена зростаючою потребою в ефективному моніторингу споживання електроенергії, особливо в умовах воєнного стану в Україні, коли енергосистема перебуває під постійними загрозами та потребує максимально ефективного управління ресурсами.

У роботі проведено комплексний аналіз існуючих методів виявлення аномалій, які класифіковано на три основні категорії: точкові аномалії, що представляють окремі відхилення від типового патерна споживання; контекстуальні аномалії, які залежать від конкретного часового або просторового оточення; та колективні аномалії, що виникають у групах взаємопов'язаних даних.

Дослідження демонструє переваги децентралізованих підходів до обробки даних, зокрема використання технологій edge computing та fog computing, які дозволяють здійснювати аналіз інформації безпосередньо на пристроях обліку або в їх безпосередній близькості. Порівняльний аналіз централізованих та децентралізованих методів показує, що гібридні системи, які поєднують переваги обох підходів, демонструють найкращі результати у практичних застосуваннях.

Особливу увагу приділено аналізу ефективності різних алгоритмів машинного навчання для виявлення аномалій. Розглянуто статистичні методи, які базуються на ймовірнісних моделях та дозволяють відносно точно визначати межі нормальності за умови достатньої кількості історичних даних. Проаналізовано класифікаційні методи контрольованого навчання, що потребують попередньо маркованих даних для навчання моделей, але забезпечують високу точність виявлення відомих типів аномалій.

Розглянуто перспективи подальшого розвитку технологій виявлення аномалій у контексті інтеграції з IoT-пристроями, розвитку технологій та впровадження більш складних алгоритмів глибокого навчання.

Ключові слова: *виявлення аномалій; лічильники; машинне навчання; edge computing; децентралізована обробка даних; статистичний аналіз; IoT.*

Актуальність теми. Виявлення аномалій у показах лічильників відіграє ключову роль як для користувачів, так і для постачальників електроенергії. З одного боку, користувачі зацікавлені в коректності зчитаних даних, тому відстеження ймовірних відхилень допомагає виявити помилки зчитування або некоректну обробку показів. З іншого боку, для постачальників будь-яка аномалія може стати сигналом про потенційні проблеми – як технічного, так і нетехнічного характеру, що вимагає додаткової уваги до конкретного споживача або групи споживачів. Виявлені у показах відхилення можуть бути зумовлені технічними або нетехнічними чинниками. До технічних чинників належать збої приладів обліку, похибки при передачі даних і несправності програмного забезпечення, яке обробляє інформацію з лічильників [9]. Нетехнічні чинники здебільшого пов'язані з людським фактором: від помилок під час ручного внесення показів до цілеспрямованого втручання в роботу лічильників. Основною проблемою, що потребує постійного контролю з боку постачальників, є крадіжки: лічильники попередніх поколінь могли бути модифіковані фізично, а сучасні можна зламувати програмно [20, 3]. Такі дії спричиняють суттєві втрати [23, 3] і, водночас, підвищують вартість надання послуг для населення. Крім безпосередніх фінансових збитків, втручання в роботу лічильників ускладнює аналітику й планування побудови смарт-систем і автоматичного управління енергомережами [22]. Також у сучасних реаліях війни, коли енергосистема України перебуває під обстрілами, це ще більше ускладнює роботу енергодиспетчерів у питаннях регулювання відключень.

Аналіз останніх досліджень та публікації, на які спираються автори. Поняття «аномалій у споживанні енергії» доволі широке, оскільки різні типи відхилень вирізняються своєю природою та причинами, відповідно вимагаючи специфічних методів виявлення. Автор [20] дослідив поняття «аномальних відхилень» у контексті великих обсягів даних і запропонував методи їх попередньої фільтрації на ранніх етапах аналізу. Основний акцент у численних роботах приділено теоретичним основам і практичним аспектам обробки великих обсягів даних, зокрема даних смарт-лічильників.

Так [23] зазначають, що через зростаючу кількість підключених пристроїв (Internet of Things) фахівці змушені розробляти високопродуктивні алгоритми.

Використання методів машинного навчання різної складності (від класичних статистичних алгоритмів до глибинних нейронних мереж) докладно висвітлено в роботах [9, 2, 13]. У цих джерелах підкреслено важливість адаптивності моделей та їхньої здатності справлятися з динамічними змінами профілю споживання.

Згідно з [21], специфіка енергетичних даних полягає у частій наявності нетипових стрибків споживання, викликаних або сезонними чинниками, або діями користувачів.

Застосування класифікації аномалій на точкові, контекстуальні та колективні дозволяє більш точно ідентифікувати проблемні випадки [14, 18]. Аналогічний підхід відображено й у праці [15], де пропонується обробляти часові ряди за допомогою методів статистичного аналізу й технік глибинного навчання задля підвищення надійності виявлення колективних аномальних патернів.

Згідно з [23], окремі алгоритми можуть по-різному реагувати на різні типи аномалій, тому комбіновані (гібридні) системи виявлення часто дають кращі результати, ніж використання одного методу. Автор [22] наголошує, що реалізація цих підходів вимагає надійних апаратно-програмних платформ, здатних масштабуватися під високі навантаження.

Саме тому в сучасних дослідженнях з'являються пропозиції інтегрувати обчислення в хмару [9, 3] або на «край» мережі (edge/fog computing) [8]. Це підтверджується у [18], де доведено, що обробка даних ближче до джерела суттєво знижує затримки й навантаження на центральні вузли та підвищує швидкість реагування на аномалії. Згідно з дослідженням [19], децентралізоване середовище покращує захист від втрат, зокрема коли йдеться про раннє виявлення крадіжок електроенергії на рівні локальних вузлів.

Метою статті є дослідження наукових підходів до виявлення аномалій у показах лічильників.

Викладення основного матеріалу.

Поняття аномальної поведінки у споживанні та їх види

У дослідженні [22] дається таке визначення аномалії як суттєвого відхилення від характерного патерна, що може свідчити про нетипове споживання або несправності вимірювального обладнання. Згідно з [23], раннє виявлення таких відхилень є критично важливим для забезпечення надійної роботи інтелектуальних електромереж (Smart Grid), а також для запобігання фінансовим втратам, пов'язаним із крадіжками електроенергії. Аномалією також вважається суттєве відхилення від нормального патерна чи історичного профілю споживання [20].

У даному дослідженні під аномалією розуміємо суттєве відхилення від нормального патерна або історичного профілю енергоспоживання, що може сигналізувати про можливі технічні збої чи нетехнічні втрати.

При дослідженні такого явища як аномалії зазвичай [11] ділять аномалії на 3 групи, які візуалізовано схемою на рисунку 1.

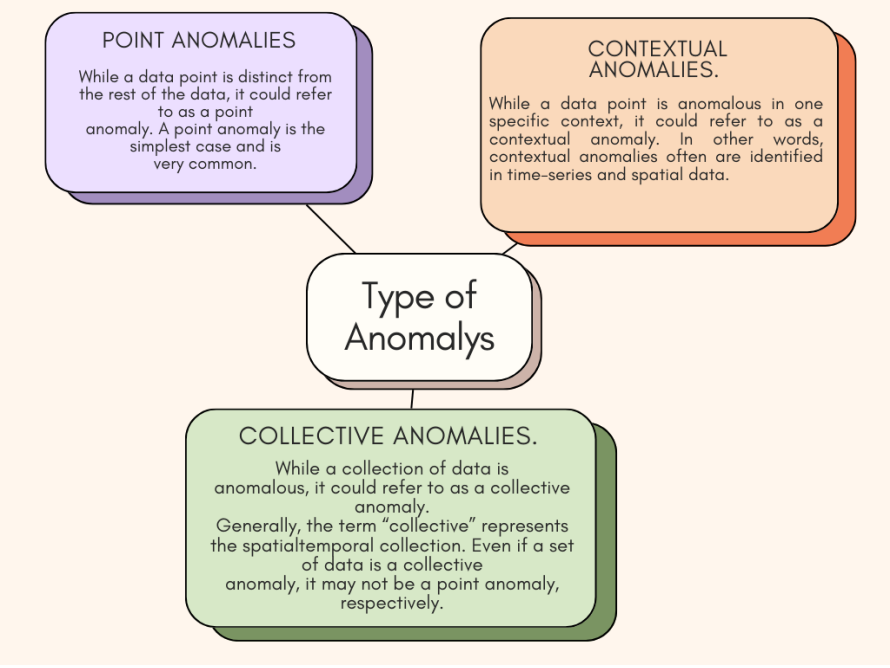

Рис. 1. Групи аномалій

Точкова аномалія – відхилення окремого значення за межі очікуваного діапазону та невідповідність типовим патернам споживання [6]. Такі аномалії легко помітити, оскільки вони відрізняються від прогнозованої поведінки; відповідно, для їх виявлення зазвичай використовуються прості статистичні методи, порівнюючи дані з прогнозованими значеннями.

Контекстуальні аномалії залежать від певного оточення чи часу доби. Наприклад, значення, яке в ранковий період вважається адекватним, увечері або в нічний час може бути підозрілим, особливо коли йдеться про житловий сектор чи інші об'єкти з чітко вираженим профілем споживання [20, 9].

Колективні аномалії виникають, коли ціла група даних або період спостережень показують поведінку, що не відповідає нормі. Хоча окремі значення можуть здаватися звичайними, у сукупності вони формують відхилення від типової поведінки. Такі аномалії часто зустрічаються в часових рядах, наприклад, у даних електролічильників за тиждень або місяць. Раптове зростання чи зниження споживання у певному районі без очевидних причин може свідчити про технічні несправності, зміну звичок споживачів чи несанкціоноване використання [11]. Виявлення таких аномалій стає можливим завдяки аналізу даних із різних джерел. Наприклад, порівняння показів смарт-лічильників у різних районах дозволяє побачити загальну аномальну тенденцію, навіть якщо окремі покази виглядають нормальними [2, 7, 11].

Використання хмарних обчислень у «розумних» електромережах

Застосування хмарних обчислень (Cloud Computing) у «розумних» електромережах відкриває широкі можливості для обробки, аналізу та зберігання великих обсягів даних, які генеруються смарт-лічильниками та іншими сенсорами мережі [18]. Смарт-лічильники постійно фіксують показники споживання електроенергії, передаючи їх у централізовані системи для подальшого аналізу.

Традиційні підходи до обробки таких даних часто стикаються з обмеженнями продуктивності та масштабованості, що ускладнює виявлення аномалій, особливо у випадках нетехнічних втрат, таких як крадіжки електроенергії чи маніпуляції з лічильниками. Хмарні платформи надають можливість масштабованої обробки даних, дозволяючи аналізувати споживання енергії в режимі реального часу [18]. Це особливо важливо, коли застосовуються складні методи машинного навчання та глибокі нейронні мережі для класифікації та виявлення аномальних шаблонів споживання [22]. Використання хмарних рішень забезпечує гнучкість та можливість збільшення обчислювальних ресурсів у разі необхідності обробки великого масиву даних [21]. Завдяки централізованому управлінню та аналізу зменшується навантаження на локальні сервери електромережі, що підвищує ефективність роботи всієї системи [8]. Безперервний моніторинг і постійне оновлення алгоритмів дозволяє адаптувати моделі до нових патернів споживання, що сприяє ранньому виявленню шахрайства та інших аномальних ситуацій [7]. Крім того, сучасні хмарні архітектури підтримують інтеграцію з іншими технологіями, такими як Edge Computing, що дає змогу виконувати попередню обробку даних безпосередньо на пристроях і лише узагальнені результати надсилати у хмару для більш глибокого аналізу [5].

Децентралізовані методи виявлення аномалій споживання електроенергії в основному авторами базуються на використанні edge та cloud обчислень, у тому числі й розподіленій обробці даних. Їх головна перевага полягає у можливості аналізувати дані в реальному часі безпосередньо на пристроях обліку електроенергії, так званих edge device [18].

В основі цього підходу лежить встановлення розумних лічильників (smart meter or smart device) у кожному домогосподарстві, які здійснюють первинний аналіз даних. Використання edge computing технологій дозволяє суттєво зменшити затримки та підвищити ефективність обробки даних порівняно з традиційними хмарними рішеннями.

Система використовує гібридні предиктори споживання, які поєднують прогнозування на один крок вперед із правило-орієнтованими детекторами аномалій. Для зменшення проблем перенавчання застосовуються байєсівські критерії. Важливим компонентом є напівконтрольовані згорткові нейронні мережі, які складаються з двох підмереж – одна займається реконструкцією даних з немаркованих прикладів, а інша відповідає за класифікацію маркованих даних.

Практичне впровадження цих методів продемонструвало високу ефективність у реальних умовах. Зокрема, успішний досвід використання має найбільша електроенергетична компанія Іспанії Endesa, де ця технологія допомагає ефективно виявляти нетехнічні втрати та аномалії у споживанні електроенергії.

Підходи до виявлення аномалій

Підходи до виявлення аномалій можна поділити за кількома критеріями, такими як типи алгоритмів та наявність міток у даних. Згідно з аналізом наукової літератури, статистичні методи виявлення аномалій, зокрема методи ймовірнісних моделей, дозволяють побудувати математичні моделі, що припускають певний розподіл нормальних і аномальних даних.

У контексті виявлення аномалій у споживанні електроенергії активно досліджуються та впроваджуються різні фреймворки, зокрема централізовані (Big Data-аналіз у хмарі) та децентралізовані (edge/fog computing). Загальна мета полягає в ідентифікації крадіжок або несправностей через нетипові патерни споживання. З огляду на складність аналізу великих обсягів даних та необхідність оперативного

реагування на аномальні ситуації, фахівці розглядають можливість використання різноманітних обчислювальних платформ, що дозволяють ефективно обробляти інформацію у реальному часі [12]. Методи аналізу базуються на зборі великих обсягів даних від смарт-лічильників, їхньому очищенні, попередній обробці та класифікації за допомогою алгоритмів машинного навчання [19]. Централізовані підходи використовують потужності хмарних обчислень для аналізу загальних тенденцій, тоді як децентралізовані дозволяють здійснювати обробку ближче до місця генерації даних, що підвищує швидкість виявлення аномалій [12]. Розвиток технологій IoT сприяє інтеграції в системи розумних мереж, що дозволяє більш точно контролювати споживання та прогнозувати потенційні загрози [19].

Загалом підходи до виявлення аномалій можна розділити за типами алгоритмів та доступністю міток у даних [18] (рис. 2):

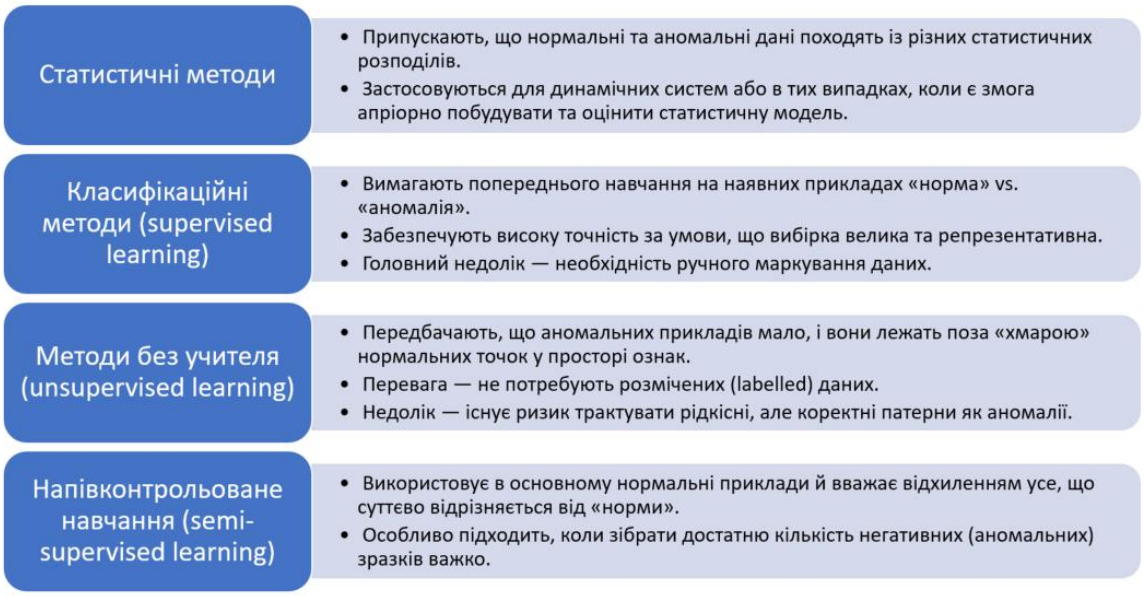

Рис. 2. Методи виявлення аномалій

Підходи до виявлення аномалій поділяються залежно від методів аналізу даних та доступності міток.

Наприклад, ймовірнісні моделі, згідно з Тейлором, дозволяють відносно точно визначати межі нормальності, якщо зібрані достатні дані про середовище [4]. Ці моделі використовуються переважно для обробки даних динамічних систем або для випадків, коли є можливість побудувати апріорну статистичну модель без наявності явних міток.

Статистичні методи використовують ймовірнісні моделі, що дозволяють оцінювати розподіл нормальних та аномальних споживань [11]. Вони ефективні для аналізу динамічних систем, де можливо апріорно оцінити статистичні характеристики процесу [1]. Ці методи особливо корисні у випадках, коли історичні дані містять достатню кількість прикладів аномальних ситуацій, що дозволяє моделювати їхні розподіли та прогнозувати подальші події.

Класифікаційні методи (supervised learning) базуються на попередньому навчанні моделей на позначених наборах даних, що містять нормальні та аномальні зразки [12]. Вони мають високу точність за умови великої та репрезентативної вибірки, проте їхнім недоліком є необхідність попереднього маркування даних [7]. Використання таких методів можливе у поєднанні з автоматизованими підходами маркування, що базуються на синтетичному створенні аномальних даних або використанні експертних систем [2].

Методи без учителя (unsupervised learning) передбачають, що аномальні спостереження відрізняються від основної маси даних за певними характеристиками [6]. Такі підходи корисні у випадках, коли немає розмічених даних, проте можуть призводити до помилкового розпізнавання рідкісних, але нормальних патернів як аномалій [10]. До таких методів належать алгоритми кластеризації, аналізу щільності даних та автоматичного визначення відхилень від загальних тенденцій [17].

Напівконтрольоване навчання (semi-supervised learning) поєднує переваги контрольованого та неконтрольованого навчання [16]. Воно використовує здебільшого нормальні зразки та виявляє відхилення від цих норм, що є ефективним підходом у випадках, коли аномальні дані рідкісні та важкодоступні [13]. Такий підхід дозволяє адаптивно змінювати модель залежно від поточних змін у даних, що робить його особливо корисним для роботи у режимі реального часу.

У [14] доводять, що підхід без націнки підходить для виявлення аномалій у випадках, коли такі аномалії не зустрічаються часто, навіть серед нормальних випадків. Він дозволяє здійснювати виявлення, коли аномалій дуже мало і вони істотно відрізняються від нормальних даних. Проте серед недоліків таких методів можна виділити деякий ризик ідентифікації нормальних точок як аномальних, особливо в контексті малопредставлених даних.

Висновки та перспективи подальших досліджень. Проведене дослідження показало, що аномалії у споживанні електроенергії можна класифікувати на три основні групи. Точкові аномалії представляють собою окремі відхилення від типового патерна споживання, контекстуальні аномалії залежать від певного оточення чи часу доби, а колективні аномалії виникають, коли ціла група даних показує відхилення від норми. Така класифікація дозволяє більш точно ідентифікувати проблемні випадки та обирати відповідні методи їх виявлення.

Використання edge computing та децентралізованих методів обробки даних демонструє значні переваги порівняно з традиційними централізованими підходами. Зокрема, спостерігається суттєве зменшення затримок у передачі даних, підвищення швидкості виявлення аномалій, можливість аналізу даних безпосередньо на пристроях обліку та зменшення навантаження на центральні вузли. Це особливо важливо в умовах реального часу, коли швидкість реагування на аномальні ситуації може критично впливати на стабільність енергосистеми.

Комбінування різних алгоритмів машинного навчання, включаючи статистичні методи, класифікаційні підходи та інші, показує кращі результати порівняно з використанням окремих методів. Гібридні системи забезпечують вищу точність виявлення аномалій, кращу адаптивність до нових патернів споживання та зменшення кількості хибних спрацьовувань. Це підтверджує доцільність використання комплексного підходу при розробці систем моніторингу.

Подальший розвиток технологій виявлення аномалій пов'язаний з інтеграцією з IoT-пристроями та smart-grid технологіями, використанням більш складних алгоритмів глибокого навчання, розробкою адаптивних систем, здатних самостійно навчатися на нових даних, та впровадженням хмарних і edge-обчислень для забезпечення масштабованості рішень. Водночас існують певні виклики та обмеження, які потребують уваги при практичному впровадженні. Основними з них є необхідність великих обсягів якісних даних для навчання моделей, складність налаштування параметрів для різних типів споживачів, потреба в постійному оновленні алгоритмів через зміни у патернах споживання та забезпечення кібербезпеки децентралізованих систем.

Список використаної літератури:

1. Natural Gas Consumption Forecasting for Anomaly Detection / *L.Baldacci, M.Golfarelli, D.Lombardi, F.Sami* // Expert Systems with Applications. – 2016. – № 62. DOI: 10.1016/j.eswa.2016.06.013.
2. *Banad C.* Electricity Consumption Anomaly Detection Model Using Deep Learning / *C.Banad*. – 2019 [Electronic resource]. – Access mode : http://norma.ncirl.ie/3848/.
3. Amplified locality-sensitive hashing-based recommender systems with privacy protection / *X.Chi, C.Yan, H.Wang and other* // Concurrency Computat Pract Exper. – 2022. – № 34. DOI: 10.1002/cpe.5681.
4. Real-Time Anomaly Detection in Data Centers for Log-based Predictive Maintenance using an Evolving Fuzzy-Rule-Based Approach / *L.Decker, D.Leite, L.Giommi, D.Bonacorsi*. – 2020. DOI: 10.48550/arXiv.2004.13527.
5. Survey on Smart Grid Potential Applications and Communication Requirements / *V.Gungor, D.Sahin, T.Kocak and other* // Industrial Informatics, IEEE Transactions on. – 2013. – № 9. – P. 28–42. DOI: 10.1109/TII.2012.2218253.
6. *Hodge V.* A Survey of Outlier Detection Methodologies / *V.Hodge, J.Austin* // Artificial Intelligence Review. – 2004. – № 22. – P. 85–126. DOI: 10.1023/B:AIRE.0000045502.10941.a9.
7. *Jokar P.* Electricity Theft Detection in AMI Using Customers' Consumption Patterns / *P.Jokar, N.Arianpoo* // IEEE Transactions on Smart Grid. – 2015. – № 7. – P. 1–1. DOI: 10.1109/TSG.2015.2425222.
8. *Kabalci Y.* A survey on smart metering and smart grid communication / *Y.Kabalci* // Renewable and Sustainable Energy Reviews. – 2016. – Vol. 57. – P. 302–318. DOI: 10.1016/j.rser.2015.12.114.
9. *Карпа Д.М.* Нейромережеві засоби прогнозування споживання енергоресурсів / *Д.М. Карпа, І.Г. Цмоць, Ю.В. Опотяк* // Scientific Bulletin of UNFU. – 2018. – № 28. – С. 140–146. DOI: 10.15421/40280529.
10. Distributed Online One-Class Support Vector Machine for Anomaly Detection Over Networks / X.Miao, Y.Liu, H.Zhao, Ch.Li // IEEE Transactions on Cybernetics. – 2018. – P. 1–14. DOI: 10.1109/TCYB.2018.2804940.
11. *Moghaddass R.* A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data / *R.Moghaddass, J.Wang* // IEEE Transactions on Smart Grid. – 2017. – P. 1–1. DOI: 10.1109/TSG.2017.2697440.
12. Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines / *J.Nagi, K.Yap, S.Tiong and other* // Power Delivery, IEEE Transactions on. – 2010. – № 25. – P. 1162–1171. DOI: 10.1109/TPWRD.2009.2030890.
13. Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes / *M.Sabokrou, M.Fayyaz, M.Fathy and other* // Computer Vision and Image Understanding. – 2018. – № 172. DOI: 10.1016/j.cviu.2018.02.006.

14. Survey of Security Advances in Smart Grid: A Data Driven Approach / *S.Tan, D.De, W.-Z.Song and other* // IEEE Communications Surveys & Tutorials. – 2017. – Vol. 19. – № 1. – P. 397–422. DOI: 10.1109/COMST.2016.2616442.
15. *Tuballa M.L.* A review of the development of Smart Grid technologies / *M.L. Tuballa, M.L. Abundo* // Renewable and Sustainable Energy Reviews. – 2016. – Vol. 59. – P. 710–725. DOI: 10.1016/j.rser.2016.01.011.
16. Anomaly-Based Intrusion Detection System Using Support Vector Machine / *P.Vigneshwar, S.Kishore, J.Balasundaram, S.Sivamohan*. – 2020. DOI: 10.1007/978-981-15-0199-9_62.
17. *Wazid M.* An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks / *M.Wazid, A.K. Das* // Wireless Personal Communications. – 2016. – № 90. DOI: 10.1007/s11277-016-3433-3.
18. Dynamic Resource Provisioning With Fault Tolerance for Data-Intensive Meteorological Workflows in Cloud / *X.Xu, R.Mo, . Dai, W.Lin and other //* IEEE Transactions on Industrial Informatics. – 2019. DOI: 10.1109/TII.2019.2959258.
19. An anomaly detection framework for identifying energy theft and defective meters in smart grids / *S.C. Yip, Wooi-Nee Tan, Ch.Kwang Tan and other* // International Journal of Electrical Power & Energy Systems. – 2018. – № 101. – P. 189–203. DOI: 10.1016/j.ijepes.2018.03.025.
20. Аналіз методів виявлення аномалій у даних про споживання електроенергії / *М.Р. Братищенко, Т.В. Філімончук, Г.В. Майстренко, В.І. Сітніков* // Системи управління, навігації та зв'язку. – 2024. – № 1. – С. 45–49. DOI: 10.26906/SUNZ.2024.1.045.
21. *Вишневський О.* Machine Learning Methods to Increase the Energy Efficiency of Buildings / *О.Вишневський, Л.Журавчак* // SISN. – 2023. – Vol. 14. – С. 189–209. DOI: 10.23939/sisn2023.14.189.
22. *Цюцюра М.* Оцінка алгоритмів виявлення аномалій за допомогою методів машинного навчання / *М.Цюцюра, А.Коваленко* // Управління розвитком складних систем. – 2024. – № 58. – С. 80–85. DOI: 10.32347/2412-9933.2024.58.80-85.
23. *Яковець В.* Розробка методів виявлення аномалій у веб-додатках із використанням інтелектуального аналізу даних / *В.Яковець* // Наукові нотатки. – 2025. – № 1. – С. 86–92. DOI: 10.36910/775.24153966.2024.79.12.

References:

1. Baldacci, L., Golfarelli, M., Lombardi, D. and Sami, F. (2016), «Natural Gas Consumption Forecasting for Anomaly Detection», *Expert Systems with Applications*, No. 62, doi: 10.1016/j.eswa.2016.06.013.
2. Banad, C. (2019), «Electricity Consumption Anomaly Detection Model Using Deep Learning», [Online], available at: http://norma.ncirl.ie/3848/
3. Chi, X., Yan, C., Wang, H. et al. (2022), «Amplified locality-sensitive hashing-based recommender systems with privacy protection», *Concurrency Computat Pract Exper*, No. 34, doi: doi.org/10.1002/cpe.5681.
4. Decker, L., Leite, D., Giommi, L. and Bonacorsi, D. (2020), «Real-Time Anomaly Detection in Data Centers for Log-based Predictive Maintenance using an Evolving Fuzzy-Rule-Based Approach», doi: 10.48550/arXiv.2004.13527.
5. *Gungor, V., Sahin, D., Kocak, T.*et al. (2013), «A Survey on Smart Grid Potential Applications and Communication Requirements», *Industrial Informatics, IEEE Transactions on*, No. 9, pp. 28–42, doi: 10.1109/TII.2012.2218253.
6. Hodge, V. and Austin, J. (2004), «A Survey of Outlier Detection Methodologies», *Artificial Intelligence Review*, No. 22, pp. 85–126, doi: 10.1023/B:AIRE.0000045502.10941.a9.
7. Jokar, P. and Arianpoo, N. (2015), «Electricity Theft Detection in AMI Using Customers' Consumption Patterns», *IEEE Transactions on Smart Grid*, No. 7, pp. 1–1, doi: 10.1109/TSG.2015.2425222.
8. Kabalci, Y. (2016), «A survey on smart metering and smart grid communication», *Renewable and Sustainable Energy Reviews*, Vol. 57, pp. 302–318, doi: 10.1016/j.rser.2015.12.114.
9. Karpa, D.M., Tsmots, I.H. and Opotyak, Y.V. (2018), «Neiromerezhevi zasoby prohnozuvannia spozhyvannia enerhoresursiv», *Scientific Bulletin of UNFU*, No. 28, pp. 140–146, doi: 10.15421/40280529.
10. Miao, X., Liu, Y., Zhao, H. and Li, Ch. (2018), «Distributed Online One-Class Support Vector Machine for Anomaly Detection Over Networks», *IEEE Transactions on Cybernetics*, pp. 1–14, doi: 10.1109/TCYB.2018.2804940.
11. Moghaddass, R. and Wang, J. (2017), «A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data», *IEEE Transactions on Smart Grid*, pp. 1–1, doi: 10.1109/TSG.2017.2697440.
12. Nagi, J., Yap, K., Tiong, S. et al. (2010), «Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines», *Power Delivery, IEEE Transactions on*, No. 25, pp. 1162–1171, doi: 10.1109/TPWRD.2009.2030890.
13. Sabokrou, M., Fayyaz, M., Fathy, M. et al. (2018), «Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes», *Computer Vision and Image Understanding*, No. 172, doi: 10.1016/j.cviu.2018.02.006.
14. Tan, S., De, D., Song, W.-Z., et al. (2017), «Survey of Security Advances in Smart Grid: A Data Driven Approach», *IEEE Communications Surveys & Tutorials*, Vol. 19, No. 1, pp. 397–422, doi: 10.1109/COMST.2016.2616442.
15. Tuballa, M.L. and Abundo, M.L. (2016), «A review of the development of Smart Grid technologies», *Renewable and Sustainable Energy Reviews*, Vol. 59, pp. 710–725, doi: 10.1016/j.rser.2016.01.011.
16. Vigneshwar, P., Kishore, S., Balasundaram, J. and Sivamohan, S. (2020), «Anomaly-Based Intrusion Detection System Using Support Vector Machine», doi: 10.1007/978-981-15-0199-9_62.
17. Wazid, M. and Das, A.K. (2016), «An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks», *Wireless Personal Communications*, No. 90, doi: 10.1007/s11277-016-3433-3.

18. Xu, X., Mo, R., Dai, F., et al. (2019), «Dynamic Resource Provisioning With Fault Tolerance for Data-Intensive Meteorological Workflows in Cloud», *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2019.2959258.
19. Yip, S.C., Tan, Wooi-Nee, Tan, Ch.Kwang et al. (2018), «An anomaly detection framework for identifying energy theft and defective meters in smart grids», *International Journal of Electrical Power & Energy Systems*, No. 101, pp. 189–203, doi: 10.1016/j.ijepes.2018.03.025.
20. Bratyshchenko, M.R., Filimonchuk, T.V., Maistrenko, H.V. and Sitnikov, V.I. (2024), «Analiz metodiv vyiavlennia anomalii u danykh pro spozhyvannia elektroenerhii», *Systemy upravlinnia, navihatsii ta zviazku*, 2024, No. 1, pp. 45–49, doi: 10.26906/SUNZ.2024.1.045.
21. Vyshnevskyi, O. and Zhuravchak, L. (2023), «Machine Learning Methods to Increase the Energy Efficiency of Buildings», *SISN*, Vol. 14, pp. 189–209, doi: 10.23939/sisn2023.14.189.
22. Tsiutsiura, M. and Kovalenko, A. (2024), «Otsinka alhorytmiv vyiavlennia anomalii za dopomohoiu metodiv mashynnoho navchannia», *Upravlinnia rozvytkom skladnykh system*, No. 58, pp. 80–85, doi: 10.32347/2412-9933.2024.58.80-85.
23. Yakovets, V. (2025), «Rozrobka metodiv vyiavlennia anomalii u veb-dodatkakh iz vykorystanniam intelektualnoho analizu danykh», *Naukovi notatky*, No. 1, pp. 86–92, doi: 10.36910/775.24153966.2024.79.12.

Фуріхата Денис Вікторович – аспірант, старший викладач кафедри комп'ютерних наук Державного університету «Житомирська політехніка».

Наукові інтереси:
- веборієнтовані системи
- Edge computing.

Вакалюк Тетяна Анатоліївна – доктор педагогічних наук, професор, завідувач кафедри інженерії програмного забезпечення Державного університету «Житомирська політехніка».

Наукові інтереси:
- Edge computing, cloud computing;
- IoT, аномалії, виявлення аномалій.

Furikhata D.V., Vakalyuk T.A.

Theoretical approaches to detecting anomalies in meter readings in scientific literature

The article is devoted to the study of modern scientific approaches to detecting anomalies in meter readings in the context of the development of intelligent energy networks. The study's relevance is due to the growing need for effective monitoring of electricity consumption, especially in the context of martial law in Ukraine, when the energy system is under constant threat and requires the most efficient management of resources. The paper provides a comprehensive analysis of existing methods for detecting anomalies, which are classified into three main categories: point anomalies, which represent individual deviations from the typical consumption pattern; contextual anomalies, which depend on the specific temporal or spatial environment; and collective anomalies, which arise in groups of interrelated data. The study demonstrates the advantages of decentralised approaches to data processing, particularly the use of edge computing and fog computing technologies, which allow information to be analysed directly on metering devices or in their immediate vicinity. A comparative analysis of centralised and decentralised methods shows that hybrid systems, which combine the advantages of both approaches, demonstrate the best results in practical applications. Particular attention is paid to analysing the effectiveness of various machine learning algorithms for anomaly detection. Statistical methods based on probabilistic models are considered, which allow relatively accurate determination of normal limits provided sufficient historical data is available. Classification methods of supervised learning are analysed, which require pre-labelled data for model training but provide high accuracy in detecting known types of anomalies. The prospects for further development of anomaly detection technologies in the context of integrating IoT devices, technology development and implementing more complex deep learning algorithms are considered.

Keywords: anomaly detection; meters; machine learning; edge computing; decentralised data processing; statistical analysis; IoT.

Стаття надійшла до редакції 27.03.2025.