УДК 004.8:621.39
DOI: 10.31673/2412-9070.2025.025596
В. О. ЗАВАЦЬКИЙ, аспірант;
ORCID: 0009-0005-5297-4127
В. Б. БІЛАВКА, аспірант;
ORCID: 0009-0000-5053-2601
К. П. СТОРЧАК, доктор техн. наук, професор,
ORCID: 0000-0001-9295-4685
Державний університет інформаційно-комунікаційних технологій, Київ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЯВЛЕННІ АНОМАЛІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Телекомунікаційні мережі стають дедалі більш динамічними та складними через величезні обсяги даних, які вони обробляють. У результаті виявлення аномальних подій у цих мережах є важливим для забезпечення безпеки та безперебійної роботи. Традиційні методи виявлення аномалій, які ґрунтуються на правилах, більше не є ефективними в умовах швидко змінюваного телекомунікаційного середовища. Таким чином, штучний інтелект відіграє важливу роль у подоланні цих недоліків.

У статті проводиться критичний аналіз ролі штучного інтелекту, зокрема методів глибокого навчання, у сучасних системах виявлення аномалій в телекомунікаційних мережах. Розглядається еволюція методів – від ранніх стратегій до сучасних методів, що базуються на штучному інтелекті.

Підкреслюється важливість використання гібридних моделей для підвищення надійності та стійкості. Це дозволить телекомунікаційним операторам проактивно керувати аномаліями та оптимізувати продуктивність у середовищі, керованому даними.

Ключові слова: Штучний інтелект, телекомунікаційні мережі, машинне навчання, глибоке навчання, аномалії, згорткова нейронна мережа, масштабованість.

Вступ

Основною метою виявлення аномалій у телекомунікаційній інфраструктурі є ідентифікація та усунення існуючих і потенційних загроз безпеці, надійності та продуктивності телекомунікаційних систем. Оскільки сучасні телекомунікаційні мережі розширюються, підтримують дедалі складніші моделі трафіку та інтегрують нові комунікаційні технології, традиційні методи виявлення аномалій на основі правил більше не є достатньо ефективними [1]. Такі застарілі системи мають труднощі з масштабуванням, адаптацією та забезпеченням реакції в реальному часі в умовах зростаючих обсягів даних і нових загроз. Це призводить до збоїв і непередбачуваних подій. Виникнення несправностей або несподіваних подій у мережі може спричинити значні втрати, зниження рівня обслуговування та серйозні порушення безпеки, що робить виявлення аномалій критично важливим для забезпечення доступності та захисту мережі.

Отже, необхідність виявлення аномалій у режимі реального часу зумовлена потребою запобігати несподіваним подіям і збоям, забезпечувати безперервне обслуговування, оптимізувати продуктивність і протидіяти загрозам безпеці, таким як DDoS-атаки, шахрайство та витоки даних [2]. Це можливо завдяки застосуванню штучного інтелекту у телекомунікаційному секторі.

Основна частина

Еволюція виявлення аномалій в телекомунікаційній інфраструктурі відображає технологічний прогрес, а також зростаючу складність телекомунікаційних мереж. З 1960-х років ця галузь пройшла шлях від ручних методів з встановленими пороговими значеннями до передових технологій штучного інтелекту (ШІ) та глибокого навчання. Ключові етапи включають введе-

ння автоматизованих систем на основі правил у 1980-х роках, що дозволили здійснювати базове виявлення аномалій через попередньо визначені пороги. У 2000-х роках зростання технологій машинного навчання привело до створення статистичних та прогностичних моделей, які покращили точність виявлення та масштабованість. Останнім часом досягнення в галузі глибокого навчання дозволили здійснювати аналіз великих, складних даних в режимі реального часу, значно підвищивши точність виявлення та швидкість реагування. Ці досягнення підкреслюють шлях галузі до обробки великих наборів даних з більш швидким і точним виявленням аномалій та можливістю реагування, що відображає прогрес технологій телекомунікаційних мереж.

Історично склалося так, що основним методом виявлення аномалій в телекомунікаціях були системи, засновані на правилах, які переважно використовували експертні знання. Мережеві адміністратори та мережеві інженери визначають певні стандарти та рівні толерантності на основі використання мережі, знань та досвіду [3]. Вони застосовують ці правила для контролю трафіку в мережі та використовують додаткові параметри вимірів для спрацьовування тривог, коли ці правила порушуються.

Ще однією проблемою був високий рівень помилкових і хибних спрацьовувань: моделі, засновані на правилах, не могли врахувати всіх особливостей і деталей мережевої активності. Більш того, ці методи функціонували лише після події, що ускладнювало вжиття заходів до того, як стануться небажані інциденти, коли певні заходи могли б запобігти або зменшити негативні наслідки [4].

Коли логіко-дедуктивні фреймворки почали виявлятися недостатніми для вирішення складних завдань, фокус уваги змістився в бік ШІ та його застосовність до задачі виявлення аномалій. Розвиток машинного навчання з використанням як керованого, так і некерованого навчання призвів до створення більш вдосконалених інтелектуальних та адаптивних систем виявлення аномалій. Популярні методи керованого навчання, такі як метод опорних векторів (SVM), дерева рішень і штучні нейронні мережі, спочатку розглядалися для вирішення проблем виявлення аномалій.

Виявлення аномалій за допомогою ШІ — це ідентифікація повторюваних патернів, які не входять в стандартний діапазон, за допомогою ШІ та машинного навчання. На відміну від традиційних методів, виявлення аномалій за допомогою ШІ не працює лише на основі фіксованих рівнів або базових математичних методів. Він використовує моделі, які навчаються на даних, що їм надаються, і можуть адаптуватися до змін у патернах [5]. Найбільш поширена процедура включає в себе сприйняття даних, їх перетворення, розробку моделі та подальше спостереження. Багатоваріантна регресія, нейронні мережі або алгоритми кластеризації захоплюють системну частину заданих патернів і навчаються на історичних даних. Ці моделі можуть виявляти відхилення в патернах, прогнозуючи відхилення, коли нові потоки даних надходять до моделей.

SVM використовує алгоритм керованого навчання, включаючи дерева рішень та випадкові ліси (RF), як традиційні методи, які найчастіше застосовуються до виявлення аномалій [6]. Ці алгоритми навчаються на мічених або керованих даних, де проводиться початкове вивчення нормальної та нав'язливої поведінки. Після завершення навчання вони можуть розрізняти типові та нетипові приклади вхідних даних з практичною точністю [7]. Тим не менш, процес отримання високоякісних маркованих даних є складним і займає багато часу, що значно знижує ефективність методів, що контролюються. Виявлення аномалій на основі ШІ в телекомунікаційній інфраструктурі охоплює різноманітні техніки, кожна з яких має свої унікальні переваги та виклики.

Традиційні методи машинного навчання, такі як k-найближчі сусіди (KNN), ізоляційний ліс (IF) і метод головних компонент (PCA), пропонують простоту та масштабованість для виявлення аномалій у низько вимірюваних та структурованих наборах даних. Наприклад, KNN та коефіцієнт локального відхилення (LOF) ефективні для виявлення аномалій у середовищах, де нормальна і аномальна поведінка чітко визначена, як у випадку виявлення шахрайства. Однак ці моделі стикаються з проблемами масштабованості та високовимірними даними, що

робить їх менш придатними для динамічних, масштабних телекомунікаційних мереж. PCA ефективний для зменшення розмірності та ізоляції аномалій, однак його припущення про лінійність обмежує його ефективність при роботі з більш складними наборами даних [8].

Методи глибокого навчання, зокрема рекурентні нейронні мережі (RNN), довготривала короткочасна пам'ять (LSTM) та автоенкодери, пропонують більш складні рішення, охоплюючи нелінійні та часові залежності. Ці моделі добре підходять для обробки послідовних даних, таких як часового ряду мережевого трафіку. Наприклад, LSTM відмінно виявляє довгострокові патерни та прогнозує майбутні аномалії. Однак моделі глибокого навчання є обчислювально витратними і вимагають великих обсягів тренувальних даних, що створює проблему для реального застосування в телекомунікаціях. Складність і чутливість цих моделей до гіперпараметрів також додають до експлуатаційних витрат, що ускладнює їх впровадження в масштабних системах без значного налаштування. Згорткова нейронна мережа (CNN), RNN та автоенкодери є одними з основних технік ШІ для виявлення аномалій в телекомунікаційних мережах [9]. CNN витягують ознаки з даних мережевого трафіку для виявлення атак, таких як DDoS. RNN обробляють дані часових рядів, виявляючи помилки та вторгнення. Автоенкодери ідентифікують аномалії шляхом реконструкції вхідних даних, позначаючи неправильні патерни [10]. Архітектура CNN, яка показана на рис. 1, складається з шарів згортки та об'єднання для вилучення ознак, за якими слідують повністю з'єднані шари для класифікації. Така структурована конструкція дозволяє CNN ефективно обробляти просторові ознаки, що робить їх особливо здатними до виявлення патернів та аномалій у даних телекомунікаційних мереж.

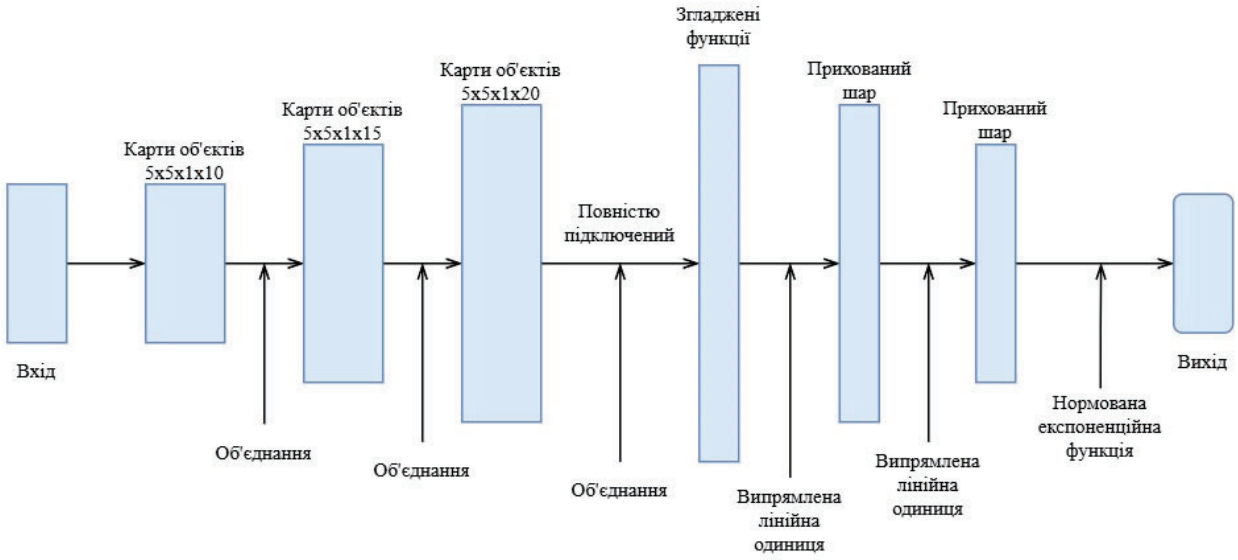

Рис. 1. Демонстрація архітектури CNN

Гібридні та ансамблеві методи набирають популярності, оскільки поєднують переваги традиційних та глибоких методів навчання. Ансамблеві методи – покращують точність, знижуючи дисперсію, що робить їх більш стійкими для виявлення аномалій у шумних та не збалансованих наборах даних, типових для телекомунікаційних мереж. Гібридні методи – об’єднують предметно-специфічні знання з методами ШІ, щоб покращити рівень виявлення складних моделей і рідкісних подій. Ці методи особливо ефективні для виявлення аномалій у багатовимірних даних, де комбінація методів може забезпечити вищу стійкість та кращу генералізацію для різних типів аномалій.

Нові тенденції, такі як федеративне навчання та периферійні обчислення, сприяють вирішенню основних проблем у виявленні аномалій в телекомунікаціях, зокрема масштабованості та конфіденційності [11]. Федеративне навчання дозволяє навчати моделі на розподілених пристроях без централізації сирих даних, що зменшує затримку та покращує масштабованість для реального часу виявлення аномалій [12]. Цей підхід особливо вигідний для телекомунікаційних мереж, де дані часто розподілені між численними вузлами, а конфіденційність є важливим питанням. Периферійні обчислення ще більше покращують виявлення аномалій в реальному

часі, зменшуючи обчислювальне навантаження на централізовані системи та дозволяючи виявляти аномалії ближче до джерела даних.

Традиційні методи машинного навчання пропонують простоту та легкість впровадження, тоді як передові методи глибокого навчання та гібридні методи забезпечують більш високу точність для складних і динамічних телекомунікаційних систем. Новітні тенденції в ШІ, такі як федеративне навчання та периферійні обчислення, прокладають шлях до більш ефективних, масштабованих та конфіденційних рішень. Однак обчислювальні вимоги та потреби в даних для моделей глибокого навчання залишаються значною перешкодою для виявлення аномалій у реальному часі в телекомунікаційній інфраструктурі, що вимагає постійної оптимізації та розвитку [13].

Телекомунікаційні мережі характеризуються великими обсягами даних в реальному часі, розподіленими архітектурами та динамічними трафіками. Ці характеристики значною мірою впливають на вибір і ефективність методів ШІ для виявлення аномалій, оскільки вони потребують методів, які можуть масштабуватися, обробляти часові залежності та підтримувати продуктивність з низькою затримкою. Розуміння цих унікальних аспектів телекомунікаційної інфраструктури є важливим для вибору відповідних методів виявлення аномалій на основі ШІ.

Телекомунікаційні мережі генерують величезні обсяги даних, які постійно надходять з різних джерел, таких як: активність користувачів, журнали мережевого обладнання та шаблони трафіку. Висока пропускна здатність вимагає від методів виявлення аномалій не лише ефективності, але й здатності працювати в реальному часі. Наприклад, традиційні методи, такі як KNN або LOF, мають труднощі з обробкою даних в реальному часі через високу обчислювальну вартість та неспроможність ефективно масштабуватися [14]. Натомість методи, такі як IF і RF, добре підходять для обробки великих наборів даних у реальному часі завдяки швидким процесам прийняття рішень, що дозволяє операторам зв'язку контролювати стан мережі з мінімальними затримками.

Практичне впровадження цих методів можна побачити в використанні IF для виявлення шахрайства в телекомунікаціях, де критично важливо оперативно виявляти підозрілі дії, щоб запобігти фінансовим втратам. Подібним чином, RF використовувався в моніторингу несправностей мережі, де необхідно одночасно аналізувати кілька джерел даних для швидкого виявлення аномалій. Ці методи пропонують значні переваги над старими системами, основаними на правилах, які часто пропускають малопомітні або мінливі загрози в динамічному середовищі трафіку телекомунікаційних систем.

Телекомунікаційні мережі за своєю суттю є розподіленими джерелами даних, які розподілені між численними вузлами, таких як базові станції, маршрутизатори та мобільні пристрої. Такі методи, як федеративне навчання та периферійні обчислення, набувають популярності, оскільки дозволяють здійснювати виявлення аномалій на периферії мережі, ближче до джерел даних. Навчаючи моделі локально на кожному вузлі, федеративне навчання забезпечує збереження конфіденційності даних, що є критичним для телекомунікаційних постачальників, які керують чутливою інформацією про клієнтів.

Важливим прикладом є використання федеративного навчання для виявлення аномалій мережевого трафіку на межі мереж 5G. У цьому сценарії розподілені моделі ШІ, такі як автоенкодери та LSTM, навчаються на локалізованих даних і агрегуються по всій мережі. Такий підхід не тільки знижує потребу у груповому передаванні даних, але й забезпечує адаптацію моделей до специфічних патернів трафіку кожного регіону.

Динамічна природа мережевого трафіку в телекомунікаційній інфраструктурі вимагає методів, які можуть ефективно моделювати тимчасові залежності. Аномалії часто виникають як відхилення від очікуваних патернів з часом, що вимагає моделей ШІ, які можуть фіксувати та передбачати дані часових рядів. Моделі RNN та LSTM є особливо ефективними в таких сценаріях, навчаючись на історичних даних для прогнозування майбутньої поведінки [15].

Моделі на основі LSTM продемонстрували високу ефективність у виявленні аномалій у мережевих часових рядах, таких як затримка в мережі та втрата пакетів. Їх здатність адаптуватися

до динамічних і змінних навантажень трафіку робить їх ідеальними для виявлення незвичних патернів, що сигналізують про потенційні збої в сервісах.

Масштабованість є ще одним критичним фактором при виборі методів ШІ для виявлення аномалій в телекомунікаціях. Оскільки мережі зростають у розмірах і складності, обчислювальні вимоги до моделей ШІ зростають. Для зменшення розмірності часто використовують такі методи, як PCA та автоенкодери, що дозволяє ефективно аналізувати великі потоки даних. Ці методи зменшують складність даних, зосереджуючись на найбільш значущих ознаках, дозволяючи здійснювати реальне виявлення аномалій без перевантаження обчислювальних ресурсів.

Однак масштабованість часто йде на шкоду точності. Моделі глибокого навчання, хоча й потужні, можуть мати труднощі з обробкою великих даних, що генеруються телекомунікаційними мережами, якщо вони не оптимізовані належним чином. Для вирішення цієї проблеми виникли гібридні методи ШІ, які поєднують швидкість і простоту традиційних моделей із точністю глибокого навчання.

У майбутньому периферійні обчислення та федеративне навчання продовжать відігравати ключову роль у покращенні реального виявлення аномалій в розподілених телекомунікаційних мережах. Як показано на рис. 2, методи ШІ забезпечують надійну основу для вирішення ключових проблем в телекомунікаційній інфраструктурі.

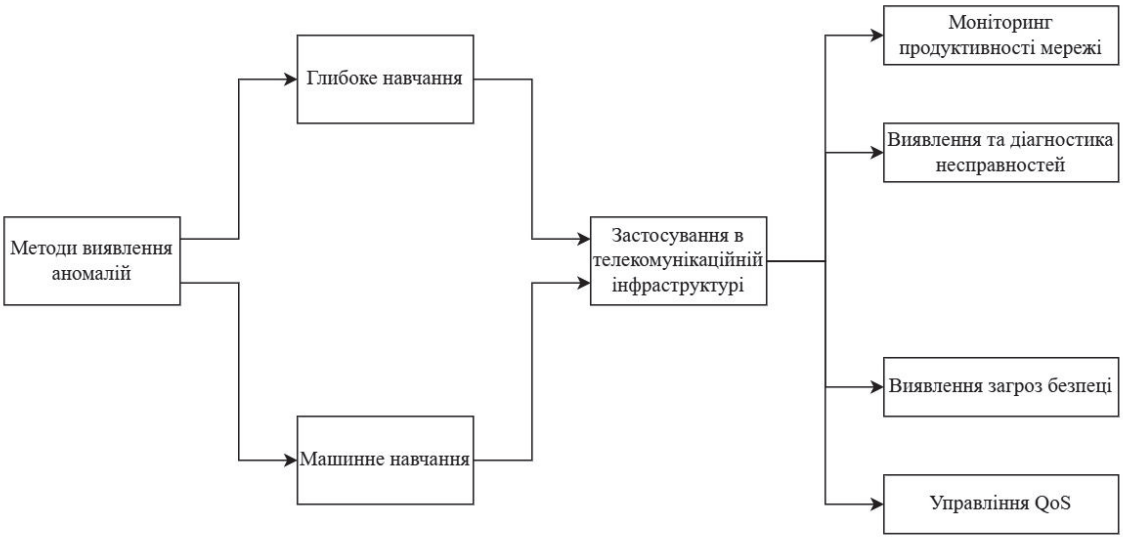

Рис. 2. Методи ШІ та їх застосування в телекомунікаційній інфраструктурі

Тому, специфічні характеристики телекомунікаційних мереж, такі як великі обсяги даних у реальному часі, розподілені архітектури та часові залежності, сильно впливають на вибір та ефективність методів виявлення аномалій на основі ШІ. У той час як традиційні методи пропонують простоту та ефективність, глибоке навчання, гібридні моделі та нові тенденції, такі як периферійні обчислення, визначають майбутнє виявлення аномалій у телекомунікаціях, покращуючи масштабованість, точність та можливості моніторингу у реальному часі.

Висновки

Методи штучного інтелекту демонструють високу ефективність у виявленні аномалій в телекомунікаційних середовищах. Зокрема, методи глибокого навчання, такі як згорткова нейронна мережа та автоенкодери, продемонстрували вищу точність і ефективність у виявленні аномалій в мережах. Ці передові методи чудово справляються з розпізнаванням складних шаблонів у великих наборах даних, що робить їх ідеальними для динамічної природи телекомунікацій. Однак традиційні моделі машинного навчання, такі як метод опорних векторів і дерева рішень, все ще мають свою цінність, особливо в невеликих або менш складних застосуваннях, де їхні обчислювальні вимоги є більш керованими.

Незважаючи на багатообіцяючі можливості виявлення аномалій на основі штучного інтелекту, на шляху їх впровадження в телекомунікаційній інфраструктурі залишається низка проблем. Однією з найактуальніших проблем є обробка величезних обсягів даних, які безперервно генеруються телекомунікаційними мережами. Ефективна обробка цих великомасштабних потоків даних в режимі реального часу залишається складним завданням, що вимагає впровадження передових технологій, таких як розподілені обчислення або периферійний штучний інтелект, для забезпечення своєчасного виявлення з мінімальною затримкою. Крім того, шумна і незбалансована природа телекомунікаційних даних створює проблеми, які вимагають ретельної попередньої обробки даних і вибору відповідних методів моделювання для підвищення надійності систем виявлення аномалій.

Масштабованість є ще однією важливою проблемою, оскільки моделі штучного інтелекту повинні бути ефективно реалізовані в рамках великих розподілених телекомунікаційних мереж. Збільшення обсягу мережевого трафіку вимагає, щоб моделі не тільки ефективно працювали при великих навантаженнях, а й залишалися адаптованими до змінних умов. Безперервне обслуговування моделей та їхнє перенавчання є необхідними для збереження точності та надійності, особливо у разі зсуву моделі, що може виникнути, коли поведінка мережі змінюється з часом. Оскільки телекомунікаційні мережі продовжують рости і ставати складнішими, вирішення цих проблем буде ключовим для успішного впровадження рішень для виявлення аномалій на основі штучного інтелекту.

Отже, хоча методи штучного інтелекту мають значний потенціал для покращення виявлення аномалій у телекомунікаціях, їхнє повне використання вимагатиме подолання основних викликів, пов'язаних з обсягами даних, затримкою, масштабованістю та обслуговуванням моделей. Зосередившись на цих аспектах, телекомунікаційні оператори зможуть краще підготуватися до роботи зі складністю сучасних мереж і зберегти високу якість обслуговування в умовах зростаючої цифровізації.

Список літератури

1. Abbasi M, Shahraki A, Taherkordi A (2021) Deep learning for network traffic monitoring and analysis (NTMA): a survey. Comput Commun 170:19–41.

2. Nv RR et al (2024) Enhancing anomaly detection: a comprehensive approach with MTBO feature selection and TVETBOOptimized Quad-LSTM classification. Comput Electr Eng 119:109536.

3. Palakurti NR (2024) Challenges and future directions in anomaly detection. Practical applications of data processing, algorithms, and modeling. IGI Global, pp 269–284.

4. Cui M, Zhang DY (2021) Artificial intelligence and computational pathology. Lab Investig 101(4):412–422.

5. Himeur Y, Ghanem K, Alsalemi A, Bensaali F, Amira A (2021) Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives. Appl Energy 287:116601.

6. Nassif AB, Talib MA, Nasir Q, Dakalbab FM (2021) Machine learning for anomaly detection: a systematic review. IEEE Access 9:78658–78700.

7. Ali SA (2024) Anomaly detection in telecommunication networks: leveraging novel big data and machine learning techniques for proactive fault management. Educ Adm Theory Pract 30(5):5751–5770.

8. Hasan BMS, Abdulazeez AM (2021) A review of principal component analysis algorithm for dimensionality reduction. J Soft Comput Data Min 2(1):20–30.

9. Hwang R-H, Peng M-C, Huang C-W, Lin P-C, Nguyen V-L (2020) An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access 8:30387–30399.

10. Krupski J, Graniszewski W, Iwanowski M (2021) Data transformation schemes for CNN-based network traffic analysis: a survey. Electronics 10(16):2021.

11. Marengo A (2024) Navigating the Nexus of AI and IoT: a comprehensive review of data analytics and privacy paradigms. Internet of Things, p 101318.

12. Ramineni A, Jayashree J, Vijayashree J, Konda R (2024) Machine learning for big data and neural networks. Cognitive machine intelligence. CRC Press, pp 58–86.

13. Banik S, Saha SK, Banik T, Hossain SM (2023) Anomaly detection techniques in smart grid systems: a review. In: 2023 IEEE World AI IoT Congress (AIIoT). IEEE, pp 0331–0337.

14. Scaranti GF, Carvalho LF, Barbon S, Proença ML (2020) Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks. IEEE Access 8:100172–100184.

15. Wang Z, Li J, Xu Z, Yang S, He D, Chan S (2023a) Application of deep neural network with frequency domain filtering in the field of intrusion detection. Int J Intell Syst 2023(1):8825587.

V. Zavatkyi, V. Bilavka, K. Storchak

USING ARTIFICIAL INTELLIGENCE IN ANOMALY DETECTION TO IMPROVE THE EFFICIENCY OF TELECOMMUNICATIONS NETWORKS

Telecommunications networks are becoming increasingly dynamic and complex due to the huge amounts of data they process. As a result, detecting anomalous events in these networks is essential to ensure security and business continuity. Traditional rule-based anomaly detection methods are no longer effective in the rapidly changing telecommunications environment. Thus, artificial intelligence plays an important role in overcoming these shortcomings.

The article critically analyzes the role of artificial intelligence, in particular deep learning methods, in modern systems for detecting anomalies in telecommunication networks. The evolution of methods is considered - from early strategies to modern methods based on artificial intelligence.

In addition to improving the accuracy of anomaly detection, the use of artificial intelligence allows you to adapt to new types of threats in real time. Systems built on machine learning are able to update their models independently as new behavioral patterns emerge in the network, which significantly reduces the time required to respond to incidents. Particularly promising are architectures based on recurrent neural networks and auto-encoders, which work effectively with data sequences and can detect even weakly expressed or hidden anomalies. In addition, the combination of deep learning methods with big data processing mechanisms allows for the scalability of solutions required to process information in networks with millions of users. The integration of such intelligent systems into the telecommunications infrastructure not only increases the level of security, but also contributes to the construction of self-learning networks capable of operating effectively in a highly dynamic environment. Moreover, these technologies open up opportunities for predictive maintenance, which reduces costs and minimizes downtime for critical services.

The importance of using hybrid models to increase reliability and resilience is emphasized. This will allow telecom operators to proactively manage anomalies and optimize performance in a data-driven environment.

Keywords: Artificial intelligence, telecommunication networks, machine learning, deep learning, anomalies, convolutional neural network, scalability.