УДК 004.8:004.7

М.Ю. Дмитрук [1]

О. В. Онищук [2]

Д.В. Карлов [2]

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ АВАРІЙНИХ СИТУАЦІЙ НА ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

[1] Вінницький національний технічний університет

[2] Харківський національний університет Повітряних Сил ім. І. Кожедуба

Анотація

У доповіді розглядається інноваційний підхід до підвищення надійності інфокомунікаційних мереж шляхом використання технологій штучного інтелекту для прогнозування аварійних ситуацій. Запропонований підхід ґрунтується на застосуванні алгоритмів машинного навчання та нейронних мереж для аналізу великих обсягів даних і виявлення потенційних відмов мережевого обладнання. Використання інтелектуальних систем моніторингу дозволяє своєчасно ідентифікувати аномалії, мінімізувати ризики збоїв та підвищити ефективність управління інфраструктурою. Представлено огляд сучасних методів прогнозування, їх переваги, а також перспективні напрямки подальшого вдосконалення систем моніторингу інфокомунікаційних мереж.

Ключові слова: штучний інтелект, інфокомунікаційні мережі, прогнозування, аварійні ситуації, машинне навчання, нейронні мережі, моніторинг, надійність, аналіз даних.

Abstract

TThe report considers an innovative approach to increasing the reliability of infocommunication networks by using artificial intelligence technologies to predict emergency situations. The proposed approach is based on machine learning and neural network software algorithms to analyze large amounts of data and identify detected failed network devices. The use of intelligent monitoring systems allows you to safely identify anomalies, minimize the risks of failures and increase the efficiency of infrastructure management. An overview of modern forecasting methods, their advantages, as well as promising areas for further improvement of the infocommunication network monitoring system is presented.

Keywords: artificial intelligence, infocommunication networks, forecasting, emergencies, machine learning, neural networks, monitoring, reliability, data analysis.

Сучасні інфокомунікаційні мережі є складними багаторівневими системами, від безперебійної роботи яких залежить функціонування критично важливої інфраструктури, зокрема енергетики, транспорту, банківських систем та засобів зв’язку [1]. В умовах зростання кількості інфокомунікаційних мереж та збільшення кількості задіяного обладнання підвищується ризик виникнення аварійних ситуацій, що потребує впровадження інтелектуальних систем моніторингу та прогнозування. [2]

У цьому контексті особливої актуальності набуває розвиток технологій штучного інтелекту, які дедалі ширше застосовуються у різних галузях — від медицини та енергетики до телекомунікацій.

Використання алгоритмів машинного навчання, глибоких нейронних мереж і методів обробки великих даних забезпечує здатність систем самостійно аналізувати інформаційні потоки, виявляти приховані закономірності та приймати рішення без безпосереднього втручання людини [3]. У сфері інфокомунікацій штучний інтелект стає ключовим інструментом для автоматизації процесів управління, прогнозування відмов обладнання та підвищення ефективності функціонування мереж.

Застосування методів штучного інтелекту, зокрема машинного навчання та нейронних мереж, дозволить здійснювати раннє виявлення аномалій у роботі мережі на основі аналізу великих обсягів даних. Алгоритми класифікації та прогнозування, що базуються на основі минулих аварійних ситуацій , можуть визначати ймовірність виникнення аварії та попереджати операторів про потенційні ризики [4].

Для реалізації таких систем необхідне застосування моделей глибокого навчання, рекурентні нейронні мережі (RNN, LSTM) та баєсівські мережі, які забезпечують точне прогнозування змін у параметрах трафіку й стані мережевого обладнання. Важливою складовою є інтеграція інтелектуальних систем із системами моніторингу (SNMP, NetFlow, Zabbix) для автоматизованого аналізу даних у реальному часі [5].

Впровадження штучного інтелект у процес прогнозування аварійних ситуацій підвищить надійність, безпеку інфокомунікаційних мереж та експлуатаційну стійкість, зменшить витрати на технічне обслуговування та скоротить час реагування на інциденти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. **Куліш О. В. Інформаційні системи та мережі.** — Київ : Кондор, 2021. — 312 с.
2. **Величко В. В., Бондаренко І. М. Надійність і живучість інфокомунікаційних систем.** — Харків : ХНУРЕ, 2020. — 276 с.
3. **Дьяконов В. П. Штучний інтелект. Велика енциклопедія.** — Київ : Діалектика, 2020. — 640 с.
4. **Гнатюк С. О. Штучний інтелект у системах кібербезпеки** // Наукові праці Одеської національної академії зв’язку ім. О. С. Попова. — 2022. — № 2. — С. 45–52.
5. **Пилипенко О. О., Лисенко І. В. Методи машинного навчання для виявлення аномалій у комп’ютерних мережах** // Вісник Вінницького національного технічного університету. — 2023. — № 1. — С. 58–64.

Дмитрук Максим Юрійович – студент групи ТСМ 25-м, факультет інформаційних електронних систем, e-mail: rordm279@gmail.com@gmail.com.

Онищук Олег Володимирович - к.т.н., доцент кафедри авіаційних радіотехнічних систем навігації та посадки Харківського національного університету Повітряних Сил ім. І. Кожедуба, м. Харків, e-mail: onyschukoleg@gmail.com.

Карлов Дмитро Володимирович — доктор технічних наук, старший науковий співробітник, начальник кафедри авіаційних радіотехнічних систем навігації та посадки Харківського національного університету Повітряних Сил ім. І. Кожедуба, м. Харків, e-mail: zeroua108@ukr.net

Maksym Yuriyovych Dmytruk - student, Faculty of Information Electronic Systems, e-mail: rordm279@gmail.com@gmail.com.

Onyshchuk Oleh -Ph.D., Associate Professor of Department of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, e-mail: onyschukoleg@gmail.com.

Karlov Dmitriy V. — Doctor of Engineering Science Senior Researcher Head of Department of Ivan Kozhedub Kharkiv National Air Force University, e-mail: zeroua108@ukr.net