УДК 621.39:004.451.2:004.8
DOI https://doi.org/10.32782/2663-5941/2024.6.1/22

Луцюк А.В.
Національний університет «Львівська політехніка»

ПРЕДИКТИВНИЙ МОНІТОРИНГ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ СПЕЦІАЛІЗОВАНОЇ МОДЕЛІ МАШИННОГО НАВЧАННЯ

Сучасні інформаційно-комунікаційні системи, зокрема мережі Інтернету речей (IoT), характеризуються швидким зростанням складності через збільшення кількості підключених пристроїв та обсягів мережного трафіку. Це створює значні виклики для традиційних методів моніторингу та керування, які не завжди здатні забезпечити необхідний рівень стабільності, безпеки та якості обслуговування (QoS) через обмежені можливості обробки великих обсягів даних у реальному часі. У зв'язку з цим виникає потреба у впровадженні нових підходів, здатних прогнозувати потенційні проблеми в інформаційно-комунікаційній мережі ще до їхнього виникнення.

В роботі розроблено та досліджено метод предиктивного моніторингу інформаційно-комунікаційних систем та мереж на основі машинного навчання, що базується на спеціалізованій моделі, яка здатна забезпечувати високу точність прогнозування з використанням відносно невеликої кількості параметрів моделі. Як основу для цієї моделі запропоновано просту нейронну мережу, яка дає змогу спростити процес навчання та не потребує значних обчислювальних ресурсів, що робить її придатною для впровадження в реальних мережних пристроях з обмеженими ресурсами. Для навчання моделі використано набір даних LUFlow, що містить промарковану інформацію про мережний трафік, зібраний за допомогою спеціальних інструментів моніторингу та захоплення трафіку.

У ході дослідження проведено аналіз ключових параметрів, що впливають на точність прогнозування, зокрема обсягів вхідного та вихідного трафіку, номери портів та IP-адреси джерела і призначення. Використані функції активації ELU та оптимізатор Adamax забезпечили стабільний процес навчання моделі та високу точність класифікації, яка досягла 92%. Це підтверджує ефективність запропонованого підходу для предиктивного моніторингу в інформаційно-комунікаційних системах.

Результати роботи свідчать про перспективність використання машинного навчання для прогнозування станів інформаційно-комунікаційних систем. Запропонована модель дозволяє не лише виявляти відомі аномалії в режимі реального часу, але й передбачати виникнення нових на основі попередніх даних моніторингу, що підвищує відмовостійкість мережі та покращує якість обслуговування користувачів. Подальші дослідження можуть бути спрямовані на оптимізацію архітектури нейронної мережі та розширення набору даних для підвищення точності та універсальності моделі.

Ключові слова: *система моніторингу, предиктивний моніторинг, інформаційно-комунікаційна система, машинне навчання, нейронна мережа.*

Постановка проблеми. Сучасні інформаційно-комунікаційні системи, зокрема мережі Інтернету речей (IoT), стають дедалі більш складними через стрімке зростання кількості мережного обладнання та обсягів трафіку. Це призводить до суттєвого ускладнення процесу моніторингу та керування такими системами. Традиційні методи аналізу та керування мережами вже не в змозі повністю забезпечити стабільність та безпеку функціонування цих систем через обмежені можливості обробки та аналізу даних у реальному часі. Зростаючі вимоги до забезпечення якості обслуговування (QoS), безпеки мережі та ефективного використання ресурсів потребують нових підходів до моніторингу, які здатні передбачати потенційні проблеми та аномалії ще до їхнього виникнення.

Одним із перспективних напрямків вирішення цієї проблеми є впровадження методів машинного навчання для прогнозування станів мережних систем. Використання предиктивного моніторингу дозволяє не тільки виявляти аномалії (збій обладнання, зміна характеристики трафіку, атаки, тощо), а й передбачати їх на основі аналізу історичних даних та виявлених шаблонів (патернів) у мережному трафіку. Проте, існує низка нерозв'язаних питань, пов'язаних із вибором оптимальних моделей машинного навчання, адаптацією цих моделей до різних типів мереж та їхньою здатністю працювати з великими обсягами даних у реальному часі. Ці виклики вимагають подальшого дослідження для створення ефективних та надійних систем виявлення та прогнозування аномалій.

Аналіз останніх досліджень і публікацій. Системи моніторингу в інформаційно-комунікаційних системах є критично важливими для забезпечення надійності та якості обслуговування. Зі зростанням складності мереж та обсягів трафіку традиційні методи моніторингу стають менш ефективними, що спонукає до впровадження методів машинного навчання для предиктивного моніторингу. Над цією проблемою зосереджені як науковці так і бізнес.

У дослідженні [1] розглядаються сучасні методи машинного навчання, які застосовують для моніторингу мереж у реальному часі. Автори підкреслюють важливість швидкої обробки даних та точності виявлення аномалій, що є ключовими для підтримки стабільної роботи інформаційно-комунікаційних систем.

У іншій схожій роботі [2] досліджують застосування глибоких нейронних мереж для аналізу мережного трафіку та виявлення аномалій. Хоча результати демонструють високу точність, автори зазначають, що такі моделі вимагають значних обчислювальних ресурсів, що може бути обмеженням для їх впровадження в реальних інформаційно-комунікаційних мережах.

У роботі [3] розглядають використання машинного навчання для прогнозування стану систем та виявлення потенційних збоїв. Автори підкреслюють важливість підготовки якісних наборів даних для навчання моделей, оскільки це безпосередньо впливає на точність прогнозів.

Попри значний прогрес у застосуванні машинного навчання для моніторингу інформаційно-комунікаційних систем, залишаються наступні виклики:

– *обчислювальні ресурси* – глибокі нейронні мережі забезпечують високу точність, але вимагають значних обчислювальних ресурсів, що може бути недоступним у деяких середовищах;

– *підготовка даних* – якість та репрезентативність даних для навчання моделей є критично важливими, але часто є обмеження щодо доступності таких даних;

– *масштабованість* – адаптація моделей до великих мереж з високою динамікою трафіку залишається складним завданням.

З урахуванням згаданих викликів, у роботі запропоновано у якості основи моделі машинного навчання просту нейронну мережа, яка дає змогу спростити та прискорити процес навчання та не потребує значних обчислювальних ресурсів, що робить її придатною для впровадження в реальних інформаційно-комунікаційних мережах. Також увагу зосереджено на покращенні наборів даних для збільшення ефективності навчання, оскільки дані, зібрані в реальних умовах, є гетерогенними, і знижують ефективність навчання.

Постановка завдання. Моніторинг інформаційно-комунікаційних систем є ключовим інструментом для забезпечення відмовостійкості, ефективності роботи мережі та високої якості користувацького досвіду. Системи моніторингу базуються на апаратних і програмних компонентах, що відслідковують та аналізують параметри програмно-апаратних систем, включно з мережним трафіком. У загальному вигляді методи моніторингу поділяються на активні та пасивні [4].

Активний моніторинг, який часто називають синтетичним, базується на створенні моделей, що імітують поточну поведінку мережі, замість використання реальних даних користувачів [5]. Такий підхід дозволяє виявляти потенційні проблеми до їх виникнення, оцінюючи продуктивність мережі в реальному часі. Однак цей метод потребує значних обчислювальних ресурсів, оскільки базується на складних алгоритмах і прогнозних моделях.

Пасивний моніторинг, у свою чергу, використовує реальні дані, які генеруються користувачами мережі, що дозволяє отримати цілісне уявлення про поточний стан мережі. Незважаючи на високу точність, цей підхід має обмеження – він не дозволяє прогнозувати проблеми, а лише виявляє ті, які вже сталися, і потребує негайного втручання [6].

Кожен із цих методів має свої переваги та недоліки. Зокрема, активний моніторинг здатний передбачати аномалії, але залежить від точності передбачень і потребує більше ресурсів. У свою чергу пасивний моніторинг надає точні дані про поточний стан системи, але не дозволяє уникнути вже виниклих проблем [7].

У зв’язку зі стрімким зростанням обсягів мережного трафіку та кількості користувачів інформаційно-комунікаційних систем, перед системами моніторингу постають такі нові виклики: аналіз і зберігання великих обсягів даних; використання даних трафіку для бізнес-аналітики; інтеграція та безпека обробки даних; неоднорідність вхідних даних та необхідність уніфікації підходів до моніторингу [8].

Ці проблеми вимагають розробки нових підходів, які поєднують активні та пасивні методи моніторингу, і орієнтуються на застосування сучасних технологій, таких як машинне навчання. Одним із перспективних напрямів є предиктивний моніторинг, який дозволяє не лише аналізувати поточний стан мережі, але й прогнозувати мож-

ливі аномалії. Предиктивний моніторинг вузлів покликаний уникнути часової затримки, що виникає між подією та реакцією на подію. Добитися подолання часової затримки дозволяє наявність окремої, додаткової складової в системі моніторингу, що аналізує вхідні дані та в подальшому намагається визначити тенденцію зміни показників. Власне ця складова і створює таку подію як передбачення. Передбачення ($T_{передбачення}$) виникає раніше, ще до виникнення самої події ($T_{події}$). Таким чином, час реакції на подію в предиктивній системі можна описати формулою 1:

$$\Delta T = T_{передбачення} - T_{події} \quad (1)$$

де ΔT – це часовий інтервал між передбаченням події та її фактичною фіксацією.

Оскільки предиктивна система моніторингу працює на випередження, то спостерігаємо ситуацію, що, за нормальних умов роботи, часова затримка буде від'ємною, що означає виграш часу для реакції на подію ще до її виникнення. Тобто, що стосується самої події, момент її фіксації – це прогнозована із певною точністю величина, котра повинна передбачатися задля її уникнення. Використання машинного навчання у цьому контексті забезпечує автоматизацію процесу виявлення змін у стані системи та запобігає виникненню нештатних ситуацій.

Метою є розроблення та дослідження методу предиктивного моніторингу на основі машинного навчання, що дозволяє знизити ризики виникнення в інформаційно-комунікаційних системах аномалій за рахунок виявлення змін у стані системи до їхнього критичного впливу на систему. Пропонований підхід зосереджується на класифікації мережного трафіку з високою точністю при мінімальних обчислювальних витратах, а також на забезпеченні ефективної даних для навчання моделей.

Виклад основного матеріалу. У межах цієї статті використовується набір даних LUFlow Network Intrusion Detection Data Set [9]. LUFlow – це потоковий набір даних, створений і промаркований з урахуванням кореляції зловмисної активності, призначений для тренування моделей і виявлення потенційних вторгнень у систему. Дані отримано за допомогою мережної пастки (honeypots) – спеціальних вузлів або ресурсів, які слугують приманкою для залучення зловмисного трафіку. Метою використання мережної пастки є навмисне провокування виникнення аномалій для подальшого аналізу зібраного трафіку [9]. Для збору телеметрії в цих вузлах інформаційно-комунікаційних систем застосовувався інструмент Cisco Joy.

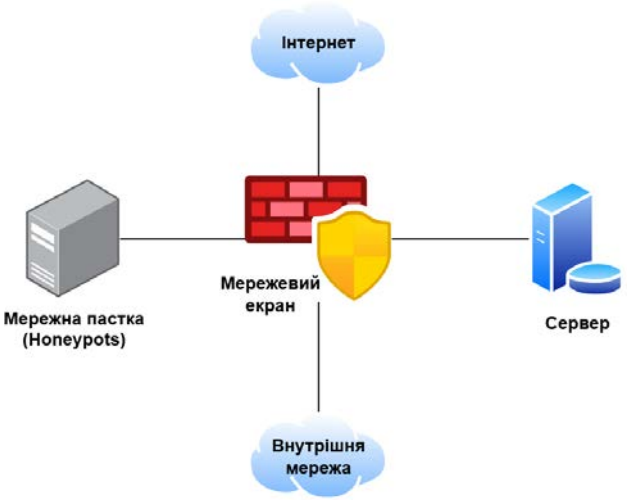

Рис. 1. Принцип застосування мережної пастки

Зібрані дані за допомогою інструментів Cisco промарковані в залежності від типу трафіку. Класів трафіку, представлених в наборі даних (табл. 1), всього 3. Перший клас має маркування benign, що позначає звичайний трафік в мережі. В свою чергу malicious – це аномальний трафік який вдалося виявити та маркувати. Але оскільки наявність вкидів в реальних інформаційно-комунікаційних системах є нормою [5], то в наборі даних представлений клас outlier, котрий не можна точно віднести ні до нормального, ні до зловмисного трафіку.

Таблиця 1

Приклади даних для кожного із класів

Параметр / Маркування	benign	malicious	outlier
src_ip	786	786	786
src_port	68		47613
dest_ip	786	786	786
dest_port	67		31306
protocol	17	1	6
bytes_in	0	8	0
bytes_out	600	8	0
numpktsin	0	1	0
numpktsout	2	1	1
entropy	1.615865	2.75	0.0
total_entropy	969.5192	43.99	0.0
duration	7.17	8.4e-5	0.0

Звертаючись до конкретних прикладів наведених у таблиці 1, варто зазначити, що так званий malicious приклад трафіку має різку відмінність у вигляді відсутності source port and destination port. Задля кращого розуміння набору даних

(табл. 2) варто звернутися до попарної кореляції за методом Пірсона та проаналізувати залежність параметрів (рис. 2).

Якщо опиратися на отримані показники попарної кореляції, то значення label сильно корелює із такими параметрами як: bytes out, destination port, destination ip, source port, source ip, total entropy. В свою чергу time_end та time_start є такими, що слабо корелюють з іншими параметрами. Параметрами, що мають слабку кореляцію можна знехтувати у процесі навчання [10].

Процес налаштування параметрів нейронної мережі здійснено ітеративно, шляхом багаторазового тестування різних конфігурацій моделі. Це включало підбір оптимальної кількості шарів, нейронів, функцій активації та інших гіперпараметрів з метою досягнення балансу між точністю моделі та її складністю. Кожна ітерація базувалася на аналізі результатів попередніх, дозволяючи поступово вдосконалювати модель для забезпечення її стабільності та узгодженості з поставленими цілями.

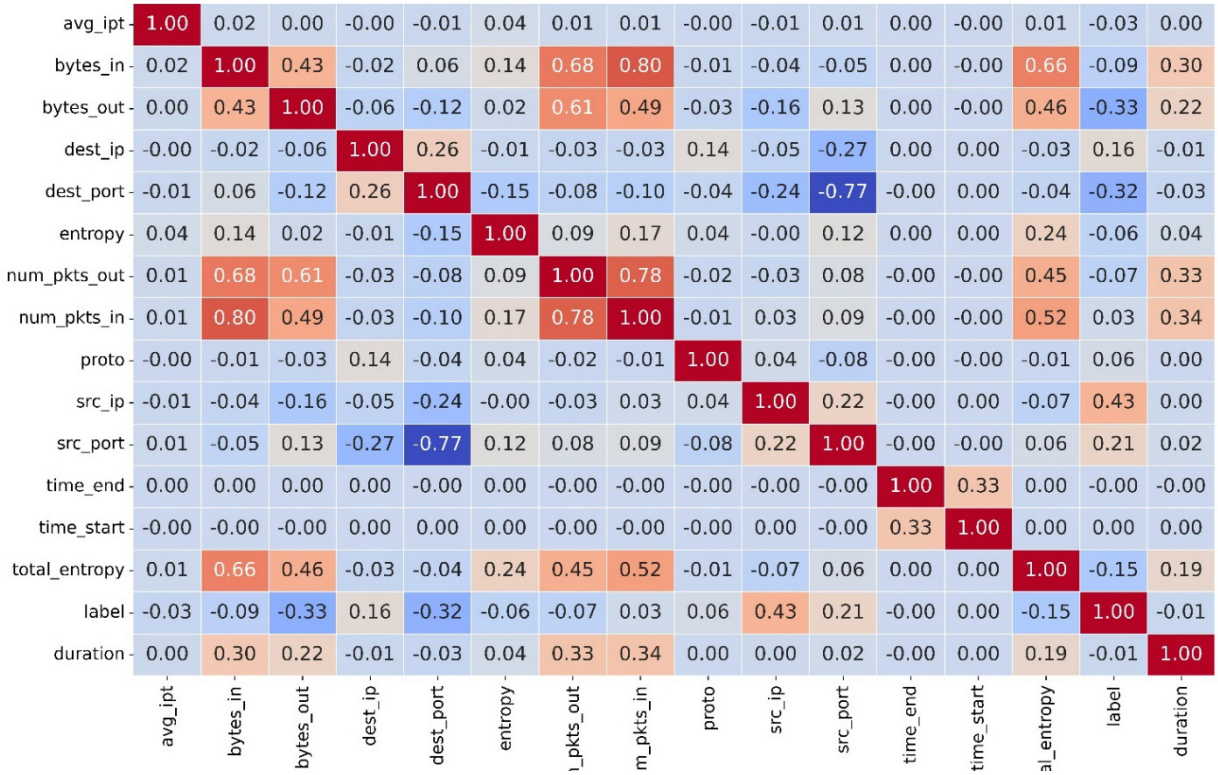

Рис. 2. Попарна кореляція за Пірсоном

Таблиця 2

Опис параметрів набору даних

Назва параметра	Опис параметра
src_ip	Анонімізована IP-адреса джерела
src_port	Номер порту джерела
dest_ip	Анонімізована IP-адреса призначення
dest_port	Номер порту призначення
protocol	Номер протоколу за яким працює потік
bytes_in	Кількість байтів, переданих від джерела
bytes_out	Кількість байтів, переданих від призначення
numpktsin	Кількість пакетів даних від джерела до місця призначення
numpktsout	Кількість пакетів від пункту призначення до джерела
entropy	Ентропія в бітах на байт полів даних у потоці
total_entropy	Загальна ентропія в байтах за всіма байтами в полях даних потоку
mean_ipt	Середнє значення міжпакетного часу прибуття потоку
duration	Час тривалості потоку з точністю до мікросекунди
label	Означення потоку. Розмітка

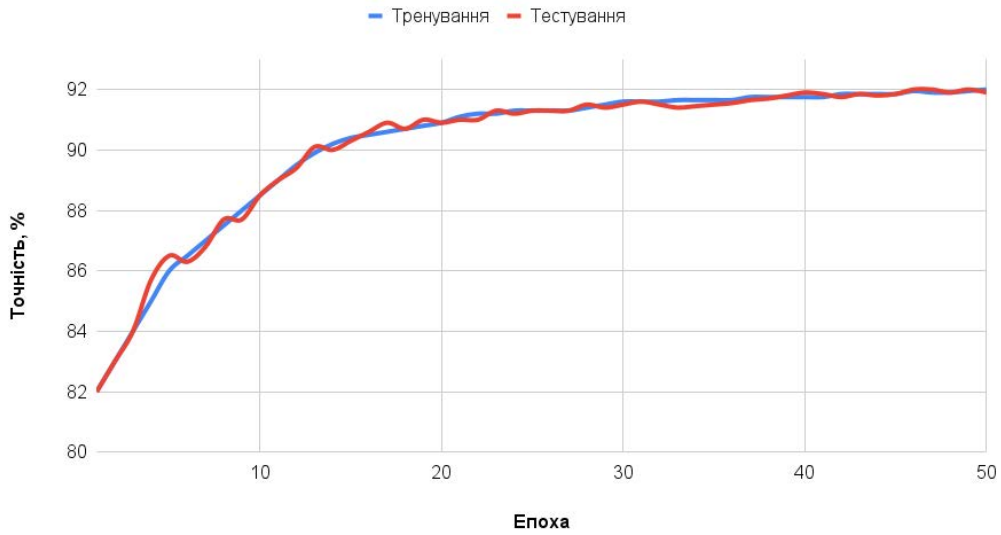

Рис. 3. Результати навчання та тестування моделі

Однак існує важлива проблема – оптимальні параметри, підібрані на етапі навчання моделі, не завжди гарантують таку ж точність під час роботи з реальними даними. Тому необхідно враховувати цей аспект і періодично повторювати процес навчання модель, адаптуючи її до змін даних з плином часу. Це основний недолік спеціалізованих моделей у порівнянні з доступними сьогодні узагальненими (GPT, Claude, тощо).

Проведені ітеративні дослідження дозволили визначити оптимальний баланс параметрів для нейронної мережі, що забезпечує точність прогнозування на рівні 92% (рис. 3).

Для забезпечення стабільного зростання точності протягом усіх епох навчання та уникнення вимикання нейронів при обробленні від'ємних значень було обрано функцію активації ELU. Крім того, для оптимізації процесу навчання використовувався оптимізатор Adamax, що показав високу ефективність у забезпеченні стабілізації і досягнення високої точності в процесі навчання моделі.

Модель має класичну каскадну структуру, де виходи нейронів одного шару є вхідними даними для наступного шару. Загальна кількість зв'язків між нейронами становить 12 707. Така конфігурація дозволила досягти балансу між складністю моделі та швидкістю її навчання.

Після завершення етапів навчання та тестування модель збережена для подальшого використання у задачах прогнозування. Крім того, її можна завантажити та продовжити навчання, що є критично важливим у контексті змінного характеру даних у інформаційно-комунікаційних системах. Такі зміни можуть включати перехід раніше нештатних ситуацій до каласу нормальних, що зумовлює необхідність адаптації моделі до нових умов.

Таким чином, модель демонструє високу точність (92%) прогнозування, зберігаючи можливість подальшого вдосконалення для адаптації до реальних умов експлуатації. Це засвідчує перспективність подальшої роботи у використанні нейронної мережі для покращення роботи систем моніторингу. Слід зазначити, що результати є проміжними. Завдяки більш точному підбору параметрів нейронної мережі та зміні архітектури нейронної мережі, потенційно можливо досягти кращих показників на використаному в досліджені наборі даних.

Висновки. У статті розроблено та досліджено метод предиктивного моніторингу інформаційно-комунікаційних систем на основі машинного навчання. Запропонована проста нейронна мережа продемонструвала високу точність класифікації мережного трафіку, досягаючи 92% при мінімальних обчислювальних витратах. Це робить модель придатною для впровадження в реальних інформаційно-комунікаційних мережах, де ресурси можуть бути обмеженими.

Аналіз набору даних LUFlow дозволив виділити ключові параметри, що найбільше впливають на точність прогнозування. Використання функції активації ELU та оптимізатора Adamax забезпечило стабільну збіжність моделі та уникнення проблем, пов'язаних з обробкою від'ємних значень. Лінійна структура нейронної мережі з 12 707 зв'язками між нейронами дозволила досягти оптимального балансу між складністю моделі та швидкістю її навчання.

Важливим аспектом дослідження стало підкреслення необхідності регулярного перенавчання моделі для адаптації до змін у мережному трафіку, що є типовим для інформаційно-комунікаційних систем. Модель може бути завантажена та продовжена у навчанні, що забезпечує її гнучкість та довгострокову ефективність.

Результати дослідження підтверджують перспективність використання машинного навчання для предиктивного моніторингу інформаційно-комунікаційних систем. Подальша робота може бути спрямована на оптимізацію параметрів моделі, експерименти з альтернативними архітектурами нейронних мереж та розширення наборів даних для підвищення точності та надійності прогнозування. Це відкриває можливості для більш ефективного керування мережами, підвищення їх відмовостійкості та якості обслуговування користувачів.

Список літератури:

1. Bian J., et al. Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey. IEEE Internet of Things Journal. 2022. Т. 9. № 11. С. 8364–8386. DOI: 10.1109/JIOT.2022.3161050.

2. Liu M., Yang L. IoT Network Traffic Analysis with Deep Learning (Version 1) [Електронний ресурс]. arXiv. 2024. URL: https://doi.org/10.48550/ARXIV.2402.04469.

3. Li H., Wang X., Feng Y., Qi Y., Tian J. Driving intelligent IoT monitoring and control through cloud computing and machine learning [Електронний ресурс]. arXiv [cs.AI]. 2024. URL: https://doi.org/10.48550/ARXIV.2403.18100.

4. Faychuk V., Lavriv O., Stryhalyuk B., Shpur O., Demydov I., Bak R. Performance of routing algorithm remote operation in cloud environment for IoT devices. International Journal of Electronics and Telecommunications. 2019. Т. 65. № 3. С. 367–373.

5. Lutsiv N., Maksymyuk T., Beshley M., Lavriv O., Andrushchak V., Sachenko A., Vokorokos L., Gazda J. Deep semisupervised learning-based network anomaly detection in heterogeneous information systems. Computers, Materials & Continua. 2022. Т. 70. № 1. С. 413–431.

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

7. Kurt B., Zeydan E., Yabas U., Karatepe I. A., Kurt G. K., Cemgil A. T. A Network Monitoring System for High Speed Network Traffic. 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). London, UK, 2016. С. 1–3. DOI: 10.1109/SAHCN.2016.7732965.

8. Lotfollahi M., Shirali hossein zade R., Jafari Siavoshani M., Saberian M. Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning. Soft Computing. 2020. Т. 24. DOI: 10.1007/s00500-019-04030-2.

9. Mills R. LUFlow Network Intrusion Detection Data Set [Електронний ресурс]. Kaggle. 2023. URL: https://doi.org/10.34740/KAGGLE/DSV/6403282.

10. Sahay R., Geethakumari G., Modugu K., Mitra B. Traffic Convergence Detection in IoT LLNs: A Multilayer Perceptron based Mechanism. 2018 IEEE Symposium Series on Computational Intelligence (SSCI). Bangalore, India, 2018. С. 1715–1722. DOI: 10.1109/SSCI.2018.8628921

Lutsiuk A.V. PREDICTIVE MONITORING OF INFORMATION AND COMMUNICATION SYSTEMS USING A SPECIALIZED MACHINE LEARNING MODEL

Modern information and communication systems, particularly Internet of Things (IoT) networks, are characterized by rapidly increasing complexity due to the growing number of connected devices and network traffic volumes. This presents significant challenges for traditional monitoring and management methods, which often fail to provide the required levels of stability, security, and quality of service (QoS) due to their limited capacity to process large amounts of data in real time. Consequently, there is a pressing need for innovative approaches capable of predicting potential issues in information and communication networks before they occur.

This study develops and examines a method for predictive monitoring of information and communication systems and networks based on a machine learning approach. A specialized model is proposed, capable of delivering high prediction accuracy while requiring a relatively small number of parameters. The core of the model is a simple neural network, which simplifies the training process and does not demand significant computational resources, making it suitable for deployment in real-world network devices with limited resources. The LUFlow dataset, containing labeled information on network traffic collected through specialized monitoring and capture tools, was utilized to train the model.

The research involved analyzing key parameters influencing prediction accuracy, such as incoming and outgoing traffic volumes, port numbers, and source and destination IP addresses. The use of ELU activation functions and the Adamax optimizer ensured a stable training process and high classification accuracy, reaching 92%. These results confirm the effectiveness of the proposed approach for predictive monitoring in information and communication systems.

The findings demonstrate the potential of machine learning in predicting the states of information and communication systems. The proposed model not only detects known anomalies in real time but also forecasts the occurrence of new ones based on historical monitoring data, thereby improving network resilience and enhancing user quality of service. Future studies may focus on optimizing the neural network architecture and expanding the dataset to increase the model's accuracy and versatility.

Key words: *monitoring system, predictive monitoring, information and communication system, machine learning, neural network.*