УДК 004.22

https://doi.org/10.52058/2786-6025-2025-13(54)-2354-2374

Нежуренко Олександр Григорович кандидат технічних наук, старший викладач кафедри комп'ютерних наук та інформаційних технологій, Житомирський державний університет імені Івана Франка, https://orcid.org/0009-0007-4594-9606

AI-DRIVEN NETWORKING: МОДЕЛІ АВТОМАТИЧНОГО УПРАВЛІННЯ МЕРЕЖАМИ

Анотація. У статті досліджено концепцію мереж на основі штучного інтелекту (МНОШІ) в якості фундаментальної основи для побудови автономних, адаптивних та масштабованих телекомунікаційних систем, здатних функціонувати в умовах зростаючої складності цифрової інфраструктури. Обґрунтовано, що традиційні методи мережевого управління втрачають ефективність через збільшення обсягів та варіативності телеметричних даних, підвищення динамічності трафіку та еволюцію загроз. Показано, що інтеграція моделей машинного навчання у структуру МНОШІ забезпечує можливість інтелектуального опрацювання потокової телеметрії, прогнозування станів мережі, раннього виявлення аномалій, оптимізації маршрутів та формування автономних рішень у режимі реального часу.

У роботі розкрито проблематику впровадження ШІ-орієнтованих систем, зокрема питання стандартизації телеметрії, низької інтерпретованості глибинних моделей, складності інтеграції у мультивендорні та гетерогенні середовища, а також ризики змагальних атак на моделі машинного навчання. Систематизовано ключові передумови створення МНОШІ, серед яких – архітектурна організація збору та потокової обробки даних, побудова моделювальної інфраструктури, розроблення механізмів оркестрації, формування контрольованої автономії та впровадження кіберстійких методів забезпечення роботи моделей. Запропоновано узагальнену етапну модель реалізації МНОШІ, що охоплює аналіз стану мережевої інфраструктури, визначення цілей автоматизації, підготовку даних, навчання моделей, інтеграцію з оркестраторами та розгортання замкненого контуру автономного управління з адаптивним перенавчанням.

На основі прикладних сценаріїв у сферах медицини, фінансових сервісів, телекомунікацій та промисловості продемонстровано практичну ефективність МНОШІ у підвищенні стійкості, продуктивності та передбачуваності мережевих систем. Отримані результати підтверджують, що МНОШІ формують

технологічну платформу для мереж наступного покоління, орієнтованих на самокерування, масштабованість і високий рівень надійності.

Ключові слова: мережі на основі штучного інтелекту, машинне навчання; автоматизація, телеметрія; автономне управління; IoT.

Nezhurenko Oleksandr PhD in Technical Sciences, Senior Lecturer of the Department of Computer Science and Information Technology, Zhytomyr Ivan Franko State University, https://orcid.org/0009-0007-4594-9606

AI-DRIVEN NETWORKING: MODELS FOR AUTOMATED NETWORK MANAGEMENT

Abstract. The article explores the concept of artificial intelligence-based networks (AIBN) as a fundamental basis for building autonomous, adaptive, and scalable telecommunications systems capable of functioning in the increasingly complex digital infrastructure. It is argued that traditional network management methods are losing their effectiveness due to the increase in the volume and variability of telemetry data, the increased dynamism of traffic, and the evolution of threats. It is shown that the integration of machine learning models into the AIBN structure provides the ability to intelligently process streaming telemetry, predict network states, detect anomalies early, optimize routes, and form autonomous decisions in real time.

The paper reveals the problems of implementing AI-oriented systems, in particular the issues of telemetry standardization, low interpretability of deep models, the complexity of integration into multi-vendor and heterogeneous environments, as well as the risks of competitive attacks on machine learning models. The key prerequisites for creating AIBN are systematized, including the architectural organization of data collection and streaming processing, the construction of a simulation infrastructure, the development of orchestration mechanisms, the formation of controlled autonomy, and the implementation of cyber-resilient methods for ensuring the operation of models.

A generalized phased model for AIBN implementation is proposed, covering network infrastructure analysis, automation goal setting, data preparation, model training, integration with orchestrators, and deployment of a closed-loop autonomous control system with adaptive retraining.

Based on applied scenarios in the fields of medicine, financial services, telecommunications, and industry, the practical effectiveness of AIBN in increasing the resilience, performance, and predictability of network systems has been demonstrated. The results confirm that AIBN form a technological platform for next-generation networks focused on self-management, scalability, and high reliability.

Keywords: artificial intelligence-based networks, machine learning; automation, telemetry; autonomous control; IoT.

Постановка проблеми. Розвиток сучасних інформаційних технологій (ІТ) та стрімка цифрова трансформація соціально-економічних систем спричинили глибоку еволюцію мережевих технологій (МТ), у межах якої сучасні комп'ютерні мережі перестали бути в якості статичної або передбачуваної інфраструктури. Вони поступово перетворювалися на складні, багаторівневі та динамічні екосистеми, що обслуговують хмарні сервіси, системи реального часу, мультимедійні потоки, мережі 5G та 6G, промислові пристрої Інтернет речей (IoT) та розподілені мережеві системи. В таких умовах значно зростають обсяги, швидкість і варіативність мережевого трафіку, а також супроводжується ускладненням топології та логіки взаємодії між елементами мережі [1].

Для високодинамічного середовища традиційні підходи щодо управління мережами, які засновані на статичних правилах, ручній конфігурації та швидкому реагуванні на інциденти є недостатніми та менш ефективними. Наприклад, адміністратор фізично не здатний обробний потоки телеметрії (NetFlow/IPFIX, SYSLOG, SNMP або DPI тощо) у режимі реального часу, здійснити точну діагностику аномалій або адаптувати маршрути до швидкозмінних умов трафіку. Дослідження свідчать, що до 70-80% інцидентів у масштабних мережах спричинені помилками конфігурації, що підкреслює критичність людського фактору [2].

Водночас виникають також нові виклики продуктивності та безпеки. Динамічні перевантаження та атаки, наприклад, мережеві атаки (DDoS) або атаки «нульового дня» (Zero-day attack), внутрішні порушення політик доступу та складні сценарії міжмережевої взаємодії потребують миттєвої реакції [3]. У потоковій передачі фінансових даних, зокрема в системах високочастотної торгівлі затримки на рівні мікросекунд визначають прибутковість операцій, що висуває екстремальні вимоги до стабільності, прогнозованості та оптимізації мережевих шляхів.

Традиційні методи маршрутизації чи QoS-політики не можуть забезпечити таку точність у реальному часі.

У відповідь на ці виклики формується підхід AI-driven networking або мережа на основі штучного інтелекту (МНОШІ) – архітектурна та методологічна концепція, що передбачає інтеграцію алгоритмів машинного навчання (МН), інтелектуальну автоматизацію, предиктивний аналіз та автономне прийняття рішень у процеси управління мережевою інфраструктурою. Використання ШІ може забезпечити автоматичне виявлення аномалій, прогнозування відмов, самостійну оптимізацію маршрутизаторів, адаптивні

політики безпеки, механізми самовідновлення (Self-healing) та механізми на основі намірів (Intent-based) конфігурації, коли адміністратор визначає ціль, а система сама генерує оптимальні дії [4].

Разом із тим, впровадження моделей AI-driven супроводжується низкою наукових і технічних проблем, що потребують ґрунтовного вивчення. Серед основних викликів можна виділити [5]:

- надійність та повнота телеметричних даних, оскільки дані можуть бути фрагментованими, несумісними або недоступними через обмеження застарілого обладнання;
- контрольованість та прозорість МН-моделей, оскільки «Чорні скриньки» глибинних мереж містять ризики некерованих змін конфігурації, ускладнюють аудит і знижують довіру адміністраторів;
- інтеграція у гетерогенні інфраструктури, де мережа може містити SDN, IoT, 5G-сегменти та обладнання, а ШІ-модель має працювати поверх усіх цих шарів;
- безпека автономних рішень, оскільки деякі сценарії можуть охоплювати сценарії, де моделі можуть стати ціллю змагальних атак (adversarial attacks), зо здатні спричинити небезпечні автоматизовані дії;
- складність обчислень та затрати ресурсів, де обробка потокової телеметрії, робота навчання з підкріпленням та глибинних моделей потребує оптимізації для функціонування з мінімальною латентністю.

З огляду на викладене, основна наукова проблема полягає в тому, що сучасні мережеві системи потребують інтелектуальних, інтерпретованих, масштабованих і безпечних моделей МНОШІ, здатних забезпечувати автономне, адаптивне та прогнозуюче управління мережевими ресурсами в режимі реального часу. Необхідно розробити підходи, які поєднуватимуть високу точність МН-аналітики, гарантії кіберстійкості, можливість пояснення рішень, гнучку інтеграцію з гетерогенними інфраструктурами та підтримку критично важливих сценаріїв від мультимедійного трафіку до високочастотної фінансової торгівлі [1].

Розв’язання цієї проблеми вимагає комплексного міждисциплінарного підходу, що охоплює моделювання телеметричних потоків, алгоритми МН, оптимізаційні методи, принципи побудови комп’ютерних мереж, кібербезпеку та інженерію розподілених систем. Лише створення цілісних і надійних моделей МНОШІ дозволить забезпечити новий рівень автономності, ефективності та стійкості сучасних і майбутніх цифрових мереж.

Аналіз останніх досліджень та публікацій. Проблематика інтеграції методів ШІ в процесі автоматизованого управління мережами поступово переходить у статус одного з ключових напрямів розвитку сучасних телекомунікаційних систем. Зростання складності мережевих інфраструктур, поява

мереж 5G/6G, індустріального IoT та хмарних платформ зумовлюють потребу у створенні нових моделей, здатних забезпечити автономність, адаптивність і безпеку керування мережевими процесами. Останні дослідження демонструють високий рівень наукового інтересу до застосування алгоритмів МН для аналізу мережевої телеметрії, оптимізації ресурсів, виявлення інцидентів та підтримки рішень у режимі реального часу.

Зокрема, у роботі [6] представлено систематизований огляд ШІ в контексті МТ. Авторами охарактеризовано ключові напрями використання та впровад-ження ШІ, включаючи маршрутизацію, QoS-оптимізацію, безпеку та керування трафіком. Попри загальність викладу, це дослідження є важливим із погляду формування цілісного уявлення про спектр можливостей МНОШІ, хоча й не пропонує детальних практичних моделей або експериментальних рішень.

Водночас з цим, у роботі [7] розглядається комплексний підхід щодо автоматизованого управління мережевими інцидентами, який включає їх виявлення, класифікацію та діагностику за допомогою методів МН. Авторами запропоновано цілісне бачення, що охоплює повний життєвий цикл інцидентів у сучасних мережах. Особливу увагу приділено поясненню моделей, що є критично важливим для їх інтеграції у мережеві операційні середовища. Проте відсутність механізмів гарантування безпечного автоматизованого виконання рішень у реальному часі залишається суттєвим обмеженням.

Потенціал МНОШІ оптимізації мереж охарактеризовано в роботі [8], де автори детально аналізують можливості алгоритмів МН для підвищення продуктивності мереж шляхом балансування навантаження, зниження затримок і покращення пропускної здатності. Хоча результати демонструють значні переваги інтелектуальних моделей, більшість експериментів виконано за допомогою середовища симуляції, що створює ризик невідповідності реальним сценаріям мережевого функціонування.

У статті [9] вивчається МНОШІ архітектура AIDA, орієнтована на промислові IoT-мережі. Запропонована система поєднує МН, оптимізацію та децентралізовану обробку потокових даних, що дозволяє забезпечити стійке функціонування промислових мереж із жорсткими вимогами до затримок і надійності.

Робота демонструє, як ШІ може підтримувати автономність у специфічних промислових сценаріях, хоча автори визнають обмеженість застосування цієї архітектури в умовах гетерогенних телекомунікаційних середовищ.

У статті [10] розглянуто роль ШІ у мережах наступного покоління, з акцентом на здатності ШІ-моделей забезпечувати автономне налаштування мережевих топологій і покращення роботи SDN-контролерів. Автори підкреслюють перспективність автономних рішень у контексті QoS-, SLA- та fault-

tolerance-вимог. Однак робота має переважно концептуальний характер і не надає прототипів або моделей, що можуть бути застосовані на практиці.

Зрештою, у роботі [11] авторам вдалося сфокусуватися на створенні інфраструктурного та інтенційно-орієнтованого датасету для 5G-and-beyond мереж, що відкриває можливості для розроблення високоточних моделей МНОШІ контролю.

Наголошується на важливості деталізованої телеметрії для навчання алгоритмів автономного управління, а також продемонстровано потенціал інтеграції даних у мережеві системи, побудовані за принципом intent-based networking. Однак автори вказують, що практична інтеграція таких моделей у гетерогенні мережі й далі залишається складним завданням.

Проведений аналіз показує, що наукова спільнота активно досліджує застосування ШІ для автоматизації управління мережами, однак залишаються суттєві прогалини.

Попри високі темпи розвитку окремих напрямів, відсутня узагальнена модель управління для МНОШІ, яка зможе забезпечувати цілісний процес переходу від аналізу телеметрії до прийняття і валідації автономних рішень у гетерогенних середовищах.

Недостатньо опрацьованими залишаються питання обґрунтованості рішень, інтегрованої безпеки МН-моделей, роботи з нестабільною телеметрією та захисту від adversarial атак.

Це визначає актуальність подальших досліджень, спрямованих на створення концептуаль-них і технологічних основ для побудови надійних, масштабованих і безпечних мережевих систем МНОШІ.

Постановка мети та завдання. Метою дослідження є розроблення узагальненої моделі впровадження МНОШІ, яка базується на інтеграції телеметричних механізмів, моделей машинного навчання та систем мережевої оркестрації для забезпечення автономного, адаптивного та безпечного управління сучасними мережевими інфраструктурами. Для досягнення поставленої мети необхідно розглянути наступні завдання: проаналізувати сучасний стан традиційної та інтелектуальної мережевої автоматизації; дослідити архітектурні підходи та моделі машинного навчання, що застосовуються в МНОШІ; визначити основні проблеми, виклики та обмеження впровадження МНОШІ; сформувати систему передумов та етапів впровадження автоматизованих моделей управління; проаналізувати практичні приклади застосування моделей МНОШІ у різних галузях.

Виклад основного матеріалу. Послідовність викладу основного матеріалу ґрунтується на науково-технічній логіці переходу від концептуальних засад до прикладної реалізації автоматизованих систем управління мережею на основі ШІ.

Спершу здійснюється порівняльний аналіз традиційних методів мережевої автоматизації та моделей МНОШІ, що дозволяє визначити принципові відмінності у механізмах адаптації, прогнозування та автономності.

Такий підхід є необхідним для виявлення технологічних обмежень класичних систем і формування аргументованих підстав для переходу до інтелектуальної автоматизації. Далі розглядаються ключові виклики та проблеми впровадження МНОШІ, оскільки саме вони визначають вимоги до архітектури даних, стійкості моделей, інтеграційних механізмів та рівня автономії. Послідовне опрацювання цих аспектів створює методологічну основу для формування передумов і етапів впровадження, що відображають технічну еволюцію системи від збору телеметрії до замкненого контуру автономного керування.

Лише після побудови такої логічної рамки стає можливим обґрунтоване подання практичних сценаріїв застосування МНОШІ у реальних галузях, що підтверджує ефективність та універсальність описаної моделі.

Автоматизація МНОШІ та порівняння з традиційною мережевою автоматизацією.

Концепція МНОШІ, формує новий етап еволюції телекомунікаційних систем, у межах якого ШІ виступає ключовим механізмом аналізу, адаптації та автоматизації мережевих процесів. На відміну від традиційних підходів, орієнтованих на статичні правила, ручні конфігурації та реактивне усунення інцидентів, МНОШІ спрямовані на створення динамічного, самонавчального середовища, здатного прогнозувати зміни стану мережі, оптимізувати розподіл ресурсів і приймати рішення в режимі реального часу. Завдяки концепції МНОШІ відбувається зміна парадигми: від реактивного управління мережею до проактивних та автономних систем, що можуть адаптуватися до змін без участі людини. Традиційні методи не передбачають глибокого прогнозування майбутніх сценаріїв, що створює обмеження в умовах високої динаміки трафіку, характерної для 5G/6G-мереж, хмарних платформ та промислових IoT-систем [12]. Основними функціями МНОШІ є інтелектуальний аналіз телеметрії, прогнозування навантажень, виявлення аномалій, оптимізація маршрутів, формування політик безпеки, а також підтримка автономного обслуговування мережевих сервісів. Завдяки використанню алгоритмів МН такі системи здатні переробляти великі обсяги гетерогенних даних, включно з NetFlow-записами, SNMP-показниками, логами, даними OpenTelemetry та поведінковими патернами трафіку. Це дає змогу формувати високоточні профілі мережевої активності та виявляти приховані аномалії, які залишаються непомітними для традиційних систем моніторингу. На рис. 1 показано схему МНОШІ, де відбувається трансформація мережевої інфраструктури за допомогою інтелектуальної автоматизації основних процесів.

Рис. 1. Схема автоматизації МНОШІ на основі ШІ
Джерело: сформовано автором на основі [12]

Запровадження МНОШІ дозволяє подолати ці обмеження, оскільки системи стають здатними автоматично приймати рішення з оптимізацією параметрів мережі, що досягається в залежності від прогнозованих станів і забезпечення автономності різних рівнів – від рекомендаційних механізмів до повністю самокерованих режимів роботи. Переваги такого підходу включають підвищення ефективності використання ресурсів, зменшення кількості інцидентів, мінімізацію людського фактору, покращення операційної прозорості й можливість роботи у масштабних гетерогенних інфраструктурах.

Розглянемо в табл. 1 основні відмінності між традиційною мережевою автоматизацією з реактивним управлінням та автоматизацію МНОШІ з проактивно-інтелектуальними системами.

Таблиця 1

Відмінності між традиційною мережевою автоматизацією та автоматизацію МНОШІ

Фактори	Традиційна мережева автоматизація	Автоматизація МНОШІ
Адаптивність	Працює лише за фіксованим набором правил, через що важко адаптуватися, коли система змінюється або з’являються нові сценарії.	Використовує алгоритми МН для самостійного налаштування, виявлення аномалій та адаптації до змін у режимі реального часу.

Фактори	Традиційна мережева автоматизація	Автоматизація МНОШІ
Швидкість реагування	Реагує на основі заздалегідь визначених тригерів та правил, але непередбачені ситуації часто вимагають ручного втручання інженерів.	Може передбачати проблеми та швидше реагувати, аналізуючи дані та приймаючи проактивні рішення.
Масштабованість	Може масштабуватися, але процес складний. Кожне розширення потребує нових правил і конфігурацій, що може бути трудомістким.	Легко масштабується, оскільки ШІ може обробляти великі дані та оптимізувати ресурси без постійного ручного налаштування.
Надійність	Стабільна у середовищах з незначними змінами та добре працює для повторюваних завдань, але помилки часто виникають, коли умови змінюються.	Забезпечує вищу надійність, оскільки система навчається на основі даних та зменшує кількість помилок, коли змінюються умови мережі.
Безпека	Безпека залежить від правил, визначених людиною, якщо правила неправильні або відсутні, систему можна легко зламати.	Може виявляти аномалії, проактивно запобігати ризикам безпеки та підтримувати постійний моніторинг безпеки.
Вартість	Низькі початкові витрати на прості завдання, але з часом обслуговування та масштабування стають дорогими.	Вимагає початкових інвестицій у ШІ та інфраструктуру, але з часом знижує експлуатаційні витрати завдяки розумній автоматизації.

Джерело: сформовано автором на основі [13]

Проблеми та виклики впровадження МНОШІ для автоматизованого управління мережами

Впровадження концепції МНОШІ супроводжується значними викликами. Найсуттєвіші з них пов’язані з якістю телеметричних даних, складністю інтерпретації роботи моделей, інтеграцією у середовища з різнорідним

обладнанням, а також ризиками впливу змагальних атак на моделі машинного навчання. Це пояснюється тим, що впровадження такої концепції у сучасні телекомунікаційні інфраструктури, попри її значний потенціал містить низку фундаментальних, технічних, організаційних і безпекових проблем. Ці обмеження гальмують перехід від традиційного управління до повністю автономних мережевих систем [1, 5]. Основні проблеми можна згрупувати за кількома критичними напрямами, як показано в табл. 2.

Таблиця 2

Основні проблеми впровадження МНОШІ

Проблеми	Суть проблеми	Ключові виклики та наслідки
Проблеми даних та телеметрії	Неповнота, шумність, фрагментованість телеметрії, де дані надходять з різних джерел (NetFlow, SNMP, SYSLOG), які мають різні формати та тимчасові зсуви.	Відсутність стандартизованих форматів; різна якість даних на обладнанні різних поколінь; необхідність очищення.
	Надвисока швидкість генерування подій у 5G, дата-центрах, IoT.	Неможливість обробки мільйонів подій в реальному часі, потреба у складній потоковій аналітиці.
Обмеження та ризики моделей	«Чорна скринька» моделей – низька інтерпретація глибинних алгоритмів	Аудит рішень є важким; низька довіра інженерів; ризики неконтрольованих конфігурацій.
	Нестійкість до змін середовища.	Втрата точності при новому типі трафіку; помилки у пікових або аварійних умовах; потреба в постійному навчанні та перенавченні.
	Хибні позитивні та негативні рішення.	Блокування легітимного трафіку; порушення SLA; деградація продуктивності.

Проблеми	Суть проблеми	Ключові виклики та наслідки
Інтеграція у гетерогенні інфраструктури	Наявність у мережі традиційних SDN, NFV, 5G та IoT компонентів створює складність інтеграції.	Відсутність універсальних API; різний рівень автоматизації пристроїв; неможливість повної підтримки на основі намірів моделей.
Проблеми автономного прийняття рішень	Негарантована безпека автономних дій	Відсутність перевірок і механізмів відкату; ризик поширення помилок; неоднорідність підходів між вендорами.
	Конфлікти конфігурацій	Дії моделі можуть суперечити політикам безпеки; порушення корпоративних правил; ризики порушення SLA.
Безпекові виклики	Змагальні атаки на моделі ШІ	Підміна даних; обман моделей; крадіжка моделі; наслідком може бути неправильна маршрутизація, обрив трафіку, відкриття векторів атаки.
	Конфіденційність телеметрії	Ризики витоку критичних даних; проблеми відповідності GDPR/ISO.
Обчислювальні та часові обмеження	Висока вартість обчислень, оскільки моделі потребують відеопроцесорів (GPU), тензорного блоку обробки (TPU) та Edge-обробки.	Підвищення CAPEX/OPEX; складність технічного обслуговування.
	Затримка у реальному часі.	ШІ-моделі не завжди вкладаються у 1-10 мс для 5G або 6G та NFT.

Проблеми	Суть проблеми	Ключові виклики та наслідки
Організаційні та кадрові проблеми	Нестача експертизи серед інженерів.	Відсутність навичок роботи з МН; нестача фахівців з MLOps, data engineering.
	Спротив змінам	Недовіра до автоматизації; страх втрати контролю; організаційний саботаж.
Відсутність загальноприйнятих стандартів	Концепція МНОШІ перебуває на ранньому етапі.	Відсутня єдина архітектура; відсутні стандартні протоколи автономії; невизначеність інтеграційних фреймворків.

Джерело: сформовано автором на основі [5, 7, 13]

Передумови та етапи впровадження автоматизації МНОШІ

Впровадження автоматизованих моделей управління МНОШІ є складним, багатоступеневим процесом, що охоплює підготовку телеметричних даних, моделювання, інтеграцію механізмів прийняття рішень та експлуатацію в реальному середовищі. Ефективність цього процесу визначається послідовністю етапів та якістю виконання ключових передумов, які забезпечують можливість створення надійної, адаптивної та кіберстійкої системи управління мережею [5].

Передумови впровадження включають комплексний аналіз існуючої мережевої інфраструктури, визначення цілей автоматизації та формування технічних вимог до системи ШІ. Критичною складовою є організація якісного збору телеметрії, формування уніфікованого масиву даних та побудова масштабованої інфраструктури обробки, що дозволяє навчати та експлуатувати моделі машинного навчання. На основі цих підготовчих елементів розробляються моделі для аналізу, прогнозування, оптимізації та автономного управління, які інтегруються з інструментами оркестрації, контролерами SDN/NFV та системами OSS/BSS.

Для того, щоб краще зрозуміти, як впроваджується автоматизація МНОШІ для автоматичного управління мережами розглянемо спочатку основні передумови (табл. 3), які безпосередньо впливають на етапи впровадження автоматизації на самому підприємстві.

Таблиця 3

Передумови впровадження МНОШІ

Передумови	Пояснення та завдання	Ключовий результат
Оцінювання інфраструктури та визначення цілей автоматизації	Фундамент, який передбачає собою формування технічних вимог і визначення того, які саме мережеві процеси мають бути автоматизовані. Основні завдання охоплюють: 1) аудит існуючої мережевої архітектури; 2) визначення вузьких місць (латентність, пропускна здатність тощо); оцінювання доступних джерел телеметрії; формування цілей автоматизації (автоматичне виявлення аномалій прогнозування навантаження, динамічна політика безпеки тощо).	Технічне бачення системи МНОШІ та набір вимог до моделей ШІ.
Проєктування архітектури збору та обробки телеметрії	Оскільки якість моделей МН напряму залежить від даних важливо побудувати надійну інфраструктуру телеметрії. Для цього виконуються такі завдання: 1) визначення телеметричних джерел (NetFlow/IPFIX, SNMP тощо); 2) забезпечення потокової обробки; стандартизація форматів даних; очищення, нормалізація, агрегування та синхронізація часових міток; 3) створення озера даних (Data Lake) для збереж. та аналізу великих наборів даних (Kafka, Pulsar).	Уніфікований масив телеметрії, придатний для навчання моделей.
Розроблення та навчання моделей НМ	На цьому етапі створюються інтелектуальні моделі для виявлення інцидентів, прогнозування станів або оптимізації конфігурації. Типи моделей охоплюють: для аналізу стану мережі (виявл. аномалій, класиф. трафіку, причинно-наслідковий аналіз); для прогн. (часові ряди, регресія на осн. і МН, графічні нейронні мережі для топологій); для автоном. управ. (навч. з підкріпленням, оптимізація політики); для безп. (виявл. вторгнень, моніт. відповідн. намірам).	Завданням та результ. є вибір оптимальної МН-парадигми залежно від задачі, формування навчальних наборів та оцінювання точності та продуктивності моделей

Передумови	Пояснення та завдання	Ключовий результат
Інтеграція моделей у системи оркестрації та керування	Ключовий перехід від аналітики до автономного управління, що охоплює такі складові процесу: інтеграція з SDN-контролерами, NFV-оркестраторами, системами OSS/BSS; створення API для взаємодії моделей з мережевими компонентами; розроблення механізмів конфігурації на основі намірів; проєктування MLOps-процесів (CI та CD моделей)	Моделі можуть не лише аналізувати стан мережі, але й виконувати реальні дії.
Впровадження контрольованої автономії	На цьому етапі створюється система зворотного зв'язку, де рішення, прийняті моделлю, виконуються автоматично або напівавтоматично. Основні елементи охоплюють: автоматизоване внесення змін у конфігурації маршрутизаторів, комутаторів; механізми безпечного відкату; симуляційне тестування автономності (L1 рекомендації, L2 автоматизація з підтвердженням, L3 часткова автономність, L4 повна автономність).	Формується повноцінна замкнена модель управління мережевими процесами на основі моделей ШІ для конкретних конфігураційних дій.
Моніторинг, валідація та адаптивне перенавчання моделей	Після запуску системи МНОШІ повинна підтримуватися в актуальному, адаптованому до змін стані. З цією метою виконуються завдання: безперервний моніторинг якості моделей; відстеження продуктивності мережі та SLA-показників; періодичне перенавчання моделей; збирання нових даних для покращення точності.	Стійка та еволюційна система автономного управління.
Забезпечення безпеки та кіберстійкості моделей	На завершальному етапі формується комплексний захист системи, де ключовими є захист моделей від змагальних атак, безпечне зберігання телеметричних даних, перевірка відповідності політикам безпеки, аудит рішень та контроль.	створення стійкої та безпечної ШІ-орієнтованої мережевої інфраструктури

Джерело: сформовано автором на основі [12-13]

На основі вищезазначених передумов розглянемо етапи реалізації та впровадження МНОШІ безпосередньо на самому підприємстві.

Послідовність етапів реалізації МНОШІ на підприємстві передбачає початкову перевірку мережевих налаштувань, визначення чітких і вимірюваних цілей, вибір технологій та інструментів із підтримкою API та високою масштабованістю.

Реалізація здійснюється наступним чином.

1. Перевірка поточних налаштувань, де на початку необхідно переглянути всю мережеву інфраструктуру від пристроїв та архітектури до використовуваних API. Команда IT-спеціалістів повинна оцінити можливості збору даних та навички роботи зі ШІ або модельним навчанням (у разі, якщо є прогалини – їх заповнюють за допомогою навчання або найму нових співробітників, перш ніж розпочати проєкт).

2. Визначення цілей, наприклад, скорочення часу реагування на інциденти, підтримка стабільності мережі, покращення продуктивності ключових програм або зниження операційних витрат. Кожна ціль повинна мати вимірювані показники для відстеження прогресу та результатів.

3. Вибір інструментів та технологій, де в якості технологій можна використовувати AIOps для аналізу мережевих даних, хмарні або гібридні хмарні технології для масштабованості, а високопродуктивні обчислення (HPC) або периферійні обчислення можна використовувати для інтенсивної обробки. На цьому етапі необхідно переконатися, що інструменти підтримують інтеграцію API, мають високу надійність та відповідають довгостроковій стратегії.

4. Створення масштабованої інфраструктури даних, оскільки міцна основа даних є ключовою для ШІ. Підприємствам та компаніям потрібен безперервний збір даних, централізоване та масштабоване сховище, а також стандартизовані та зашифровані дані. Щойно дані стануть чистими, чіткими та безпечними, моделі ШІ зможуть надавати точну аналітику.

5. Проведення тестування, де замість того, щоб розгорнути всю систему одразу доцільніше розпочати з обмеженої області мережі. На цьому етапі необхідно автоматизувати прості завдання, такі як налаштування трафіку або виправлення поширених помилок. Після тестування записуються реальні (фактичні) результати, де необхідно порівняти їх з цілями та навчити, перш ніж масштабувати систему.

6. Зробити автоматизацію керованою подіями з налаштуванням сценаріїв, де ШІ миттєво може реагувати на мережеві події. Це включає контроль доступу, моніторинг аномалій, шифрування даних та регулярні аудити. Не менш важливим на цьому етапі є дотримання правил захисту даних, таких як GDPR або HIPAA.

7. Вимірювання, повторення та покращення, де необхідно створити систему відстеження ефективності для порівняння результатів із цілями. На цьому етапі необхідно постійно налаштовувати моделі ШІ з урахуванням нових даних, а також заохочувати випробування технологій з інвестуванням в навчання персоналу з питань ШІ та модельного навчання, щоб залишатися конкурентоспроможними у довгостроковій перспективі.

Для успішного впровадження автоматизації МНОШІ команді впровадження потрібні міцні та глибокі знання в кількох областях: мережі (розуміння архітектури мережі, протоколів маршрутизації та транспортування, а також знайомство з конфігурацією та роботою обладнання), наука про дані, ШІ та модельне навчання (необхідно вміти обробляти великі обсяги даних, фільтрувати та нормалізувати їх, а також створювати та навчати моделі МН для підтримки прийняття рішень), розробка програмного забезпечення (мати практичні навички програмування, використовувати мережеві API та писати скрипти або автоматизовані робочі процеси для інтеграції в щоденні операції).

Тому автоматизація МНОШІ формується як цілісний процес, що поєднує технічну підготовку, аналітичне моделювання, технологічну інтеграцію та організаційну зрілість. Вона забезпечує перехід від традиційного ручного управління до інтелектуальної, саморегульованої мережевої екосистеми, здатної підтримувати високу продуктивність, стійкість та ефективність у сучасних умовах розвитку цифрової інфраструктури.

Приклади практичного застосування моделей автоматизації МНОШІ

Автоматизація мереж, яка побудована на алгоритмах ШІ є ключовим елементом сучасних цифрових екосистем, де моделі МНОШІ забезпечують можливість не лише аналізувати телеметрію та мережеву поведінку в режимі реального часу, але й автономно реагувати на зміни навантаження, усувати збій та оптимізувати використання ресурсів. Системи такого типу здатні поєднувати МН, прогнозну аналітику, механізми виявлення аномалій та адаптивне конфігурування інфраструктури, що робить їх корисними у галузях, де критичними є швидкість реакції, точність і безперебійність роботи.

Завдяки своїй гнучкості та здатності працювати з великими обсягами різнорідних даних, МНОШІ успішно інтегруються у промисловість, телекомунікації, медицину, фінанси та виробничі середовища. Впровадження таких систем дозволяє переходити від традиційних статичних рішень до розумних мережевих платформ, які забезпечують самостійну конфігурацію, самовідновлення та проактивне управління.

Практичне використання МНОШІ демонструє, як теоретичні моделі прогнозування, оптимізації та автономного управління перетворюються на реальні інженерні рішення, здатні функціонувати у складних і динамічних

інфраструктурах. У різних галузях промисловості МНОШІ не лише підвищує ефективність керування мережевими ресурсами, а й забезпечує новий рівень адаптивності завдяки здатності системи самостійно аналізувати телеметрію, виявляти критичні події та приймати оптимальні дії у режимі реального часу. Саме тому технологія активно впроваджується в секторах, де надійність, безперервність та швидкість реакції є визначальними – від медицини та фінансових сервісів до телекомунікацій та промислового виробництва.

Розглянемо застосування моделей автоматизації МНОШІ на прикладі різних форм інтеграції у практичні процеси, зокрема для медицини, фінансів, телекомунікацій та виробництва. Такі приклади моделей спрямовані на те, як інтелектуальна автоматизація трансформує операційні моделі та підвищує рівень автономності мережевих систем.

1. Практичне застосування моделей автоматизації МНОШІ у медичній сфері. Використання МН та ШІ змінює принципи функціонування охорони здоров'я, від догляду за пацієнтами до управління даними. Моделі автоматизації МНОШІ в даному випадку містять периферійні пристрої, або IoT-пристрої, які безпосередньо є ключовими компонентами для збору даних пацієнтів. Сценарій автоматизації такої моделі передбачає собою наступне:

- цілодобовий дистанційний моніторинг пацієнтів, де підключена до медичних або периферійних пристроїв система збирає дані про здоров’я в реальному часі, а ШІ забезпечує виявлення ранніх ознак відхилення та надсилає миттєві сповіщення;
- завдяки використанню IoT-пристроїв пацієнти мають можливість перевіряти важливі показники (артеріальний тиск, частота серцевих скорочень тощо) без необхідності залучення медичного персоналу;
- інтеграція даних та аналітику здоров’я за допомогою ШІ та автоматизації МНОШІ, де дані з медичних пристроїв, рецептів та медичних записів об’єднуються, після чого моделі на основі ШІ здійснюють прогнозування ризиків, що допомагає лікарям у прийнятті рішень.

2. Фінансова галузь використовує ШІ для автоматизації робочих процесів та зниження ризиків, де МНОШІ може застосовуватися для таких сценаріїв:

- застосування МНОШІ для моделі автоматизованої фінансової звітності супроводжується системами, які збирають дані з різних джерел та реєстрів, таких як банківські операції, реєстри обліку та бухгалтерські системи, які перевіряють узгодженість та генерують заплановані звіти;
- моделі кредитного скорингу та ризику на основі ШІ, де на основі історії, профілів клієнтів та їхньої поведінки ШІ призначає кредитні рейтинги та рівні ризику;
- моніторинг транзакцій та виявлення аномалій, де ШІ відстежує транзакціях у внутрішніх мережах, API та банкоматах з метою виявлення

підозрілої активності, шахрайства, збоїв мережі або атак, а згодом запускає автоматичні реакції, наприклад, ізоляція, сповіщення або перенаправлення тощо.

3. Практичне застосування моделей МНОШІ у сфері телекомунікацій є надзвичайно важливим, оскільки телекомунікаційні постачальники використовують ШІ для оптимізації інфраструктури та забезпечення стабільності послуг. В цьому випадку для автоматичного управління можуть застосуватися МНОШІ в декількох аспектах:

1) самовідновлювальні мережі, коли виникають вузькі місця або помилки передачі, де системи автоматично перенаправляє трафік, балансує навантаження або відновлює з'єднання без ручної роботи;

2) мережа на основі намірів, де інженерами встановлюються цілі (наприклад, збільшення пропускної здатності для регіону віртуальної мережі або застосування політики пріоритету відео тощо), а ШІ перетворює їх на конфігурації мережі та розгортає їх;

3) керування якістю периферійних послуг, де ШІ здатний покращити швидке перемикання між технологіями Wi-Fi, 5G та дротовими мережами, а також контролює периферійні програми, наприклад, технології віртуальної та доповненої реальності (AR, VR), IoT, щоб забезпечити безперебійний користувацький досвід.

4. Технологічні підприємства, які займаються виробництвом сировини або товарів використовують сучасне обладнання, зокрема машини, які можуть працювати в поєднанні з ШІ з метою оптимізації процесів та зменшення кількості збоїв обладнання. Моделі МНОШІ можуть використовуватися в якості моніторингу машини в режимі реального часу (датчики збирають дані, відображають стан машини, вимірюють продуктивність та виявляють ранні ознак проблем експлуатації), прогнозного обслуговування (ШІ аналізує дані датчиків, такі як вібрація, температура та звук, щоб прогнозувати несправності або збій та планувати технічне обслуговування завчасно до того, як вони відбудуться), оптимізації виробництва та розумного управління ресурсами (ШІ, яке керує обладнанням економить енергію та відстежує дані про навколишнє середовище та автоматично реагує на зміни).

Висновки. У дослідженні проведено комплексний аналіз концепції МНОШІ, що визначає сучасний етап розвитку телекомунікаційних систем та мережевих технологій. Показано, що традиційні підходи до автоматизації мереж, які засновані на статичних правилах та реактивному управлінні стають недостатніми в умовах зростання масштабованості, динамічності та різнорідності цифрової інфраструктури. Інтеграція моделей МН у процеси управління мережею забезпечує якісно новий рівень автономності, адаптивності та прогнозованості.

Встановлено, що МНОШІ здатні виконувати інтелектуальний аналіз телеметрії, прогнозувати стани мережі, виявляти аномалії, оптимізувати маршрути, автоматично коригувати конфігурації та забезпечувати самовідновлення мережевих сервісів. Розглянуто основні виклики, пов'язані з впровадженням МНОШІ, зокрема проблеми якості даних, інтерпретації моделей, інтеграції у гетерогенні інфраструктури, забезпечення безпеки та кіберстійкості. Проаналізовано передумови та етапи впровадження автоматизації МНОШІ, які охоплюють підготовку телеметричної інфраструктури, проєктування моделей, їх інтеграцію, а також організацію контрольованої автономії. Наведені приклади практичного застосування демонструють ефективність моделей МНОШІ в медицині, фінансовому секторі, телекомунікаціях та виробництві.

Таким чином, МНОШІ формують універсальну платформу для побудови самокерованих мереж наступного покоління, забезпечуючи підвищення ефективності, безпеки, масштабованості та надійності цифрової інфраструктури. Подальші дослідження повинні бути спрямовані на формування єдиних стандартів, розроблення інтерпретованих моделей та інтеграцію механізмів кіберстійкості для забезпечення безпечної експлуатації інтелектуальних мереж на прикладі МНОШІ.

Література:

1. Song L. et al. Networking systems of AI: On the convergence of computing and communications //*IEEE Internet of Things Journal*. – 2022. – Т. 9. – №. 20. – P. 20352-20381. https://doi.org/10.1109/JIOT.2022.3172270

2. Moreno-Sancho A. A. et al. A data infrastructure for heterogeneous telemetry adaptation: application to Netflow-based cryptojacking detection //Annals of Telecommunications. – 2024. – Т. 79. – №. 3. – P. 241-256. https://doi.org/10.1007/s12243-023-00991-6

3. Осіпов, Я. В. Атака нульового дня (n-day attack). Що це і як з цим боротися? // Актуальні питання протидії кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.). – Харків : ХНУВС, 2018. – С. 306-309. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/5596

4. Manevannan Ramasamy. AI-powered network automation: Emerging trends and applications. *World Journal of Advanced Research and Reviews*. – 2025. Т. 26. №. 2. P. 1443-1449. https://doi.org/10.30574/wjarr.2025.26.2.1691

5. Rella B. P. R. et al. AI-Driven Network Optimization for Real-Time Financial Data Streaming in High-Frequency Trading Systems //2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0. – IEEE, 2025. – P. 1-6. https://doi.org/10.1109/OTCON65728.2025.11070794

6. Mistry H. K. et al. Artificial intelligence for networking //Educational Administration: Theory and Practice. – 2024. – Т. 30. – №. 7. – P. 813-821. https://doi.org/10.53555/kuey.v30i7.6854

7. Hamadanian P. et al. A holistic view of ai-driven network incident management //Proceedings of the 22nd ACM Workshop on Hot Topics in Networks. – 2023. – P. 180-188. https://doi.org/10.1145/3626111.362817

8. Umoga U. J. et al. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency //Magna Scientia Advanced Research and Reviews. – 2024. – Т. 10. – №. 1. – P. 368-378. https://doi.org/10.30574/msarr.2024.10.1.0028

9. Chahed H. et al. AIDA—A holistic AI-driven networking and processing framework for industrial IoT applications //Internet of Things. – 2023. – Т. 22. – P. 1-22. https://doi.org/10.1016/j.iot.2023.100805

10. Dandamudi S. R. P. et al. The Role of Artificial Intelligence in Next-Generation Data Networking //International Journal of Advanced Engineering Technologies and Innovations. – Т. 10. – №. 2. – P. 795-806. URL: https://www.neliti.com/publications/603930/the-role-of-artificial-intelligence-in-next-generation-data-networking

11. Andrade-Hoz J., Wang Q., Alcaraz-Calero J. M. Infrastructure-wide and intent-based networking dataset for 5G-and-beyond AI-driven autonomous networks //Sensors. – 2024. – Т. 24. – №. 3. – P. 1-25. https://doi.org/10.3390/s24030783

12. TMA solutions. How AI-driven network automation transforms modern IT systems: TMA case study. – 2025. URL: https://www.tmasolutions.com/insights/ai-driven-network-automation

13. Sukumar Kathirvel. Rise of AI-Driven Networking: Transforming Network Infrastructure Through Intelligent Automation //*vThink. Newsroom. – 2025.* URL: https://www.vthink.co.in/blogs/rise-of-ai-driven-networking-transforming-network-infrastructure-through-intelligent-automation

References:

1. Song, L., Hu, X., Zhang, G., Spachos, P., Plataniotis, K. N., & Wu, H. (2022). Networking systems of AI: On the convergence of computing and communications. *IEEE Internet of Things Journal*, *9*(20), 20352-20381. https://doi.org/10.1109/JIOT.2022.3172270

2. Moreno-Sancho, A. A., Pastor, A., Martinez-Casanueva, I. D., González-Sánchez, D., & Triana, L. B. (2024). A data infrastructure for heterogeneous telemetry adaptation: application to Netflow-based cryptojacking detection. *Annals of Telecommunications*, *79*(3), 241-256. https://doi.org/10.1007/s12243-023-00991-6

3. Osipov, Ya. V. (2018). Ataka nulovoho dnia (n-day attack). Shcho tse i yak z tsym borotysia? [Zero-day attack (n-day attack). What is it and how can it be combated?]. Aktualni pytannia protydii kiberzlochynnosti ta torhivli liudmy : zb. materialiv Vseukr. nauk.-prakt. konf. (Kharkiv, 23 lystop. 2018 r.). Kharkiv, 306-309. Retrieved from: http://dspace.univd.edu.ua/xmlui/handle/123456789/5596 [In Ukrainian].

4. Manevannan Ramasamy (2025). AI-powered network automation: Emerging trends and applications. World Journal of Advanced Research and Reviews, 26(02), 1443-1449. https://doi.org/ 10.30574/wjarr.2025.26.2.1691

5. Rella, B. P. R., Asundi, S., Kumawat, R., Pujari, T. D., Kaushik, K., & Arora, A. S. (2025). AI-Driven Network Optimization for Real-Time Financial Data Streaming in High-Frequency Trading Systems. In *2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0* (pp. 1-6). IEEE. https://doi.org/10.1109/OTCON65728.2025.11070794

6. Mistry, H. K., Mavani, C., Goswami, A., & Patel, R. (2024). Artificial intelligence for networking. *Educational Administration: Theory and Practice*, *30*(7), 813-821. https://doi.org/10.53555/kuey.v30i7.6854

7. Hamadanian, P., Arzani, B., Fouladi, S., Kakarla, S. K. R., Fonseca, R., Billor, D., ... & Chandra, R. (2023, November). A holistic view of ai-driven network incident management.

In *Proceedings of the 22nd ACM Workshop on Hot Topics in Networks* (pp. 180-188). https://doi.org/10.1145/3626111.362817

8. Umoga, U.J., Sodiya, E.O., Ugwuanyi, E.D., Jacks, B.S., Lottu, O.A., Daraojimba, O. D., & Obaigbena, A. (2024). Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. *Magna Scientia Advanced Research and Reviews*, *10*(1), 368-378. https://doi.org/10.30574/msarr.2024.10.1.0028

9. Chahed, H., Usman, M., Chatterjee, A., Bayram, F., Chaudhary, R., Brunstrom, A., ... & Kassler, A. (2023). AIDA—A holistic AI-driven networking and processing framework for industrial IoT applications. *Internet of Things*, *22*, 1-22. https://doi.org/10.1016/j.iot.2023.100805

10. Dandamudi, S. R. P., Sajja, J., Khanna, A., & farooq Mohi-U-din, S. The Role of Artificial Intelligence in Next-Generation Data Networking. *International Journal of Advanced Engineering Technologies and Innovations*, *10*(2), 795-806. URL: https://www.neliti.com/publications/603930/the-role-of-artificial-intelligence-in-next-generation-data-networking

11. Andrade-Hoz, J., Wang, Q., & Alcaraz-Calero, J. M. (2024). Infrastructure-wide and intent-based networking dataset for 5G-and-beyond AI-driven autonomous networks. *Sensors*, *24*(3), 1-25. https://doi.org/10.3390/s24030783

12. TMAsolutions (2025). How AI-driven network automation transforms modern IT systems: TMA case study.. URL: https://www.tmasolutions.com/insights/ai-driven-network-automation

13. Sukumar Kathirvel (2025). Rise of AI-Driven Networking: Transforming Network Infrastructure Through Intelligent Automation //*vThink. Newsroom.* URL: https://www.vthink.co.in/blogs/rise-of-ai-driven-networking-transforming-network-infrastructure-through-intelligent-automation