УДК 004.89:004.056.53 DOI https://doi.org/10.35546/kntu2078-4481.2026.1.47

О. М. СУПРУН
кандидат фізико-математичних наук, доцент,
доцент кафедри інтелектуальних кібернетичних систем
Державний університет «Київський авіаційний інститут»
ORCID: 0000-0002-1196-5655

Я. Я. КРАВЧУК
веб-розробник
ORCID: 0009-0006-1593-9995

О. О. СУПРУН
асистент кафедри інтелектуальних програмних систем
Київський національний університет імені Тараса Шевченка
ORCID: 0000-0002-6243-3720

ГІБРИДНІ АРХІТЕКТУРИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ ПОВЕДІНКОВИХ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ

Актуальність дослідження зумовлена стрімким зростанням обсягів і різноманітності мережевого трафіку, ускладненням архітектур сучасних розподілених мереж та зростанням частоти складних кіберінцидентів, що проявляються у формі поведінкових аномалій. За таких умов традиційні сигнатурні та окремі модельні підходи аналізу трафіку не забезпечують достатньої точності, стійкості й завчасності реагування, що зумовлює потребу в застосуванні комплексних інтелектуальних підходів до прогнозування аномальної мережевої поведінки.

Метою статті є обґрунтування підходів і підвищення ефективності прогнозування поведінкових аномалій у мережевому трафіку на основі використання гібридних архітектур штучного інтелекту (далі – ШІ), здатних забезпечити адаптивне, стійке та випереджальне виявлення аномальної мережевої поведінки в умовах динамічних і гетерогенних мережевих середовищ.

Методи дослідження ґрунтуються на теоретичному аналізі сучасних наукових джерел у сфері ШІ та кібербезпеки, системному підході до дослідження мережевих процесів, логічному узагальненні результатів і порівняльному аналізі підходів до прогнозування аномалій у мережевому трафіку із застосуванням різних класів інтелектуальних моделей.

Результати дослідження свідчать, що ізольоване застосування окремих моделей ШІ є обмежено ефективним у завданнях раннього прогнозування поведінкових аномалій, тоді як їхнє архітектурне поєднання дає змогу комплексно враховувати часові, структурні та контекстні характеристики трафіку. З'ясовано, що гібридні архітектури ШІ підвищують точність і стійкість прогнозів, зменшують чутливість моделей до дрейфу даних і створюють часову перевагу для превентивного реагування. Ідентифіковано основні науково-практичні проблеми впровадження таких рішень, пов'язані з обмеженою якістю навчальних даних, масштабованістю систем, інтерпретованістю результатів і ризиками цілеспрямованого спотворення моделей.

Висновки. Гібридні архітектури ШІ доцільно розглядати як системну основу для інтелектуального аналізу мережевого трафіку, яка забезпечує перехід від реактивного виявлення інцидентів до проактивного, прогнозно-орієнтованого управління кібербезпекою.

Перспективи подальших досліджень пов'язані з поглибленням теоретичних засад побудови гібридних архітектур ШІ, розробленням узгоджених критеріїв оцінювання якості раннього прогнозування та дослідженням підходів до підвищення стійкості інтелектуальних систем аналізу трафіку в розподілених і критичних мережевих інфраструктурах.

Ключові слова: *кібербезпека мереж, раннє виявлення загроз, прогнозний аналіз, адаптивні моделі, аномальна поведінка, розподілені мережі, стійкість моделей, дрейф даних, пояснюваність рішень.*

O. M. SUPRUN
Candidate of Physical and Mathematical Sciences, Associate Professor,
Associate Professor at the Department of Intelligent Cybernetic Systems
State University Kyiv Aviation Institute
ORCID: 0000-0002-1196-5655

Ya. Ya. KRAVCHUK
Web-Developer
ORCID: 0009-0006-1593-9995

O. O. SUPRUN
Assistant at the Department of Intelligent Software Systems
Taras Shevchenko National University of Kyiv
ORCID: 0000-0002-6243-3720

HYBRID ARTIFICIAL INTELLIGENCE ARCHITECTURES FOR PREDICTING BEHAVIORAL ANOMALIES IN NETWORK TRAFFIC

The relevance of this study is driven by the rapid growth in the volume and diversity of network traffic, increasing complexity of modern distributed network architectures, and a rising frequency of sophisticated cyber incidents manifested as behavioral anomalies. Under these conditions, traditional signature-based and isolated model-driven traffic analysis approaches fail to provide sufficient accuracy, robustness, and timeliness of response, which necessitates the adoption of integrated intelligent methods for predicting anomalous network behavior.

The purpose of the article is to substantiate methodological approaches and to improve the effectiveness of predicting behavioral anomalies in network traffic through the use of hybrid artificial intelligence architectures, hereinafter referred to as AI, capable of providing adaptive, robust, and anticipatory detection of anomalous network behavior in dynamic and heterogeneous network environments.

The research methods are based on a theoretical analysis of contemporary scientific sources in the fields of AI and cybersecurity, a systems approach to the study of network processes, logical generalization of results, and comparative analysis of approaches to anomaly prediction in network traffic using different classes of intelligent models.

The research results demonstrate that the isolated application of individual AI models is of limited effectiveness for early prediction of behavioral anomalies, whereas their architectural integration enables comprehensive consideration of temporal, structural, and contextual characteristics of traffic. It is established that hybrid AI architectures improve prediction accuracy and robustness, reduce model sensitivity to data drift, and create a temporal advantage for preventive response. Key scientific and practical challenges in the implementation of such solutions are identified, including limited quality of training data, system scalability, interpretability of results, and risks of targeted model manipulation.

Conclusions. Hybrid AI architectures should be considered a systemic foundation for intelligent network traffic analysis, enabling a transition from reactive incident detection to proactive, prediction-oriented cybersecurity management.

Prospects for further research are associated with deepening the theoretical foundations of hybrid AI architecture design, developing harmonized criteria for evaluating the quality of early prediction, and investigating approaches to enhancing the robustness of intelligent traffic analysis systems in distributed and critical network infrastructures.

Key words: *network cybersecurity, early threat detection, predictive analysis, adaptive models, anomalous behavior, distributed networks, model robustness, data drift, explainability of decisions.*

Постановка проблеми

Стрімка цифровізація суспільства, зростання обсягів передаваних даних і ускладнення архітектур мережевих інфраструктур зумовлюють істотне підвищення вразливості інформаційних систем до поведінкових аномалій у мережевому трафіку, які часто є індикаторами кіберінцидентів, прихованих атак або збоїв у функціонуванні розподілених сервісів. За цих умов традиційні сигнатурні та статистичні методи моніторингу мережі виявляються недостатніми через обмежену здатність адаптуватися до динамічних змін середовища, еволюції загроз і появи нових, раніше невідомих сценаріїв зловмисної поведінки. Актуалізується потреба в застосуванні ШІ як інструменту інтелектуального аналізу мережевого трафіку, здатного виявляти складні нелінійні залежності, навчатися на великих масивах гетерогенних даних та забезпечувати прогнозне виявлення аномалій ще до переходу їх у фазу активної атаки. Водночас застосування окремих моделей ШІ, зокрема лише статистичних, традиційних машинних або глибоких нейронних підходів, не завжди гарантує необхідний рівень точності, стійкості та інтерпретованості результатів у реальних умовах експлуатації мереж. Це зумовлює науково-практичну проблему розроблення гібридних архітектур ШІ, що поєднують переваги різних методів аналізу даних і сприяють підвищенню ефективності прогнозування поведінкових аномалій у мережевому трафіку. Розв'язання цієї проблеми безпосередньо пов'язане з важливими науковими завданнями розвитку інтелектуальних методів кібербезпеки, теорії адаптивних систем та аналізу складних динамічних процесів, а також із практичними завданнями забезпечення стійкості критичних інформаційних інфраструктур, підвищення оперативності реагування на кіберзагрози та зниження ризиків економічних і соціальних втрат у цифровому середовищі.

Аналіз останніх досліджень і публікацій

Огляд сучасних наукових публікацій, присвячених гібридним архітектурам ШІ для прогнозування поведінкових аномалій у мережевому трафіку, засвідчує формування комплексного підходу, що поєднує архітектурні

рішення, методи прогнозування, алгоритми детекції та засоби підвищення інтерпретованості результатів. Важливою передумовою розвитку таких систем є формування масштабованої та гнучкої технологічної основи. У роботі Ю. Бершчанського (Y. Bershchanskyi) та співавт. розглянуто контейнеризований дизайн систем ШІ для хмарних і кіберфізичних середовищ, що забезпечує модульну інтеграцію різнорідних аналітичних компонентів і є основою для реалізації гібридних архітектур аналізу мережевого трафіку [1]. Питання захищеної обробки даних у таких системах доповнюється дослідженням І. Р. Опірського зі співавт., у якому проаналізовано технічні особливості реалізації шифрування даних у середовищі Android, що є принципово важливим для збереження цілісності та конфіденційності мережевих потоків [2]. Організаційно-технологічні аспекти впровадження складних програмних рішень висвітлено в праці І. Хунко (I. Hunko), де обґрунтовано підходи до скорочення часу тестування програмного забезпечення, актуальні для швидкого розгортання гібридних систем аналізу трафіку [3]. Архітектурно-алгоритмічний рівень цієї проблеми доповнюється дослідженням Х. Білала (H. Bilal) та співавт., у якому запропоновано гібридну генеративну архітектуру TrafficAI для симуляції й адаптивного прогнозування трафіку в реальному часі [4].

Значна кількість досліджень зосереджена на розвитку гібридних моделей прогнозування мережевого трафіку, здатних ураховувати часові залежності та нелінійні поведінкові патерни. Зокрема, Т. Х. Альдх'яні (T. H. Aldhyani) та співавтори запропонували інтелектуальну гібридну модель, яка поєднує класичні методи аналізу часових рядів і алгоритми машинного навчання для підвищення точності прогнозування мережевого трафіку [5]. Поглиблення цього підходу простежується в дослідженні Н. Саїні (N. Saini) та співавт., де гібридну ансамблеву модель використано для аналізу поведінкових відхилень і складних атак, що мають прогнозний характер [6]. Інтеграцію часових кореляцій у гібридні схеми аналізу трафіку реалізовано в роботі А. Х. Насрін Фатіма (A. H. Nasreen Fathima) та співавт., де встановлено підвищення точності детекції аномалій через урахування динамічних залежностей у даних [7]. Алгоритмічні можливості ШІ для аналізу аномальної поведінки в мережевій безпеці узагальнено в дослідженні Х. Цао (H. Cao), яке підтверджує доцільність комбінування різних моделей у прогнозному аналізі мережевого трафіку [8].

Окремий блок досліджень присвячено застосуванню гібридних моделей машинного та глибокого навчання безпосередньо для виявлення поведінкових аномалій і вторгнень у мережевому трафіку. Д. К. Редді (D. K. Reddy) та співавт. продемонстрували ефективність глибоких нейронних мереж для аналізу трафіку інтернету речей (Internet of Things, IoT) у контексті інфраструктур «розумних міст» [9]. Поєднання глибинного представлення ознак і часової динаміки реалізовано в гібридній архітектурі DBN–LSTM, яку запропонували А. Чень (A. Chen) та співавт. для детекції поведінкових аномалій у мережевих даних [10]. Просторово-часовий підхід до аналізу трафіку розвинено в роботі В. Ло (W. Lo) та співавт., де гібридна модель системи виявлення вторгнень орієнтована на транспортні мережі [11]. Аналогічну ідеологію поєднання глибоких моделей застосували І. Уллах (I. Ullah) та співавт. для виявлення аномальної активності в IoT-мережах [12].

Завершальний блок робіт стосується узагальнюваності, інтерпретованості та розширення функціональних можливостей гібридних архітектур аналізу мережевого трафіку. С. Даршан (S. Darshan) та співавтори дослідили гібридні підходи до прогнозування та оцінювання аномалій у програмно керованих мережах, наголошуючи на необхідності поєднання різних моделей аналізу в єдиній системі [13]. У комплексному огляді А. Насчіта (A. Nascita) та співавт. систематизовано підходи explainable artificial intelligence у задачах класифікації, прогнозування інтернет-трафіку та виявлення вторгнень, що є критично важливим для практичного впровадження гібридних моделей [14]. В. С. Рао (V. S. Rao) та співавт. продемонстрували ефективність поєднання згорткових нейронних мереж і генеративно-змагальних моделей для виявлення аномалій у мережевому трафіку, підкресливши роль генеративних компонентів у підсиленні детекційних можливостей систем [15].

Попри активне застосування моделей ШІ для аналізу мережевого трафіку, залишаються нерозв'язаними питання раннього прогнозування поведінкових аномалій за умови високої змінності мережевих процесів. Недостатньо обґрунтованими є підходи до поєднання різних методів ШІ в гібридних архітектурах, а також їхня ефективність у розподілених мережевих середовищах. Обмежено досліджено проблеми якості навчальних даних, масштабованості, інтерпретованості прогнозів і стійкості моделей до цілеспрямованого спотворення, що стримує практичне впровадження таких рішень.

У роботі системно проаналізовано можливості ШІ для прогнозування поведінкових аномалій, обґрунтовано доцільність використання гібридних архітектур, а також досліджено їхню ефективність у ранньому прогнозуванні в розподілених мережах. Запропоновано практичні рекомендації щодо впровадження гібридних архітектур ШІ з урахуванням виявлених обмежень, що сприяє підвищенню рівня кібербезпеки та оперативності реагування на аномальні події.

Формулювання мети дослідження

Метою статті є підвищення ефективності прогнозування поведінкових аномалій у мережевому трафіку на основі використання гібридних архітектур ШІ, здатних забезпечити адаптивне, стійке та завчасне виявлення аномальної мережевої поведінки в умовах динамічних і гетерогенних мережевих середовищ.

Для досягнення поставленої мети передбачено розв'язання таких завдань:

1. Проаналізувати можливості застосування моделей ШІ для прогнозування поведінкових аномалій у мережевому трафіку та обґрунтувати доцільність поєднання різних методів ШІ в межах гібридних архітектур з урахуванням змінності мережевих процесів.
2. Дослідити ефективність гібридних архітектур ШІ в завданнях раннього прогнозування поведінкових аномалій у розподілених мережевих середовищах і виявити основні науково-практичні проблеми їхнього застосування.
3. Розробити практичні рекомендації щодо впровадження гібридних архітектур ШІ в системи аналізу мережевого трафіку з метою підвищення рівня кібербезпеки та оперативності реагування на аномальні події.

Викладення основного матеріалу дослідження

Оцінювання можливостей застосування моделей ШІ для прогнозування поведінкових аномалій у мережевому трафіку зумовлюється необхідністю адекватного врахування змінності мережевих процесів, нелінійної природи трафіку та високої динаміки взаємодії між користувачами, сервісами й мережевими протоколами. У сучасних мережах характеристики трафіку змінюються під впливом масштабування хмарних сервісів, поширення IoT-пристроїв, мобільних платформ і зашифрованих каналів передавання даних, що ускладнює формування стабільних шаблонів нормальної поведінки. За цих умов моделі ШІ розглядаються не лише як інструмент класифікації або виявлення відхилень, а як засіб прогнозування майбутніх змін у поведінці трафіку на основі історичних і потокових даних, що дає змогу перейти від реактивних до проактивних механізмів кіберзахисту (табл. 1).

Таблиця 1

Можливості моделей ШІ для прогнозування поведінкових аномалій у мережевому трафіку

Тип моделей ШІ	Основні можливості	Обмеження в умовах змінного трафіку
Статистичні та ймовірнісні моделі	Виявлення базових відхилень від середніх імовірнісних характеристик трафіку	Низька адаптивність до різких змін і складних нелінійних залежностей
Класичні моделі машинного навчання	Класифікація та прогнозування аномалій на основі ознак трафіку	Залежність від якості ознак і необхідність регулярного перенавчання
Глибинні нейронні моделі	Моделювання складних часових і просторових залежностей у трафіку	Висока обчислювальна складність і обмежена інтерпретованість
Послідовні та рекурентні моделі	Прогнозування динаміки трафіку в часовому вимірі	Чутливість до шумів і дрейфу даних
Самонавчальні та адаптивні моделі	Пристосування до нових патернів мережевої поведінки в режимі реального часу	Ризики накопичення помилок і складність контролю навчання

Джерело: сформовано на основі [5, p. 130437; 6; 7, p. 136812; 8, p. 118610; 12, p. 3170].

У практичних умовах експлуатації сучасних мережевих інфраструктур моделі ШІ застосовуються як інструмент прогнозного аналізу, що інтегрується в системи моніторингу трафіку та виявлення вторгнень і працює на основі потокових даних у режимі, близькому до реального часу. Статистичні та ймовірнісні моделі застосовуються для формування базових профілів нормальної поведінки мережі й дають змогу оперативно фіксувати відхилення, спричинені нетиповими сплесками трафіку або порушенням часових закономірностей [12, p. 3170]. Традиційні моделі машинного навчання – для прогнозування ймовірності переходу мережевого стану в аномальний режим на основі наборів агрегованих ознак, що є характерним для корпоративних мереж і центрів обробки даних із відносно стабільною структурою сервісів. Глибинні нейронні та послідовні моделі – у складних розподілених середовищах, де необхідно враховувати довготривалі часові залежності та взаємодію між багатьма потоками, зокрема для раннього виявлення повільних або багатофазних атак, які не проявляються у формі різких аномалій. Адаптивні та самонавчальні моделі ШІ – для корекції прогнозів у разі дрейфу даних, спричиненого змінами конфігурації мережі, появою нових сервісів або зміною поведінки користувачів, що є характерним для хмарних і гібридних інфраструктур. Практична цінність такого підходу полягає в можливості завчасно виявляти потенційно небезпечні тенденції в трафіку та переході від реактивного реагування до проактивного управління мережевою безпекою без надмірного зростання кількості хибних спрацювань [7, p. 136812].

Поєднання різних методів ШІ у межах гібридних архітектур зумовлене необхідністю одночасного врахування різних аспектів мережевої поведінки, які не можуть бути повноцінно охоплені єдиною моделлю. Аномальна мережна поведінка формується під впливом часових змін трафіку, структурних взаємодій між вузлами, протокольних особливостей і контексту використання сервісів, що потребує розподілу аналітичних функцій між кількома взаємопов'язаними компонентами. Гібридні архітектури дають змогу підвищити точність прогнозування через взаємне доповнення моделей, а також забезпечити стійкість результатів у разі зміни режимів роботи мережі або появи нових типів аномалій (табл. 2).

У реальних умовах експлуатації мереж гібридні архітектури реалізуються як багаторівневі системи, де різні компоненти ШІ послідовно або паралельно аналізують трафік із різною глибиною та часовим горизонтом. На етапі попередньої обробки інтелектуальні модулі формують узгоджені представлення даних, що дає змогу прогнозним моделям працювати зі стабільнішими й менш зашумленими ознаками навіть за нерівномірних навантажень або

Таблиця 2

Комбінації методів ШІ в гібридних архітектурах прогнозування аномальної мережевої поведінки

Комбінація методів ШІ	Функціональне призначення в архітектурі	Практичний ефект
Формування ознак + прогнозна модель	виокремлення інформативних характеристик і подальший прогноз	зниження впливу шумів, стабільніші прогнози
Інтерпретований блок + модель прогнозування	контроль логіки прогнозування та оцінювання ризиків	зменшення хибних спрацювань, керованість рішень
Ансамбль різнорідних моделей	паралельне прогнозування та агрегування результатів	стійкість до деградації окремих моделей
Часові моделі + графові компоненти	аналіз динаміки та міжвузлових взаємодій	прогноз поширення аномалій у мережі
Базова модель + механізм адаптації	контроль дрейфу та корекція параметрів	збереження якості у разі зміни трафіку

Джерело: сформовано на основі [5, p. 130440; 6; 7, p. 136815; 10, p. 5; 15, p. 891].

Таблиця 3

Ефективність гібридних архітектур ШІ для раннього прогнозування аномалій у розподілених мережах

Архітектурна схема	Особливості аналізу в розподіленому середовищі	Практичний результат
Локально-глобальна інтеграція	узгодження локальних прогнозів на вузлах	раннє виявлення кумулятивних відхилень
Ієрархічне прогнозування	різні горизонти прогнозу для рівнів мережі	скорочення часу реагування
Децентралізована взаємодія	обмін узагальненими оцінками без сирих даних	стійкість до втрат зв'язку
Прогнозування з випередженням	оцінка майбутніх станів трафіку	превентивне управління
Контекстноорієнтований аналіз	урахування ролі сегмента або сервісу	зниження кількості хибних тривог

Джерело: сформовано на основі [4, p. 8; 9; 11, p. 6; 12, p. 3175; 14, p. 526].

змін структури трафіку. Ансамблеві підходи застосовуються в середовищах зі змішаними типами аномалій, де одні моделі ефективні для короткочасних сплесків активності, а інші – для повільних, тривалих відхилень, що зменшує ризик пропуску складних сценаріїв. Поєднання часових і графових компонентів застосовується в корпоративних та хмарних мережах для прогнозування не лише факту появи аномалії, а і її потенційного поширення між сервісами або сегментами, що є важливим для завчасної локалізації інцидентів [5, p. 130440]. Адаптаційні механізми в складі гібридних архітектур забезпечують контроль дрейфу даних і своєчасне оновлення параметрів моделей, що дає змогу підтримувати стабільну якість прогнозування в умовах постійних змін мережевих конфігурацій і поведінки користувачів без надмірного збільшення обчислювальних витрат.

Ефективність гібридних архітектур ШІ в завданнях раннього прогнозування поведінкових аномалій у розподілених мережевих середовищах зумовлена їхньою здатністю узгоджувати часткові спостереження, отримані на різних рівнях інфраструктури, у цілісне прогностичне уявлення про майбутній стан мережі. За умов асинхронності подій, обмеженої доступності глобальних даних і просторової розподіленості трафіку важливого значення набуває виявлення слабких і непрямих ознак аномальної поведінки, які окремо не мають критичного характеру, але в сукупності формують передумови мережевих інцидентів. Гібридні архітектури дають змогу поєднувати локальні прогностичні оцінки з глобальними механізмами узгодження, що створює основу для завчасного виявлення небезпечних тенденцій у мережевій поведінці (табл. 3).

У сучасних розподілених мережах гібридні архітектури ШІ застосовуються для побудови прогностичних моделей, що працюють у різних часових і просторових масштабах, забезпечуючи синхронізацію локальних спостережень із глобальними закономірностями. Локальні модулі здійснюють швидку оцінку змін поведінки трафіку в межах окремих сегментів або вузлів, тоді як центральні або координаційні компоненти аналізують узгодженість цих змін у ширшому контексті функціонування мережі. У хмарних та міжорганізаційних інфраструктурах такий підхід дає змогу виявляти поступове формування складних аномальних сценаріїв, зокрема синхронізовані відхилення в кількох сервісах, що свідчать про підготовчу фазу атаки або деградацію сервісів [4, p. 8]. Ієрархічна організація прогнозування забезпечує поєднання короткострокових сигналів з довгостроковими тенденціями, що підвищує точність ранніх попереджень і зменшує ризик передчасних або необґрунтованих реакцій. У децентралізованих середовищах практичну цінність має використання узагальнених прогностичних оцінок замість повного обміну даними, що дає змогу зберігати конфіденційність і знижувати навантаження на мережу без втрати прогностичної точності [14, p. 526]. Сукупно це забезпечує системам безпеки часову перевагу для планування адаптивних заходів, локалізації потенційних інцидентів і оптимального розподілу ресурсів до переходу аномальної поведінки в критичну фазу.

Застосування гібридних архітектур ШІ для прогнозування поведінкових аномалій у мережевому трафіку супроводжується низкою взаємопов'язаних науково-практичних проблем, які істотно впливають на перевіреність і стабільність результатів у реальних умовах експлуатації. Однією з основних проблем є обмежена якість і репрезентативність навчальних даних, що проявляється в дисбалансі між нормальними та аномальними класами, неповноті маркування, наявності зашумлених або застарілих зразків і невідповідності історичних даних поточним

режимам роботи мережі. У гібридних архітектурах ця проблема ускладнюється накопиченням похибок між компонентами, коли помилки попередніх модулів поширюються на наступні рівні аналізу та спотворюють прогнозні оцінки. Значним викликом залишається масштабованість рішень, оскільки багатокомпонентні архітектури потребують узгодженої обробки великих обсягів потокових даних у режимі, близькому до реального часу, що зумовлює зростання обчислювальних витрат, затримок та складності розгортання в розподілених середовищах. Додатково виникають проблеми синхронізації між компонентами, балансування навантаження та підтримання стабільної якості прогнозу за умов нерівномірного трафіку. Інтерпретованість гібридних моделей є ще одним критичним аспектом, оскільки поєднання різнорідних методів ШІ часто унеможливлює відстеження причин формування прогнозу, знижує прозорість ухвалення рішень та їхню валідацію фахівцями з кібербезпеки. Це особливо проблематично в середовищах, де результати аналізу використовуються для автоматизованого реагування або мають правові й організаційні наслідки [15, p. 891]. Окрему групу становлять ризики цілеспрямованого викривлення моделей, зокрема через отруєння навчальних даних, маніпуляцію ознаками трафіку або адаптивну поведінку зловмисників, які навмисно формують шаблони, що вводять гібридні системи в оману. У складних архітектурах такі атаки можуть бути локалізованими на окремих компонентах, але мати непропорційний вплив на загальний результат прогнозування.

Упровадження гібридних архітектур ШІ в системи аналізу мережевого трафіку доцільно здійснювати як інженерно керований процес, у якому узгоджуються вимоги кібербезпеки, продуктивності та відтворюваності результатів на всіх етапах життєвого циклу моделі. Практично обґрунтованим є проєктування архітектури на основі принципу функціональної декомпозиції, коли окремі компоненти відповідають за попередню нормалізацію та фільтрацію шумів, формування поведінкових ознак, прогнозування аномалій, оцінювання невизначеності та контекстну валідацію результату з урахуванням мережевих політик. Для зменшення ризику деградації якості в експлуатації необхідно закладати механізми контролю дрейфу даних і регламент оновлення моделей, який поєднує планове перенавчання з подієвими тригерами, наприклад у разі зміни топології, введенні нових сервісів або появі нетипових профілів трафіку. Важливо забезпечувати репрезентативність навчальних вибірок шляхом комбінування історичних логів із контрольованими сценаріями тестування та верифікації, а також мінімізувати вплив дисбалансу класів через коректну постановку метрик і порогів ухвалення рішення, орієнтованих не лише на точність, а й на вартість пропуску інциденту та хибної тривоги.

З позицій оперативності реагування гібридні архітектури доцільно інтегрувати з механізмами автоматизованого реагування на інциденти, однак із керованими рівнями автоматизації: для подій із високою невизначеністю доцільним є напівавтоматичний режим із пріоритизацією, збагаченням контексту і маршрутизацією до аналітика, тоді як для стабільно розпізнаваних сценаріїв – автоматичні дії типу тимчасового обмеження сесій, сегментації доступу або ізоляції вузла в межах політик. Практична ефективність підвищується шляхом упровадження оцінки невизначеності та ансамблевого узгодження прогнозів, що дає змогу ранжувати сповіщення та уникати «перевантаження тривогами» в центрах моніторингу. Для забезпечення масштабованості рекомендовано розгортати компоненти обробки трафіку ближче до джерел даних у критичних сегментах і залишати централізованим рівень узгодження, кореляції та формування управлінського рішення, що зменшує затримки й мережеві витрати без втрати цілісності аналітики.

Окремої уваги потребує інтерпретованість: у практичній реалізації варто забезпечувати пояснювані артефакти для кожного попередження, зокрема перелік основних ознак / тригерів, контекстний профіль вузла або сервісу, часову динаміку відхилення та очікуваний сценарій розвитку події. Це підвищує довіру до рішень ШІ, пришвидшує триаж інцидентів і скорочує час до локалізації першопричини. Для зниження ризиків цілеспрямованого викривлення моделей необхідно застосовувати контроль цілісності даних і каналів збору, виявлення аномалій у самих навчальних потоках, ізоляцію контурів навчання від виробничих контурів, а також регулярні перевірки стійкості до навмисних маніпуляцій трафіком у межах сценарного тестування. У практичному вимірі впровадження має супроводжуватися системою моніторингу якості моделей у часі, де фіксуються зміни метрик, частота хибних спрацювань, затримки обробки та ефективність реагування, а також визначеними критеріями деградації, після яких ініціюється перегляд ознак, компонентів або конфігурації гібридної архітектури. Така організація забезпечує не лише підвищення рівня кібербезпеки, а й кероване скорочення часу виявлення та реагування на аномальні події в умовах сучасних динамічних мережевих середовищ.

Висновки

У результаті дослідження встановлено, що гібридні архітектури ШІ забезпечують принципово вищу ефективність прогнозування поведінкових аномалій у мережевому трафіку порівняно з ізольованими моделями, оскільки дають змогу інтегрувати часові, структурні та контекстні характеристики мережевої поведінки в єдине прогностичне представлення. Доведено, що саме архітектурне поєднання різнорідних методів ШІ створює умови для переходу від реактивного виявлення інцидентів до раннього прогнозування аномальних тенденцій, що підвищує стійкість мереж і забезпечує часову перевагу для превентивного реагування. Водночас ідентифіковано основні науково-практичні проблеми застосування гібридних архітектур ШІ, зокрема обмежену якість і динамічну

нестабільність навчальних даних, накопичення похибок між компонентами, складність масштабування багаторівневих рішень у розподілених середовищах, недостатню інтерпретованість прогнозів і підвищену вразливість до цілеспрямованих адверсаріальних впливів. Показано, що ці проблеми мають системний характер і безпосередньо впливають на надійність та керованість прогнозних рішень у реальних умовах експлуатації. Практичні рекомендації, сформульовані в роботі, обґрунтовують доцільність інженерно керованого впровадження гібридних архітектур ШІ з обов'язковим урахуванням механізмів адаптації, контролю дрейфу даних, оцінювання невизначеності та пояснюваності результатів, а також інтеграції прогнозних модулів із контурами оперативного реагування на інциденти. Перспективи подальших досліджень пов'язані з формалізацією принципів побудови гібридних архітектур, розробленням стандартизованих метрик оцінювання раннього прогнозування та стійкості моделей, а також із поглибленням досліджень захисту гібридних систем ШІ від адверсаріальних впливів у критичних і розподілених мережевих середовищах.

Список використаної літератури

1. Bershchanskyi Y., Klym H., Shevchuk Y. Containerized Artificial Intelligent System Design in Cloud and Cyber-Physical Systems. *Advances in Cyber-Physical Systems*. 2024. Vol. 9, no. 2. P. 151–157. URL: https://doi.org/10.23939/acps2024.02.151 (date of access: 05.01.2026).

2. Опірський І. Р., Хохлачова Ю. Є., Стефанків А. В., Шевчук Ю. А. Аналіз технічних особливостей реалізації шифрування даних на SD-картах в Android. *Сучасний захист інформації*. 2025. Вип. 1, № 61. С. 219–228. DOI: https://doi.org/10.31673/2409-7292.2025.016526

3. Hunko I. How to Effectively Reduce Software Testing Time: From Requirements to Regression. Lodz: Futurity Research Publishing, 2025. 158 p. URL: https://futurity-publishing.com/wp-content/uploads/2025/04/7%D0%9F-29.03.25-3.pdf

4. Hybrid TrafficAI: A Generative AI Framework for Real-Time Traffic Simulation and Adaptive Behavior Modeling / H. Bilal et al. *IEEE Transactions on Intelligent Transportation Systems*. 2025. P. 1–17. URL: https://doi.org/10.1109/tits.2025.3571041 (date of access: 05.01.2026).

5. Intelligent Hybrid Model to Enhance Time Series Models for Predicting Network Traffic / T. H. H. Aldhyani et al. *IEEE Access*. 2020. Vol. 8. P. 130431–130451. URL: https://doi.org/10.1109/access.2020.3009169 (date of access: 05.01.2026).

6. A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection / N. Saini et al. *Concurrency and Computation: Practice and Experience*. 2023. Vol. 35, № 28. Article e7865. URL: https://doi.org/10.1002/cpe.7865 (date of access: 05.01.2026).

7. Nasreen Fathima A. H., Syed Ibrahim S. P., Khraisat A. Enhancing Network Traffic Anomaly Detection: Leveraging Temporal Correlation Index in a Hybrid Framework. *IEEE Access*. 2024. Vol. 12. P. 136805–136824.URL: https://doi.org/10.1109/access.2024.3458903 (date of access: 05.01.2026).

8. Cao H. The detection of abnormal behavior by artificial intelligence algorithms under network security. *IEEE Access: Practical Innovations, Open Solutions*. 2024. Vol. 12. P. 118605-118617. URL: https://doi.org/10.1109/access.2024.3436541 (date of access: 07.01.2026).

9. Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities / D. K. Reddy et al. *Transactions on Emerging Telecommunications Technologies*. 2020. URL: https://doi.org/10.1002/ett.4121 (date of access: 05.01.2026).

10. An efficient network behavior anomaly detection using a hybrid DBN-LSTM network / A. Chen et al. *Computers & Security*. 2022. Vol. 114. P. 102600. URL: https://doi.org/10.1016/j.cose.2021.102600 (date of access: 05.01.2026)

11. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic / W. Lo et al. *Vehicular Communications*. 2022. Vol. 35. P. 100471. URL: https://doi.org/10.1016/j.vehcom.2022.100471 (date of access: 05.01.2026).

12. Nascita A., Aceto G., Ciuonzo D., Montieri A., Persico V., Pescapé A. A Survey on Explainable Artificial Intelligence for Internet Traffic Classification and Prediction, and Intrusion Detection. *IEEE Communications Surveys & Tutorials*. 2025. Vol. 27, № 5. P. 3165–3198. URL: https://doi.org/10.1109/comst.2024.3504955 (date of access: 05.01.2026).

13. Ullah I., Ullah A., Sajjad M. Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks. *IoT*. 2021. Vol. 2, no. 3. P. 428–448. URL: https://doi.org/10.3390/iot2030022 (date of access: 05.01.2026).

14. Darshan S., Radhika N., Radhika G. Predicting and Evaluating Anomaly Detection and Traffic Analysis on Software Defined Networks Using a Hybrid Machine Learning Approach. *Lecture Notes in Electrical Engineering*. Singapore, 2025. P. 521–532. URL: https://doi.org/10.1007/978-981-97-4540-1_38 (date of access: 05.01.2026).

15. AI Driven Anomaly Detection in Network Traffic Using Hybrid CNN-GAN / V. S. Rao et al. *Journal of Advances in Information Technology*. 2024. Vol. 15, no. 7. P. 886–895. URL: https://doi.org/10.12720/jait.15.7.886-895 (date of access: 05.01.2026).

References

1. Bershchanskyi, Y., Klym, H., & Shevchuk, Y. (2024). Containerized Artificial Intelligent System Design in Cloud and Cyber-Physical Systems. *Advances in Cyber-Physical Systems*, *9*(2), 151–157. https://doi.org/10.23939/acps2024.02.151

2. Opirskyi I. R., Khokhlachova Yu. Ye., Stefankiv A. V., Shevchuk Yu. A. (2025) Analiz tekhnichnykh osoblyvostei realizatsii shyfruvannia danykh na SD-kartakh v Android [Analysis of technical features of data encryption implementation on SD cards in Android]. *Suchasnyi zakhyst informatsii*, no. 1 (61), pp. 219–228. DOI: https://doi.org/10.31673/2409-7292.2025.016526

3. Hunko, I. (2025). *How to effectively reduce software testing time: From requirements to regression*. Futurity Research Publishing. https://futurity-publishing.com/wp-content/uploads/2025/04/7%D0%9F-29.03.25-3.pdf

4. Bilal, H., Rehman, A., Aslam, M. S., Ullah, I., Chang, W.-J., Kumar, N., & Almuhaideb, A. M. (2025). Hybrid TrafficAI: A Generative AI Framework for Real-Time Traffic Simulation and Adaptive Behavior Modeling. *IEEE Transactions on Intelligent Transportation Systems*, 1–17. https://doi.org/10.1109/tits.2025.3571041

5. Aldhyani, T. H. H., Alrasheedi, M., Alqarni, A. A., Alzahrani, M. Y., & Bamhdi, A. M. (2020). Intelligent Hybrid Model to Enhance Time Series Models for Predicting Network Traffic. *IEEE Access*, *8*, 130431–130451. https://doi.org/10.1109/access.2020.3009169

5. Saini, N., Bhat Kasaragod, V., Prakasha, K., & Das, A. K. (2023). A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection. *Concurrency and Computation: Practice & Experience*, *35*(28). https://doi.org/10.1002/cpe.7865

6. Nasreen Fathima, A. H., Ibrahim, S. P. S., & Khraisat, A. (2024). Enhancing network traffic anomaly detection: Leveraging temporal correlation index in a hybrid framework. *IEEE Access: Practical Innovations, Open Solutions*, *12*, 136805–136824. https://doi.org/10.1109/access.2024.3458903

7. Cao, H. (2024). The detection of abnormal behavior by artificial intelligence algorithms under network security. *IEEE Access: Practical Innovations, Open Solutions*, *12*, 118605–118617. https://doi.org/10.1109/access.2024.3436541

8. Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2020). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4121

9. Chen, A., Fu, Y., Zheng, X., & Lu, G. (2022). An efficient network behavior anomaly detection using a hybrid DBN-LSTM network. *Computers & Security*, *114*, 102600. https://doi.org/10.1016/j.cose.2021.102600

10. Lo, W., Alqahtani, H., Thakur, K., Almadhor, A., Chander, S., & Kumar, G. (2022). A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. *Vehicular Communications*, *35*, 100471. https://doi.org/10.1016/j.vehcom.2022.100471

11. Nascita, A., Aceto, G., Ciuonzo, D., Montieri, A., Persico, V., & Pescapé, A. (2025). A survey on explainable artificial intelligence for Internet traffic classification and prediction, and intrusion detection. *IEEE Communications Surveys & Tutorials*, *27*(5), 3165–3198. https://doi.org/10.1109/COMST.2024.3504955

12. Ullah, I., Ullah, A., & Sajjad, M. (2021). Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks. *IoT*, *2*(3), 428–448. https://doi.org/10.3390/iot2030022

13. Darshan, S., Radhika, N., & Radhika, G. (2025). Predicting and Evaluating Anomaly Detection and Traffic Analysis on Software Defined Networks Using a Hybrid Machine Learning Approach. In *Lecture Notes in Electrical Engineering* (pp. 521–532). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-4540-1_38

14. Rao, V. S., Balakrishna, R., El-Ebiary, Y. A. B., Thapar, P., Saravanan, K. A., & Godla, S. R. (2024). AI Driven Anomaly Detection in Network Traffic Using Hybrid CNN-GAN. *Journal of Advances in Information Technology*, *15*(7), 886–895. https://doi.org/10.12720/jait.15.7.886-895

Дата першого надходження статті до видання: 05.01.2026
Дата прийняття статті до друку після рецензування: 10.02.2026
Дата публікації (оприлюднення) статті: 30.04.2026