УДК 004.8:004.056.5:621.039.58
DOI https://doi.org/10.32782/2663-5941/2025.3.2/48

Соловій П.С.
Національний університет «Львівська політехніка»

Назаренко В.В.
Національний університет «Львівська політехніка»

ВПРОВАДЖЕННЯ ШІ У СПЕЦІАЛІЗОВАНІ КОМП'ЮТЕРНІ СИСТЕМИ ДЛЯ ПІДТРИМКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті розглянуто теоретичні та практичні аспекти впровадження штучного інтелекту у спеціалізовані комп'ютерні системи, орієнтовані на підтримку функціонування об'єктів критичної інфраструктури. Проаналізовано сучасні підходи до інтеграції інтелектуальних алгоритмів у системи моніторингу, прогнозування загроз та управління інформаційними потоками в умовах підвищених ризиків. Особлива увага приділяється використанню багаторівневих нейронних мереж і методів глибинного навчання, які дозволяють підвищити стійкість комп'ютерних систем до динамічних змін середовища та забезпечити високоточне виявлення потенційних технічних і кіберзагроз.

Висвітлено застосування алгоритмів матричної факторизації для зменшення розмірності даних без втрати критичної інформації, що оптимізує процес прийняття рішень у системах реального часу. Описано механізми роботи багатошарового персептрону із зворотним поширенням помилки для адаптивного навчання моделей прогнозування. Проаналізовано роль метаевристичних методів оптимізації у процесі налаштування комп'ютерних систем безпеки, зокрема в умовах неповноти або надлишковості даних.

Окремо розглянуто можливості використання методів оптимізації ансамблів моделей (МОА) для підвищення узагальнюючої здатності спеціалізованих комп'ютерних систем і забезпечення їх самокорекції на основі безперервного зворотного зв'язку. Акцентовано увагу на перспективах застосування інтелектуальних рекомендаційних систем як одного з компонентів підтримки критичної інфраструктури, зокрема для розподілу ресурсів, прогнозування відмов і формування стратегій управління ризиками.

У підсумку підкреслено, що впровадження штучного інтелекту у спеціалізовані комп'ютерні системи є ключовим чинником підвищення ефективності, надійності та стійкості об'єктів критичної інфраструктури. Запропоновані алгоритмічні рішення сприяють розвитку програмних комплексів нового покоління із вбудованими модулями інтелектуальної підтримки прийняття рішень, що забезпечує адаптивність систем у нестабільних умовах та відкриває нові перспективи їх удосконалення.

Ключові слова: *штучний інтелект, спеціалізовані комп'ютерні системи, критична інфраструктура, глибинне навчання, матрична факторизація, метаевристичні методи оптимізації, рекомендаційні системи.*

Постановка проблеми. Впровадження штучного інтелекту у спеціалізовані комп'ютерні системи для підтримки критичної інфраструктури супроводжується низкою комплексних викликів, пов'язаних із забезпеченням надійності, стійкості та адаптивності таких систем в умовах зростання кількості кіберзагроз та мінливості зовнішнього середовища. Незважаючи на активний розвиток технологій глибинного навчання та алгоритмів машинного аналізу даних, інтеграція цих рішень у реальні системи критичного призначення стикається із суттєвими обмеженнями ресурсів, вимогами до роботи в реальному часі, необхідністю оперативного відновлення функціональності після атак або збоїв.

Однією з ключових проблем є адаптація алгоритмів штучного інтелекту до умов експлуатації спеціалізованих комп'ютерних систем, що повинні забезпечувати безперервне функціонування об'єктів енергетики, транспорту, зв'язку та інших критичних галузей. Стандартні методи оптимізації нейронних мереж, такі як стохастичний градієнтний спуск, часто виявляються недостатньо стійкими до нестабільних вхідних даних та змінних режимів роботи системи, що створює загрозу втрати керованості процесами в умовах надзвичайних ситуацій.

Особливе значення має проблема забезпечення балансу між високою точністю прогнозування та обмеженою пропускною здатністю

комп'ютерних систем, які функціонують у реальному часі. У критичних інфраструктурах недопустима затримка у прийнятті рішень або надмірне навантаження на обчислювальні ресурси, що зумовлює необхідність оптимізації моделей за критеріями енергоефективності, швидкодії та стійкості.

Актуальним є також завдання створення самонавчальних та самовідновлюваних інтелектуальних систем, здатних безперервно адаптуватися до змін у середовищі експлуатації без потреби повного перенавчання. Це вимагає впровадження метаевристичних методів оптимізації, які дозволяють підвищити гнучкість налаштування моделей та забезпечити їхню стійкість у нестабільних і непередбачуваних умовах.

Таким чином, основна проблема полягає у розробці ефективних технологій впровадження штучного інтелекту в архітектуру спеціалізованих комп'ютерних систем для критичної інфраструктури, що забезпечують високу точність аналізу, стійкість до атак і технічних відмов, можливість роботи в реальному часі та адаптивність до змін середовища при мінімальних обчислювальних витратах.

Аналіз останніх досліджень і публікацій. Теоретичні аспекти впровадження штучного інтелекту в спеціалізовані комп'ютерні системи для підтримки критичної інфраструктури були досліджені різними вітчизняними науковцями, які зосереджували увагу на питаннях кібербезпеки, діджиталізації економіки та захисту інформаційного середовища.

Зокрема, М. Гуцалюк у своїй праці проаналізував стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості об'єктів критичної інфраструктури України. Автор відзначив важливість побудови адаптивних інформаційних систем із використанням інструментів штучного інтелекту, які можуть оперативно реагувати на зміну загрозового середовища [1, с. 170]. У дослідженні Н. Ткачук розглянуто процес діджиталізації фінансово-економічної сфери в Україні, зокрема в аспекті впровадження інноваційних інформаційних технологій для підтримки безперервності фінансових процесів, що має безпосереднє відношення до критичної інфраструктури [2, с. 20]. Як зазначено в праці, застосування алгоритмів штучного інтелекту сприяє підвищенню стійкості та гнучкості систем управління у кризових умовах.

Детальне висвітлення використання штучного інтелекту для забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах воєнного стану наведено у статті С. Казьмірука та ін. Дослідники акцентували увагу на необхідності використання моделей машинного навчання для раннього виявлення загроз та оптимізації процесів захисту [3, с. 2]. С. Цяпа проаналізував правові та організаційні механізми захисту критичної інформаційної інфраструктури від кібератак, звертаючи увагу на необхідність інтеграції інтелектуальних систем в існуючі платформи захисту, що забезпечить своєчасне виявлення і нейтралізацію загроз [4, с. 125].

Окрему увагу слід приділити роботі С. Гнатюка та ін., які запропонували концепцію системи корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. Запропоновані підходи базуються на використанні технологій штучного інтелекту для обробки великого обсягу інформації у реальному часі [5, с. 180–182]. Питання захисту економічних систем від кіберзагроз у контексті цифрової трансформації економіки було досліджено Г. Михальченком та ін., які акцентували увагу на потребі створення програмних комплексів на основі нейронних мереж для забезпечення кібербезпеки фінансових установ [6, с. 380].

На міжнародному рівні актуальні проблеми застосування штучного інтелекту для захисту критичної інфраструктури висвітлено у праці G. S. Jadoun та співавторів, де проаналізовано загрози, пов'язані із використанням ШІ у кібербезпеці, і запропоновано контрзаходи, що базуються на автоматизованих системах виявлення атак [7, с. 1–13]. O. Okusi зосередив увагу на можливостях застосування штучного інтелекту та машинного навчання для забезпечення захисту національної критичної інфраструктури, підкресливши важливість розвитку адаптивних моделей реагування [8, с. 1–11]. У роботі A. Chehri, I. Fofana та X. Yang розглянуто підходи до моделювання ризиків для розумних електричних мереж у добу великих даних і штучного інтелекту, що є перспективним напрямом для розвитку енергетичної критичної інфраструктури [9, с. 3196]. Крім того, I. R. Kusumasari та співавтори дослідили проблеми й можливості використання штучного інтелекту як інструменту підтримки прийняття бізнес-рішень у цифрову епоху, що є надзвичайно важливим для стабільності функціонування економічно важливих секторів [10, с. 17].

Таким чином, проведений аналіз свідчить про високий рівень наукового інтересу до теми

інтеграції інтелектуальних систем у структури критичної інфраструктури. Проте, незважаючи на наявність численних досліджень, потребує подальшого розвитку питання комплексного використання метаевристичних методів оптимізації в нейронних мережах для підвищення ефективності програмних рішень у сфері критичної інфраструктури.

Постановка завдання. Метою статті є дослідження теоретичних і практичних аспектів впровадження штучного інтелекту в спеціалізовані комп'ютерні системи для підтримки критичної інфраструктури, з акцентом на застосуванні метаевристичних методів оптимізації в архітектурах нейронних мереж з метою підвищення їхньої ефективності, стійкості та адаптивності в умовах реального часу.

Виклад основного матеріалу. Впровадження штучного інтелекту у спеціалізовані комп'ютерні системи підтримки критичної інфраструктури є одним із ключових напрямів розвитку сучасних інформаційних технологій. Особливість даного процесу полягає у необхідності забезпечення безперервної, надійної та адаптивної роботи систем в умовах змінного загрозового середовища. Для досягнення цього рівня функціонування застосовуються алгоритми машинного навчання, глибинного навчання, метаевристичні методи оптимізації та моделі прогнозування [1, с. 170].

Одним із базових підходів до реалізації інтелектуальної обробки даних у спеціалізованих комп'ютерних системах є використання багатошарових нейронних мереж, що дозволяють формувати складні залежності між вхідними параметрами системи. Багатошарові персептрони (Multilayer Perceptrons, MLP) забезпечують обробку великої кількості змінних за рахунок наявності кількох прихованих шарів, де кожен шар виконує роль нелінійного перетворення простору ознак. Адаптивне навчання таких мереж за допомогою алгоритму зворотного поширення помилки (Backpropagation) забезпечує можливість оперативного оновлення вагових коефіцієнтів моделі на основі надходження нових даних без необхідності повного перенавчання [5, с. 180].

Для систем, що працюють в умовах критичної інфраструктури, особливе значення має використання архітектур, які забезпечують швидку конвергенцію і стійкість до змін вхідних потоків інформації. Серед таких архітектур можна виокремити згорткові нейронні мережі (Convolutional Neural Networks, CNN), що застосовуються для обробки структурованих і частково структурованих даних, а також рекурентні нейронні мережі (Recurrent Neural Networks, RNN) та їхні модифікації, такі як довготривала короткочасна пам'ять (Long Short-Term Memory, LSTM), які призначені для роботи з послідовностями подій у часі [8, с. 5].

У випадках, коли необхідно одночасно враховувати як просторові, так і часові залежності, ефективними виявляються гібридні моделі, що поєднують можливості CNN та LSTM. Наприклад, системи раннього виявлення загроз у мережах критичної інфраструктури застосовують комбіновані архітектури CNN-LSTM для швидкої фільтрації вхідних потоків даних і прогнозування аномалій на основі історичних патернів поведінки мережевих пристроїв [9, с. 3196].

Наявність можливості безперервного оновлення моделей без повного перенавчання має вирішальне значення для забезпечення оперативного реагування на нові типи загроз і змін у структурі даних. Це особливо важливо для комп'ютерних систем, що функціонують у критичних умовах, де швидкість і точність прийняття рішень безпосередньо впливають на надійність і безпеку об'єктів інфраструктури. Підвищення гнучкості моделей за рахунок впровадження сучасних архітектур і адаптивних методів навчання є одним із основних шляхів підвищення ефективності спеціалізованих комп'ютерних систем для підтримки критичних процесів.

Для оптимізації навчання та підвищення стійкості моделей у спеціалізованих комп'ютерних системах підтримки критичної інфраструктури широко використовуються метаевристичні методи оптимізації, що демонструють високу ефективність в умовах складних і багатовимірних просторів рішень. Серед найбільш розповсюджених варто відзначити генетичні алгоритми (Genetic Algorithms, GA), алгоритми рою частинок (Particle Swarm Optimization, PSO) та мурашині алгоритми (Ant Colony Optimization, ACO) (Рис. 1).

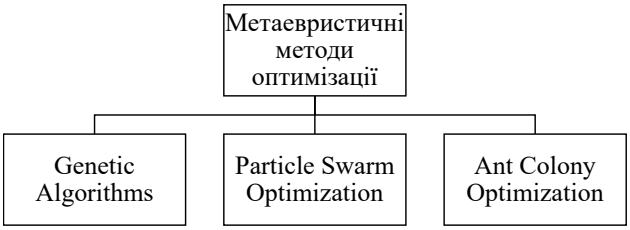

Рис. 1. Метаевристичні методи оптимізації у спеціалізованих комп'ютерних системах підтримки критичної інфраструктури

Генетичні алгоритми (GA) базуються на принципах природного добору та еволюції. Вони імітують біологічні процеси спадковості, мутацій і відбору найкращих рішень для поступового поліпшення характеристик моделей. Застосування GA у спеціалізованих комп'ютерних системах дозволяє ефективно налаштовувати параметри нейронних мереж, забезпечуючи високу адаптивність моделей до нових типів даних без необхідності ручної оптимізації гіперпараметрів.

Алгоритм рою частинок (PSO) моделює колективну поведінку живих істот, наприклад, зграї птахів або косяків риб. У контексті навчання моделей PSO дозволяє координовано досліджувати простір параметрів за рахунок обміну інформацією між «частинками» – можливими рішеннями. Особливістю PSO є висока швидкість збіжності до оптимального рішення, що є критичним фактором у реальному часі для систем підтримки критичної інфраструктури [6, с. 380].

Мурашині алгоритми (ACO) імітують механізми колективної поведінки мурах, які прокладають найкоротші маршрути між джерелом їжі та мурашником, використовуючи феромонні мітки. У комп'ютерних системах ACO дозволяють ефективно вирішувати задачі маршрутизації даних, розподілу навантаження та побудови стійких комунікаційних маршрутів в умовах високої динаміки середовища [10, с. 17].

Застосування зазначених метаевристичних підходів забезпечує подолання обмежень класичних методів оптимізації, таких як стохастичний градієнтний спуск (Stochastic Gradient Descent, SGD), які схильні застрягати у локальних мінімумах, особливо в умовах складних ландшафтів функцій втрат. Метаевристичні алгоритми, завдяки своїй стохастичній природі та можливості глобального пошуку, дозволяють знаходити більш якісні рішення навіть при наявності нерівномірно розподілених або частково зашумлених даних, що є типовим для інформаційних потоків у системах критичної інфраструктури [9, с. 3196].

У процесі впровадження штучного інтелекту у спеціалізовані комп'ютерні системи важливу роль відіграє використання методів матричної факторизації, які дозволяють ефективно зменшити розмірність вхідних даних без втрати критичної інформації. Матрична факторизація (Matrix Factorization) забезпечує поділ великих матриць на декілька менш розмірних матриць, що містять приховані (латентні) особливості вихідних даних. У системах моніторингу критичної інфраструктури це дає змогу підвищити швидкість обробки даних, зменшити обчислювальні навантаження і водночас зберегти релевантність та точність формування рішень [5, с. 179].

Одним із найбільш застосовуваних методів є сингулярне розкладення матриці (Singular Value Decomposition, SVD), яке розкладає матрицю спостережень на добуток трьох менших матриць, що відображають основні напрямки варіацій у даних. Використання SVD дозволяє зосередити аналіз лише на тих компонентах, які несуть максимальну кількість інформації, ігноруючи другорядні шуми або випадкові збурення.

Іншим підходом є метод латентних чинників (Latent Factor Models), який широко використовується у рекомендаційних системах для виявлення прихованих залежностей між об'єктами та ознаками. У контексті підтримки критичної інфраструктури це дозволяє, наприклад, ефективно прогнозувати технічні відмови обладнання на основі неповних або фрагментарних даних, що надходять із сенсорних мереж.

Особливу увагу привертає також метод стохастичної матричної факторизації (Stochastic Matrix Factorization, SMF), що оптимізує процес розкладання для великих потоків даних у режимі реального часу. Використання SMF дозволяє спеціалізованим комп'ютерним системам обробляти великі масиви телеметричної інформації без істотного падіння продуктивності навіть при постійному надходженні нових даних.

Зменшення обсягу оброблюваної інформації без втрати ключових ознак істотно підвищує продуктивність комп'ютерних систем у режимі реального часу, що критично важливо для об'єктів енергетичної, транспортної, фінансової та комунікаційної інфраструктури. В умовах постійних змін і динаміки загроз, оптимізація обчислювальних процесів за допомогою методів матричної факторизації дозволяє не тільки забезпечити швидке прийняття рішень, а й зберегти стабільність та безперервність функціонування критичних об'єктів навіть під час кризових ситуацій.

Прикладом ефективної реалізації такого підходу є системи прогнозування технічних відмов на енергетичних об'єктах, де алгоритми матричної факторизації використовуються для виявлення латентних закономірностей між різними параметрами роботи обладнання [2, с. 22]. За рахунок цього можна своєчасно виявляти аномалії у роботі критичних вузлів і запобігати виникненню серйозних аварій.

Іншою важливою складовою інтеграції штучного інтелекту у спеціалізовані комп'ютерні системи є застосування методів оптимізації ансамблів моделей (MOA). Ансамблювання дозволяє поєднати сильні сторони різних алгоритмів, знижуючи ризик помилкових рішень та підвищуючи стійкість системи до випадкових збурень у даних [4, с. 126]. Застосування MOA особливо ефективне у середовищах із високою динамікою загроз, де окремі моделі можуть не справлятися з новими сценаріями атак.

Практичні приклади впровадження MOA включають системи управління інцидентами в транспортній інфраструктурі, де використання ансамблів моделей дозволяє значно скоротити час виявлення порушень без зниження точності оцінки загроз [5, с. 182]. У результаті досягається підвищення загальної надійності комп'ютерних систем, що обслуговують критичні об'єкти.

З огляду на вимоги роботи у реальному часі, інтеграція глибинного навчання в спеціалізовані комп'ютерні системи передбачає оптимізацію архітектури нейронних мереж. Застосовуються методи редукції глибини мереж без втрати їхньої прогнозної здатності або використання мобільних архітектур, таких як MobileNet, оптимізованих для обмежених обчислювальних ресурсів [6, с. 379]. Це забезпечує можливість використання інтелектуальних функцій навіть на пристроях із середнім рівнем обчислювальної потужності, що характерно для багатьох систем об'єктів критичної інфраструктури.

Окрему увагу приділяють питанням побудови самонавчальних систем, які здатні безперервно адаптувати свої моделі відповідно до змін умов експлуатації. У системах, що підтримують об'єкти критичної інфраструктури, така здатність є ключовою, оскільки дозволяє реагувати на зміну технічних параметрів, поведінкових патернів користувачів чи нові типи загроз без потреби зупиняти роботу або виконувати повне перенавчання моделі. Створення таких систем базується на використанні алгоритмів активного навчання (Active Learning), що дозволяють вибирати найбільш інформативні зразки для донавчання моделей, а також механізмів безперервного контролю за ефективністю моделей у процесі їх функціонування (Continuous Monitoring and Evaluation) [1, с. 172].

Одним із найбільш ефективних підходів є реалізація архітектур з онлайн-навчанням (Online Learning), де модель оновлює свої параметри одразу після надходження кожного нового пакету даних. Такі алгоритми, як Stochastic Gradient Descent (SGD) у режимі онлайн або Adaptive Moment Estimation (Adam) у варіації для потокових даних, дозволяють інтегрувати нову інформацію з мінімальними обчислювальними витратами і без ризику втрати накопиченого досвіду.

Значну роль у побудові самонавчальних систем відіграють алгоритми псевдонагляду (Semi-Supervised Learning) та самоорганізовані карти Кохонена (Self-Organizing Maps, SOM), які дозволяють формувати нові структури класифікації даних на основі непозначених або частково анотованих наборів даних. Це дає можливість системам підтримки критичної інфраструктури своєчасно виявляти нові загрози або аномальні патерни без потреби в постійно актуалізованих вручну еталонних вибірках.

Створення самонавчальних систем також базується на принципах мультиагентних технологій, де окремі підсистеми працюють незалежно і здатні самостійно приймати рішення про необхідність адаптації моделей у відповідь на зміну умов експлуатації. У критичних системах це дозволяє зменшити час реагування на нові типи загроз і забезпечити локальну самовідновлюваність окремих функціональних блоків без втрати загальної працездатності системи. Впровадження таких технологій дозволяє не тільки підвищити точність прогнозування загроз, своєчасно виявляючи нові аномалії у поведінці систем або мереж, але й формує основу для створення адаптивних захисних бар'єрів, які здатні еволюціонувати разом із зміною характеру загроз. Це має особливе значення в умовах функціонування критичних об'єктів, де стабільність, безперервність та оперативність реагування на потенційні ризики є визначальними чинниками загальної безпеки.

Інтеграція штучного інтелекту також суттєво змінює підходи до забезпечення безпеки інформаційних потоків у спеціалізованих комп'ютерних системах, орієнтованих на підтримку критичної інфраструктури. Одним із перспективних напрямів є застосування адаптивних методів шифрування, побудованих на базі нейронних мереж, які використовують механізми глибинного навчання для автоматичної генерації криптографічних ключів та алгоритмів шифрування. Такі підходи дозволяють досягти високого рівня динамічності у захисті даних, забезпечуючи адаптацію криптографічних механізмів до зміни середовища загроз у режимі реального часу [4, с. 127].

Одним із прикладів є використання рекурентних нейронних мереж (Recurrent Neural

Networks, RNN) або їхніх модифікацій, зокрема довготривалої короткочасної пам'яті (Long Short-Term Memory, LSTM), для створення складних шифрувальних схем, що мінімізують ймовірність злому навіть у разі застосування сучасних методів криптоаналізу. Крім того, досліджуються підходи до використання генеративно-змагальних мереж (Generative Adversarial Networks, GAN) для побудови систем шифрування та дешифрування, які унеможливлюють підробку або несанкціоновану модифікацію інформаційних потоків.

Застосування таких технологій забезпечує підвищений рівень захисту даних без надмірного збільшення навантаження на системні ресурси. Завдяки можливості оптимізувати процеси шифрування через машинне навчання, спеціалізовані комп'ютерні системи зберігають високу швидкість обробки інформації, що є критично важливим в умовах обмеженої пропускної здатності або при необхідності роботи у режимі реального часу.

Це особливо важливо для об'єктів критичної інфраструктури, таких як енергетичні системи, транспортні мережі або центри обробки даних, де інформаційні потоки мають високу чутливість, стратегічне значення і потребують максимального рівня захисту як від зовнішніх кібератак, так і від внутрішніх загроз. Використання інтелектуальних механізмів шифрування дозволяє суттєво підвищити рівень кіберстійкості критичних систем, забезпечуючи надійність і безпеку обміну даними навіть у складних умовах інформаційної протидії.

Для систематизації основних напрямків інтеграції штучного інтелекту у спеціалізовані комп'ютерні системи підтримки критичної інфраструктури у таблиці 1 подано узагальнення застосовуваних методів, їх призначення та практичних сфер використання.

Таким чином, впровадження штучного інтелекту в спеціалізовані комп'ютерні системи для підтримки критичної інфраструктури базується на комплексному використанні глибинного навчання, метаевристичних методів оптимізації, матричної факторизації та оптимізації ансамблів моделей. Ефективна інтеграція цих технологій забезпечує підвищення стійкості, надійності та адаптивності об'єктів критичної інфраструктури в умовах зростаючих загроз і нестабільного середовища.

Висновки. У даному дослідженні розглянуто теоретичні та практичні аспекти впровадження штучного інтелекту у спеціалізовані комп'ютерні системи, призначені для підтримки функціонування об'єктів критичної інфраструктури. Проаналізовано можливості застосування глибинного навчання, алгоритмів матричної факторизації, метаевристичних методів оптимізації та технологій ансамблювання моделей для забезпечення стійкості, надійності та адаптивності інформаційних систем у середовищах підвищеного ризику. Доведено, що використання багатошарових нейронних мереж із механізмом зворотного поширення помилки сприяє підвищенню точності прогнозування загроз та оптимізації процесів прийняття рішень у реальному часі. Застосування метаевристичних підходів, таких як генетичні алгоритми та алгоритми рою частинок, забезпечує ефективний пошук оптимальних параметрів моделей у складних та нестабільних середовищах експлуатації. Результати дослідження свідчать про доцільність впровадження матричної факторизації для зменшення розмір-

Таблиця 1

Методи впровадження штучного інтелекту у спеціалізовані комп'ютерні системи критичної інфраструктури

Метод або технологія	Призначення	Приклад застосування
Глибинне навчання	Аналіз великих обсягів даних, виявлення складних залежностей	Системи прогнозування технічних відмов обладнання
Матрична факторизація	Зменшення розмірності даних, оптимізація обчислювань	Оптимізація рішень у системах моніторингу мережевої активності
Метаевристичні методи оптимізації	Пошук глобальних оптимумів у складних просторах рішень	Налаштування параметрів адаптивних нейронних мереж
Оптимізація ансамблів моделей (MOA)	Підвищення точності та стійкості прогнозування	Інтегровані системи виявлення кіберзагроз
Адаптивні методи шифрування на базі ШІ	Захист інформаційних потоків в умовах високої динаміки	Шифрування даних у системах диспетчеризації енергомереж
Самонавчальні системи	Безперервне оновлення моделей без повного перенавчання	Реагування на нові типи атак у критичній інформаційній інфраструктурі

ності вхідних даних без втрати суттєвої інформації, що дозволяє підвищити швидкість роботи спеціалізованих комп'ютерних систем без зниження рівня інформативності результатів. Використання оптимізації ансамблів моделей (МОА) дозволяє суттєво збільшити стійкість систем до випадкових змін у середовищі функціонування та підвищити точність комплексної оцінки загроз. Підкреслено, що створення самонавчальних і самокоригувальних систем на базі ШІ є одним із перспективних напрямів розвитку спеціалізованих комп'ютерних комплексів для критичної інфраструктури. Такі системи здатні безперервно оновлювати свої внутрішні моделі без необхідності повного перенавчання, що є критичним у нестабільних умовах та при обмежених ресурсах. У підсумку впровадження штучного інтелекту у спеціалізовані комп'ютерні системи відкриває нові можливості для забезпечення надійності, безперервності та безпеки функціонування об'єктів критичної інфраструктури. Запропоновані підходи дозволяють підвищити ефективність управління ризиками, оптимізувати використання ресурсів та забезпечити адаптивність систем до постійно змінних умов загрозового середовища.

Список літератури:

1. Гуцалюк М. В. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. *Інформація і право.* 2024. № 2 (49). С. 164–177. DOI: https://doi.org/10.37750/2616-6798.2024.2(49).306199.

2. Ткачук Н. Діджиталізація фінансово-економічної сфери в Україні: стан та перспективи розвитку. *Економічний журнал Волинського національного університету імені Лесі Українки.* 2022. № 3 (31). С. 18–28. DOI: https://doi.org/10.29038/2786-4618-2022-03-18-28.

3. Казьмірук С. Д., Леонов Б. Д., Омельян О. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 6. С. 1–5. DOI: https://doi.org/10.32782/2524-0374/2024-6/49.

4. Цяпа С. М. Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. *Інформація і право.* 2021. № 4 (39). С. 121–128. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248832.

5. Гнатюк С., та ін. Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка.* 2023. № 3 (19). С. 176–196. DOI: https://doi.org/10.28925/2663-4023.2023.19.176196.

6. Михальченко Г. Г., Снітко Ю. М., Іваненко В. О. Кібербезпека в економіці: захист від кіберзагроз у диджиталізованому світі. *Наукові записки Львівського університету бізнесу та права.* 2023. № 38. С. 377–384. DOI: http://dx.doi.org/10.5281/zenodo.10012434.

7. Jadoun G. S., Bhatt D. P., Mathur V., Kaur A. The threat of artificial intelligence in cyber security: risk and countermeasures. *AIP Conference Proceedings.* 2025. Vol. 3191, No. 1. P. 1–13. DOI: https://doi.org/10.1063/5.0248313.

8. Okusi O. Leveraging AI and machine learning for the protection of critical national infrastructure. *Asian Journal of Research in Computer Science.* 2024. Vol. 17, No. 10. P. 1–11. DOI: https://doi.org/10.9734/ajrcos/2024/v17i10505.

9. Chehri A., Fofana I., Yang X. Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability.* 2021. Vol. 13, No. 6. P. 3196. DOI: https://doi.org/10.3390/su13063196.

10. Kusumasari I. R., Putri P. A., Murdiana N., Puspita D. R. Challenges and opportunities for using artificial intelligence as a supporting tool in business decision making in the digital era. *Jurnal Bisnis dan Komunikasi Digital.* 2025. Vol. 2, No. 2. P. 17–17. DOI: https://doi.org/10.47134/jbkd.v2i2.3469.

Solovii P.S., Nazarenko V.V. IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE INTO SPECIALIZED COMPUTER SYSTEMS FOR CRITICAL INFRASTRUCTURE SUPPORT

The article examines the theoretical and practical aspects of implementing artificial intelligence into specialized computer systems aimed at supporting the functioning of critical infrastructure facilities. Modern approaches to integrating intelligent algorithms into monitoring systems, threat forecasting, and information flow management under conditions of elevated risks are analyzed. Special attention is given to the use of multilayer neural networks and deep learning methods, which enhance the resilience of computer systems to dynamic environmental changes and ensure high-precision detection of potential technical and cyber threats.

The application of matrix factorization algorithms for dimensionality reduction without the loss of critical information is highlighted, optimizing decision-making processes in real-time systems. The mechanisms of

multilayer perceptron operations with backpropagation for adaptive model training are described. The role of metaheuristic optimization methods in configuring security-focused computer systems, particularly in conditions of data incompleteness or redundancy, is analyzed.

The article separately addresses the potential of ensemble model optimization methods (EMO) to enhance the generalization capabilities of specialized computer systems and ensure their self-correction based on continuous feedback. Particular emphasis is placed on the prospects of using intelligent recommendation systems as one of the components supporting critical infrastructure, especially for resource allocation, failure prediction, and risk management strategy development.

In conclusion, it is emphasized that the implementation of artificial intelligence in specialized computer systems is a key factor in improving the efficiency, reliability, and resilience of critical infrastructure facilities. The proposed algorithmic solutions contribute to the development of next-generation software systems with integrated decision support modules, providing system adaptability under unstable conditions and opening new perspectives for their further advancement.

Key words: *artificial intelligence, specialized computer systems, critical infrastructure, deep learning, matrix factorization, metaheuristic optimization methods, recommendation systems.*