especially with increasing size n. It was found that increasing the stretch factor s simplifies the attack due to the increase in the number of collisions, while increasing the seed size n, on the contrary, reduces its effectiveness due to the exponential growth of the state space. The results obtained clarify the influence of the predicate structure and parameters of the Goldreich generator on its stability and can serve as a theoretical basis for predicting their behavior with increasing n and designing more secure cryptographic generators.

Keywords: pseudorandom sequence generator, Goldreich generator, cryptanalysis, “guess-and-determine” attack, low locality, nonlinearity, collisions.

Надійшла до редакції (Received): 13.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.8:004.056:004.75 DOI: 10.31673/2409-7292.2026.024106

Костюк Юлія Володимирівна
доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5423-0985
E-mail: y.kostiuk@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7775-6039
E-mail: p.skladannyi@kubg.edu.ua

Кучаковська Галина Андріївна
кандидат педагогічних наук, старший викладач кафедри комп’ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-4555-896X
E-mail: h.kuchakovska@kubg.edu.ua

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА АДАПТИВНОГО ВИЯВЛЕННЯ АНОМАЛІЙ У РОЗПОДІЛЕНИХ СЕРЕДОВИЩАХ НА ОСНОВІ ГІБРИДНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

У статті розглянуто проблему виявлення аномалій у розподілених інформаційних середовищах, що функціонують в умовах динамічних навантажень, високої інтенсивності інформаційних потоків, неоднорідності даних та зростання кіберзагроз. Актуальність дослідження зумовлена розвитком хмарних технологій, Internet of Things (IoT) та систем обробки великих даних, що ускладнює моніторинг стану інформаційних систем і потребує застосування інтелектуальних методів аналізу. Встановлено, що традиційні підходи, засновані на статичних правилах і порогових значеннях, не забезпечують достатньої точності та адаптивності, що призводить до помилкових спрацьовувань або пропуску критичних подій. Метою дослідження є розроблення інтелектуальної інформаційної системи адаптивного виявлення аномалій на основі гібридних моделей штучного інтелекту. Для її досягнення використано нейронні мережі, методи машинного навчання та нечітку логіку. Запропоновано архітектуру системи з модулями збору даних, прогнозування, виявлення аномалій та прийняття рішень. Розроблено математичну модель оцінювання аномалій на основі відхилення між фактичними та прогнозованими параметрами, а також інтегральний показник з урахуванням вразливості та критичності. Реалізовано механізм нечіткого логічного виведення для формування керуючих впливів. Проведено імітаційне моделювання для різних сценаріїв, що підтвердило підвищення точності виявлення аномалій, зменшення помилкових спрацьовувань і скорочення часу реагування системи.

Ключові слова: інтелектуальна інформаційна система; хмарні технології; розподілені системи; виявлення аномалій; машинне навчання; нейронні мережі; нечітка логіка; адаптивні системи; штучний інтелект.

© Горячий О. Я., Юрченко А. О. Аналіз ефективності атаки типу «вгадай та визнач» на генератор псевдовипадкових послідовностей Гольдрайха з модифікованим предикатом P_5. Сучасний захист інформації, 2(66), 41–54. https://doi.org/10.31673/2409-7292.2026.026904

Вступ

Сучасний розвиток інформаційних технологій характеризується стрімким поширенням розподілених обчислювальних середовищ, хмарних сервісів, Internet of Things (IoT) та систем обробки великих даних, що зумовлює істотне зростання складності інформаційних систем [1, 8]. У таких умовах значно підвищується обсяг і швидкість обробки даних, зростає кількість джерел інформації, а також посилюється вплив зовнішніх і внутрішніх факторів, що можуть призводити до виникнення аномальних станів системи. Аномалії можуть бути наслідком як технічних збоїв, перевантажень або помилок конфігурації, так і проявом кіберзагроз, що створює додаткові ризики для стабільності функціонування інформаційних систем підприємства. У зв'язку з цим задача своєчасного та точного виявлення аномалій у розподілених середовищах набуває особливої актуальності.

Традиційні методи виявлення аномалій, що базуються на використанні фіксованих правил, сигнатурного аналізу або порогових значень, мають обмежену ефективність у динамічних умовах функціонування сучасних інформаційних систем. Вони не здатні адекватно враховувати зміну поведінкових характеристик системи, наявність шуму в даних та невизначеність середовища, що призводить до зростання кількості хибних спрацьовувань і зниження загальної надійності моніторингу [2, 7-8, 11]. Це обумовлює необхідність розроблення нових підходів, орієнтованих на використання інтелектуальних методів аналізу даних, здатних забезпечити адаптивність, самонавчання та гнучкість у прийнятті рішень.

Перспективним напрямом розв'язання зазначеної проблеми є застосування гібридних моделей штучного інтелекту, що поєднують можливості нейронних мереж, методів машинного навчання та нечіткої логіки [3, 5, 13]. Такий підхід дозволяє ефективно поєднати здатність до прогнозування складних нелінійних процесів із можливістю інтерпретованого прийняття рішень в умовах невизначеності, що є критично важливим для забезпечення надійного функціонування розподілених інформаційних систем.

Наукова новизна отриманих результатів полягає у розробленні моделі інтелектуальної інформаційної системи адаптивного виявлення аномалій у розподілених середовищах, яка базується на інтеграції прогнозної нейромережевої компоненти, аналітичних методів машинного навчання та механізмів нечіткого логічного виведення [5, 7]. На відміну від існуючих підходів, запропонована модель враховує не лише відхилення між фактичними та прогнозованими параметрами системи, але й рівень вразливості та критичність інформаційних ресурсів, що узгоджується з сучасними підходами до ризик-орієнтованого аналізу в інформаційній безпеці [10, 12, 20] і дозволяє підвищити обґрунтованість прийняття рішень та адаптивність системи до змінних умов функціонування.

Теоретичне значення дослідження полягає у подальшому розвитку методів побудови інтелектуальних інформаційних систем на основі гібридних моделей штучного інтелекту, а також у формалізації процесу виявлення аномалій у розподілених середовищах із урахуванням невизначеності та нелінійного характеру поведінки систем [27-28]. Запропоновані моделі та підходи можуть бути використані як основа для подальших досліджень у галузі аналізу даних, кібербезпеки та адаптивного управління інформаційними системами.

Практичне значення отриманих результатів полягає у можливості застосування розробленої системи для підвищення ефективності моніторингу та управління станом інформаційних систем підприємства, зокрема у хмарних інфраструктурах, IoT-середовищах та розподілених обчислювальних мережах [3-5, 8, 13, 21]. Використання запропонованого підходу дозволяє зменшити кількість помилкових спрацьовувань, підвищити точність виявлення аномалій та скоротити час реагування на критичні події, що сприяє підвищенню загального рівня надійності та безпеки функціонування інформаційних систем.

Аналіз літературних джерел і постановка проблеми

У сучасних дослідженнях проблема виявлення аномалій у розподілених інформаційних системах активно розвивається у контексті застосування методів машинного навчання,

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

глибинного навчання та гібридних підходів. Зокрема, у роботі [1] проведено комплексний огляд методів виявлення аномалій у розподілених IoT-системах, де проаналізовано статистичні, машинні та глибинні підходи. Автори підкреслюють, що ключовими викликами є обробка великих обсягів гетерогенних даних у реальному часі та забезпечення адаптивності моделей до змінних умов функціонування систем.

У дослідженні [2] запропоновано підхід до виявлення аномалій у хмарних середовищах із використанням вбудовування знань у графи (knowledge graph embedding) та методів машинного навчання, що дозволяє враховувати взаємозв'язки між компонентами системи. Водночас у роботі [4] розроблено метод прогнозування аномалій на основі дифузійних моделей, який забезпечує можливість виявлення відхилень до їх фактичного прояву, що є важливим для проактивного управління станом системи. Проте зазначені підходи мають обмеження щодо універсальності застосування та потребують адаптації до різних типів розподілених середовищ.

Суттєвий розвиток отримали мультимодальні підходи до виявлення аномалій. Так, у роботі [5] запропоновано гібридну модель, яка поєднує аналіз логів, метрик та подій із використанням нейронних мереж і механізмів уваги. Отримані результати демонструють підвищення точності виявлення аномалій та зменшення кількості хибних спрацьовувань. Разом із тим автори зазначають, що більшість сучасних моделей орієнтовані на централізовану обробку даних і недостатньо враховують специфіку розподілених систем.

У роботі [3] розглянуто використання федеративного навчання та пояснюваного штучного інтелекту для виявлення аномалій у хмарних мережах, що дозволяє підвищити рівень конфіденційності даних та прозорість прийняття рішень. Подальший розвиток цього напряму представлено у роботі [7], де здійснено систематичний аналіз методів федеративного навчання з точки зору масштабованості, адаптивності та ефективності виявлення аномалій у розподілених середовищах.

Окрему увагу приділено аналізу журналів подій та трасування у розподілених системах. Зокрема, у роботі [8] здійснено комплексний огляд сучасних підходів до виявлення аномалій на основі аналізу логів у розподілених системах, де розглянуто методи машинного та глибинного навчання, підходи до структуризації лог-даних, а також практичні аспекти їх використання в індустріальних середовищах. Автори підкреслюють важливість автоматизованої обробки великих обсягів неструктурованих логів, а також необхідність врахування часових залежностей і контексту подій для підвищення точності виявлення аномалій. Водночас у дослідженні [6] розглянуто застосування методів машинного навчання у розподілених системах комп'ютерного зору, що підкреслює важливість прискорення обробки даних і використання розподілених обчислювальних ресурсів для підвищення ефективності аналітичних систем.

Незважаючи на значну кількість досліджень, існує низка невирішених проблем. По-перше, більшість існуючих підходів орієнтовані на використання окремих методів аналізу (нейронні мережі, графові або статистичні моделі), що обмежує їх ефективність у складних динамічних середовищах. По-друге, недостатньо досліджено питання інтеграції прогнозування, аналізу та прийняття рішень у межах єдиної адаптивної системи. По-третє, залишається відкритою проблема інтерпретованості результатів при використанні складних моделей глибинного навчання [9, 21, 27]. Крім того, більшість підходів не враховують одночасно рівень вразливості та критичність інформаційних ресурсів при оцінюванні аномалій [10, 12, 20], що знижує ефективність управлінських рішень у реальних умовах функціонування систем.

Таким чином, аналіз сучасних наукових праць підтверджує доцільність розроблення гібридних інтелектуальних моделей, які поєднують можливості прогнозування, аналізу багатоджерельних даних та адаптивного прийняття рішень [7, 28], що і визначає напрям дослідження, представленого у даній статті.

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

Сучасні інформаційні системи підприємства все частіше реалізуються у вигляді розподілених середовищ, які поєднують хмарні платформи, мережеві сервіси, IoT-пристрої та різнорідні обчислювальні ресурси [1, 8, 23]. Така архітектура забезпечує високу масштабованість, гнучкість і продуктивність, однак водночас суттєво ускладнює процеси контролю та управління станом системи. В умовах динамічних навантажень, змінної структури інформаційних потоків і неоднорідності джерел даних виникає значна кількість відхилень від нормального режиму функціонування, які можуть свідчити як про технічні збої [15, 17], так і про потенційні кіберзагрози.

Загальна проблема полягає у необхідності забезпечення своєчасного, точного та адаптивного виявлення аномалій у розподілених інформаційних середовищах, що є критично важливим для підтримки стабільності, надійності та безпеки функціонування інформаційних систем підприємства [13, 21]. При цьому складність задачі обумовлюється рядом факторів, зокрема великою кількістю параметрів, що характеризують стан системи, високою швидкістю зміни цих параметрів, наявністю шуму та невизначеності в даних [27], а також нелінійним характером взаємозв'язків між компонентами системи.

Існуючі підходи до виявлення аномалій, що базуються на сигнатурному аналізі, статистичних методах або використанні фіксованих порогових значень, не забезпечують належної ефективності в умовах динамічних розподілених середовищ [8, 25]. Вони є малочутливими до нових типів аномалій, не враховують зміну поведінкових характеристик системи в часі та не забезпечують достатньої адаптивності до умов функціонування [11, 19]. Це призводить до збільшення кількості хибних спрацьовувань або, навпаки, пропуску критичних подій, що негативно впливає на загальну ефективність систем моніторингу та управління. Зазначена проблема безпосередньо пов'язана з важливими науковими та практичними завданнями у галузі інформаційних систем і технологій, зокрема розробленням інтелектуальних систем моніторингу, забезпеченням кібербезпеки, оптимізацією використання ресурсів та підвищенням надійності функціонування розподілених інфраструктур [3, 5, 7]. У практичному аспекті її розв'язання дозволяє забезпечити безперервність бізнес-процесів підприємства, мінімізувати ризики відмов системи та підвищити ефективність реагування на інциденти.

Таким чином, існує об'єктивна потреба у створенні нових підходів до виявлення аномалій, які б поєднували високу точність аналізу даних із здатністю адаптуватися до змінних умов функціонування системи [2, 27]. Це обумовлює необхідність розроблення інтелектуальних інформаційних систем на основі гібридних моделей штучного інтелекту, що дозволяють інтегрувати методи прогнозування, аналізу та прийняття рішень у межах єдиного адаптивного механізму.

Метою статті є розроблення інтелектуальної інформаційної системи адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту, що поєднують методи машинного навчання, нейронні мережі та нечітку логіку, з метою підвищення точності діагностики стану системи, зменшення кількості помилкових спрацьовувань і забезпечення своєчасного реагування на відхилення в умовах динамічної зміни параметрів функціонування. Для досягнення поставленої мети у статті вирішуються такі завдання: аналіз існуючих підходів до виявлення аномалій у розподілених інформаційних системах; розроблення архітектури інтелектуальної системи адаптивного моніторингу; формалізація математичної моделі оцінювання аномалій із урахуванням прогнозованих параметрів, рівня вразливості та критичності ресурсів; розроблення механізму прийняття рішень на основі нечіткого логічного виведення; проведення імітаційного моделювання [24] для оцінки ефективності запропонованого підходу.

Виклад основного матеріалу

Інтелектуальна система адаптивного виявлення аномалій у розподілених середовищах повинна забезпечувати комплексний аналіз стану інформаційної системи з урахуванням

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

динаміки її функціонування, невизначеності даних та багатофакторного впливу зовнішніх і внутрішніх загроз [8, 23]. У запропонованому підході реалізовано гібридну модель, яка поєднує прогнозування поведінки системи на основі нейронних мереж, аналітичне оцінювання відхилень за допомогою математичних моделей та адаптивне прийняття рішень із використанням нечіткої логіки [5, 7, 26-27]. Така інтеграція дозволяє забезпечити не лише виявлення аномалій, але й їх інтерпретацію та формування керуючих впливів у реальному часі.

Запропонована інтелектуальна інформаційна система має модульну архітектуру та включає сукупність взаємопов'язаних функціональних компонентів. Зокрема, система містить модуль збору даних, який забезпечує отримання інформації з різнорідних джерел, таких як мережеві вузли, сервери, сенсори IoT та журнали подій, мережеві телеметричні дані та події безпеки, агреговані засобами SIEM [8, 14, 17]; модуль попередньої обробки та нормалізації, що виконує очищення, узгодження та підготовку даних до подальшого аналізу [11, 25]; модуль прогнозування стану системи на основі нейромережевих моделей, який формує очікувані значення параметрів [4-5]; модуль оцінювання аномальності та ризику, що визначає відхилення від нормального стану та інтегральний показник ризику [10, 12, 20]; модуль нечіткого логічного виведення, який забезпечує прийняття рішень в умовах невизначеності [7, 21]; а також модуль формування та вибору керуючого впливу, що реалізує оптимальну стратегію реагування на виявлені аномалії. Взаємодія зазначених модулів забезпечує реалізацію замкненого циклу адаптивного моніторингу, який охоплює етапи спостереження за станом системи, аналізу та прогнозування, виявлення відхилень, прийняття рішень і корекції параметрів моделі в процесі її функціонування.

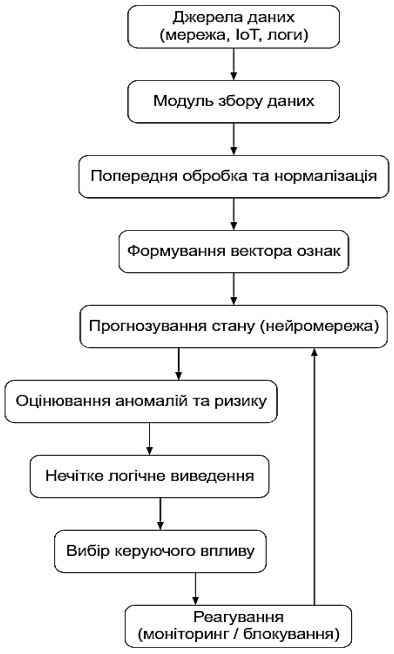

Рис. 1. Архітектура інтелектуальної інформаційної системи адаптивного виявлення аномалій у розподілених середовищах

На рис. 1 подано архітектуру інтелектуальної інформаційної системи адаптивного виявлення аномалій, яка включає послідовні етапи збору даних, попередньої обробки, формування ознак, прогнозування стану системи, оцінювання аномалій і ризику, нечіткого логічного виведення та вибору керуючого впливу. Передбачено зворотний зв'язок від модуля реагування до блоку прогнозування, що забезпечує адаптацію моделі до змін у середовищі.

У процесі дослідження запропоновано інтелектуальну інформаційну систему адаптивного виявлення аномалій у розподілених середовищах, яка базується на гібридному

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

поєднанні методів машинного навчання, нейронних мереж і нечіткої логіки [5, 7, 27]. Формалізація функціонування системи здійснюється шляхом представлення стану розподіленої інформаційної системи у вигляді вектора параметрів:

$$X(t) = \{x_1(t), x_2(t), \dots, x_n(t)\}, \quad (1)$$

де $x_i(t)$ – значення і-го параметра у момент часу t, що характеризує навантаження, затримки, пропускну здатність або інші метрики функціонування системи [17]. Параметри вектора стану формуються на основі даних із різнорідних джерел, зокрема мережевих показників і характеристик трафіку, системних метрик і поведінкових характеристик користувачів [8, 16, 19]. З метою забезпечення коректності подальшого аналізу виконується попередня нормалізація та синхронізація даних у часовому вимірі, що дозволяє узгодити різні масштаби вимірювання та частоту надходження інформації.

На етапі попередньої обробки даних виконується формування узгодженого вектора ознак, який використовується для подальшого аналізу та прогнозування. Зокрема, здійснюється нормалізація параметрів, фільтрація шумових компонентів, агрегація даних у межах часових вікон, а також перетворення сирих подій і логів у структуровані ознаки, придатні для обробки нейромережевими моделями. У результаті формується розширений вектор ознак: $X^*(t)$, який більш повно відображає поточний стан розподіленої системи

Для прогнозування поведінки системи використовується нейромережева модель, результат якої подається як вектор прогнозованих значень: $\hat{X}(t) = \{\hat{x}_1(t), \hat{x}_2(t), \dots, \hat{x}_n(t)\}$, що дозволяє підвищити інформативність ознак та забезпечити більш точне прогнозування стану системи.

Відхилення між фактичними та прогнозованими значеннями визначається як показник аномалії $A(t)$, що обчислюється за формулою:

$$A(t) = \sqrt{\sum_{i=1}^{n} w_i \cdot \left(x_i^*(t) - \hat{x}_i(t)\right)^2}, \quad (2)$$

де $A(t)$ характеризує інтегральну величину відхилення системи від нормального стану, w_i – ваговий коефіцієнт, що відображає значущість і-го параметра. В умовах розподіленого середовища різні параметри системи мають неоднакову діагностичну цінність, зокрема мережеві показники, ресурсні характеристики та поведінкові ознаки можуть по-різному впливати на оцінювання стану системи [5, 13]. Урахування вагових коефіцієнтів дозволяє підвищити чутливість моделі до критичних змін і зменшити вплив другорядних параметрів, що забезпечує більш точне виявлення аномалій. Вагові коефіцієнти можуть визначатися як експертно, так і на основі навчальних даних шляхом оптимізації функції втрат.

Для врахування впливу різних факторів вводиться нормалізований показник аномальності:

$$A_n(t) = \frac{A(t)}{A_{max}}, \quad (3)$$

де A_{max} – максимальне допустиме значення відхилення. Подальше оцінювання стану системи здійснюється з урахуванням рівня вразливості $V(t)$ та критичності ресурсів $C(t)$, що формують інтегральний показник ризику:

$$R(t) = \alpha A_n(t) + \beta V(t) + \gamma C(t), \quad (4)$$

де α, β, γ – вагові коефіцієнти, що визначають значущість відповідних складових. Вагові коефіцієнти α, β, γ можуть визначатися як на основі експертного оцінювання, так і шляхом оптимізації на основі навчальних даних [10, 12, 20]. Така структура інтегрального ризику узгоджується з сучасними ризик-орієнтованими підходами до оцінювання стану інформаційних систем і критичності ресурсів. Це дозволяє адаптувати модель до специфіки

конкретного середовища та забезпечити баланс між чутливістю до аномалій, уразливістю системи та критичністю ресурсів.

Для більш гнучкого та інтерпретованого оцінювання стану системи доцільно перейти від детермінованої оцінки ризику до ймовірнісної інтерпретації аномалії. З цією метою вводиться функція ймовірності виникнення аномального стану, яка визначається на основі логістичної функції:

$$P_{an}(t) = \frac{1}{1+e^{-k(R(t)-R_0)}}, \tag{5}$$

де $P_{an}(t)$ – ймовірність виникнення аномалії, $R(t)$ – інтегральний показник ризику, R_0 – порогове значення ризику, що відповідає переходу системи у критичний стан, k – коефіцієнт чутливості моделі [9, 21]. Запропонована функція дозволяє згладити різкі переходи між станами системи та забезпечити більш стабільне і точне прийняття рішень в умовах невизначеності. Отримане значення ймовірності використовується як додатковий критерій у системі нечіткого прийняття рішень, що підвищує її адаптивність.

Параметри R_0 та k визначаються залежно від особливостей функціонування інформаційної системи та вимог до чутливості моделі. Зокрема, значення R_0 задає пороговий рівень ризику, при якому система переходить у стан підвищеної небезпеки, тоді як коефіцієнт k визначає крутизну логістичної функції та чутливість моделі до змін ризику. Вибір зазначених параметрів може здійснюватися як на основі навчальної вибірки шляхом оптимізації функції втрат, так і експертним шляхом відповідно до допустимого рівня ризику та специфіки розподіленого середовища.

Для відображення динаміки зміни стану системи використовується похідна ризику:

$$\frac{dR(t)}{dt} = \lim_{\Delta t \to 0} \frac{R(t+\Delta t)-R(t)}{\Delta t}, \tag{6}$$

що дозволяє оцінити швидкість розвитку аномалії. На відміну від традиційних підходів, у запропонованій моделі враховується не лише поточний стан системи, але й прогнозована динаміка його зміни. Це дозволяє здійснювати раннє виявлення потенційних аномалій до їх фактичного прояву та забезпечити проактивне реагування. Такий підхід відповідає сучасним методам прогнозного виявлення аномалій і проактивного керування станом системи [4, 5].

З метою класифікації стану системи вводиться функція належності нечітких множин:

$$\mu_A(R) = \begin{cases} 0, & R < R_1 \\ \frac{R-R_1}{R_2-R_1}, & R_1 \le R < R_2, \\ 1, & R \ge R_2 \end{cases} \tag{7}$$

де R_1, R_2 – порогові значення рівня ризику. На основі функцій належності формується база нечітких правил, які визначають логіку прийняття рішень. Наприклад, при високому рівні ризику та швидкому зростанні відхилення система формує критичний рівень реагування, тоді як при середніх значеннях здійснюється моніторинг, безперервна оцінка доступу та часткове обмеження доступу відповідно до принципів Zero Trust [18]. Це дозволяє забезпечити гнучкість і адаптивність керування.

На рис. 2 наведено результати порівняльного аналізу методів кластеризації у вигляді трьох підграфіків, розташованих вертикально, що забезпечує зручність візуального зіставлення їх ефективності. Перший підграфік відображає залежність середньоквадратичної помилки (MSE) від кількості кластерів для методу K-середніх. Спостерігається монотонне зменшення значення MSE зі збільшенням кількості кластерів, що свідчить про підвищення якості кластеризації, проте темп покращення поступово знижується, що вказує на наявність оптимального значення параметра k. Другий підграфік ілюструє результати методу DBSCAN, де показано залежність кількості виявлених кластерів від параметра min_samples. Із

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

зростанням цього параметра кількість кластерів зменшується, що пояснюється підвищенням вимог до щільності даних і, відповідно, укрупненням кластерів або віднесенням частини точок до шуму. Третій підграфік демонструє результати ієрархічного групування, де також спостерігається зниження MSE зі збільшенням кількості кластерів. Характер зміни подібний до методу K-середніх, однак значення помилки дещо відрізняються, що свідчить про відмінності у підходах до формування кластерної структури [25, 28]. Таким чином, представлений рисунок наочно демонструє поведінку різних методів кластеризації залежно від їх параметрів та дозволяє обґрунтовано обрати оптимальні налаштування для задачі аналізу даних.

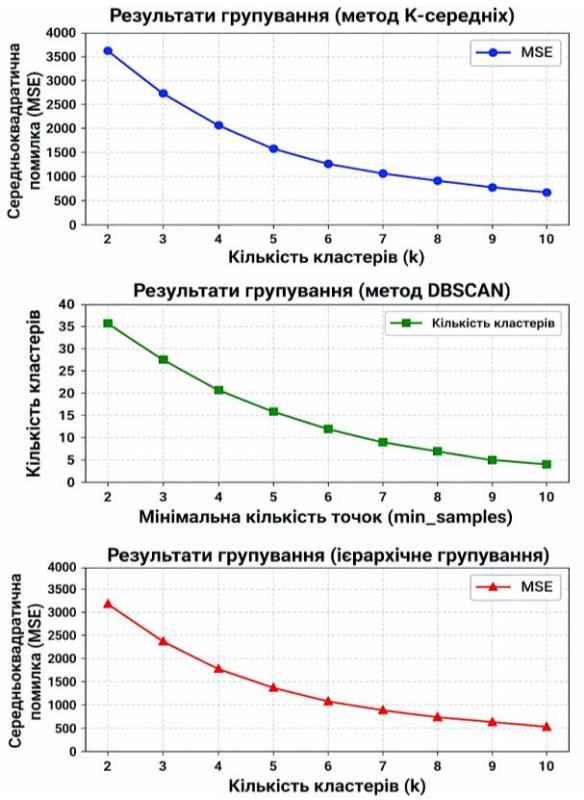

Рис. 2. Функції належності нечітких змінних ризику R(t) та керуючого впливу U(t) у системі адаптивного виявлення аномалій

На основі отриманих значень формується керуючий вплив $U(t)$, який визначається як результат нечіткого логічного виведення:

$$U(t) = \sum_{j=1}^{m} w_j \cdot u_j, \tag{8}$$

де w_j – ваги правил, u_j – відповідні дії системи. Отриманий керуючий вплив інтерпретується у вигляді конкретних управлінських дій, таких як моніторинг, динамічне обмеження доступу, локалізація аномалії або повне блокування [7, 18, 21]. Це забезпечує практичну реалізацію системи та можливість її інтеграції у реальні інформаційні середовища.

З метою підвищення обґрунтованості прийняття рішень у системі вводиться функція оптимального вибору керуючого впливу, яка дозволяє визначити найбільш ефективну дію з урахуванням поточного рівня ризику та витрат на реагування:

$$U^*(t) = \arg\min_{u \in D}(\lambda_1 R(t) + \lambda_2 Cost(u)), \tag{9}$$

де $U^*(t)$ – оптимальний керуючий вплив, D – множина допустимих дій системи, $Cost(u)$ – функція вартості або ресурсних витрат для реалізації дії u, λ_1, λ_2 – вагові коефіцієнти, що

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

визначають баланс між рівнем ризику та витратами на реагування [10, 12, 20]. Запропонований підхід дозволяє не лише реагувати на аномалії, але й здійснювати раціональний вибір дій, мінімізуючи сукупні втрати системи та забезпечуючи ефективне використання ресурсів.

Важливим елементом запропонованої моделі є інтеграція ймовірнісної оцінки аномалії у процес прийняття оптимального рішення. Зокрема, значення $P_{an}(t)$ використовується для коригування вагових коефіцієнтів у функції оптимізації, що дозволяє адаптувати стратегію реагування залежно від рівня невизначеності та ризику. У цьому випадку функція оптимального керування може бути уточнена таким чином:

$$U^*(t) = \arg\min_{u \in D}(\lambda_1 P_{an}(t) + \lambda_2 Cost(u)), \tag{10}$$

де $P_{an}(t)$ – ймовірність виникнення аномалії, $Cost(u)$ – функція витрат на реалізацію керуючої дії u, λ_1, λ_2 – вагові коефіцієнти, що визначають баланс між рівнем загрози та витратами на реагування [9, 21, 27]. Такий підхід дозволяє забезпечити більш гнучке та адаптивне прийняття рішень, оскільки при зростанні ймовірності аномалії система надає пріоритет швидкому реагуванню, тоді як при низьких значеннях ймовірності – мінімізує зайві витрати ресурсів. Запропонована інтеграція дозволяє перейти від детермінованого реагування до ймовірнісно-адаптивного управління станом системи.

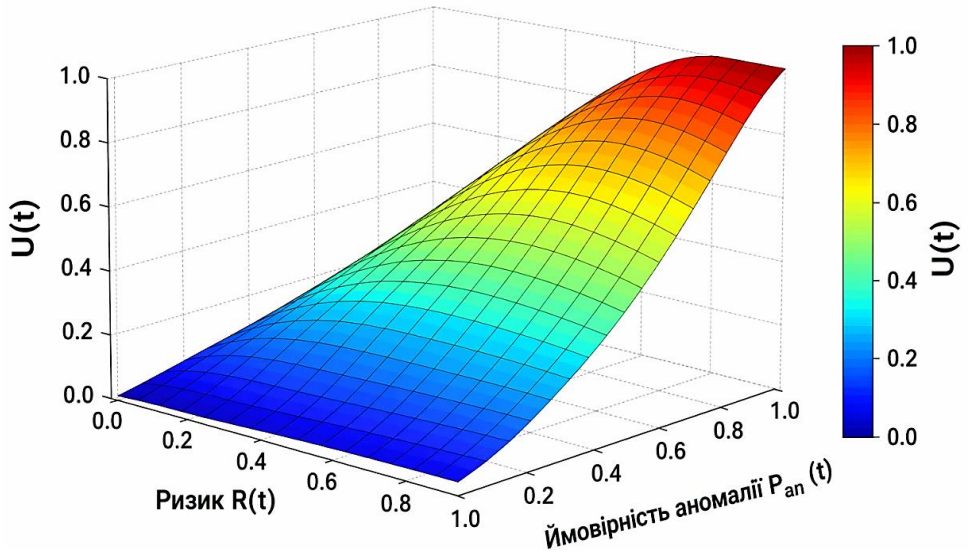

Рис. 3. Поверхня залежності керуючого впливу U(t) від ризику R(t) та ймовірності аномалії $P_{an}(t)$

На рис. 3 наведено поверхню залежності керуючого впливу $U(t)$ від інтегрального показника ризику $R(t)$ та ймовірності виникнення аномалії $P_{an}(t)$. Поверхня має виражений нелінійний характер, що відображає складний взаємозв'язок між рівнем загрози та інтенсивністю реагування системи [27-28]. Зі зростанням ризику та ймовірності аномалії значення $U(t)$ монотонно зростає, що відповідає переходу системи до більш інтенсивних керуючих дій. Найвищі значення $U(t)$ спостерігаються в області високого ризику та високої ймовірності аномалії, що відповідає критичному режиму функціонування системи та необхідності негайного реагування.

Отримане оптимальне значення керуючого впливу $U^*(t)$ є безперервною величиною, яка потребує інтерпретації у вигляді конкретних управлінських дій. З цією метою вводиться множина дискретних рішень $D = \{d_1, d_2, d_3, d_4\}$, де d_1 відповідає пасивному моніторингу стану системи, d_2– підвищеному контролю та обмеженню доступу, d_3 – локалізації аномального сегмента на основі графового аналізу взаємозв'язків між компонентами

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

середовища [22], а d_4 – повному блокуванню або аварійному реагуванню. Відображення безперервного значення $U^*(t)$ у множину дискретних дій здійснюється на основі порогових значень, що дозволяє забезпечити узгодження математичної моделі з практичними механізмами функціонування інформаційної системи [13, 21]. Такий підхід забезпечує перехід від оптимізаційного формулювання задачі до реалізації адаптивного управління станом системи в реальних умовах. Граничні значення переходу між діями можуть адаптивно змінюватися залежно від історії функціонування системи.

Рис. 4. Схема функціонування моделі адаптивного виявлення аномалій і вибору керуючого впливу

На рис. 4 подано схему функціонування моделі адаптивного виявлення аномалій, яка відображає послідовність етапів обробки даних: від збору та попередньої обробки інформації до прогнозування стану системи, оцінювання рівня аномальності та ризику, формування керуючого впливу й вибору оптимальної дії реагування. Залежно від наявності критичного стану система переходить до локалізації загрози або блоку моніторингу, після чого виконується адаптація параметрів моделі.

Для підвищення адаптивності системи вводиться функція корекції параметрів:

$$\theta(t+1) = \theta(t) + \eta \cdot \nabla L(t), \tag{11}$$

де θ – параметри моделі, η – швидкість навчання, $L(t)$ – функція втрат. У процесі навчання коригуються параметри нейромережевої моделі, що відповідають за точність прогнозування стану системи, а також параметри функцій оцінювання аномалій [27]. Це дозволяє системі адаптуватися до змінних умов функціонування та підвищувати ефективність виявлення відхилень.

Теоретичне значення отриманих результатів полягає у формалізації багаторівневого процесу адаптивного виявлення аномалій у розподілених інформаційних середовищах. Запропонована модель інтегрує прогнозні, ризик-орієнтовані, ймовірнісні та нечітко-логічні механізми оцінювання стану системи, що дозволяє описати складні нелінійні процеси її

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

функціонування в умовах невизначеності [5, 7, 27]. Такий підхід забезпечує узгодження різних рівнів аналізу – від обробки даних і прогнозування до прийняття рішень – у межах єдиної формалізованої структури, що розширює теоретичні засади побудови інтелектуальних інформаційних систем адаптивного типу.

Оцінювання ефективності роботи системи здійснюється за допомогою метрик точності:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \tag{12}$$

де TP, TN, FP, FN – кількість істинно позитивних, істинно негативних, хибно позитивних та хибно негативних результатів. Додатково використовується F1-міра:

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision+Recall}, \tag{13}$$

що дозволяє комплексно оцінити якість класифікації. Для визначення часу реагування системи вводиться показник:

$$T_r = t_{response} - t_{detection}, \tag{14}$$

де $t_{detection}$ – момент виявлення аномалії, $t_{response}$ – момент реакції системи. Таким чином, запропонована модель забезпечує інтеграцію прогнозування, оцінювання ризику та адаптивного прийняття рішень [25], що дозволяє підвищити ефективність виявлення аномалій у розподілених інформаційних середовищах [26].

Для оцінювання ефективності запропонованої моделі проведено імітаційне моделювання її функціонування в умовах розподіленого середовища. Дослідження виконано на синтетично згенерованих та частково реальних даних, що відображають типові режими роботи інформаційної системи.

Для оцінювання ефективності запропонованої моделі проведено імітаційне моделювання її функціонування в умовах розподіленого середовища [5, 8, 25]. З метою систематизації умов експерименту та забезпечення формалізованого аналізу було виділено три базові сценарії, що відповідають типових режимам роботи інформаційної системи. Узагальнена характеристика сценаріїв, відповідних значень показників та реакцій системи наведена в табл. 1.

Таблиця 1

Характеристика сценаріїв імітаційного моделювання функціонування системи

Сценарій	**Вхідні умови (параметри)**	**Значення показників $A_n(t)$, $R(t)$**	**$P_{an}(t)$**	**Оптимальна дія $U^*(t)$**	**Тип реагування**
S1	Нормальне навантаження, стабільний трафік, відсутність аномалій	$A_n(t) \approx 0.05 - 0.15$; $R(t)$ – низький	Низька (≈0–0.2)	$u \to min$	Пасивний моніторинг d_1
S2	Перевантаження: зростання трафіку, затримок, зниження пропускної здатності	$A_n(t) \approx 0.3 - 0.6$; $R(t)$ – середній	Середня (≈0.3–0.7)	$u \to$ середнє	Підвищений контроль d_2
S3	Аномальна активність: різкі відхилення параметрів, атака	$A_n(t) \approx 0.7 - 1.0$; $R(t)$ – високий	Висока (≈0.8–1)	$u \to max$	Локалізація / блокування $d_3 - d_4$

Як наведено в табл. 1, кожен сценарій характеризується відповідними значеннями показників аномальності, інтегрального ризику та ймовірності виникнення аномалії, що безпосередньо впливає на вибір оптимального керуючого впливу системи. У нормальному

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

режимі функціонування система підтримує пасивний моніторинг, тоді як у разі перевантаження переходить до режиму підвищеного контролю. У сценарії аномальної активності формується критичний керуючий вплив, спрямований на локалізацію або блокування загрози. Це підтверджує здатність запропонованої моделі адаптивно змінювати поведінку залежно від поточного стану середовища.

З метою комплексного аналізу було розглянуто три основні сценарії функціонування системи: нормальний режим роботи, режим перевантаження обчислювальних ресурсів та сценарій аномальної активності, що відповідає поширеним підходам до експериментального оцінювання систем виявлення аномалій [5, 8, 24, 25]. У першому сценарії система демонструє стабільну поведінку з низьким рівнем хибних спрацьовувань, що підтверджує її здатність коректно ідентифікувати нормальний стан. У другому сценарії, що відповідає зростанню навантаження, спостерігається підвищення інтегрального показника ризику, внаслідок чого система адаптивно переходить до режиму підвищеного контролю та часткового обмеження доступу. У третьому сценарії, який моделює аномальну активність або атаку, система формує критичний керуючий вплив із пріоритетом швидкого реагування, що включає локалізацію або блокування відповідного сегмента [18, 22].

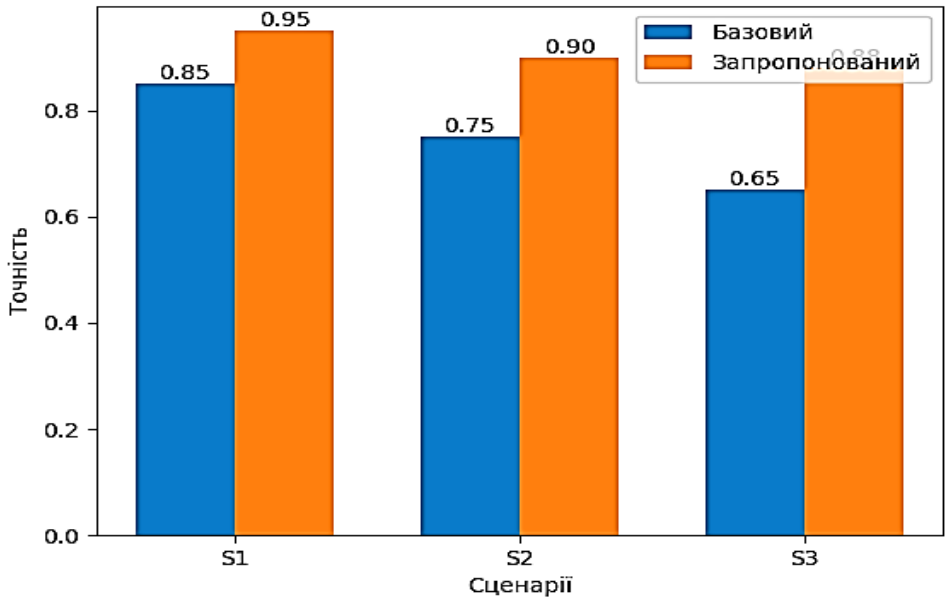

Рис. 5. Порівняння ефективності базового та запропонованого підходів у сценаріях моделювання S1–S3

На рис. 5 наведено порівняння ефективності базового та запропонованого підходів у сценаріях моделювання S1–S3. Як видно з представлених результатів, запропонований підхід демонструє стабільно вищі значення точності виявлення аномалій у всіх розглянутих сценаріях. Зокрема, у нормальному режимі (S1) спостерігається незначний приріст ефективності, що свідчить про коректну ідентифікацію штатного стану системи. У сценарії перевантаження (S2) та аномальної активності (S3) різниця між підходами суттєво зростає, що підтверджує здатність запропонованої моделі адаптивно реагувати на зміни стану середовища та більш ефективно виявляти відхилення.

На рис. 6 представлено приріст ефективності запропонованого підходу відносно базового у сценаріях S1–S3. Аналіз результатів показує, що найбільший приріст ефективності досягається у сценарії аномальної активності (S3), де він становить близько 0.23, що свідчить про високу результативність моделі в умовах критичних відхилень. У сценарії перевантаження (S2) приріст становить приблизно 0.15, що також підтверджує здатність системи адаптуватися

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

до змін навантаження. У нормальному режимі (S1) приріст є мінімальним (близько 0.10), що є очікуваним і вказує на відсутність надмірного реагування системи у стабільних умовах. Отримані результати підтверджують ефективність використання гібридних моделей штучного інтелекту для підвищення якості виявлення аномалій.

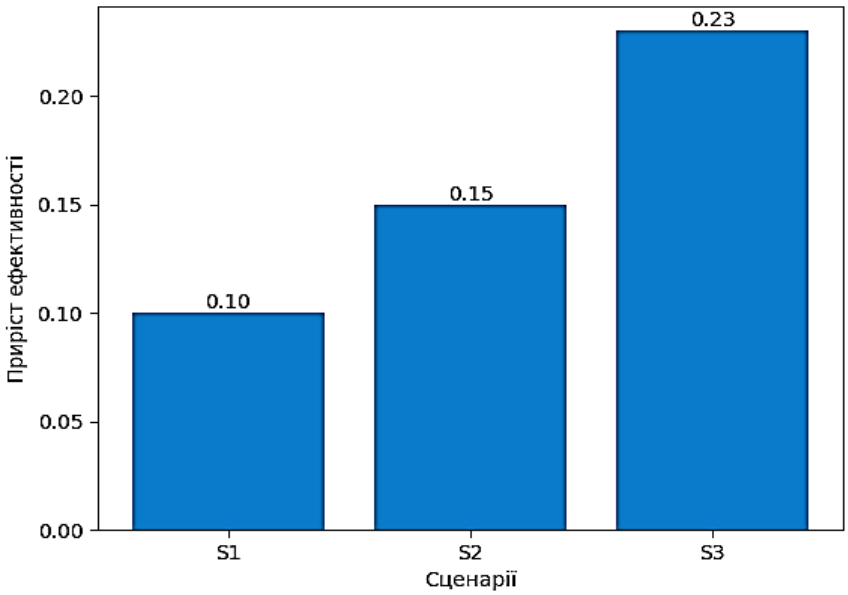

Рис. 6. Приріст ефективності запропонованого підходу відносно базового у сценаріях S1–S3

Отримані результати показали, що запропонований підхід забезпечує підвищення точності виявлення аномалій, що підтверджується зростанням показників Accuracy та F1-міри порівняно з базовими пороговими методами [11, 25]. Крім того, спостерігається зменшення часу реагування системи на аномальні події, що свідчить про ефективність використання гібридних моделей штучного інтелекту для адаптивного управління станом розподілених інформаційних систем [27]. Порівняльний аналіз показав, що за результатами проведеного імітаційного моделювання запропонована модель зменшує кількість хибних спрацьовувань у середньому на 15–20% [24-25].

Наукова новизна отриманих результатів полягає у розробленні інтегрованої моделі інтелектуальної інформаційної системи адаптивного виявлення аномалій у розподілених середовищах, яка, на відміну від існуючих підходів, поєднує чотири взаємопов'язані рівні обробки інформації. Перший рівень забезпечує прогнозування стану системи на основі нейромережевих моделей, другий – ризик-орієнтоване оцінювання відхилень з урахуванням вразливості та критичності ресурсів, третій – ймовірнісну інтерпретацію аномалій на основі логістичної функції, а четвертий – оптимізаційний вибір керуючого впливу з урахуванням рівня загроз і витрат на реагування. Така інтеграція дозволяє перейти від окремих методів аналізу до єдиної адаптивної системи прийняття рішень, що забезпечує підвищення точності, інтерпретованості та ефективності реагування в умовах динамічних розподілених середовищ. Запропонований підхід формує нову концепцію побудови інтелектуальних систем моніторингу та управління станом інформаційних систем.

Запропонований підхід відрізняється від існуючих тим, що поєднує прогнозування, оцінювання ризику та адаптивне прийняття рішень у межах єдиної інтелектуальної системи. Це дозволяє враховувати динамічний характер розподілених середовищ, зменшити кількість помилкових спрацьовувань та підвищити швидкість реагування на аномальні події [13, 21, 23]. Практична цінність моделі полягає у можливості її застосування в хмарних інфраструктурах, IoT-системах та корпоративних мережах для забезпечення надійного та безпечного

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

функціонування інформаційних систем. Розроблена модель може слугувати основою для створення програмного модуля моніторингу в системах управління IT-інфраструктурою підприємства, виявлення інцидентів кібербезпеки та автоматизованої підтримки прийняття рішень для адміністраторів і аналітиків безпеки. Отримані результати підтверджують доцільність використання гібридних моделей штучного інтелекту для побудови адаптивних систем моніторингу нового покоління.

Обговорення

Для оцінювання ефективності запропонованої моделі проведено імітаційне моделювання її функціонування та дослідження поведінки інформаційних об'єктів у розподіленому середовищі [24]. На відміну від традиційних методів, що базуються на фіксованих порогах або сигнатурному аналізі, запропонована модель забезпечує більш гнучке врахування динаміки зміни стану системи та невизначеності даних [17, 25]. Інтеграція нейромережевого прогнозування, ризик-орієнтованого оцінювання, ймовірнісної інтерпретації та нечіткого логічного виведення дозволяє досягти високої точності виявлення аномалій та зменшити кількість хибних спрацьовувань.

Порівняння результатів із базовими підходами показало, що використання гібридної моделі забезпечує підвищення показників Accuracy та F1-міри, а також скорочення часу реагування системи на аномальні події. Особливо це проявляється у сценаріях перевантаження та аномальної активності [18, 22], де система демонструє здатність до своєчасного переходу в режим підвищеного контролю або критичного реагування.

Разом із тим, слід зазначити, що ефективність моделі залежить від якості навчальних даних, коректності налаштування параметрів та вибору вагових коефіцієнтів. Крім того, використання нейромережевих компонентів може ускладнювати інтерпретацію результатів, що потребує додаткового розвитку методів пояснюваного штучного інтелекту.

Висновки

У статті розроблено інтелектуальну інформаційну систему адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Запропоновано архітектуру системи та математичну модель, що поєднує прогнозування стану системи, оцінювання аномальності, ризик-орієнтований підхід, ймовірнісну інтерпретацію та оптимізаційний вибір керуючого впливу. Проведене імітаційне моделювання підтвердило підвищення точності виявлення аномалій, зменшення кількості хибних спрацьовувань та скорочення часу реагування порівняно з традиційними підходами.

Отримані результати мають як теоретичне, так і практичне значення, оскільки дозволяють формалізувати процес адаптивного моніторингу стану інформаційних систем та забезпечити його ефективну реалізацію в умовах динамічних розподілених середовищ.

Перспективи подальших досліджень полягають у розширенні функціональних можливостей системи за рахунок використання більш складних моделей глибинного навчання, інтеграції методів пояснюваного штучного інтелекту для підвищення інтерпретованості результатів, а також впровадження запропонованого підходу у реальні інформаційні системи підприємств із подальшою експериментальною перевіркою його ефективності. Дослідження проведено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022).

Перелік посилань

1. Pustelnyk, P. Y., & Levus, Y. V. (2025). Real-time anomaly detection in distributed IoT systems: A comprehensive review and comparative analysis. Visnyk of the National University "Lviv Polytechnic". Series: Information Systems and Networks, 17, 160–169. https://doi.org/10.23939/sisn2025.17.160.

2. Mitropoulou, K., Kokkinos, P., Soumplis, P., & Varvarigos, M. (2023). Anomaly detection in cloud computing using knowledge graph embedding and machine learning mechanisms. Journal of Grid Computing, 22. https://doi.org/10.1007/s10723-023-09727-1.

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

3. Idamakanti, P. (2025). Cloud network anomaly detection using federated learning and explainable AI. International Journal on Science and Technology, 16. https://doi.org/10.71097/IJSAT.v16.i3.7336.

4. Lee, C., Yang, T., Chen, Z., Su, Y., & Lyu, M. R. (2023). Maat: Performance metric anomaly anticipation for cloud services with conditional diffusion. In 2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE) (pp. 116–128). IEEE. https://doi.org/10.1109/ASE56229.2023.00082.

5. Liu, W., Sun, D., Yang, H., Wang, Y., & Huang, W. (2025). Manod: A multi-modal anomaly detection framework for distributed system. Neural Networks, 193, Article 107999. https://doi.org/10.1016/j.neunet.2025.107999.

6. Siddique, H., Neves, M., Kuzniar, C., & Haque, I. (2021). Towards network-accelerated ML-based distributed computer vision systems. In 2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 122–129). IEEE. https://doi.org/10.1109/ICPADS53394.2021.00021.

7. Lim, L.-H., Ong, L.-Y., & Leow, M.-C. (2025). Federated learning for anomaly detection: A systematic review on scalability, adaptability, and benchmarking framework. Future Internet, 17(8), 375. https://doi.org/ 10.3390/fi17080375.

8. Wei, X., Wang, J., Sun, C.-A., Towey, D., Zhang, S., Zuo, W., Yu, Y., Ruan, R., & Song, G. (2024). Log-based anomaly detection for distributed systems: State of the art, industry experience, and open issues. Journal of Software: Evolution and Process, 36. https://doi.org/10.1002/smr.2650.

9. Abououf, M., Singh, S., Mizouni, R., & Otrok, H. (2023). Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. IEEE Internet of Things Journal, 1–1. https://doi.org /10.1109/JIOT.2023.3296809.

10. Костюк, Ю., Довженко, Н., Мазур, Н., Складанний, П., & Рзаєва, С. (2025). Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань. Кібербезпека: освіта, наука, техніка, 3(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710.

11. Anusha, R. S., Dadavali, S. P., Akash, D., Vinay, M. G., Tapkire, M., & Manjunath, N. (2024). Efficient learning-driven anomaly detection and classification for IoT-based monitoring systems. Journal of Electrical Systems, 20(11), 3749–3758. https://doi.org/10.52783/jes.8237.

12. Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка, 4(28), 633–655. https://doi.org/10.28925/2663-4023.2025.28.857.

13. Balega, M., Farag, W., Wu, X.-W., Ezekiel, S., & Good, Z. (2024). Enhancing IoT security: Optimizing anomaly detection through machine learning. Electronics, 13(11), 2148. https://doi.org/10.3390/electronics13112148.

14. Костюк, Ю. В., & Складанний, П. М. (2026). Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393.

15. Cauteruccio, F., Cinelli, L., Corradini, E., Terracina, G., Ursino, D., Virgili, L., Savaglio, C., Liotta, A., & Fortino, G. (2021). A framework for anomaly detection and classification in multiple IoT scenarios. Future Generation Computer Systems, 114, 322–335. https://doi.org/10.1016/j.future.2020.08.010.

16. Костюк, Ю., Рзаєва, С., & Рзаєв, Д. (2026). Інтелектуальний аналіз мережевого трафіку для виявлення інцидентів інформаційної безпеки. Наука і техніка сьогодні, 2(56), 1909–1928. https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928.

17. DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A survey of AI-based anomaly detection in IoT and sensor networks. Sensors, 23(3), 1352. https://doi.org/10.3390/s23031352.

18. Складанний, П., Костюк, Ю., & Рзаєва, С. (2026). Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. Математичні машини і системи, 1, 29–46. https://doi.org/10.34121/1028-9763-2026-1-29-46.

19. Dickson, S. M. (2024). Detection of anomalies in Internet of Things (IoT) devices and sensors. Radinka Journal of Science and Systematic Literature Review, 2(3), 475–481. https://doi.org/10.56778/rjslr.v2i3.347.

20. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Кібербезпека: освіта, наука, техніка, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956.

21. Gad, I. M. (2025). TOCA-IoT: Threshold optimization and causal analysis for IoT network anomaly detection based on explainable random forest. Algorithms, 18, 117. https://doi.org/10.3390/a18020117.

22. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Кібербезпека: освіта, наука, техніка, 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938.

23. Idhalama, O., & Oredo, J. (2024). Exploring the next generation Internet of Things (IoT) requirements and applications: A comprehensive overview. Information Development. https://doi.org/10.1177/02666669241267852.

24. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Rzaieva, S. (2025). Intelligent system for simulation modeling and research of information objects. In Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025) (Vol. 4053, pp. 237–251). CEUR-WS.

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106

25. Jaiswal, A., & Koupaei, A. N. (2024). Deep comparison analysis: Statistical methods and deep learning for network anomaly detection. International Journal of Computer Science and Information Security, 22. https://doi.org/10.5281/zenodo.14051106.

26. Складанний, П., Костюк, Ю., Рзаєва, С., Самойленко, Ю., & Савченко, Т. (2025). Розробка модульних нейронних мереж для виявлення різних класів мережевих атак. Кібербезпека: освіта, наука, техніка, 3(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772.

27. Zamanzadeh Draban, Z., Webb, G., Pan, S., Aggarwal, C., & Salehi, M. (2022). Deep learning for time series anomaly detection: A survey. arXiv. https://doi.org/10.48550/arXiv.2211.05244

28. Liso, A., et al. (2024). A review of deep learning-based anomaly detection strategies in Industry 4.0 focused on application fields, sensing equipment, and algorithms. IEEE Access, 12, 93911–93923. https://doi.org/10.1109/ACCESS.2024.3424488.

Yuliia Kostyuk
PhD in Computer Science, Associate Professor, Department of Information and Cyber Security named after Professor Volodymyr Buryachko
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-5423-0985
E-mail: y.kostiuk@kubg.edu.ua

Pavlo Skladannyi
Candidate of Technical Sciences, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachko
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
E-mail: p.skladannyi@kubg.edu.ua

Halyna Kuchakovska
Candidate of Pedagogical Sciences, Senior Lecturer, Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-4555-896X
E-mail: h.kuchakovska@kubg.edu.ua

INTELLIGENT INFORMATION SYSTEM FOR ADAPTIVE ANOMALIES DETECTION IN DISTRIBUTED ENVIRONMENTS BASED ON HYBRID ARTIFICIAL INTELLIGENCE MODELS

The article considers the problem of anomaly detection in distributed information environments operating under dynamic loads, high intensity of information flows, data heterogeneity and the growth of cyber threats. The relevance of the study is due to the development of cloud technologies, the Internet of Things (IoT) and big data processing systems, which complicates the monitoring of the state of information systems and requires the use of intelligent analysis methods. It has been established that traditional approaches based on static rules and threshold values do not provide sufficient accuracy and adaptability, which leads to false positives or missing critical events. The purpose of the study is to develop an intelligent information system for adaptive anomaly detection based on hybrid artificial intelligence models. To achieve this, neural networks, machine learning methods and fuzzy logic were used. A system architecture with data collection, forecasting, anomaly detection and decision-making modules is proposed. A mathematical model for assessing anomalies based on the deviation between actual and predicted parameters, as well as an integral indicator taking into account vulnerability and criticality, has been developed. A fuzzy logic inference mechanism has been implemented to form control influences. Simulation modeling has been conducted for various scenarios, which confirmed an increase in the accuracy of anomaly detection, a decrease in false positives, and a reduction in the system response time.

Keywords: intelligent information system; cloud technologies; distributed systems; anomaly detection; machine learning; neural networks; fuzzy logic; adaptive systems; artificial intelligence.

Надійшла до редакції (Received): 15.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Костюк Ю.В., Складанний П.М., Кучаковська Г.А. Інтелектуальна інформаційна система адаптивного виявлення аномалій у розподілених середовищах на основі гібридних моделей штучного інтелекту. Сучасний захист інформації, 2(66), 54–69.
https://doi.org/10.31673/2409-7292.2026.024106