

DOI: <https://doi.org/10.15407/elmodel.48.02.103>
УДК 004.056

І.В. Мартинюк ^{2,3*}, аспірант, **Н.В. Заїка** ^{1,2**}, аспірант,
М.Ю. Комаров ^{1,2***}, канд. техн. наук, **Г.В. Мартинюк** ^{2,4****}, канд. техн. наук

¹ Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Україна, 03164, Київ, вул. Олега Мудрака, 15

² Державний науково-дослідний інститут технологій кібербезпеки
Україна, 03142, Київ, вул. М. Залізняка, 3, корпус 6

³ Національний університет «Київський авіаційний інститут»
Україна, 03058, Київ, пр-т Гузара Любомира 1;

⁴ Маріупольський державний університет
Україна, 03037, Київ, вул. Преображенська, 6
E-mail: imartyniukiv@gmail.com; * ORCID: <https://orcid.org/0009-0003-5565-0828>,
nazar2611@gmail.com; ** ORCID: <https://orcid.org/0000-0002-5791-8926>,
m.komarov@cip.gov.ua; *** ORCID: <https://orcid.org/0000-0002-5739-8959>,
ganna.martyniuk@gmail.com; **** ORCID: <https://orcid.org/0000-0003-4234-025X>

Інтелектуальна аналітика для підвищення стійкості об'єктів критичної інфраструктури

Розглянуто підвищення стійкості об'єктів критичної інфраструктури (ОКІ) через інтелектуальну аналітику та машинне навчання. Основна ідея полягає у використанні адаптивних моделей машинного навчання (Machine Learning (ML)) для раннього виявлення інцидентів та автоматизованого прогнозування навантажень. Інтеграція метрик Mean Time to Detect (MTTD) та Mean Time to Recover (MTTR) для циклу з безперервного вдосконалення дозволяє значно підвищити ефективність моніторингу та управління ризиками, забезпечує підвищену кіберрезильєнтність та адаптивність ОКІ у динамічних умовах.

К л ю ч о в і с л о в а: машинне навчання, кібербезпека, критична інформаційна інфраструктура, резильєнтність, моніторинг.

Постановка проблеми. Сучасні системи моніторингу об'єктів критичної інфраструктури (ОКІ) здебільшого базуються на статичних порогових правилах, що обмежує їхню ефективність в умовах зростаючої гетерогенності телеметричних даних, динамічних навантажень та складних кіберзагроз. Це призводить до збільшення показників часу виявлення та реагування на інциденти метрик Mean Time to Detect (MTTD) та Mean Time to Recover (MTTR) і, як наслідок, до зниження рівня кіберрезильєнтності критичних сервісів.



© І.В. Мартинюк, Н.В. Заїка, М.Ю. Комаров, Г.В. Мартинюк, 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

У роботі обґрунтовано доцільність застосування адаптивних методів машинного навчання як інструменту інтелектуального аналізу даних моніторингу. Запропонований підхід враховує різноманітність джерел даних (метрики, часові ряди, журнали подій), вимоги до інтерпретованості результатів та обмеження виробничих систем моніторингу, зокрема платформи Zabbix.

Мета та завдання. Метою дослідження є розроблення методології машинного навчання (Machine Learning (ML)), а саме ML-орієнтованого моніторингу об'єктів критичної інфраструктури на базі Zabbix, спрямованої на зменшення MTTD і MTTR та підвищення загального рівня кіберрезильєнтності. Методологія передбачає адаптивний вибір моделей ML залежно від типу задачі моніторингу, характеристик даних і цільових сценаріїв використання.

У межах дослідження розглянуто підходи до виявлення аномалій, прогнозування часових рядів та аналізу журналів подій із використанням спеціалізованих ML-моделей, а також роль криптографічних механізмів у забезпеченні цілісності та достовірності даних моніторингу. Отримані результати формують методологічну основу для впровадження інтелектуальних механізмів аналізу даних у системах моніторингу критичної інфраструктури.

Для досягнення поставленої мети передбачено виконання таких основних завдань:

- проаналізувати типи та властивості даних моніторингу OKI з позицій застосування методів машинного навчання;
- обґрунтувати вибір класів ML-моделей для виявлення аномалій, прогнозування та класифікації інцидентів;
- розробити підхід до інтеграції ML-компонентів у систему моніторингу Zabbix;
- визначити показники оцінювання ефективності запропонованої методології в контексті кіберрезильєнтності OKI.

Сучасні системи моніторингу OKI, як правило, спираються на фіксовані порогові правила, що обмежує їхню здатність ефективно виявляти складні або комбіновані інциденти. Можна розширити кількість метрик або додати нові елементи для відстеження [1], але зростання динамічності навантажень та складності кіберзагроз створює необхідність переходу від реактивного моніторингу до прогностично-орієнтованого аналізу. У цьому контексті адаптивна аналітика на основі ML є ключовим інструментом підвищення кіберрезильєнтності.

Адаптивна аналітика передбачає використання ML-моделей для аналізу багатовимірних телеметричних даних, включно з метриками продуктивності, логами та подіями безпеки. Моделі здатні виявляти латентні ано-

малії без необхідності задавати жорсткі порогові значення, адаптуватися до змін навантаження та оновлюватися на основі нових даних. Типовий конвеєр обробки даних включає збір телеметрії через Zabbix, збереження в DataLake, аналіз ML-моделлю та передачу оцінки ризику у вигляді тригерів або рекомендацій для реагування.

Залежно від наявності мічених даних застосовуються різні підходи: контрольовані моделі (Logistic Regression, Support Vector Machine (SVM), Random Forest) для класифікації інцидентів, неконтрольовані (Isolation Forest (IF)), One-Class SVM) для виявлення аномалій та напівконтрольовані методи для сценаріїв з обмеженою розміткою. Для лінійних моделей часто використовується спеціалізована бібліотека та алгоритмічний підхід для ефективного навчання лінійних моделей класифікації та регресії на великих обсягах даних (LIBLINEAR), що забезпечує швидке навчання, масштабованість і інтерпретованість коефіцієнтів.

Аналіз методів ML у межах даного дослідження виконано диференційовано для кожного типу прикладних задач, що виникають у процесі моніторингу та управління станом об'єктів критичної інформаційної інфраструктури з використанням платформи Zabbix. Такий підхід зумовлений гетерогенністю даних моніторингу, які є неоднорідними за кількома вимірами одночасно, що унеможливорює застосування єдиного універсального методу аналізу або моделі машинного навчання, та потребує різною часовою динамікою метрик та вимогами до результатів у виробничому середовищі. Основною метою аналізу є обґрунтований вибір моделей ML, які можуть бути інтегровані у систему моніторингу без порушення її стабільності та масштабованості.

Порівняння алгоритмів здійснювалося за сукупністю ключових критеріїв, серед яких визначальними є точність виявлення відхилень і прогнозування отриманих результатів для інженерного персоналу, а також обробка даних у режимі, близькому до реального часу. Особливу увагу приділено обчислювальній складності моделей, оскільки системи моніторингу критичної інфраструктури зазвичай функціонують в умовах обмежених ресурсів та високих вимог до безперервності роботи [2]. Дані моніторингу включають: числові часові ряди (CPU load, latency, packetloss), бінарні та категоріальні події (statusup/down, severitylevel), текстові дані (логи систем, помилки, повідомлення), агреговані показники (availability) та нерегулярні події (alerts, incidents). При цьому гетерогенність за якістю даних визначатиметься кількістю пропусків, шумом та хибними спрацюваннями системи оповіщення.

Для задач виявлення аномалій у потоках метрик моніторингу (anomalydetection), таких як різкі зміни навантаження, аномалії споживання ресурсів або ознаки деградації сервісів, найбільш доцільними визначено ме-

тоди IF та моделі на основі автоенкодерів. IF характеризується низькою обчислювальною складністю, відсутністю потреби у маркованих даних та високою ефективністю при роботі з багатовимірними числовими метриками, що робить його придатним для онлайн-аналізу даних через програму Zabbix.

Isolation Forest (IF) — це алгоритм машинного навчання для виявлення аномалій (anomalydetection), який ґрунтується на ідеї ізоляції нетипових спостережень в системі, коли випадково розбивається простір ознак та будується набір випадкових дерев. Обчислюється середня довжина шляху до ізоляції для кожної точки. Чим коротший шлях, тим вища аномальність. Для задач виявлення аномалій у багатовимірній телеметрії систем моніторингу застосовано автоенкодерні моделі, які навчаються на нормальних режимах функціонування та ідентифікують аномалії на основі зростання похибки реконструкції [3].

Автоенкодери (Autoencoders) — це клас нейронних мереж, призначених для автоматичного навчання компактного подання даних шляхом їх стискування та подальшого відновлення, які широко застосовуються для виявлення аномалій у складних та гетерогенних даних моніторингу. Автоенкодери, у свою чергу, дозволяють виявляти складні нелінійні залежності у даних та є ефективними для аналізу довготривалих поведінкових патернів, однак потребують більших обчислювальних ресурсів і попереднього навчання на історичних даних. Дані походять з мережевого та серверного обладнання, систем безпеки (IDS/IPS, SIEM), зовнішніх сенсорів (дрони, аудит, персонал). Кожне джерело має власну семантику, рівень надійності та шум. Використання автоенкодерів у системах моніторингу сприяє зменшенню показника MTTD та підвищує загальний рівень кіберрезильєнтності об'єктів критичної інфраструктури за рахунок раннього виявлення прихованих аномалій.

Аномальність точки x визначається як:

$$s(x, n) = 2^{\frac{-E(h(x))}{c(n)}},$$

де $E(h(x))$ — математичне сподівання довжини шляху ізоляції точки x у деревах ізоляції. Менше значення $E(h(x))$ означає, що точка ізолюється швидше, що є характерною ознакою аномальних спостережень.

$c(n)$ — коефіцієнт, який відповідає середній довжині шляху для випадкових даних розміру n . Використовується для приведення значення $E(h(x))$ до порівнюваної шкали незалежно від обсягу вибірки.

$s(x) \rightarrow 1$ — значення аномального стану, що вказує на високу ймовірність того, що спостереження x є аномалією (швидка ізоляція в більшості дерев).

$s(x) \rightarrow 0$ — значення скору, характерне для нормальної поведінки, коли точка потребує більшої кількості розбиттів для ізоляції та добре інтегрується у загальний розподіл даних.

У задачах прогнозування часових рядів (forecasting), зокрема для планування навантаження, оцінювання доступності ресурсів та прогнозування потенційних відмов, Моделі Auto Regressive Integrated Moving Average (ARIMA) — це клас статистичних моделей аналізу та прогнозування часових рядів, що використовуються для опису динаміки показників у часі на основі їхніх власних попередніх значень та випадкових збурень. ARIMA складається з трьох компонентів:

- AR (Auto Regressive) — авторегресійна частина, що описує залежність поточного значення показника від його попередніх значень;
- I (Integrated) — інтегрування, яке полягає у диференціюванні часового ряду для досягнення стаціонарності;
- MA (Moving Average) — ковзне середнє, що моделює вплив випадкових похибок попередніх кроків.

У контексті моніторингу об'єктів критичної інфраструктури, зокрема на основі метрик Zabbix, моделі ARIMA застосовуються для:

- прогнозування навантаження на ресурси (CPU, пам'ять, мережа);
- оцінювання тенденцій деградації продуктивності;
- виявлення відхилень від очікуваної поведінки;
- підтримки планування потужностей.

Ключовими перевагами ARIMA є висока інтерпретованість, помірні обчислювальні витрати та ефективність для стаціонарних або квазістаціонарних часових рядів із сезонною структурою, що робить ці моделі доцільними для використання у виробничих системах моніторингу. Обмеженням є зниження точності у випадках складної нелінійної динаміки та різких змін режимів роботи системи.

Водночас у складних динамічних середовищах OKI, де присутні нелінійні ефекти, довгострокові залежності та зміна режимів роботи, більш доцільним є використання рекурентних нейронних мереж типу Long Short-Term Memory (LSTM). Рекурентні нейронні мережі типу LSTM — це спеціалізований клас нейронних мереж, призначений для моделювання часових послідовностей та процесів із довгостроковими залежностями, де поточний стан системи визначається не лише останніми, а й віддаленими у часі подіями.

На відміну від класичних рекурентних нейронних мереж, LSTM-архітектура містить механізм керованої пам'яті, що реалізується через систему логічних «воріт» (gates), які регулюють:

- збереження релевантної інформації у внутрішньому стані;
- оновлення пам'яті новими даними;

- відбір інформації для формування вихідного прогнозу.

Такі моделі здатні враховувати історичний контекст на значних часових інтервалах, що підвищує точність прогнозування деградації ресурсів і дозволяє завчасно ідентифікувати передумови відмов. Обмеженням LSTM-підходів є потреба у значному обсязі історичних даних, складність налаштування та підвищені вимоги до обчислювальних ресурсів, що необхідно враховувати під час впровадження у промислові системи моніторингу [4].

Для аналізу журналів подій та логів (loganalysis), які зазвичай містять напівструктуровані або неструктуровані текстові дані, найбільш ефективним виявився комбінований підхід. Він передбачає попередній розбір, нормалізацію та структурування логів із використанням шаблонних і статистичних алгоритмів, після чого застосовуються нейронні моделі, здатні враховувати контекст подій і часову послідовність записів. Такий підхід дозволяє не лише виявляти окремі аномальні повідомлення, а й ідентифікувати складні ланцюжки подій, що відповідають багатокроковим сценаріям розвитку інцидентів, критично важливим для систем раннього попередження.

Узагальнені результати порівняльного аналізу свідчать, що використання універсального алгоритму машинного навчання для всіх типів задач моніторингу є недоцільним. Найбільш ефективним є адаптивний підхід, за якого вибір моделі здійснюється з урахуванням типу даних (метрики, часові ряди, логи), вимог до затримки обробки, рівня інтерпретованості та цільового сценарію використання. Такий підхід узгоджується з запропонованим у роботі алгоритмом вибору моделей і формує методологічну основу для впровадження інтелектуальних механізмів аналізу даних у системах моніторингу критичної інфраструктури на базі Zabbix, сприяючи зменшенню MTTD та MTTR і підвищенню загального рівня кіберрезильєнтності ОКИ [5].

Роль криптографічних механізмів у забезпеченні достовірності та резильєнтності моніторингу. Криптографічний захист формує довірний контур даних, у межах якого результати ML-аналізу залишаються коректними та відтворюваними. Це є критично важливим для адаптивних моделей прогнозування та виявлення аномалій, оскільки компрометація навчальних або вхідних даних може призвести до деградації точності, зростання MTTD та помилкових спрацювань. Поряд із інтелектуальними методами аналізу даних, важливу роль у формуванні кіберрезильєнтності об'єктів критичної інфраструктури відіграють криптографічні механізми захисту телеметрії, журналів подій та керуючих повідомлень [6]. Надійність оцінювання MTTD і MTTR безпосередньо залежить від цілісності, автентичності та конфіденційності даних моніторингу, оскільки спотворення або підміна метрик і логів призводять до хибних рішень і зростання часу виявлення інцидентів. Криптографічна хеш-функція — це детермі-

нована функція $H(x)$, яка для довільного вхідного повідомлення x формує компактний хеш-образ фіксованої довжини, що має властивості стійкості до колізій, стійкості до знаходження прообразу та лавиноподібного ефекту. Найпоширенішими сучасними алгоритмами є SHA-256, SHA-384, SHA-512, BLAKE2, SHA-3.

Протокол Transport Layer Security (TLS) забезпечує криптографічний захист каналів передавання телеметрії та журналів подій у системах моніторингу об'єктів критичної інфраструктури. TLS є сучасним стандартом захищеного з'єднання, що замінив застарілий протокол Secure Sockets Layer (SSL), і широко використовується у критичних інформаційних системах, зокрема в архітектурах моніторингу типу Zabbix [7]. Застосування TLS підвищує конфіденційність, цілісність та автентичність даних, що є передумовою коректного оцінювання показників MTTD і MTTR та надійної роботи адаптивних моделей машинного навчання. Захищений транспортний рівень формує довірене середовище аналізу, мінімізує ризики підміни даних і підвищує загальний рівень кіберрезильєнтності OKI.

У виробничих середовищах на базі Zabbix криптографія використовується для:

- захисту каналів передачі телеметрії між агентами та сервером (TLS, сертифікатна автентифікація);
- забезпечення автентичності джерел подій та логів за допомогою цифрових підписів і контрольних хеш-функцій;
- запобігання несанкціонованій модифікації історичних даних, що використовуються для навчання моделей машинного навчання.

Логіка та етапи ситуаційного аналізу в контексті оцінювання кіберрезильєнтності OKI. Ситуаційний аналіз у межах забезпечення кіберрезильєнтності об'єктів критичної інфраструктури розглядається як системний інструмент передпроектного дослідження, спрямований на формалізацію складної проблемної ситуації, виявлення ключових факторів впливу та обґрунтування управлінських рішень. Його логіка базується на послідовному переході від фіксації поточного стану інформаційно-технологічної системи до оцінювання можливих сценаріїв розвитку кіберінцидентів і наслідків їх реалізації [8]. Такий підхід забезпечує цілісне бачення стану OKI, зменшує невизначеність та створює аналітичне підґрунтя для оптимізації показників MTTD і MTTR як ключових індикаторів кіберрезильєнтності.

Першим етапом ситуаційного аналізу є фіксація поточного стану системи, що включає опис архітектури OKI, наявних засобів моніторингу, журналювання подій і реагування на інциденти. На цьому етапі здійснюється аналіз фактичних значень MTTD та MTTR на основі історичних даних, зокрема телеметрії та логів, отриманих із систем моніторингу типу Zabbix. Це доз-

воляє сформувати базову оцінку рівня кіберрезильєнтності та виявити первинні ознаки неефективності процесів виявлення і реагування.

Другий етап полягає у визначенні меж аналізу та рівнів деталізації, що є критично важливим для роботи з великими обсягами різномірних даних. На цьому кроці встановлюються часові інтервали спостереження, перелік контрольованих компонентів (мережеві вузли, сервери, прикладні сервіси), а також рівень агрегації метрик. Чітке визначення меж аналізу дозволяє узгодити вимоги до точності моделей машинного навчання з обчислювальними можливостями виробничого середовища.

Третій етап передбачає ідентифікацію ключових факторів, що впливають на рівень кіберрезильєнтності ОКІ. До таких факторів належать технічні характеристики інфраструктури, якість телеметрії, ефективність алгоритмів аналізу даних, рівень автоматизації реагування, а також людський фактор, зокрема підготовленість персоналу та дотримання практик кібергігієни. Для системної структуризації впливів внутрішнього і зовнішнього середовища у передпроектному та ситуаційному аналізі застосовується комплекс методів SWOT-аналізу, PEST(LE)-аналізу та аналізу зацікавлених сторін. SWOT-аналіз, це скорочення від Strengths (Сильні сторони), Weaknesses (Слабкі сторони), Opportunities (Можливості), Threats (Загрози), який дозволяє ідентифікувати внутрішні сильні та слабкі сторони об'єкта дослідження, а також зовнішні можливості і загрози, що формують поле стратегічних рішень. PEST(LE)-аналіз допомагає зрозуміти масштабні тенденції, на які компанія не може вплинути, але має враховувати наступні фактори: Political (Політичні), Economic (Економічні), Sociological (Соціологічні), Technological (Технологічні), Legal (Правові), Environmental (Екологічні). Аналіз зацікавлених сторін спрямований на виявлення ключових акторів (Stakeholders), їхніх інтересів, рівнів впливу та потенційних конфліктів, що дозволяє враховувати людський і організаційний фактор у процесі прийняття рішень.

Сукупне застосування зазначених методів формує багатовимірну модель середовища, знижує рівень невизначеності та створює методологічну основу для обґрунтованого вибору управлінських і проектних рішень [9—11]. На цьому етапі доцільним є застосування методів SWOT-аналізу, PEST(LE)-аналізу та аналізу зацікавлених сторін для структуризації впливів внутрішнього і зовнішнього середовища. Коротко методи можливо описати наступним чином:

- SWOT — що добре / погано і які є шанси та загрози;
- PEST(LE) — що відбувається навколо на рівні держави, економіки, законів, технологій;
- Stakeholders — хто реально впливає і від кого залежить успіх.

Четвертий етап полягає в аналізі причинно-наслідкових зв'язків, що дозволяє встановити залежності між виявленими факторами та значеннями

MTTD і MTTR. Зокрема, аналізуються причини запізненого виявлення інцидентів, обмеження порогових механізмів моніторингу та вплив складних або комбінованих атак. На цьому етапі обґрунтовується доцільність використання адаптивних ML-методів, таких як IF, автоенкодери або LSTM-моделі, для зменшення часу виявлення аномалій і прискорення реагування.

П'ятий етап спрямований на формування альтернатив і сценаріїв розвитку подій, що відображають різні стратегії підвищення кіберрезильєнтності OKI. Сценарії можуть включати впровадження нових ML-моделей, розширення джерел моніторингу (наприклад, за рахунок допоміжних модулів або зовнішніх сенсорів), автоматизацію процесів реагування або підвищення кваліфікації персоналу. Кожен сценарій оцінюється з точки зору його впливу на інтегральний показник резильєнтності.

Завершальним етапом є оцінювання потенційних наслідків, що передбачає кількісне порівняння сценаріїв на основі інтегральної математичної моделі оцінювання резильєнтності OKI. Це дозволяє пов'язати технічні рішення з їх впливом на MTTD, MTTR та загальний рівень стійкості системи, а також обґрунтувати управлінські рішення щодо пріоритетів інвестування в кіберзахист.

Висновки

Показано, що вибір алгоритмів машинного навчання для всіх задач моніторингу критичної інфраструктури потребує адаптивного підходу, за якого вибір моделей здійснюється з урахуванням типу даних, часових вимог та цільових сценаріїв використання.

Розглянуто етапи ситуаційного аналізу в контексті оцінювання кіберрезильєнтності OKI при застосуванні спеціалізованих ML-методів для виявлення аномалій, прогнозування та аналізу логів, які дозволяють суттєво зменшити показники MTTD та MTTR, підвищуючи оперативність реагування та стійкість критичних сервісів у системах моніторингу на базі Zabbix та сприяє підвищенню загального рівня кіберрезильєнтності об'єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Martyniuk I., Martyniuk H., Yevchenko Y. Improving the method of monitoring the state of the website by detecting user interface vulnerabilities and browser errors // CEUR Workshop Proceedings. 2025. Vol. 4024. P. 157—162.
2. Zimelewicz E., Biesialska M., Zhang X., Back T., Briand L. Machine Learning-Enabled Systems: Model Deployment and Monitoring Challenges // Proceedings of the 42nd International Conference on Software Engineering. Seoul, Republic of Korea, 2020. P. 38—49. DOI: 10.1145/3377811.3380394.

3. Ruff L., Kauffmann J., Vandermeulen R. et al. A Unifying Review of Deep and Classical Anomaly Detection // *Proceedings of the IEEE*. 2022. Vol. 110, No. 5. P. 756—782. DOI: 10.1109/JPROC.2022.3158238.
4. Martyniuk I.V., Okhrimenko T.O. Methodology and classification of open-source ML methods for IT monitoring based on the Zabbixsystem // *Ukrainian Scientific Journal of Information Security*, 2025, vol. 31, issue 2, pp. 87—92.
5. Narayan A., Kumar R., Singh A. AI-Driven Anomaly Detectionin Nagiosand Zabbix Logs // *International Journal of Computer Applications*. 2021. Vol. 174, No. 27. P. 15—22. URL: <https://www.ijcaonline.org/archives/volume174/number27/> (дата звернення: 22.12.2025).
6. Applications containers security model — Misnik O. // Collection “Information Technology and Security”, Vol. 8, No 1 (2020), pp. 58—66. DOI:10.20535/2411-1031.2020.8.1.218004.its.iszzi.kpi.ua
7. Zabbix (n.d.) Monitor anything — networks, cloud, websites, IoT, and more. Available at: <https://www.zabbix.com/> (Accessed: 15 december 2025).
8. Невольніченко А.І., Чумаченко С.М., Михайлова А.В., Пиріков О.В., Мурасов Р.К. Моделювання загроз виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури з використанням методу системної динаміки. // *Таврійський науковий вісник. Серія: Технічні науки*, 2022. Том 3. С. 88—99
9. Bershchanskyi Y., Klym H., Shevchuk Y. Containerized Artificial Intelligent System Designin Cloud and Cyber-Physical Systems. // *Advancesin Cyber-Physical Systems (ACPS)*, Vol. 9, No 2 (2024), pp. 151—157. DOI:10.23939/acps2024.02.151.
10. Bershchanskyi Y., Stepanov O. Machine learning model developmentin Kubeflow cloud-native systems. // *ACPS*, Vol. 10, No 1 (2025), pp. 83—88. DOI: 10.23939/acps2025.01.083.
11. Semerikov S.O., Zubov D., Kupin A., Kosei M., Holiver V. Models and Technologies for Autoscaling Based on Machine Learning for Microservices Architecture. // *Proceedings of the 8th International Conferenceon Computational Linguistics and Intelligent Systems*, Lviv, 2024, pp. 316—330.

REFERENCES

1. Martyniuk I., Martyniuk H., Yevchenko Y. (2025). Improving the method of monitoring the state of the website by detecting user interface vulnerabilities and browser errors. *CEUR Workshop Proceedings*. Vol. 4024. Pp. 157-162.
2. Zimelewicz E., Biesialska M., Zhang X., Bäck T., Briand L. (2020). Machine learning-enabled systems: model deployment and monitoring challenges. *Proceedings of the 42nd International Conference on Software Engineering*. Seoul, Republic of Korea. Pp. 38-49. DOI: 10.1145/3377811.3380394.
3. Ruff L., Kauffmann J., Vandermeulen R. et al. (2022). A unifying review of deep and classical anomaly detection. *Proceedings of the IEEE*. 110(5). Pp. 756-782. DOI: 10.1109/JPROC.2022.3158238.
4. Martyniuk I.V., Okhrimenko T.O. (2025). Methodology and classification of open-source ML methods for IT monitoring based on the Zabbix system. *Ukrainian Scientific Journal of Information Security*. 31(2). Pp. 87-92.
5. Narayan A., Kumar R., Singh A. (2021). AI-driven anomaly detection in Nagios and Zabbix logs. *International Journal of Computer Applications*. 174(27). Pp. 15-22. URL: <https://www.ijcaonline.org/archives/volume174/number27/> (date of access: 22.12.2025).

6. Misnik O. Application container security model. (2020). Information Technology and Security. 8(1). Pp. 58-66. DOI: 10.20535/2411-1031.2020.8.1.218004.
7. Zabbix. Monitor anything — networks, cloud, websites, IoT, and more. URL: <https://www.zabbix.com/> (date of access: 15.12.2025).
8. Nevolnichenko A. I., Chumachenko S. M., Mykhailova A. V., Pyrikov O. V., Murasov R. K. Modeling threats of emergency situations at critical infrastructure facilities using the system dynamics method. (2022). Tavria Scientific Bulletin. Series: Technical Sciences. 3, pp. 88-99.
9. Bershchanskyi Y., Klym H., Shevchuk Y. Containerized artificial intelligence system design in cloud and cyber-physical systems. (2024). Advances in Cyber-Physical Systems. 9(2), pp. 151-157. DOI: 10.23939/acps2024.02.151.
10. Bershchanskyi Y., Stepanov O. Machine learning model development in Kubeflow cloud-native systems. (2025). Advances in Cyber-Physical Systems. 10(1), pp. 83-88. DOI: 10.23939/acps2025.01.083.
11. Semerikov S. O., Zubov D., Kupin A., Kosei M., Holiver V. Models and technologies for autoscaling based on machine learning for microservices architecture. (2024). Proceedings of the 8th International Conference on Computational Linguistics and Intelligent Systems. Lviv. Pp. 316-330.

I. Martyniuk, N. Zaika, M. Komarov, H. Martyniuk

INTELLIGENT ANALYTICS FOR ENHANCING THE RESILIENCE OF CRITICAL INFRASTRUCTURE

This paper addresses the enhancement of resilience of critical infrastructure objects (CIOs) through intelligent analytics and machine learning techniques. The core idea is based on the use of adaptive models for early incident detection and automated load forecasting. The integration of Mean Time to Detect (MTTD) and Mean Time to Recover (MTTR) metrics into a continuous improvement cycle significantly increases the effectiveness of monitoring and risk management, ensuring enhanced cyber resilience and adaptability of critical infrastructure under dynamic operating conditions.

K e y w o r d s: artificial intelligence, machine learning, critical information infrastructure, resilience, monitoring.

МАРТИНЮК Ігор Вадимович, аспірант Національного університету «Київський авіаційний інститут»; інженер Державного науково-дослідного інституту технологій кібербезпеки. У 2011 р. закінчив Національний авіаційний університет. Область наукових досліджень — кібербезпека та захист інформації.

ЗАЙКА Назар Валентинович, аспірант Інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України; мол. наук. співробітник Державного науково-дослідного інституту технологій кібербезпеки. У 2014 р. закінчив Національний технічний університет України «Київський політехнічний інститут». Область наукових досліджень — комп'ютерні науки.

КОМАРОВ Максим Юрійович, канд. техн. наук, ст. наук. співробітник, викладач Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 2002 р. закінчив Спеціальний факультет Національного технічного університету України «Київський політехнічний інститут». Область наукових досліджень — інформаційні технології, кібербезпека та захист інформації, комп'ютерна безпека.

МАРТИНЮК Ганна Вадимівна, канд. техн. наук, доцент, завідувач кафедри системного аналізу та інформаційних технологій Маріупольського державного університету; провідний науковий співробітник Державного науково-дослідного інституту технологій кібербезпеки. У 2011 р. закінчила Національний авіаційний університет. Область наукових досліджень — стеганографія, стегоаналіз, обробка шумових сигналів, захист інформації.

Дата надходження статті: 17.02.2026;
дата прийняття статті до друку після рецензування: 20.03.2026;
дата публікації (оприлюднення) статті: 28.04.2026