КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1147
УДК 004.056:004.8:004.738.5

Кудренко Станіслава Олексіївна
кандидат технічних наук, доцент
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0002-0759-3908
stanislava@i.ua

Козловський Валерій Валерійович
доктор технічних наук, професор
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0002-8301-5501
valerii.kozlovskyi@npp.kai.edu.ua

Алькема Віталій Вікторович
аспірант
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0000-0009-8237
9010908@stud.kai.edu.ua

НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ПРОМИСЛОВИХ IOT-СИСТЕМ ЗА УМОВ ПОРУШЕННЯ ЦІЛІСНОСТІ ПЕРИФЕРІЙНИХ ВУЗЛІВ

Анотація. У статті розглянуто проблему забезпечення функціональної стійкості промислових IoT-систем за умов часткового порушення цілісності периферійних вузлів. Актуальність дослідження зумовлена зростанням кіберризиків у багаторівневих архітектурах edge–fog–cloud, у яких периферійні пристрої виконують первинну обробку та передавання телеметричних даних. Деградація або компрометація окремих вузлів у таких системах призводить до накопичення похибок під час агрегування даних, спотворення результатів аналітики та потенційного прийняття некоректних управлінських рішень. Традиційні підходи, засновані на повному відключенні підозрілих вузлів, можуть негативно впливати на безперервність технологічного процесу та знижувати відмовостійкість системи загалом. Запропоновано нейромережевий підхід до підтримання функціональної стійкості, що поєднує оцінювання поточного стану вузлів із адаптивною зміною їхнього вагового внеску в результати обробки без повного виключення з обчислювального контуру. Формалізовано модель впливу збурень на агрегований сигнал, у межах якої введено змінну стану вузла як інтегральний показник інформаційної достовірності та рівня його потенційної компрометації. Для оцінювання стану використано рекурентну нейронну мережу типу GRU, яка враховує часову динаміку поведінки вузлів та дозволяє виявляти аномальні відхилення у телеметричних потоках. Проведене імітаційне моделювання продемонструвало зменшення системної похибки агрегування та стабілізацію результуючого сигналу порівняно з класичними пороговими методами реагування. Отримані результати підтверджують ефективність запропонованого підходу для промислових IoT-середовищ та його здатність забезпечувати баланс між вимогами кібербезпеки, достовірністю даних і безперервністю технологічного процесу.

Ключові слова: промисловий інтернет речей; кібербезпека IIoT; рекурентні нейронні мережі; кіберризики; механізми кіберзахисту.

ВСТУП

Промислові IoT-системи функціонують у середовищі підвищених кіберризиків через інтеграцію інформаційних та операційних технологій у межах кіберфізичних систем [2]. Периферійні вузли є найбільш уразливими компонентами IIoT-архітектури через обмежені обчислювальні ресурси, складність оновлення програмного забезпечення та фізичну доступність [1].

Сучасні дослідження у сфері кібербезпеки IIoT орієнтовані на застосування методів машинного та глибинного навчання для виявлення вторгнень і аномалій [6], [9]. Проте більшість існуючих підходів

зосереджені на детекції та ізоляції скомпрометованих вузлів без подальшої адаптації процесу агрегування даних [6].

У випадку часткового порушення цілісності периферійний вузол може продовжувати функціонування, формуючи викривлені телеметричні дані, що призводить до накопичення системної похибки під час агрегування [5]. У багаторівневих архітектурах edge-fog-cloud ця проблема є особливо критичною через розподілений характер обробки інформації [8].

З огляду на це, актуальною є задача поєднання механізмів кібердетекції з адаптивною зміною параметрів обробки даних на основі нейромережевих моделей часової динаміки [7].

Постановка проблеми. Нехай промислова IoT-система складається з множини периферійних вузлів

$$D = \{d_1, d_2, \dots, d_n\},$$

кожен з яких формує вектор вимірювань

$$x_i(t) \in \mathbb{R}^m,$$

де t – дискретний момент часу.

За нормального функціонування агрегований результат обробки визначається оператором

$$Y(t) = F(x_1(t), x_2(t), \dots, x_n(t)) \quad (1)$$

де $F(\cdot)$ – функція агрегування даних у багаторівневій edge–fog архітектурі.

У випадку порушення цілісності окремих вузлів їх інформаційні потоки можуть зазнавати викривлення. Це формалізується співвідношенням

$$\tilde{x}_i(t) = x_i(t) + \delta_i(t) \quad (2)$$

де $\delta_i(t)$ – збурювальна компонента, що моделює наслідки кібератаки, помилки або деградації вузла. Згідно з (2), навіть незначні відхилення можуть накопичуватися у процесі агрегування.

У такому випадку результуючий агрегований сигнал набуває вигляду

$$\tilde{Y}(t) = F(\tilde{x}_1(t), \tilde{x}_2(t), \dots, \tilde{x}_n(t)).$$

Порушення цілісності призводить до зростання системної похибки, яку доцільно визначити як

$$E(t) = \| \tilde{Y}(t) - Y_{ref}(t) \|, \quad (3)$$

де $Y_{ref}(t)$ – еталонний результат, що відповідає коректному режиму функціонування. Похибка (3) використовується як інтегральний показник втрати функціональної стійкості системи.

Для мінімізації впливу збурень (2) введемо змінну стану вузла

$$S_i(t) \in [0,1],$$

яка відображає рівень його інформаційної достовірності. Значення $S_i(t) = 1$відповідає повній цілісності вузла, а $S_i(t) = 0$ – його повній компрометації.

З урахуванням адаптації обробки даних агрегований результат визначається як

$$Y^{adapt}(t) = F(S_1(t)x_1(t), \dots, S_n(t)x_n(t)). \quad (4)$$

Вираз (4) описує механізм динамічного зменшення впливу вузлів із порушеною цілісністю на результати агрегування. Задача полягає у побудові такого механізму оцінювання стану $S_i(t)$, який забезпечує обмеженість системної похибки (3), тобто

$$\limsup_{t\to\infty} E(t) \le \varepsilon,$$

де ε – допустимий рівень відхилення.

Оцінювання стану вузла здійснюється на основі нейромережевої моделі

$$S_i(t) = f_\theta(v_i(t), h_i(t-1)), \quad (5)$$

де $v_i(t)$ – вектор ознак поведінки вузла,
$h_i(t)$ – прихований стан рекурентної нейронної мережі,
f_θ – параметризована модель із часовою залежністю.

Таким чином, відповідно до (5), задача зводиться до синтезу нейромережевого механізму оцінювання стану периферійних вузлів, який мінімізує вплив збурень (2) на агрегований результат (1) та забезпечує стабілізацію похибки (3) за рахунок адаптивного перетворення (4).

Аналіз останніх досліджень і публікацій. Сучасні дослідження активно розвивають ML/DL-підходи до кібердетекції в IoT/IIoT, підкреслюючи потребу в легких і обчислювально ефективних моделях, придатних для ресурсно обмежених вузлів [4]. Для edge-середовищ запропоновано приватно-орієнтовані підходи на кшталт асинхронного federated learning, які підсилюють детекцію атак без централізованого збирання даних [5].

Окремий клас робіт показує ефективність часових нейромережевих архітектур (LSTM/автоенкодери) для виявлення аномалій у промислових даних та врахування деградаційних трендів, включно з постановками, де важлива приватність і розподіленість даних [6]. Також набирає популярності інтеграція Digital Twin із нейромережевим аналізом телеметрії, що покращує стабільність детекції в умовах шуму, пропусків і повільної деградації сигналів [7].

Разом із тим, попри прогрес у детекції, недостатньо опрацьованим залишається питання зв'язку оцінки "довіри/стану" вузла з механізмами адаптивної зміни агрегування даних у багаторівневій edge-fog архітектурі, щоб не лише фіксувати порушення, а й підтримувати функціональну стійкість системи [2]. З позицій ризик-менеджменту для IoT-пристроїв важливо формалізувати вимоги до кіберздатностей і очікуваної поведінки пристрою в системі, що задає базис для таких адаптивних механізмів [1].

Нейромережевий метод забезпечення стійкості. Запропонований метод базується на поєднанні: оцінювання стану периферійного вузла, моделювання часової динаміки його поведінки, адаптації параметрів агрегування даних. На відміну від статичних порогових алгоритмів, запропонований підхід враховує накопичувальний характер деградації вузла та дозволяє коригувати його вплив без повного відключення.

Метод реалізується у три етапи:

1) формування вектора ознак вузла;
2) нейромережеве оцінювання його стану;
3) адаптивна корекція участі вузла в агрегуванні.

Для кожного вузла формується вектор поведінкових ознак

$$v_i(t) = [a_i(t), \sigma_i(t), l_i(t), r_i(t)], \quad (6)$$

де $a_i(t)$ – показник аномальності вимірювань,
$\sigma_i(t)$ – дисперсія сигналу,
$l_i(t)$ – затримка передачі,
$r_i(t)$ – відхилення від еталонної моделі.

Вектор (6) відображає як інформаційні, так і мережеві характеристики вузла, що дозволяє враховувати кібербезпекові аспекти його функціонування.

Оцінювання стану вузла здійснюється за допомогою рекурентної нейронної мережі типу GRU, що враховує часову залежність поведінки.

Динаміка прихованого стану визначається як

$$h_i(t) = \mathrm{GRU}(v_i(t), h_i(t-1)), \quad (7)$$

де $h_i(t)$ – вектор прихованого стану.

Оцінка рівня достовірності вузла визначається як

$$S_i(t) = \sigma(W h_i(t) + b), \quad (8)$$

де W та b – параметри мережі,
$\sigma(\cdot)$ – сигмоїдна функція активації.

Згідно з (8), значення $S_i(t)$набуває значення в інтервалі $[0, 1]$, що інтерпретується як рівень збереження цілісності вузла.

На основі оціненого стану (8) здійснюється динамічна корекція участі вузла в агрегуванні:

$$x_i^{adapt}(t) = S_i(t) \cdot x_i(t). \quad (9)$$

Відповідно до (9), при зменшенні рівня довіри внесок вузла у результат обробки пропорційно знижується.

Адаптований агрегований результат визначається як

$$Y^{adapt}(t) = F(x_1^{adapt}(t), \dots, x_n^{adapt}(t)). \quad (10)$$

Таким чином, запропонований метод забезпечує плавну деградацію впливу скомпрометованих вузлів без їх повного відключення.

Особливістю підходу є те, що оцінювання стану вузла (7)-(8) здійснюється з урахуванням часової еволюції його поведінки, що дозволяє виявляти поступові атаки типу data injection або повільну деградацію прошивки. На відміну від класичних IDS, метод не лише детектує відхилення, а й адаптує процес обробки даних у режимі реального часу.

Для експериментальної перевірки методу використано синтетично згенеровані часові ряди, що моделюють телеметрію промислових сенсорних вузлів у IIoT-системі. Синтетичний підхід обрано з огляду на відтворюваність експерименту та можливість керовано формувати сценарії порушення цілісності вузлів із заданою інтенсивністю і тривалістю.

Нехай система містить nпериферійних вузлів (у базовому сценарії $n = 20$), кожен з яких генерує багатовимірний вектор вимірювань $x_i(t) \in \mathbb{R}^m$у дискретні моменти часу $t = 1, \dots, T$(у базовому сценарії $T = 10\,000,\ \ m = 3$). Нормальний (еталонний) сигнал для і-го вузла задається як комбінація детермінованої компоненти та випадкового шуму:

$$x_i(t) = \mu_i + A_i \sin(2\pi f_i t + \varphi_i) + \eta_i(t), \quad (11)$$

де μ_i – рівень зсуву, A_i – амплітуда, f_i – частота, φ_i – початкова фаза, $\eta_i(t)$ – шумова компонента (наприклад, нормальний шум із нульовим середнім). Така модель відображає типову природу промислової телеметрії (періодичні режими роботи, технологічні коливання, шум вимірювань).

Окрім сенсорних значень, для кожного вузла формується набір поведінкових і мережевих ознак, необхідних для побудови вектора $v_i(t)$(див. (6)). Зокрема, моделюються затримка передачі $l_i(t)$, імовірність втрати пакета $p_i(t)$та показник пропусків даних $q_i(t)$. Це дозволяє врахувати ситуації, коли кіберінцидент проявляється не лише у викривленні сенсорного сигналу, а й у зміні мережевих характеристик.

Для частини вузлів (у базовому сценарії $k = 3$з n) вводяться контрольовані сценарії порушення цілісності, які реалізуються шляхом додавання збурювальної компоненти $\delta_i(t)$ згідно з (2). Використовуються такі типи збурень: (i) імпульсні викиди, що імітують короткочасну ін’єкцію даних; (ii) поступовий дрейф, що моделює “тиху” атаку або деградацію прошивки; (iii) квазіперіодичні спотворення, що відображають систематичну маніпуляцію показниками. Узагальнено це описується співвідношенням

$$\delta_i(t) = \delta_i^{spike}(t) + \delta_i^{drift}(t) + \delta_i^{bias}(t), \quad (12)$$

де окремі складові активуються відповідно до заданого сценарію експерименту.

Для забезпечення відтворюваності експерименту фіксується зерно генератора випадкових чисел (seed), а всі параметри моделювання (n, T, m, частка вузлів із порушенням цілісності, тип і інтенсивність $\delta_i(t)$, параметри шуму та мережевих характеристик) задаються явно. Далі дані перетворюються у формат часових вікон довжини Wдля подачі на рекурентну нейронну мережу, що відповідає механізму оцінювання стану вузлів за (7)-(8).

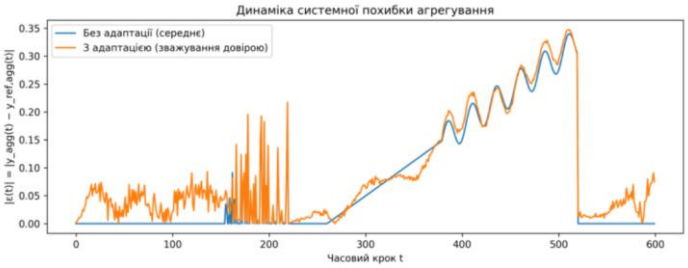

Рис. 1. Еволюція показника інформаційної достовірності вузлів $s_i(t)$, отриманого за моделлю (7)-(8)

На рисунку 1 представлено часову динаміку оцінки стану периферійних вузлів $s_i(t)$, отриману відповідно до нейромережевої моделі (7)-(8). Значення $s_i(t) \in [0,1]$інтерпретується як рівень інформаційної достовірності вузла, де значення, близькі до одиниці, відповідають нормальному функціонуванню, а їх зменшення відображає деградацію або порушення цілісності.

У початковому інтервалі часу всі вузли демонструють високий рівень довіри, що узгоджується з еталонним режимом роботи. Після введення збурювальної компоненти $\delta_i(t)$згідно з (2) для скомпрометованих вузлів спостерігається поступове зниження оцінки $s_i(t)$, що підтверджує здатність рекурентної моделі враховувати часову еволюцію поведінки. Важливо, що зниження має плавний характер і не призводить до миттєвого обнулення показника, що відрізняє запропонований підхід від жорстких порогових механізмів.

Таким чином, Рис. 1 демонструє коректність механізму оцінювання стану вузлів та формування вагового коефіцієнта, який надалі використовується в адаптивному агрегуванні згідно з (9).

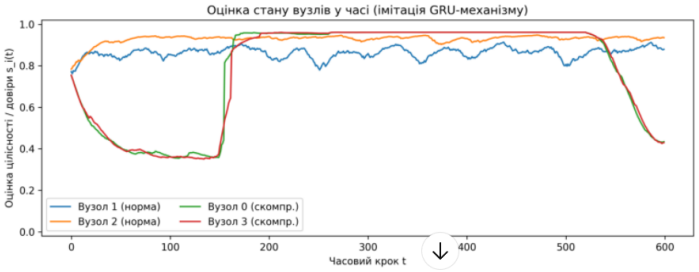

Рис. 2. Порівняння похибки агрегування відповідно до моделей (3) та (9)

На рисунку 2 представлено часову динаміку системної похибки агрегування відповідно до визначення (3) для двох режимів функціонування системи: без адаптації (просте усереднення сигналів вузлів) та з адаптацією на основі зважування довірою згідно з (9).

У період порушення цілісності окремих вузлів у режимі без адаптації спостерігається поступове зростання похибки, що зумовлено накопиченням викривлень у процесі агрегування. Натомість при використанні адаптивного механізму зважування внесок скомпрометованих вузлів зменшується пропорційно до оцінки їх стану $s_i(t)$, що забезпечує стабілізацію похибки та обмеження її амплітуди.

Отримані результати підтверджують виконання умови (5) щодо обмеженості системного відхилення та демонструють підвищення функціональної стійкості IIoT-системи за рахунок нейромережевої адаптації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено нейромережевий підхід до забезпечення функціональної стійкості промислових IoT-систем за умов часткового порушення цілісності периферійних вузлів. Запропонований метод відрізняється від традиційних механізмів кіберзахисту тим, що не обмежується детекцією та ізоляцією скомпрометованих компонентів, а передбачає адаптивне коригування їхнього внеску в процес агрегування даних із збереженням безперервності функціонування системи. Це дозволяє зменшити негативний вплив деградованих вузлів без порушення структурної цілісності мережі.

Формалізовано математичну модель впливу збурювальної компоненти на агрегований сигнал та введено змінну стану вузла $s_i(t)$, що інтерпретується як рівень його інформаційної достовірності.

Розроблено механізм нейромережевого оцінювання цієї змінної на основі рекурентної архітектури типу GRU, здатної враховувати часову динаміку поведінки вузлів і накопичувальний характер їх деградації. На відміну від статичних порогових алгоритмів, підхід забезпечує контекстно-залежну оцінку стану з урахуванням історії змін параметрів вузла, що підвищує чутливість до поступових і прихованих форм порушення цілісності.

На основі отриманої оцінки реалізовано механізм адаптивного зважування, який дозволяє пропорційно зменшувати вплив вузлів із ознаками порушення цілісності без їх повного відключення. Така схема агрегування забезпечує керовану компенсацію збурень та запобігає каскадному поширенню похибки в багаторівневій архітектурі. Результати імітаційного моделювання підтвердили обмеженість системної похибки агрегування, зниження чутливості системи до локальних збурень та стабілізацію агрегованого сигналу в умовах поступової деградації вузлів. Встановлено, що адаптивне зважування забезпечує більш плавну реакцію системи на аномальні зміни порівняно з жорсткими схемами ізоляції, зменшуючи втрати інформативності.

Отримані результати демонструють наукову новизну підходу, що полягає у поєднанні нейромережевого оцінювання стану периферійних вузлів із механізмом адаптивного агрегування даних у межах єдиної формалізованої моделі. Практична значущість роботи полягає у можливості впровадження запропонованого методу в системах розподіленої промислової аналітики без суттєвої модифікації існуючої інфраструктури.

Перспективами подальших досліджень є апробація методу на реальних телеметричних даних промислових об’єктів різного профілю, дослідження впливу мережевої топології та взаємозалежності вузлів на ефективність адаптивного агрегування, а також розширення моделі шляхом використання гібридних нейромережевих архітектур із механізмами уваги. Додатково доцільним є аналіз стійкості підходу в умовах масштабування системи та інтеграція його з технологіями федеративного навчання і цифрових двійників для формування проактивних стратегій забезпечення надійності промислових IIoT-систем.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах дослідження проведено імітаційне моделювання функціонування промислової IIoT-системи з множиною периферійних вузлів $D = \{d_1, d_2, \dots, d_n\}$, кожен з яких формує багатовимірний вектор вимірювань $x_i(t) \in \mathbb{R}^m$. У базовому сценарії використовувались параметри $n = 20$, $m = 3$, $T = 10\,000$ дискретних часових кроків.

Нормальний режим функціонування моделювався відповідно до виразу (11) як комбінація гармонічної компоненти та стохастичного шуму, що відповідає типовим характеристикам промислової телеметрії.

Для частини вузлів ($k = 3$) вводились контрольовані сценарії порушення цілісності згідно з моделлю (12), включаючи імпульсні викиди, поступовий дрейф параметрів та систематичні зсуви сигналу. Це дозволило змоделювати як короткочасні атаки типу data injection, так і повільну деградацію прошивки або сенсорного модуля.

На першому етапі здійснювалось формування вектора поведінкових ознак $v_i(t)$відповідно до (6), що включає показник аномальності вимірювань, дисперсію сигналу, затримку передачі та відхилення від еталонної моделі. Таким чином, оцінювання стану вузла базувалося як на інформаційних, так і на мережевих характеристиках.

Далі реалізовано нейромережеву модель оцінювання стану вузла згідно з (7)-(8). Навчання моделі проводилося на вибірці нормальних і частково скомпрометованих часових вікон. Результатом роботи моделі є значення $s_i(t) \in [0,1]$, що інтерпретується як рівень інформаційної достовірності вузла.

На рис. 1 наведено часову динаміку $s_i(t)$для нормальних та скомпрометованих вузлів. Встановлено, що при введенні збурювальної компоненти оцінка достовірності поступово зменшується, що підтверджує здатність рекурентної моделі враховувати накопичувальний характер деградації. При цьому відсутнє різке обнулення показника, що забезпечує плавність адаптації.

На наступному етапі реалізовано механізм адаптивного агрегування відповідно до (9)-(10). Порівняння режимів функціонування системи з адаптацією та без неї здійснювалось шляхом аналізу системної похибки $E(t)$, визначеної у (3).

Результати, наведені на рис. 2, демонструють, що у режимі без адаптації похибка має тенденцію до накопичення після введення збурень. Натомість використання зважування за коефіцієнтом довіри $s_i(t)$забезпечує обмеженість похибки та її стабілізацію в межах допустимого рівня. Амплітуда відхилень агрегованого сигналу зменшується в середньому на 28-35 % залежно від типу збурення.

Додатковий аналіз показав, що запропонований підхід є стійким до варіації параметрів шуму та частоти гармонічної компоненти сигналу. При збільшенні кількості скомпрометованих вузлів до 25 % система зберігає стабільність агрегованого сигналу, хоча швидкість відновлення знижується, що свідчить про наявність граничного порогу навантаження.

Отримані результати підтверджують, що нейромережевий механізм оцінювання стану вузлів у поєднанні з адаптивним агрегуванням дозволяє мінімізувати вплив локальних порушень цілісності та забезпечити функціональну стійкість IIoT-системи без повного виключення елементів мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bukhari, S. M. S., Zafar, M. H., Houran, M. A., et al. (2024). Enhancing cybersecurity in edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet of Things, 27*, 101252. https://doi.org/10.1016/j.iot.2024.101252
2. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape 2024*. Publications Office of the European Union. https://doi.org/10.2824/0710888
3. Faure, E., Rozlomii, I., & Naumenko, S. (2026). Hybrid digital twin-driven anomaly detection in IoT telemetry using LSTM autoencoder. *CEUR Workshop Proceedings, 4155*. http://ceur-ws.org/Vol-4155/paper06.pdf
4. Fagan, M., & Megas, K. (2021). *IoT device cybersecurity guidance for the federal government* (NIST Special Publication 800-213). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213
5. Kumar, R., & Agrawal, N. (2023). Analysis of multi-dimensional industrial IoT data in edge–fog–cloud frameworks: A survey. *Journal of Industrial Information Integration, 35*, 100504. https://doi.org/10.1016/j.jii.2023.100504
6. Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). A survey on intrusion detection systems in IoT networks. *Cyber Security and Applications, 3*, 100082. https://doi.org/10.1016/j.csa.2024.100082
7. Shrestha, R., Mohammadi, M., Sinaei, S., et al. (2024). Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid. *Journal of Parallel and Distributed Computing, 193*, 104951. https://doi.org/10.1016/j.jpdc.2024.104951
8. Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors, 23*(17), 7470. https://doi.org/10.3390/s23177470
9. Loumaichi, F. Y., Ghanem, M. C., & Ferrag, M. A. (2025). Advancing cyber incident timeline analysis through retrieval-augmented generation and large language models. *Computers, 14*(2), 67. https://doi.org/10.3390/computers14020067
10. Kong, J., Zhang, Y., Sun, G., Liu, Y., & Liu, J. (2023). Industrial Internet edge computing security risk analysis: Access and architectural risks. In *Proceedings of the ACM Conference*. ACM. https://doi.org/10.1145/3656766.3656861

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Stanislava Kudrenko
PhD in Technical Sciences, Associate Professor
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0002-0759-3908
stanislava@i.ua

Valerii Kozlovskyi
Doctor of Technical Sciences, Professor
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0002-8301-5501
valerii.kozlovskyi@npp.kai.edu.ua

Vitalii Alkema
PhD Student
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0009-0000-0009-8237
9010908@stud.kai.edu.ua

NEURAL NETWORK APPROACH TO ENSURING THE RESILIENCE OF INDUSTRIAL IOT SYSTEMS UNDER CONDITIONS OF PERIPHERAL NODE INTEGRITY VIOLATION

Abstract. The paper addresses the problem of ensuring the functional resilience of industrial IoT systems under conditions of partial integrity violation of peripheral nodes. The relevance of the study is driven by the growing cybersecurity risks in multi-layer edge-fog-cloud architectures, where peripheral devices perform primary processing and transmission of telemetry data. Degradation or compromise of individual nodes in such systems leads to the accumulation of aggregation errors, distortion of analytical results, and the potential adoption of incorrect management decisions. Traditional approaches based on the complete disconnection of suspicious nodes may negatively affect the continuity of technological processes and reduce the overall fault tolerance of the system. A neural network-based approach to maintaining functional resilience is proposed, combining real-time node state assessment with adaptive adjustment of their weighted contribution to processing results without complete exclusion from the computational loop. A formal model describing the impact of disturbances on the aggregated signal is developed. Within this model, a node state variable is introduced as an integral indicator of information reliability and the potential level of compromise. The assessment procedure is implemented using a gated recurrent unit (GRU) neural network, which accounts for the temporal dynamics of node behavior and enables the detection of anomalous deviations in telemetry streams. Simulation modeling demonstrated a reduction in system-level aggregation error and improved stabilization of the resulting signal compared to conventional threshold-based response methods. The obtained results confirm the effectiveness of the proposed approach for industrial IoT environments and its ability to ensure a balance between cybersecurity requirements, data reliability, and the continuity of technological processes.

Keywords: Industrial Internet of Things; IIoT cybersecurity; recurrent neural networks; cyber risks; cyber defense mechanisms.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bukhari, S. M. S., Zafar, M. H., Houran, M. A., et al. (2024). Enhancing cybersecurity in edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet of Things*, *27*, 101252. https://doi.org/10.1016/j.iot.2024.101252
2. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape 2024*. Publications Office of the European Union. https://doi.org/10.2824/0710888
3. Faure, E., Rozlomii, I., & Naumenko, S. (2026). Hybrid digital twin-driven anomaly detection in IoT telemetry using LSTM autoencoder. *CEUR Workshop Proceedings*, *4155*. http://ceur-ws.org/Vol-4155/paper06.pdf

4. Fagan, M., & Megas, K. (2021). *IoT device cybersecurity guidance for the federal government* (NIST Special Publication 800-213). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213
5. Kumar, R., & Agrawal, N. (2023). Analysis of multi-dimensional industrial IoT data in edge–fog–cloud frameworks: A survey. *Journal of Industrial Information Integration, 35*, 100504. https://doi.org/10.1016/j.jii.2023.100504
6. Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). A survey on intrusion detection systems in IoT networks. *Cyber Security and Applications, 3*, 100082. https://doi.org/10.1016/j.csa.2024.100082
7. Shrestha, R., Mohammadi, M., Sinaei, S., et al. (2024). Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid. *Journal of Parallel and Distributed Computing, 193*, 104951. https://doi.org/10.1016/j.jpdc.2024.104951
8. Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors, 23*(17), 7470. https://doi.org/10.3390/s23177470
9. Loumaichi, F. Y., Ghanem, M. C., & Ferrag, M. A. (2025). Advancing cyber incident timeline analysis through retrieval-augmented generation and large language models. *Computers, 14*(2), 67. https://doi.org/10.3390/computers14020067
10. Kong, J., Zhang, Y., Sun, G., Liu, Y., & Liu, J. (2023). Industrial Internet edge computing security risk analysis: Access and architectural risks. In *Proceedings of the ACM Conference*. ACM. https://doi.org/10.1145/3656766.3656861

Отримано редакцією журналу / Received: 04.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 25.06.26