КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1282
УДК 004.056:004.738.5:004.77

Прокопович-Ткаченко Дмитро Ігорович
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів, м. Дніпро, Україна;
Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України», м. Київ, Україна;
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID:0000-0002-6590-3898
omega2417@gmail.com

Хрушков Борис Сергійович
незалежний дослідник у сфері кібербезпеки
Університет митної справи та фінансів, м. Дніпро, Україна
ORCID:0009-0002-3978-5012
ghoststad88@gmail.com

Бабенко Костянтин Євгенович
аспірант кафедри комп'ютерних наук та інформаційних технологій
Дніпровський національний університет імені Олеся Гончара, м. Дніпро, Україна
ORCID:0009-0009-0945-7078
babenko-k@365.dnu.edu.ua

Козаченко Ігор Миколайович
начальник підрозділу Державного центру кіберзахисту
Державний центр кіберзахисту
Державної служби спеціального зв'язку та захисту інформації України, м. Київ, Україна
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, м. Київ, Україна
ORCID:0000-0002-0774-7284
i.kozachenko@cip.gov.ua

Черкаський Давид Олександрович
аспірант кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна
ORCID:0009-0003-8516-6252
Cherkaskyi.Dav.O@nmu.one

ФРЕЙМВОРК БЕЗПЕКИ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ ЗА МОДЕЛЛЮ OSI У СИСТЕМАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Статтю присвячено розробленню та експериментальному обґрунтуванню фреймворку кібербезпеки для мережевої взаємодії систем критичної інфраструктури, який поєднує кросрівневий моніторинг за моделлю OSI, дозволений блокчейн, консенсус PBFT, смарт-контракти виявлення інцидентів та автоматизоване реагування. Актуальність дослідження зумовлена тим, що об'єкти енергетики, водопостачання, транспорту, телекомунікацій та інших секторів критичної інфраструктури дедалі частіше зазнають багатоетапних кібератак, які охоплюють кілька рівнів мережевої взаємодії та можуть поєднувати маніпуляції з трафіком, ін'єкцію хибних команд, відмову в обслуговуванні та модифікацію журналів подій. Традиційні централізовані системи виявлення вторгнень залишаються вразливими до компрометації сховищ журналів і створюють єдину точку відмови, що обмежує доказову цінність зібраних подій безпеки. Метою статті є формування цілісної архітектури, у якій агенти моніторингу збирають метадані протокольних блоків даних рівнів L2-L7, хеші та стислі ознаки подій фіксуються в незмінному розподіленому реєстрі, а смарт-контракти виконують кросрівневу кореляцію та ініціюють сценарії реагування. У роботі формалізовано модель загроз, описано структуру блокчейн-реєстру, механізм адаптивної оцінки довіри вузлів, інтегральну оцінку аномальності подій та

алгоритм функціонування фреймворку. Експериментальна перевірка на емуляційному стенді показала, що запропонований підхід забезпечує вищу F1-міру виявлення порівняно із сигнатурною IDS, RF-IDS та централізованим варіантом зберігання подій, зберігаючи прийнятну наскрізну затримку для сценаріїв моніторингу критичної інфраструктури. Отримані результати підтверджують доцільність використання дозволених блокчейн-мереж як довіреного шару журналювання, верифікації та координації реагування на інциденти у розподілених кіберфізичних середовищах.

Ключові слова: кібербезпека; критична інфраструктура; модель OSI; блокчейн; консенсус PBFT; смарт-контракти; системи виявлення вторгнень.

ВСТУП

Постановка проблеми. Об'єкти критичної інфраструктури (КІ) – енергетичні мережі, системи водопостачання, транспортні та телекомунікаційні комплекси – є пріоритетними цілями кібератак, кількість і складність яких стабільно зростає [1, 2]. За даними Агентства Європейського Союзу з питань кібербезпеки, атаки на промислові та інфраструктурні системи належать до провідних категорій загроз останніх років [3]. Особливістю таких атак є їхній багаторівневий характер: зловмисники комбінують підміну кадрів на канальному рівні, маніпуляції маршрутизацією на мережевому рівні, виснаження ресурсів транспортного рівня та ін'єкції команд у прикладні промислові протоколи.

Регуляторний контекст додатково посилює вимоги до захисту КІ. Рамка кібербезпеки NIST CSF 2.0 [2] визначає функції ідентифікації, захисту, виявлення, реагування та відновлення як обов'язкові складові керування ризиками, а стандарт ISO/IEC 27001:2022 [4] вимагає документованої та доказової фіксації інцидентів. Директива ЄС NIS2 поширює зобов'язання щодо звітування про інциденти на операторів суттєвих послуг, що робить цілісність журналів подій не лише технічною, а й комплаєнс-вимогою. Отже, засоби захисту КІ мають одночасно виявляти атаки на різних рівнях мережевої взаємодії та гарантувати неспростовність зафіксованих свідчень.

Традиційні системи виявлення вторгнень (Intrusion Detection System, IDS) для КІ здебільшого будуються за централізованою архітектурою: журнали подій та результати аналізу зберігаються на виділеному сервері [5]. Така архітектура має два принципові недоліки. По-перше, сервер журналювання є єдиною точкою відмови та привабливою ціллю для атакувальника, який після компрометації може модифікувати або видалити свідчення вторгнення. По-друге, централізований аналіз, як правило, обмежується одним-двома рівнями моделі OSI, що унеможливлює кореляцію ознак багаторівневих атак.

Технологія блокчейн забезпечує незмінність (immutability), децентралізацію та криптографічну перевірюваність записів [6-8], що робить її природним кандидатом для захищеного журналювання подій безпеки. Водночас відомі застосування блокчейну в кібербезпеці зосереджені переважно на автентифікації пристроїв або обміні індикаторами компрометації і не інтегрують реєстр із кросрівневим виявленням атак у режимі, близькому до реального часу.

Аналіз останніх досліджень і публікацій. Дослідження, дотичні до цієї роботи, доцільно згрупувати за чотирма напрямами: системи виявлення вторгнень для КІ, застосування блокчейну в кібербезпеці, кросрівневий мережевий моніторинг та автоматизоване реагування на інциденти.

Виявлення вторгнень у КІ. Класичні сигнатурні та аномалійні IDS адаптовано до промислових протоколів (Modbus/TCP, DNP3) у низці робіт [9, 10]. Еталонні датасети, зокрема CICIDS2017 [5], уможливили відтворюване порівняння методів машинного навчання; ансамблеві класифікатори на кшталт випадкового лісу демонструють F1-міру понад 92 % на мережевих потоках [11]. Утім, зазначені системи зберігають результати централізовано і не гарантують цілісності доказової бази після компрометації сервера.

Блокчейн у кібербезпеці. Після появи Bitcoin [6] та платформ смарт-контрактів [12] дозволені блокчейни, насамперед Hyperledger Fabric [7], знайшли застосування у промислових сценаріях з обмеженим колом учасників. Протокол практичної візантійської відмовостійкості (Practical Byzantine Fault Tolerance, PBFT) [8] забезпечує фіналізацію транзакцій за прийнятної затримки в мережах із десятками вузлів. Оглядові праці [1, 13, 14] систематизують застосування блокчейну для розумних міст і промислового Інтернету речей, однак констатують брак рішень, у яких реєстр інтегровано безпосередньо в контур виявлення атак.

Кросрівневий моніторинг. Роботи з кросрівневого аналізу [15, 16] показують, що кореляція ознак кількох рівнів OSI суттєво підвищує повноту виявлення багатоетапних атак порівняно з аналізом лише мережевого потоку. Проте відомі підходи не розв'язують задачі довіреного обміну ознаками між розподіленими сенсорами.

Автоматизоване реагування. Огляд рішень класу SOAR (Security Orchestration, Automation and Response) [17] засвідчує, що якість автоматичного реагування критично залежить від достовірності вхідних подій – саме тієї властивості, яку забезпечує незмінний реєстр. Нормативні рамки NIST CSF 2.0 [2] та ISO/IEC 27001 [4] додатково вимагають доказової фіксації інцидентів.

Таблиця 1 узагальнює порівняння репрезентативних підходів за чотирма критеріями: охоплення рівнів OSI, наявність гарантій цілісності журналів, стійкість до компрометації сенсорів та автоматизація реагування. Як видно з таблиці, кожен окремий напрям розв'язує частину задачі: класичні IDS дають високу якість виявлення без гарантій цілісності; блокчейн-рішення забезпечують незмінність, але слабко інтегровані з виявленням; кросрівневі підходи покращують повноту, залишаючи відкритим питання довіри до розподілених сенсорів.

Таблиця 1

Порівняння репрезентативних груп підходів («+» – властивість забезпечено, «±» – частково, «−» – відсутня)

Група підходів	Рівні OSI	Цілісність журналів	Стійкість сенсорів	SOAR
Сигнатурні/аномалійні IDS [5, 9-11]	L3-L4	−	−	−
Блокчейн для автентифікації/обміну IoC [1, 13, 14]	L7	+	±	−
Кросрівневі IDS [15, 16]	L2-L7	−	−	−
SOAR-платформи [17]	–	±	−	+
Запропонований фреймворк	L2-L7	+	+	+

Прогалина дослідження. Аналіз (таблиця 1) показує, що в літературі відсутній цілісний фреймворк, який одночасно (i) корелює ознаки атак на рівнях L2-L7 моделі OSI, (ii) фіксує події безпеки в незмінному розподіленому реєстрі з візантійською відмовостійкістю та (iii) замикає контур автоматизованим реагуванням на основі смарт-контрактів. Заповнення цієї прогалини і є предметом подальших розділів.

Метою статті є розроблення та експериментальна оцінка фреймворку безпеки, який поєднує кросрівневий моніторинг мережевої взаємодії за моделлю OSI з дозволеним блокчейном і смарт-контрактами виявлення для систем КІ. Для досягнення поставленої мети необхідно вирішити такі задачі:

1. Формалізувати модель загроз для мережевої взаємодії КІ, що охоплює атаки на рівнях L2-L7 моделі OSI, та сформулювати вимоги до захищеного журналювання подій.
2. Запропонувати чотирирівневу архітектуру фреймворку, в якій агенти моніторингу, дозволений блокчейн із консенсусом PBFT, смарт-контракти виявлення та модуль реагування утворюють замкнений контур керування безпекою.
3. Розробити механізм кросрівневої кореляції ознак з адаптивним оцінюванням довіри вузлів реєстру.
4. Виконати експериментальну оцінку на емуляційному стенді, яка продемонструвала перевагу фреймворку над базовими підходами за точністю виявлення та прийнятні накладні витрати за затримкою.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретичну основу дослідження становлять положення кібербезпеки критичної інфраструктури, кросрівневого аналізу мережевої взаємодії за моделлю OSI, концепція дозволених блокчейн-мереж та механізми автоматизованого реагування на інциденти. Модель OSI використано як аналітичну рамку для зіставлення ознак атак на канальному, мережевому, транспортному та прикладному рівнях.

Дозволений блокчейн розглядається як довірений шар журналювання, у якому незмінність записів забезпечується криптографічним зв’язуванням блоків, а узгодження стану реєстру здійснюється консенсусом PBFT. Смарт-контракти в такій архітектурі виконують роль формалізованих правил кореляції подій, оцінювання довіри джерел і запуску сценаріїв реагування.

МЕТОДИКА ДОСЛІДЖЕННЯ

Модель загроз і постановка задачі. Розглядається мережа КІ з множиною вузлів $V = \{v_1, \ldots, v_n\}$, що обмінюються протокольними блоками даних (Protocol Data Unit, PDU) на рівнях L = {L2, L3, L4, L7} моделі OSI. Модель атакувальника задається множиною спроможностей

$$A = \{aDoS, aMitM, ainj, atamp\}, \quad (1)$$

де a_{DoS} – атаки відмови в обслуговуванні на рівнях L3-L4; a_{MitM} – перехоплення та підміна трафіку («людина посередині») на рівнях L2-L3; a_{inj} – ін'єкція хибних команд у прикладні протоколи рівня L7; a_{tamp} – модифікація або видалення журналів подій безпеки. Атакувальник може компрометувати до f вузлів реєстру, але не контролює канали розповсюдження ключів. Задача полягає в побудові функції виявлення, що максимізує F1-міру класифікації подій за обмеження на наскрізну затримку виявлення, та в гарантуванні незмінності зафіксованих подій за наявності f зловмисних вузлів.

Архітектура фреймворку. Рисунок 1 подає загальну архітектуру запропонованого фреймворку, що складається з чотирьох функціональних шарів. Перший шар утворюють агенти моніторингу, розгорнуті на межових пристроях мережі КІ: вони пасивно вилучають метадані PDU рівнів L2-L7 (адреси, прапорці, розміри, часові мітки, коди функцій промислових протоколів), не втручаючись у технологічний трафік. Другий шар – дозволений блокчейн, вузли якого підтримують реєстр подій безпеки та досягають згоди за протоколом PBFT. Третій шар реалізує логіку виявлення у формі смарт-контрактів, що виконуються детерміновано на всіх вузлах-валідаторах. Четвертий шар – модуль реагування класу SOAR, який за підтвердженим інцидентом ініціює дії (ізоляція сегмента, оновлення правил фільтрації) та повертає оновлені політики агентам моніторингу, замикаючи контур керування.

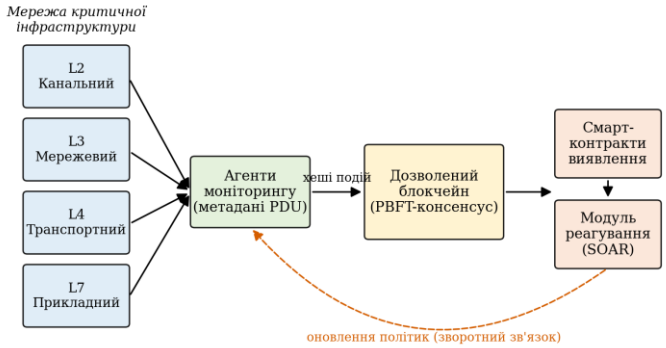

Рис. 1. Архітектура запропонованого фреймворку. Агенти збирають метадані PDU рівнів L2-L7, хеші подій фіксуються в дозволеному блокчейні з консенсусом PBFT, смарт-контракти виконують виявлення, а модуль SOAR реалізує реагування зі зворотним зв'язком до агентів.

Потік даних у фреймворку організовано за принципом мінімізації навантаження на реєстр: у блокчейн записуються лише хеші подій, стислі вектори ознак та результати класифікації, тоді як первинні захоплення трафіку зберігаються локально на агентах з можливістю верифікації за хешем на вимогу. Такий поділ on-chain та off-chain даних утримує розмір транзакції в межах 1-2 кБ і забезпечує конфіденційність технологічного трафіку. Керування доступом реалізовано засобами інфраструктури відкритих ключів дозволеної мережі: кожен агент і валідатор володіє сертифікатом, виданим центром сертифікації оператора КІ, що виключає участь неавторизованих вузлів.

Структура реєстру та гарантії цілісності. Події безпеки агрегуються у блоки. Заголовок i-го блоку зв'язується з попереднім криптографічним хешем:

$$Hi = SHA\text{-}256(Hi{-}1 \,\|\, ri \,\|\, ti \,\|\, MRKi), \quad (2)$$

де H_{i-1} – хеш попереднього блоку; r_i – випадковий одноразовий номер; t_i – часова мітка; MRK_i – корінь дерева Меркла над множиною подій блоку; ‖ позначає конкатенацію. Завдяки ланцюжку хешів у формулі (2) модифікація будь-якої історичної події вимагає переобчислення всіх наступних блоків на більшості вузлів. Стійкість консенсусу PBFT до зловмисних учасників визначається класичним обмеженням

$$N \geq 3f + 1, \quad (3)$$

де N – загальна кількість вузлів-валідаторів, а f – максимальна кількість візантійських (довільно несправних) вузлів [8]. У розгортаннях фреймворку значення N обирається згідно з нерівністю (3) з операційного запасу $f \geq 1$.

Адаптивна оцінка довіри вузлів. Для зниження впливу скомпрометованих агентів кожному джерелу подій j призначається динамічна оцінка довіри, що оновлюється експоненційним згладжуванням:

$$Tj(t) = \lambda Tj(t-1) + (1 - \lambda)\cdot Vj / (Vj + Ij), \quad (4)$$

де $T_j(t) \in [0, 1]$ – оцінка довіри вузла j у момент t; $\lambda \in (0, 1)$ – коефіцієнт інерції (у експериментах $\lambda = 0.9$); V_j та I_j – кількість підтверджених (валідних) і спростованих подій вузла за поточне вікно відповідно. Події від вузлів із T_j нижче порогу 0.5 виключаються з кореляції до відновлення довіри.

Кросрівневе виявлення. Смарт-контракт виявлення обчислює інтегральну оцінку аномальності події x як зважену суму рівневих оцінок:

$$S(x) = \Sigma l \in L\ wl\cdot sl(xl),\ \Sigma l \in L\ wl = 1, \quad (5)$$

де sl(xl) ∈ [0, 1] – оцінка аномальності ознак рівня l, отримана градієнтним бустингом над деревами рішень, навченим поза ланцюгом (off-chain) і зафіксованим у реєстрі у вигляді контрольної суми моделі; wl – ваги рівнів, підібрані на валідаційній вибірці (wL2 = 0.15, wL3 = 0.30, wL4 = 0.25, wL7 = 0.30; емуляційні дані). Подія класифікується як атака, якщо S(x) перевищує поріг θ = 0.62, обраний за максимумом F1 на валідації.

Наскрізна затримка виявлення декомпонується як:

$$\tau det = \tau agg + \tau cons + \tau sc, \quad (6)$$

де τ_{agg} – час агрегування ознак агентом; τ_{cons} – затримка консенсусу PBFT; τ_{sc} – час виконання смарт-контракту. Складові формули (6) вимірюються окремо в розділі 4 для локалізації вузьких місць.

Алгоритм функціонування. Узагальнений цикл оброблення однієї події безпеки (Алгоритм 1) складається з таких кроків:

Крок 1. агент моніторингу вилучає метадані PDU рівнів L2–L7 і формує вектор ознак x із часовою міткою та ідентифікатором джерела;

Крок 2. агент обчислює хеш SHA-256 вектора ознак і надсилає транзакцію (хеш, стислі ознаки, підпис) до найближчого вузла-валідатора;

Крок 3. валідатори перевіряють підпис і оцінку довіри джерела за формулою (4); транзакції від вузлів з T_j < 0.5 відхиляються;

Крок 4. прийняті транзакції впорядковуються протоколом PBFT і включаються до чергового блоку згідно з формулою (2);

Крок 5. після фіналізації блоку смарт-контракт виявлення обчислює інтегральну оцінку S(x) за формулою (5) і за перевищення порогу θ створює запис інциденту;

Крок 6. модуль реагування зчитує підтверджений інцидент, виконує визначений сценарій (ізоляція сегмента, блокування джерела, сповіщення оператора) та публікує в реєстрі оновлені політики моніторингу;

Крок 7. агенти застосовують оновлені політики, після чого оцінки довіри джерел коригуються за результатами верифікації подій.

Кроки 1-2 виконуються локально на агентах і не блокують технологічний трафік; кроки 3-5 – розподілено на валідаторах; складність смарт-контракту виявлення лінійна за кількістю рівневих ознак, що забезпечує детермінований час виконання, необхідний для консенсусного середовища [18].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експериментальний стенд і дані. Оцінювання виконано на емуляційному стенді, конфігурацію якого узагальнює таблиця 2. Мережу КІ емульовано в Mininet з топологією підстанції (24 кінцеві пристрої, 6 комутаторів); блокчейн розгорнуто на платформі Hyperledger Fabric v2.5 [7] з 4–16 вузлами-валідаторами. Навчальну та тестову вибірки сформовано з двох джерел: публічного датасету CICIDS2017 [5] (класи DoS та MitM-подібні атаки) і синтетичного SCADA-трафіку Modbus/TCP з ін'єкціями хибних команд, згенерованого відповідно до тактик матриці MITRE ATT&CK for ICS [19, 20]. Загальний обсяг – 1,84 млн потоків (70 % навчання, 10 % валідація, 20 % тестування; стратифікація за класами). Кожен експеримент повторено 10 разів із різними випадковими зернами; наведено середні значення та 95 % довірчі інтервали. [Усі числові значення – дані емуляційного стенда, що потребують польової валідації.]

Передоброблення охоплювало агрегування пакетів у двонаправлені потоки, вилучення 78 потокових ознак, нормалізацію за медіаною та міжквартильним розмахом, а також балансування

навчальної вибірки методом стратифікованого підвибирання мажоритарного класу до співвідношення 3:1. Якість класифікації оцінювано точністю (accuracy), влучністю (precision, *P*), повнотою (recall, *R*) та F1-мірою, що обчислюється як

$$F1 = 2PR / (P + R), \quad (7)$$

де *P* – частка істинних атак серед подій, класифікованих як атаки, а *R* – частка виявлених атак серед усіх фактичних. Значення у формулі (7) усереднювались макроусередненням за класами атак. Продуктивність блокчейн-шару характеризувалась пропускною здатністю реєстру (транзакцій за секунду) та складовими затримки за формулою (6), вимірюваними інструментом Hyperledger Caliper [21].

Таблиця 2

Конфігурація експериментального стенда (емуляційний стенд)

Параметр	Значення
Емуляція мережі	Mininet 2.3, топологія підстанції: 24 хости, 6 комутаторів
Блокчейн-платформа	Hyperledger Fabric v2.5, консенсус PBFT
Кількість валідаторів	4 / 8 / 16 (варіюється)
Апаратне забезпечення	4 сервери: 16 vCPU, 64 GB RAM, 10 GbE
Дані	CICIDS2017 + синтетичний Modbus/TCP; 1,84 млн потоків
Класи	Норма, DoS, MitM, Ін'єкція команд
Повторюваність	n = 10 прогонів; mean ± 95 % CI

Продуктивність блокчейн-шару. Рисунок 2 демонструє залежність пропускної здатності реєстру та затримки консенсусу від вхідного навантаження для конфігурації з чотирма валідаторами. До навантаження приблизно 800 транзакцій за секунду пропускна здатність зростає майже лінійно (рис. 2, а), досягаючи насичення на рівні 842 тр/с; подальше збільшення навантаження не підвищує пропускної здатності, натомість затримка консенсусу зростає надлінійно (рис. 2, б) – з 187 мс за 500 тр/с до 596 мс за 1000 тр/с. Отже, робочою зоною фреймворку слід вважати навантаження до 700-800 тр/с, що з запасом перекриває інтенсивність подій безпеки типової підстанції.

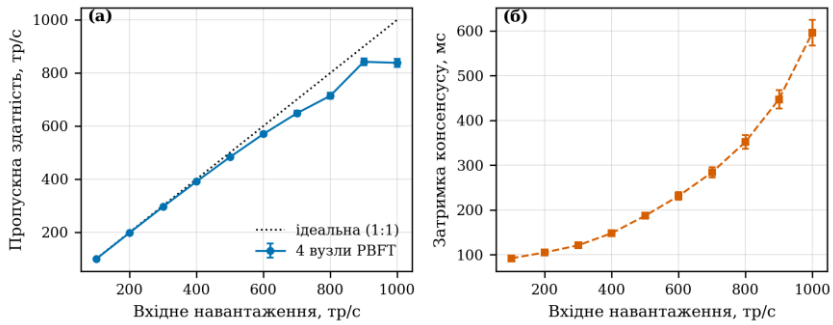

Рис. 2. Продуктивність блокчейн-шару (4 вузли PBFT, n = 10, вуса – 95 % CI):
(а) пропускна здатність проти вхідного навантаження; пунктир – ідеальна характеристика 1:1;
(б) затримка консенсусу проти навантаження. Дані емуляційного стенда.

Декомпозиція наскрізної затримки за формулою (6) у робочій точці 500 тр/с дала такі складові: агрегування ознак агентом τ_agg = 19 мс (8,7 %), консенсус τ_cons = 187 мс (85,8 %), виконання смарт-контракту τ_sc = 12 мс (5,5 %); сумарно τ_det = 218 мс. Домінування консенсусної складової вказує, що подальше зниження затримки слід шукати саме в оптимізації протоколу узгодження – пакетуванні транзакцій, конвеєризації фаз PBFT або переході до комітетних схем [22], а не в спрощенні логіки виявлення.

Якість виявлення атак. Запропонований фреймворк порівняно з трьома базовими підходами: сигнатурною IDS (Suricata з промисловим набором правил), класифікатором випадкового лісу над потоковими ознаками (RF-IDS) та варіантом фреймворку без блокчейн-шару (централізоване зберігання подій). Таблиця 3 подає зведені метрики; рисунок 3 візуалізує їх із довірчими інтервалами. Фреймворк досягає точності 97,4 % та F1-міри 96,3 %, перевищуючи RF-IDS на 3,5 п.п. за F1, а сигнатурний підхід –

на 9,2 п.п. Перевага над безблокчейновим варіантом (+1,2 п.п. F1) зумовлена механізмом довіри вузлів за формулою (4), який пригнічує хибні події скомпрометованих агентів. Відмінності статистично значущі за критерієм Вілкоксона для парних вибірок ($p < 0.01$, $n = 10$).

Таблиця 3

Порівняння якості виявлення та затримки (mean, n = 10; найкращі значення — жирним). Дані емуляційного стенда

Модель	Точність, %	Precision, %	Recall, %	F1, %	τ_det, мс
Сигнатурна IDS	88,6	90,1	84,3	87,1	95
RF-IDS	94,1	93,2	92,5	92,8	142
Без блокчейну	96,2	95,5	94,8	95,1	163
Запропонований	97.4	96,8	95,9	96,3	218

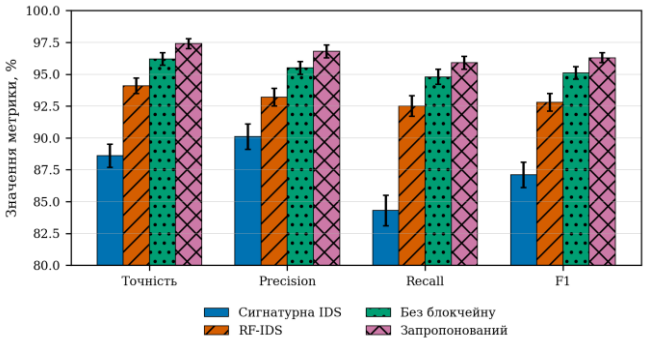

Рис. 3. Порівняння моделей за чотирма метриками якості (mean ± 95% CI, n = 10). Штрихування дублює колір для читаності у чорно-білому друці. Дані емуляційного стенда.

Розподіл помилок за класами ілюструє рисунок 4. Найвищу повноту досягнуто для класу «Норма» (0,985) та DoS-атак (0,968); найскладнішим є клас MitM (0,941), де 3,4 % подій хибно віднесено до норми через подібність легітимного ARP-трафіку до підготовчої фази атаки. Частка хибнопозитивних спрацювань загалом становить 1,5 %, що прийнятно для операційних центрів безпеки КІ.

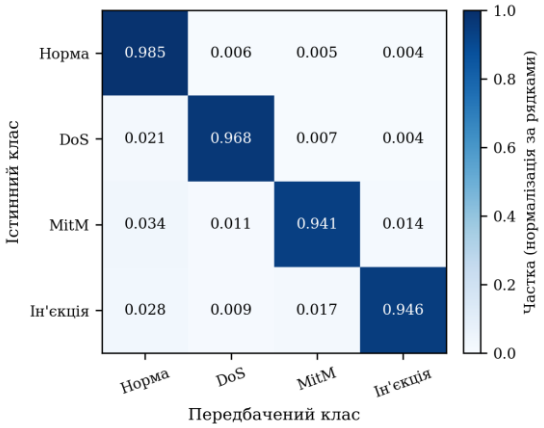

Рис. 4. Нормалізована за рядками матриця невідповідностей запропонованого фреймворку на тестовій вибірці (частки; сума в рядку дорівнює 1). Дані емуляційного стенда.

Абляційне дослідження. Внесок окремих компонентів оцінено вилученням кожного з них із повної конфігурації (таблиця 4, рисунок 5). Найбільшу деградацію (−4,9 п.п. F1) спричиняє вилучення смарт-контрактів виявлення із заміною на порогові правила; вилучення кросрівневої кореляції за формулою (5) коштує −3,2 п.п., що підтверджує цінність ознак кількох рівнів OSI. Заміна блокчейн-реєстру централізованою базою даних знижує F1 на 1,2 п.п. у сценарії з одним скомпрометованим агентом і, що суттєвіше, позбавляє систему гарантій незмінності доказової бази.

Таблиця 4

Абляційне дослідження: зміна F1 відносно повної конфігурації (96.3 %). Дані емуляційного стенда

Вилучений компонент	F1, %	ΔF1, п.п.
Смарт-контракти виявлення	91.4	−4.9
Кросрівнева кореляція (L2–L7)	93.1	−3.2
Оцінка довіри вузлів	94.5	−1.8
Блокчейн-реєстр (централізована БД)	95.1	−1.2
Модуль реагування (SOAR)	95.7	−0.6

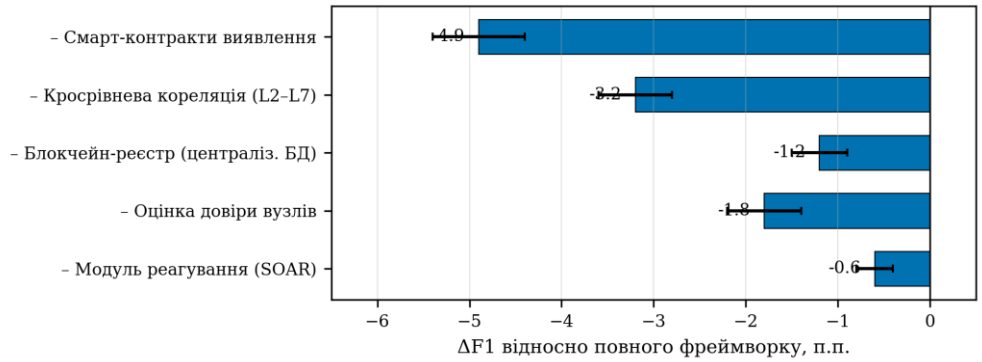

Рис. 5. Зміна F1-міри після вилучення окремих компонентів відносно повного фреймворку (вуса – 95 % CI, n = 10). Дані емуляційного стенда.

Масштабованість за кількістю валідаторів. Вплив розміру мережі валідаторів оцінено для конфігурацій з 4, 8 та 16 вузлами за фіксованого навантаження 500 тр/с. Затримка консенсусу зросла з 187 мс (4 вузли) до 264 мс (8 вузлів) та 412 мс (16 вузлів), що узгоджується з квадратичною комунікаційною складністю PBFT за кількістю учасників [8]; пропускна здатність у точці насичення знизилась з 842 до 731 та 583 тр/с відповідно. Гранична кількість толерованих зловмисних вузлів за формулою (3) при цьому зросла з f = 1 до f = 2 та f = 5. Отже, вибір розміру мережі є компромісом між відмовостійкістю та продуктивністю: для типового об'єкта КІ з одним оператором доцільні 4–8 валідаторів, тоді як міжорганізаційні федерації, що потребують $f \geq 3$, мають закладати відповідний запас продуктивності або переходити до ієрархічних схем консенсусу [22].

Обговорення результатів і обмеження дослідження. Отримані результати свідчать, що інтеграція дозволеного блокчейну в контур виявлення не лише забезпечує незмінність доказової бази, а й дає вимірюваний приріст якості класифікації завдяки механізму довіри вузлів: хибні події скомпрометованих агентів послаблюються ще до етапу кореляції. Ціною є збільшення наскрізної затримки виявлення з 163 до 218 мс (формула (6)); декомпозиція показує, що 86 % приросту припадає на консенсус PBFT. Для подій безпеки КІ, де типовий цикл реагування вимірюється секундами, така затримка є прийнятною, однак для задач захисту в реальному часі на рівні окремих кадрів вона може бути завеликою.

Порівняння з опублікованими результатами блокчейн-орієнтованих IDS для промислового Інтернету речей [13, 14, 23] показує, що досягнута F1-міра перебуває на рівні кращих відомих рішень або перевищує його, при цьому запропонований фреймворк додатково охоплює чотири рівні OSI замість одного-двох. Пряме кількісне зіставлення, утім, ускладнене відмінністю датасетів і протоколів оцінювання.

З погляду практичного впровадження фреймворк природно відображається на функції NIST CSF 2.0 [2]: агенти моніторингу реалізують функцію виявлення (Detect), незмінний реєстр підтримує функції реагування та відновлення (Respond, Recover) доказовою базою інцидентів, а механізм довіри вузлів посилює функцію захисту (Protect) у частині цілісності телеметрії. Пасивний характер агентів дозволяє поетапне розгортання без модифікації наявного технологічного обладнання, що є суттєвим для об'єктів КІ з тривалими циклами сертифікації, і узгоджується з принципами архітектури нульової довіри для операційних технологій [24]. Додатковою перевагою дозволеної моделі блокчейну є сумісність із вимогами конфіденційності: у реєстрі фіксуються хеші та агреговані ознаки, а не первинний трафік.

Обмеження. По-перше, усі наведені числові результати отримано на емуляційному стенді із синтетичною складовою трафіку; перенесення результатів на реальні об'єкти КІ потребує окремої

польової валідації. По-друге, масштабованість консенсусу PBFT досліджено лише до 16 валідаторів; для великих федерацій операторів доцільні ієрархічні або комітетні схеми консенсусу. По-третє, модель загроз не охоплює атаки на самі криптографічні примітиви, зокрема з боку квантових обчислювачів, та фізичні атаки на агенти. По-четверте, енергетичні й адміністративні накладні витрати експлуатації блокчейн-шару в цій роботі не оцінювались.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі запропоновано та експериментально оцінено фреймворк безпеки для мережевої взаємодії систем критичної інфраструктури, який поєднує кросрівневий моніторинг за моделлю OSI, дозволений блокчейн із консенсусом PBFT, смарт-контракти виявлення та автоматизоване реагування. На емуляційному стенді фреймворк досяг точності 97,4 % і F1-міри 96,3 %, перевершивши сигнатурний, ансамблевий та безблокчейновий базові підходи на 1,2-9,2 п.п. F1 за середньої затримки виявлення 218 мс і пропускної здатності реєстру 842 тр/с; абляційне дослідження підтвердило внесок кожного компонента. Подальші дослідження буде спрямовано на: (i) польову валідацію на діючому об'єкті енергетичної інфраструктури, зокрема з використанням цифрових двійників [25]; (ii) масштабовані схеми консенсусу та федеративне навчання моделей виявлення для федерацій із десятками операторів [26]; (iii) інтеграцію постквантових криптографічних примітивів у структуру реєстру [27].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. *Sensors, 23*(7), 3681. https://doi.org/10.3390/s23073681
2. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
3. European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
4. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection-Information security management systems-Requirements*. ISO. https://www.iso.org/standard/27001
5. Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)* (pp. 108-116). SciTePress. https://doi.org/10.5220/0006639801080116
6. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
7. Androulaki, E., Barger, A., Bortnikov, V., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference (EuroSys 2018)* (Article 30, pp. 1-15). ACM. https://doi.org/10.1145/3190508.3190538
8. Castro, M., & Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems, 20*(4), 398–461. https://doi.org/10.1145/571637.571640
9. Wang, W., Mosse, D., Sun, Y., & Zhang, L. (2021). Industrial control malicious traffic anomaly detection system based on improved deep autoencoder. *Frontiers in Energy Research, 8*, 555145. https://doi.org/10.3389/fenrg.2020.555145
10. Supeno, B. A., Mohamed Radzi, N. A. B., & Al-Haiqi, A. (2025). Machine learning-based anomaly detection for Modbus and DNP3 protocols in industrial control systems. In *2025 International Conference on Technology and Policy in Energy and Electric Power (ICT-PEP)*. IEEE. https://doi.org/10.1109/ICT-PEP67281.2025.11232367
11. Azhar, M., Perveen, S., Iqbal, A., & Lee, B. (2024). IDRandom-Forest: Advanced Random Forest for real-time intrusion detection. *IEEE Access, 12*, 113842-113854. https://doi.org/10.1109/ACCESS.2024.3443408
12. Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf
13. Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2023). A secure and trusted mechanism for Industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics, 19*(2), 1894–1902. https://doi.org/10.1109/TII.2022.3182121
14. Ghadi, Y. Y., et al. (2025). A hybrid AI-blockchain security framework for smart grids. *Scientific Reports, 15*, 05257. https://doi.org/10.1038/s41598-025-05257-w

15. Georgiades, M., et al. (2025). An explainable AI approach for interpretable cross-layer intrusion detection. *Electronics, 14*(16), 3218. https://doi.org/10.3390/electronics14163218
16. Maosa, H., et al. (2024). A hierarchical security event correlation model for real-time intrusion detection. *Cybersecurity, 4*(1), 4. https://doi.org/10.3390/cyber4010004
17. Karlzén, H., & Sommestad, T. (2023). Automatic incident response solutions: A review of proposed solutions' input and output. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023)* (Article 37, pp. 1–9). ACM. https://doi.org/10.1145/3600160.3605066
18. Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology, 159*, 107221. https://doi.org/10.1016/j.infsof.2023.107221
19. MITRE Corporation. (2026). *MITRE ATT&CK® knowledge base*. https://attack.mitre.org/
20. Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). MITRE ATT&CK: State of the art and way forward. *ACM Computing Surveys, 57*(2), Article 39. https://doi.org/10.1145/3687300
21. Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2022). An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Computers & Industrial Engineering, 173*, 108716. https://doi.org/10.1016/j.cie.2022.108716
22. Liu, W., Zhang, X., Feng, W., Huang, M., & Xu, Y. (2022). Optimization of PBFT algorithm based on QoS-aware trust service evaluation. *Sensors, 22*(12), 4590. https://doi.org/10.3390/s22124590
23. Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D.-S. (2024). Tides of blockchain in IoT cybersecurity. *Sensors, 24*(10), 3111. https://doi.org/10.3390/s24103111
24. Ortmann, M., et al. (2024). *Zero trust architectures for interconnected industry*. Fraunhofer Institute for Production Technology IPT. https://doi.org/10.24406/publica-3778
25. Barreto, N. E. M., et al. (2025). Cyber-physical power system digital twins – A study on resilience, flexibility and cybersecurity. *Energies, 18*(22), 5960. https://doi.org/10.3390/en18225960
26. Novikova, E., Doynikova, E., & Golubev, S. (2022). Federated learning for intrusion detection in the critical infrastructures: Vertically partitioned data use case. *Algorithms, 15*(4), 104. https://doi.org/10.3390/a15040104
27. Castiglione, A., Esposito, J. G., Loia, V., Nappi, M., Pero, C., & Polsinelli, M. (2025). Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Transactions on Industrial Informatics, 21*(2), 1674–1683. https://doi.org/10.1109/TII.2024.3485796

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Dmytro Prokopovych-Tkachenko
Candidate of Technical Sciences, Associate Professor,
Head of the Department of Cybersecurity and Information Technologies
University of Customs and Finance, Dnipro, Ukraine;
Scientific Research Institute of Informatics, Security and Law of the
National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine;
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID:0000-0002-6590-3898
omega2417@gmail.com

Borys Khrushkov
Independent researcher in cybersecurity
University of Customs and Finance, Dnipro, Ukraine
ORCID:0009-0002-3978-5012
ghoststad88@gmail.com

Kostiantyn Babenko
PhD Student, Department of Computer Science and Information Technologies
Oles Honchar Dnipro National University, Dnipro, Ukraine
ORCID:0009-0009-0945-7078
babenko-k@365.dnu.edu.ua

Ihor Kozachenko
Head of a unit of the State Cyber Protection Centre
Senior Lecturer at the Department of Software Engineering and Cybersecurity
State Cyber Protection Centre of the
State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine;
State University of Trade and Economics, Kyiv, Ukraine
ORCID:0000-0002-0774-7284
i.kozachenko@cip.gov.ua

Davyd Cherkaskyi
PhD Student, Department of Information Security and Telecommunications
Dnipro University of Technology, Dnipro, Ukraine
ORCID:0009-0003-8516-6252
Cherkaskyi.Dav.O@nmu.one

BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR OSI MODEL NETWORK INTERACTION IN CRITICAL INFRASTRUCTURE SYSTEMS

Abstract. The article develops and experimentally evaluates a cybersecurity framework for network interaction in critical infrastructure systems by combining cross-layer OSI monitoring, permissioned blockchain, PBFT consensus, smart-contract-based detection and automated response. The relevance of the study is determined by the growing exposure of energy, water supply, transport, telecommunications and other critical infrastructure sectors to multi-stage cyberattacks that affect several layers of network communication and may include traffic manipulation, false command injection, denial-of-service actions and tampering with security logs. Conventional centralized intrusion detection architectures remain vulnerable to the compromise of event repositories and create a single point of failure, which limits the evidentiary value and operational reliability of collected security events. The aim of the article is to propose an integrated architecture in which monitoring agents collect metadata of protocol data units from OSI layers L2-L7, hashes and compressed event features are recorded in an immutable distributed ledger, and smart contracts perform cross-layer correlation and initiate response scenarios. The paper formalizes the threat model, describes the structure of the blockchain registry, introduces an adaptive trust assessment mechanism for event sources, defines an integral anomaly score and presents the operational algorithm of the framework. Experimental evaluation on an emulation testbed demonstrates that the proposed approach achieves a higher F1 score than a signature-based IDS, an RF-IDS and a centralized event-storage variant while preserving acceptable end-to-end

detection latency for critical infrastructure monitoring scenarios. The results confirm the feasibility of using permissioned blockchain networks as a trusted layer for logging, verification and response coordination in distributed cyber-physical environments where the integrity and traceability of security evidence are essential.

Keywords: cybersecurity; critical infrastructure; OSI model; blockchain; PBFT consensus; smart contracts; intrusion detection systems.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. *Sensors, 23*(7), 3681. https://doi.org/10.3390/s23073681
2. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
3. European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
4. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection-Information security management systems-Requirements*. ISO. https://www.iso.org/standard/27001
5. Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)* (pp. 108-116). SciTePress. https://doi.org/10.5220/0006639801080116
6. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
7. Androulaki, E., Barger, A., Bortnikov, V., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference (EuroSys 2018)* (Article 30, pp. 1-15). ACM. https://doi.org/10.1145/3190508.3190538
8. Castro, M., & Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems, 20*(4), 398–461. https://doi.org/10.1145/571637.571640
9. Wang, W., Mosse, D., Sun, Y., & Zhang, L. (2021). Industrial control malicious traffic anomaly detection system based on improved deep autoencoder. *Frontiers in Energy Research, 8*, 555145. https://doi.org/10.3389/fenrg.2020.555145
10. Supeno, B. A., Mohamed Radzi, N. A. B., & Al-Haiqi, A. (2025). Machine learning-based anomaly detection for Modbus and DNP3 protocols in industrial control systems. In *2025 International Conference on Technology and Policy in Energy and Electric Power (ICT-PEP)*. IEEE. https://doi.org/10.1109/ICT-PEP67281.2025.11232367
11. Azhar, M., Perveen, S., Iqbal, A., & Lee, B. (2024). IDRandom-Forest: Advanced Random Forest for real-time intrusion detection. *IEEE Access, 12*, 113842-113854. https://doi.org/10.1109/ACCESS.2024.3443408
12. Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf
13. Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2023). A secure and trusted mechanism for Industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics, 19*(2), 1894–1902. https://doi.org/10.1109/TII.2022.3182121
14. Ghadi, Y. Y., et al. (2025). A hybrid AI-blockchain security framework for smart grids. *Scientific Reports, 15*, 05257. https://doi.org/10.1038/s41598-025-05257-w
15. Georgiades, M., et al. (2025). An explainable AI approach for interpretable cross-layer intrusion detection. *Electronics, 14*(16), 3218. https://doi.org/10.3390/electronics14163218
16. Maosa, H., et al. (2024). A hierarchical security event correlation model for real-time intrusion detection. *Cybersecurity, 4*(1), 4. https://doi.org/10.3390/cyber4010004
17. Karlzén, H., & Sommestad, T. (2023). Automatic incident response solutions: A review of proposed solutions' input and output. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023)* (Article 37, pp. 1–9). ACM. https://doi.org/10.1145/3600160.3605066
18. Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology, 159*, 107221. https://doi.org/10.1016/j.infsof.2023.107221
19. MITRE Corporation. (2026). *MITRE ATT&CK® knowledge base*. https://attack.mitre.org/

20. Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). MITRE ATT&CK: State of the art and way forward. *ACM Computing Surveys, 57*(2), Article 39. https://doi.org/10.1145/3687300
21. Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2022). An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Computers & Industrial Engineering, 173*, 108716. https://doi.org/10.1016/j.cie.2022.108716
22. Liu, W., Zhang, X., Feng, W., Huang, M., & Xu, Y. (2022). Optimization of PBFT algorithm based on QoS-aware trust service evaluation. *Sensors, 22*(12), 4590. https://doi.org/10.3390/s22124590
23. Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D.-S. (2024). Tides of blockchain in IoT cybersecurity. *Sensors, 24*(10), 3111. https://doi.org/10.3390/s24103111
24. Ortmann, M., et al. (2024). *Zero trust architectures for interconnected industry*. Fraunhofer Institute for Production Technology IPT. https://doi.org/10.24406/publica-3778
25. Barreto, N. E. M., et al. (2025). Cyber-physical power system digital twins – A study on resilience, flexibility and cybersecurity. *Energies, 18*(22), 5960. https://doi.org/10.3390/en18225960
26. Novikova, E., Doynikova, E., & Golubev, S. (2022). Federated learning for intrusion detection in the critical infrastructures: Vertically partitioned data use case. *Algorithms, 15*(4), 104. https://doi.org/10.3390/a15040104
27. Castiglione, A., Esposito, J. G., Loia, V., Nappi, M., Pero, C., & Polsinelli, M. (2025). Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Transactions on Industrial Informatics, 21*(2), 1674–1683. https://doi.org/10.1109/TII.2024.3485796

Отримано редакцією журналу / Received: 07.02.26
Прорецензовано / Revised: 20.02.26
Схвалено до друку / Accepted: 24.09.26