УДК 004.056.5:004.738.5 DOI 10.18372/2073-4751.87.21688

Пастущак Д.В.,
orcid.org/0009-0008-9120-8291,
e-mail: 3910994@stud.kai.edu.ua,
Міщенко А.В.,
orcid.org/0000-0001-8376-1777,
e-mail: andrii.mishchenko@npp.kai.edu.ua

МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ IoT-СИСТЕМ: СУЧАСНІ ПРАКТИКИ ТА ПЕРСПЕКТИВИ ДОСЛІДЖЕНЬ

Національний університет «Київський авіаційний інститут»

Вступ

Інтернет речей (IoT) став невід'ємною складовою цифрової інфраструктури промисловості, транспорту, охорони здоров'я та інших критичних секторів [3], [6]. Масове розгортання пристроїв водночас надає зловмисникам широкі можливості для пошуку вразливих цілей [8] – зокрема, у блокчейн-мережах розподіленої відновлюваної енергетики зафіксовано SQL-ін'єкції, підміну даних (спуфінг) та атаки «людина посередині» [4], а безпека IoT безпосередньо пов'язана із захистом критичної інфраструктури та національною безпекою [8]. Особливо небезпечною є інтеграція IoT з кіберфізичними та промисловими системами, де компрометація впливає на фізичні процеси [10], [13], а ботнети показали, як легко незахищені пристрої використовуються для масштабних DDoS-атак [16].

IoT-мережі поєднують різнорідні технології, що спричиняє проблеми сумісності, обмеженої обчислювальної потужності, пам'яті та мережевого підключення пристроїв [3]. Обмеження ресурсів ускладнюють застосування повноцінних засобів захисту [8], [14], а пристрої часто працюють на застарілих прошивках через обмежені можливості оновлення [8]. Неоднорідність середовищ [9], [13] та слабка автентифікація, зокрема стандартні паролі, які користувачі рідко змінюють [8], [18], посилюють ці вразливості.

Для захисту IoT запропоновано виявлення вторгнень на основі машинного навчання [1], [13], [15], [16], блокчейн-рішення для автентифікації та управління довірою [5], [7], [9], обчислення на рівні Fog та федеративне навчання [2], [6], [11], а також енергоефективні механізми безпеки [8]. Апаратні атаки розглянуто у [17], методологію тестування IoT-пристроїв – у [18]. Водночас залишаються невирішеними питання розриву між лабораторною точністю методів та їх застосовністю на пристроях з обмеженими ресурсами [8], [12], інтеграції різних методів захисту в єдину систему [2], [9] та відсутності формалізованих критеріїв вибору засобів захисту для різних рівнів архітектури [3], [14].

Мета

Метою статті є систематизація та порівняльний аналіз сучасних методів підвищення захищеності IoT-систем із формалізацією критеріїв їх вибору для рівнів архітектури Edge–Fog–Cloud, а також визначення перспективних напрямів досліджень.

Основна частина

Рівень Edge: криптографічні рішення для пристроїв з обмеженими ресурсами

Рівень Edge утворюють кінцеві пристрої з обмеженими обчислювальними ресурсами та автономним живленням, тому засоби захисту цього рівня мають бути ощадними за обчисленнями та енергоспоживанням [8], [14].

Для IoT-пристроїв із суворими обмеженнями обчислювальної потужності та енергії розроблено легковагову криптографію: блокові шифри PRESENT, SIMON, SPECK, оптимізовані для малих блоків даних і мінімальних накладних витрат [14], [20], [21], а також еліптичну криптографію, що забезпечує рівень безпеки

RSA за менших розмірів ключів [14], [18]. Серед стандартизованих легковагових рішень слід виділити родину Ascon: у 2025 р. NIST затвердив Ascon-AEAD128, Ascon-Hash256 та Ascon-XOF128 для пристроїв з обмеженими ресурсами [25], а перехід до Ascon як стандарту легковагової криптографії відзначено і в оглядах [14]. Енерговитрати визначаються добутком споживаної потужності на час активної роботи вузла [9]; для операції шифрування повідомлення це дає:

$$E_{enc} = P \cdot t_{enc} = \frac{P \cdot L}{v} \qquad (1)$$

де P – потужність, що споживає мікроконтролер під час шифрування, Вт; L – довжина повідомлення, біт; v – швидкодія алгоритму, біт/с. За припущення сталої потужності та швидкодії енерговитрати обернено пропорційні швидкодії алгоритму, що й зумовлює перевагу легковагових шифрів для автономних пристроїв.

Розвиток квантових обчислень потребує квантово-стійких алгоритмів [14], оскільки ECC без додаткових заходів вразлива до постквантових атак [3], [7]. Механізм інкапсуляції ключів ML-KEM, стандартизований у FIPS 203 на основі CRYSTALS-Kyber [22], застосовують для узгодження ключів, а схему цифрового підпису ML-DSA, стандартизовану у FIPS 204 на основі CRYSTALS-Dilithium [23], – для підписів та автентифікації. Такі схеми потребують значних обчислень: у [7] для їх прискорення застосовано графічні процесори (GPU). Зменшити накладні витрати криптографії дають змогу апаратні криптографічні модулі та TPM [8], [14].

На основі джерел [7], [14], [18], [20]–[22], [25] проведено порівняльний аналіз криптографічних рішень (табл. 1).

Таблиця 1. Порівняльний аналіз криптографічних рішень для IoT

Алгоритм	**Тип**	**Розмір ключа, біт**	**Швидкодія**	**Енерго-витрати**	**Квантова стійкість**	**Джерела**
AES-256	Симетричний шифр	256	Помірна (програмно)	Підвищені	Стійкий (128 біт)	[14], [18]
PRESENT	Легковаговий симетричний шифр	80/128	Висока (апаратно)	Низькі	Залежить від довжини ключа	[14], [20]
SIMON/SPECK	Легковагові симетричні шифри	64–256	Висока	Низькі	Залежить від довжини ключа	[14], [21]
Ascon-AEAD128	Легковаговий автентифікований шифр (AEAD)	128	Висока	Низькі	Залежить від довжини ключа	[14], [25]
ECC-256	Узгодження ключів, підписи	256	Висока	Низькі	Вразливий	[7], [18]
CRYSTALS-Kyber (ML-KEM)	Постквантова інкапсуляція ключів	6400–12544 (відкр. ключ)	Знижена	Підвищені	Стійкий	[7], [22]
** Оцінки швидкодії та енерговитрат є якісними й залежать від реалізації, платформи та апаратного прискорення; симетричні шифри та механізми узгодження ключів виконують різні функції і не є взаємозамінними*						

Результати табл. 1 свідчать, що для пристроїв з обмеженими ресурсами доцільними є легковагові шифри, причому для нових розробок перевагу варто надавати стандартизованому Ascon-AEAD128 [25], а для автентифікації та

узгодження ключів – ECC [14], [18]. AES-256 зберігає стійкість до квантових атак завдяки довжині ключа [18], тоді як ECC вразлива до них, натомість ML-KEM (Kyber) має значно більші ключі, тому доцільність його застосування слід перевіряти для конкретного мікроконтролера [7], [22]. Слід також враховувати, що PRESENT має 64-бітний блок, який обмежує безпечний обсяг даних, зашифрованих на одному ключі, а PRESENT-80 через довжину ключа не підходить для довготривалого захисту; SIMON і SPECK не є стандартами NIST.

Рівень Edge: захист від апаратних атак

Безпечне завантаження. Безпечне завантаження (secure boot) забезпечує запуск лише прошивки з перевіреним цифровим підписом, що за коректної реалізації запобігає запуску непідписаного або модифікованого коду; перевірку доцільно виконувати з опорою на апаратний корінь довіри, зокрема TPM [8], [17], [18].

Виявлення фізичного втручання та побічні канали. Апаратні засоби з вбудованим виявленням втручання ускладнюють несанкціонований доступ до ключів [8], [17]. Атаки через побічні канали (аналіз енергоспоживання) та ін'єкцію помилок детально розглянуто в [17]; вони залишаються актуальними для легковагових криптографічних реалізацій [14], [17].

Отже, на рівні Edge основу захисту становлять легковагові криптографічні алгоритми, безпечне завантаження та апаратні засоби виявлення втручання, а вибір між ними обмежений насамперед ресурсами пристрою [8], [14], [17].

Рівень Fog: розподілені системи виявлення вторгнень

Централізоване оброблення даних IoT обмежене мережевими накладними витратами, затримками та ризиками для конфіденційності [11], [16], тоді як обчислення на рівні Fog наближають оброблення до периметра мережі та зменшують затримку [6]. Сумарний час виконання завдань у системі Fog–Cloud визначається як [2]:

$$T_{tot} = \sum_{i=1}^{X} \frac{D_i}{PR_F} + \sum_{j=1}^{Y} \frac{D_j}{PR_C} \quad (2)$$

де X, Y – кількість завдань, оброблених на вузлі рівня Fog та у Cloud; D_i, D_j – обсяг даних завдання; PR_F, PR_C – швидкість оброблення даних вузлом рівня Fog і серверами Cloud з урахуванням затримки поширення [2]. За умови достатньої продуктивності вузла рівня Fog і меншої ефективної затримки порівняно з Cloud перенесення аналізу трафіку на цей рівень зменшує Y, а отже, і частку завдань із найбільшою затримкою.

Федеративне навчання дає змогу навчати моделі без передавання необроблених даних; у базовому алгоритмі FedAvg глобальна модель формується агрегуванням параметрів [19]:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k \quad (3)$$

де K – кількість учасників; n_k – обсяг локальної вибірки k-го учасника; n – загальний обсяг вибірок; w^k_{t+1} – параметри локальної моделі. У [11] для неоднорідних (non-IID) даних вузли рівня Fog спільно навчають модель без доступу до даних один одного: приватні ідентифікатори класів перешкоджають відновленню даних GAN-атаками, агрегування виконує алгоритм FedProx, а серед розглянутих загроз – атаки логічного виведення та отруєння даних.

Для порівняння систем виявлення вторгнень (СВВ) використовують частку виявлених атак, частку хибних тривог та F-міру [11], [13], [16]:

$$TPR = \frac{TP}{TP+FN}, \; FPR = \frac{FP}{FP+TN} \quad (4)$$

$$F_1 = \frac{2 \cdot Pr \cdot TPR}{Pr+TPR} \quad (5)$$

де TP, TN – кількість правильно класифікованих атак і нормальних подій; FP, FN – кількість хибних тривог і пропущених атак; $Pr = TP/(TP + FP)$ – прецизійність (precision). Для IoT критичним є показник FPR, оскільки навіть невелика частка хибних тривог за обсягу в мільйони подій перевантажує операторів.

Характеристики методів виявлення вторгнень за даними джерел [1], [10], [11], [13], [15] наведено в табл. 2.

Таблиця 2. Характеристики методів виявлення вторгнень для IoT за даними джерел

Метод	**Дж.**	**Набір даних**	**Accuracy, %**	**F1, %**	**Розміщення**	**Необроблені дані за межі вузла**
Beta Hebbian Learning	[1]	Трафік MQTT	–*	–*	Візуальний аналіз експертом	Не вказано
Ensemble Learning	[13]	Edge-IIoTset / CICIoT2023	96,01 / 93,19	95,94 / 93,24	Не вказано	Не вказано
Few-Shot Learning (1D-CNN + ProtoNet, 10-shot)	[15]	MQTT-IoT-IDS2020 / CICIDS2017	99,44 / 93,13	99,42 / 92,40	Не вказано	Не вказано
LSTM-CNN	[10]	CICIoT2023, Malimg	91,66 (LSTM)	92,00 (LSTM)	Бортовий комп'ютер верстата	Так (віддалене сховище)
PP-FDL (федеративне)	[11]	MNIST / CIFAR-10	93,07 / 84,21	92,09 / 83,21	Fog + Cloud	Ні
* *метод візуального аналізу, числові метрики не наводяться*						

Дані табл. 2 не можна порівнювати безпосередньо, оскільки отримані на різних наборах даних. Найвищу F-міру показав Few-Shot Learning на MQTT-IoT-IDS2020 (99,42 %) [15], ансамблеве навчання – 95,94 % на Edge-IIoTset ціною підвищених обчислювальних вимог [13]. Метод BHL [1] призначений для візуального аналізу оператором і числових метрик не має. Виявлення в [10] виконується на бортовому комп'ютері верстата, проте сам верстат зберігає дані у віддаленому сховищі, тому повна локальність даних не підтверджена; у [11] сирі дані не залишають вузол рівня Fog, однак PP-FDL перевірено лише на MNIST і CIFAR-10, а глибокі моделі складно розгортати безпосередньо на IoT-пристроях через обмеження пам'яті [16].

Рівень Cloud: модель нульової довіри

Модель Zero Trust ґрунтується на принципі «ніколи не довіряй, завжди перевіряй» і не вважає довіреною жодну сутність усередині чи поза мережею [7]. Блокчейн не є обов'язковим складником моделі, проте у поєднанні з нею забезпечує децентралізоване управління доступом: за результатами експерименту в [7] досягнуто 98 % збереження конфіденційності та 96 % ефективності контролю доступу, а у [9] блокчейн застосовано для безпечної інтеграції сенсорних мереж в екосистеми Fog–Cloud. Накладні витрати на постійні перевірки можна зменшити апаратними криптографічними модулями [8].

Систематизація методів захисту за рівнями архітектури

За аналогією зі зваженими моделями оцінювання вузлів і завдань у [2], [9] для вибору методів захисту на *j*-му рівні архітектури запропоновано інтегральний показник:

$$Q_j = \sum_{i=1}^{m} \alpha_i q_{ij} \qquad (6)$$

де q_{ij} – нормована оцінка *j*-го методу за *i*-м критерієм; α_i – ваговий коефіцієнт критерію ($\sum \alpha_i = 1$); m – кількість критеріїв. На основі [2], [3], [6], [7], [9], [17] отримано систематизацію, наведену в табл. 3.

Таблиця 3. Систематизація методів захисту за рівнями IoT-архітектури

Рівень	Основні загрози	Методи захисту	Ефективність	Складність впровадження
Edge (пристрої)	Фізичний доступ, атаки через побічні канали	Secure boot, захист від втручання, легковагові шифри	Висока	Середня
Комунікації	Перехоплення, підміна	TLS, шифрування каналу	Висока	Низька
Fog (шлюзи)	Перевантаження шкідливими завданнями, Sybil	Розподілені СВВ, федеративне навчання, управління довірою	Середня	Висока
Cloud (центри)	Ризики централізованого розгортання: єдина точка відмови, масовий витік даних	Zero Trust, блокчейн	Висока	Дуже висока

Табл. 3 показує необхідність диференційованого підходу: на рівні Edge пріоритетним є захист від фізичних атак [17], рівень Fog є доцільним для розподілених СВВ на основі федеративного навчання [6], [11], а на рівні Cloud – Zero Trust у поєднанні з блокчейн-автентифікацією [7], [9].

Для ілюстрації застосування (6) розраховано Q_j для методів з табл. 2, що мають числові метрики, за трьома критеріями: якість виявлення (q_1 – найвища F-міра з табл. 2), ресурсоощадність (q_2: 0,25 – джерело вказує на підвищені обчислювальні вимоги [13], [16]; 0,5 – даних немає; 0,75 – джерело повідомляє про знижені накладні витрати порівняно з аналогами [11]) та конфіденційність (q_3: 1,0 – джерело вказує, що необроблені дані не залишають вузол [11]; 0,5 – не вказано; 0,25 – джерело вказує на передавання даних у віддалене сховище [10]). Ваги (α_1; α_2; α_3) задано експертно з урахуванням пріоритетів рівнів, визначених у джерелах: для Edge – обмеження ресурсів та енергії [8], [14] (0,2; 0,6; 0,2); для Fog – затримка та конфіденційність [6], [11] (0,3; 0,3; 0,4); для Cloud – ресурси не є обмеженням [2], [6] (0,6; 0,1; 0,3). Результати наведено в табл. 4.

Таблиця 4. Ілюстративний розрахунок інтегрального показника Q для методів виявлення вторгнень

Метод	q1 (якість)	q2 (ресурсо-ощадність)	q3 (конфіден-ційність)	Q (Edge)	Q (Fog)	Q (Cloud)
Ensemble Learning	0,96	0,25	0,50	0,44	0,56	0,75
Few-Shot Learning	0,99	0,50	0,50	0,60	0,65	0,79
LSTM-CNN	0,92	0,25	0,25	0,38	0,45	0,65
PP-FDL	0,92	0,75	1,00	0,83	0,90	0,93

Згідно з табл. 4, за прийнятих оцінок і ваг найвищий показник на всіх рівнях має федеративне навчання PP-FDL (0,83; 0,90; 0,93), друге місце на рівні Edge посідає Few-Shot Learning (0,60), на рівнях Fog і Cloud – також Few-Shot Learning (0,65; 0,79). Цей

розрахунок є ілюстративним сценарієм багатокритеріального оцінювання, а не емпіричним рейтингом методів: оцінки q_1 отримано на різних наборах даних, а q_2 і q_3 мають якісний характер і залежать від повноти опису в джерелах. Аналіз чутливості показав, що на рівні Fog перевага федеративного навчання зберігається за будь-якої ваги конфіденційності α_3 від 0,2 до 0,6 (за рівних $\alpha_1 = \alpha_2$). Значення для рівня Edge є умовними, оскільки PP-FDL [11] за архітектурою належить до рівнів Fog і Cloud, а оптимізацію для кінцевих пристроїв з обмеженими ресурсами автори відносять до невирішених питань. Обґрунтований рейтинг потребує експериментального порівняння методів на єдиному наборі даних і на однаковій апаратурі.

Практичні рекомендації

Фізична безпека. Налагоджувальні інтерфейси JTAG, UART та SWD у виробничому режимі слід вимикати або блокувати, обмежувати фізичний доступ до них і застосовувати автентифіковане налагодження, а криптографічні ключі зберігати в захищених апаратних модулях [8], [17], [18].

Прошивка та оновлення. Необхідно застосовувати безпечне завантаження [3], [8], [17], [18] та регламент управління вразливостями, що забезпечує своєчасне оновлення прошивок і програмного забезпечення; пристрій має перевіряти цифровий підпис оновлення відкритим ключем видавця [8].

Протоколи та доступ. Для захисту даних під час передавання слід використовувати TLS/DTLS [8], зокрема для MQTT, який сам не шифрує трафік і має працювати поверх TLS [1], а для Wi-Fi – стандарт WPA3 [8]. Від захоплення пристроїв захищають надійні паролі, вимкнення непотрібних служб і списки контролю доступу [3], [8].

Організаційні заходи. Для систематизації управління ризиками доцільно використовувати NIST Cybersecurity Framework 2.0 з функціями Govern, Identify, Protect, Detect, Respond і Recover [24], відмовлятися від стандартних облікових даних і проводити тестування захищеності пристроїв за структурованою методологією [18].

Висновки

1. Безпека IoT є комплексною проблемою, що охоплює всі рівні архітектури Edge–Fog–Cloud, зокрема обмеження ресурсів пристроїв, недоліки прошивки й протоколів та організаційні фактори, і потребує спеціалізованих легковагових та апаратно захищених рішень [3], [8].

2. Для пристроїв рівня Edge найпридатнішими є легковагові блокові шифри та ECC, тоді як постквантові схеми на основі решіток мають значно більші ключі, тому їх застосовність слід перевіряти для конкретної апаратної платформи [7], [22].

3. За умови достатньої продуктивності вузлів розміщення СВВ на рівні Fog зменшує частку завдань з найбільшою затримкою (2), а федеративне навчання (3) дає змогу не передавати необроблені дані; водночас метрики методів у джерелах отримано на різних наборах даних, що унеможливлює їх пряме порівняння [2], [11], [15].

4. Запропонований інтегральний показник (6) формалізує вибір методів захисту для рівнів Edge–Fog–Cloud. Ілюстративний розрахунок за наявними в джерелах оцінками дає найвищий показник для федеративного навчання на рівні Fog (0,90), стійкий до зміни ваги конфіденційності в діапазоні 0,2–0,6; цей результат не є емпіричним рейтингом методів і потребує експериментальної перевірки.

Перспективами подальших досліджень є експериментальне порівняння методів виявлення вторгнень на єдиному наборі даних та IoT-апаратурі, визначення вагових коефіцієнтів показника (6) методами експертного оцінювання та оцінка постквантових схем на мікроконтролерах.

Література

1. Michelena Á., García Ordás M.T., Aveleira-Mata J., et al. Beta Hebbian Learning for intrusion detection in networks with MQTT Protocols for IoT devices. Logic

Journal of the IGPL. 2024. Vol. 32(2). P. 352–365. DOI: 10.1093/jigpal/jzae013.

2. Alvi A.N., Ali B., Saleh M.S., et al. Secure Computing for Fog-Enabled Industrial IoT. Sensors. 2024. Vol. 24(7). Art. 2098. DOI: 10.3390/s24072098.

3. Szymoniak S., Piątkowski J., Kurkowski M. Defense and Security Mechanisms in the Internet of Things: A Review. Applied Sciences. 2025. Vol. 15(2). Art. 499. DOI: 10.3390/app15020499.

4. Faheem M., Al-Khasawneh M.A., Khan A.A., et al. Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: A study on big datasets. Data in Brief. 2024. Vol. 53. Art. 110212. DOI: 10.1016/j.dib.2024.110212.

5. Chen Y., Yang X., Li T., et al. A blockchain-empowered authentication scheme for worm detection in wireless sensor network. Digital Communications and Networks. 2024. Vol. 10(2). P. 265–272. DOI: 10.1016/j.dcan.2022.04.007.

6. Al-Shareeda M.A., Alsadhan A.A., Qasim H.H., et al. The fog computing for internet of things: review, characteristics and challenges, and open issues. Bulletin of Electrical Engineering and Informatics. 2024. Vol. 13(2). P. 1080–1089. DOI: 10.11591/eei.v13i2.5555.

7. Aleisa M.A. Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. IEEE Access. 2025. Vol. 13. P. 18660–18676. DOI: 10.1109/ACCESS.2025.3529309.

8. He P., Zhou Y., Qin X. A Survey on Energy-Aware Security Mechanisms for the Internet of Things. Future Internet. 2024. Vol. 16(4). Art. 128. DOI: 10.3390/fi16040128.

9. Rehman A., Alharbi O. Bioinspired Blockchain Framework for Secure and Scalable Wireless Sensor Network Integration in Fog–Cloud Ecosystems. Computers. 2025. Vol. 14(1). Art. 3. DOI: 10.3390/computers14010003.

10. Saeidlou S., Ghadiminia N., Oti-Sarpong K. Cyber-Physical System Security for Manufacturing Industry 4.0 Using LSTM-CNN Parallel Orchestration. IEEE Access. 2025. Vol. 13. P. 3788–3801. DOI: 10.1109/ACCESS.2025.3525520.

11. Abdel-Basset M., Hawash H., Moustafa N., et al. Privacy-preserved learning from non-i.i.d data in fog-assisted IoT: A federated learning approach. Digital Communications and Networks. 2024. Vol. 10(2). P. 404–415. DOI: 10.1016/j.dcan.2022.12.013.

12. Abdullah A., Albaihani A.N.A., Osman B., et al. Detecting Wormhole Attack in Environmental Monitoring System for Agriculture using Deep Learning. Journal of Advanced Research in Applied Sciences and Engineering Technology. 2025. Vol. 51(2). P. 153–176. DOI: 10.37934/araset.51.2.153176.

13. Jeffrey N., Tan Q., Villar J.R. Using Ensemble Learning for Anomaly Detection in Cyber–Physical Systems. Electronics. 2024. Vol. 13(7). Art. 1391. DOI: 10.3390/electronics13071391.

14. Wakili A., Bakkali S. Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. Cyber Security and Applications. 2025. Vol. 3. Art. 100084. DOI: 10.1016/j.csa.2025.100084.

15. Althiyabi T., Ahmad I., Alassafi M.O. Enhancing IoT Security: A Few-Shot Learning Approach for Intrusion Detection. Mathematics. 2024. Vol. 12(7). Art. 1055. DOI: 10.3390/math12071055.

16. Lefoane M., Ghafir I., Kabir S., et al. Internet of Things botnets: A survey on Artificial Intelligence based detection techniques. Journal of Network and Computer Applications. 2025. Vol. 236. Art. 104110. DOI: 10.1016/j.jnca.2025.104110.

17. van Woudenberg J., O'Flynn C. The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. San Francisco : No Starch Press,2021. 512 p.

18. Chantzis F., Stais I., Calderon P.,et al. Practical IoT Hacking:The Definitive Guide to Attacking the Internet of Things.San Francisco:No Starch Press,2021. 464 p.

19. McMahan H.B., Moore E., Ramage D., et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS). 2017. PMLR 54. P. 1273–1282.

20. Bogdanov A., Knudsen L.R., Leander G., et al. PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems – CHES 2007. LNCS 4727. Berlin : Springer, 2007. P. 450–466. DOI: 10.1007/978-3-540-74735-2_31.

21. Beaulieu R., Shors D., Smith J., et al. The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive.2013.Report 2013/404.

22. National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203.Gaithersburg,2024.DOI: 10.6028/NIST.FIPS.203.

23. National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. FIPS 204. Gaithersburg,2024.DOI:10.6028/NIST.FIPS.204.

24. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Papers, CSWP 29. Gaithersburg, 2024. DOI: 10.6028/NIST.CSWP.29.

25. Sönmez Turan M., McKay K.A., Chang D.,et al. Ascon-Based Lightweight Cryptography Standards for Constrained Devices:Authenticated Encryption, Hash, and Extendable Output Functions. NIST Special Publication 800-232.Gaithersburg,2025.DOI: 10.6028/NIST.SP.800-232.

Пастущак Д.В., Міщенко А.В.

МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ IoT-СИСТЕМ: СУЧАСНІ ПРАКТИКИ ТА ПЕРСПЕКТИВИ ДОСЛІДЖЕНЬ

У статті систематизовано сучасні методи підвищення захищеності IoT-систем. Проаналізовано виклики безпеки IoT, зумовлені обмеженими ресурсами пристроїв, недоліками протоколів та організаційними факторами. Розглянуто засоби захисту рівнів Edge, Fog і Cloud: проведено порівняльний аналіз криптографічних рішень для пристроїв з обмеженими ресурсами та методів виявлення вторгнень на основі штучного інтелекту за опублікованими метриками якості. Формалізовано енерговитрати на шифрування та час оброблення в системі Fog–Cloud, запропоновано інтегральний показник вибору методів захисту для рівнів архітектури Edge–Fog–Cloud і виконано аналіз його чутливості. Сформульовано практичні рекомендації щодо фізичної безпеки, прошивки, протоколів та організаційних заходів.

Ключові слова: *Інтернет речей, кібербезпека, легковагова криптографія, системи виявлення вторгнень, федеративне навчання, обчислення Fog.*

Pastushchak D., Mishchenko A.

METHODS FOR ENHANCING THE SECURITY OF IoT SYSTEMS: CURRENT PRACTICES AND RESEARCH PERSPECTIVES

The paper systematizes current methods for improving the security of IoT systems. Security challenges caused by resource-constrained devices, protocol weaknesses and organizational factors are analyzed. Protection measures for the Edge, Fog and Cloud layers are considered: a comparative analysis of cryptographic solutions for constrained devices and of artificial intelligence-based intrusion detection methods based on published quality metrics is carried out. Encryption energy consumption and processing time in a Fog–Cloud system are formalized, an integral indicator for selecting protection methods for the Edge–Fog–Cloud architecture layers is proposed, and its sensitivity is analyzed. Practical recommendations on physical security, firmware, protocols and organizational measures are formulated.

Keywords: *Internet of Things, cybersecurity, lightweight cryptography, intrusion detection systems, federated learning, fog computing.*

Стаття подана до редакції: 03*/10/2026*
Стаття прийнята до опублікування:11/10/2026
Стаття опублікована: 10/11/2026

Стаття поширюється на умовах ліцензії CC BY 4.0