УДК 004.056.5:004.738.5
DOI https://doi.org/10.32782/tnv-tech.2026.1.1.22

КІБЕРБЕЗПЕКА ІОТ-МЕРЕЖ: НОВІ ЗАГРОЗИ ТА АРХІТЕКТУРНІ МОДЕЛІ ЗАХИСТУ

Нежуренко О. Г. *– кандидат технічних наук,*
старший викладач кафедри комп'ютерних наук та інформаційних технологій
Житомирського державного університету імені Івана Франка
ORCID ID: 0009-0007-4594-9606

Проаналізовано підходи до безпеки мереж Інтернету речей включно з AI-based технологіями виявлення DDoS-загроз, моделями архітектури нульової довіри та методами захисту від шкідливого ПЗ для екосистем з більш ніж 50 мільярдами підключенних пристроїв.

Мета дослідження – вивчити моделі безпеки для IoT-мереж і проаналізувати сучасні загрози в heterogeneous IoT-системах.

Наукова новизна роботи полягає у дослідженні застосування штучного інтелекту для виявлення аномалій у трафіку IoT через поєднання нейронних мереж CNN, RNN та LSTM які показують точність 94–97% та рівень помилкових спрацювань 1.8–3.5%, аналізі математичних моделей розповсюдження кібератак на основі дискретних систем зі станами Susceptible Infected Recovered для прогнозування поширення шкідливих програм через розрахунок базового коефіцієнта відтворення R0, систематизації підходів до пріоритезації вразливостей з використанням оцінки CVSS для визначення рівня загроз а саме: критичні 9.0–10.0, високі 7.0–8.9, середні 4.0–6.9 низькі 0.1–3.9 та розробці рекомендацій щодо впровадження архітектури нульової довіри для екосистем IoT з динамічною оцінкою довіри безперервною автентифікацією мікросегментацією та автоматизованим застосуванням політик для забезпечення доступності 99.7% з часом реагування на інциденти 3–5 хвилин замість звичних 45 хвилин.

Дані досліджень підтверджують ефективність інтегрованого підходу до безпеки. Використання ML-алгоритмів дозволяє виявляти DDoS-атаки з точністю від 94 до 97 відсотків. Модель нульової довіри забезпечує ізоляцію скомпрометованих пристроїв. Технологія blockchain гарантує цілісність даних. Такий комплексний підхід скорочує час реагування з 45 хвилин до 3–5 хвилин. При цьому кількість успішних атак знижується на 68%.

Висновки. Кібербезпека мереж Інтернету речей вимагає інтеграції декількох компонентів. AI-засновані засоби виявлення загроз є першим елементом. Архітектура Zero Trust забезпечує другий рівень захисту. Федеративне навчання зберігає конфіденційність даних. Оптимізовані криптографічні рішення підходять для пристроїв з обмеженими ресурсами.

Ключові слова: *IoT-безпека, розподілені атаки відмови в обслуговуванні, машинне навчання, архітектура нульової довіри, intrusion detection systems.*

Nezhurenko O. H. Cybersecurity of IoT networks: new threats and architectural protection models

Architectural approaches for cybersecurity in IoT networks was studied including technologies for DDoS attack detection based on artificial intelligence, Zero Trust Architecture models and malware propagation protection mechanisms for multi-level protection implementation in systems with over 50 billion connected devices.

The purpose of the article is to investigate modern architectural models for protecting IoT networks and analyse new cyber threats arising in heterogeneous Internet of Things environments.

The scientific novelty consists in a comprehensive study of the application of artificial intelligence methods to detect anomalies in IoT traffic through a combination of Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) architectures with a detection accuracy of 94–97% and a false positive rate of 1.8–3.5%, analysis of mathematical models of the spread of cyberattacks based on discrete-time compartmental systems with SIR-like states (Susceptible, Infected, Recovered) to predict malware propagation by calculating the basic reproduction number R0 as an epidemic threshold,

systematization of vulnerability prioritization frameworks using CVSS scoring to categorize the criticality of threats (Critical 9.0–10.0, High 7.0–8.9, Medium 4.0–6.9, Low 0.1-3.9) and development of recommendations for the implementation of a zero-trust architecture for IoT ecosystems with dynamic trust scoring, continuous authentication, micro-segmentation and automated policy enforcement to ensure 99.7% uptime with incident response time of 3–5 minutes instead of the traditional 45 minutes.

Results. It was verified that the combined approaches of machine learning for DDoS attack detection (accuracy 94–97%) Zero Trust Architecture for isolating compromised devices and blockchain technologies for ensuring data integrity have the ability to decrease the incident response time from 45 minutes to 3-5 minutes and reduce successful attacks by 68% that are observed.

Conclusions. For guaranteeing IoT network cybersecurity it has the aim to combine AI-based detection mechanisms zero-trust architecture federated learning for privacy protection and lightweight cryptographic mechanisms to accommodate resource-constrained devices that are used.

Key words: *IoT security, distributed denial of service attacks, machine learning, zero-trust architecture, intrusion detection systems.*

Вступ. IoT змінив підходи до технологічних систем через інтеграцію фізичних об'єктів з цифровими мережами. Обсяг підключених девайсів сягне понад 50 млрд включно з розумними будинками, індустріальним обладнанням, медичними пристроями та транспортними системами. Основні проблеми безпеки виникають через слабкі паролі які встановлені виробниками, відсутність своєчасних оновлень програмного забезпечення та різноманітність протоколів передачі даних. Для забезпечення стабільної роботи потрібна доступність на рівні 99,99%, системи виявлення аномалій які працюють в режимі реального часу, швидке реагування на інциденти та низьке навантаження на процесори пристроїв. Вимоги до проектування системи має на меті охоплення забезпечення безперервності обслуговування на 99,99% розподілені механізми поведінкової аналітики, автономну оркестрацію реагування на загрози та мінімізацію обчислювальних витрат для вбудованих процесорів що застосовуються.

Головна складність полягає у виборі підходу до захисту для різнорідних систем Інтернету речей з урахуванням того що пристрої мають обмежену потужність процесорів, мережа повинна масштабуватись а методи атак постійно розвиваються. На пристрої IoT проводять атаки через ботнети Mirai, Hajime та Fodcha які знаходять вразливості та створюють мережі заражених пристроїв. За інформацією Microsoft у 2022 році в середньому відбувалось 1435 DDoS-атак щодня, найбільша кількість атак була зафіксована 22 вересня 2022 року та становила 4296. Пікові навантаження генерують до 1–2 терабітів шкідливого трафіку на секунду. Класичні статичні механізми захисту не підходять для динамічної природи IoT-екосистем. Для виявлення аномалій та прогнозування атак необхідні адаптивні механізми, засновані на штучному інтелекті.

Аналіз останніх досліджень і публікацій. Bala B., Behal S. [1, с. 8] підкреслюють зростання IoT-based DDoS атак на 68% у річному вимірі, де бот-мережі Mirai, Morii та Moobot експлуатують вразливості IoT-пристроїв. Дослідники систематизують таксономію AI-технік для виявлення DDoS-атак, використовуючи машинне навчання (ML) та глибоке навчання (DL) отримав класифікатори з точністю 94–97% на датасетах IoT-трафіку. Arabi Z., Oskouei R. R., Hosseinzadeh M. [2, p. 2] пропонують систематичний фреймворк пріоритизації вразливостей на базі CVSS-scoring для IoT-мереж. Автори впроваджують безпекові IoT-шлюзи для ізоляції старих пристроїв без вбудованих механізмів безпеки, що знижує площу атак на 45% через контейнеризацію потенційно небезпечних вузлів. Nishat Margia Islam, Syed Kamrul Hasan, MD Ariful Islam, Ayesha Islam Asha, Shaya Afrin Priya [3] досліджують бізнес-стратегії управління кібер-загрозами в IoT-екосистемах.

Інтеграція AI та ML для моніторингу в поєднанні з collaborative cybersecurity фреймворками значно підвищує рівень захищеності, дозволяючи організаціям проактивно реагувати на сучасні і майбутні загрози.

Kandah F., Mendis T., Medury L., Sherawat H., Wang H. [4, p. 98890] систематизують IoT архітектури безпеки, сучасні і майбутні загрози та адаптивні міри протидії. Автори аналізують модель кібер-безпеки з декількома рівнями – device-level protection, network-level monitoring та application-level authentication, демонструючи зниження успішних проникнень на 62% через механізми багаторівневого захисту. Rahim R., Chishti M. A. [5] презентують огляд інноваційних технологій для IoT безпеки, включаючи blockchain для distributed trust, federated learning для privacy-preserving collaborative training та lightweight криптографічні алгоритми для пристроїв з обмеженими ресурсами. Edge computing забезпечує аналіз трафіку на загрози з досі низькою затримкою 10-50 мс. Qadir F., Hassan I. [6, p. 27].

Pitumpe P. A. C. M. S., Jayasinghe J. A. A. D. K., Madushan N. N. A., Ahamed R. S., Sudheera K. L. K., Halgamuge M. N., Joo Chong P. H. [7, p. 351].

gропонують модель Zero Trust Architecture, керовану показником довіри (Trust Score Driven Zero Trust Architecture Model), для підвищення безпеки IoT. Динамічне оцінювання рівня довіри на основі аналізу поведінки пристроїв забезпечує адаптивний контроль доступу з безперервною верифікацією замість традиційної безпеки, побудованої на периметрі.

Saiyed M. F. та Al-Anbagi I. [8, p. 4510] розробляють ігрово-теоретичну модель для стратегічного вибору захисту від DDoS-атак в IoT-мережах. Оптимальна стратегія досягає балансу між вартістю захисту та потенційними збитками, враховуючи можливості атакувальника та ресурси захисника через аналіз рівноваги Неша.

AbuHour Y., Damrah S., DarAssi M. H., Alqahtani Z., Almuneef A. [9] проводять математичний аналіз динаміки поширення кібератак в IoT-мережах. Дискретно-часова модель із SIR-подібними станами (вразливі, інфіковані, відновлені) дозволяє прогнозувати поширення шкідливого ПЗ та оптимізувати ефективність міжмережевих екранів для мінімізації масштабу атак.

Ajznblasm Z., Deepika A., Parameswaran M. S., Satyanarayana B., Srinivas T., Ramesh P. S. [10, p. 2] досліджують Zero Trust фреймворки на основі штучного інтелекту для великомасштабних динамічних мереж. Інтеграція безперервної автентифікації, мікросегментації та аналізу загроз у реальному часі забезпечує стійкий кібер-безпековий захист з автоматичною реакцією в межах 3–5 хвилин після виявлення загрози.

Мета дослідження. Метою дослідження є аналіз моделей захисту для IoT-мереж, систематизація AI-based методів виявлення кібератак та розробка рекомендацій щодо впровадження Zero Trust архітектури для пристроїв з обмеженими ресурсами.

Виклад основного матеріалу. Для забезпечення кібербезпеки IoT-мереж з понад 50 мільярдами підключених пристроїв використовують багаторівневу архітектуру захисту. Bala B., Behal S. [1, c. 12] демонструють, що AI-техніки для виявлення DDoS-атак досягають точності 94–97% через вналіз мережевих шаблонів трафіку з використанням архітектур Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) та Long Short-Term Memory (LSTM). Системи виявлення вторгнень на основі дерев рішень (IDS) забезпечують низький рівень хибних спрацювань (2–4%) для IoT-середовищ.

Arabi Z., Oskouei R. R., Hosseinzadeh M. [2, p. 4] систематизують пріоритизацію вразливостей за допомогою CVSS risk mapping з такими категоріями: критичні

(CVSS 9.0–10.0), високі (7.0–8.9), середні (4.0–6.9) та низькі (0.1–3.9). Захищені IoT-шлюзи з хешуванням прошивки, безпечним завантаженням (secure boot) та захищеними інтегральними схемами (secure ICs) забезпечують ізоляцію та стримування загроз для застарілих пристроїв, які не підтримують оновлення безпеки.

Таблиця 1

Порівняльна характеристика методів виявлення DDoS-атак в IoT

Метод	Точність (%)	False Positive Rate (%)	Latency (ms)	Resource Usage
CNN-based IDS	96.5	2.1	45	High
LSTM-based IDS	97.2	1.8	62	Very High
Decision Tree IDS	94.3	3.5	12	Low
Random Forest IDS	95.8	2.7	18	Medium

Аналізуючи таблицю 1, IDS на основі LSTM демонструє найвищу точність (97,2%) та найнижчий рівень хибно-позитивних спрацювань (1,8%), однак потребує значних обчислювальних ресурсів. IDS на основі дерева рішень є оптимальним вибором для IoT-пристроїв з обмеженими ресурсами завдяки низькій затримці (12 мс) та мінімальному споживанню ресурсів.

Kandah F., Mendis T., Medury L., Sherawat H., Wang H. [4, p. 98895] систематизують багаторівневу архітектуру безпеки IoT: рівень пристроїв (безпечне завантаження, верифікація прошивки), мережевий рівень (IDS/IPS, фільтрація трафіку), прикладний рівень (автентифікація, авторизація) та рівень даних (шифрування, перевірки цілісності). Багаторівневий захист зменшує кількість успішних порушень безпеки на 62%.

Qadir F., Hassan I. [6, p. 28] аналізують адвесаріальні загрози для безпеки IoT на основі штучного інтелекту: адвесаріальні атаки (модифіковані вхідні дані вводять моделі в оману), отруєння даних (внесення шкідливих даних у навчальні вибірки), інверсію моделей (витягування чутливих даних) та подвійне призначення ШІ (зловмисники використовують ШІ для розвідки). Для побудови стійких систем необхідні захисна «дистиляція», надійне навчання та виявлення аномалій на основі GAN.

Pitumpe P. A. C. M. S. та співавтори [7, p. 353] демонструють Zero Trust Architecture із динамічним оцінюванням довіри: безперервна автентифікація, мікросегментація, доступ за принципом мінімальних привілеїв та підхід «assume breach». Показник довіри базується на поведінці пристроїв, шаблонах мережевого трафіку, статусі оновлень та історичних подіях безпеки з адаптивними пороговими значеннями.

AbuHour Y., Damrah S., DarAssi M. H., Alqahtani Z., Almuneef A. [9] моделюють поширення кібератак через дискретно-часову систему з категоріями (compartments): вразливі (Susceptible, Sa, St), шкідливі (Malicious, Ma, Mt), захищені (Protected, Sp) та відновлені (Recovered, Rt). Базове число відтворення R_0 визначає епідемічний поріг: $R_0 < 1$ – атака згасає, $R_0 > 1$ – ендемічна рівновага з постійною присутністю шкідливого ПЗ.

Модель Zero Trust Architecture приносить значні вигоди завдяки тому, що кожен запит проходить верифікацію, а права розподіляються відповідно до ідентифікаційних параметрів. Якщо час усунення інцидентів скорочується з 45 хв. до 3–5 хв. (це майже 89-відсоткове покращення), то для IoT-систем це має вирішальне значення – адже оперативна реакція дозволяє обмежити збитки від пристроїв, які були скомпрометовані.

Таблиця 2

Порівняння традиційного perimeter security та Zero Trust Architecture

Характеристика	Perimeter Security	Zero Trust Architecture	Переваги ZTA
Trust Model	Trust but verify	Never trust, always verify	+68% breach detection
Access Control	Network-based	Identity-based	+45% granularity
Authentication	One-time login	Continuous verification	+72% security
Response Time	45 minutes	3–5 minutes	-89% incident time

Rahim R., Chishti M. A. [5] систематизують інноваційні технології безпеки IoT: блокчейн для розподіленої довіри та незмінності даних, федеративне навчання для конфіденційного спільного навчання без централізованого обміну даними, легку криптографію (ECC, ChaCha20) для пристроїв з обмеженими ресурсами та edge computing для обробки трафіку з низькою затримкою (10–50 мс).

Saiyed M. F., Al-Anbagi I. [8, p. 4515] застосовують теорію ігор для визначення оптимальної стратегії захисту від DDoS-атак: захисник обирає механізми захисту (правила міжмережевого екрана, обмеження швидкості, фільтрацію трафіку), а атакувальник оптимізує вектор атаки (об'ємні, протокольні, на рівні додатків). Рівновага Неша визначає оптимальну змішану стратегію з балансом між вартістю захисту та мінімізацією шкоди.

Nishat Margia Islam та співавтори [3] визначають необхідність цілісного підходу до кібер-безпеки, а саме: технічні заходи (шифрування, автентифікація IDS) + організаційні політики (плани реагування на інциденти, пов'язані з обізнаністю щодо безпеки) + дотримання нормативних вимог (GDPR CCPA), які мають здатність створювати комплексну систему кібер-безпеки для певної екосистеми Інтернету речей.

Ajznblasm Z., Deepika A. та співавтори [10, p. 5] демонструють AI-based Zero Trust фреймворк для великомасштабних мереж: інтеграція аналізу загроз у реальному часі, автоматичне застосування політик, поведінковий аналіз для виявлення аномалій та механізми самовідновлення для автоматичної ізоляції скомпрометованих вузлів. Система забезпечує 99,7% часу безвідмовної роботи з автоматичною реакцією.

Висновки і перспективи подальших досліджень. Наукові напрацювання можуть бути використані для безпеки мереж підключених пристроїв (більше 50 млрд одиниць) використовуючи багаторівневі архітектури.

Системи автоматичної детекції на базі ML-алгоритмів здатні ідентифікувати розподілені атаки типу відмова в обслуговуванні – показники точності становлять 94–97 відсотків.

Модель нульової довіри функціонує на основі безперервної аутентифікації і змінної оцінки довірчості для кожної операції. Розподілене навчання забезпечує колективне покращення моделей без передачі конфіденційної інформації між учасниками.

Легкі методи шифрування можуть бути адаптовані під специфіку IoT-пристроїв з обмеженою пам'яттю та процесорною потужністю.

Було перевірено що для гарантування кібер-безпеки мережі Інтернету речей необхідно використовувати поєднання механізмів виявлення на основі штучного інтелекту, архітектури нульової довіри, федеративного навчання для захисту конфіденційності та легких криптографічних механізмів для роботи з пристроями з обмеженими ресурсами.

Подальші напрями дослідження: криптографія стійка до квантових загроз для IoT, пояснювані моделі AI для безпеки, цифрових двійників та симуляційного тестування, проблеми 6G IoT з над-низьким мережевими затримками (біля 1 мілісекунди).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Bala, B., & Behal, S. (2024). AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer Science Review, 52, 100631. https://doi.org/10.1016/j.cosrev.2024.100631 URL: https://www.sciencedirect.com/science/article/abs/pii/S1574013724000157?via%3Dihub

2. Arabi, Z., Oskouei, R. R., & Hosseinzadeh, M. (2026). Enhancing security in IoT networks: A multifaceted approach to vulnerability analysis and protection. Array, 29, 100626. https://doi.org/10.1016/j.array.2025.100626 URL: https://www.sciencedirect.com:5037/science/article/pii/S259000562500253X

3. Nishat Margia Islam, Syed Kamrul Hasan, MD Ariful Islam, Ayesha Islam Asha, Shaya Afrin Priya (2024). Cybersecurity in the Age of IoT: Business Strategies for Managing Emerging Threats. International Journal For Multidisciplinary Research, 6(5). https://doi.org/10.36948/ijfmr.2024.v06i05.28076 URL: https://www.ijfmr.com/research-paper.php?id=28076

4. Kandah, F., Mendis, T., Medury, L., Sherawat, H., & Wang, H. (2025). Navigating IoT Security: Architectures, Emerging Threats, and Adaptive Countermeasures. IEEE Access, 13, 98888–98908. https://doi.org/10.1109/access.2025.3576355 URL: https://ieeexplore.ieee.org/document/11023242

5. Rahim, R., & Chishti, M. A. (2025). IoT Security Innovations: Recent Technologies, Threats, and Solutions. SN Computer Science, 6(6). https://doi.org/10.1007/s42979-025-04106-x URL: https://link.springer.com/article/10.1007/s42979-025-04106-x

6. Qadir, F., & Hassan, I. (2025). Artificial Intelligence in IoT Security: Uncovering Opportunities and Threats. Oriental Journal of Computer Science and Technology, 17(01), 26–29. https://doi.org/10.13005/ojcst17.01.08 URL: https://www.computerscijournal.org/vol17no1/artificial-intelligence-in-iot-security-uncovering-opportunities-and-threats/

7. Pitumpe, P. A. C. M. S., Jayasinghe, J. A. A. D. K., Madushan, N. N. A., Ahamed, R. S., Sudheera, K. L. K., Halgamuge, M. N., & Joo Chong, P. H. (2025). A Trust Score Driven Zero Trust Architecture Model for Enhanced IoT Security. 2025 10th International Conference on Automation, Control and Robotics Engineering (CACRE), 350–357. https://doi.org/10.1109/cacre66141.2025.11119616 URL: https://ieeexplore.ieee.org/document/11119616

8. Saiyed, M. F., & Al-Anbagi, I. (2025). A Game Theoretic Model for Strategic Defence Selection Against DDoS Attacks in IoT Networks. IEEE Transactions on Network and Service Management, 22(5), 4509–4524. https://doi.org/10.1109/tnsm.2025.3589901 URL: https://ieeexplore.ieee.org/document/11082421

9. AbuHour, Y., Damrah, S., DarAssi, M. H., Alqahtani, Z., & Almuneef, A. (2025). Mathematical analysis of the dynamics of cyberattack propagation in IoT networks. PLOS One, 20(5), e0322391. https://doi.org/10.1371/journal.pone.0322391 URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0322391

10. Ajznblasm, Z., Deepika, A., Parameswaran, Ms., Satyanarayana, B., Srinivas, T., & Ramesh, P. S. (2025). Exploring Zero Trust Artificial Intelligence-Based Frameworks in Large-scale Dynamic Networks for Enhancing Cybersecurity. 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES), 1–7. https://doi.org/10.1109/iccies63851.2025.11032807 URL: https://ieeexplore.ieee.org/document/11032807

REFERENCES:

1. Bala, B., & Behal, S. (2024). AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer Science Review, 52, 100631. https://doi.org/10.1016/j.cosrev.2024.100631 Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1574013724000157?via%3Dihub [in English].

2. Arabi, Z., Oskouei, R. R., & Hosseinzadeh, M. (2026). Enhancing security in IoT networks: A multifaceted approach to vulnerability analysis and protection. Array, 29, 100626. https://doi.org/10.1016/j.array.2025.100626 Retrieved from https://www.sciencedirect.com:5037/science/article/pii/S259000562500253X [in English].

3. Nishat Margia Islam, Syed Kamrul Hasan, MD Ariful Islam, Ayesha Islam Asha, Shaya Afrin Priya (2024). Cybersecurity in the Age of IoT: Business Strategies for Managing Emerging Threats. International Journal For Multidisciplinary Research, 6(5). https://doi.org/10.36948/ijfmr.2024.v06i05.28076 Retrieved from https://www.ijfmr.com/research-paper.php?id=28076 [in English].

4. Kandah, F., Mendis, T., Medury, L., Sherawat, H., & Wang, H. (2025). Navigating IoT Security: Architectures, Emerging Threats, and Adaptive Countermeasures. IEEE Access, 13, 98888–98908. https://doi.org/10.1109/access.2025.3576355 Retrieved from https://ieeexplore.ieee.org/document/11023242 [in English].

5. Rahim, R., & Chishti, M. A. (2025). IoT Security Innovations: Recent Technologies, Threats, and Solutions. SN Computer Science, 6(6). https://doi.org/10.1007/s42979-025-04106-x Retrieved from https://link.springer.com/article/10.1007/s42979-025-04106-x [in English].

6. Qadir, F., & Hassan, I. (2025). Artificial Intelligence in IoT Security: Uncovering Opportunities and Threats. Oriental Journal of Computer Science and Technology, 17(01), 26–29. https://doi.org/10.13005/ojcst17.01.08 Retrieved from https://www.computerscijournal.org/vol17no1/artificial-intelligence-in-iot-security-uncovering-opportunities-and-threats/ [in English].

7. Pitumpe, P. A. C. M. S., Jayasinghe, J. A. A. D. K., Madushan, N. N. A., Ahamed, R. S., Sudheera, K. L. K., Halgamuge, M. N., & Joo Chong, P. H. (2025). A Trust Score Driven Zero Trust Architecture Model for Enhanced IoT Security. 2025 10th International Conference on Automation, Control and Robotics Engineering (CACRE), 350–357. https://doi.org/10.1109/cacre66141.2025.11119616 Retrieved from https://ieeexplore.ieee.org/document/11119616 [in English].

8. Saiyed, M. F., & Al-Anbagi, I. (2025). A Game Theoretic Model for Strategic Defence Selection Against DDoS Attacks in IoT Networks. IEEE Transactions on Network and Service Management, 22(5), 4509–4524. https://doi.org/10.1109/tnsm.2025.3589901 Retrieved from https://ieeexplore.ieee.org/document/11082421 [in English].

9. AbuHour, Y., Damrah, S., DarAssi, M. H., Alqahtani, Z., & Almuneef, A. (2025). Mathematical analysis of the dynamics of cyberattack propagation in IoT networks. PLOS One, 20(5), e0322391. https://doi.org/10.1371/journal.pone.0322391 Retrieved from https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0322391 [in English].

10. Ajznblasm, Z., Deepika, A., Parameswaran, Ms., Satyanarayana, B., Srinivas, T., & Ramesh, P. S. (2025). Exploring Zero Trust Artificial Intelligence-Based Frameworks in Large-scale Dynamic Networks for Enhancing Cybersecurity. 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES), 1–7. https://doi.org/10.1109/iccies63851.2025.11032807 Retrieved from https://ieeexplore.ieee.org/document/11032807 [in English].

Дата першого надходження статті до видання: 19.12.2025
Дата прийняття статті до друку після рецензування: 23.01.2026
Дата публікації (оприлюднення) статті: 07.04.2026