УДК 004.056.5:004.738.5

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ДАНИХ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Гребенюк Є. А.
e-mail: yelyzaveta.hrebeniuk@nure.ua
Науковий керівник – д.т.н., доц. Чала О. В.
Харківський національний університет радіоелектроніки, каф. ІСТ
м. Харків, Україна

Cryptographic mechanisms play a crucial role in ensuring the security of Internet of Things (IoT) systems. Due to the rapid growth of connected devices, IoT networks face numerous security challenges such as unauthorized access, data interception, and manipulation of transmitted information. This paper analyzes key cryptographic approaches used to protect IoT environments, including symmetric encryption, asymmetric encryption, and lightweight cryptographic algorithms designed for resource-constrained devices. The advantages and limitations of these mechanisms are discussed, as well as their applicability in real IoT scenarios. The study highlights the importance of selecting efficient cryptographic solutions that balance security, performance, and energy consumption in IoT systems.

Інтернет речей (Internet of Things, IoT) є однією з ключових технологій сучасної цифрової трансформації, що забезпечує взаємодію великої кількості фізичних пристроїв через мережу Інтернет. До IoT-екосистеми входять сенсори, побутові пристрої, медичне обладнання, промислові системи, транспортні засоби та інші об’єкти, здатні збирати, передавати й обробляти дані. Активне впровадження таких технологій у сферах розумних будинків, охорони здоров’я, електронної комерції та промислового виробництва призводить до стрімкого зростання обсягів даних, що циркулюють у мережі [1].

Разом із розширенням IoT-інфраструктури зростає і кількість загроз безпеці. Через обмежені обчислювальні ресурси багатьох пристроїв та їх масове розгортання такі системи часто стають вразливими до різних типів атак. Серед найбільш поширених ризиків можна виділити несанкціонований доступ до пристроїв, перехоплення інформації під час передавання, підміну даних та компрометацію мережевих вузлів. Це створює серйозні виклики для забезпечення конфіденційності, цілісності та достовірності інформації в IoT-мережах.

У зв’язку з цим важливу роль відіграють криптографічні методи захисту, які дозволяють забезпечити безпечну передачу даних, аутентифікацію пристроїв та запобігти несанкціонованому доступу до інформації. Використання сучасних криптографічних алгоритмів та протоколів є одним із

ключових підходів до підвищення рівня безпеки систем Інтернету речей.

Системи Інтернету речей характеризуються високим рівнем взаємозв'язку між пристроями та постійним обміном інформацією. Така особливість створює значну кількість потенційних точок входу для кіберзловмисників. Однією з поширених проблем є перехоплення даних під час передавання мережею. У разі відсутності належного шифрування конфіденційна інформація може бути отримана сторонніми особами.

Ще однією загрозою є атаки типу Man-in-the-Middle, під час яких зловмисник перехоплює комунікацію між двома пристроями та може змінювати передану інформацію. Також можливі атаки, спрямовані на отримання несанкціонованого доступу до IoT-пристроїв, що дозволяє змінювати їхні налаштування або використовувати їх як частину ботнетів.

Додатковою проблемою є обмеженість апаратних ресурсів більшості IoT-пристроїв. Через низьку обчислювальну потужність та обмежене енергоспоживання застосування традиційних криптографічних алгоритмів може бути складним. Саме тому виникає необхідність розробки спеціальних криптографічних рішень, адаптованих до особливостей таких систем [2].

Для забезпечення безпеки IoT-мереж застосовується низка криптографічних підходів, які дозволяють захищати інформацію на різних етапах її обробки та передавання.

Одним із найбільш поширених методів є симетричне шифрування, при якому один і той самий секретний ключ використовується як для шифрування, так і для дешифрування даних. До найвідоміших алгоритмів належить AES (Advanced Encryption Standard), який широко застосовується для захисту інформації в різних інформаційних системах. Перевагою симетричного шифрування є висока швидкість обробки даних, що робить його придатним для використання в IoT-мережах. Однак головна проблема полягає в необхідності безпечної передачі секретного ключа між сторонами, оскільки компрометація ключа ставить під загрозу всю систему.

Асиметричне шифрування ґрунтується на використанні пари взаємопов'язаних ключів – відкритого та закритого. Такий підхід забезпечує більш високий рівень безпеки під час обміну ключами та аутентифікації пристроїв. До найбільш поширених алгоритмів належать RSA та Elliptic Curve Cryptography (ECC). Останній алгоритм особливо ефективний для IoT-систем, оскільки забезпечує високий рівень криптографічного захисту при відносно невеликих розмірах ключів [3].

З огляду на обмежені ресурси IoT-пристроїв важливе значення має так звана легковагова криптографія (lightweight cryptography). Такі алгоритми розробляються спеціально для пристроїв із низькою обчислювальною потужністю та обмеженим енергоспоживанням. Вони забезпечують прийнятний рівень безпеки при мінімальному використанні ресурсів системи.

До прикладів легковагових алгоритмів належать PRESENT, SPECK та

SIMON, які застосовуються у бездротових сенсорних мережах, RFID-системах та інших IoT-середовищах. Основною метою таких алгоритмів є досягнення балансу між рівнем безпеки, продуктивністю та енергоспоживанням [4].

Використання криптографічних механізмів забезпечує низку важливих переваг для IoT-систем. Насамперед це підвищення рівня конфіденційності даних, оскільки шифрування унеможливлює доступ сторонніх осіб до інформації. Крім того, криптографічні методи дозволяють гарантувати цілісність даних та здійснювати автентифікацію пристроїв у мережі.

Разом із тим існують і певні труднощі, пов'язані з використанням криптографії в IoT. До них належать обмежені апаратні ресурси пристроїв, складність управління криптографічними ключами та необхідність забезпечення масштабованості системи при великій кількості підключених пристроїв. Тому важливим напрямом досліджень є розробка нових алгоритмів і протоколів, які поєднують високий рівень безпеки з ефективним використанням ресурсів [3].

Інтернет речей відіграє важливу роль у розвитку сучасних інформаційних технологій, однак широке впровадження IoT-пристроїв супроводжується зростанням ризиків кібербезпеки. Через обмежені ресурси багатьох пристроїв традиційні підходи до захисту інформації не завжди можуть бути ефективно реалізовані.

Криптографічні механізми є одним із основних інструментів забезпечення безпеки в IoT-системах. Використання симетричного та асиметричного шифрування, а також легковагових криптографічних алгоритмів дозволяє захищати інформацію, забезпечувати автентифікацію пристроїв та підтримувати безпечний обмін даними.

Подальші дослідження у цій сфері повинні бути спрямовані на розробку нових криптографічних методів, оптимізованих для IoT-середовища, а також на вдосконалення механізмів управління ключами та інтеграцію криптографії з іншими технологіями інформаційної безпеки.

Список використаних джерел:

1. J. Jusak, S. Kerrison. Integration of IoT and Distributed Ledger Technologies: A Survey, Challenges, and Future Directions, 2026. URL: https://dl.acm.org/doi/10.1145/3789255 (дата звернення: 12.03.2026).

2. H. Damghani, L. Damghani, H. Hosseinian, R. Sharifi. Classification of attacks on IoT, 2019. P. 245-255. URL: https://surl.lu/ggndns (дата звернення: 12.03.2026).

3. Основи криптографічного захисту інформації : електронний навчальний посібник комбінованого (локального та мережного) використання / Яремчук Ю. Є., Салієва О. В., Бондаренко І. О. – Вінниця : ВНТУ, 2024. – 139 с. URL: https://pdf.lib.vntu.edu.ua/books/2024/Yaremchuk_2024_139.pdf (дата звернення: 12.03.2026).

4. M Khan, E Kozyri, H Dagenborg. Systematic Review of Lightweight Cryptographic Algorithms, 2026. 48 p. URL: https://arxiv.org/abs/2602.14731 (дата звернення: 12.03.2026).