УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.06**

А.М. ЄВГЕНЬЄВ, З.М. СИДОРЕНКО, О.В. СЄВЄРІНОВ, канд. техн. наук

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У СИСТЕМАХ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ВИКОРИСТАННЯ ЗАВАДОСТІЙКИХ КОДІВ

Вступ

Промисловий Інтернет речей (Industrial Internet of Things, IIoT) – це сучасна технологія, яка об'єднує інтелектуальні сенсори, пристрої та програмне забезпечення з метою автоматизованого контролю, збору даних і управління виробничими процесами. Попри значні переваги, впровадження IIoT несе ряд серйозних проблем безпеки, які можуть призвести до витоку конфіденційної інформації, фінансових втрат або фізичної шкоди для обладнання та персоналу. Одним із основних викликів, пов'язаних з безпекою IIoT, є забезпечення цілісності інформації, тобто збереження її точності, достовірності та незмінності протягом усього життєвого циклу – від збору до обробки й зберігання [1].

Порушення цілісності даних у IIoT-системах може спричинити збої у функціонуванні обладнання, виробничі інциденти та суттєве зниження рівня довіри до системи. В умовах промислового середовища, де активно застосовуються автоматизовані технології та велика кількість взаємодіючих пристроїв, ця проблема набуває особливої гостроти.

Мета статті – розглянути наявні підходи до забезпечення цілісності даних у IIoT та проаналізувати можливості використання завадостійких кодів, зокрема кодів Гоппи, для підвищення рівня інформаційної безпеки.

Основні проблеми безпеки IIoT

Незважаючи на такі переваги впровадження IIoT, як підвищення ефективності та зниження витрат, впровадження таких систем породжує низку викликів у сфері інформаційної безпеки.

По-перше, це застаріле або вразливе програмне забезпечення пристроїв IIoT. Через тривалий життєвий цикл промислових пристроїв оновлення програмного забезпечення може бути складним або навіть неможливим. У результаті багато елементів IIoT залишаються відкритими до атак через відомі вразливості.

По-друге, це відсутність шифрування або його недостатній рівень. У багатьох випадках дані передаються між пристроями IIoT у відкритому вигляді або з використанням застарілих методів шифрування, що дозволяє зловмисникам проводити атаки "людина посередині", перехоплювати або модифікувати інформацію.

Проблемним питанням є відсутність єдиних стандартів безпеки. Відсутність загальноприйнятих стандартів безпеки для IIoT-пристроїв призводить до хаотичного підходу до їх розробки та інтеграції. Також використання різних виробників створює труднощі у забезпеченні єдиної політики безпеки.

Крім того, багато пристроїв IIoT мають обмежені обчислювальні ресурси, що ускладнює реалізацію на них складних протоколів автентифікації. IIoT-пристрої часто використовують слабкі або стандартні паролі за замовчуванням, не мають механізмів багатофакторної автентифікації. Тому вразливості в автентифікації можуть призвести до того, що зловмисники отримають несанкціонований доступ до даних систем.

Однією з головних проблем IIoT є забезпечення цілісності даних. У промислових середовищах навіть незначне спотворення даних може мати серйозні наслідки: порушення технологічного процесу, аварії обладнання або вихід з ладу систем управління. Дані, що передаються від датчиків або приймаються автоматизованими системами, повинні залишатися незмінними під час передачі і зберігання. Проте через велику кількість вузлів і слабкий

захист деяких пристроїв ця інформація може бути перехоплена, змінена або знищена без виявлення даного факту.

Для забезпечення цілісності даних пропонується застосовувати нові підходи, що поєднують сучасні криптографічні засоби та завадостійке кодування.

Методи забезпечення цілісності даних в системах IIoT

На сьогодні для збереження цілісності в промислових мережах застосовуються такі рішення [1]:

– криптографічні геш-функції на основі алгоритмів SHA-2, SHA-3 для формування контрольної суми (гешу);

– цифрові підписи з використанням алгоритмів RSA, ECDSA, постквантових схем на решітках;

– захищені протоколи передачі даних з шифруванням (TLS, DTLS, MQTT-SN), що реалізують контроль цілісності, наприклад, через HMAC;

– апаратні модулі безпеки (TPM, HSM), які забезпечують автентифікацію пристроїв;

– зберігання інформації з пристроїв IIoT у блокчейні або розподілених реєстрах, де будь-які зміни реєструються.

Проте, попри розвиток цих технологій, вони не завжди ефективно захищають від усіх можливих загроз, зокрема через неможливість виправлення помилок, спричинених перешкодами або збоями. Крім того, більшість традиційних алгоритмів шифрування, як-от AES, RSA або ECC, не гарантують стійкості в умовах постквантового періоду.

Саме тому перспективним напрямом є інтеграція криптографії з методами завадостійкого кодування.

Тривалий час відомі кодові криптосистеми McEliece, Rao-Nam і Niederreiter – це криптографічні системи, що базуються на завданнях теорії завадостійкого кодування, зокрема, на складності декодування випадкового лінійного блочного коду – однієї з фундаментальних задач у теорії завадостійкого кодування. Кодові криптосистеми також демонструють високу продуктивність (швидкість обчислень), перевищуючи традиційні криптографічні системи, як-от RSA чи ECC. Їхня особливість – стійкість до атак квантових комп'ютерів, що робить їх перспективними для постквантової криптографії [5, 6].

Забезпечення цілісності інформації полягає у введенні в інформацію надмірності (автентифікатора), що дозволяє з заданою імовірністю встановлювати дійсність переданого повідомлення. Різниця між кодами автентифікації і завадостійкими кодами полягає в тім, що більшість завадостійких кодів мають одне правило кодування, а коди автентифікації мають багато правил кодування, з яких передавач або приймач може вибирати для використання одне ключове (секретне) правило.

Основою двоключової криптосистеми McEliece та одноключової системи Rao-Nam є коди Гоппи – один із підкласів альтернантних кодів, що мають кращі характеристики серед лінійних блокових кодів. Їх ключова перевага полягає в можливості побудови великої кількості кодів із заданими параметрами. Саме це робить коди Гоппи придатними для криптографічних цілей та відкриває можливості для одночасного досягнення високої завадостійкості та цілісності даних у IIoT, а також дозволяють перетворювати інформацію з високою швидкістю.

Аналіз можливостей кодів Гоппи щодо забезпечення цілісності та завадостійкості даних у системах IIoT

Широко застосовувані для захисту від помилок завадостійкі коди не забезпечують цілісності інформації, оскільки мають одне правило кодування, що відповідає фіксованому коду. Отже, можна припустити, що використання для підвищення достовірності даних завадостійких кодів, що мають досить багато правил кодування, дозволить забезпечити цілісність

інформації, що передається, якщо обране правило кодування тримається в таємниці від зловмисника.

Реалізація цього припущення може бути пов'язана із застосуванням кодів Гоппи, які мають найкращі характеристики класу лінійних блокових кодів. Характерною властивістю кодів Гоппи є той факт, що є велика кількість способів формування коду із заданими параметрами, що потенційно може вирішити задачу не тільки забезпечення високої стійкості до завад, але і цілісності даних в системах IIoT.

Коди Гоппи є підкласом альтернативних кодів, які у свою чергу тісно пов'язані з узагальненими кодами Ріда–Соломона (ОРС) [7 – 9]. Коди Гоппи формують широку категорію кодів, до якої належать БЧХ-коди, коди Срівестави, а також узагальнення Ченя–Чоя. Вони мають доведені характеристики на границі Варшамова–Гілберта, що робить їх ефективними для створення безпечних та надійних систем передачі даних. Крім того, завдяки наявності великої кількості багаточленів $G(x)$, які задають код з параметрами не нижчими від заданих, ці багаточлени можуть виступати в ролі криптографічного ключа.

Крім того, велика кількість багаточленів Гоппи, що визначають код з параметрами не гірше заданих, дозволяє використовувати дані коди для контролю цілісності даних, а можливість визначення всієї множини кодових слів за допомогою одного багаточлена дозволяє останній використовувати як ключ відносно невеликої довжини.

Для визначення q-ичного коду Гоппи [8, 9] довжини n використовуються два об'єкти:

– многочлен Гоппи $G(x)$ ступеня t з коефіцієнтами з поля GF(q^m);

– підмножина $L=\{\alpha_1, \alpha_2, ..., \alpha_n\}$ така, що всі елементи L різні, а α_i належить GF(q^m) і $G(\alpha_i)\neq 0$ для всіх $\alpha_i=L$.

Код Гоппи прийнято позначати Г(L,G)-код.

Коди Гоппи є одним з небагатьох класів лінійних блокових кодів, що мають велику кількість законів формування при фіксованих параметрах коду, що явно спричинило створення на їх основі систем криптозахисту. Така система вперше була запропонована Мак-Елісом як система з відкритим ключем [10]. У системі Мак-Еліса секретний ключ складається з матриці, що породжує, двійкового коду Гоппи G, невиродженої матриці S і матриці перестановок P, які її маскують. Відкритим ключем є матриця кодування $G'=S\cdot G\cdot P$ звичайного лінійного коду. При шифруванні повідомлення x множиться на відкриту матрицю кодування G' і до результату додається локально згенерований шумовий блок z. Щоб розшифрувати отриманий шифртекст v необхідно помножити його на P^{-1}, декодувати $v\cdot P^{-1}$, отримавши в результаті слово в коді Гоппи, а потім помножити це слово на S^{-1}, відновивши тим самим вихідне повідомлення x.

Іншим варіантом використання кодів Гоппи є модифікована система Рао–Нама [10], в якій матриця коду Гоппи G, що породжує, є секретним ключем. При зашифруванні повідомлення x випадково вибирається вектор помилок z і обчислюється шифртекст $v = x\cdot G + z$. Якінебудь способи розкриття такої криптосистеми поки що не відомі. Ця система не використовувалася раніше, як і система Макеліса, через велику довжину ключа, що дорівнює $k\cdot n$ символів матриці коду, що породжує, в двійковому випадку.

Пропонується для забезпечення цілісності та завадостійкості даних в якості ключа замість матриці, що породжує, вибирати примітивний багаточлен Гоппи $G(x)$ і перетворення виконувати в частотній області. В цьому випадку загальна кількість ключів системи визначається кількістю багаточленів примітивної довжини, що не приводяться, $N_q(t)$ (рис. 1).

Аналіз отриманих результатів показує, що зі збільшенням довжини n коду Гоппи при фіксованій мінімальній відстані $d=2t+1$ кількість багаточленів ступеня t, що не приводяться, росте набагато швидше, ніж при збільшенні ступеня багаточлена при фіксованій довжині коду n (чи відповідно фіксованого розміру поля q). Це означає, що довгі коди є кращими з погляду працевтрат на розкриття їхнього закону формування.

Оцінка можливості кодів Гоппи щодо забезпечення цілісності

Оцінимо можливості скорочених кодів Гоппи щодо забезпечення цілісності у випадку вибору зловмисником стратегії нав'язування помилкових даних. При випадковому виборі зловмисником *n*-послідовностей імовірність нав'язування буде розраховуватися згідно з виразом

(1)

де n – довжина коду Гоппи; k – кількість інформаційних символів коду Гоппи; t – кількість помилок, що виправляються кодом.

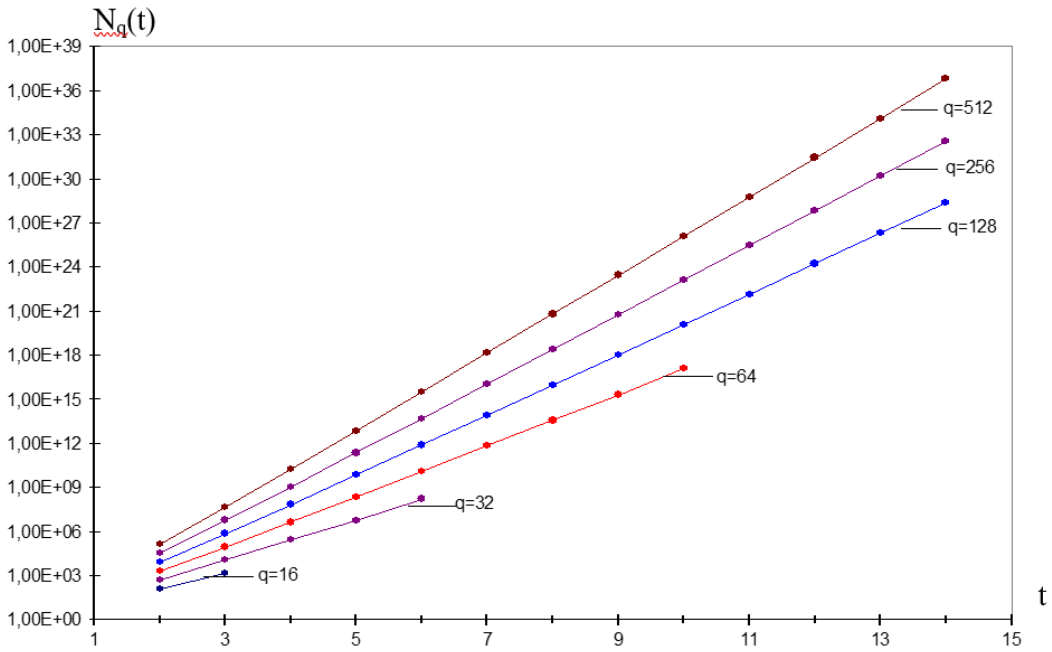

Рис. 1. Залежність кількості багаточленів Гоппи, що не приводяться, $N_q(t)$ від їх ступеня t для різних полів Галуа GF(q)

На рис. 2 представлено залежності імовірності нав'язування $P_{нав.}$ від довжини двійкових кодів Гоппи при швидкості коду R = 1/3, 1/2, 2/3.

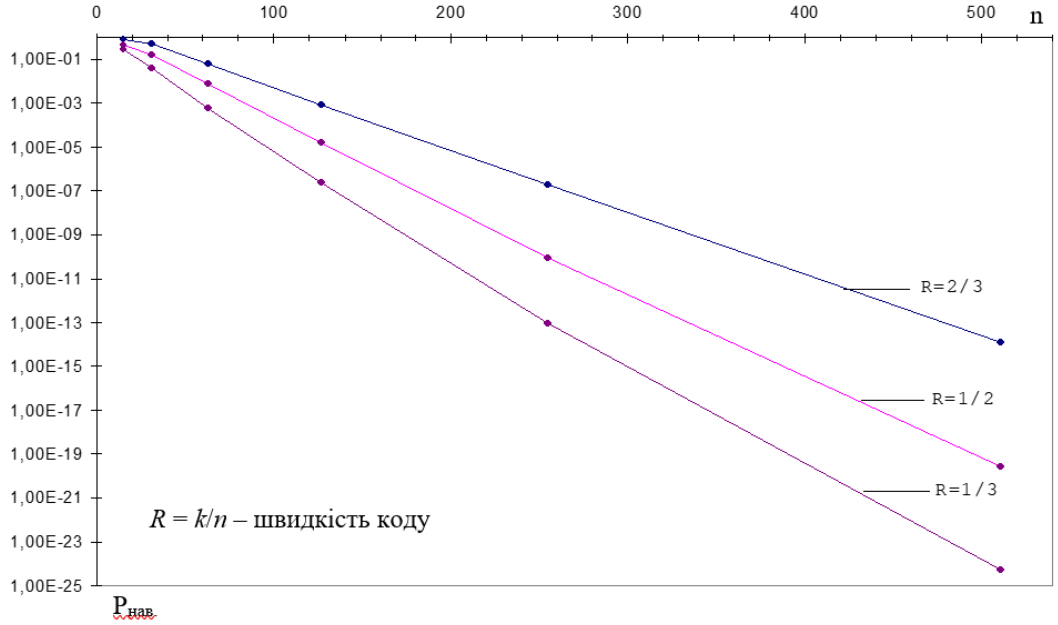

Рис. 2. Залежність імовірності нав'язування $P_{нав.}$ від довжини двійкових кодів Гоппи

Аналіз даних залежностей показує, що зменшення швидкості і збільшення довжини коду приводить до зниження імовірності нав'язування. Це пояснюється зменшенням відношення кількості кодових слів до кількості всіляких n-послідовностей з ростом довжини коду.

Отже, при використанні в системі IIoT кодів Гоппи вираз (1) дає верхню границю імовірності нав'язування.

Висновки

Аналіз класу лінійних блокових кодів – кодів Гоппи показав, що останні володіють високими потенційними можливостями для забезпечення цілісності і завадостійкості каналів передачі даних. Для даних кодів довжини порядку 256 символів загальне число правил кодування є порівнянним із загальним числом ключів існуючих криптосистем, а для кодів більшої довжини значно перевершує, що робить їх перспективними для застосування у постквантову епоху. Аналіз криптостійкості за умови, що зловмиснику невідомий закон формування коду, дозволяє зробити висновок про можливість суттєвого зниження імовірності нав'язування помилкових повідомлень на основі використання таких кодів при збереженні заданих вимог по завадостійкості. Для кодів з фіксованою швидкістю R імовірність нав'язування суттєво знижується зі збільшенням довжини коду n.

Таким чином, застосування кодів Гоппи в системах IIoT може забезпечити не лише завадостійке кодування, а й захист цілісності даних. Це робить їх перспективним рішенням у сфері побудови надійних, захищених і стійких до майбутніх викликів інформаційних систем у промисловості.

Список літератури:

1. Сирадоєв А.О., Можаєв О.О. (2024). Дослідження споживчого і промислового Інтернету речей.

2. Melenti Y. et al. Development of post-quantum cryptosystems based on the Rao-Nam scheme // Eastern-European Journal of Enterprise Technologies. 2025. 1 (9(133)). P. 35–48.

3. Керничний В., Сєвєрінов О.В. Аналіз стійкості криптосистеми McEliece // Global Cyber Security Forum: матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листоп. 2019 р. Харків : ХНУРЕ, 2019. С. 55–56.

4. Шипілов Д.В., Халімов Г.З. Аналіз постквантової криптосистеми McEliece // Комп'ютерні та інформаційні системи і технології. ХНУРЕ, 2019. С. 83–84.

5. Dam D. T., Tran T. H., Hoang V. P., Pham C. K., & Hoang T. T. A survey of post-quantum cryptography: Start of a new race // Cryptography. 2023. 7(3). P 40.

6. Melenti Y., Korol O., Shulha V., Milevskyi S., Sievierinov O., Voitko O., ... & Pashayeva S. DEVELOPMENT OF POST-QUANTUM CRYPTOSYSTEMS BASED ON THE RAO-NAM SCHEME // Eastern-European Journal of Enterprise Technologies. 2025. 133(9).

7. Blahut R. E. (1983). Theory and practice of error control codes. (No Title).

8. Goppa V. D. A new class of linear error-correcting codes // Probl. Inf. Transm. 1970. № 6. P. 300–304.

9. Tsfasman M.A., Vladut S.G., Zink Th. Modular Gurves, Shimura Gurves and Goppa Codes, Bitter than Varshamov-Gilbert Bound // Math. Nachrichten. 1982. Vol. 109. P. 21–28.

10. Diffie W. (1988). The first ten years of public-key cryptography // Proceedings of the IEEE. 1988. № 76(5). P.560–577.

Надійшла до редколегії 14.03.2025

Відомості про авторів:

Євгеньєв Андрій Михайлович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: andrii.yevheniev@nure.ua; ORCID: https://orcid.org/0000-0003-4365-5675

Сидоренко Зоя Михайлівна – Харківський національний університет радіоелектроніки, аспірантка кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: zoia.sydorenko@nure.ua; ORCID: https://orcid.org/0000-0002-0104-6807

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.sievierinov@nure.ua; ORCID: https://orcid.org/0000-0002-6327-6405