Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 2 (189) *ISSN 3083-7650 (0135-1710) (print)*

УДК 004.056: 621.391.15 DOI: https://doi.org/10.30837/0135-1710.2026.189.235

Сидоренко З. М., Сєвєрінов О. В.

МЕТОД ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ ІЗ ВИКОРИСТАННЯМ МОДИФІКОВАНОГО ЗАВАДОСТІЙКОГО КОДУ В СИСТЕМАХ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

Предметом вивчення є методи модифікації завадостійких кодів для забезпечення цілісності даних у системах промислового Інтернету речей. **Мета дослідження** – розробити метод забезпечення цілісності даних у системах промислового Інтернету речей за допомогою застосування модифікованих завадостійких кодів, а саме скорочених кодів Гоппи для виявлення та виправлення помилок, що виникають під час передавання й оброблення інформації. **Завдання:** аналіз методів модифікації завадостійких кодів, а саме кодів Гоппи, з метою зашумлення повідомлення для забезпечення цілісності даних у системах промислового Інтернету речей; дослідження методів скорочення кодів Гоппи та визначення найбільш доцільних конструкцій для забезпечення завадостійкості та цілісності даних; розроблення методу забезпечення цілісності даних із використанням скороченого завадостійкого коду в системах промислового Інтернету речей. Для виконання окреслених завдань застосовано **методи:** теоретичні методи аналізу й математичного моделювання, емпіричні методи порівняльного аналізу характеристик кодів, а також елементи комп'ютерного експерименту для розрахунку й оцінювання параметрів скорочених кодів Гоппи. **Досягнуті результати.** Проаналізовано методи модифікації кодів Гоппи, для побудови системи забезпечення цілісності даних в IIoT запропоновано метод скорочення кодів, що дає змогу зберігати мінімальну кодову відстань і формувати коди із заданими параметрами. Досліджено конструкції скорочення кодів Гоппи, обґрунтовано доцільність використання скорочених кодів Гоппи на основі багаточленів, що не приводяться. Запропоновано метод забезпечення цілісності даних із застосуванням скорочених кодів Гоппи. **Висновки.** Упровадження процедур скорочення кодів Гоппи, побудованих на основі багаточленів, що не приводяться, дає змогу формувати кодові конструкції для забезпечення цілісності даних у системах промислового Інтернету речей, які одночасно мають високі властивості завадостійкості. Запропоновано метод забезпечення цілісності даних з використанням скорочених кодів Гоппи, що забезпечує гнучке налаштування параметрів коду й має перспективи гарантувати інформаційну скритність повідомлень.

Ключові слова: промисловий Інтернет речей; завадостійкість; цілісність; завадостійкий код; код Гоппи; модифікація коду; скорочений код.

Вступ

Нині впровадження промислового Інтернету речей (IIoT) супроводжується значними перешкодами. Вони пов'язані з тим, що в процесі створення цих систем промислові активи об'єднують в одну систему, під'єднану до мережі Інтернет, тобто вони стають вразливими до кібератак. Тому проблеми безпеки під час впровадження промислового Інтернету речей є основним пріоритетом у сучасних умовах. Крім того, успішна стратегія IIoT вимагає єдиної архітектури даних, яка може обробляти величезні обсяги інформації. У таких умовах основна увага має бути зосереджена на створенні безпечного й безперебійного потоку даних.

Промисловий Інтернет речей – це система об'єднаних комп'ютерних мереж і під'єднаних до них промислових (виробничих) об'єктів із вбудованими датчиками й програмним забезпеченням для збору інформації та її обміну з можливістю віддаленого контролю й управління в автоматизованому режимі [1, 2]. Системи промислового IIoT визначаються значною кількістю сенсорів, контролерів і виконавчих пристроїв, що обмінюються даними через бездротові або промислові мережі. Такі канали зв'язку часто піддаються впливу електромагнітних завад, втрат пакетів, затримок або навіть цілеспрямованих атак [1, 2].

У цих умовах постає подвійне завдання – захист від спотворення інформації через ненавмисні технічні помилки й контроль цілісності даних проти зловмисних змін. Це також визначається вимогами низки стандартів для систем IIoT, а саме IEC 61000, серії IEC 62443 та ISO/IEC 27001. У цьому разі основна увага зосереджується на необхідності забезпечення цілісності даних у системах IIoT. Так, відповідно до стандарту IEC 62443-3-3, забезпечення цілісності даних є обов'язковим складником безпеки промислового Інтернету речей, що реалізується через вимоги до цілісності системи (System Integrity) й механізми виявлення несанкційних змін інформації та запобігання їм [3].

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189)
ISSN 3083-7650 (0135-1710) (print) Management Information System and Devices. 2026. No. 2 (189)

Одним із підходів до розв'язання завдання захисту від спотворення інформації та забезпечення цілісності даних є застосування в системах промислового IIoT завадостійких (коригувальних) кодів, а саме кодів Гоппи [4]. Коди Гоппи – один із підкласів альтернантних кодів, які мають кращі характеристики серед лінійних блокових кодів і доведені властивості на межі Варшамова – Гілберта. Їх основна перевага перед іншими завадостійкими кодами полягає в можливості побудови значної кількості кодових слів із заданими параметрами. Це робить їх придатними для криптографічних цілей, а саме забезпечення цілісності даних у системах промислового Інтернету речей.

Перша криптографічна система на основі кодів Гоппи була запропонована Макелісом як система з відкритим ключем [5]. У цій системі секретний ключ містить породжувальну матрицю, двійковий код Гоппи G, невироджену матрицю S і матрицю перестановок P, які її маскують. Відкритим ключем є матриця кодування $G' = S \times G \times P$ звичайного лінійного коду. Іншим варіантом використання кодів Гоппи є модифікована система Рао – Нама, в якій породжувальна матриця коду Гоппи G є секретним ключем. Системи Макеліса й Рао – Нама практично не використовувалися через велику на той час довжину ключа, що дорівнює $k \times n$ символів породжувальної матриці коду.

Стійкість даних криптографічних систем базується на складності декодування випадкового лінійного блочного коду – однієї з фундаментальних задач у теорії завадостійкого кодування, а також відновлення структури коду. Для маскування структури коду під випадковий код використовуються різні методи: долучення матриці перестановок, які її маскують, породжувальна матриця, додавання до кодового слова випадкового вектора помилок, а також процедури модифікації коду.

У роботі [4] для забезпечення цілісності та завадостійкості даних запропоновано використовувати коди Гоппи, а ключем замість породжувальної матриці обирати примітивний багаточлен Гоппи $G(x)$. У цьому разі загальна кількість ключів системи визначається кількістю багаточленів примітивної довжини, що не приводяться.

Крім того, в системах захисту даних у IIoT запропоновано застосовувати модифіковані коди Гоппи, що дасть змогу не тільки одночасно досягти високих властивостей цілісності та завадостійкості даних, а також забезпечить конфіденційність інформації.

Аналіз літературних джерел і визначення проблеми

Упродовж 2016–2017 років Національний інститут стандартів і технологій США (NIST) почав проєкт з відбору найкращих постквантових алгоритмів для стандартизації та заміни класичних криптографічних алгоритмів. Класична схема Макеліса [5] залишилася одним із найсильніших кандидатів і ввійшла до фіналістів NIST [6]. У зв'язку з цим з'явилась низка досліджень із застосування завадостійких кодів у криптографічних алгоритмах. Відомі кодові криптосистеми розвивали Макеліс, Рао – Нам і Нідеррайтер [7]. Здебільшого вони спрямовані на розроблення симетричних і асиметричних криптосистем на основі модифікованих схем Макеліса, Рао – Нама й Нідеррайтера.

Так, у праці [8] запропоновано механізми безпеки в гібридно-криптокодових системах, основаних на модифікованих асиметричних системах Нідеррайтера й Макеліса, для використання в методах двофакторної автентифікації на одноразових паролях. Ці модифіковані системи запропоновано будувати на еліптичних кодах замість класичних кодів Гоппи.

У роботі [9] розглянуто класичні системи на основі коду Гоппи й оцінено їх безпеку з огляду на квантові прискорення найефективніших атак, а також запропоновано схеми, основані на кодах QC-LDPC, QC-MDPC і мономіальних кодах.

Автори досліджень [10, 11] розглядають криптосистеми з відкритим ключем на основі кодових схем Макеліса й Нідеррайтера. З огляду на криптосистеми Макеліса запропоновано нову схему цифрового підпису.

У роботі [12] проаналізовано використання симетричної криптокодової конструкції на основі системи Рао – Нама на алгебро-геометричних і дефектних кодах, що забезпечує можливість суттєвого зменшення обсягу ключових даних в інфраструктурі на базі мобільних і смарт-технологій.

Однак у розглянутих та інших подібних дослідженнях висвітлено питання розвитку класичних схем Макеліса, Рао – Нама й Нідеррайтера й побудови на їх основі класичних криптографічних симетричних або асиметричних схем шифрування, схем цифрового підпису та генерації ключів.

Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 2 (189) *ISSN 3083-7650 (0135-1710) (print)*

Ці системи побудовані на використанні різних завадостійких кодів, але не розглядаються для комбінованого застосування з метою захисту від спотворення інформації через ненавмисні технічні помилки й контролю цілісності даних.

Автори праці [13] проаналізували постквантові алгоритми, подані в проєкті NIST. Підтверджено, що більшість алгоритмів, побудованих на кодах, окрім класичної схеми Макеліса з кодами Гоппи, були зламані або суттєво ослаблені. Автори запропонували статичний завадостійкий код не використовувати, а здійснювати його динамічне перетворення за допомогою процедур модифікації (скорочення, додавання) коду.

Мета й завдання дослідження

Використання модифікованих кодів Гоппи в каналах передачі даних системи промислового Інтернету речей для захисту від помилок може забезпечити високі характеристики щодо завадостійкості та цілісності інформації, яка передається.

Аналіз літератури [14–16] дає змогу виокремити шість основних методів модифікації коду: збільшення довжини коду способом додавання інформаційних або перевірчих символів, зменшення довжини кодового блоку внаслідок викидання (вилучення) інформаційних або перевірчих символів, а також збільшення (додавання) чи зменшення (вилучення) кодових слів за незмінної довжини блоку.

Отже, постає завдання – проаналізувати методи модифікації завадостійких кодів, а саме кодів Гоппи, з метою зашумлення повідомлення для забезпечення цілісності даних у системах промислового IIoT.

Мета роботи – підвищити ефективність забезпечення цілісності даних у системах промислового Інтернету речей за допомогою застосування модифікованих завадостійких кодів, а саме скорочених кодів Гоппи.

Крім того, необхідно розглянути особливості використання кодів Гоппи для забезпечення цілісності даних, проаналізувати методи скорочення цих кодів і визначити найбільш доцільні методи для впровадження в системах промислового IIoT з метою забезпечення завадостійкості та цілісності даних.

Методи дослідження

Для аналізу методів модифікації завадостійких кодів Гоппи з метою сприяння цілісності даних у системах промислового Інтернету речей, дослідження особливостей їх застосування, аналізу методів скорочення кодів Гоппи та визначення найбільш доцільних методів для використання в системах промислового IIoT для забезпечення завадостійкості та цілісності даних було впроваджено теоретичні методи аналізу й математичного моделювання, емпіричні методи порівняльного аналізу характеристик кодів, а також елементи комп'ютерного експерименту для розрахунку й оцінювання параметрів скорочених кодів Гоппи.

Аналіз методів модифікації завадостійкого коду

Розглянемо основні методи модифікації коду щодо кодів Гоппи з метою визначення доцільності їх використання для зашумлення повідомлень у системах забезпечення цілісності.

Код Гоппи може бути подовжений (Lengthening) способом долучення додаткових символів. Звичайний спосіб подовження коду полягає в послідовному виконанні двох операцій: поповнення коду внаслідок додавання вектора $(1\,1\,...\,1)$ (якщо він не належить коду) й розширення його за допомогою загальної перевірки на парність. Внаслідок цих операцій кількість інформаційних символів збільшиться на одиницю.

Код Гоппи може бути розширений (Extending) способом долучення додаткових перевірчих символів. Зазвичай такою модифікацією є впровадження однієї загальної перевірки на парність. Значення відповідного перевірчого символу $a(\infty)$ дорівнює

$$a(\infty) = -\sum_{i=0}^{n} a(\alpha),$$

де $\alpha \in GF(q^m)$; $GF(q^m)$ – Galois Field, скінченне поле Галуа; q – основа поля; m – степінь розширення поля; $a(\alpha)$ – символи кодового слова; n – довжина коду.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189)
ISSN 3083-7650 (0135-1710) (print) Management Information System and Devices. 2026. No. 2 (189)

Тоді вектор $a' = \left(a(0), a(1), \ldots, a\left(\alpha^{n-1}\right), a(\infty)\right)$ належить розширеному коду Гоппи тоді й тільки тоді, коли [14–16]

$$\sum_{i=0}^{n} \frac{\alpha^i a(\alpha)}{G(\alpha)} = 0, \quad i = 0,1,\ldots,n,$$

де $\alpha \in GF\left(q^m\right) \cap \{\infty\}$.

Унаслідок додавання загальної перевірки на парність вага кожного кодового слова стає парною, а кодова відстань збільшується на одиницю. Так, вихідний код Гоппи $Y(n,k,d)$ (n – довжина кодового слова, k – кількість інформаційних символів у кодовому слові, d – мінімальна відстань коду) буде модифіковано в код $Y'(n+1,k,d+1)$. Якщо Y має перевірчу матрицю H, тоді Y' матиме перевірчу матрицю

$$H' = \begin{pmatrix} 111\ldots1 \\ 0 \\ \vdots \quad H \\ 0 \end{pmatrix}.$$

Код Гоппи може бути поповнений за допомогою додавання нових слів (Augmenting). Найпростіший спосіб поповнення коду полягає в додаванні до нього вектора $(1\,1\,\ldots\,1)$ (якщо він не належить коду). Це еквівалентно додаванню вектора $(1\,1\,\ldots\,1)$ до породжувальної матриці. Якщо Y – двійковий (n,k,d)-код Гоппи, який містить вектор $(1\,1\,\ldots\,1)$, то поповнений код дорівнює $Y' = Y \cap \{1+Y\}$, тобто Y містить кодові слова Y та їх доповнення і є $(n,k+1,d')$-кодом. Мінімальна відстань поповненого коду $d' = \min\{d, n-d_a\}$, де d_a – найбільша вага кодових слів коду Y. Іноді код Гоппи з багаточленом Гоппи $G(x)$ може бути поповнений до коду тієї самої довжини, багаточлен Гоппи якого є множником $G(x)$.

Код Гоппи з викиданням (Expurgating) утворюється способом вилучення деяких кодових слів. Так, якщо двійковий (n,k,d)-код Y містить кодові слова парної та непарної ваги, то отримаємо код із викиданням $Y'(n,k-1,d')$, якщо брати кодові слова тільки парної або непарної ваги. Якщо d непарне й викидаються всі слова непарної ваги, тоді $d' > d$. У частотній області ця процедура проводиться способом додаткових обмежень у систему рівнянь, що визначають код Гоппи.

Код Гоппи може бути виколотий (Puncturing) унаслідок вилучення деяких перевірчих символів. Ця процедура обернена до процедури розширення коду. Загалом у процесі виколювання однієї кодової координати довжина коду зменшується на одиницю і, якщо не подбати про вибір символу, що кодується, відстань коду зменшиться на одиницю.

Розглянемо процедуру скорочення коду (Shortening). Нехай лінійний (n,k)-код має породжувальну матрицю, i стовпців якої є лінійно незалежними $(i < k)$. Безліч векторів довжини $n-i$, отриманих вилученням i компонент кодових векторів, утворюють лінійний $(n-i,k-i)$-код. Ця процедура називається скороченням, а код – скороченим кодом [14–16]. Породжувальна матриця скороченого коду виходить з породжувальної матриці початкового коду вилученням i рядків та i стовпців. Перевірча матриця виходить вилученням i стовпців із перевірчої матриці початкового коду. У разі скорочення коду символи, що викидаються, покладаються рівними нулю й тому не передаються, але на приймальній стороні декодер їх відновлює, так що декодування здійснюється на повній довжині коду. Якщо мінімальна відстань початкового коду дорівнює d, мінімальна відстань скороченого коду не менша ніж d.

З розглянутих методів модифікації найбільш прийнятним для побудови системи забезпечення завадостійкості та цілісності інформації, що передається, для промислового Інтернету речей є скорочення кодів. Методи скорочення не змінюють мінімальну відстань d початкового коду. Крім того, методи скорочення дають змогу будувати сімейства кодів із заданими параметрами: довжиною кодового блоку n і кількістю інформаційних символів k.

Оскільки модифікацію коду пропонується використовувати для зашумлення повідомлення, то символи скорочення можна застосовувати як секретний ключ, тому що вони не передаються, а відновлюються на приймальній стороні, і декодування здійснюється на повній довжині початкового коду. Тому вірогідно зловмисник не може однозначно відновити скорочене кодове слово до повної довжини й визначити ключовий багаточлен Гоппи $G(x)$.

Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 2 (189) *ISSN 3083-7650 (0135-1710) (print)*

Також скорочення кодів часто приводить до кодів із найкращими параметрами. Це видно з таблиці кращих кодів [17]. У [17] доведено, що за великих n скорочені коди досягають нижньої межі Варшамова – Гілберта. Наприклад, скорочений $(55,16,19)$-код Гоппи, що задається багаточленом $G(x)$ ступеня 9, є найкращим серед відповідних кодів таблиць [17]. Скорочений $(239,123,35)$-код Гоппи, що задається багаточленом $G(x)$ ступеня 17, цікавий тим, що автори [18] отримують з нього цілу низку кодів довжини 227 і мінімальною відстанню 29, які також є кращими серед відповідних відомих кодів. Отже, застосовуючи процедуру скорочення до кодів Гоппи можна будувати на їх основі кодові конструкції, які мають не тільки високі характеристики завадостійкості, але й значну кількість способів формування коду, що дає змогу будувати на їх основі системи забезпечення цілісності інформації. Постає завдання – проаналізувати методи формування скорочених кодів Гоппи.

Дослідження методів скорочення кодів Гоппи

Скорочені коди Гоппи будуються на елементах поля L, визначеного на $GF(q^m)-\{\alpha_1,\alpha_2,\ldots,\alpha_p,\}$, де $\alpha_1 \in GF(q^m), i=\overline{1,p}.$

Є два варіанти побудови скороченого коду. У першому варіанті багаточленом коду Гоппи $G(x)$ обирається багаточлен, що має некратні корені в полі $GF(q^m)$ і за умови скорочення викидаються нульові частоти на позиціях коренів багаточлена $G(x)$. Довжина скороченого коду в цьому разі дорівнюватиме $(n-p)$, де p – кількість коренів багаточлена коду Гоппи.

У другому варіанті як $G(x)$ обирається багаточлен, що не приводиться, а з поля $GF(q^m)$ викидаються деякі символи (частоти). Тоді довжина коду зменшиться на кількість символів (частот), що викидаються.

У побудові скороченого коду Гоппи на основі багаточлена $G(x)$, що має некратні корені, кількість коренів p, а отже, і символів скорочення визначатиме ступінь багаточлена Гоппи t і, відповідно, кодову відстань d. Тому в цьому разі кількість інформаційних символів дорівнюватиме

$$k' = k - p \geq n - mt - p = n - m(2p+1) - p.$$

Нехай маємо багаточлени коду Гоппи, що містять p_1 і $p_2 = p_1 + 1$ коренів, тоді:

$$k_1' = n - m(2p_1+1) - p_1;$$

$$k_2' = n - m(2p_2+1) - p_2 = n - m(2p_1+3) - p_1 - 1;$$

$$k_1' - k_2' = n - m(2p_1+1) - p_1 - n + m(2p_1+3) + p_1 + 1 = 2m+1.$$

Отже, внаслідок зміни кількості символів скорочення (коренів багаточлена Гоппи) на одиницю кількість інформаційних символів змінюватиметься на $2m+1$ біт, а також значно змінюватиметься швидкість коду $V = k'/n'$.

У табл. 1 подано параметри скорочених кодів Гоппи, отримані за допомогою комп'ютерного моделювання для багаточленів кодів Гоппи $G(x)$ з різною кількістю коренів.

Таблиця 1. *Параметри кодів Гоппи для багаточленів із коренями*

Кількість коренів	Розмірність поля			
	GF(32)	GF(64)	GF(128)	GF(256)
2	30, 25, 5	62, 50, 5	126, 112, 5	254, 238, 5
3	29, 14, 7	61, 43, 7	125, 104, 7	253, 229, 7
4	28, 8, 9	60, 36, 9	124, 96, 9	252, 220, 9
5	27, 4, 11	59, 29, 11	123, 88, 11	251, 211, 11
6	26, 2, 13	58, 22, 13 58, 23, 13	122, 80, 13	250, 202, 13
7	–	57, 15, 15 57, 16, 15 57, 17, 15	121, 72, 15	249, 193, 15
8	–	56, 8, 17 56, 9, 17 56, 10, 17 56, 16, 17	120, 64, 17	248, 184, 17

Аналіз наведених параметрів демонструє, що значна зміна інформаційної довжини коду й кодової відстані за умови скорочення на один символ не дає змогу гнучко змінювати параметри коду Гоппи.

Кількість багаточленів, обумовлених своїми коренями, дорівнює кількості комбінацій усіх неповторюваних елементів поля $GF(q^m)$

$$N_k = C_{q^m}^{p},$$

де p – кількість коренів багаточлена Гоппи $G(x)$.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189)
ISSN 3083-7650 (0135-1710) (print) Management Information System and Devices. 2026. No. 2 (189)

Кількість $N_q(t)$ багаточленів, що не приводяться, ступеня t визначається виразом

$$N_q(t)=\frac{1}{t}\sum_{r|t}\mu(t/r)q^r,$$

де $r|t$ означає, що сума береться за всіма позитивними дільниками r числа t; $\mu(t/r)$ – функція Мебіуса.

На рис. 1 подано графіки залежності кількості багаточленів $G(x)$, що не приводяться, $N_q(t)$, і багаточленів з коренями $N_k(t)$ від їх степеня для кодів над різними полями.

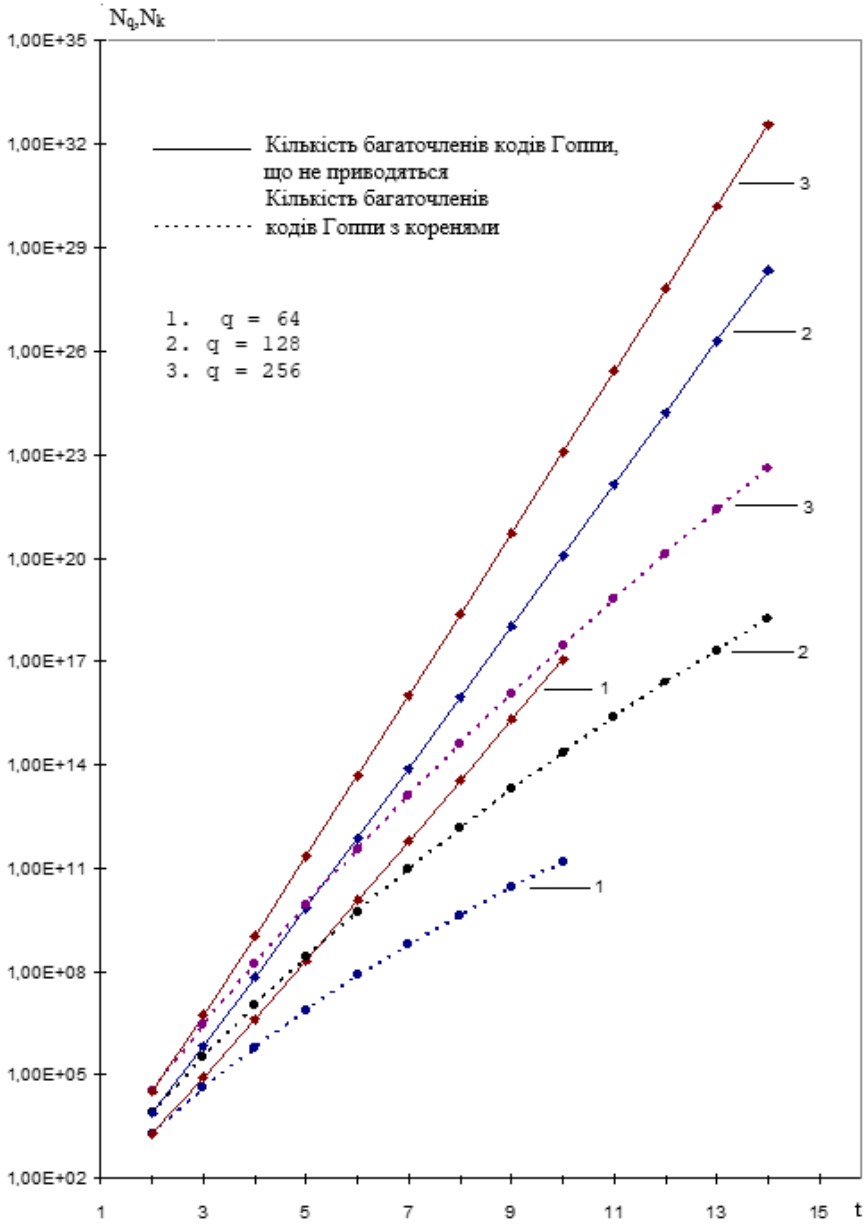

Рис. 1. Залежність кількості багаточленів кодів Гоппи від степеня багаточлена t

Аналіз наведених залежностей демонструє, що за однакових ступенів кількість багаточленів, що не приводяться, $N_q(t)$ перевершує кількість багаточленів з коренями $N_k(t)$. Крім того, зі збільшенням кількості символів скорочення ця перевага зростає. Ще одним недоліком кодів Гоппи, побудованих на основі багаточленів із коренями, є те, що зловмисник під час криптоаналізу, вгадуючи символи скорочення, одночасно визначає і багаточлен Гоппи $G(x)$.

Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 2 (189) *ISSN 3083-7650 (0135-1710) (print)*

Отже, для побудови системи забезпечення цілісності даних у системах промислового Інтернету речей доцільно обирати скорочені коди Гоппи на основі багаточленів, що не приводяться.

Далі розглянемо методи скорочення кодів Гоппи, сформованих на основі багаточленів, що не приводяться. Для цього варіанта відомо три методи скорочення.

Конструкція скорочення № 1

Нехай код Гоппи $Y(n,k,d)$, $N=2^k$ має перевірчу матрицю H. Тоді матриця H з викресленими p стовпцями є перевірчою матрицею коду $Y'(n',k',d)$ з параметрами: $n'=n-p$, $k'=k-p$.

Якщо викреслюються p стовпців у перевірчій матриці H, що відповідають перевірчим елементам коду, то способом додаткових лінійних перетворень перевірча матриця приводиться до канонічного східчастого вигляду. Лінійні перетворення над рядками перевірчої матриці не змінюють параметрів коду й викреслення p перевірчих стовпців буде еквівалентно завданню p нулів інформаційним елементам. Такі символи не передаються. Отже, інформаційна й загальна довжини коду в цьому разі також зменшаться на p символів.

Конструкція скорочення № 2

Нехай код Гоппи $Y(n,k,d)$, $N=2^k$ має перевірчу матрицю H і деяку множину P із p позицій, яка покриває цілком h векторів із матриці H (тобто всі ненульові позиції цих h векторів належать множині P). Тоді множина слів із викресленими p позиціями множини P утворять код $Y'(n',k',d)$ з параметрами [17, 19]:

$$n'=n-p,\quad k'=k-p+h.$$

Конструкція скорочення Хелгерта і Стінаффа

Нехай код Гоппи $Y(n,k,d)$ має породжувальну матрицю $G(k\times n)$ такого вигляду:

$$G=\left(\begin{array}{c|c}\underbrace{11\ldots1}_{G_1} & \underbrace{00\ldots0}_{G_2}\end{array}\right),$$

де кількість одиниць у першому рядку дорівнює d.

Тоді $G2$ є породжувальною матрицею альтернантного коду Гоппи $Y'(n',k',d')$ з параметрами [17]

$$n'=n-d,\quad k'=k-1,\quad d'\ge d/2.$$

Розглянемо можливість застосування описаних методів для забезпечення цілісності даних у системах промислового Інтернету речей.

Друга конструкція дає змогу отримати параметри коду, кращі порівняно з іншими методами скорочення. Однак для її застосування необхідно знати кількість одиниць у будь-якому рядку перевірчої матриці H коду Гоппи $Y(n,k,d)$, яка не менша, ніж мінімальна відстань d' дуального коду Y'. Для оцінювання дуальної відстані здебільшого використовується частковий комп'ютерний перебір слів дуального коду [20]. Однак для кодів Гоппи такі оцінки не відомі. Оскільки коди БЧХ є підкласом кодів Гоппи, скористаємося оцінками дуальної відстані для кодів БЧХ. У табл. 2 подано результати розрахунку верхньої оцінки дуальної відстані, отримані відповідно до [21], для кодів БЧХ зі швидкістю $R=1/2$.

Таблиця 2. *Верхня оцінка дуальної відстані для кодів БЧХ зі швидкістю* $R=1/2$

n,k,d	511,259 ,57	255,127,33	127,64,19	63,27,13	31,16, 7
d'	128	64	32	16	8

У табл. 3 запропоновано параметри скорочених двійкових кодів Гоппи n', k', отримані за допомогою комп'ютерного моделювання для описаної конструкції скорочення. У цьому разі d_1 позначає мінімальну кількість одиниць в одному рядку, а d_2 – в об'єднанні двох рядків перевірчої матриці H коду Гоппи.

Аналіз досягнутих результатів демонструє, що цей метод не дає змогу скорочувати коди на незначну кількість символів. Отже, у цьому разі неможливо гнучко змінювати параметри коду, а також здебільшого скорочення приводить до кодів, рівних за довжиною кодам меншого поля Галуа. А, як відомо, зі збільшенням розмірності коду, за однакових d, швидкість коду зменшується, тобто значне скорочення коду більшого поля приводить до коду з меншою кількістю інформаційних символів, ніж скорочення на кілька бітів коду меншого поля.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189)
ISSN 3083-7650 (0135-1710) (print) Management Information System and Devices. 2026. No. 2 (189)

Таблиця 3. *Параметри деяких скорочених кодів Гоппи*

m	n, k, d	d_1	d_2	n_1', k_1', d	n_2', k_2', d
7	127, 92, 11	≤ 32	≤ 48	95, 61, 11	76, 46, 11
	127, 57, 21	≤ 22		105, 37, 21	
	127, 50, 23	≤ 16	≤ 24	111, 36, 23	103, 28, 29
	127, 36, 29	≤ 14	≤ 24	113, 23, 29	103, 14, 29
8	255, 223, 9	≤ 96		159, 128, 9	
	255, 191, 17	≤ 64		191, 128, 17	
	255, 159, 25	≤ 48	≤ 99	207, 112, 25	156, 62, 25
	255, 143, 29	≤ 48	≤ 85	207, 96, 29	170, 60, 29
9	511, 457, 13	≤ 184		327, 274, 13	
	511, 421, 21	≤ 172		339, 250, 21	
	511, 385, 29	≤ 156		355, 230, 29	

Метод Хелгерта і Стінаффа дає змогу скорочувати код Гоппи мінімум на $d_{\min}$ символів. У табл. 4 подано конструктивну кодову відстань деяких кодів Гоппи зі швидкістю $R = 1/2$, розраховану за допомогою комп'ютерного моделювання.

Таблиця 4. *Конструктивна кодова відстань кодів Гоппи зі швидкістю* $R = 1/2$

n	511	255	127	63	31
d	61	37	21	13	7

Аналіз показників із табл. 4 демонструє, що метод Хелгерта і Стінаффа має ті самі недоліки, що й друга конструкція скорочення. Отже, найбільш ефективний захист має перший метод, що дає змогу скорочувати коди Гоппи на будь-яку кількість символів.

Отже, застосування процедур скорочення до кодів Гоппи сприяє отриманню кодів, що мають задані характеристики із завадостійкості та можуть бути використані для забезпечення цілісності даних у системах промислового Інтернету речей.

Метод забезпечення цілісності даних із застосуванням скорочених кодів Гоппи

На основі проведених досліджень запропоновано метод забезпечення цілісності даних у системах промислового Інтернету речей з використанням скорочених кодів Гоппи.

Метод оснований на застосуванні в каналах передачі даних систем промислового IIoT кодових конструкцій скорочених кодів Гоппи, які гарантують одночасне забезпечення завадостійкості, тобто виявлення й виправлення випадкових помилок, контроль цілісності даних і мають потенційну можливість реалізувати інформаційну скритність повідомлень.

Особливістю кодів Гоппи є наявність значної кількості способів формування коду із заданими параметрами, що визначаються багаточленом Гоппи $G(x)$ ступеня t з коефіцієнтами з поля $GF(qm)$.

Як ключові дані запропоновано використовувати багаточлен Гоппи $G(x)$, а також кількість і позиції символів скорочення.

Параметрами цього методу обираємо:

– поле Галуа $GF(qm)$;

– багаточлен Гоппи $G(x)$, що не приводиться;

– початковий код Гоппи $Y(n,k,d)$;

– кількість символів скорочення p і множину позиції символів скорочення.

Запропонований метод дає змогу реалізувати комбінований підхід до забезпечення захисту від випадкових помилок і цілісності даних. Він поєднує методи завадостійкого кодування й елементи криптографічного захисту на основі скорочених кодових конструкцій. Використання скорочених кодів Гоппи в системах промислового IIoT забезпечує високу ефективність захисту від випадкових завад, гарантує контроль цілісності даних і потенційну інформаційну скритність повідомлень.

Перевагою запропонованого методу є потенційна можливість підвищувати стійкість завдяки впровадженню динамічної зміни параметрів скороченого коду Гоппи.

Приклад системи забезпечення цілісності даних у системах промислового Інтернету речей

У сучасних системах промислового IIoT найбільш поширеними є платформи Siemens

Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 2 (189) *ISSN 3083-7650 (0135-1710) (print)*

MindSphere, PTC ThingWorx, GE Digital Predix та IBM Maximo Application Suite. Для прикладу системи забезпечення цілісності було обрано платформу Siemens MindSphere, що забезпечує інтеграцію промислових сенсорів, контролерів, SCADA-систем і хмарних сервісів для реалізації моніторингу й автоматизованого управління виробничими процесами. Для передачі даних можуть застосовуватися різні види зв'язку, тому на канальному рівні використовуються різні протоколи, а саме Ethernet / PROFINET, Wi-Fi (IEEE 802.11ac/ax, IEEE 802.15.4 / WirelessHART / ZigBee, LoRaWAN, 5G NR Industrial IoT. У перелічених протоколах одним із методів забезпечення завадостійкості передачі є застосування CRC – циклічного завадостійкого коду в режимі виявлення помилок. Водночас залежно від призначення пакету й типів даних, що передаються, їх параметри дуже широко змінюються. Динамічний характер деяких пакетів у системах IIoT не дає змоги використовувати коди Гоппи з механізмом виправлення помилок. Тому запропоновано застосовувати пакети від промислових датчиків, які передають фіксовані за довжиною дані за протоколом PROFINET IRT. Розмір корисних показників датчика становить $k = 512$ бітів (64 Байти). Для забезпечення цілісності даних у цьому разі пропонується використати двійковий скорочений код Гоппи над полем $GF(210)$, що допоможе отримати максимальну довжину кодового слова $n_{\max} = 210 = 1024$ біти. Якщо обрати можливість коду виправляти помилки, створені короткими імпульсними індустріальними завадами, то оберемо $t = 3$. Тоді кількість перевірчих символів дорівнюватиме $r = mt = 10 \times 3 = 30$. Оскільки в пакеті під перевірку зарезервовано 32 біти, то 2 біти залишаться як апаратний padding для вирівнювання рівно в 4 Байти $(r = 32)$. Тоді для $k = 512$ бітів повна довжина пакету дорівнюватиме 544 біти.

Висновки

У статті досліджено питання забезпечення цілісності даних у сучасних системах промислового Інтернету речей в умовах дії ненавмисних завад і впливів кіберзловмисників. З огляду на це запропоновано комбіноване рішення щодо застосування завадостійких кодів, які мають високі характеристики завадостійкості й чимало способів формування коду із заданими параметрами, а саме кодів Гоппи.

У роботі встановлено, що використання модифікованих кодів Гоппи дасть змогу забезпечити не тільки завадостійкість і цілісність даних у системах IIoT, але й потенційно має перспективи гарантувати інформаційну скритність повідомлень. Дослідження методів модифікації завадостійких кодів продемонструвало, що більшість із них або обмежують здатність гнучкої зміни параметрів коду, або призводять до зниження його характеристик завадостійкості, що унеможливлює їх одночасне використання для забезпечення цілісності даних і захисту їх від перешкод у системах промислового Інтернету речей. На підставі проведеного аналізу визначено, що для комбінованого забезпечення цілісності та завадостійкості даних можна впроваджувати методи скорочення кодів. Ці методи потенційно здатні забезпечувати задану кодову відстань і формувати сімейства кодів Гоппи із різними параметрами.

Дослідження методів скорочення кодів Гоппи, побудованих на основі багаточленів із коренями й багаточленів, які не приводяться, підтвердили, що більш доцільним є використання кодів, сформованих на основі багаточленів, що не приводяться. Вони не тільки дають змогу формувати значну кількість кодових конструкцій, але й впливають на стійкість системи забезпечення цілісності даних унаслідок ускладнення задачі визначення структури коду.

Проведений аналіз конструкцій скорочення кодів Гоппи продемонстрував, що для побудови комбінованої системи забезпечення цілісності та завадостійкості даних найбільш ефективною є перша конструкція скорочення, яка забезпечує зміну параметрів коду на довільну кількість символів скорочення без погіршення його характеристик завадостійкості. Крім того, використання символів скорочення як ключових даних дає потенційну можливість у цьому разі забезпечити інформаційну скритність повідомлень у системах IIoT.

Отже, досягнуті результати досліджень підтверджують, що застосування процедур скорочення до кодів Гоппи сприяє формуванню кодових конструкцій, які можуть забезпечити цілісність і завадостійкість даних у системах промислового Інтернету речей.

Для подальших досліджень становить інтерес розроблення методів формування кодових слів

ISSN 3083-7715 (online) *Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189)*
ISSN 3083-7650 (0135-1710) (print) *Management Information System and Devices. 2026. No. 2 (189)*

скорочених кодів Гоппи, що забезпечують інформаційну скритність, а також застосування запропонованих рішень у сучасних системах IIoT.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів, зокрема фінансового, особистого, авторського чи будь-якого іншого характеру, який міг би вплинути на дослідження, а також на результати, опубліковані в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

Використання засобів штучного інтелекту

Автори підтверджують, що не застосовували технології ШІ для написання цієї роботи.

References

1. Mishra, N., Islam, S. K. H., Zeadally, S. (2024), "A survey on security and cryptographic perspective of Industrial-Internet-of-Things", *Internet of Things*, 25, Article 101037. DOI: https://doi.org/10.1016/j.iot.2023.101037
2. Wang, M., Sun, Y., Sun, H., Zhang, B. (2023), "Security Issues on Industrial Internet of Things: Overview and Challenges", *Computers*, 12(12), Article 256. DOI: https://doi.org/10.3390/computers12120256
3. Makrakis, G. M., Roberson, D., Kolias, C., Cook, D. (2023), "WIPP: Towards IEC 62443-3-3 Network Compliance via Software-Defined Networking in Digital Substations", In: *2023 Resilience Week (RWS)*. IEEE, pp. 1–7. DOI: https://doi.org/10.1109/RWS58133.2023.10284649
4. Yevheniev, A., Sydorenko, Z., Sievierinov, O. (2025), "Ensuring data integrity in industrial Internet of Things systems using error-correcting codes", *Radiotekhnika*, (221), pp. 46-50. DOI: https://doi.org/10.30837/rt.2025.2.221.06
5. Singh, H. (2019), "Code based cryptography: Classic McEliece"? *arXiv preprint arXiv:1907.12754*. DOI: https://doi.org/10.48550/arXiv.1907.12754
6. García-Morchón, O., Marojevic, V., Kumar, S. (2024), "Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process", *Technologies*, 12(12), Article 241. DOI: https://doi.org/10.3390/technologies12120241
7. Halim, S.K.,Sugeng, K.A. (2024), "Application of Goppa Code in Niederreiter Cryptosystem", *AIP Conference Proceedings*, 3163(1), Article 030002. DOI: https://doi.org/10.1063/5.0213630
8. Yevseiev, S., Kots, H., Minukhin, S., Korol, O., Kholodkova, A. (2017), "The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes", *Eastern-European Journal of Enterprise Technologies*, Vol. 5(9 (89), pp. 19–35. DOI: https://doi.org/10.15587/1729-4061.2017.109879
9. Baldi, M., Santini, P., Cancellieri, G. (2017), "Post-quantum cryptography based on codes: State of the art and open challenges", *in 2017 AEIT International Annual Conference.* Piscataway, NJ: IEEE, pp. 1–6. DOI: https://doi.org/10.23919/AEIT.2017.8240549
10. Kuznetsov, A., Pushkar’ov, A., Kiyan, N., Kuznetsova, T. (2018), "Code-based electronic digital signature", in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. Kyiv, Ukraine: IEEE, pp. 331–336. DOI: https://doi.org/10.1109/DESSERT.2018.8409154
11. Gorbenko, Y., Kiian, A., Pushkar’ov, A., Korneiko, O., Smirnov, S., Kuznetsova, T. (2019), "Code-based hybrid cryptosystem: Comparative studies and analysis of efficiency", *International Journal of Computing*, 18(4), pp. 372–380. DOI: https://doi.org/10.47839/ijc.18.4.1608
12. Melenti, Y., Korol, O., Shulha, V., Milevskyi, S., Sievierinov, O., Voitko, O., Rzayev, K., Husarova, I., Kravchenko, S., Pashayeva, S. (2025), "Development of post-quantum cryptosystems based on the Rao-Nam scheme’, *Eastern-European Journal of Enterprise Technologies*, Vol. 1(9(133)), pp. 35–48. DOI: https://doi.org/10.15587/1729-4061.2025.323195
13. Balamurugan, C., Singh, K., Ganesan, G., Rajarajan, M. (2021), "Post-quantum and code-based cryptography-some prospective research directions", *Cryptography*, Vol. 5(4), pp. 38. DOI: https://doi.org/10.3390/cryptography5040038
14. Admaty, N., Litsyn, S., Keren, O. (2012), "Puncturing, expurgating and expanding the q-ary BCH based robust codes", In: *2012 IEEE 27th Convention of Electrical and Electronics Engineers in Israel (IEEEI 2012)*. IEEE. DOI: https://doi.org/10.1109/EEEI.2012.6376995

Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 2 (189) *ISSN 3083-7650 (0135-1710) (print)*

15. Chen, X., Cheng, K., Li, X., Mao, S. (2023), "Random Shortening of Linear Codes and Applications". In: *Computing and Combinatorics: 29th International Conference, COCOON 2023, Tianjin, China, August 4–6, 2023, Proceedings*. Lecture Notes in Computer Science, vol. 14455. Cham: Springer, pp. 184–197. DOI: https://doi.org/10.1007/978-3-031-49193-1_14
16. Balamurugan, C., Singh, K., Ganesan, G., Rajarajan, M. (2021), "Post-Quantum and Code-Based Cryptography - Some Prospective Research Directions", *Cryptography*, Vol. 5(4), Article 38. DOI: https://doi.org/10.3390/cryptography5040038
17. Fedorchenko, V., Yeroshenko, O., Shmatko, O., Kolomiitsev, O., Omarov, M. (2024), "Password hashing methods and algorithms on the .Net platform", *Advanced Information Systems*, Vol. 8, No. 4, pp. 82–92. DOI: https://doi.org/10.20998/2522-9052.2024.4.11
18. Bezzateev, S. V., Shekhunova, N. A. (1995), "Subclass of binary Goppa codes with minimal distance equal to the design distance", *IEEE Transactions on Information Theory*, Vol. 41(2), pp. 554–555. DOI: https://doi.org/10.1109/18.370170
19. Zinoviev V. A., Litsyn S. N. (1984), "On Shortening of Codes". *Problems of Information Transmission*, Vol. 20, No. 1, pp. 1–7.
20. Krasikov, I., Litsyn, S. (2001), "On the Distance Distributions of BCH Codes and Their Duals". *Designs, Codes and Cryptography*, Vol. 23(2), pp. 223–232. DOI: https://doi.org/10.1023/A:1011220817609
21. Ding, C., Li, C. (2024), "BCH cyclic codes", *Discrete Mathematics*, Vol. 347(6), Article 113918. DOI: https://doi.org/10.1016/j.disc.2024.113918

Received (Надійшла) 06.04.2026
Accepted for publication (Прийнята до друку) 17.05.2026
Publication date (Дата публікації) 29.05.2026

Відомості про авторів / About the Authors

Сидоренко Зоя Михайловна – Харківський національний університет радіоелектроніки, аспірантка кафедри безпеки інформаційних технологій; м. Харків, Україна;
Zoia Sydorenko – Kharkiv National University of Radio Electronics, Postgraduate Student of the Department of Information Technology Security; Kharkiv, Ukraine;
e-mail: zoia.sydorenko@nure.ua
ORCID ID: https://orcid.org/0000-0002-0104-6807

Сєвєрінов Олександр Васильович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій; м. Харків, Україна;
Oleksandr Sievierinov – PhD (Technical Sciences), Associate Professor, Kharkiv National University of Radio Electronics, Professor of the Department of Information Technology Security, Kharkiv, Ukraine;
e-mail: oleksandr.sievierinov@nure.ua
ORCID ID: http://orcid.org/0000-0002-6327-6405

METHOD FOR ENSURING DATA INTEGRITY USING A MODIFIED ERROR-CORRECTING CODE IN INDUSTRIAL INTERNET OF THINGS SYSTEMS

The subject of the study is methods for modifying error-correcting codes to ensure data integrity in Industrial Internet of Things (IIoT) systems. The purpose of the research is to develop a method for ensuring data integrity in Industrial Internet of Things systems through the application of modified error-correcting codes, namely shortened Goppa codes, for the detection and correction of errors arising during information transmission and processing. Objectives: to analyze methods for modifying error-correcting codes, particularly Goppa codes, in order to introduce message obfuscation for ensuring data integrity in Industrial Internet of Things systems; to investigate methods for shortening Goppa codes and determine the most appropriate constructions for providing error resistance and data integrity; to develop a method for ensuring data integrity using a shortened error-correcting code in Industrial Internet of Things systems. To accomplish the outlined objectives, the following methods were applied: theoretical methods of analysis and mathematical modeling, empirical methods of comparative analysis

ISSN 3083-7715 (online) *Автоматизовані системи управління та прилади автоматики. 2026. № 2 (189)*
ISSN 3083-7650 (0135-1710) (print) *Management Information System and Devices. 2026. No. 2 (189)*

of code characteristics, as well as elements of computer experimentation for calculating and evaluating the parameters of shortened Goppa codes. Results achieved. Methods for modifying Goppa codes were analyzed. For constructing a data integrity assurance system in IIoT, a code-shortening method was proposed that preserves the minimum code distance and enables the formation of codes with specified parameters. Constructions for shortening Goppa codes were investigated, and the feasibility of using shortened Goppa codes based on irreducible polynomials was substantiated. A method for ensuring data integrity using shortened Goppa codes was proposed. Conclusions. The implementation of shortening procedures for Goppa codes constructed on the basis of irreducible polynomials makes it possible to form code constructions for ensuring data integrity in Industrial Internet of Things systems while simultaneously maintaining high error-resistance properties. A method for ensuring data integrity using shortened Goppa codes has been proposed, providing flexible adjustment of code parameters and offering prospects for guaranteeing the information concealment of messages.

Keywords: Industrial Internet of Things; error resistance; integrity; error-correcting code; Goppa code; code modification; shortened code.

Бібліографічні описи / Bibliographic descriptions

Сидоренко З. М., Сєвєрінов О. В. Метод забезпечення цілісності даних із використанням модифікованого завадостійкого коду в системах промислового інтернету речей. *Автоматизовані системи управління та прилади автоматики*. 2026. № 2 (189). С. 235–246. DOI: https://doi.org/10.30837/0135-1710.2026.189.235

Sydorenko, Z., Sievierinov, O. (2026), "Method for ensuring data integrity using a modified error-correcting code in industrial internet of things systems", *Management Information System and Devices*, No. 2 (189), P. 235–246. DOI: https://doi.org/10.30837/0135-1710.2026.189.235