ОЦІНКА СТІЙКОСТІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЗІ СКОРОЧЕНИМИ КОДАМИ ГОППИ

Сидоренко З.М., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В даний час забезпечення цілісності даних у системах IIoT є критичним аспектом інформаційної безпеки, оскільки у промисловому середовищі порушення цілісності може призвести до неправильного функціонування обладнання, аварій та втрати довіри до системи [1].

Перспективним рішенням для забезпечення цілісності даних у системах IIoT є поєднання криптографії та завадостійкого кодування. Запропоновано для забезпечення цілісності даних використовувати завадостійкі коди Гоппи, що дозволить вирішувати такі завдання, як забезпечення цілісності та інформаційної скритності каналів передачі даних у системах IIoT [1, 2].

Для забезпечення функціонування даної системи забезпечення цілісності з скороченими кодами Гоппи необхідно провести оцінку її стійкості.

Метою доповіді є оцінка стійкості системи забезпечення цілісності зі скороченими кодами Гоппи у системах промислового Інтернету речей.

Основним методом перевірки стійкості будь-якої криптосистеми є експертний криптоаналіз в умовах, сприятливих для криптоаналітика [3]. Стійкість більшості систем цілісності спирається не на теоретичну неможливість їхнього розкриття, а на практичну складність такого розкриття, що звичайно виражається в необхідних для цієї мети часових працевтратах (безпечному часі Tsec). При обчисленні нижньої границі цього часу виникає складна задача: знайти найкращий спосіб розкриття системи захисту інформації, тому що завжди існує можливість, що криптоаналітик знайде новий метод аналізу, що вимагає значно менших часових працевтрат.

Стійкість схем, побудованих на кодах Гоппи заснована на складності рішення відомої в теорії завадостійкого кодування важко вирішуваної задачі декодування випадкового коду. Дана задача є NP-важкою, що означає відсутність відомих ефективних (поліноміальних) алгоритмів її точного розв'язання для довільних кодів. Аналогічна обчислювальна складність лежить в основі побудови кодових криптосистем, таких як система Мак-Еліса.

В роботі була проведена оцінка стійкості кодових конструкцій скорочених кодів Гоппи при повному переборі всіх можливих ключів, а також оцінка, заснована на визначенні даних кодів в часовій та частотній області.

При аналізі можливих шляхів розкриття ключових даних системи забезпечення цілісності виходили з того, що задачею криптоаналітика є одержання насамперед закону формування кодових послідовностей.

Одним зі шляхів розкриття будь-якої системи захисту є повний перебір усіх можливих ключів. Однак даний метод не завжди є самим коротким. Тому що для кодів Гоппи вся безліч кодових слів задається за допомогою одного багаточлена G(x), то зловмисник може спробувати розкрити ключові дані,

ґрунтуючись на визначенні даного коду. У цьому випадку розкриття ключового багаточлена еквівалентно рішенню деякої математичної задачі.

Так як тільки один багаточлен Гоппи фіксованого ступеня визначає відповідну безліч кодових слів скороченого коду заданої довжини. Час криптоаналізу Tstar у випадку повного перебору всіх можливих ключів буде визначатися виразом

$$T_{star} = P_д \, I/V = 2^i \, C^i_n \, N_q(t) \, n\log^2 n \, Pд/V,$$

де I – обчислювальна складність криптоаналізу;

V – максимальна продуктивність ЕОМ зловмисника;

n – довжина коду Гоппи;

$N_q(t)$ – кількість багаточленів Гоппи, що неприводяться;

I – кількість символів скорочення коду;

Рд - припустима імовірність успішного криптоаналізу.

Проведена оцінка стійкості системи забезпечення цілісності, заснована на визначенні даних кодів в часовій області. У цьому випадку безпечний час T_{math} буде дорівнювати:

$$T_{math} = I/V = 5 \cdot 2^i C^i_n \, w^2 n\log^2 n \, / \, V,$$

де w – вага кодового слова скороченого коду Гоппи.

В роботі проведена оцінка стійкості системи забезпечення цілісності, заснована на визначенні даних кодів в частотній області. Безпечний час T_{math} у цьому випадку буде дорівнювати:

$$T_{math} = I/V = 3 \cdot 2^i C^i_n \cdot (n\text{-}z) z^2 n\log n \, / \, V,$$

де z – кількість нульових символів у кодовому слові скороченого коду Гоппи.

Порівнюючи вирази оцінки стійкості можна помітити, що при рівному числі символів скорочення, найменшу обчислювальну складність дає криптоаналіз в часовій області. що приблизно в n/3logn раз менше обчислювальних операцій, чим у частотній області. Тому при виборі кодів Гоппи, що задовольняють заданим вимогам до цілісності інформації і стійкості ключа доцільно використовувати вираз, заснований на визначенні даних кодів в часовій області. За результатами криптоаналізу в часовій області були отримані характеристики, що дозволяють визначити необхідні умови реалізації заданої стійкості ключа.

Список літератури

1. Yevheniev, A. M., Sydorenko, Z. M., & Sievierinov, O. V. (2025). Забезпечення цілісності даних у системах промислового інтернету речей на основі використання завадостійких кодів. Radiotekhnika, (221), 46-50.

2. Євгеньєв, А. М., Сидоренко, З. М., & Сєвєрінов, О. В. (2025). *Метод забезпечення цілісності даних у системах промислового інтернету речей*. Тези доповідей п'ятнадцятої міжнародної науково-технічної конференції, 24–25 квітня 2025 року, Том 3: секції 3, 4. - Баку – Харків – Жиліна – 2025.

3. Горбенко, Ю. І., & Ганзя, Р. С. (2014). Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем. *Восточно-Европейский журнал передовых технологий*, *1*(9 (67)), 8-16.