ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056.55 https://doi.org/10.31713/vt320198

Джоші А., аспірант (Національний університет водного господарства та природокористування, м. Рівне)

РОЗПОДІЛЕНЕ ЗБЕРЕЖЕННЯ ДАНИХ З ВИКОРИСТАННЯМ ЗАВАДОСТІЙКОГО КОДУВАННЯ

Проведено огляд теоретичних відомостей з теорії інформації та кодування, аналіз сучасних завадостійких кодів на предмет їх застосовності для збереження даних. Проаналізовано доцільність створення розподіленого сховища даних, основним механізмом збереження інформації якого є завадостійке кодування Ріда-Соломона.
Ключові слова: **розподілені застосунки, завадостійке кодування.**

Постановка проблеми. Останнім часом питання збереження та управління персональними даними стало одним з найважливіших в сфері інформаційних технологій. У 2018 році Європейським Союзом було прийнята постанова щодо захисту персональних даних осіб в межах Європейського Союзу – загальний регламент про захист даних, основною метою якого є посилення та уніфікація захисту персональних даних [1]. Зважаючи на зовнішню орієнтованість, цей документ має безпосередній вплив і на український ринок надання послуг з розробки програмного забезпечення.

До ключових принципів регламенту про захист даних належать:

- цілісність і конфіденційність – при обробці даних необхідно забезпечити захист персональних даних від несанкціонованої чи незаконної обробки, знищення чи ушкодження;
- точність – неточні персональні дані мають бути видалені або виправлені.

Саме тому вивчення методів та інструментів, здатних підвищити захищеність інформаційних систем є актуальною задачею в умовах підвищення вимог до обробки та збереження конфіденційної інформації. Нині для неможливості знищення інформаційних об'єктів все частіше використовуються розподілені сховища даних, а проблема управління доступом вирішується за допомогою математичних методів захисту інформації.

Аналіз останніх досліджень та публікацій. Проблемам розпо-

ділених застосунків присвячені дослідження таких авторів як Ендрю Таненбаум, Джош Лонг та Брендан Бьорнс. Аналіз останніх досліджень у цій галузі свідчить про доцільність вивчення розподілених систем та методів збереження інформації в них. Варто зазначити доцільність окремого вивчення таких принципів побудови розподілених сховищ даних як цілісність та конфіденційність. Вивченням цих вимог займалися наступні автори: Бессалов А. В. та Джеймс Планк.

Мета і завдання дослідження. Метою дослідження є вивчення доцільності використання завадостійкого кодування як методу розподіленого збереження даних. З метою досягнення поставленої мети було передбачено розв'язання наступних завдань:

• огляд теоретичних відомостей з теорії інформації та кодування

• аналіз сучасних завадостійких кодів на предмет їх застосовності для збереження даних

• огляд теоретичних відомостей з систем шифрування з відкритими ключами, алгоритмів цифрового підпису

• аналіз алгоритмів цифрового підпису на предмет їх застосовності для управління доступом до персональних даних

• побудова розподіленого сховища даних

Виклад основного матеріалу. Відомо, що коди Ріда-Соломона можуть використовуватися для забезпечення виправлення помилок в RAID-системах. RAID (Redundant Array of Independent Disks) – технологія віртуалізації даних, що об'єднує декілька дисків в логічний елемент для введення надлишковості та забезпечення підвищення продуктивності [3].

Основна проблема збереження даних в розподілених системах наступна. Нехай в системі існує n пристроїв збереження даних $D_1, D_2, ..., D_n$, кожен з яких вміщає k байтів. Такі пристрої прийнято називати *пристроями збереження даних.* Також в систему додаються m пристроїв $C_1, C_2, ..., C_n$, кожен з яких також вміщає k байтів. Такі пристрої називають *пристроями контрольних сум.* Значення, що міститься в пристроях контрольних сум повинно бути обраховано на основі даних, що містяться в пристроях збереження даних. Суть проблеми полягає в визначенні алгоритму обрахунку значень контрольних сум таким чином, щоб при відмові будь-яких m пристроїв з набору $D_1, D_2, ..., D_n, C_1, C_2, ..., C_n$, їх зміст можна було відновити з даних пристроїв, що продовжують свою роботу.

Коди виправлення помилок були відкриті математиками ще десятки років назад. Проте технологія розподілення даних між багатьма пристроями збереження даних, із забезпеченням швидкості пе-

редачі інформації та можливістю самовідновлення, є досить новою. Першим прототипом подібних систем стала технологія RAID, в якій невеликі жорсткі диски групувалися в масив, що забезпечував відносно велику ємність, швидкість передачі інформації та надійність. З того часу, технологія почала використовуватися для розробки мережевих файлових систем, що забезпечували б високу надійність та швидкість передачі інформації. Такі системи почали називати *RAID-подібними* системами [2].

Проблема збереження даних в розподілених системах є однією з найбільш гострих і для всіх RAID-подібних систем. Якщо збереження даних забезпечується набором з n пристроїв, то шанс, що хоча б один з цих пристроїв вийде з ладу, є досить високим. Відповідно, відмовостійкість стає однією з найбільш важливих вимог, що виставляються до RAID-подібних систем.

Для невеликих значень n кількості пристроїв збереження даних, один пристрій контрольної суми може виявитися достатнім для забезпечення відмовостійкості. Подібна конфігурація використовувалася в одному з базових рівнів RAID 5, та називається $(n+1)$-*парністю.* За використання подібної конфігурації, кожен байт інформації, що міститься на пристрої контрольної суми обраховується як побітове додавання за модулем 2 (XOR). Відповідно, якщо якийсь один пристрій збереження даних з $(n+1)$ пристроїв перестане функціонувати, його інформація може бути відновлена з тих n пристроїв, що продовжили свою роботу. Перевагами такого підходу є його простота реалізації. Реалізація вимагає лише одного надлишкового пристрою збереження даних та лише однієї додаткової операції запису до одного пристрою. Зрозуміло, що найбільшим недоліком такої системи є неможливість її відновлення від декількох одночасних збоїв пристроїв збереження даних.

З ростом кількості пристроїв n, можливість відновлення від одночасних збоїв стає все важливішою. Існує декілька технологій для відновлення від m одночасних збоїв. Найбільш звична технологія відновлення – технологія, що базується на кодах Ріда-Соломона. Дана технологія також знайшла своє застосування і в RAID-подібних системах. Системи, побудовані на основі такого підходу є значно складнішими в реалізації, ніж системи побудовані на основі принципу $(n+1)$-парності, проте існує можливість управління рівнем відмовостійкості за рахунок наявності контролю над кількістю пристроїв збереження даних та кількістю пристроїв контрольних сум.

Поняття помилки в розподілених системах збереження даних є

дещо відмінним від звичайного поняття помилки в теорії інформації та кодування. Помилка в розподілених системах розцінюється як *стирання.* При відмові пристрою, він може бути вимкненим, або зв'язок до пристрою може бути відсутнім. Звичне поняття помилки полягає в збереженні та отриманні некоректних значень. Визначення значень на кожному пристрої контрольних сум C_i вимагає введення перетворення (функції) F_i, що може бути застосована до даних на всіх пристроях збереження інформації.

Кодування Ріда-Соломона в RAID системах розбиває кожен пристрій збереження даних на *слова*. Довжина кожного слова дорівнює w бітів, де w може змінюватися відповідно до зовнішніх обмежень. Відповідно, пристрій збереження даних містить $l = \frac{8k}{w}$ слів кожен. Функції кодування F_i працюють над словами, відповідно $x_{i,j}$ відповідає за j-те слово пристрою X_i (рис. 1).

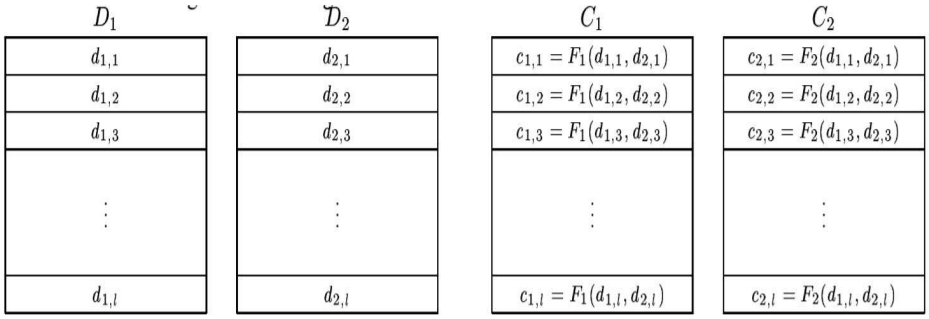

Рис. 1. Розподіл інформації між пристроями збереження даних

Для обрахування слова контрольної суми c_i для пристрою C_i, необхідно застосувати функцію F_i наступним чином

$$c_i = F_i(d_1, d_2, ..., d_n). \quad (1)$$

Якщо інформаційне слово на пристрої D_j змінюється з d_j на d'_j, то кожне слово контрольної суми повинно бути перераховано застосуванням функції $G_{i,j}$ наступним чином

$$c'_i = G_{i,j}(d_j, d'_j, c_i). \quad (2)$$

У випадку відмови не більше m пристроїв, система може бути відновлена за наступним алгоритмом. Першим кроком є створення функції для відновлення слів в пристроях збереження даних, що викликали відмову. Наступним кроком є перерахунок значень пристро-

їв контрольних сум застосуванням перетворення F_i.

У випадку, коли $m=1$, можна застосувати звичайний метод $(n+1)$-парності. У цьому випадку є лише один пристрій контрольних сум C_1 та слово складається лише з одного біту $(w=1)$. Для того, щоб обрахувати значення слова контрольної суми c_1 необхідно просто обрахувати суму всіх інформаційних слів за модулем 2

$$c_1 = F_1(d_1,...,d_n) = d_1 \oplus d_2 \oplus ... \oplus d_n . \quad (3)$$

Якщо інформаційне слово на пристрої D_j змінюється з d_j на d'_j, то значення c_1 повинно бути перераховано наступним чином

$$c'_1 = G_{1,j}(d_j, d'_j, c_1) = c_1 \oplus d_j \oplus d'_j . \quad (4)$$

Якщо зв'язок до пристрою збереження D_j втрачається, то кожне слово може бути відновлене наступним чином

$$d_j = d_1 \oplus ... \oplus d_{j-1} \oplus d_{j+1} \oplus ... \oplus d_n + c_1 . \quad (5)$$

Тобто, в розглянутому вище випадку система є стійкою до відмов одиночних пристроїв збереження даних.

У випадку, коли $m>1$, застосовується наступний принцип. Визначаються перетворення F_i таким чином, щоб це перетворення було лінійною комбінацією інформаційних слів

$$c_i = F_i(d_1, d_2, ..., d_n) = \sum_{j=1}^{n} d_j f_{i,j} . \quad (6)$$

При представленні інформаційних та слів контрольних сум у вигляді векторів D та C, та перетворень F_i як рядків матриці F, то (6) можна представити наступним чином

$$FD = C . \quad (7)$$

У випадку кодування Ріда-Соломона в RAID системах матриця F визначається як матриця Вандермора розмірності $m \times n$: $f_{i,j} = j^{i-1}$ і в такому випадку (7) приймає наступний вигляд

$$\begin{bmatrix} f_{1,1} & f_{1,2} & \dots & f_{1,n} \\ f_{2,1} & f_{2,2} & \dots & f_{2,n} \\ \dots & \dots & \dots & \dots \\ f_{m,1} & f_{m,2} & \dots & f_{m,n} \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \dots \\ d_n \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & n \\ \dots & \dots & \dots & \dots \\ 1 & 2^{m-1} & \dots & n^{m-1} \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \dots \\ d_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_m \end{bmatrix} \quad (8)$$

Якщо одне із інформаційних слів d_j змінюється на d'_j то кожне із слів контрольних сум також змінюється за наступним принципом

$$c'_i = G_{i,j}\left(d_j, d'_j, c_i\right) = c_i + f_{i,j}\left(d'_j - d_j\right). \quad (9)$$

Для відновлення від стирань визначається матриця A та вектор E наступним чином

$$A = \begin{bmatrix} I \\ F \end{bmatrix}, \quad E = \begin{bmatrix} D \\ C \end{bmatrix}. \quad (10)$$

Відповідно, має місце рівність

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2 & \dots & n \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 2^{m-1} & 3^{m-1} & \dots & n^{m-1} \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \dots \\ d_n \end{bmatrix} = \begin{bmatrix} d_1 \\ d_2 \\ \dots \\ d_n \\ c_1 \\ c_2 \\ \dots \\ c_m \end{bmatrix}. \quad (11)$$

Кожен пристрій збереження інформації може розглядатися як рядок матриці A та відповідне значення вектору E. Якщо зв'язок з пристроєм втрачається, це зображується видаленням відповідного рядка з матриці A та значення з вектору E. Отримана матриця позначається як A', а новий вектор E' для якого виконується рівність

$$A'D = E'. \quad (12)$$

При одночасній втраті зв'язку до m пристроїв збереження інформації A' має розмірність $n \times n$. Лінійна незалежність рядків отриманою матриці забезпечується тим, що F є матрицею Вандермора, тому кожна підмножина n рядків матриці A є лінійно незалежною множиною векторів. При відновленні всіх значень D, значення слів контрольних сум можуть бути обраховані на їх основі.

Варто звернути увагу, що всі операції над матрицями є загальноприйнятими з лінійної алгебри, проте операції додавання та множення дещо змінені. Операція додавання $(+)$ заміняється на побітове додавання за модулем 2 $(\oplus)$, а операція множення визначається як логарифмування над скінченим полем Галуа.

Існує дві основні реалізації кодування Ріда-Соломона в RAID системах: RAID-контролер та розподілена система контрольних точок (рис. 2, рис. 3).

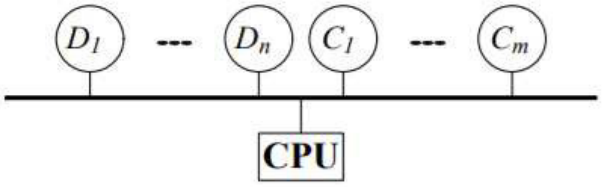

Рис. 2. RAID-контролер

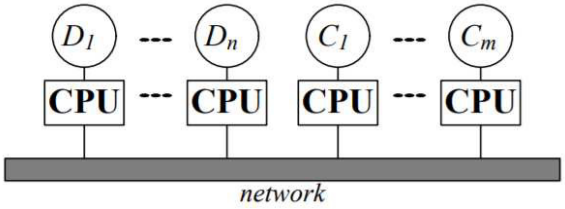

Рис. 3. Система контрольних точок

Система на основі RAID-контролеру складається з одного центрального обробника, що управляє пристроями збереження інформації. Система контрольних точок є розподіленою системою, в якій кожен пристрій збереження інформації управляється виділеним обробником, а самі обробники зв'язані через комунікаційну мережу.

В системах побудованих на основі RAID-контролеру файлова система повинна розбивати вхідну інформацію на n блоків для кожного з пристроїв збереження інформації, обраховувати значення m блоків для кожного з пристроїв контрольних сум та виконувати запис кожного з $n+m$ блоків.

В розподілених системах контрольних точок, використання кодування Ріда-Соломона в RAID-системах дещо відрізняється від того, що використовується в RAID-контролерах. В таких системах є дві основні операції: *створення контрольних точок* та *відновлення.* Для операції створення контрольних точок припускається, що пристрої збереження інформації вже містять якусь інформацію, але пристрої контрольних сум ще не використані. Існує два основних підходи, що можуть бути застосовані для ініціалізації пристроїв контрольних сум (рис. 4, рис. 5).

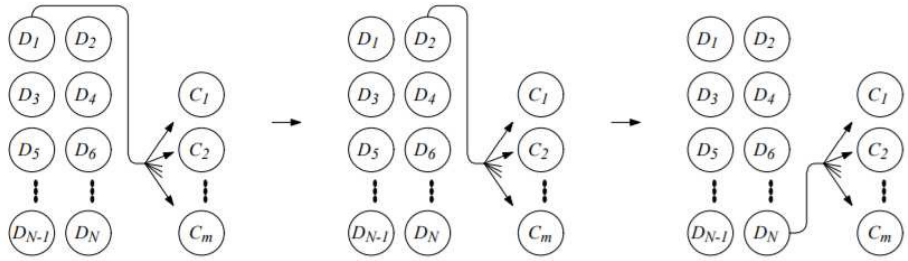

Рис. 4. Алгоритм трансляції

Алгоритм трансляції полягає в наступному. Кожен пристрій контрольних сум створюється з нульовим значенням. Після цього кожен пристрій збереження інформації D_j транслює свої дані кожному пристрою контрольних сум C_i. Після отримання інформації від пристрою D_j, C_i множить своє значення перетворенням $f_{i,j}$ та побітово додає його за модулем 2 до збереженого значення.

Алгоритм агрегації полягає в тому, що кожен пристрій збереження інформації D_j множить своє значення перетворенням $f_{i,j}$, після значення з кожного пристрою збереження інформації отримуються та побітово додаються за модулем 2. Отриманий результат надсилається пристрою контрольних сум C_i.

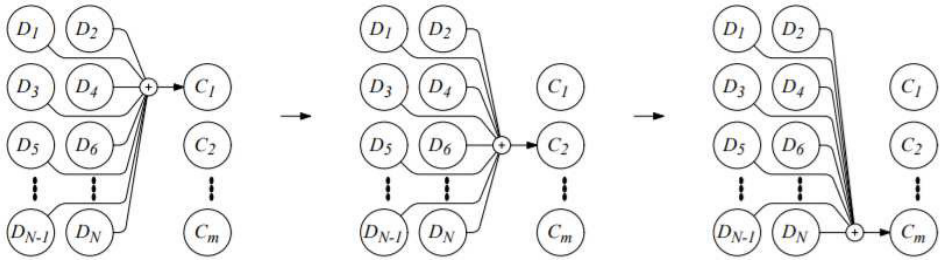

Рис. 5. Алгоритм агрегації

Вибір відповідного алгоритму визначається характеристиками мережі, що використовується для комунікації між пристроями та обробниками. Відновлення після втрати зв'язку виконується обробником кожного пристрою збереження інформації.

Висновки

Розглянуто переваги розширених кодів Ріда-Соломона в практичних реалізаціях в системах кодування за рахунок узгодження з байтовою структурою комп'ютерних даних. Описано можливе застосування кодів Ріда-Соломона в каскадних кодах як зовнішніх кодів каскаду.

Описано можливість використання кодів Ріда-Соломона для збереження даних в розподілених системах. Наведено принципи вирішення проблеми обрахунку значень контрольних сум таким чином, щоб при втраті будь-якого заданого числа пристроїв збереження інформації була можливість відновити дані з пристроїв, що продовжують свою роботу. Розглянуто основні алгоритми вирішення даної проблеми, описано алгоритм кодування та алгоритм відновлення системи після втрати пристроїв збереження даних.

Описано методи перевірки парності для випадку одного при-

строю контрольних сум та метод кодування Ріда-Соломона в RAID системах для випадку кількості пристроїв контрольних сум, що більше одного.

Також наведено дві основні реалізації кодування Ріда-Соломона в RAID системах: RAID-контролер та розподілена система контрольних точок, наведені особливості їх реалізації, принципи вибору конкретної реалізації в залежності від зовнішніх умов та вимог, що ставляться до системи.

1. Regulation of the European parliament and of the council of on the protection natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. **2.** James S. Plank. A tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like systems. Knoxville: University of Tennessee. 2007. 19 с. **3.** Бессалов А. В. Основи теорії інформації та кодування. Київ : НТУУ «КПІ», 2011. 270 с.

REFERENCES:

1. Regulation of the European parliament and of the council of on the protection natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. **2.** James S. Plank. A tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like systems. Knoxville: University of Tennessee. 2007. 19 s. **3.** Bessalov A. V. Osnovy teorii informatsii ta koduvannia. Kyiv : NTUU «KPI», 2011. 270 s.

Dzhoshi A., Post-graduate Student (National University of Water and Environmental Engineering, Rivne)

DISTRIBUTED DATA STORAGE USING ERROR CORRECTION CODES

In this work, the information theory and coding review was done as well as analysis of the modern error correction codes data storage application. Distributed data storage implementation based on error correction codes was done.
Advantages of Reed-Solomon's extended codes in practical implementations in coding systems are using adjustment with byte structure of computer data. Possible use of Reed-Solomon codes in

cascade codes as external cascade codes is described.
The possibility of using Reed-Solomon codes for data storing in distributed systems is described. The principles of solving the problem of checksum values calculation are given in such a way that in case of loss of any given storage devices number, it would be possible to recover data from devices that continue working. The basic algorithms for solving this problem are considered, the algorithm of coding and algorithm of system recovery after loss of storage devices is described.
The methods of parity checking for the case of one checksum device and the Reed-Solomon encoding method for RAID systems for the number of checksum devices greater than one are described.
There are also two main implementations of Reed-Solomon encoding in RAID systems: the RAID controller and the distributed control point system, the specifics of their implementation, the principles of choosing a specific implementation depending on external conditions and system requirements.
***Keywords*: distributed applications, error correction codes.**

Джоши А., аспирант (Национальный университет водного хозяйства и природопользования, г. Ровно)

РАСПРЕДЕЛЕННОЕ ХРАНЕНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Проведен обзор теоретических сведений по теории информации и кодирования, анализ современных помехоустойчивых кодов на предмет их применимости для хранения данных. Проанализирована целесообразность создания распределенного хранилища данных, основным механизмом сохранения информации которого является помехоустойчивое кодирование Рида-Соломона.
Рассмотрены преимущества расширенных кодов Рида-Соломона в практических реализациях в системах кодирования за счет согласования с байтовой структурой компьютерных данных. Описаны возможности применения кодов Рида-Соломона в каскадных кодах как внешних кодов каскада.

Описано использование кодов Рида-Соломона для сохранения данных в распределенных системах. Приведены принципы решения проблемы расчета значений контрольных сумм таким образом, чтобы при потере любого заданного числа устройств хранения информации была возможность восстановить данные с устройств, продолжающих свою работу. Рассмотрены основные алгоритмы решения данной проблемы, описан алгоритм кодирования и алгоритм восстановления системы после потери устройств хранения данных.

Описаны методы проверки четности для случая одного устройства контрольных сумм и метод кодирования Рида-Соломона в RAID системах для случая количества устройств контрольных сумм, больше одного.

Также приведены две основные реализации кодирования Рида-Соломона в RAID системах: RAID-контроллер и распределенная система точек, приведены особенности их реализации, принципы выбора конкретной реализации в зависимости от внешних условий и требований, предъявляемых к системе.

Ключевые слова: **распределенные приложения, помехоустойчивое кодирования.**
