

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»,
Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»,
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

КОЛЯДА КОСТЯНТИН ВЯЧЕСЛАВОВИЧ

УДК 004.934

ДИСЕРТАЦІЯ
МЕТОДИ І ЗАСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ
ВІДНОВЛЕННЯ ДАНИХ, ВТРАЧЕНИХ ПРИ ЇХ ВІДДАЛЕНОМУ
ЗБЕРІГАННІ ТА ПЕРЕДАЧІ В МЕРЕЖАХ

Спеціальність 05.13.05 – Комп’ютерні системи та компоненти

Галузь знань – Інформаційні технології

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Коляда К.В.

Науковий керівник Романкевич Олексій Михайлович,
доктор технічних наук, професор

Київ – 2021

АНОТАЦІЯ

Коляда К. В. Методи і засоби підвищення ефективності відновлення даних, втрачених при їх віддаленому зберіганні та передачі в мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп’ютерні системи та компоненти. – Національний технічний університет України ”Київський політехнічний інститут імені Ігоря Сікорського”, Київ, 2021.

Дисертація присвячена проблемі підвищення ефективності відновлення даних, втрачених при їх віддаленому зберіганні в розподілених системах або при передачі по глобальним мережам.

В роботі проведено аналіз факторів, що впливають на ефективність відновлення даних, втрачених під час їх довготривалого зберігання на віддалених розподілених системах, а також в процесі їх передачі по глобальним мережам. Відновлення втрачених під час зберігання даних здійснюється за рахунок резервних даних, які також зберігаються на віддалених розподілених системах. Відновлення втрачених, або затриманих понад критичний проміжок часу даних при передачі в мережах також здійснюється шляхом передачі резервної інформації разом з основною.

Основний акцент в дисертаційному дослідженні зроблено на підвищенні швидкості відновлення втрачених даних та зменшенні об’єму резервних даних за рахунок урахування особливостей реальних систем віддаленого зберігання даних користувачів.

Для прискорення відновлення втрачених при віддаленому зберіганні даних розроблено метод, оснований на використанні розріджених матриць формування резервних блоків. В реальних системах віддаленого зберігання інформації користувачів та системах комп’ютерного управління віддаленими об’єктами з використанням Інтернету в якості середовища обміну даних,

важливу роль відіграє час відновлення втрачених інформаційних блоків чи затриманих доставкою понад критичний час пакетів даних.

Для систем віддаленого зберігання даних час відновлення складається з двох складових: часу доставки резервних та інформаційних блоків, потрібних для процесу відновлення, та часу виконання обчислень по реконструюванню втрачених блоків. Для систем комп'ютерного управління з обміном даними через Інтернет, час відновлення втрачених чи затриманих пакетів визначається лише часом реалізації обчислень.

Для прискорення процесу відновлення втрачених даних за рахунок зменшення кількості інформаційних та резервних блоків, які використовуються для реконструкції втрачених блоків, пропонується модифікована процедура формування резервних блоків. Ця процедура передбачає побудову матриці A таким чином, щоб кожен її рядок містив ε одиниць, де ε - кількість блоків, які потрібно транспортувати по мережі для відновлення інформаційного блоку. При цьому з необхідністю збільшується кількість m потрібних для відновлення резервних блоків.

Теоретично обґрунтовано та детально розроблено метод побудови розрідженої матриці формування резервних блоків інформації. Виклад запропонованого методу ілюструється числовими прикладами. Виконано теоретичний аналіз ефективності запропонованого методу прискорення відновлення втрачених при віддаленому зберіганні блоків даних. Показано, що змінюючи ступінь розрідженості методу можна гнучко змінювати показники швидкодії. Теоретичні розрахунки підтверджені проведеними експериментальними дослідженнями.

Запропоновано також метод формування резервних пакетів при передачі даних в глобальних мережах, а також технологія їх використання для відновлення втрачених чи пошкоджених пакетів. Наведено математичне та технічне обґрунтування запропонованого методу. На основі отриманих

теоретичних результатів розроблено технологію формування резервних пакетів, які передаються по мережі разом з інформаційними пакетами.

Розроблена технологія прискореного відновлення втрачених пакетів з використанням передобчислень, результати яких в формі специфікацій відновлення зберігаються в табличній пам'яті.

Основна перевага запропонованого методу в порівнянні з відомими полягає в прискоренні процесу відновлення втрачених пакетів, використанні простих лінійних перетворень, що забезпечує ефективну апаратну реалізацію.

Запропоновані процедури відновлення даних за рахунок передачі резервних блоків даних не відміняють процесів і процедур, передбачені моделлю OSI та стеком TCP/IP, і виконуються паралельно з ними на різних рівнях і різними процесорними засобами. По закінченні відновлення даних за запропонованими методами вони використовуються не чекаючи закінчення процесів, передбачених моделлю OSI та стеком TCP/IP.

Теоретично обґрунтовано, розроблено та досліджено метод відновлення “пачок” пакетів та невеликої кількості окремих пакетів, який відрізняється способом побудови матриці формування резервних пакетів, число яких, за рахунок спеціалізації на визначеному домінуючому типі втрат пакетів, зменшено у порівнянні з відомими методами.

Суть запропонованого методу побудови матриці формування резервних пакетів полягає в тому, що вони розділяються на дві групи. Одиниці в рядках першої групи знаходяться на відстані, яка дорівнює максимальній довжині пачки пакетів. Це розвозляє розрідити матрицю і, відповідно зменшити кількість операцій, для відновлення втрачених пакетів.

Теоретичними та експериментальними дослідженнями показано, що розроблений метод, за рахунок його орієнтації на визначеному домінуючому типі втрат інформаційних пакетів дозволяє, в середньому на 30-40% скоротити кількість резервних пакетів, що передаються по глобальним

мережам. Запропонований в рамках методу спосіб побудови матриці формування резервних пакетів забезпечує, при цьому скорочення часу відновлення втраченої “пачки” інформаційних пакетів в 2-4 раз, в залежності від довжини “пачки”, за рахунок розрідження матриці, що має наслідком зменшення обчислювальної складності операцій, пов’язаних з їх реконструюванням.

Запропоноване ефективне технологічне рішення обчислювальної реалізації створених методів у вигляді способу відновлення втрачених інформаційних блоків на основі попередньо створених таблиць специфікацій, який за рахунок оптимізації вибору варіанту реконструювання за критерієм мінімуму кількості блоків даних, які використовуються для цього, а також за рахунок застосування передобчислень, що разом виключають з процесу безпосереднього відновлення ті обчислення, які пов’язані з розв’язанням систем рівнянь, дозволяє на 10-15% прискорити обчислювальну реалізацію реконструювання втрачених блоків в порівнянні з відомими технологіями.

Суттєво новими елементами запропонованого способу відновлення блоків даних на основі таблиць специфікацій від відомих таблиць стандартного розташування, які використовуються в завадостійких кодах є те, що таблиці специфікації дозволяють оптимізувати процедуру відновлення за критерієм мінімуму блоків, що транспортуються для відновлення втрачених блоків, що забезпечує мінімальний час реконструювання втрачених даних, а також використання perfect хеш-адресації таблиці, що також дозволяє скоротити час пошуку в таблиці потрібної специфікації. Принциповою відмінністю запропонованих таблиць специфікацій від таблиць стандартного розташування є те, що на відміну від останніх, які містять в собі скореговані коди даних, специфікації описують математичні операції, які потрібно здійснити для того, щоб отримати відновлені коди втрачених інформаційних блоків при їх віддаленому зберіганні чи втрачених інформаційних пакетів при їх відновленні на стороні приймача.

Розроблено програмні засоби для реалізації синтезу матриць формування резервних блоків за розробленими методами, а також алгоритми та програми для побудови таблиць специфікацій відновлення втрачених блоків. Експериментальні дослідження програмних засоби для практичної реалізації запропонованих в дисертаційному дослідженні методів відновлення втрачених при віддаленому зберіганні блоків даних та втрачених в процесі передачі по глобальним мережам пакетам практично довели працездатність розроблених методів за умови довільних конфігурацій втрат інформаційних та резервних блоків.

Ключові слова: віддалене зберігання даних, хмарні технології, відновлюючі коди, лінійні коди, відновлення втрачених пакетів в мережах, лінійні коди, реконструюючі коди, надійність передачі даних в глобальних мережах в реальному часі

ABSTRACT

Koliada K. V. Methods and tools for increasing the efficiency of recovering of data lost during remote storage and transmission in networks. – Skilled scientific work entitled to manuscript.

Thesis for a PhD degree by specialty 05.13.05 – Computer system and components. National Technical University of Ukraine “Igor Sykorsky Kiev Polytechnic Institute”, Kyiv, 2021.

The dissertation is devoted to the problem of increasing the efficiency of data recovery, lost during their remote storage in distributed systems or during transmission over global networks.

The analysis of factors is carried out in the work. affecting the efficiency of data recovery lost during their long-term storage on remote distributed systems, as well as in the process of their transmission over global networks. Recovery of data lost during storage is carried out at the expense of backup data, which is also stored on remote distributed systems. Recovery of lost or delayed over a critical period of time data during transmission in networks is also carried out by transmitting backup information along with the main.

The main emphasis in the dissertation research is on increasing the speed of recovery of lost data and reducing the amount of backup data by taking into account the features of real systems for remote storage of user data.

To accelerate the recovery of data lost during remote storage, a method based on the use of sparse matrices for the formation of backup blocks has been developed. In real systems for remote storage of user information and computer management systems for remote objects using the Internet as a medium of data exchange, the time of recovery of lost information blocks or delayed delivery of critical data packets plays an important role.

For remote storage systems, the recovery time consists of two components: the delivery time of backup and information blocks required for the recovery process, and the time of calculations to reconstruct the lost blocks. For computer control

systems with Internet communication, the recovery time of lost or delayed packets is determined only by the time of implementation of calculations.

To speed up the process of recovering lost data by reducing the number of information and backup blocks used to reconstruct lost blocks, a modified procedure for forming formation of reserve blocks backup blocks is proposed. This procedure involves constructing the matrix for forming formation of reserve blocks so that each of its rows contains ε units, where ε is the number of blocks that need to be transported over the network to recover the information block. This necessarily increases the number of m required to restore backup units.

The method of construction of a sparse matrix of formation of reserve blocks of information is theoretically substantiated and developed in detail. The presentation of the proposed method is illustrated by numerical examples. Theoretical analysis of the efficiency of the proposed method of accelerating the recovery of data blocks lost during remote storage is performed. It is shown that by changing the degree of rarefaction of the method it is possible to flexibly change the performance indicators. Theoretical calculations are confirmed by experimental studies.

For increasing the efficiency of recovery of data lost during their distributed storage the method for recovering information blocks with their distributed storage no more than r at each of the remote repository has been developed. The method is based on the use of a matrix to form reserve blocks, which is orthogonal within adjacent r columns, and any three columns of the matrix contain an orthogonal submatrix. This guarantees recovery of all r blocks stored in one repository, as well as three blocks that are in different repositories. The method uses a smaller number of redundancy blocks, so there is a lower level of redundancy in comparison with the known methods, which are focused on restoring any r blocks.

The redundancy blocks are proposed to be formed in the form of logical sums of information blocks subsets, which are mapping by the matrix. Reasoning from there are not more than r blocks are placed on each remote repositories, a method

has been developed for constructing a matrix for the formation of redundancy blocks. The method provides for the presence in the constructed matrix of an orthogonal submatrix of size $r \times r$, formed by columns that correspond to blocks contained in one repositories. In addition, the method guarantees the existence of an orthogonal submatrix 3×3 in any three columns of the matrix.

It has been theoretically and experimentally proved that the proposed method makes it possible to reduce excess of redundancy by taking into account the specifics of real information losses that are stored on remote media. The method guarantees data recovery in case of loss of access to one repository as a result of cataclysms or three blocks in different repositories as a result of hardware breakdown or program errors.

A new method of redundant packet formation for data transmission in global networks, as well as a technology of their usage for restoring of lost and damaged data packets is proposed. In article the method for guaranteed restoring not more than three lost and damaged data packets is presented. Mathematical and technical justification of the proposed method is given.

Each of the redundant reserve packet proposed to form as the logical sum of certain subsets of data packets. Formed reserve packets are transmitted together with information packets. The rules of redundancy packets formed whose ensures of the existence of an orthogonal system of equations, which solves the process of reconstruction of lost information packets are mathematically rigorously proven. Based on obtained theoretical results the technologies for redundant packet formation for data transmission in global networks has been developed. The developed technologies are illustrated via examples.

To accelerate the reconstruction of lost packets, the method involves the usage of special pre-computational tables. The technology of forming such tables whose contained specifications for lost packets restoring for different variants packets (main or redundancy) loss is described in detail. Each reconstructed packet is restoring as the logical sum of predefined by specification subsets of data and

redundant reserve no loss packets. The developed method for specification forming ensured the low calculation complexity of packets restoring process.

The main advantage of the proposed method for restoring of lost data packets in global networks in comparison with known methods consist of accelerating of packets reconstruction process by using simple transformation. This provides the possibility of reconstruction lost data packet in global networks in real time. The proposed method ensured high efficiency for hardware implementations.

The proposed procedures for data recovery by transferring backup data blocks do not override the processes and procedures provided by the OSI model and the TCP / IP stack, and are performed in parallel with them at different levels and by different processors. Upon completion of data recovery according to the proposed methods, they are used without waiting for the completion of the processes provided by the OSI model and the TCP / IP stack.

The method of recovery of Burst Packet Loss and a small number of individual packets is theoretically substantiated, developed and investigated.

The essence of the proposed method of constructing a matrix for the formation of backup packets is that they are divided into two groups. The units in the rows of the first group are at a distance equal to the maximum length of the packet packet. This will dilute the matrix and, accordingly, reduce the number of operations to recover lost packets.

Theoretical and experimental studies have shown that the developed method, due to its focus on a certain dominant type of information packet loss, allows, on average, to reduce by 30-40% the number of backup packets transmitted over global networks. The method proposed in the method of constructing a matrix of formation of backup packets provides, while reducing the recovery time of the Burst Packet Loss by 2-4 times, depending on the length of the Burst Packet Loss, by diluting the matrix associated with their reconstruction.

An effective technological solution for computational implementation of the created methods in the form of a method of recovering lost information blocks

based on pre-created tables of specifications, which by optimizing the choice of reconstruction by the criterion of minimum number of data blocks used for this, and exclude from the process of direct recovery those calculations that are associated with the solution of systems of equations, allows to accelerate by 10-15% the computational implementation of the reconstruction of lost blocks in comparison with known technologies.

Significantly new elements of the proposed method of recovering data blocks based on specification tables from known standard location tables used in noise-tolerant codes are that the specification tables allow optimizing the recovery procedure by the criterion of minimum blocks transported to recover lost blocks, lost data, as well as the use of perfect hash addressing table, which also reduces the search time in the table of the desired specification. The main difference between the proposed specification tables and standard layout tables is that, unlike the latter, which contain adjusted data codes, the specifications describe the mathematical operations that must be performed in order to obtain the recovered codes of lost information blocks when stored remotely or lost information packets when they are restored on the receiver side.

Software tools for realization of synthesis of matrices of formation of reserve blocks by the developed methods, and also algorithms and programs for construction of tables of specifications of restoration of the lost blocks are developed. Experimental studies of software for practical implementation of the proposed in the dissertation research methods of recovery of data blocks lost during remote storage and lost in the process of transmission over global networks packets practically proved the efficiency of the developed methods under arbitrary configurations of information and backup blocks.

Keywords: distributed data storage, cloud technologies, erased codes, linear codes, reconstruction lost packet in network, linear codes, recoverable codes, reliability of data transmission in global network in real time.

Список публікацій за темою дисертаційної роботи

1. Коляда К.В. Метод відновлення даних при їх розподіленому зберіганні на віддалених сховищах / К.В. Коляда, В.О. Романкевич, М.М. Орлова, О.П. Марковський // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – № 40. – 2020. – С.44-50.
2. Коляда К.В. Метод резервування та відновлення втрачених даних в глобальних мережах / К.В. Коляда, О.П. Марковський, В.Г. Саверченко, А.І. Торошанко// Телекомунікаційні та інформаційні технології. – № 1 (66). – 2020. – С.4-14.
3. Koliada K.V. Usage of linear erasure codes for increasing reliability and efficiency of information delivery on the internet / K.V. Koliada, N.G. Bardis, O.P. Markovskyi // International Journal of Circuits, Systems and Signal Processing – 2019. – Vol.13. – P.585-592.
4. Дичка И.А. Сравнительный анализ надежности запоминающих устройств с аппаратурной и кодовой избыточностью / И.А. Дичка, К.В. Коляда // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1990. – № 27. – С.35-38.
5. Дичка И.А. Способ коррекции модульных ошибок в запоминающих устройствах / И.А. Дичка, К.В. Коляда, А.В. Наконечный // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1990. – № 27. – С. 51-54.
6. Дичка И.А. Сравнительный анализ надежности ЗУ с использованием различных корректирующих кодов / И.А. Дичка, Е.Ф. Колесник, К.В. Коляда // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1989. – № 26. – С. 46-50.
7. Коляда К.В. Организация структур ПЗУ с сжатием данных / К.В.Коляда, И.А.Дичка // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1988. – № 25. – С. 30-34.

8. Коляда К.В. Применение обобщенного модульного кода Хемминга в компьютерных системах / К.В. Коляда, И.А. Дичка // Міжнародна науково-практична конференція "Проблеми інформатики та комп'ютерної техніки" (ПІКТ – 2013), Чернівецький національний університет імені Юрія Федьковича: Тези доповідей – Чернівці, 27-31 травня 2013 р. – С. 86-88.
9. Дичка И.А. Применение обобщенного кода Хемминга для обеспечения помехоустойчивости информационных систем / И.А. Дичка, К.В. Коляда, Е.С. Сулема // Тези доповідей 3-ї Української конференції з автоматичного керування "Автоматика-96". – Севастополь: СевГТУ, 1996. – Ч. II, С. 165-166.

З М І С Т

	Стор.
ВСТУП	16
Р О З Д І Л 1. АНАЛІЗ ПРОБЛЕМИ ЕФЕКТИВНОГО ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ ПРИ ЇХ ВІДДАЛЕНОМУ ЗБЕРІГАННІ ТА ПЕРЕДАЧІ ПО ГЛОБАЛЬНИМ МЕРЕЖАМ	23
1.1 Аналіз проблеми надійності віддаленого зберігання даних	24
в розподілених системах	
1.2 Аналіз задач відновлення втрачених даних в глобальних	35
мережах	
1.3 Огляд технологій відновлення втрачених даних	42
Висновки до розділу 1.....	46
Р О З Д І Л 2. РОЗРОБКА МЕТОДІВ ЕФЕКТИВНОГО	48
ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ В РОЗПОДІЛЕНИХ СИСТЕМАХ ЇХ ВІДДАЛЕНОГО ЗБЕРІГАННЯ	
2.1 Аналіз моделей відновлення втрачених даних в системах	49
їх віддаленого зберігання	
2.2 Розробка методу прискореного відновлення втрачених	53
при віддаленому зберіганні блоків даних	
2.3 Метод відновлення всіх блоків даних на одному сховищі та трьох... 64	
блоків на різних сховищах	
Висновки до розділу 2	72
Р О З Д І Л 3. ОРГАНІЗАЦІЯ ЕФЕКТИВНОГО ВІДНОВЛЕННЯ	74
ВТРАЧЕНИХ ПРИ ПЕРЕДАЧІ В ГЛОБАЛЬНИХ МЕРЕЖАХ ПАКЕТІВ	
3.1 Метод відновлення втрачених при передачі в глобальних	75
мережах пакетів з урахуванням статистики їх втрат	
3.2 Розробка ефективного відновлення “пачок” втрачених	85
при передачі в глобальних мережах пакетів	
3.3 Організація ефективного відновлення “пачок” втрачених	93
при передачі в глобальних мережах пакетів	

	Стор.
3.4. Аналіз проблеми багаторівневого забезпечення надійності передачі даних в мережі Інтернет	102
Висновки до розділу 3	104
Р О З Д І Л 4. РОЗРОБКА ТЕХНОЛОГІЧНИХ АСПЕКТІВ	107
ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ	
4.1. Аналіз чинників технологічної ефективності процесів відновлення втрачених даних	107
4.2. Розробка способу прискореного відновлення втрачених блоків на основі попередньо створених таблиць специфікацій	113
4.3 Організація швидкого пошуку в таблиці специфікацій	124
Висновки до розділу 4	128
ВИСНОВКИ	130
Список використаних джерел	132
ДОДАТОК А. Лістинг програми	142
ДОДАТОК Б. Перелік наукових публікацій за темою дисертації	148

ВСТУП

Актуальність теми. Динамічний прогрес технологій передачі даних та глобальних мереж суттєво змінює організацію комп'ютерної обробки інформації, надавши потужний імпульс розвитку розподілених систем обробки та зберігання даних. На сьогоднішній день масового застосування набули технології розподіленого зберігання даних користувачів на віддалених носіях.

Важлива перевага цих технологій полягає в більшій надійності в порівнянні із зберіганням даних користувачів на їх власних накопичувачах. Інформація користувачів при їх віддаленому зберіганні потенційно може бути втрачена в результаті цілеспрямованих хакерських чи вірусних атак, помилок в роботі програмного забезпечення, відмов технічних засобів, катаклізмів природного та техногенного характеру.

Основним фактором високої надійності віддаленого зберігання інформації виступає рознесення її по різних, географічно віддалених сховищах, що локалізує втрати даних, які можуть бути відновлені за рахунок резервування. Тобто механізми резервування та відновлення втрачених даних є складовою частиною технології багаторівневого забезпечення надійності віддаленого зберігання даних користувачів.

Відповідно, динамічний розвиток систем віддаленого зберігання даних користувачів диктує необхідність адекватного вдосконалення методів та засобів резервування та відновлення втрачених даних.

Іншим важливим наслідком швидкого прогресу технології Інтернет стало розширення її використання в якості засобу обміну даними в комп'ютерних системах моніторингу стану та управління об'єктами реального світу. В якості таких об'єктів виступають побутові прилади в рамках популярної нині концепції “розумних речей”, віддалені технологічні процеси, засоби відеоспостереження тощо. Для таких застосувань Інтернету критичними є надійність та своєчасність доставки пакетів. Один з найбільш

дієвих способів забезпечення надійності та своєчасності доставки пакетів даних в системах реального часу полягає в застосуванні резервних пакетів, які посилаються разом з інформаційними і використовуються для відновлення втрачених або затриманих при передачі понад критичний час даних.

Таким чином, наукова задача підвищення ефективності резервування та відновлення втрачених блоків даних при їх розподіленому зберіганні на віддалених носіях чи передачі по глобальній мережі в системах комп'ютерного управління є актуальною для сучасного етапу розвитку інформаційних і комп'ютерних технологій.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконувалось на кафедрі системного програмування і спеціалізованих комп'ютерних систем КПП імені Ігоря Сікорського в рамках держбюджетної теми “Методи, моделі, структури та компоненти спеціалізованих комп'ютерних систем моніторингу об'єктів критичного застосування” (номер держреєстрації 0117U004280) згідно з науковим напрямком “Дослідження та розробка нових високоефективних архітектур комп'ютерних систем і мереж загального і спеціального призначення, топологічної організації розподілених систем та комунікаційних технологій в них”.

Мета і завдання дослідження. Мета роботи полягає в підвищенні ефективності відновлення даних, втрачених при їх віддаленому зберіганні або при передачі по глобальним мережам.

Основні задачі дослідження у відповідності до поставленої мети полягають у наступному.

1. Аналіз особливостей сучасного та перспективного стану технологій розподіленого віддаленого зберігання інформації і транспортування пакетів даних по глобальним мережам, обґрунтування критеріїв ефективності резервування даних в віддалених сховищах та при передачі по мережам.

Критичний огляд, з позицій визначених критеріїв, існуючих методів резервування та відновлення втрачених даних, виявлення можливостей підвищення їх ефективності, а також визначення напрямків досліджень по реалізації цих можливостей.

2. Розробка методу прискорення процесу реконструювання втрачених інформаційних блоків користувачів шляхом зменшення кількості потрібних для цього невтрачених блоків, що дозволяє знизити витрати часу на їх передачу по мережі та кількість обчислювальних операцій по відновленню втрачених даних.

3. Розробка методу відновлення даних за наявності обмежень на кількість блоків, що зберігаються на одному віддаленому сховищі, який дозволяє реконструювати всю інформацію користувача в ситуації втрати доступу до одного зі сховищ, а також обмежену кількість блоків даних, що зберігаються на різних сховищах, і який забезпечує зменшення надлишковості резервування в порівнянні з відомими методами.

4. Дослідження можливості підвищення ефективності оперативного реконструювання втрачених чи затриманих понад критичний час пакетів даних в глобальних мережах, за рахунок урахування статистичних характеристик їх втрат та часу передачі, а також розробка на цій основі методу відновлення втрачених пакетів даних з побудовою матриці формування резервних пакетів шляхом пріоритетного вибору її базових компонентів.

5. Розробка технології відновлення втрачених блоків даних за розробленими методами, здатної забезпечити високу швидкодію процесу реконструювання даних за рахунок вибору оптимального, в сенсі мінімуму кількості потрібних для цього операцій, варіанту відновлення, а також використання передобчислень, яке дозволяє виключити з процесу обчислення, пов'язані з розв'язанням систем рівнянь.

6. Розробка алгоритмів та програмних засобів для синтезу матриць формування резервних блоків, а також засобів для побудови таблиць специфікацій відновлення втрачених блоків. Експериментальне дослідження ефективності запропонованих методів резервування та відновлення даних.

Об'єкт дослідження – процеси резервування інформації користувачів при довготривалому розподіленому зберіганні на віддалених сховищах чи при її передачі в глобальних мережах, а також процеси відновлення втрачених або тимчасово недоступних блоків даних чи втрачених або затриманих пакетів при їх передачі в мережах.

Предмет дослідження – методи і засоби формування резервних блоків, а також способи їх використання для відновлення втраченої інформації.

Методи дослідження базуються на теорії ймовірності та математичної статистики, теорії булевих функцій та комбінаторики, теорії завадостійкого кодування, теорії організації обчислювальних процесів, методах організації резервування, а також на використанні методів моделювання.

Наукова новизна одержаних результатів полягає в наступному.

1. Вперше запропоновано метод прискорення відновлення втраченої при віддаленому зберіганні інформації, відмінність якого полягає в формуванні резервних блоків на основі рекурентної функції Галуа з обмеженою кількістю одиничних компонент та її циклічних зсувів, що дозволяє зменшити число невтрачених блоків потрібних для реконструкції, і тим самим знизити витрати часу на їх транспортування по мережі та виконання обчислювальних операцій над ними.

2. Вперше запропоновано метод відновлення інформації при її розподіленому зберіганні не більш ніж по r блоків на кожному з віддалених сховищ, який відрізняється тим, що формування резервних блоків здійснюється на основі спеціальним чином синтезованої фрагментарно-ортогональної матриці, завдяки чому гарантується реконструкція даних при втраті доступу до одного сховища, а також трьох блоків, які зберігаються на

різних сховищах, що забезпечує зменшення надлишковості резервування в порівнянні з відомими методами.

3. Вдосконалено метод відновлення затриманих при передачі інформаційних пакетів даних, за рахунок використання системи пріоритетів при виборі компонентів матриці формування обмеженої кількості резервних пакетів з урахуванням статистичних характеристик затримок транспортування пакетів, що дозволяє підвищити ймовірність можливості відновлення втраченої чи затриманої інформації і тим самим прискорити передачу даних в глобальних мережах.

4. Вперше запропоновано спосіб відновлення втрачених інформаційних блоків на основі попередньо створених таблиць специфікацій, який відрізняється використанням хеш-адресації без колізій, а також способом відновлення за критерієм мінімуму кількості невтрачених блоків, що використовуються для реконструювання даних, що дозволяє на 10-15% прискорити процес відновлення в порівнянні з відомими технологіями.

Практичне значення одержаних результатів роботи визначається тим, що їх використання дозволяє більш ефективно реалізувати технологію забезпечення надійності зберігання інформації широкого кола користувачів на віддалених сховищах. Розроблені в роботі методи дозволяють адаптувати технологію резервування та відновлення постійно чи тимчасово втрачених даних до конкретних вимог користувача та особливостей організації віддаленого зберігання інформації. Зокрема, відповідно до вимог користувача, можуть налаштовуватися часові характеристики процесу відновлення втрачених даних.

Використання результатів роботи при резервуванні та відновленні втрачених чи затриманих інформаційних пакетів в глобальних мережах дозволяє прискорити доставку даних. Це має велике практичне значення для систем моніторингу стану віддалених об'єктів та комп'ютерного управління

ними в реальному часі, які використовують глобальні мережі в якості середовища передачі даних.

Особистий внесок здобувача полягає в теоретичному обґрунтуванні одержаних результатів, експериментальній їх перевірці та дослідженні, а також в створенні програмних продуктів для практичного використання одержаних результатів.

Всі результати, що наведені в дисертації отримані автором самостійно. У роботах, що написані в співавторстві, автору належать: [1] – вдосконалення методу відновлення затриманих при передачі інформаційних пакетів даних, за рахунок використання системи пріоритетів при виборі компонентів матриці формування резервних пакетів; [2] – метод відновлення інформації при втраті доступу до одного сховища, а також трьох блоків, які зберігаються на різних сховищах; [3] – спосіб відновлення втрачених інформаційних блоків на основі попередньо створених таблиць специфікацій, [4] – обґрунтування вибору критеріїв ефективності резервування даних та порівняльний аналіз, з позиції обраних критеріїв, відновлення даних з використанням резервування та корегуючих кодів; [5] – спосіб використання попередньо створених таблиць специфікацій для ефективного відновлення втраченої інформації; [6] – порівняльний аналіз відновлюючих та корегуючих кодів; [7] – підхід до відновлення всіх блоків даних користувача, що зберігаються на одному сховищі; [8] – метод прискорення відновлення втраченої при віддаленому зберіганні інформації за рахунок розрідження матриці формування резервних блоків даних.

Дисертаційна робота виконана на кафедрі системного програмування і спеціалізованих комп'ютерних систем КПП ім. Ігоря Сікорського.

Науковий керівник доктор технічних наук, професор Романкевич О.М.

Апробація результатів дисертації. Основні результати дисертації доповідались та обговорювались на 6 науково-технічних конференціях, в тому числі двох міжнародних.

1. International Conference of World Scientific and Engineering Academy and Society - Mathematics and Computers in Sciences and Industry. Aug. 24-26, 2019, Corfu Island, Greece.
2. III-й Міжнародній науково-практичній конференції «Проблеми інформатики та комп'ютерної техніки» (ПІКТ – 2013), 27-31 травня 2013р., Чернівці.
3. III-й Українській конференції з автоматичного керування "Автоматика-96". 12-16 травня 1996 р., м. Севастополь.
4. Науково-технічній конференції молодих вчених "Актуальные проблемы в области радиоэлектроники, автоматики, вычислительной техники, энергетики, машиностроения и промышленных технологий", 24-26 жовтня 1988 р., м. Київ.
5. Всеукраїнській науково-практичній конференції "Передача и обработка данных в системах управления и сетях". 7-9 лютого 1989 р., м. Київ.
6. VI Координаційній нараді "Развитие методов проектирования и изготовления интегральных запоминающих устройств", 2-3 лютого 1988 р., м. Київ.

Публікації. Основні положення дисертаційної роботи опубліковані в 9 наукових працях, серед яких 8 статей у наукових фахових виданнях (в тому числі одна стаття, яка реферується міжнародними наукометричними базами даних ISI Thomson's Scientific and Technical Proceedings, ISTEP/ISI Proceedings, EI's Engineering Information Index, EI Compendex, DBLP, ACM, SCOPUS, Google Scholar та IEEE Xplore), 7 статей, що входять до наукометричної бази даних РІНЦ та тези доповідей на конференціях.

Структура та об'єм роботи. Дисертаційна робота складається з вступу, чотирьох розділів, висновків та додатків. Загальний обсяг роботи складає 141 сторінку, робота містить 4 рисунки, 11 таблиць та список використаної літератури із 78 найменувань, 2 додатки.

Р О З Д І Л 1

АНАЛІЗ ПРОБЛЕМИ ЕФЕКТИВНОГО ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ ПРИ ЇХ ВІДДАЛЕНОМУ ЗБЕРІГАННІ ТА ПЕРЕДАЧІ ПО ГЛОБАЛЬНИМ МЕРЕЖАМ

Динамічний розвиток розподілених систем обробки та зберігання даних неможливий без ефективного вирішення ряду наукових задач, чільне місце серед яких посідає забезпечення надійності та безперебійності доступу до віддаленої інформації користувачів. За умови швидкого зростання об'ємів такої інформації і розширення кола користувачів технологій віддаленого зберігання даних набуває ваги задача підвищення ефективності методів та засобів резервування та відновлення інформації в рамках таких технологій [1]. Це вимагає постійного пошуку нових підходів, методів та розробки засобів забезпечення неперервності доступу до даних шляхом їх відновлення з використанням резервної інформації.

В цьому ракурсі резервування та відновлення втрачених даних відіграють важливу роль в технології забезпечення високої надійності розподіленого зберігання інформації користувачів. Відповідно, подальший розвиток технологій віддаленого зберігання даних диктує необхідність адекватного вдосконалення методів їх резервування та відновлення втраченої інформації.

Необхідним елементом досліджень, направлених на вдосконалення і розвиток технологій відновлення втрачених при віддаленому зберіганні і передачі по глобальним мережам даних є аналіз сучасного та перспективного стану технологій розподіленого віддаленого зберігання інформації і транспортування пакетів даних по глобальним мережам, обґрунтування критеріїв ефективності їх відновлення в разі втрати даних, огляд, з позицій визначених критеріїв, існуючих методів резервування та відновлення втрачених даних, виявлення можливостей підвищення їх

ефективності, а також визначення напрямків досліджень по реалізації цих можливостей.

1.1 Аналіз проблеми надійності віддаленого зберігання даних в розподілених системах

Досягнутий в останнє десятиліття прогрес глобальних мереж кардинально змінив організацію комп'ютерної обробки інформації на користь розподілених систем зберігання даних та віддалених обчислень. Широкого розповсюдження набула практика розподіленого зберігання інформації користувачів на віддалених сховищах [2]. Крім таких очевидних переваг, як практичну відсутність обмежень на об'єм пам'яті, доступність інформації користувача для широкого кола інших користувачів, зручність обміну даними, сучасна технологія зберігання інформації в хмарах забезпечує якісно більш високий рівень надійності. Схематично, основні переваги віддаленого зберігання даних показані на рис.1.1.



Рис.1.1 Основні переваги віддаленого зберігання даних

Дані користувачів, які зберігаються на власних обчислювальних платформах чи на віддалених сховищах можуть бути втрачені в результаті дії чинників, які схематично показані на рис.1.2.

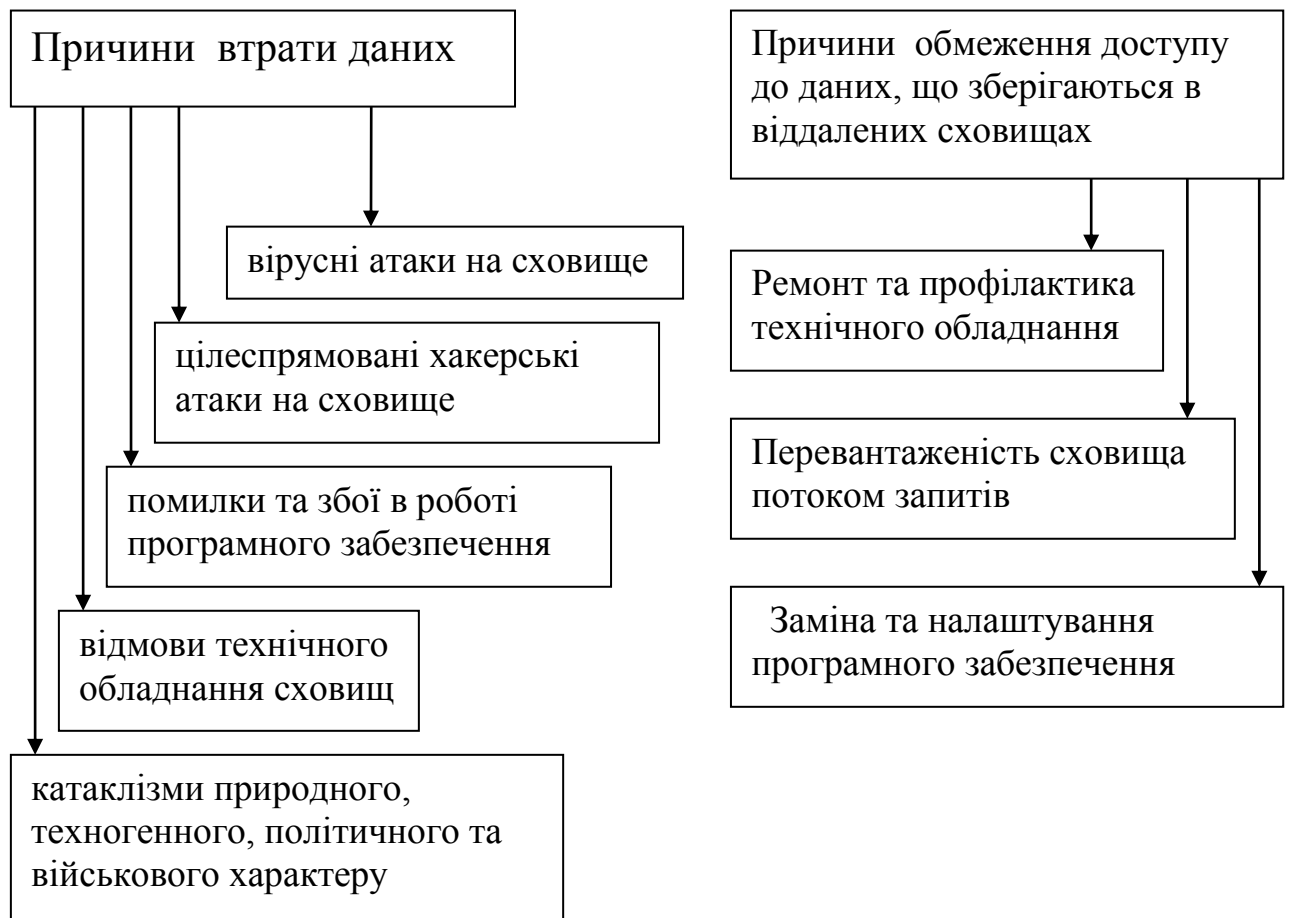


Рис.1.2. Причини втрати інформації при її віддаленому зберіганні

Втрата даних при їх зберіганні на магнітних, оптичних чи твердотільних (флеш-пам'ять) накопичувачах може відбуватися в результаті виходу з ладу обладнання, помилок в роботі програмного забезпечення, хакерських атак, дій вірусних програм, комп'ютерних хробаків, катаклізмів політичного, терористичного, природного, військового чи техногенного характеру [3].

При цьому можуть втрачатися як окремі блоки даних, так і всі інформація на певному сховищі. При зберіганні даних користувачів хмарі, основну роль в забезпеченні надійності відіграє рознесення даних користувача по різним, географічно віддаленим, сховищам [4]. Це обмежує втрати даних під дією наведених вище причин, відносно невеликим об'ємом.

Крім втрат даних, вони можуть бути тимчасово недоступними для користувача по причинах виходу з ладу обладнання, проведення профілактичних робіт, перевантаження сховища чи мережі.

Незважаючи на не це, об'єктивно спостерігається стійка динаміка розширення кола користувачів, які зберігають свої дані на віддалених сховищах. віддалене зберігання даних забезпечує вищу надійність збереженості даних [5].

Зростаюче розповсюдження віддаленого зберігання даних широкими колами користувачів в рамках хмарних технологій зумовлене меншою ймовірністю втрати інформації, наявністю значних за обсягом ресурсів пам'яті, простотою обміну та розповсюдження даних. Підвищення надійності зберігання інформації зумовлене, головним чином, за рахунок розподілення даних по різних сховищах: наведені вище причини втрати не можуть одночасно реалізуватися на географічно рознесених вузлах і саме це обмежує об'єм втраченої інформації, яка може бути відновлена за рахунок резервування [6].

В рамках окремого вузла організовано розподілення даних по носіях, доступ користувачів до даних, їх захист, резервування в разі втрати доступу до одного або декількох носіїв.

Очевидно, що резервування на рівні одного вузла практично не дозволяє зменшити ймовірність втрат інформації, викликаних катаклізмами, хакерськими атаками та збоями в роботі програмного забезпечення.

Сьогодні потужний прогрес Інтернету надав можливість здійснювати резервування на рівні користувача або групи користувачів. При цьому повною мірою можна задіяти можливості рознесеності зберігання інформації для локалізації її можливих втрат. Тільки цей чинник здатен реально забезпечити захист даних від втрат внаслідок катаклізмів. Проте рознесення зберігання даних користувача негативно впливає на швидкість доступу до даних – їх потрібно зібрати з різних сховищ [7].

Тому для підвищення надійності зберігання даних користувачів з урахуванням їх специфічних вимог, резервування має здійснюватися на рівні, вищому ніж рівень окремого вузла [8].

На рис 1.3. схематично показано критерії ефективності резервування та відновлення даних при їх віддаленому зберіганні.

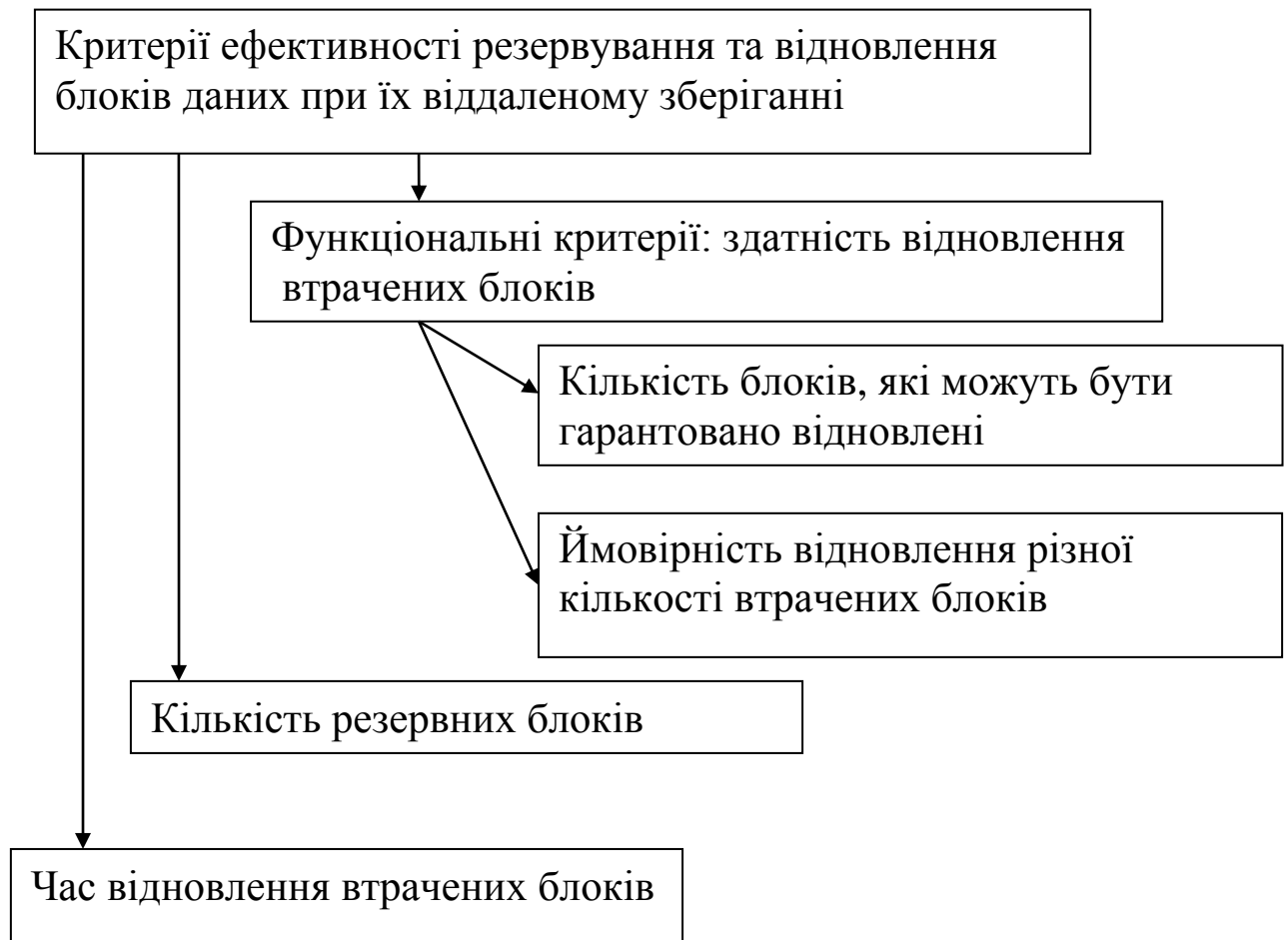


Рис.1.3 Критерії ефективності засобів резервування та відновлення даних при їх віддаленому зберіганні.

Наведені на рис.1.3 критерії протирічають одне одному, тому ефективність визначається ступенем вирішення компромісу між цими критеріями в залежності від важливості кожного критерію, яка, в свою чергу, визначається конкретикою застосування.

Для визначення цілі дослідження потрібно коротко охарактеризувати існуючі системи резервування та відновлення даних.

Для сучасних систем зберігання інформації характерним є багаторівнева організація засобів забезпечення надійності. Зокрема, якщо дані зберігаються на магнітних чи оптичних дисках, то перший рівень утворюють корегуючі коди (error correcting code – ECC) кожного з секторів [9]. За діючими стандартами [10] – це чотири контрольні байти, які додаються до 512 інформаційних байтів сектору і з їх допомогою можна локалізувати та виправити довільні два байти з 512 інформаційних байтів сектору.

Перший рівень в забезпеченні надійності зберігання даних утворюють засоби, що функціонують на рівні секторів магнітних чи оптичних носіїв. В процесі їх форматування здійснюється контрольне зчитування інформації з них: при виявленні двох чи більше спотворених байтів, сектор позначається як дефектний і запис на нього інформації блокується. Крім того, кожен сектор включає, крім 512-ти інформаційних, 4 резервних байти, які являють собою контрольні символи коду Ріда-Соломона [11] і, відповідно, забезпечують можливість виправлення двох байтів або виявлення факту спотворення більшої кількості байтів. Тобто, на першому рівні використовуються класичні корегуючі коди [12], які передбачають реалізацію двох фаз виправлення даних: локалізацію спотворених символів та їх відновлення.

В сховищах віддаленого зберігання даних користувачів, другий рівень в забезпеченні надійності утворюють резервні накопичувачі. Найбільш розвинутою технологією цього рівня є широко відома RAID (Redundant Array of Independent Disks) [13].

Спочатку система RAID була створена для прискорення роботи з недорогими дисковими пристроями. Відповідно, аббревіатура RAID утворювалася від - “Redundant Array of Inexpensive Disks” (надлишковий масив недорогих дисків) [14]. Типовим представником цього першого покоління став RAID-0, в якому використовується n накопичувачів, які працюють паралельно. Інформаційний файл розділяється на блоки, які

записуються одночасно на всі n накопичувачів. Аналогічним чином здійснює читання інформації: з n одночасно зчитуються блоки, які компонуються в файл даних. Використання RAID-0 дозволяє прискорити роботу з дисковими накопичувачами приблизно в n раз [15].

З часом технологія RAID стала розвиватися в напрямку підвищення надійності зберігання даних на накопичувачів і аббревіатура RAID стала розумітися як скорочення від “Redundant Array of Independent Disks”. Першим зразком такої концепції стала система RAID-1, в якому однакова інформація записується одночасно на два, чи більшу кількість дисків. Тобто, RAID-1 – система дзеркального резервування з повним дублюванням даних. Така система забезпечує максимальну швидкість відновлення даних з втраченого накопичувача.

Система RAID-2 реалізує відновлення даних з одного накопичувача з використанням кодів Хемінга [16]. Відповідно, при збереженні інформації на n накопичувачах формуються контролі коди Хемінга, які зберігаються на $\lceil \log_2 n \rceil$ резервних накопичувачах. Це дозволяє відновити дані з будь-якого одного накопичувача. Крім того, система RAID-2, подібно до RAID-0 здійснює одночасне звернення (для запису чи читання) до n накопичувачів, що забезпечує прискорення роботи з дисковими накопичувачами. Певний недолік системи RAID-2 полягає в тому, що прийнятний для практики рівень надлишковості досягається лише при великих значеннях n . Система RAID-2 за своїми функціональними можливостями є корегуючою, тобто вона дозволяє корегувати велику кількість байтів за умови, що пошкоджено не більше одного однойменного байту.

Система RAID-3 та схожа з ним RAID-4 використовує один резервний накопичувач, на якому зберігаються суми за модулем два всіх однойменних інформаційних блоків на основних накопичувачах [16]. Це дозволяє відновити дані з будь-якого одного накопичувача.

Система RAID-5 також використовує в якості резервних даних суму за модулем два однойменних блоків всіх інформаційних накопичувачів. Проте, на відміну від RAID-3 резервні блоки розміщуються не на одному накопичувачу, а на всіх $n+1$ накопичувачах. RAID-5 дозволяє відновлювати тільки один втрачений блок з однаковим номером і всі втрачені блоки на одному чи різних накопичувачах, за умови, що вони мають різні номери.

Система RAID-6 використовує два резервні блоки для відновлення двох із n інформаційних блоків. Відповідно, система потребує для своєї реалізації 2 резервних накопичувача [17]. Реально використовуються $n+2$ накопичувача з рознесенням резервних блоків по різних накопичувачам. Фактично RAID-6 гарантує відновлення 2 однойменних блоків за умови збереження інших n інформаційних та резервних блоків. Іншими словами, RAID-6 дозволяє відновлювати дані з будь-яких двох втрачених накопичувачів.

Сучасні моделі RAID виходять з того, що локалізація втраченої інформації точно відома [15]. Це визначає доцільність використання для відновлення втрачених даних максимально рознесених кодів, або MDS (Maximum Distance Separable)-кодів. Для відновлення двох чи більшої кількості втрачених блоків можуть бути використані різні різновиди MDS-кодів: коди Ріда Соломона [14], матричні коди типу EVENODD [18], RDP [19], Х-коди [20], В-коди [20], С-коди [21].

Архітектура RAID ефективна для накопичувачів на жорстких магнітних дисках. Однак для твердотільних накопичувачів, типу flash-накопичувачів ці коди не відзначаються ефективністю в силу їх надмірності. Використання твердотільних накопичувачів ставить нові вимоги до проектування кодів, здатних ефективно відновлювати дані, що зберігаються на таких накопичувачах.

На відміну від жорстких дисків, твердо тільні накопичувачі швидше втрачають здатність до зберігання даних в залежності від часу та кількості перезаписувань. Зі зростанням часу зберігання даних та кількості

перезаписувань даних суттєвим чином зростає ймовірність виникнення помилок.

Основні недоліки систем забезпечення відновлення даних в сховищах типу RAID полягають в тому, вони не захищені від катаклізмів, здатних зруйнувати всю інформацію, що зберігаються в сховищі, не дозволяють відновлювати більше двох блоків, не враховують специфічних вимог щодо надійності зберігання даних кожного з користувачів.

Вказані недоліки можуть бути подолані на третьому рівні забезпеченні надійності віддаленого зберігання даних [22], тобто на рівні користувача. Досягнутий на сьогодні прогрес технології глобальних мереж надає можливість здійснювати резервування і відновлення даних на рівні користувача або групи користувачів. При цьому повною мірою можна задіяти можливості рознесеності зберігання інформації для локалізації її можливих втрат. Тільки цей чинник здатен реально забезпечити захист даних від втрат внаслідок катаклізмів. Проте рознесення зберігання даних користувача негативно впливає на швидкість доступу до даних – їх потрібно зібрати з різних сховищ [23].

Таким чином, для підвищення надійності зберігання даних користувачів з урахуванням їх специфічних вимог, резервування має здійснюватися на рівні, вищому ніж рівень окремого сховища.

Вище зазначалося, що прийнята в системі RAID-6 орієнтація на відновлення лише двох блоків даних може вважатися прийнятною лише для середнього рівня вимог до надійності зберігання. Разом з тим, існує коло користувачів, специфіка яких висуває суттєво більш жорсткі вимоги до надійності зберігання даних. Крім того, постійно розширюється використання твердотільних накопичувачів, типу flash-накопичувачів. Ці пристрої мають значно меншу технічну надійність, яка сильно залежить від часу зберігання та кількості циклів перезапису інформації [24]. З наведеного

впливає наявність об'єктивної необхідності в розробці методів резервування, здатних відновлювати більшу ніж два втрачених блоки даних [25].

Аналіз можливостей використання згаданих вище MDS-кодів для відновлення більш ніж двох блоків даних показує, що при зі зростанням числа блоків, що можуть бути реконструювані при втратах, швидко зростає потрібна для цього кількість резервних блоків. Тому виникає потреба в розробці методу резервування, який би забезпечував вирішення задачі відновлення даних з урахуванням практики їх втрат в реальних системах віддаленого зберігання з використанням помірної кількості резервних блоків.

Найбільш дієвим чинником забезпечення надійності віддаленого зберігання інформації користувачів є її рознесення по різних сховищам. Тільки рознесене зберігання здатне обмежити втрати даних користувача при різного роду катаклізмах.

Більш ефективно використання для цієї цілі спеціальних відновлюючих кодів. Більшість таких кодів мають за основу лінійні перетворення, і це зумовлює швидке зростання кількості резервних носіїв, при збільшенні числа носіїв до яких втрачено доступ.

Загальною рисою відомих технологій відновлення даних з носіїв, до яких втрачено доступ є те, що вони реалізовані в рамках окремого вузла зберігання інформації. Це означає, що в разі втрати доступу до вузла в результаті тимчасового виходу його з ладу, перевантаження, вірусної атаки, відключення від мережі, техногенних або природних катаклізмів, відомі механізми відновлення даних або доступу до них для конкретного користувача не спрацьовують.

Таким чином, існуючі методи відновлення доступу до даних в системах їх віддаленого зберігання не гарантують вирішення цієї задачі в разі втрати доступу до вузла зберігання інформації.

Доведено також, що існуючі методи резервування даних мають високий рівень надлишковості і що число резервних носіїв може бути зменшено без втрати здатності відновлювати дані.

В роботах [26-28] запропоновано організацію резервування та відновлення даних на основі діагональних контрольних сум. Ця організація забезпечує теоретичний мінімум інформаційної надлишковості резервування. Недоліком організації є те, що вона не забезпечує можливості відновлення даних при втраті резервних блоків даних.

Динамічний прогрес систем віддаленого зберігання даних в розподілених системах ставить нові вимоги до засобів забезпечення неперервності доступу до інформації з боку користувачів. Схематично основні чинники цього процесу показані на рис.1.4.



Рис. 1.4 Основні чинники, що зумовлюють необхідність підвищення ефективності відновлення даних при їх віддаленому зберіганні

Основні резерви підвищення ефективності засобів відновлення даних, що зберігаються віддалено полягають в урахуванні особливостей реальних систем. Існуючі методи створені математиками і орієнтовані на ідеалізовану модель рознесених систем віддаленого зберігання даних. У той час як MDS-коди є оптимальними з позицій співвідношення ймовірності відновлення втрачених даних і інформаційної надлишковості, відмічається [29], що вони не забезпечують потрібної для задач практики ефективності в силу того, що не враховують показників часу відновлення даних, обмежень на розміщення блоків даних, можливість постійної зміни та корегування інформації користувачами.

Тут можна виділити три випадки [30]:

- зміна інформації в існуючих блоках ;
- видалення блоків даних;
- додавання блоків даних

При цьому не враховується що на практиці користувач постійно змінює інформацію в блоках, а також кількість самих блоків. Все це потребує значних ресурсів при використанні традиційних підходів до формування резервних кодів.

В сучасних умовах відмічається [31] зростання кількості реальних систем зберігання великих об'ємів даних на великому числі потенційно ненадійних вузлів пам'яті. До таких систем повною мірою можна віднести такі системи віддаленого зберігання даних як Facebook's codes Hadoop, Google Colossus, Microsoft Azure [32], а також системи зберігання даних на основі peer-to-peer технологій : OceanStore[33], Total Recall[34] DHash++[35]. Динамічне розширення практичного використання подібних систем диктує необхідність якісного вдосконалення технології застосування відновлюючих кодів для забезпечення високої надійності зберігання даних. До теперішнього часу, основним засобом забезпечення надійності зберігання інформації в означених вище системах було дублювання даних. Проте зі збільшенням

об'ємом інформації, що зберігається в таких системах зменшується ефективність дублювання, яке потребує значного рівня інформаційної надлишковості. Використання відновлюючих кодів забезпечує суттєво більшу надійність при меншому рівні надлишковості. До теперішнього часу використання відновлюючих кодів для подібних застосувань обмежувалося часом транспортування блоків, що використовуються для відновлення втраченої інформації. проте швидкий прогрес швидкісних характеристик глобальних мереж змінює стан речей і відкриває перспективи для нових застосувань технологіям відновлення даних.

1.2 Аналіз задач відновлення втрачених даних в глобальних мережах

Проблема надійності передачі даних в глобальних мережах посідає чільне місце в мережових технологіях від самого початку їх розвитку. Боротьба з помилками передачі даних в мережах носить динамічний характер, який визначається розвитком технологічної бази.

Ефективність спеціальних засобів гарантування безпомилкової доставки даних в мережах визначається вирішенням компромісу між показниками надійності передачі (ймовірність отримання повідомлення без помилок) і об'ємом ресурсів, що залучаються для цього (затримка доставки даних, об'єм додаткової інформації, що передається для виправлення виникаючих помилок, обчислювальна складність процедур локалізації та виправлення помилок) [36].

Відповідно до специфіки задачі та обмежень на наявні ресурси, для забезпечення надійної передачі даних в глобальних мережах застосовується широкий спектр засобів.

У сучасних мережах [37] використовується дві базові технології: повторна передача пакету при виявленні помилки передачі та виправлення

обмеженої кількості помилок з використанням корегуючих кодів, які локалізують та виправляють спотворені символи пакету.

Технологія повторної передачі (Automatic Repeat Request – ARQ) – це метод забезпечення надійності транспортування даних, який передбачає повторну передачу за відсутністю через певний проміжок часу підтвердження приймача про безпомилковий прийом пакету [38].

На практиці використовуються три протоколи реалізації ARQ:

Існує декілька варіантів реалізації механізму ARQ. Підтвердження правильності того, що пакет прийнято правильно може здійснюватися спеціальним пакетом, або вставкою спеціальної групи бітів в інформаційний пакет, що передається в зворотному напрямку в межах протоколів дуплексного обміну даними. На практиці використовується два різновиди підтвердження: позитивне (ACK) та негативне (NACK). Сторона, що здійснює передачу інформації (центр комутації пакетів), не отримавши на проміжку заданого інтервалу часу сигналу підтвердження (ACK) коректного отримання сигналу щодо того, що пакет не отримано (NACK) здійснює повторну передачу пакету. Для цього всі відправлені пакети протягом певного проміжку часу мають зберігатися в пам'яті центра комутації.

Діючими протоколами передбачено три способи реакції на сигнали підтвердження:

- Стартстопний (SAW — *Stop And Wait*), який передбачає послідовну передачу пакету, після кожного з яких очікується на інформацію про підтвердження прийому. Якщо поступить сигнал NACK, або буде вичерпано заданий інтервал часу, центр комутації здійснює повторну передачу пакету. Цей протокол ефективний при напівдуплексній передачі інформації, коли передачі передаючої та приймаючої сторін передуються. Проте цей метод втрачає ефективність в умовах повно дуплексного зв'язку, особливо, якщо час розповсюдження сигналу по каналу помітним чином більший за час передачі пакету, що є типовим для супутникових каналів.

- З поверненням на N кадрів (GBN – Go Back N), який називається потоковим контролем передачі. Протоколи сімейства TCP широко використовують цей протокол для передачі даних по IP, який не забезпечує повної гарантії доставки пакетів.
- Селективного (виборочного) повтору (SR – Selective Repeat). Цей метод активно використовується для передачі даних в локальних мережах з високим рівнем зовнішніх завад.

В цілому, ARQ підходить, якщо канал зв'язку має різну або невідому ємність, як це має місце в Інтернеті. Однак ARQ вимагає наявності зворотного каналу, призводить до можливого збільшення затримки внаслідок повторних передач, а також вимагає обслуговування буферів і таймерів для повторних передач, що у випадку перевантаження мережі може спричинити навантаження на сервер і загальну пропускну здатність мережі [39]. Наприклад, ARQ використовується на короткохвильових радіоканалах у вигляді ARQ-E або поєднується з мультиплексуванням як ARQ-M.

З огляду на застосування глобальних мереж в якості середовища обміну даними в системах комп'ютерного управління реального часу, технологія ARQ має суттєвий недолік – вона спричиняє суттєві затримки передачі даних [40].

Швидкий прогрес технології глобальних мереж спричиняє динамічне розширення її застосування: Інтернет витісняє традиційні технології: телебачення та телефонію, а з появою портативних радіомодемів він активно використовується в системах дистанційного моніторингу стану об'єктів реального світу та управління ними в реальному часі. Це суттєвим чином підвищує рівень вимог до оперативності та надійності доставки даних в глобальних мережах [41].

В таких мережах транспортування пакетів даних здійснюється за різними маршрутами. При цьому існує можливість їх затримок внаслідок щільного трафіку, втрат при використанні peer-to-peer мережових технологій

[42] або виникнення помилок передачі в ефірних каналах. Все це, з огляду на специфіку нових сфер застосування Інтернету, диктує необхідність застосування спеціальних засобів забезпечення оперативності та надійності доставки пакетів даних. Один з напрямків вирішення цієї нагальної проблеми полягає в формуванні та передачі резервних пакетів, які можуть бути використані для швидкого відновлення втрачених чи затриманих понад критичний час інформаційних пакетів.

Структурно виправлення помилок може здійснюватися на рівні окремих символів кожного пакету, або ж цілих пакетів [43] з використанням резервних пакетів. В останньому варіанті процедура обробки помилок здійснюється на кінцевій точці доставки пакетів.

Основний недолік здійснення виправлення помилок на рівні окремих символів полягає в тому, що експоненційне зростання обчислювальної складності процедур локалізації і виправлення спотворених символів при збільшенні їх кількості, суттєво обмежує корегуючу здатність. У сучасних умовах збільшення питомої ваги ефірних каналів передачі даних в мережах зросла ймовірність помилок передачі, зумовлена впливом зовнішніх електромагнітних завад. Причому, тривалість дії завади значно перевищує час передачі одного символу. Це має наслідком те, що домінуючим типом помилок стають групи суміжних спотворених символів, виправлення яких за допомогою корегуючих кодів Ріда-Соломона потребує значних часових і обчислювальних ресурсів [44].

До того ж технології виправлення помилок на рівні символів не дозволяють відновлювати пакети, що були втрачені в процесі передачі.

Тому в останні роки більше уваги приділяється методам підвищення надійності, що працюють на рівні пакетів [45]. Переважна більшість цих методів базується на використанні відновлюючих кодів (erasures-кодів) [46-47]. Крім глобальних мереж, такі коди широко використовуються також в системах розподіленого віддаленого зберігання інформації [48]. На відміну

від корегуючих кодів, відновлюючі коди не вирішують задачу виявлення пошкоджених при передачі пакетів: це виконується за рахунок вбудованих в пакети CRC-кодів. Для відновлення пошкоджених або втрачених пакетів додатково по мережі передаються резервні пакети, які частково акумулюють в собі інформацію, що міститься в основних пакетах. Задача відновлюючих кодів полягає в реконструкції втрачених або пошкоджених при передачі пакетів на основі інформації, що міститься в резервних пакетах.

Переважна більшість відновлюючих кодів для формування резервних пакетів використовують лінійні операції (LT-кодування). Це забезпечує швидку та ефективну обчислювальну реалізацію процесу відновлення. Найбільш відомим типом відновлюючих кодів є Raptor [50], який дозволяє відновлювати довільну кількість втрачених пакетів з n переданих. Така висока здатність до відновлення даних досягається за рахунок високого рівня надлишковості – більшого ніж 100%.

Основна відмінність існуючих лінійних відновлюючих кодів полягає в способі формування резервних пакетів. У найпростішому випадку це просте дублювання основних пакетів [50] – яке дозволяє гранично спростити процедури формування резервних пакетів та відновлення втрачених або пошкоджених пакетів.

У більшості існуючих відновлюючих кодів формування резервних пакетів здійснюється таким чином, щоб гарантувати відновлення заданої кількості втрачених пакетів [50]. Такий підхід виправданий для відновлення інформації, що зберігається в розподіленій пам'яті на віддалених носіях.

Наприклад, якщо інформаційна посилка складається з 3-х пакетів, то для гарантування їх відновлення потрібно сформувати і пересилати п'ять резервних пакетів. Але вже при трьох резервних пакетах, за умови раціонального їх формування, ймовірність відновлення основних пакетів при втраті трьох із 6-ти складає 0.93, а ймовірності відновлення основного пакету при втраті одного або двох пакетів дорівнює одиниці. Це свідчить про те, що

в існуючих відновлюючих кодах, які орієнтуються на гарантоване відновлення певної кількості втрачених пакетів, не досягається висока ефективність резервування. Так, якщо при оцінці ефективності вважати за ресурси лише кількість резервних пакетів, які додатково передаються по мережах, то ефективність використання трьох пакетів на 34% вища в порівнянні з використанням п'яти резервних пакетів [61].

Динамічний прогрес засобів передачі інформації та мережевих технологій визначає швидкий розвиток засобів виявлення, локалізації та виправлення помилок передачі даних. Основна особливість задачі нейтралізації помилок передачі в глобальних мережах полягає в багаторівневому характері її вирішення [51]: як правило, виявлення помилок здійснюється на внутрішньопакетному рівні, на цьому ж рівні при обмеженій кратності помилок може здійснюватися їх локалізація [14] та виправлення. При більшій кратності помилок, яке не може бути виправлено внутрішньопакетною на здійснюється повторна передача пакету [39], що суттєво збільшує час доставки інформації. Тому в сучасних глобальних мережах активно використовується виправлення помилок передачі даних на рівні пакетів [52], тобто корегуються не окремі біти чи символи пакету, а відновлюється весь пакет [53]. Використання такого підходу дозволяє також вирішувати задачі відновлення втрачених або затриманих понад встановлений часовий ліміт пакетів.

Використання класичних корегуючих кодів [14] які орієнтовані на комплексне вирішення задачі локалізації та виправлення помилок, на рівні пакетів, неефективне в силу того, що задачу локалізації помилок не потрібно вирішувати.

До теперішнього часу запропоновано ряд способів [48-50] формування резервних пакетів і відновлення за їх допомогою втрачених інформаційних пакетів. В більшості робіт ця задача вирішується з позицій використання мінімальної кількості резервних пакетів. Відповідно, для цього

використовуються нелінійні, зокрема, циклічні коди [53, 55]. Проте використання таких відновлюючих кодів потребує значних обчислювальних ресурсів для відновлення втрачених пакетів, об'єм яких експоненційно зростає з кількістю втрачених інформаційних пакетів. Фактично, для відновлення пакетів в тій чи іншій формі потрібно вирішувати систему рівнянь. При використанні нелінійних відновлюючих кодів, відповідно, потрібно вирішувати нелінійну систему рівнянь, яке може виконане лише методом перебору. Це прийнятне лише при невеликій розмірності системи, зокрема не більшій 2-х [56]. Тому відомі методи втрачають свою ефективність при необхідності відновлювання трьох і більше втрачених пакетів. Крім того, використання нелінійних перетворень вимагає громіздких обчислень, апаратна реалізація яких потребує складних схем.

В роботі [50] для вирішення цих проблем пропонується використовувати лінійні перетворення, що дозволяє значно прискорити обчислювальну реалізацію процесу відновлення втрачених пакетів, а також спростити схему при апаратній реалізації. Проте запропонована в [50] схема дозволяє відновлювати лише частину втрачених пакетів. Тобто в цій схемі існують варіанти втрати резервних та основних пакетів не можуть бути відновлені. іншими словами, схема [50] реалізує ймовірнісне відновлення втрачених пакетів.

На основі проведеного огляду та аналізу літературних джерел можна зробити наступні висновки. Створені до теперішнього часу методи реконструювання втрачених інформаційних пакетів з використанням резервних не забезпечують прийнятною для широкого кола практичних застосувань швидкості обчислювальної реалізації, що не дозволяє реалізувати відновлення втраченої інформації в реальному часі.

Основним резервом прискорення швидкості відновлення втрачених пакетів є використання простих в реалізації лінійних булевих перетворень

вкупі з оптимізаційним вибором для багатоваріантних процедур реконструювання.

1.3 Огляд технологій відновлення втрачених даних

В основі значної частини існуючих засобів відновлення втрачених даних, як зазначалося вище, лежить використання MDS-кодів. При використанні в якості відновлюючих кодів MDS-кодів в розподілених системах зберігання даних досягається теоретично максимальна ймовірність відновлення даних при заданій надлишковості пам'яті [56].

Фактично, MDS-коди лежать в основі будь-якого з відмостійких блочних кодів. Блочний код здійснює відображення k -бітового інформаційного блоку в n -бітове кодове слово, $n > k$ з використанням $n-k$ надлишкових бітів. Блокові коди називаються лінійними, якщо сума за модулем 2 довільної підмножини кодових слів відноситься до множини кодових слів [66].

Кодова відстань, як число бітів, в яких відрізняються кодові слова визначається мінімальною вагою Хемінга утворюючої матриці блокового коду. Наприклад, якщо утворююча матриця G ($n=6, k=3$) має вигляд

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \quad (1.1)$$

то кодова відстань між кодовими словами дорівнює трьом.

Кодування інформаційного слова, заданого бінарним вектором $a = \{a_0, a_1, \dots, a_k\}$ зводиться до множення його на утворюючу матрицю G лінійного коду: $\bar{b} = \bar{a} \cdot G$, в результаті чого утворюється n -бітовий вектор $\bar{b} = \{b_0, b_1, \dots, b_n\}$, в якому до інформаційного слова додаються контрольні біти. Наприклад, при використанні утворюючої матриці G (1.1) інформаційне слово $a = 101$ кодується кодовим словом $b = 101\ 101$.

Для декодування блокових лінійних кодів формується перевірна матриця H . Ця матриця формується у вигляді: $H = [P^T: I_{n-k}]$, де I_{n-k} –

одинична матриця розмірністю $n-k$, P^T – транспонована підматриця P матриці $G = \begin{bmatrix} I_k & P_{n-k} \end{bmatrix}$. Для наведеної вище утворюючої утворюючої матриці G (1.1) підматриці P та P^T мають наступний вигляд:

$$P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad P^T = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Відповідно, перевірна матриця H має наступний вигляд:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Рядки перевірочної матриці H ортогональні рядкам утворюючої матриці G . Це означає, що для матриць G і H виконується наступна умова [66]:

$$G \cdot H^T = 0 \quad (1.2)$$

З умови (1.2) ортогональності утворюючої та перевірочної матриць лінійних кодів випливає, що кожне кодове слово b , яке утворене в результаті добутку $a \cdot G$ також задовольняє умові ортогональності: $\bar{b} \cdot H^T = \bar{a} \cdot G \cdot H^T = 0$. При спотворенні кодового слова в процесі зберігання або передачі, до нього додається вектор помилки $\bar{e} = \{e_1, e_2, \dots, e_n\}$: $\bar{c} = \bar{b} \oplus \bar{e}$. В процесі декодування коду c здійснюється обчислення синдрому $S = \{s_1, s_2, \dots, s_{n-k}\}$ у вигляді добутку $S = c \cdot H^T$. Код синдрому S залежить тільки від вектору помилки: $S = c \cdot H^T = (e \oplus b) \cdot H^T = e \cdot H^T \oplus b \cdot H^T = e \cdot H^T$. Відповідно, якщо код синдрому S складається з нульових компонентів, то код c належить множині дозволених кодових слів. Якщо синдром не дорівнює нулю, то він несе в собі інформацію про вектор помилки. Наприклад, якщо кодове слово $b = 101 \ 101$, а вектор помилки $e = 010 \ 000$, то $c = 111 \ 101$. Синдром S , обчислений як добуток $c \cdot H^T$ дорівнює $e \cdot H^T$ і має вигляд: 010 . Кожний із можливих кодів синдромів однозначно співставляється коду помилки, який, в свою чергу, однозначно визначає локацію спотвореного символу в кодовій комбінації. В таблиці 1.1 наведено,

в якості прикладу, таблицю синдромів для виправлення однократних помилок з використанням утворюючої матриці G (1.1).

Таблиця 1.1.

Приклад таблиці синдромів для виправлення однократних помилок

Вектор помилки	100000	010000	001000	000100	000010	000001
Код синдрому	100	010	001	011	111	110

Технологічно, декодування полягає і створенні, з використанням транспонованої перевірконої матриці, таблиці синдромів. Для кожного прийнятого коду здійснюється обчислення синдрому шляхом його множення на транспоновану перевірочну матрицю. По обчисленому таким чином синдрому по таблиці синдромів знаходиться вектор помилки. До останнього логічно додається прийнятий код, в результаті чого отримується скорегований код.

В практиці виправлення помилок з використанням завадостійкого кодування часто використовуються стандартні таблиці розташування. Використання цих попередньо створених таблиць дозволяє прискорити безпосередній процес відновлення спотворених символів повідомлень за рахунок перед обчислень. Відповідно, відомі технології відновлення втрачених даних на основі корегуючих кодів допускають можливість попереднього обчислення відновленого коду для всіх можливих спотворень блоку даних. Ці обчислення, за звичай, оформлюються у вигляді стандартної таблиці розташування [64, 65].

Якщо V – це лінійний (n, k) - код, v_0 - нулевий вектор, а v_1, v_2, \dots, v_{m-1} – інші кодові вектори, де $m=2^k$, то в стандартній таблиці декодування кодові вектори організуються наступним чином. Перший рядок таблиці містить в першій колонці нулевий вектор v_0 . Під вектором v_0 в таблиці поміщаються вектори, в які трансформується нульовий вектор в процесі передачі при заданій кратності помилок. Ці вектори можна позначити через q_1, q_2, \dots, q_t , де $t=2^{n-k}-1$. Відповідно, в першому рядку стандартної таблиці поміщаються вектори v_1, v_2, \dots, v_{m-1} . Заповнення всіх інших рядків стандартної таблиці

описується наступним чином: кожен елемент таблиці $\beta_{i,j}$, що знаходиться в i -тому рядку на j -тій позиції ($i \in \{2,3,\dots,t\}$, $j \in \{2,3,\dots,m-1\}$) обчислюється у вигляді суми за модулем два коду q_i , що знаходиться в першому стовпці i -го рядка стандартної матриці та коду v_j , що знаходиться на j -тій позиції першого рядка стандартної матриці: $\beta_{i,j} = q_i \oplus v_j$. Фактично, описана стандартна таблиця повною мірою співпадає з таблицею декодування; відповідно, оскільки лінійний код V являє собою підгрупу групи $(B^n, +)$, то наведене розкладення являє собою розкладення групи B^n по підгрупі V . При цьому стандартна таблиця містить в собі значення всіх можливих кодів розрядністю n . Рядки стандартної таблиці є суміжними класами, а вектори в першому стовпці таблиці – утворюючими векторами суміжних класів. Відповідно, таблиця стандартного розташування може бути представлена у наступному вигляді:

$$\begin{array}{cccccc}
 v_0 & v_1 & \cdots & v_{m-2} & v_{m-1} \\
 q_1 & q_1 \oplus v_1 & \cdots & q_1 \oplus v_{m-2} & q_1 \oplus v_{m-1} \\
 & & \vdots & & \\
 q_t & q_t \oplus v_1 & \cdots & q_t \oplus v_{m-1} & q_t \oplus v_m
 \end{array}$$

Якщо таблиця стандартного розташування використовується якості таблиці прискореного декодування, то прийнятий вектор, який знаходиться в j -тому рядку таблиці декодується в кодовий вектор q_j – тобто елемент першого стовпця цього рядка.

Наприклад, якщо утворююча матриця G ($n=6$, $k=3$) має вигляд

$$G = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{vmatrix}$$

то множина коректних векторів $V = \{ 000\ 000, 100\ 011, 010\ 101, 001\ 110, 110\ 110, 101\ 101, 011\ 011, 111\ 000 \}$. Відповідно, таблиця стандартного розташування має такий вигляд:

000000	100011	010101	001110	110110	101101	011011	111000
100000	000011	110101	101110	010110	001101	111011	011000
010000	110011	000101	011110	100110	111101	001011	101000
001000	101011	011101	000110	111110	100101	010011	110000
000100	100111	010001	001010	110010	101001	011111	111100
000010	100001	010111	001100	110100	101111	011001	111010
000001	100010	010100	001101	110111	101100	011010	111001

Основна відмінність технологій відновлення даних, які втрачені в процесі віддаленого зберігання чи передачі по глобальним мережах від тих, які застосовуються при корекції даних з застосуванням завадостійких кодів полягає в тому, що розв'язання лінійного рівняння безпосередньо не відновлює дані, а лише задає математично процедуру реконструювання даних. Сам процес відновлення передбачає транспортування по мережі блоків даних, потрібних для реконструювання втрачених блоків, їх буферизацію і виконання обчислювальних операцій по безпосередньому відновленню втрачених блоків [63].

Задача реконструювання блоків даних, які зберігаються на віддалених розподілених системах, не допускає подібного вирішення, оскільки при відновленні блоків, доступ до яких постійно чи тимчасово втрачено, потрібної для їх відновлення інформації ще немає: вона зберігається віддалено, як і втрачені блоки.

Висновки до розділу 1

В результаті досліджень, які складають перший розділ дисертаційної роботи і направлена на аналіз особливостей сучасного та перспективного стану технологій розподіленого віддаленого зберігання інформації та огляд, з існуючих методів резервування та відновлення втрачених даних можуть бути зроблені наступні висновки.

1. Досягнутий в останні роки прогрес технології глобальних мереж надає можливість здійснювати резервування на рівні користувача або групи

користувачів. При цьому повною мірою можна задіяти можливості рознесеності зберігання інформації для локалізації її можливих втрат. Тільки цей чинник здатен реально забезпечити захист даних від втрат внаслідок катаклізмів. Проте рознесення зберігання даних користувача негативно впливає на швидкість доступу до даних – їх потрібно зібрати з різних сховищ.

Тому для підвищення надійності зберігання даних користувачів з урахуванням їх специфічних вимог, резервування має здійснюватися на рівні, вищому ніж рівень окремого вузла.

2. Виконано аналіз сучасного стану та перспектив розвитку технологій розподіленого віддаленого зберігання інформації та транспортування пакетів даних по глобальним мережам, обрано критерії ефективності засобів резервування та відновлення втрачених даних в віддалених сховищах і при передачі по мережам. Показано, що в сучасних умовах зростає значимість часу відновлення втрачених даних. Виявлено, що дієвим резервом підвищення ефективності резервування та відновлення даних є урахування особливостей організації їх віддаленого зберігання в реальних системах.

РОЗДІЛ 2

РОЗРОБКА МЕТОДІВ ЕФЕКТИВНОГО ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ В РОЗПОДІЛЕНИХ СИСТЕМАХ ЇХ ВІДДАЛЕНОГО ЗБЕРІГАННЯ

Проведений в попередньому розділі аналіз ефективності резервування та відновлення даних в розподілених системах їх віддаленого зберігання показав, що переважна більшість отриманих до сьогоднішнього для рішень оптимізують співвідношення між лише двома чинниками: кількістю блоків даних, що можуть бути реконструювані та числом резервних блоків, що використовуються для вирішення цієї задачі [67].

Практика реального використання систем розподіленого зберігання даних показує, що в сучасних умовах їх ефективність визначається більш широким спектром показників. Зокрема, для багатьох важливих для практики застосувань, які використовують віддалене зберігання даних в хмарах, критичним чинником ефективності є висока оперативність доступу до інформації. Для таких застосувань резервування збережених даних відіграє роль засобу для прискорення доступу до них. В разі виникнення критичної затримки з доставкою блоку даних, що викликана перевантаженням відповідного вузла, профілактичними та ремонтними роботами на ньому, цей блок може бути оперативно реконструйований з використанням блоків, доступ до яких здійснюється швидко.

Проведений аналіз показує, що вагомим джерелом підвищення реальної ефективності відновлення втрачених даних може стати урахування особливостей функціонування реальних систем віддаленого зберігання даних.

Вказані чинники визначають необхідність спеціальних досліджень особливостей реальних систем віддаленого зберігання даних, які можуть бути використані для підвищення ефективності відновлення втрачених даних

і, його прискорення, а також розробки на цій основі відповідних методів, придатних для практичного застосування.

2.1 Аналіз моделей відновлення втрачених даних в системах їх віддаленого зберігання

В рамках дисертаційної роботи досліджується декілька моделей відновлення втрачених даних:

- Модель автономного резервування та відновлення блоків даних користувача, що рознесено зберігаються на віддалених сховищах.
- Модель комбінованого резервування та відновлення блоків даних користувача, які рознесено зберігаються на віддалених сховищах та системного резервування всіх блоків в рамках окремого вузла чи сховища в цілому.
- Модель резервування та відновлення даних, яка передбачає обмеження на кількість блоків користувача, що зберігаються на кожному з віддалених сховищ.
- Модель втрат та затримок передачі інформаційних пакетів користувачів в глобальних мережах.

Перші три з цих моделей відображають резервування та відновлення даних при їх розподіленому зберіганні на віддалених сховищах. Четверта модель формалізує представлення процесів відновлення даних в глобальних мережах.

В рамках першої з наведених вище моделей збереження інформації на віддалених носіях користувач зберігає на віддалених серверах n інформаційних блоків B_1, B_2, \dots, B_n . Для відновлення в разі незворотного або тимчасового доступу частини з них формується m резервних блоків R_1, R_2, \dots, R_m у вигляді лінійних перетворень над інформаційними блоками:

$$\forall l \in \{1, 2, \dots, m\} : R_l = \bigoplus_{j=1}^n a_{l,j} \cdot B_j, \quad (2.1)$$

де $a_{l,j} \in \{0,1\}$ – бінарні коефіцієнти матриці A , яка визначає порядок формування резервних блоків даних:

$$A = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \cdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{vmatrix}.$$

Сформовані інформаційні блоки R_1, R_2, \dots, R_m також зберігаються на віддалених сховищах.

В разі втрати резервних блоків, номери яких утворюють множину Ψ та h інформаційних блоків, номери яких складають множину Ω , останні можуть бути відновлені за умови наявності в матриці A ортогональної підматриці, стовпці якої належать множині Ω , а рядки, не належать множині Ψ .

Ця узагальнена умова може конкретизуватися у наступному вигляді:

1. Кожен стовпець матриці A має містити в собі не менше h одиниць. Ця визначається можливістю відновлення одного інформаційного блоку в ситуації коли $h-1$ інших втрачених блоків відносяться до категорії резервних:

$$\forall i \in \{1, 2, \dots, n\} : \sum_{j=1}^m a_{ji} \geq h. \quad (2.2)$$

2. Кожна довільна пара стовпців матриці A має відрізнятися не менш ніж в $h-1$ рядках. Іншими словами, Хемінгова відстань між будь-якою парою стовпців матриці A має бути не менше $h-1$. Це гарантує можливість відновлення довільної пари втрачених інформаційних блоків за умови, що втрачено ще $h-2$ резервних блоків. Дійсно, якщо втрачені v -тий та w -тий блоки даних, $v, w \in \{1, 2, \dots, n\}$, $v \neq w$, то при втраті $h-2$ резервних блоків, з якими, в найгіршому випадку, співвідносяться рядки матриці A , в яких v -тий та w -тий стовпці мають різні значення, то гарантовано існує j -рядок, $j \in \{1, 2, \dots, m\}$, в якому $a_{jv} \neq a_{jw}$. Без втрати узагальнення можна вважати $a_{jv}=1$, відповідно $a_{jw}=0$. Згідно з (2.3) в w -тому стовпці матриці A існує елемент $a_{yw}=1$, який асоціюється з невтраченим y -тим резервним блоком. При будь-

якому значенні a_{yv} підматриця Θ , утворена v -ти та w -тим стовпцями, а також j -тим та u -тим рядками матриці A є ортогональною, тобто надає теоретичну можливість відновлення v -того та w -того інформаційних блоків. Таким чином:

$$\forall i, j \in \{1, 2, \dots, n\} : \sum_{l=1}^m (a_{il} \oplus a_{jl}) \geq h - 2. \quad (2.3)$$

3. Кожна з $C_n^\gamma \cdot C_m^{h-\gamma} = \frac{n! \cdot (h-\gamma)! \cdot (m-h+\gamma)!}{\gamma! \cdot (n-\gamma)! \cdot m!}$ підматриць матриці A , утворених

довільним набором γ її стовпців та довільним набором $(m-h+\gamma)$ її рядків має містити в собі ортогональну підматрицю Θ , що складається з γ рядків та γ стовпців, де $2 < \gamma < h$. Цілком очевидно, що кожна із згаданих підматриць утворена з матриці A стовпцями, які співвідносяться з втраченими інформаційними блоками, а рядки – з невтраченими резервними блоками. Наявність в кожних з цих підматриць ортогональної підматриці Θ означає, що втрачені інформаційні блоки можуть бути виражені у вигляді лінійної комбінації невтрачених резервних блоків. Іншими словами, з наявності в кожній з цих підматриць ортогональної підматриці Θ гарантує можливість реконструювання γ втрачених інформаційних блоків з використанням невтрачених $(m-h+\gamma)$ резервних блоків.

4. Кожні h стовпців матриці A , мають містити в собі ортогональну підматрицю Θ , що гарантує можливість представлення втрачених інформаційних блоків через лінійні комбінації від резервних блоків, тобто відновлення блоків даних, доступ до яких постійно чи тимчасово втрачено.

Проведений аналіз показує, що втрати інформаційних блоків користувача при їх віддаленому зберіганні в першому наближенні можуть бути описані біноміальною моделлю. Ця модель розглядає події втрати пакетів як незалежні між собою. Ймовірність $p(t)$ того, що блок буде втрачено через час t визнається : $p(t) = e^{-\mu t}$, де μ - інтенсивність втрат блоків, тобто величина, зворотна до середнього часу t_c втрати блоків: $t_c = \mu^{-1}$.

Відповідно, при зберіганні q пакетів, ймовірність $P_k(t)$ того, що k з них втрачено за інтервал часу t визначається за формулою Бернуллі:

$$P_k(t) = C_q^k \cdot p^k(t) \cdot (1-p(t))^{q-k}. \quad (2.4)$$

В практичному сенсі з формули (2.4) випливає наступний порядок резервування при розподіленому зберіганні інформаційних блоків користувачів:

- 1) При необхідності розподіленого збереження n інформаційних блоків, користувач формує m резервних таким чином, щоб їх допомогою гарантовано відновлювалися не менше ніж h інформаційних блоків. Сформовані $q=m+n$ блоків розсилаються для збереження на різних серверах.
- 2) Через періодом часу τ користувач перевіряє цілісність збереження всіх q збережених блоків. Якщо w з них втрачено, $w \leq h$, то вони відновлюються з використанням резервних блоків.

Очевидно, що період τ має вибиратися таким чином, щоб за час τ ймовірність втрати більше ніж h пакетів була не більше встановленого порогового значення P_0 :

$$\sum_{k=0}^h P_k(\tau) < P_0. \quad (2.5)$$

При заданому значенню t_c та заданій ймовірності Q можливості відновлення втрачених даних з використанням формули (2.5) можна підібрати можливі значення кількості h блоків, які мають відновлюватися засобами резервування та період τ перевірки збереженості всі блоків даних користувача на віддалених носіях.

В таблиці 2.1, в якості прикладу, наведені значення параметрів h , τ та Q для значення t_c яке складає два роки тобто для ситуації коли тобто в середньому раз на два роки втрачається блок даних, який зберігається на віддаленому носіїві. З таблиці 1 можна визначити, що для заданої ймовірності $Q=0.999$ того, що дані не будуть втрачені можливими варіантами є: використання системи резервування, що здатна відновити два

блоки при періоді τ перевірки 0.37 місяця (11 днів), три блоки при періоді τ перевірки 0.88 місяці, або чотири блоки при періодичності контролю 1.6 місяці.

Таблиця 2.1

Таблиця залежності параметрів регенерації даних при кількості блоків $q=13$ і середньому часі втрати блоку – 2 роки (24 місяці)

Число h блоків, що гарантовано відновлюються	Період τ перевірки збереженості блоків (місяці)	Ймовірність Q , що втрачена інформація може бути відновлена
2	0.5	0.9973
	0.4	0.9988
	0.37	0.9990
3	2	0.9837
	1	0.9985
	0.88	0.9990
4	2	0.9975
	1	0.99985
	1.6	0.9990

З приведених досліджень можна зробити важливий практичний висновок що досягнення високих показників ефективності відновлення втрачених даних в системах їх віддаленого зберігання може бути досягнуте за рахунок комплексного застосування організаційних і технічних методів. Зокрема, показано, що для широкого класу причин втрат інформаційних блоків періодична їх регенерація дозволяє обмежити кількість втрачених блоків і, відповідно, підвищити швидкість їх відновлення.

2.2 Розробка методу прискореного відновлення втрачених при віддаленому зберіганні блоків даних

Для багатьох важливих для практики застосувань, які використовують віддалене зберігання даних в хмарах, критичним чинником ефективності є висока оперативність доступу до інформації. Для таких застосувань резервування збережених даних відіграє роль засобу для прискорення доступу до них. В разі виникнення критичної затримки з доставкою блоку даних, що викликана перевантаженням відповідного вузла, профілактичними

та ремонтними роботами на ньому, цей блок може бути оперативно реконструйований з використанням блоків, доступ до яких здійснюється швидко.

Аналогічну роль відіграє резервування і при передачі інформаційних пакетів в глобальних мережах. В разі виникнення критичної часової затримки з доставкою одного або декількох пакетів, яка викликана необхідністю повторної їх передачі між вузлами мережі, ці пакети можуть бути швидко відновлені з використанням резервних пакетів, що доставлені на пункт призначення вчасно.

Вказані чинники визначають необхідність розробки спеціальних методів до прискорення відновлення даних при їх віддаленому зберіганні та передачі по глобальними мережам. Для цього потрібно проаналізувати фактор, що впливають на швидкість відновлення даних, виявити та оцінити резерви зменшення часу їх реконструкції, розробити та дослідити методи прискорення відновлення інформації.

Для реальних систем віддаленого зберігання інформації користувачів та систем комп'ютерного управління з використанням Інтернету в якості середовища обміну даних, важливу роль відіграє час відновлення втрачених інформаційних блоків чи пакетів даних.

Крім того, механізми відновлення інформаційних блоків часто застосовуються в ситуаціях, коли виникає значна часова затримка доставки цих блоків користувачам. Затримка може бути викликана з піковими навантаженнями на сховище, на якому зберігаються затребувані користувачем блоки даних, здійсненням на ньому певних дій, пов'язаних з оптимізацією зберігання великої кількості блоків [68].

Для систем віддаленого зберігання даних час відновлення складається з двох складових: часу доставки резервних та інформаційних блоків, потрібних для процесу відновлення, та часу виконання обчислень, безпосередньо пов'язаних з реконструюванням втрачених блоків.

Якщо позначити через ε - середню кількість інформаційних блоків, з яких формується один резервний блок, тобто, середню кількість одиниць в кожному з рядків матриці A , то можна визначити кількість блоків, які потрібно доставити через глобальну мережу для реконструкції одного втраченого інформаційного блоку.

Якщо кожен з рядків матриці A містить в точності ε одиниць і при цьому забезпечується можливість гарантованого відновлення h втрачених інформаційних блоків, то, як зазначалося вище, для кожного набору з γ стовпців, де $2 < \gamma \leq h$, існує ортогональна підматриця Θ .

Оскільки в кожному рядку підматриці Θ є наявними ε одиниць, то ймовірність p_1 того, що в елемент матриці A дорівнює одиниці становить: $p_1 = \varepsilon/n$. З іншого боку, кожен рядок підматриці Θ містить в собі хоча б одну одиницю: інакше б підматриця Θ не була б ортогональною. Якщо припустити, що кількість одиниць в рядку підматриці Θ підпорядкована біноміальному закону, то середнє значення становило б $p_1 \cdot \gamma$. Проте, як зазначалося вище, кількість одиниць в рядку підматриці Θ не може дорівнювати нулю. Виходячи з цього, середня кількість ν одиниць в рядку підматриці Θ дорівнює сумі:

$$\nu = (1 - p_1)^\gamma \cdot 1 + p_1 \cdot \gamma. \quad (2.5)$$

Якщо розкласти першу складову формули (2.5) згідно біному Ньютона на адитивні складові, то ця формула може бути представлена у такому вигляді:

$$\nu = (1 - p_1 \cdot \gamma + C_\gamma^2 \cdot p_1^2 - C_\gamma^3 \cdot p_1^3 + \dots + p_1^\gamma) + p_1 \cdot \gamma \approx 1 + C_\gamma^2 \cdot p_1^2 \approx 1 + \frac{1}{2} \cdot \left(\frac{\gamma \cdot \varepsilon}{n} \right)^2. \quad (2.6)$$

В силу того, $\varepsilon \ll n$ і $\gamma \ll n$ можна вважати, що середня кількість ν одиниць в кожному з рядків підматриці Θ дорівнює одиниці. Це означає, що розв'язання системи лінійних рівнянь, яка задається підматрицею Θ , дозволяє отримати представлення втраченого інформаційного блоку у

вигляді логічної суми одного резервного блоку та $\varepsilon-1$ невтрачених блоків даних. Останні співвідносяться до $\varepsilon-1$ одиниць рядка матриці A , які не увійшли до підматриці Θ . Таким чином, для відновлення одного втраченого блоку даних потрібно доставити на обчислювальну платформу, де відбувається реконструкція, в середньому, один резервний та $\varepsilon-1$ невтрачених інформаційних блоків. Над ними потрібно виконати $\varepsilon-1$ операцій логічного додавання.

Відповідно, що середній час T_m відновлення блоку даних при зберіганні інформації в хмарах визначається формулою:

$$T_m = \varepsilon \cdot t_T + (\varepsilon - 1) \cdot t_{XOR}, \quad (2.7)$$

де t_T – час доставки блоку, що зберігаються на віддалених сховищах, t_{XOR} – час логічного додавання двох блоків; на практиці $t_{XOR} \ll t_T$.

Для систем комп'ютерного управління з обміном даними через Інтернет, час відновлення втрачених чи затриманих пакетів визначається лише часом реалізації обчислень.

При виникненні затримки в передачі одного чи декількох інформаційних пакетів, процес їх реконструкції на стороні приймача починається з моменту доставки всіх потрібних для цього ε інформаційних та резервних пакетів. При цьому середній час T_m' відновлення блоку даних при зберіганні інформації в хмарах визначається формулою:

$$T_m' = (\varepsilon - 1) \cdot t_{XOR}. \quad (2.8)$$

З формули (2.8) випливає, що найбільш дієвим шляхом прискорення процесу відновлення втрачених блоків чи недоставлених до встановленого часу пакетів, є зменшення кількості ε пакетів, з яких формується кожен з резервних блоків (пакетів). Виходячи з цього, теоретично найменший час відновлення втрачених блоків досягається при використанні простого дублювання інформаційних блоків, тобто при $\varepsilon=1$. Зразком такої концепції стала система RAID-1, в якому однакова інформація записується одночасно

на два, чи більшу кількість дисків. Тобто, RAID-1 – система дзеркального резервування з повним дублюванням даних. Така система забезпечує максимальну швидкість відновлення даних з втраченого накопичувача. Проте використання дублювання має наслідком значну надлишковість: так для гарантування відновлення h втрачених блоків від загальної кількості n блоків потрібна кількість m резервних блоків становить $m=h \cdot n$.

Тому, виникає потреба розробки технології побудови матриці A .

Для того, щоб забезпечити відновлення h інформаційних блоків, передбачається формування резервних блоків з використанням систем квазістаціонарних рекурентних функцій Галуа. Ці функції базуються на ортогональних системах функцій базису Уолша. Системи дискретних функцій Уолша являють собою системи ортонормованих прямокутних бінарних функцій. Існують різні способи впорядкування систем такого класу. При цьому з базису Уолша трансформуються в базиси Галуа чи Адамара [55]. В роботі передбачається використання систем в базисі Галуа [68].

В рамках цього відомого підходу запропонована модифікована процедура побудови матриці формування резервних блоків. Для задачі гарантованого відновлення інформаційних блоків при втраті не більше h із них потрібні прямокутні матриці, що складаються з n стовпців та m рядків.

Сутність використання систем квазістаціонарних рекурентних функцій Галуа для формування MDS кодів полягає в тому, що спочатку формується бітова послідовність $S(n)$, яка являє собою перший рядок матриці A . Наступні μ рядків матриці формуються циклічним зсувом послідовності $S(n)$.

Стартовий код $S_0 = \{s_1, s_2, \dots, s_n\}$ вибирається таким чином, щоб сума за модулем два будь-якої пари кодів, утворених циклічним зсувом коду S не співпадала ні з одним циклічно зсунутим кодом S_0 . Іншими словами, якщо позначити через U множину n -бітових кодів, утворених циклічним зсувом стартового коду S_0 : $U = \{S_0, S_1, \dots, S_{n-1}\}$, то для будь-якої пари S_i, S_j кодів, що

належать U : $S_i, S_j \in U, \forall i, j \in \{0, 1, \dots, n-1\}$ їх сума за модулем два не належить множині U : $S_i \oplus S_j \notin U$.

$$\forall S_i, S_j \in U, i, j \in \{0, 1, \dots, n-1\}: S_i \oplus S_j \notin U$$

Для вирішення цієї задачі використовується такий підхід. Якщо бінарний код S_0 містить в собі фіксовану кількість ε одиниць, то потрібно підібрати стартовий код S_0 таким чином, щоб при циклічному зсуві співпадала мінімальна кількість одиниць.

Для підвищення ефективності цієї технології пропонується використувати вектор $E = \{e_1, e_2, \dots, e_\varepsilon\}$ – вектор відстаней між позиціями одиниць в бінарному коді S_0 . Це означає, що e_1 – різниця позицій другої та першої одиниць в коді S , e_2 – різниця номерів позицій третьої та другої одиниць в коді S ,... e_ε – циклічна різниця між позиціями останньої та першої одиниць в коді S ; цілком очевидно, що $e_1 + e_2 + \dots + e_\varepsilon = n$. Кількість ε одиниць в коді S_0 визначається як арифметична сума бітів цього коду: $\varepsilon = s_1 + s_2 + \dots + s_n$.

Основна перевага використання вектора E полягає в тому, що при зсуві відносна відстань між одиницями циклічно зсувного коду S_0 не змінюється. Може змінюватися тільки відносний порядок одиниць.

Сутність використаного підходу полягає в тому, що спочатку формується бітова послідовність $S(n)$, яка являє собою перший рядок матриці A . Наступні μ рядків матриці формуються циклічним зсувом послідовності $S(n)$ за умови, що $m \leq n$.

Прикладом системи A , яка гарантує відновлення всіх інформаційних пакетів при втраті не більше 4-х з $n+k$ переданих при $n=14$ та $k=10$ є система, перший рядок якої утворений послідовністю $S(n)$, а інші рядки – циклічним зсувом вказаної послідовності.

Послідовність $S(n)$ утворюється бітами переносу зсувного 5-розрядного регістру зі лінійною функцією зворотного зв'язку LFSR (Linear Feedback Shift Register), яка забезпечує період повторення $n=14$. Якщо позначити через $R(j)$ поточний код на регістрі на j -тому кроці, а через F – код функції зворотного

зв'язку, то послідовність формування $S(n)$ може бути описана наступним чином:

$$\forall j \in \{1, 2, \dots, n\}: R(j) = R(j-1) \cdot 2 + s_j, \quad s_j = r_1(j-1) \cdot f_1 \oplus r_2(j-1) \cdot f_2 \oplus \dots \oplus r_4(j-1) \cdot f_4$$

Початкове значення $R(0) = 30_{10} = 11110$ $F = x^6 + x^5 + x^4 = 11100$

Формування послідовності ілюструється наступною таблицею 2.2.

Таблиця 2.2

Приклад формування рядків матриці А на основі LFSR

Крок j	R	$s_j = r_5 \oplus r_4 \oplus r_3$	Крок j	R	$s_j = r_5 \oplus r_4 \oplus r_3$
0	1 1 1 1 0	1	7	0 0 0 0 1	0
1	1 1 1 0 1	1	8	0 0 0 1 0	0
2	1 1 0 1 1	0	9	0 0 1 0 0	1
3	1 0 1 1 0	0	10	0 1 0 0 1	1
4	0 1 1 0 0	0	11	1 0 0 1 1	1
5	1 1 0 0 0	0	12	0 0 1 1 1	1
6	1 0 0 0 0	1	13	0 1 1 1 1	0

В таблиці 2.3 наведені значення можливих довжин циклів повторення кодів на LFSR для різних значень числа компонентів R .

Таблиця 2.3

Значення можливих довжин циклів повторення кодів на LFSR
для різних значень числа компонентів R

Число компонентів R	Довжини циклів, для яких існує лінійна функція зворотного зв'язку
4	5, 6, 7, 15
5	5, 6, 7, 8, 12, 14, 15, 21, 31
6	5, 6, 8, 9, 10, 12, 14, 15, 21, 28, 30, 31, 47

Побудована, в якості прикладу, з використанням наведено вище матриця А формування резервних блоків має наступний вигляд

$$A = \begin{vmatrix} 1011000111 \\ 0110001111 \\ 1100011110 \\ 1000111101 \\ 0001111011 \\ 0011110110 \\ 0111101100 \\ 1111011000 \\ 1110110001 \end{vmatrix}$$

В рамках цього підходу запропонована спрощена процедура побудови матриці формування резервних блоків. Для задачі гарантованого відновлення інформаційних блоків при втраті не більше h із них потрібні прямокутні матриці, що складаються з n стовпців та m рядків.

Для прискорення процесу відновлення втрачених даних за рахунок зменшення кількості інформаційних та резервних блоків, які використовуються для реконструкції втрачених блоків, пропонується модифікована процедура формування резервних блоків. Ця процедура передбачає побудову матриці A таким чином, щоб кожен її рядок містив ε одиниць, де ε - кількість блоків, які потрібно транспортувати по мережі для відновлення інформаційного блоку. При цьому з необхідністю збільшується кількість m потрібних для відновлення резервних блоків.

При малих значеннях $\varepsilon \ll n/2$, виникає ситуація коли $m > n$. В цьому вип. Якщо кількість одиниць в коді менша або дорівнює половині всіх бітів: $\varepsilon \leq 0.5 \cdot n$, то, в принципі, можлива ситуація при якій циклічно зсунутий код не матиме співпадаючих одиниць з S_0 . При $\varepsilon = 0.5 \cdot n$ така ситуація можлива, якщо інверсний до коду S_0 код S_r також належить множині U . Але цілком очевидно, що ця умова порушує умову (2), тому при $\varepsilon \geq 0.5 \cdot n$ код S_0 має хоча б одну співаючу одиниці з кодом, утвореним шляхом циклічного зсуву S_0 . Для коду S_i , утвореного циклічним зсувом стартового коду S_0 вектор E може як співпадати з відповідним вектором коду S_0 (якщо код S_i починається

серією з не менш ніж i нулів), так і бути циклічно зсунутим вектором E стартового коду.

Для будь-яких двох n -бітових кодів: S_i, S_j , які мають по ε одиниць і таких, що один із них може бути отриманим в результаті циклічного зсуву Хемінгова відстань між ними може бути отримана шляхом аналізу відповідних векторів E .

Граничні значення Хемінгової відстані між n -бітовим кодом S_0 , що має ε одиниць та будь-яким кодом $S_i, i \in \{1, 2, \dots, n-1\}$, що являє собою циклічно зсунутий код S_0 можуть бути отримані шляхом аналізу вектору E . Як зазначалося вище, ці коди, за певних, зазначених вище умов обов'язково мають мати одну співпадаючу одиницю. Якщо припустити, що перша одиниця коду S_0 співпадає з першою одиницею коду S_i , яка є j -тою одиницею в їх відліку в векторі $E, j \in \{1, 2, \dots, \varepsilon\}$, то кількість співпадаючих одиниць в кодах S_0 та S_i пропонується визначити наступним чином шляхом аналізу вектору E .

Те, що співпадають перша одиниця в коді S_0 та j -та одиниця в коді S_i означає, що наступна (друга) одиниця в коді S_0 співпадає з циклічно наступною за j -тою одиницею в коді S_i лише за умови, що компонента e_1 вектору E співпадає з e_j : $e_1 = e_j$. Якщо $e_1 \neq e_j$, то друга одиниця в коді S_0 може співпасти з третьою одиницею в коді S_i : для цього потрібно, щоб $e_1 = e_j + e_{(j+1) \bmod \varepsilon}$ або друга одиниця в коді S_i може співпасти з третьою одиницею коду S_0 : для цього потрібно, щоб виконувалася умова: $e_1 + e_2 = e_j$.

адку пропонується використовувати додаткову бітову послідовність $S'(n)$, яка утворює $(n+1)$ -й рядок матриці A , а всі інші рядки після нього утворюються циклічним зсувом послідовності $S'(n)$. Виявлені умови вибору послідовності $S'(n)$ з урахуванням першої послідовності $S'(n)$.

При заданому значенні ε та h -кількості блоків, що мають відновлюватися при втраті, число m резервних блоків визначається з формули:

$$m = \max\left\{\frac{n \cdot h}{\varepsilon}, (h-2) \cdot \lceil \log_2(n+1) \rceil + 2\right\}. \quad (2.9)$$

Наприклад, при $n=6$ та $h=3$ можна розглянути та порівняти два варіанти побудови матриці A формування резервних блоків: при $\varepsilon = 3$ і $\varepsilon=2$. В першому варіанті згідно формули (2.9) $m=6$, а в другому $m=9$. В якості стартового коду S_1 першої матриці можна вибрати $S_1 = \{1,1,0,1,0,0\}$. Для побудови матриці A при $m=9$ згідно з запропонованим методом використовується дві послідовності S_2 та S_2' , які формуються векторами $E_2=\{2,4\}$ та $E_2'=\{1,5\}$. Відповідно, стартові коди дорівнюють: $S_2 = \{1,0,1,0,0,0\}$, і $S_2' = \{1,1,0,0,0,0\}$.

Матриці A_1 (при $\varepsilon = 3$) та A_2 (при $\varepsilon=2$) формування резервних блоків мають наступний вигляд:

$$A_1 = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{vmatrix} \quad A_2 = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{vmatrix}$$

В разі втрати другого, третього та четвертого блоків, відповідні стовпці матриць A_1 та A_2 включають відповідно ортогональні підматриці Θ_1 і Θ_2 :

$$\Theta_1 = \begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix} \quad \Theta_2 = \begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix}$$

Відновлення втрачених блоків відбувається для матриці A_1 у вигляді:

$$B_2 = R_3 \oplus B_5 \oplus B_6; \quad B_3 = R_2 \oplus B_1 \oplus B_6; \quad B_4 = R_4 \oplus B_1 \oplus B_5$$

Відновлення втрачених блоків для матриці A_2 здійснюється в такій послідовності:

$$B_4 = R_2 \oplus B_6; B_3 = R_7 \oplus B_4; B_2 = R_3 \oplus B_4$$

В рамках наведеного прикладу при $\varepsilon=3$ для відновлення трьох блоків потрібно здійснити доставку 6-ти блоків та виконати 6 операцій логічного додавання блоків.

При $\varepsilon=2$ для відновлення цих же блоків потрібно доставити 4 блоки та виконати три операції логічного додавання.

Таким чином, час відновлення в другому випадку більш ніж в 1.5 рази менший, ніж при $\varepsilon=3$, за рахунок збільшення в 1.5 рази числа резервних блоків.

В загальному випадку при використанні запропонованого методу коефіцієнт ξ прискорення відновлення визначається формулою:

$$\xi = \frac{n \cdot h}{\varepsilon \cdot (h-2) \cdot \lceil \log_2(n+1) \rceil + 2}. \quad (2.10)$$

Таким чином, в результаті проведених досліджень теоретично обґрунтовано, розроблено метод прискорення відновлення втрачених інформаційних блоків при їх розподіленому зберіганні за рахунок збільшення надлишковості резервування, зменшити час доставки по глобальній мережі інформаційних та резервних блоків для реконструювання втрачених блоків, а також зменшити кількість потрібних для цього обчислювальних операцій, що забезпечує важливе для багатьох застосувань прискорення відновлення даних.

Подальший розвиток запропонованого підходу вбачається в дослідженні можливостей прискорення процесу відновлення втрачених при віддаленому зберіганні даних за рахунок оптимізації їх розміщення на віддалених сховищах за критерієм мінімізації часу доставки блоків, потрібних для реконструкції втраченої інформації користувачів.

2.3 Метод відновлення всіх блоків даних на одному сховищі та трьох блоків на різних сховищах

Для досягнення поставленої мети досліджено характер втрат доступу до блоків даних користувачів. Характер втрат даних значною мірою визначається їх причиною. Втрати даних, викликані поломками обладнання, старінням матеріалу носія, помилками в роботі програмного забезпечення найбільш точно описуються в математичному сенсі потоками Пуассона [70]. При цьому інтенсивність втрати одного блоку даних за даними Google Cloud Storage становить близько $7 \cdot 10^{-6} \text{ год}^{-1}$ [71]. Використовуючи профілактичний періодичний контроль збереженості блоків даних можна обмежити кількість втрачених блоків.

Для втрат даних користувачів, зумовлених дією зовнішніх катаклізмів та хакерських чи вірусних атак характерним є неможливість доступу до всіх даних сховища.

Таким чином, метод має гарантувати можливість реконструкції всіх блоків даних користувача, що зберігаються на одному сховищі, втрата яких зумовлена зовнішніми катаклізмами чи хакерськими атаками та відносно невелику кількість інформаційних блоків, доступ до яких втрачено з причин відмов обладнання та помилок в роботі програм.

Для досягнення поставленої розроблено метод відновлення інформаційних блоків при їх розподіленому зберіганні не більш ніж по r на кожному з віддалених сховищ, який гарантує реконструкцію всіх r блоків при втраті доступу до одного сховища, на якому вони зберігаються, а також трьох блоків, які зберігаються на різних сховищах.

В рамках дослідження розглядається така модель збереження інформації на віддалених носіях. Користувач зберігає на віддалених серверах n інформаційних блоків B_1, B_2, \dots, B_n . Для їх відновлення при формуються m резервних блоків R_1, R_2, \dots, R_m у вигляді лінійних перетворень над інформаційними блоками:

$$\forall i \in \{1, 2, \dots, m\} : R_i = \bigoplus_{j=1}^n a_{i,j} \cdot B_j,$$

де $a_{i,j} \in \{0, 1\}$ – бінарні коефіцієнти, які утворюють матрицю A і визначають спосіб формування резервних блоків даних:

$$A = \|a_{i,j}\|, i = 1, 2, \dots, m, j = 1, 2, \dots, n.$$

Для гарантування можливості відновлення не менше трьох втрачених від загального числа $q=m+n$ блоків користувача необхідним є виконання наступних умов:

1. Кожен стовпець матриці Λ має містити не менше 3-х одиниць, що гарантує відновлення одного інформаційного блоку в ситуації, коли крім нього втрачено два резервних.
2. Хемінгова відстань між будь-якими двома стовпцями матриці Λ має бути не менше двох, що гарантує відновлення пари інформаційних блоків за умови, що втрачено один із резервних блоків. Іншими словами, після втрати одного резервного блоку всі стовпці матриці Λ мають бути різними.
3. Матриця Δ , утворена будь-якими трьома стовпцями матриці Λ , має містити в собі ортогональну квадратну підматрицю Θ , що визначає можливість представлення будь-яких трьох інформаційних блоків у вигляді лінійної комбінації інших інформаційних та резервних блоків, тим самим гарантуючи відновлення будь-яких трьох втрачених інформаційних блоків.

В роботі запропоновано наступний метод побудови матриці A формування резервних блоків для відновлення трьох втрачених блоків. Метод полягає в виконанні наступної послідовності дій:

1. Обчислюється значення k кількості двійкових розрядів для кодування номеру стовпчика за умови, що їх нумерація починається з одиниці:
$$k = \lceil \log_2(n+1) \rceil$$
2. В перші k рядків кожного стовпчика матриці A записується його порядковий номер, починаючи з одиниці.

3. В $(k+1)$ -му рядку тих стовпчиків, номери яких мають парну кількість одиниць, встановлюється одиниця, а тих, що мають непарну кількість одиниць – нуль.
4. В $(k+2)$ -му рядку тих стовпчиків, номери яких мають одну одиницю, встановлюється одиниця, а тих, що мають дві і більше одиниць – нуль.

Покажемо, що матриця A побудована згідно з запропонованим методом задовольняє сформульованим вище трьома умовами.

Оскільки нумерація стовпців згідно викладеного вище починається з одиниці, що гарантує хоча б однієї одиниці в перших k рядках кожного стовпчика матриці A . У відповідності з п.4 в $(k+2)$ -му рядку тих стовпчиків, номери яких мають лише одну одиницю, встановлюється одиниця, так, що кількість одиниць у кожному стовпчику не може бути меншою за два.

Якщо Хемінгова відстань між парою номерів дорівнює одиниці, то це можливо лише за умови, що кількість одиниць в цих номерах відрізняється на одиницю, тобто один із номерів парний, а інший – непарний. Описаний вище метод передбачає додавання одиниці в $(k+1)$ -му рядку лише тих стовпців, сума одиниць в k перших позиціях парна. Це означає, що з урахуванням $(k+1)$ -х перших компонент Хемінгова відстань між будь-якою парою стовпців матриці A гарантовано не менша двох.

Будь-які три різні номери відрізняються мінімум в двох розрядах. Це означає, що серед перших k рядків матриці A , побудованою за викладеним вище методом, для будь-яких трьох стовпців є мінімум два рядки, компоненти яких не рівні між собою і ці два рядки різні.

Якщо таких рядків рівно два, то один не є інверсією іншого. В протилежному випадку існували б два однакових номери, що протирічить викладеному методу. Якщо цих рядків рівно два і в цих двох рядках існує розряд, який дорівнює нулю в обох рядках, то серед інших перших k рядків матриці A має бути рядок, що складається з одиниць, інакше номер одного із стовпців дорівнює нулю, що входить в протиріччя з викладеним методом.

Таким чином, якщо серед перших k рядків вибраної трійки стовпців матриці A є рівно два таких, компоненти яких не рівні між собою і ці два рядки різні, але не інверсні, то можна розглядами два випадки. У першому випадку існує компонента, яка дорівнює нулю в обох рядках. Але в цьому випадку обов'язково існує і рядок, що складається з одиниць і який, разом з двома зазначеними вище рядками утворюють ортогональну систему Θ . В другому випадку в парі різних і не інверсних рядків в обох з них є дві одиниці і точно існує компонента, яка в обох рядках дорівнює одиниці. Якщо в обраних трьох стовпців матриці A в перших k рядках існує рядок, всі компоненти якого дорівнюють одиниці, то цей рядок, разом з двома згаданими вище утворює ортогональну систему Θ . Якщо в вибраних трьох номерах нема рядка, що складається з усіх одиниць, то це означає, що точно один з цих номерів має парну кількість одиниць. Згідно з п.4 викладеного методу в $(k+2)$ -му рядку цей стовпець містить одиницю, а два інші – нулі. Відповідно $(k+2)$ -й рядок разом з двома, що розглядаються, утворюють ортогональну систему Θ . Таким чином доведено, що за умови, що номери трьох вибраних стовпчиків матриці A відрізняються точно в двох розрядах (рядках), в матриці A точно існує ортогональна квадратна матриця Θ , стовпці якої є компонентами вибраних стовпців.

Якщо номери трьох вибраних стовпчиків матриці A відрізняються більш ніж в двох розрядах, то існує не менше трьох різних рядків з не рівними між собою компонентами.

За аналогією з викладеним вище можна розглядати два випадки. У першому в усіх трьох різних рядках існує компонента яка дорівнює нулю, а в другому випадку такої компоненти нема.

Якщо в цих трьох рядках існує компонента, яка дорівнює в них нулю, то дві інших компоненти утворюють пари $\{0,1\}$, $\{1,0\}$, $\{1,1\}$. При цьому обов'язково існує і рядок, що складається з одиниць. В протилежному випадку треба допустити існування нульового номеру, що входить в

протириччя з викладеним методом. В цій ситуації рядок вибраної трійки номерів, що складається з одиниць разом з рядками, що містять пари $\{0,1\}$, $\{1,0\}$ утворюють ортогональну систему Θ . В другому випадку серед k перших рядків обраної трійки стовпців матриці A існує мінімум три різні рядки, причому жодна компонента не дорівнює нулю в усіх трьох рядках, ці три рядки утворюють ортогональну систему Θ якщо серед них є хоча б один з непарним числом одиниць. Якщо серед трійки рядків нема рядків з непарною кількістю одиниць, то вони не утворюють ортогональної системи. Якщо серед інших рядків вибраної трійки номерів є рядок, що складається з одиниць, то він утворює ортогональну систему Θ з будь-якою парою наведених вище стовпців.

Якщо три різних рядки трійки номерів дорівнюють $\{0,1,1\}$, $\{1,0,1\}$ та $\{1,1,0\}$ і всі інші рядки вибраної трійки номерів однакові з наведеними трьома або складаються з нулів, то серед вибраних номерів обов'язково будуть такі, число одиниць в котрих парне. Причому кількість таких стовпців обов'язково непарна тому, що кожен рядок трійки номерів містить парну кількість одиниць. Згідно з п.4 викладеного методу в $(k+2)$ -му рядку в таких стовпцях розміщуються одиниці. Відповідно, $(k+2)$ -й рядку міститься завжди непарна кількість одиниць. Цей рядок разом з будь-якою парою рядків $\{0,1,1\}$, $\{1,0,1\}$ та $\{1,1,0\}$ утворюють ортогональну систему. Наприклад, номери 7, 9 і 14 містять чотири таких рядка: $\{0,1,1\}$, $\{1,0,1\}$, $\{1,0,1\}$ та $\{1,1,0\}$. Сума одиниць в номері 7 непарна, в номері 9 парна і в номері 14 – непарна. Тому $(k+2)$ -й рядок формується у вигляді $\{0,1,0\}$, тобто містить непарну кількість одиниць. Очевидно, що цей рядок разом з рядками $\{0,1,1\}$, $\{1,0,1\}$ утворюють ортогональну систему Θ .

Таким чином, доведено, що матриця A сформована за викладеним методом повністю відповідає умовам, які зумовлюють гарантовану можливість всіх втрачених інформаційних блоків за умови втрати не більше трьох від загального числа інформаційних та резервних блоків.

З запропонованого методу очевидно, що кількість резервних блоків для гарантованого відновлення інформаційних пакетів за умови втрати не більше трьох від загальної кількості блоків визначається формулою:

$$m \geq \lceil \log_2(n+1) \rceil + 2. \quad (2.11)$$

На основі проведених теоретичних досліджень запропоновано метод, який гарантує реконструкцію всіх r блоків при втраті доступу до одного сховища, на якому вони зберігаються, а також трьох блоків, які зберігаються на різних сховищах.

Розроблений метод передбачає, що стовпці матриці A розділяються на $g = \lceil n/r \rceil$ фрагментів так, що в перших $g-1$ фрагментах міститься по r стовпців, а g -й фрагмент містить $n-r \cdot (g-1)$ стовпців.

Побудову матриці A пропонується здійснювати наступним порядком:

1. Встановити індекс j в нуль: $j=0$.
2. $(i+j) \bmod r$ -тий рядок кожного i -того фрагменту матриці A , $i \in \{1, 2, \dots, g\}$, заповнюється $(r-j)$ - розрядним кодом, що складається одиниць на $(r+j-1-i) \bmod r$ – позиції та циклічно наступних за нею в рамках r -бітового фрагменту $r-1-j$ нулів.
3. Здійснюється інкремент індексу j : $j=j+1$. Якщо $j < r$, то виконується перехід на повторне виконання п.2.
4. Невизначені елементи перших $\lceil \log_2(n+1) \rceil$ рядків матриці A заповнюються таким чином, щоб для кожного стовпця вони утворювали унікальний номер, починаючи з одиниці.
5. Наступні рядки матриці A заповнюється таким чином, щоб кількість одиниць в кожному зі стовпців матриці A була не меншою трьох.

Наприклад, для $r=4$ і $n=15$ матриця A формування резервних блоків, побудована за розробленим методом, має наступний вигляд.

$$A = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

При втраті всіх блоків $B_9, B_{10}, \dots, B_{12}$, які зберігаються на 3-му сховищі, відповідні стовпці матриці A містять в собі ортогональну підматрицю Θ :

$$\Theta = \begin{vmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{vmatrix}$$

Відповідно, втрачені блоки відновлюються наступним порядком:

$$B_9 = R_6 \oplus B_2 \oplus B_3 \oplus B_5 \oplus B_6 \oplus B_{14}$$

$$B_{10} = R_3 \oplus B_2 \oplus B_4 \oplus B_7 \oplus B_8 \oplus B_{13} \oplus B_{14} \oplus B_{15}$$

$$B_{11} = R_4 \oplus B_1 \oplus B_3 \oplus B_5 \oplus B_7 \oplus B_8 \oplus B_{10} \oplus B_{13}$$

$$B_{12} = R_1 \oplus B_{11} \oplus B_4 \oplus B_5 \oplus B_6 \oplus B_7 \oplus B_8 \oplus B_{14}$$

При втраті трьох блоків B_1, B_7, B_{12} , що зберігаються на різних сховищах, відповідні стовпці матриці A містять ортогональну підматрицю Θ :

$$\Theta = \begin{vmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix}$$

Відповідно, втрачені блоки відновлюються наступним порядком:

$$B_7 = R_3 \oplus B_2 \oplus B_4 \oplus B_6 \oplus B_{10} \oplus B_{13} \oplus B_{14} \oplus B_{15}$$

$$B_{12} = R_1 \oplus B_7 \oplus B_4 \oplus B_5 \oplus B_6 \oplus B_8 \oplus B_{11} \oplus B_{12} \oplus B_{14}$$

$$B_1 = R_5 \oplus B_2 \oplus B_3 \oplus B_6 \oplus B_9 \oplus B_{10} \oplus B_{12} \oplus B_{15}$$

Таким чином, запропонований метод формування резервних блоків і відновлення інформаційних блоків при їх розподіленому зберіганні не більш ніж по r на кожному з віддалених сховищ, гарантує реконструкцію всіх r блоків при втраті доступу до одного сховища, на якому вони зберігаються, а

також будь-яких трьох інформаційних блоків, які зберігаються на різних сховищах.

Основний ефект запропонованого методу полягає в тому, що суттєвим чином зменшується надлишковість резервування в порівнянні з відомими методами за рахунок урахування особливостей втрати доступу до даних при їх віддаленому зберіганні. Надлишковість резервування зменшується в μ раз, чисельне значення μ визначається формулою:

$$\mu = \frac{(r-2) \cdot \log_2(n+1) + 2}{r+2}. \quad (2.12)$$

Зокрема, для наведеного прикладу кількість резервних блоків для відновлення 4-х, довільно локалізованих по сховищам блоків, дорівнює 10, а в запропонованому методі, який дозволяє відновлювати 4 блоки, що зберігаються на одному сховищі і три, довільно локалізованих блоків, потрібно 6 резервних блоків. Відповідно, надлишковість резервування зменшується в $\mu = 1.67$ раз.

В результаті проведених досліджень теоретично обґрунтовано, розроблено метод відновлення інформаційних блоків при їх розподіленому зберіганні не більш ніж по r на кожному з віддалених сховищ, який базується на використанні для формування резервних блоків матриці, що є ортогональною в межах суміжних r стовпців, а також будь-які три стовпці якої містять ортогональну підматрицю, що гарантує реконструкцію всіх r блоків при втраті доступу до одного сховища, на якому вони зберігаються, а також трьох блоків, які зберігаються на різних сховищах. Метод використовує меншу кількість резервних блоків, тобто має нижчий рівень надлишковості резервування в порівнянні з відомими методами, орієнтованими на відновлення будь-яких r втрачених блоків.

Подальший розвиток запропонованого підходу вбачається в дослідженні можливостей прискорення процесу відновлення втрачених при віддаленому зберіганні даних за рахунок оптимізації їх розміщення на віддалених

сховищах за критерієм мінімізації часу доставки блоків, потрібних для реконструкції втраченої інформації користувачів.

Висновки до розділу 2

В результаті проведення досліджень, які складають другий розділ дисертаційної роботи і направлених на виявлення резервів підвищення ефективності відновлення втрачених даних при їх віддаленого зберіганні та реалізацію цих резервів в формі методів, придатних для практичного використання, можуть бути зроблені наступні висновки:

1. Високий рівень ефективності відновлення втрачених даних в системах їх віддаленого зберігання може бути досягнуте за рахунок комплексного застосування організаційних і технічних методів. Зокрема, показано, що для широкого класу причин втрат інформаційних блоків періодична їх регенерація дозволяє обмежити кількість втрачених блоків і, відповідно, підвищити швидкість їх відновлення.
2. Найбільш дієвим напрямком забезпечення високої надійності віддаленого зберігання даних є широке рознесення їх по різних вузлам, що дозволяє знизити ризики втрати значного за обсягом об'єму інформації від дії одного чинника і, тим самим, підвищити ефективність технологій резервування за рахунок зменшення кількості одночасно втрачених блоків, що має наслідком необхідність в меншій кількості резервних блоків.
3. Розроблено метод прискорення відновлення втрачених блоків даних, який дозволяє, за рахунок збільшення надлишковості резервування, зменшити час доставки по глобальній мережі інформаційних та резервних блоків для реконструювання втрачених блоків, а також зменшити кількість потрібних для цього обчислювальних операцій, що забезпечує важливе для багатьох застосувань прискорення відновлення даних.

4. Теоретично обґрунтовано, розроблено та досліджено метод відновлення інформаційних блоків при їх розподіленому зберіганні не більш ніж по r на кожному з віддалених сховищ, який базується на використанні для формування резервних блоків матриці, що є ортогональною в межах суміжних r стовпців, а також будь-які три стовпці якої містять ортогональну підматрицю, що гарантує реконструкцію всіх r блоків при втраті доступу до одного сховища, на якому вони зберігаються, а також трьох блоків, які зберігаються на різних сховищах. Метод використовує меншу кількість резервних блоків, тобто має нижчий рівень надлишковості резервування в порівнянні з відомими методами, орієнтованими на відновлення будь-яких r втрачених блоків.

РОЗДІЛ 3

ОРГАНІЗАЦІЯ ЕФЕКТИВНОГО ВІДНОВЛЕННЯ ВТРАЧЕНИХ ПРИ ПЕРЕДАЧІ В ГЛОБАЛЬНИХ МЕРЕЖАХ ПАКЕТІВ

Третій розділ роботи присвячено підвищенню ефективності відновлення втрачених інформаційних блоків з урахуванням реальних особливостей втрати доступу до даних при їх віддаленому зберіганні, що дозволяє зменшити надлишковість резервування в порівнянні з відомими методами.

Технологічний прорив, зумовлений появою дешевих радіомодемів, спричинив широке розповсюдження Інтернету, як засобу передачі даних в системах дистанційного контролю та управління об'єктами реального світу в реальному часі. Використання Інтернету в системах реального часу диктує якісно більш жорстокі вимоги до оперативності та надійності передачі даних. Це означає, що специфіка конкретної задачі застосування технології глобальної мережі визначає критичну межу часу, до якої інформація повинна бути доставлена на приймальну сторону. Технологія Інтернет передбачає передачу інформації пакетами різними маршрутами в залежності від трафіку. Відповідно, пакети одного інформаційного повідомлення можуть доставлятися в різні моменти часу. Одним із способів забезпечення заданої оперативності доставки даних через глобальну мережу є використання резервних пакетів, які розсилаються різними маршрутами, з тим, щоб по досягненню критичної часової межі за отриманими вчасно пакетами відновити ті, що спізнилися. Це потребує створення ефективної технології формування резервних пакетів та розробки методів відновлення втрачених або затриманих понад критичну межу часу пакетів.

В рамках дисертаційної роботи в якості основного резерву підвищення ефективності відновлення пакетів даних в глобальних мережах досліджується урахування специфічних особливостей їх втрати для різних класів практичних застосувань характеру. Відповідно, вирішення наукової задачі підвищення ефективності оперативного реконструювання втрачених пакетів

даних вирішується за рахунок створення спеціалізованих засобів відновлення пакетів для домінуючого типу їх втрат.

3.1 Метод відновлення втрачених при передачі в глобальних мережах пакетів з урахуванням статистики їх втрат

Одним із дієвих резервів підвищення ефективності оперативного реконструювання втрачених чи затриманих понад критичний час пакетів даних в глобальних мережах є урахування статистичних характеристик їх втрат та часу передачі.

Для досягнення поставленої мети пропонується метод формування резервних пакетів та відновлення з їх використанням втрачених, пошкоджених або затриманих понад критичний час основних пакетів даних.

Метод виходить з наступної моделі передачі даних інформації в глобальній мережі. Дані, що передаються організовані в n основних пакетів P_1, P_2, \dots, P_n . Кожен пакет має вбудовані засоби виявлення помилок передачі. Пакети передаються по різних маршрутах різномірної мережі, яка може включати фрагменти однорангових мереж (peer-to-peer або P2P) [56]. Для однорангових мереж, тобто при доставці інформації через ланцюжок вузлів існує можливість відключення одного з них. Це призводить до розриву віртуального каналу передачі і, відповідно, втрати деяких пакетів. Специфіка використання визначає певний критичний час доставки інформації. Пакети, що доставлені пізніше критичного часу втрачають актуальність.

Пропонований метод передбачає формування m резервних пакетів R_1, R_2, \dots, R_m , які передаються по мережі разом з n інформаційними P_1, P_2, \dots, P_n пакетами. Вважається, що в процесі передачі частина основних і резервних пакетів може бути втрачена, пошкоджена або прийти з запізненням, що перевищують критичний час доставки. Задача полягає в тому, що з використанням основних і резервних непошкоджених пакетів, що поступили на приймач до критичної часової межі відновити основні пакети даних, які

запізнилися, втрачені або пошкоджені. Якщо час доставки даних не є критичним, то з використанням резервних пакетів вирішується задача відновлення основних пакетів, які втрачені або пошкоджені.

Оскільки час відновлення втрачених основних пакетів є критичним, метод передбачає використання лінійних булевих перетворень. Такі перетворення прості і можуть виконуватися паралельно, що забезпечує високу швидкість формування резервних пакетів та відновлення втрачених основних пакетів. Значимою перевагою використання лінійних булевих перетворень є простота апаратної реалізації.

Таким чином, резервні пакети пропонується формувати з використанням лінійних перетворень над основними пакетами:

$$\forall i \in \{1, 2, \dots, m\} : R_i = \bigoplus_{j=1}^n a_{i,j} \cdot P_j, \quad (3.1)$$

де $\forall i \in \{0, \dots, m\}, j \in \{1, 2, \dots, n\} : a_{i,j} \in \{0, 1\}$.

На стороні приймача, в разі неотримання певної множини Ω основних пакетів до критичного моменту часу, вони вважаються втраченими і можуть бути відновлені шляхом виконання лінійних перетворень над отриманими вчасно основними і резервними пакетами.

Ймовірність відновлення втрачених основних пакетів визначається їх кількістю h , характеристиками та станом мережі, числом m резервних пакетів, кількістю n основних пакетів, а також способом формування резервних пакетів.

Для ефективного відновлення втрачених пакетів даних потрібно, виходячи з характеристик мережі, визначених специфікою задачі вимог щодо надійності відновлення та заданого числа основних пакетів, визначити потрібну кількість резервних пакетів, а також спосіб їх формування.

Визначення потрібної кількості резервних пакетів проводиться виходячи з вимог щодо надійності відновлення, характеристик мережі та залежності ймовірності відновлення втрачених пакетів від кількості основних та резервних пакетів.

Таким чином, для досягнення поставленої мети в рамках досліджень потрібно вирішити такі задачі:

- Теоретично обґрунтувати та розробити спосіб формування резервних пакетів, що забезпечує найбільшу ймовірність відновлення втрачених пакетів при заданих обмежень на їх кількість.

- Встановити характер залежності ймовірності відновлення втрачених пакетів від їх кількості, числа основних та резервних пакетів.

Кожному з n основних пакетів P_1, P_2, \dots, P_n співвідносяться бінарні вектори V_1, V_2, \dots, V_n , в кожному j -тому з яких лише j -та компонентта дорівнює одиниці, а всі інші дорівнюють нулю: $V_1 = \{v_{11}, v_{12}, \dots, v_{1n}\}$, $V_2 = \{v_{21}, v_{22}, \dots, v_{2n}\}$, \dots , $V_n = \{v_{n1}, v_{n2}, \dots, v_{nn}\}$, $\forall i, j \in \{1, 2, \dots, n\}$, $i \neq j$: $v_{ij} = 0$, $v_{ii} = 1$.

Спосіб формування кожного i -го з m резервних пакетів R_i , $i \in \{1, 2, \dots, m\}$ визначається відповідним бінарним вектором $a_i = \{a_{i,1}, a_{i,2}, \dots, a_{i,n}\}$. Ефективність способу формування m резервних пакетів визначається ймовірністю відновлення втрачених основних пакетів за умови, що в процесі передачі втрачено u пакетів з числа основних і резервних.

Здатність відновлення втрачених інформаційних пакетів з використанням m резервних пакетів, тобто векторів a_1, \dots, a_m , залежить від підбору стовпців матриці A і не залежить від їх порядку:

$$A = \begin{vmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{vmatrix} = \begin{vmatrix} q_{1,1} & a_{1,2} & \dots & a_{1,n} \\ q_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{vmatrix} = \begin{vmatrix} s_1 & s_2 & \dots & s_n \end{vmatrix}, \quad (3.2)$$

де $s_1 = \{a_{1,1}, a_{2,1}, \dots, a_{m,1}\}$, $s_2 = \{a_{1,2}, a_{2,2}, \dots, a_{m,2}\}$, \dots , $s_n = \{a_{1,n}, a_{2,n}, \dots, a_{m,n}\}$.

Твердження. При втраті h основних пакетів, номери яких утворюють множину Ω і втраті $\eta = u - h$ резервних пакетів, так, що номери невтрачених резервних пакетів утворюють множину Θ , основні втрачені пакети можуть бути відновлені, якщо матриця Θ утворена компонентами векторів $a \in \Theta$

номери яких входять до множини Ω , містить в собі ортогональну підматрицю, що складається з h рядків і h стовбців.

Доведення. Втрачений пакет P_j , $j \in \Omega$ може бути відновлений, якщо вектор V_j , що співвідноситься з втраченим пакетом P_j може бути представлений у вигляді лінійної функції від векторів V_i невтрачених пакетів: $i \notin \Omega$ та векторів λ_l невтрачених резервних пакетів $l \in \mathcal{G}$:

$$V_j = \bigoplus_{i \notin \Omega} d_i \cdot V_i \oplus \bigoplus_{l \in \mathcal{G}} b_l \cdot a_l, \quad (3.3)$$

де $d_1, \dots, d_n \in \{0,1\}$, $b_1, b_2, \dots, b_n \in \{0,1\}$.

Якщо існує ортогональна підматриця M , h стовпців якої співвідносяться з номерами i_1, i_2, \dots, i_h втрачених основних пакетів, $i_1, i_2, \dots, i_h \in \Omega$, а h рядків якої співвідносяться з номерами j_1, j_2, \dots, j_h підмножини $\Delta \subseteq \mathcal{G}$ невтрачених резервних пакетів, тобто існує ортогональна підматриця M :

$$M = \begin{bmatrix} a_{j_1, i_1} & a_{j_1, i_2} & \cdots & a_{j_1, i_h} \\ a_{j_2, i_1} & a_{j_2, i_2} & \cdots & a_{j_2, i_h} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j_h, i_1} & a_{j_h, i_2} & \cdots & a_{j_h, i_h} \end{bmatrix}, \quad (3.4)$$

то вектори $a_{j_1}, a_{j_2}, \dots, a_{j_h} \in \Delta$ можуть бути представлені у вигляді:

$$\begin{aligned} a_{j_1} &= a_{j_1, i_1} \cdot V_{i_1} \oplus a_{j_1, i_2} \cdot V_{i_2} \oplus \cdots \oplus a_{j_1, i_h} \cdot V_{i_h} \oplus \bigoplus_{l \notin \Omega} a_{j_1, l} \cdot V_l \\ a_{j_2} &= a_{j_2, i_1} \cdot V_{i_1} \oplus a_{j_2, i_2} \cdot V_{i_2} \oplus \cdots \oplus a_{j_2, i_h} \cdot V_{i_h} \oplus \bigoplus_{l \notin \Omega} a_{j_2, l} \cdot V_l \\ &\vdots \\ a_{j_h} &= a_{j_h, i_1} \cdot V_{i_1} \oplus a_{j_h, i_2} \cdot V_{i_2} \oplus \cdots \oplus a_{j_h, i_h} \cdot V_{i_h} \oplus \bigoplus_{l \notin \Omega} a_{j_h, l} \cdot V_l \end{aligned} \quad (3.5)$$

Система (3.5) може бути представлена у вигляді системи лінійних булевих рівнянь, невідомими якої є вектори $V_{i_1}, V_{i_2}, \dots, V_{j_h}$ які співвідносять з втраченими основними пакетами:

$$\begin{cases} a_{j_1, i_1} \cdot V_{i_1} \oplus a_{j_1, i_2} \cdot V_{i_2} \oplus \dots \oplus a_{j_1, i_h} \cdot V_{i_h} = a_{j_1} \oplus \bigoplus_{l \notin \Omega} a_{j_1, l} \cdot V_l \\ a_{j_2, i_1} \cdot V_{i_1} \oplus a_{j_2, i_2} \cdot V_{i_2} \oplus \dots \oplus a_{j_2, i_h} \cdot V_{i_h} = a_{j_2} \oplus \bigoplus_{l \notin \Omega} a_{j_2, l} \cdot V_l \\ \vdots \\ a_{j_h, i_1} \cdot V_{i_1} \oplus a_{j_h, i_2} \cdot V_{i_2} \oplus \dots \oplus a_{j_h, i_h} \cdot V_{i_h} = a_{j_h} \oplus \bigoplus_{l \notin \Omega} a_{j_h, l} \cdot V_l \end{cases}. \quad (3.6)$$

В системі (3.6) коефіцієнти при невідомих $V_{i_1}, V_{i_2}, \dots, V_{j_h}$ являють собою елементи матриці M . Відповідно, якщо матриця M є ортогональною, то система (3.6) може бути розв'язана відносно $V_{i_1}, V_{i_2}, \dots, V_{j_h}$, причому кожен із векторів $V_{i_1}, V_{i_2}, \dots, V_{j_h}$ виражається при цьому у вигляді лінійної комбінації від векторів V_i невтрачених пакетів: $i \notin \Omega$ та підмножини $\Delta \subseteq \mathfrak{S}$ векторів a_l невтрачених резервних пакетів $l \in \Delta$:

$$\forall q \in \Omega: V_q = \bigoplus_{i \notin \Omega} d_{q,i} \cdot V_i \oplus \bigoplus_{l \in \Delta} b_{q,l} \cdot \lambda_l, \quad (3.7)$$

де $\forall q \in \Omega, i \notin \Omega: d_{q,i} \in \{0,1\}$, $\forall q \in \Omega, l \in \Delta: b_{q,l} \in \{0,1\}$.

Відповідно, відновлення h втрачених основних пакетів $P_{i_1}, P_{i_2}, \dots, P_{i_h}$ може бути здійснене з використанням невтрачених основних і резервних пакетів згідно наступної формули:

$$\forall q \in \{i_1, i_2, \dots, i_h\} = \Omega: P_q = \bigoplus_{i \notin \Omega} d_{q,i} \cdot P_i \oplus \bigoplus_{l \in \Delta} b_{q,l} \cdot R_l, \quad (3.8)$$

що й було потрібно довести.

Очевидно, що ортогональна матриця Θ для конкретної локалізації втрачених пакетів може існувати лише при виконанні наступних двох умов:

- серед стовпців, номери яких належать множині Ω відсутні такі, що містять лише нульові компоненти.
- серед стовпців, номери яких належать множині Ω відсутні такі, що повторюються.

Значення ймовірності g_i визначається вибором стовпців s_1, s_2, \dots, s_n матриці Λ і не залежить від їхнього порядку. Зокрема, якщо $i=u$, тобто всі втрачені

пакети відносяться до основних, то максимальне значення ймовірності g_i досягається за умови, що всі стовпці s_1, s_2, \dots, s_n різні і жоден із них не складається лише з нульових компонентів. Очевидно, що всі стовпці можуть бути різними лише при виконанні умови $2^k > n$.

Якщо $i < u$, тобто $u-i$ резервних пакетів втрачено, з стовпців s_1, s_2, \dots, s_n виключаються компоненти, які співвідносяться з втраченими резервними пакетами. При цьому стовпці, що містять менше ніж $u-i+1$ одиниць можуть трансформуватися в стовпці, що містять лише нулі, що має наслідком зменшення ймовірності g_i .

Тому, стовпчики, що містять малу кількість одиниць доцільно вважати менш пріоритетними. З іншого боку, якщо кількість нульових компонентів стовпців s_1, s_2, \dots, s_n невелика, то при виключенні компонентів, які співвідносяться з втраченими резервними пакетами зростає ймовірність їх трансформації в однакові.

З точки зору втрати здатності відновлення втрачених основних пакетів, трансформація стовпчика матриці A , при втраті резервних пакетів, в нульовий є більш критичною ніж трансформація стовпчика в такий, всі компоненти котрого складаються з одиниць. В останній ситуації зменшення здатності відновлення зумовлюється появою стовпців, що повторюються.

Якщо втрачено h основних пакетів і після трансформовування матриці A вона містить нульовий стовпець, то якщо номер втраченого пакету збігається з номером нульового стовпця, він не може бути відновлений при всіх варіантах локалізації $h-1$ інших втрачених пакетах з $n-1$. Відповідно, це породжує $\rho_0 = C_{n-1}^{h-1}$ варіантів локалізації втрачених основних пакетів які не можуть бути виправлені.

Якщо при втраті h основних пакетів і після трансформовування матриці A вона містить стовпець, що складається з одиниць, то виникає ситуація наявності двох однакових стовпців трансформованої матриці A . Якщо номери пари втрачених основних пакетів збігаються з номерами однакових

стовпців трансформованої матриці A , то вони не можуть бути відновленими при всіх варіантах локалізації $h-2$ інших втрачених пакетах з $n-2$. Відповідно, це породжує $\rho_1 = C_{n-2}^{h-2}$ варіантів локалізації втрачених основних пакетів які не можуть бути виправлені.

Співвідношення $\nu = \rho_0 / \rho_1$ кількості варіантів локалізації основних пакетів, що не можуть бути відновлені, при появі в результаті трансформації матриці A нульового і одиничного стовпців, може бути представлене у вигляді:

$$\nu = \frac{\rho_0}{\rho_1} = \frac{C_{n-1}^{h-1}}{C_{n-2}^{h-2}} = \frac{n-1}{h-1} . \quad (3.9)$$

Враховуючи, що на практиці $n \gg h$, значення $\nu \gg 1$, тобто поява при трансформації матриці A нульового стовпчика значно більш негативно впливає на відновлюючу здатність ніж поява одиничного стовпчика. Наприклад при $n=15$ і $m=4$ в ситуації втрати 4-х пакетів, один із яких резервний і три основних ($h=3$), значення ν становить 7. Це означає, що поява в результаті трансформації матриці A нульового стовпця призводить до збільшення кількості основних пакетів, що не можуть бути відновлені і ця кількість в 7 раз більша ніж число не відновлюваних основних пакетів, зумовлених появою в результаті трансформації матриці A стовпця, що містить лише одиночні компоненти.

Виходячи з наведеного, пропонується наступна процедура визначення пріоритетів $\chi_1, \chi_2, \dots, \chi_n$ для стовпців s_1, s_2, \dots, s_n матриці A . Для стовпця s_i , $i \in \{1, 2, \dots, n\}$ можна визначити кількість його одиничних компонентів - ε_i . Стопці, що не мають одиничних компонентів, тобто ті, для яких $\varepsilon_i = 0$, не використовуються. Для стовпця s_i з $\varepsilon_i > 0$ його пріоритет χ_i пропонується визначати наступним чином:

1. Якщо $\varepsilon_i = 1$, тобто стовпець s_i містить лише одну одиницю, то йому присвоюється найнижчий пріоритет $\chi_i = 0$.

2. Якщо стовпець s_i матриці A містить лише одиничні компоненти, тобто $\varepsilon_i = m$, то $\chi_i = 1$.

3. За умови $1 < \varepsilon_i < m$, то якщо $\varepsilon_i < m/2$, то $\chi_i = 2 \cdot \min \{\varepsilon_i, m - \varepsilon_i\} - 1$, інакше, тобто якщо $\varepsilon_i \geq m/2$, то $\chi_i = 2 \cdot \min \{\varepsilon_i, m - \varepsilon_i\}$.

В якості ілюстрації в таблиці 3.1 наведені пріоритети 5-компонентних стовпців ($m=5$) залежно від кількості одиниць в них.

Таблиця 3.1

Залежність пріоритетів стовпців матриці A від кількості одиниць в них
для $m=5$

Кількість одиниць ε	Значення пріоритету χ
1	0
2	2
3	4
4	3
5	1

Ефективність запропонованого методу визначається співвідношенням його здатності відновлювати втрачені дані і об'ємом ресурсів, що витрачаються на вирішення цієї задачі. В якості оцінки об'єму ресурсів можна розглядати кількість k резервних пакетів, для формування яких потрібні витрати певні обчисленням, об'єм який пропорційний k , для доставки яких потрібно зайняти ресурси каналів передачі даних.

Тому, для порівняльної оцінки ефективності резервування пакетів різними методами, доцільно визначати ефективність E резервування відношенням ймовірності відновлення втрачених основних пакетів до кількості резервних пакетів:

$$E = \frac{1}{m} \cdot \sum_{i=1}^{n+m} q_i \cdot p_{i,m}, \quad (3.10)$$

де q_i – ймовірність того, що в процесі передачі буде втрачено i пакетів з $n+m$ переданих; $p_{i,m}$ – ймовірність того, що при втраті i пакетів з $n+m$ переданих, всі втрачені основні пакети можуть бути відновлені при використанні k резервних пакетів.

Якщо вважати, що втрата пакетів відбувається незалежно, то кількість втрачених пакетів підпорядкована біноміальному закону для якого визначена ймовірність ρ втрати одного пакету. Тоді, формула (3.10) може бути представлена у вигляді:

$$E = \frac{1}{m} \cdot \sum_{i=1}^{n+m} C_{n+m}^i \cdot \rho^i \cdot (1-\rho)^{n+m-i} \cdot p_{i,m}. \quad (3.11)$$

Як зазначалося в оглядовому розділі, існуючі відновлюючі, в свої більшості, орієнтовані на гарантування відновлення фіксованої кількості пакетів з переданих. Найчастіше в якості такої кількості виступає число основних пакетів [33]. При такому підході кількість k резервних пакетів визначається як $w(n)$ [34]. Наприклад, для гарантування відновлення трьох пакетів при $n=3$, треба передавати $w(3)=5$ резервних пакетів, а для гарантованого виправлення п'яти пакетів при такому ж числі $n=5$ основних пакетів використовується $w(5)=7$ резервних пакетів.

Відповідно, при гарантуванні відновлення n пакетів з $n+k$ переданих, ефективність E_0 може бути представлена у вигляді:

$$E_0 = \frac{1}{w(n)} \cdot \sum_{i=1}^{n+m} C_{n+w(n)}^i \cdot \rho^i \cdot (1-\rho)^{n+w(n)-i}. \quad (3.12)$$

Тоді виграш ε в ефективності резервування запропонованого методу по відношенню до відомих методів можна оцінити через відношення ефективності E резервування запропонованого методу до ефективності E_0 резервування відомих методів:

$$\varepsilon = \frac{E}{E_0}. \quad (3.13)$$

В таблиці 3.2 представлені результати порівняльного аналізу ефективності резервування для відомих і запропонованих методів резервування при передачі 3-х і 5-ти основних пакетів. При розрахунку ефективності запропонованого методу при $n=3$ і при $n=5$ використовувалися 3 резервні пакети: $m=3$.

Таблиця 3.2

Результати порівняльного аналізу ефективності резервування запропонованого методу та відомих відновлюючих кодів

n	$w(n)$	k	$\varepsilon = E/E_0$			
			$\rho=0.001$	$\rho=0.005$	$\rho=0.01$	$\rho=0.05$
3	5	3	1.24	1.25	1.26	1.31
5	7	3	1.556	1.561	1.563	1.582

Аналіз даних, представлених в таблиці 3.2 свідчить про те, що розроблений метод забезпечує вищу ефективність використання резервних пакетів для відновлення втрачених основних пакетів в порівнянні з відомими методами. Різниця в ефективності запропонованого методу зростає зі збільшенням числа основних пакетів та ймовірності втрати або пошкодження пакету в процесі його доставки.

В результаті проведених досліджень теоретично обґрунтовано, розроблено та досліджено метод формування резервних пакетів та їх використання для відновлення основних інформаційних пакетів, що можуть бути втрачені при передачі в Інтернет.

Кожен із резервних пакетів формується у вигляді логічної суми визначених підмножин інформаційних пакетів, причому регламентований розробленим методом вибір вказаних підмножин забезпечує найбільшу ймовірність існування ортогональної системи рівнянь, до розв'язання якої зводиться процес відновлення втрачених інформаційних пакетів. Це забезпечує більшу ефективність використання резервних пакетів в порівнянні з відомими методами відновлення пакетів в глобальних мережах.

Для прискорення відновлення втрачених пакетів метод передбачає використання спеціальних таблиць передобчислень. В таблицях, для кожного пакету, що відновлюється, зберігаються наперед визначені підмножини невтрачених основних та резервних пакетів, логічна сума яких являє собою втрачений пакет.

Запропонований метод орієнтований для використання в системах комп'ютерного управління віддаленими об'єктами, зв'язок з якими здійснюється через Інтернет з використанням сучасних радіо модемів.

Таким чином, розроблений метод відновлення затриманих при передачі інформаційних пакетів даних, який відрізняється використанням системи пріоритетів при виборі компонентів матриці, формування обмеженої кількості резервних пакетів з урахуванням статистичних характеристик, затримок транспортування пакетів, що дозволяє підвищити ймовірність відновлення втраченої чи затриманої інформації і тим самим прискорити передачу даних в глобальних мережах.

Показники швидкодії, на відміну від відновлення блоків даних, що зберігаються на віддалених носіях визначається не часом транспортування непошкоджених блоків даних, а лише часом виконання обчислювальних операцій, пов'язаних з відновленням втрачених інформаційних пакетів повідомлення.

3.2 Розробка ефективного відновлення “пачок” втрачених при передачі в глобальних мережах пакетів

При відновленні пакетів даних в глобальних мережах типовим випадком є втрата пачки суміжних пакетів потоку. Це викликано дією наступних чинників:

- Час дії зовнішніх завад, які викликають значне кодове спотворення пакету, що не може бути виправлене вбудованими в ньому корегуючими кодами, значно більше за час передачі одного пакету. Це означає, що для широкого кола ефірних каналів, таких, зокрема, як радіоканали та супутникові канали, під дією завад фактично втрачається не один, а група суміжних пакетів інформаційної посилки.

- При використанні peer-to-peer технологій, які нині широко застосовуються для підвищення пропускної здатності мереж, асинхронне відключення ланки віртуальної мережі має наслідком втрату групи суміжних

пакетів, які передаються за проміжок часу від моменту відключення до моменту відновлення віртуальної мережу шляхом її реконфігурації.

- В каналах [22] передачі даних мереж спостерігається виникнення імпульсних перевантажень трафіку, що може мати результатом втрату групи суміжних пакетів.

В літературі [23] відмічається, що особливу небезпеку такі типи втрат пакетів, що передаються по мережам становлять при використанні бездротових мереж в якості середовища обміну даними в системах комп'ютерного управління технологічними процесами. На сучасних підприємствах існує велика кількість потенційно небезпечних для ефірних каналів передачі даних джерел зовнішніх завад.

При високих швидкостях передачі пакетів в ефірних каналах під впливом зовнішніх електромагнітних завад виникають втрати пакетів, що носять характер “пачки”. Поняття “пачки втрачених пакетів” (BPL - Burst Packet Loss) визначається наступним чином [72]: група суміжних пакетів інформаційної посилки, яка втрачена чи доставлена з перевищенням заданого часу пересилки в результаті дії зовнішніх завад, асинхронних відключень компонентів віртуальної мережі або імпульсних перевантажень трафіку. Для оцінки пачок втрачених пакетів використовується коефіцієнт блокової втрати пакетів R_b (Burst Ratio) – яким оцінюється середнє значення втрачених або затриманих передачею понад критичний час пакетів в пачці.

Аналіз публікацій [73, 74], присвячених дослідженню BPL свідчить про те, що їх виникнення найчастіше описується, в математичному плані, біноміальною моделлю, тобто середньоквадратичне відхилення кількості пакетів в пачці втрачених визначається через середнє число втрачених пакетів. Автори публікацій [72, 74] зазначають також, що для певного кола мереж на долю BPL припадає домінуюча частина (до 96%) втрачених пакетів.

Це означає, що доцільним є створення спеціалізованих засобів, орієнтованих на відновлення BPL. Аналіз публікацій показав, що для певного кола практичних застосувань, пов'язаних з використанням бездротових мереж в якості середовища обміну інформації в системах комп'ютерного управління реальними рознесеними об'єктами і, зокрема, технологічним обладнанням найбільша ефективність забезпечення надійності передачі досягається за умови можливості виправлення BPL та 1-2 окремих пакетів. Фактично, це означає, що для широкого кола застосувань мережевих технологій в системах комп'ютерного управління для забезпечення надійності доцільно виходити з наступної моделі втрат пакетів:

- втрата переважної більшості пакетів реалізується в формі BPL і викликана дією зовнішніх завад, імпульсних підвищень трафіку ;

- втрата невеликої кількості

Для вирішення задачі ефективного відновлення втрачених пакетів інформаційної посилки, які утворюють пачку пропонується наступний підхід по побудови матриці формування резервних пакетів. В якості заданих даних виступають значення R_b та кількість n пакетів, що не утворюють пачку, але мають бути реконструйовані в разі втрати чи затримки понад встановлений граничний час доставки. Запронований спосіб побудови матриці A формування резервних пакетів та їх пересилки зводиться до виконання наступної послідовності дій:

1. Аналізом математичної моделі виникнення BPL встановлюється значення граничної кількості g втрачених пакетів в "пачці". Зокрема, якщо процес виникнення BPL описується біноміальною моделлю, найбільш часто використовується визначення границі u вигляді: $g = 3 \cdot \sqrt{R_b}$. Наприклад, якщо $R_b = 3$, то $g = 3 \cdot \sqrt{3} \approx 5$.

2. Кількість m резервних пакетів визначається наступною формулою:

$$m = g + \left\lceil \log_2 \frac{n}{g} \right\rceil. \quad (3.14)$$

3. Перші g резервні пакети використовуються для гарантованого відновлення пакетів, що входять до складу BPL. Підматриця матриці A для їх формування утворюється наступним чином:

$$\forall i \in \{1, 2, \dots, g\}, j \in \{1, 2, \dots, n\} : \begin{cases} a_{i,j} = 1, \text{ якщо } j \bmod q = i, \\ a_{i,j} = 0, \text{ якщо } j \bmod q \neq i \end{cases} \quad (3.15)$$

4. Останні $m-g$ резервні пакети забезпечують гарантоване відновлення у втрачених пакетів, які не утворюють “пачку”, тобто не належать до BPL. Підматриця матриці A для їх формування утворюється наступним чином:

$$\forall l \in \{g+1, g+2, \dots, m\}, j \in \{1, 2, \dots, n\} : \begin{cases} a_{l,j} = 1, \text{ якщо } 2^{l-g-1} \leq \left\lceil \frac{l-g}{g} \right\rceil \bmod 2^{l-g}, \\ a_{l,j} = 0, \text{ якщо } \left\lceil \frac{l-g}{g} \right\rceil \bmod 2^{l-g} < 2^{l-g-1} \end{cases} \quad (3.16)$$

Наприклад, при числі основних пакетів в потоці рівному 15: $n=15$ і при значенні $g=5$ для гарантування відновлення пакетів однієї BPL і для відновлення двох довільних інформаційних пакетів ($u=2$), матриця A формування резервних пакетів, побудована за розробленою і представленою вище процедурою має такий вигляд:

$$A = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}. \quad (3.17)$$

Сформовані описаним вище способом резервні пакети R_1, R_2, \dots, R_m включаються в потік після інформаційних пакетів P_1, P_2, \dots, P_n і пересилаються по глобальній мережі приймаючій стороні.

Відновлення втрачених пакетів відбувається в рамках наступної послідовності дій:

1. При досягненні граничної часової межі, на стороні приймача здійснюється аналіз отриманих інформаційних пакетів. Якщо втрачені пакети утворюють “пачку”, тобто мають суміжні номери: $\eta_1, \eta_2, \dots, \eta_q$: $\eta_1 < n, q \leq g, \eta_2 = \eta_1 + 1, \eta_3 = \eta_2 + 1, \dots, \eta_q = \eta_{q-1} + 1$, то відновлення втрачених при передачі по глобальній мережі інформаційних пакетів $P_{\eta_1}, P_{\eta_2}, \dots, P_{\eta_q}$ здійснюється у відповідності з наступними виразами:

$$\forall i \in \{1, 2, \dots, q\} : P_{\eta_i} = R_{(\eta_i - 1) \bmod g + 1} \oplus \bigoplus_{j=1}^{\eta_i - 1} P_j \cdot \xi_j \oplus \bigoplus_{j=\eta_i}^n P_j \cdot \xi_j, \quad (3.18)$$

де значення ξ визначається таким чином:

$$\xi_j = \begin{cases} 1, & \text{якщо } j \bmod g = \eta_i \bmod g, \\ 0, & \text{якщо } j \bmod g \neq \eta_i \bmod g \end{cases}$$

3. Якщо втрачені пакети не утворюють “пачку”, то в матриці А виділяється підматриця Н, утворена стовпцями, номери яких дорівнюють номерам втрачених блоків.

4. З матриці Н видаляються рядки, які співвідносяться зі втраченими резервними блоками з утворенням підматриці Н'. В матриці Н' віднаходиться ортогональна підматриця Θ , по якій визначаються математичні вирази для відновлення втрачених при передачі по мережі інформаційних пакетів.

Наведене може бути ілюстровано наступним прикладом. Нехай, в рамках наведеного вище прикладу, тобто за умови формування резервних пакетів у відповідності з матрицею А (3.17) втрачена “пачка” пакетів, яка складається з суміжних у часі 4-х інформаційних P_{12}, P_{13}, P_{14} та P_{15} і одного резервного пакету R_1 . Згідно з формулою (3.4) втрачені інформаційні пакети відновлюються у вигляді логічної суми резервного пакету, номер якого по модулю $g=5$ співпадає з номером пакету, що відновлюється та невтрачених при передачі інформаційних пакетів, що мають номери, залишок від ділення на $g=5$ для яких співпадає з аналогічним залишком пакету, що

реконструюється. В формальному вигляді втрачені інформаційні пакети відновлюються у відповідності з наступними виразами:

$$P_{12} = R_2 \oplus P_2 \oplus P_7$$

$$P_{13} = R_3 \oplus P_3 \oplus P_8$$

$$P_{14} = R_4 \oplus P_4 \oplus P_9$$

$$P_{15} = R_5 \oplus P_5 \oplus P_{10}$$

При втраті двох окремих пакетів, які не утворюють “пачку”, наприклад 1-го та 6-го, тобто P_1 та P_2 , згідно з описаною вище методикою, з матриці A виділяється підматриця H , що складається з першого та шостого стовпців матриці A , тобто стовпців, які співвідносяться з втраченими інформаційними пакетами. Оскільки резервні пакети не втрачені, то вказана матриця H фактично співпадає з матрицею H' і має наступний вигляд:

$$H = H' = \begin{vmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{vmatrix} \quad (3.19)$$

В підматриці (3.19) віднаходиться ортогональна підматриця Θ , утворена першим та шостим рядками матриці H :

$$\Theta = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}$$

З матриці Θ впливають математичні вирази для безпосереднього відновлення втрачених інформаційних блоків:

$$P_6 = R_6 \oplus P_7 \oplus P_8 \oplus P_9 \oplus P_{10}$$

$$P_1 = R_1 \oplus P_6 \oplus P_{11}$$

Оцінка ефективності запропонованого методу може бути здійснена шляхом порівняльного дослідження двох базових критеріїв ефективності при фіксованій кількості пакетів, що можуть бути відновлені:

- кількості резервних пакетів, які формуються і пересилаються по мережі для відновлення фіксованої кількості втрачених інформаційних пакетів;
- обчислювальна та часова складність обчислень, пов'язаних з відновлених втрачених інформаційних пакетів. Показники швидкодії, на відміну від відновлення блоків даних, що зберігаються на віддалених носіях визначається не часом транспортування непошкоджених блоків даних, а лише часом виконання обчислювальних операцій, пов'язаних з відновленням втрачених інформаційних пакетів повідомлення.

При використанні MDS кодів для гарантованого відновлення 5-ти довільних пакетів з 15-ти переданих потрібно використовувати 11 резервних блоків. Запропонований спосіб відновлення BPL передбачає гарантоване відновлення 5-ти пакетів у складі BPL та двох довільних з використанням лише 7-ми додаткових пакетів. Таким чином, за рахунок спеціалізації технології резервування та відновлення пакетів для домінуючого типу їх втрат для широкого класу застосувань досягнуто підвищення ефективності шляхом зменшення потрібних для вирішення технічної задачі ресурсів, зокрема, кількості додаткових пакетів.

В роботах [56, 57] для корекції пачок пропонується застосування зважених контрольних сум. В першому із згаданих досліджень для формування зважених контрольних сум використовуються логічні операції. Суть полягає в тому, що в якості вагових коефіцієнтів використовуються степеневі елементи поля Галуа. Це дозволяє звести задачу відновлення “пачки” пакетів до розв’язання системи лінійних булевих рівнянь. Ця задача значно простіша за розв’язання системи нелінійних рівнянь у методі Ріда-Соломона. Кількість контрольних розрядів менша, ніж при використанні коду Ріда-Соломона. Проте згадане рішення використовує більшу кількість

резервних пакетів: $m = 2 \cdot (g-1) + \log_2 n$. Показники швидкодії цього відомого методу відновлення BPL близькі до запропонованого методу. Другий відомий метод відновлення BPL фактично є аналогом згаданого вище, за відмінністю того, що він має за основу використання арифметичних операцій і він передбачає використання трьохкомпонентної контрольної суми. Задача реконструювання BPL зводиться до p операції арифметичного ділення.

Таким чином, запропонований метод відновлення BPL та невеликої кількості окремих пакетів, який відрізняється від відомих способом побудови матриці формування резервних пакетів, число яких, за рахунок спеціалізації на визначеному домінуючому типі втрат пакетів, зменшено у порівнянні з відомими методами. Розроблений метод за рахунок спеціалізації на найбільш типовому варіанті втрати пакетів в системах з ефірними та супутниковими каналами має підвищену ефективність у порівнянні з універсальними рішеннями за рахунок зменшення потрібних для відновлення резервних пакетів, та збільшення швидкодії. Прискорення відновлення BPL досягається за рахунок того, що підматриця A формування резервних пакетів, призначених для реконструювання BPL містить меншу кількість одиниць ніж матриця A , що містить стандартні MDS коди. Якщо, стандартна матриця MDS кодів містить, в середньому, $n/2$ одиниць рядку, то рядок матриці A , побудованої за запропонованим способом містить n/g одиниць. Це означає, що середня кількість N операцій логічного додавання інформаційних части пакетів в запропонованому методі визначається формулою:

$$N = R_b \cdot \frac{n}{g} = R_b \cdot \frac{n}{3 \cdot \sqrt{R_b}} = \frac{n \cdot \sqrt{R_b}}{3} . \quad (3.20)$$

При використанні універсального методу відновлення BPL з використанням стандартних MDS кодів, для відновлення R_b інформаційних пакетів потрібно виконати $N_0 = R_b \cdot n/2$ операцій логічного додавання інформаційних части пакетів. Це означає, що використання запропонованого спеціа-

лізованого методу для вирішення задачі відновлення BPL дозволяє прискорити процес відновлення пакетів в ζ раз, причому чисельне значення коефіцієнта ζ прискорення визначається наступною формулою:

$$\zeta = \frac{N_0}{N} = \frac{3 \cdot \sqrt{R_b}}{2}. \quad (3.21)$$

Значення R_b - середнього числа пакетів в втраченій “пачці” на практиці, згідно даним [45] лежить в інтервалі від 3-х до 10-х. Відповідно, теоретично обчислене за формулою (3.21) значення коефіцієнта ζ прискорення реконструювання втрачених пакетів BPL для реальних ситуацій лежить в інтервалі від 2.6 до 4.7. Експериментальні дослідження показали, що реальне прискорення дещо менше, але близьке до отриманих теоретичним шляхом оцінок.

Таким чином, теоретичними та експериментальними дослідженнями показано, що розроблений метод, за рахунок його орієнтації на визначеному домінуючому типі втрат інформаційних пакетів дозволяє, в середньому на 30-40% скоротити кількість резервних пакетів, що передаються по глобальним мережам. Запропонований в рамках методу спосіб побудови матриці формування резервних пакетів забезпечує, при цьому скорочення часу відновлення втраченої BPL на 2-4 раз рахунок розрідження матриці, що має наслідком зменшення обчислювальної складності операцій, пов'язаних з їх реконструюванням.

3.2 Організація ефективного відновлення “пачок” втрачених при передачі в глобальних мережах пакетів

Мета досліджень полягає в прискоренні обчислювальних процедур формування резервних пакетів за рахунок введення обмеження на числа пакетів, що можуть бути відновлені (до трьох).

Введення обмеження дозволяє значно спростити формування резервних пакетів та прискорити відновлення втрачених.

Для досягнення поставленої мети розв'язуються такі наукові задачі:

- теоретичне дослідження властивостей надлишкових пакетів, які гарантують можливість відновлення інформаційних пакетів в разі втрати не більше трьох пакетів з їх загального числа;
- розробка, на основі отриманих теоретичних результатів, способу формування резервних пакетів для гарантованого відновлення інформаційних пакетів при втраті не більше трьох з загальної кількості пакетів;

Пропонований метод базується на наступній моделі передачі пакетів в мережі. Інформація, яка передається організована у вигляді n основних пакетів P_1, P_2, \dots, P_n . Пакети містять контрольні коди, які дозволяють виявити помилку, що виникла в процесі передачі.

Вважається, що передача пакетів здійснюється за різними маршрутами, в залежності від зміни трафіку. При цьому, маршрут передачі може включати фрагменти однорангових peer-to-peer мереж. Для таких фрагментів існує можливість некерованого відключення одного з них, з тимчасовим порушенням віртуального каналу. При цьому можуть відбуватися втрати деяких пакетів.

Крім того, часто специфіка широкого кола практичних задач визначає критичний час доставки пакетів, після чого вони втрачають актуальність.

Таким чином, поняття втрати пакету включає три ситуації:

- виникнення помилок передачі, що не можуть бути виправлені за допомогою вбудованих в пакет контрольних кодів;
- втрата пакету в процесі передачі;
- доставка пакету після визначеної граничної часової межі.

Для відновлення втрачених пакетів пропонується разом з n основними передавати m резервних пакетів R_1, R_2, \dots, R_k , які формуються спеціальним чином з інформації, що міститься в основних пакетах.

Задля швидкого відновлення втрачених основних пакетів пропонується формувати резервні пакети та відновлювати втрачені з використанням лінійних булевих перетворень. Важлива перевага застосування перетворень

цього класу полягає в граничній простоті апаратної реалізації. Відповідно, кожен резервний пакет формується як сума за модулем два кодів певної підмножини основних пакетів згідно з формулою (3.1).

На стороні приймача, в разі неотримання певної множини Ω основних пакетів до критичного моменту часу, вони вважаються втраченими і можуть бути відновлені шляхом виконання лінійних перетворень над отриманими вчасно основними і резервними пакетами.

При втраті трьох з $n+t$ пакетів можливо три ситуації:

1. Всі три втрачених пакети відносяться до основних.
2. Два втрачених пакета відносяться до основних і один із втрачених – резервний.
3. Один втрачений пакет відноситься до основних і два – до резервних.
4. Всі три втрачених пакети відносяться до резервних.

В останньому випадку всі основні пакети отримані на стороні приймача без помилок і вчасно – відповідно задача відновлення даних не вирішується.

Якщо втрачено два резервних пакета і один з основних, то задача полягає в відновленні саме одного основного пакету. Ця задача може бути вирішена, якщо після видалення з матриці A рядків, які співвідносяться з втраченими резервними пакетами, вона не буде містити нульових стовбців. Для цього достатньо, щоб всі стовбці матриці A містили більше двох одиниць, тобто виконувалася умова:

$$\forall l \in \{1, 2, \dots, n\} : \sum_{i=1}^m a_{i,l} > 2. \quad (3.22)$$

Якщо втрачено два основних пакети і один з втрачених стовбців належить до резервних, то для відновлення втрачених основних пакетів, необхідно, щоб після видалення з матриці A рядка, який співвідноситься з втраченим резервним пакетом, всі стовбці в ній були різними. Для того, щоб ця умова виконувалася, Хемінгова відстань між стовпцями матриці A має бути більше одиниці:

$$\forall l, i \in \{1, 2, \dots, n\}, l \neq i: \sum_{j=1}^m (a_{j,l} \oplus a_{j,i}) > 1. \quad (3.23)$$

Якщо всі три втрачені пакети відносяться до класу основних і виконуються умови (3.22) і (3.23), то втрачені пакети можуть бути гарантовано відновлені за умови, що матриця A містить рядок, який складається повністю з одиниць:

$$\exists j \in \{1, 2, \dots, m\}: \prod_{i=1}^n a_{j,i} = 1. \quad (3.24)$$

Це може бути доведене наступним чином. Номери втрачених пакетів можуть бути позначені як v, w та e , $v, w, e \in \{1, 2, \dots, n\}$, причому, не порушуючи загальності, можна вважати, що $v < w < e$. Тоді можна розглядати матрицю Δ , утворену стовпцями v, w та e матриці A :

$$\Delta = \begin{vmatrix} a_{1,v} & a_{1,w} & a_{1,e} \\ a_{2,v} & a_{2,w} & a_{2,e} \\ \dots & & \\ a_{m,v} & a_{m,w} & a_{m,e} \end{vmatrix}$$

Втрачені пакети можуть бути відновлені, якщо в матриці Δ існують три рядки, які утворюють ортогональну матрицю Θ .

Для доведення цього факту доцільно дослідити диференційні властивості рядків матриці Δ . Ці властивості для кожного y -го рядка матриці Δ , $y \in \{1, 2, \dots, m\}$ характеризуються двокомпонентним бінарним вектором $d_y = \langle d_{y1}, d_{y2} \rangle$ який визначається наступним чином:

$$d_y = \langle d_{y1}, d_{y2} \rangle, \text{ де } d_{y1} = a_{y,v} \oplus a_{y,w}, d_{y2} = a_{y,v} \oplus a_{y,e}$$

Згідно з (3.22) Хемінгова відстань між першим та другим стовпчиками матриці Δ не менше 2-х. Це означає, що в матриці Δ існує не менше двох рядків для яких перша компонента вектору d дорівнює одиниці, тобто $d = \langle 1, 0 \rangle$ або $d = \langle 1, 1 \rangle$. При цьому, в силу того, що кожному значенню вектору d співвідносяться два можливих рядки матриці Δ може бути дві ситуації: два рядки, в яких відрізняються значення першого та другого стовпчиків є

інверсією одне одного, тобто співвідносяться одному значенню d (наприклад, рядки 101 та 010 є інверсними і співвідносяться значенню $d = \langle 1, 0 \rangle$) або зазначені рядки співвідносяться різним значенням d і, відповідно, не є інверсними (наприклад рядок 101, що співвідноситься з $d = \langle 1, 0 \rangle$ та рядок 011, що співвідноситься з $d = \langle 1, 1 \rangle$). Оскільки кожному значенню вектору d співвідносяться два можливих рядки матриці Δ , то, відповідно, існує не менше двох рядків матриці Δ , які належать множині: $Y_1 = \{ \langle 0, 1, 0 \rangle, \langle 1, 0, 1 \rangle, \langle 0, 1, 1 \rangle, \langle 1, 0, 0 \rangle \}$.

Цілком аналогічно можна зробити висновок про те, що в матриці Δ точно є не менше двох рядків в яких відрізняються перший та третій стовпчики, а значить, друга компонента вектору d дорівнює одиниці: $d = \langle 0, 1 \rangle$ або $d = \langle 1, 1 \rangle$. Рядки, з відмінними значеннями першої та третьої компоненти можуть співвідноситися або з одним із зазначених значень d , або з різними. Відповідно, це означає, що в матриці Δ є не менше двох рядків, які належать множині $Y_2 = \{ \langle 0, 0, 1 \rangle, \langle 1, 1, 0 \rangle, \langle 0, 1, 1 \rangle, \langle 1, 0, 0 \rangle \}$.

За аналогією правомірно стверджувати, що в матриці Δ існує не менше двох рядків, в яких відрізняються другий та третій стовпці, тобто для яких $d = \langle 0, 1 \rangle$ або $d = \langle 1, 0 \rangle$. Вказані рядки можуть бути інверсними, тобто співвідноситися з одним із зазначених значень d , або не інверсними, що означає їх відповідність обом із значень d . З цього випливає факт наявності в матриці Δ не менше двох рядків, які належать множині $Y_3 = \{ \langle 0, 0, 1 \rangle, \langle 1, 0, 1 \rangle, \langle 0, 1, 0 \rangle, \langle 1, 1, 0 \rangle \}$.

Очевидно, що перетин кожної пари множин Y_1 , Y_2 , Y_3 містить рівно дві компоненти, проте перетин всіх трьох множин – жодної, тобто $Y_1 \cap Y_2 \cap Y_3 = \emptyset$. Для того, щоб виконувалася умова (3) потрібно, щоб в матриці Δ існували два рядки які належать Y_1 , два рядки, що належать Y_2 та два рядки, які належать множині Y_3 .

Якщо два наявні в матриці Δ рядки, що належать множині Y_1 не є інверсними, то вони співвідносяться з двома різними значеннями d . У

випадку коли вказані два рядки інверсні по відношенню одне одному, вони співвідносяться з одним значенням d_1 , то вони належать обоє також до множини Y_2 або Y_3 . Якщо вони належать Y_1 і Y_2 , то для виконання (3.22) має існувати ще пара рядків, які належать Y_3 і співвідносяться з $d_2 \neq d_1$. Аналогічна ситуація має місце і коли пара рядків одночасно належать множинам Y_1 і Y_3 .

З наведеного випливає, що для виконання умови (3.23) в матриці Δ мають існувати рядки, які співвідносяться до мінімум двох різних значень d .

В таблиці 3.3 наведені всі можливі варіанти значень пари рядків матриці Δ , які співвідносяться з двома різними значеннями d . В таблиці 3.3 ці пари рядків доповнені рядом, яких складається з самих одиниць і який існує в матриці Δ згідно (3.23).

Таблиця 3.3

Ортогональні підматриці матриці Δ при всіх можливих парах значень d

Можливі пари векторів d	Можливі набори рядків, що співвідносяться парі значень d з одичним рядом			
$\langle 0,1 \rangle, \langle 1,0 \rangle$	0 0 1	0 0 1	1 1 0	1 1 0
	0 1 0	1 0 1	0 1 0	1 0 1
	1 1 1	1 1 1	1 1 1	1 1 1
$\langle 0,1 \rangle, \langle 1,1 \rangle$	0 0 1	0 0 1	1 1 0	1 1 0
	0 1 1	1 0 0	0 1 1	1 0 0
	1 1 1	1 1 1	1 1 1	1 1 1
$\langle 1,0 \rangle, \langle 1,1 \rangle$	0 1 0	1 0 1	0 1 0	1 0 1
	0 1 1	1 0 0	0 1 1	1 0 0
	1 1 1	1 1 1	1 1 1	1 1 1

З даних таблиці 3.3 видно, що кожна матриця, утворена рядками, що співвідносяться з різними d та доповнена рядком, що складається з одиниць є ортогональною.

Таким чином, аналіз даних таблиці 3.3 дозволяє зробити висновок про те, що при існуванні в матриці Δ рядків, що співвідносяться до двох різних d і наявності рядка, що містить одні лише одиниці, матриця Δ завжди містить в собі ортогональну підматрицю. А це, в свою чергу означає, що три втрачені основні пакети даних можуть бути відновлені, що й потрібно було довести.

Як зазначалося вище m резервних пакетів R_1, R_2, \dots, R_m , пропонується формуються у вигляді лінійних комбінацій однойменних бітів основних пакетів у відповідності до формули (3.1). Тому проблема формування резервних пакетів зводиться до віднаходження ефективного методу побудови матриці A , яка задовольняє умовам (3.22), (3.23) і (3.24).

Якщо Хемінгова відстань між будь-якою парою стовпців матриці A має бути згідно (3.22) не меншою 2-х, а кількість одиниць в кожному з стовпців цієї матриці у відповідності з (3.23) має бути не менше 3-х, то в якості стовпців можна вибирати m -розрядні двійкові коди, які містять 3, 5, 7, ..., m одиниць.

Достатньо очевидним є той факт, що Хемінгова відстань між відмінними двійковими кодами, що мають рівну кількість одиниць, дорівнює рівно 2.

Аналогічним, очевидним є те, що Хемінгова відстань між двійковими кодами, з різницею числа одиниць в них не меншою двох, також же не меншою двох.

Оскільки, у відповідності з (3.24), один, наприклад перший, рядок матриці A складається з одиниць, то число n можливих стовпців, що містять 3, 5, 7, ..., m одиниць можна обчислити у вигляді суми кількості перестановок 2-х одиниць в $(m-1)$ -розрядному двійковому коді, кількості перестановок 5-ти одиниць в $(m-1)$ -розрядному двійковому коді, кількості перестановок 7-ми одиниць в $(m-1)$ -розрядному двійковому коді і так далі:

$$n = \sum_{j=1}^v C_{m-1}^{2 \cdot j} \quad (3.25)$$

де $v=(m-1)/2$ при непарному значенні m і $v=m/2-1$ при парному значенні k .

Використовуючи відомі властивості біноміальних коефіцієнтів:

$$\sum_{i=0}^m C_m^i = 2^m, \quad \sum_{i=0}^m (-1)^i \cdot C_m^i = 0,$$

формула (3.25) може бути трансформована до наступного вигляду:

$$n = \sum_{j=1}^v C_{m-1}^{2 \cdot j} = 2^{m-1} - 1. \quad (3.26)$$

З використанням формули (3.26) можна визначити число m резервних пакетів, необхідних для відновлення трьох із n основних пакетів:

$$m \geq \lfloor \log_2(n+1) \rfloor + 2. \quad (3.27)$$

Наприклад, якщо кількість n основних пакетів дорівнює 12: $n=12$, то для відновлення трьох втрачених пакетів потрібно мати $m = 6$ резервних пакетів. Відповідно, матриця A формування резервних пакетів має наступний вигляд:

$$A = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{vmatrix}$$

При збільшенні кількості n основних пакетів ефективність резервування зростає. Наприклад, при $n=120$ кількість резервних пакетів становить 9, тобто 7.5% від кількості основних.

Процедура відновлення втрачених при передачі основних пакетів даних за запропонованим методом може бути ілюстрована наступним прикладом в рамках використання наведеної вище матриці A при $n=12$ і $m=6$.

При втраті, наприклад трьох пакетів, розглядається ситуація, що два з них основні, наприклад п'ятий і сьомий, тобто $v=5$ і $w=7$, а один резервний, наприклад 4-й, тобто $q=4$.

В цьому випадку підматриця Δ матриці A , що складається з стовпців матриці A , які співвідносяться з втраченими основними пакетами та рядків, що співвідносяться з невтраченими резервними пакетами має такий вигляд:

$$\Delta = \begin{vmatrix} a_{1,5} & a_{1,7} \\ a_{2,5} & a_{2,7} \\ a_{3,5} & a_{3,7} \\ a_{5,5} & a_{5,7} \\ a_{6,5} & a_{6,7} \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{vmatrix}$$

Цілком очевидно, що наведена матриця Δ містить в собі ортогональну підматрицю Θ , яка складається з третього та п'ятого рядків матриці Δ :

$$\Theta = \begin{vmatrix} a_{3,5} & a_{3,7} \\ a_{6,5} & a_{6,7} \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}$$

Якщо позначити через Y_3 та Y_6 , відповідно 3-тю та 6-ту складові резервних пакетів Q_3 та Q_6 , то з матриці Θ можна скласти наступну систем лінійних рівнянь:

$$\begin{cases} Y_3 = P_5 \oplus P_7 \\ Y_6 = P_7 \end{cases}$$

Розв'язання цієї системи рівнянь надає формули для відновлення втрачених пакетів:

$$\begin{aligned} P_7 &= Y_6 \\ P_5 &= Y_3 \oplus Y_6 \end{aligned} \quad (3.28)$$

Для того, щоб практично відновити двійкові коди втрачених пакетів потрібно визначити значення складових Y_3 та Y_6 третього та шостого резервних пакеті, які, виходячи з матриці A формуються у вигляді суми за модулем 2 таких складових:

$$\begin{aligned} Q_3 &= P_1 \oplus Y_3 \oplus P_6 \oplus P_9 \oplus P_{10} \\ Q_6 &= P_4 \oplus Y_6 \oplus P_9 \oplus P_{10} \oplus P_{12} \end{aligned}$$

Відповідно, складові Y_3 та Y_6 цих резервних пакетів можуть бути представлені у наступному вигляді:

$$\begin{aligned} Y_3 &= Q_3 \oplus P_1 \oplus P_6 \oplus P_9 \oplus P_{10} \\ Y_6 &= Q_6 \oplus P_4 \oplus P_9 \oplus P_{10} \oplus P_{12} \end{aligned}$$

Підставляючи отримані вирази Y_3 та Y_6 в формулу (3.28) для відновлення втрачених п'ятого і шостого основних пакетів можна отримати вираз для безпосереднього відновлення вказаних пакетів у вигляді суми основних та резервних пакетів, які успішно доставлені:

$$P_7 = Y_6 = Q_6 \oplus P_1 \oplus P_6 \oplus P_9 \oplus P_{10}$$

$$P_5 = Y_6 \oplus Y_3 = Q_3 \oplus Q_6 \oplus P_1 \oplus P_4 \oplus P_6 \oplus P_{12}$$

В підсумку, втрачені при передачі п'ятий та шостий основні пакети можуть бути відновлені шляхом лінійних перетворень над основними та резервними пакетами, які успішно та вчасно доставлені.

3.4. Аналіз проблеми багаторівневого забезпечення надійності передачі даних в мережі Інтернет

Динамічне поширення використання Інтернет на нові сфери застосування потребує якісно нових підходів до вирішення проблеми надійності доставки інформації. В ряді публікацій [54] відмічається, що створені десятки років тому протоколи забезпечення надійності доставки повідомлень транспортного рівня не забезпечують в сучасних умовах ефективного вирішення проблеми для нових сфер застосування глобальних мереж.

Відповідно, підвищені вимоги щодо надійності передачі даних в Інтернеті, які диктуються специфікою нових застосувань мережевих технологій потребують нових рішень, які можуть виходити за рамки існуючих стандартів та протоколів, не відміняючи останні.

В рамках поточних досліджень розвивається популярна концепція забезпечення надійності передачі даних за рахунок збільшення кількості надлишкової інформації. До цього спонукають динамічний прогрес та здешевлення апаратних засобів обчислювальної техніки, які здатна швидко реалізувати складні алгоритми відновлення втрачених даних, а також

зростання технічних характеристик пропускної здатності каналів та інфраструктури транспортування даних по комп'ютерним мережам.

З іншого боку, швидкий прогрес технологій передачі даних в глобальних мережах змінює акценти при оцінці ефективності тих чи інших засобів забезпечення надійності транспортування пакетів. В сучасних умовах динамічного зростання пропускної спроможності каналів передачі даних глобальних мереж знижується значимість критерію кількості резервних пакетів, що використовуються для реконструювання втрачених в процесі передачі інформаційних пакетів. На противагу цьому, в умовах динамічного розширення викори стання Інтернету в якості середовища обміну даними систем комп'ютерного керування технологічними об'єктами в реальному часі об'єктивно збільшується значимість критеріїв ефективності, як обчислювальна і часова складність процедур, пов'язаних з реконструюванням втрачених при транспортування глобальною мережею інформаційних пакетів.

Запропоновані в дисертаційній роботі механізми відновлення затриманих даних, за рахунок вчасно доставлених резервних блоків, ні в якій мірі не заперечують використання протоколів TCP/IP по захисту даних від помилок та втрат, оскільки діють на іншому мережовому рівні.

Існуючі механізми виправлення помилок при передачі пакету чи відновлення втрачених пакетів шляхом їх повторної передачі на транспортному рівні, в певних умовах, вносять значну затримку. Зокрема, при використанні супутникових каналів, які характеризуються високим рівнем втрат, та великими значеннями RTT (Round Triple Time), затримка, зумовлена роботою протоколів транспортного рівня може становити 100-300 мс. Запропоновані механізми дозволяють відновити втрачені дані швидше, за 5-10 мс.

Крім того, існують ситуації коли протоколи виправлення помилок та втрат транспортного рівня використовувати не можливо. Саме для цих

ситуацій запропонований механізм дозволяє відновлювати втрачену інформацію. Реалізація протоколів TCP/IP щодо виправлення помилок на термінальному рівні не завжди забезпечується відповідними апаратними засобами.

Проте, для більшої частини мереж протоколи виправлення помилок транспортного рівня працюють швидше. Разом з тим, як зазначено вище, існує доволі широкий клас мереж і застосувань, для яких запропоновані механізми забезпечують менший час відновлення втрачених даних, що й визначає їх більшу ефективність для вказаних застосувань.

Таким чином, запропоновані процеси відновлення даних за рахунок передачі резервних блоків даних не відмінюють процесів і процедур, передбачені моделлю OSI та стеком TCP/IP, і виконуються паралельно з ними на різних рівнях і різними процесорними засобами. По закінченні відновлення даних за запропонованими методами вони використовуються не чекаючи закінчення процесів, передбачених моделлю OSI та стеком TCP/IP.

Висновки до розділу 3

За результатами досліджень, направлених на підвищення ефективності оперативного реконструювання втрачених чи затриманих понад критичний час пакетів даних в глобальних мережах, за рахунок урахування статистичних характеристик їх втрат, а також специфічних особливостей цих втрат для різних класів практичних застосувань характеру, які складають третій розділ дисертаційної роботи можна зробити наступні висновки:

1. В якості основного резерву підвищення ефективності відновлення пакетів даних в глобальних мережах досліджено урахування специфічної особливості їх втрат для широкого кола практичних застосувань, а саме: втрат “пачок” пакетів в потоці, а також статистики їх затримок. Відповідно, вирішення наукової задачі підвищення ефективності оперативного

реконструювання втрачених пакетів даних вирішено за рахунок створення спеціалізованих та орієнтованих на певне коло практичних застосувань засобів відновлення пакетів в глобальних мережах.

2. Теоретично обґрунтовано, розроблено та досліджено метод відновлення “пачок” пакетів та невеликої кількості окремих пакетів, який відрізняється способом побудови матриці формування резервних пакетів, число яких, за рахунок спеціалізації на визначеному домінуючому типі втрат пакетів, зменшено у порівнянні з відомими методами. Теоретичними та експериментальними дослідженнями показано, що розроблений метод, за рахунок його орієнтації на визначеному домінуючому типі втрат інформаційних пакетів дозволяє, в середньому на 30-40% скоротити кількість резервних пакетів, що передаються по глобальним мережам. Запропонований в рамках методу спосіб побудови матриці формування резервних пакетів забезпечує, при цьому скорочення часу відновлення втраченої “пачки” інформаційних пакетів в 2-4 раз, в залежності від довжини “пачки”, за рахунок розрідження матриці, що має наслідком зменшення обчислювальної складності операцій, пов’язаних з їх реконструюванням.

3. Вдосконалено метод відновлення затриманих при передачі інформаційних пакетів даних, за рахунок використання системи пріоритетів при виборі компонентів матриці формування обмеженої кількості резервних пакетів з урахуванням статистичних характеристик затримок транспортування пакетів, що дозволяє підвищити ймовірність можливості відновлення втраченої чи затриманої інформації і тим самим прискорити передачу даних в глобальних мережах.

4. Запропоновані в дисертаційній роботі механізми відновлення частини затриманих даних, за рахунок вчасно доставлених резервних блоків, ні в якій мірі не заперечують використання протоколів TCP/IP по захисту даних від помилок та втрат, оскільки діють на іншому мережовому рівні. Розроблені процедури процеси відновлення даних за рахунок передачі резервних блоків

даних не відміняють процесів і процедур, передбачені моделлю OSI та стеком TCP/IP, і виконуються паралельно з ними на різних рівнях і різними процесорними засобами. По закінченні відновлення даних за запропонованими методами вони використовуються не чекаючи закінчення процесів, передбачених моделлю OSI та стеком TCP/IP.

5. Використання результатів роботи при резервуванні та відновленні втрачених чи затриманих інформаційних пакетів в глобальних мережах дозволяє прискорити доставку даних. Це має велике практичне значення для систем моніторингу стану віддалених об'єктів та комп'ютерного управління ними в реальному часі, які використовують глобальні мережі в якості середовища передачі даних.

Р О З Д І Л 4

РОЗРОБКА ТЕХНОЛОГІЧНИХ АСПЕКТІВ ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ

Ефективність резервування та відновлення втраченої інформації при її віддаленому зберіганні на рознесених сховищах, а також під час передачі по глобальним мережам значною мірою залежить від технологічних аспектів розв'язання системи лінійних рівнянь для визначення обчислювальної процедури відновлення. Важливою задачею дисертаційного дослідження є розробка ефективної технології відновлення втрачених блоків даних за розробленими методами, здатної забезпечити високу швидкодію процесу реконструювання даних за рахунок вибору оптимального, в сенсі мінімуму кількості потрібних для цього пересилок даних по глобальним мережам та мінімуму обчислювальних операцій по безпосередньому реконструюванню, варіанту відновлення, а також використання передобчислень, яке дозволяє виключити з процесу обчислення, пов'язані з розв'язанням систем рівнянь.

Тому важливою задачею досліджень є розробка технології відновлення втрачених блоків даних за розробленими методами, здатної забезпечити високу технологічну ефективність процесу відновлення втрачених даних на обчислювальній платформі користувача.

4.1 Аналіз чинників технологічної ефективності процесів відновлення втрачених даних

Ефективність запропонованих в двох попередніх розділах методів прискореного відновлення втрачених даних значною мірою залежить від технологічних аспектів їх практичної реалізації.

На етапі технічної реалізації, тобто при фіксації функціональних параметрів, пов'язаних зі здатністю відновлювати втрачені дані, базовими критеріями ефективності виступають:

- час відновлення втрачених даних;
- об'єм обчислювальних ресурсів, потрібних для відновлення втрачених даних;
- об'єм мережових ресурсів для відновлення втрачених даних;
- об'єм пам'яті для реалізації функцій відновлення втрачених даних.

В першому розділі було вказано на існування суттєвої відмінності між технологічними процесами корекції помилок передачі даних при застосуванні завадостійких кодів та відновлення втрачених блоків при їх віддаленому зберіганні.

Основна відмінність запропонованих технологій відновлення даних від тих, які застосовуються при корекції даних з застосуванням завадостійких кодів полягає в тому, що розв'язання лінійного рівняння безпосередньо не відновлює дані, а лише задає математично процедуру реконструювання даних. Сам процес відновлення передбачає транспортування по мережі блоків даних, потрібних для реконструювання втрачених блоків, їх буферизацію і виконання обчислювальних операцій по безпосередньому відновленню втрачених блоків.

Відповідно, відомі технології відновлення втрачених даних на основі корегуючих кодів допускають можливість попереднього обчислення відновленого коду для всіх можливих спотворень блоку даних. Ці обчислення, за звичай, оформлюються у вигляді стандартної таблиці розташування [44, 45].

Задача відновлення блоків даних, які зберігаються на віддалених системах не допускає подібного вирішення задачі відновлення, оскільки при реконструюванні блоків, доступ до яких постійно чи тимчасово втрачено, потрібної для їх відновлення інформації ще немає: вона зберігається віддалено, як і втрачені блоки. Тобто, спочатку потрібно організувати доставку інформації, потрібної для відновлення втрачених даних на обчислювальну систему користувача, де здійснюється процес відновлення.

Іншими словами, основна відмінність поставленої задачі реконструювання втрачених при віддаленому зберіганні даних від традиційної корекції помилок полягає в тому, що матриці не використовуються для безпосереднього відновлення втрачених даних. Вони лише визначають процедуру відновлення [76, 77].

Як було показано в попередніх розділах дисертації, технологічно процес відновлення втрачених блоків полягає в розв'язанні системи лінійних рівнянь, коефіцієнти котрої утворені елементами ортогональної підматриці Θ матриці A . При цьому, стовбці матриці Θ утворені з компонентів стовпців матриці A , які співвідносяться з втраченими при передачі основними пакетами, а рядки – компонентами рядків, що співвідносяться з невтраченими при передачі резервними пакетами.

Навіть при втраті граничної для відновлюючої здатності h кількості інформаційних блоків, в стовпцях матриці A , які співвідносяться з втраченими блоками даних може існувати декілька ортогональних підматриць Θ .

Наприклад, якщо кількість n інформаційних блоків дорівнює 12-ти: $n=12$, число блоків, що можуть бути гарантовано відновлені $h=4$, то число m резервних блоків становить 10: $m=10$. Матриця A формування резервних блоків, яка гарантує відновлення $4=x$ інформаційних блоків має наступний вигляд:

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}. \quad (4.1)$$

Якщо припустити, що втрачені два перші і два останні інформаційні блоки, то в підматриці А, яка утворена двома першими і двома останніми її стовпцями, можна виділити декілька ортогональних підматриць, що мають чотири рядки і чотири стовпці. Зокрема, перші чотири рядки підматриці А утворюють ортогональну підматрицю Θ_1 наступного виду:

$$\Theta_1 = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{vmatrix}$$

Розв'язок відповідної системи лінійних булевих рівнянь дозволяє отримати вирази для відновлення втрачених інформаційних блоків даних:

$$B_1 = R_1 \oplus R_2 \oplus R_3 \oplus R_4 \oplus B_6 \oplus B_7 \oplus B_8 \oplus B_{10}$$

$$B_2 = R_2 \oplus R_3 \oplus R_4 \oplus B_4 \oplus B_6 \oplus B_7 \oplus B_{10}$$

$$B_{11} = R_1 \oplus R_2 \oplus R_3 \oplus B_3 \oplus B_5 \oplus B_7 \oplus B_8$$

$$B_{12} = R_1 \oplus R_3 \oplus R_4 \oplus B_3 \oplus B_5 \oplus B_8 \oplus B_{10}$$

З наведених формул видно, що кількість операцій логічного додавання, необхідних для відновлення п'яти втрачених блоків становить 25. Число блоків даних (інформаційних та резервних), які використовуються для відновлення втрачених 4-х інформаційних блоків становить 11 (4 резервних R_1, R_2, R_3, R_4 та 7 основних: B_3, B_8, B_{10}). Це означає, що для реконструювання втрачених блоків потрібно транспортувати на обчислювальну платформу користувача одинадцять невтрачених блоків даних, які зберігаються на віддалених рознесених системах.

Якщо вибрати іншу ортогональну систему, наприклад Θ_2 , отриману другим, третім, шостим та дев'ятим рядками підматриці А:

$$\Theta_2 = \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix},$$

то розв'язок відповідної системи лінійних булевих рівнянь дозволяє отримати інший математичний вирази для відновлення втрачених інформаційних блоків B_1, B_2, B_{11}, B_{12} :

$$B_1 = R_2 \oplus R_9 \oplus B_5 \oplus B_7 \oplus B_{10}$$

$$B_2 = R_6 \oplus R_9 \oplus B_5 \oplus B_6 \oplus B_7$$

$$B_{11} = R_3 \oplus R_6 \oplus B_4 \oplus B_6$$

$$B_{12} = R_9 \oplus B_5 \oplus B_6 \oplus B_8 \oplus B_{10}$$

Цілком очевидно, що обчислювальна реалізація наведених формул потребує 15 операцій логічного додавання, тобто на 67% менше, ніж при використанні підматриці Θ_1 . Для відновлення втрачених блоків B_1, B_2, B_{11}, B_{12} в цьому варіанті потрібно транспортувати на обчислювальну платформу користувача, де здійснюється безпосереднє відновлення, 10 блоків даних (4 резервних: R_2, R_3, R_6, R_9 та 6 основних $B_4, B_5, B_6, B_7, B_8, B_{10}$).

Наведений приклад свідчить, що відновлення втрачених інформаційних блоків може здійснюватися за різними варіантами, які потребують суттєво різних об'ємів обчислень для реалізації та різної кількості числа пересилок даних, які використовуються в процесі реконструювання.

Виходячи з наведеного вище, для високотехнологічного відновлення втрачених блоків даних потрібно ефективно вирішити дві задачі:

- транспортування блоків даних, які потрібні для відновлення втрачених даних на комп'ютерну систему користувача, де здійснюються операції по реконструюванню втрачених блоків даних;
- виконання безпосереднього відновлення шляхом здійснення операцій логічного додавання над отриманими з мережі блоками.

Найбільші резерви для прискорення відновлення втрачених блоків на комп'ютерній системі користувача містяться в рамках етапу транспортування потрібних для цього блоків даних по глобальній мережі.

Зокрема, час транспортування потрібних для відновлення блоків може бути зменшений за рахунок:

- як було показано в другому розділі дисертації, дозволяє скоротити кількість використання такого способу відновлення, який потребує меншої кількості блоків, доступ до яких не втрачено, тобто за рахунок меншої кількості блоків, які потрібно транспортувати;

- вибору такого способу відновлення, який використовує блоки даних, що мають більшу доступність, тобто, з урахуванням поточного трафіку глобальної мережі та завантаженості вузлів зберігання, можуть бути доставлені за менший час.

Практичне використання першої з наведених можливостей може бути реалізоване достатньо просто шляхом вибору того, способу відновлення, для якого відповідна система лінійних рівнянь містить найменше число блоків даних потрібних для реконструювання конкретної комбінації втрачених блоків. Реалізація другого резерву прискорення транспортування потрібних для відновлення непошкоджених блоків технологічно значно більш складна в силу того, що потребує постійного моніторингу стану вузлів віддаленого зберігання даних та трафіку по маршрутам їх доставки.

Виходячи з цього, в якості основного чинника при виборі способу відновлення втрачених блоків прийнята кількість блоків даних, необхідних для реконструкції втраченої інформації. При відновленні пакетів, втрачених в процесі їх передачі по глобальній мережі, вся інформація для виконання відновлення є на стороні приймача, тому час реконструювання визначається лише кількістю пакетів, які використовуються при цьому, оскільки час реалізації обчислень пропорційний вказаній кількості.

З іншого боку, використання мінімального числа блоків для відновлення втрачених блоків забезпечує мінімум кількості обчислювальних операцій логічного давання для безпосереднього реконструювання інформації, до якої втрачено доступ. Таким чином, прийнята в основі розробки стратегія використання мінімально можливої кількості неушкоджених блоків даних забезпечує високу швидкодію процесу реконструювання даних за рахунок

вибору оптимального, в сенсі мінімуму кількості потрібних для цього операцій, варіанту відновлення, а також використання передобчислень, яке дозволяє виключити з процесу відновлення обчислення, пов'язані з розв'язанням систем лінійних рівнянь.

4.2 Розробка способу прискореного відновлення втрачених блоків на основі попередньо створених таблиць специфікацій

В математичному плані процедура відновлення m втрачених блоків даних передбачає виділення з матриці A ортогональної підматриці Θ розміром $m \times m$, стовпці якої співвідносяться з втраченими інформаційними блоками. Виділена матриця утворює систему лінійних рівнянь, розв'язання якої формує процедуру реконструювання втрачених блоків. Як показано вище, може існувати декілька варіантів виділення на матриці A ортогональної підматриці, які відрізняються кількістю невтрачених блоків, інформація яких використовується для безпосереднього відновлення втрачених блоків. Як було показано вище, теоретично, умова відновлення втрачених пакетів в процесі передачі h основних пакетів, номери яких утворюють множину Ω , полягає в наявності в трансформованій матриці L ортогональної підматриці Θ .

Таким чином, в технологічному плані процес відновлення втрачених інформаційних блоків полягає в розв'язання системи лінійних рівнянь, коефіцієнти якої утворені компонентами матриці Θ . Аналіз трансформованої матриці L на предмет виявлення в ній ортогональної підматриці Θ , формування на основі матриці Θ системи лінійних рівнянь з подальшим її розв'язанням потребує певних обчислювальних і часових ресурсів, що критично для відновлення втрачених даних в реальному часі.

Кількість q варіантів відновлення h втрачених блоків даних залежить від загального числа n інформаційних блоків та числа m резервних блоків, які використовуються для реконструювання. Кількість варіантів відновлення

втрачених блоків даних значно зростає, якщо кількість блоків, що реконструюються помітно менша за граничне значення.

Наприклад, для матриці (4.1), яка орієнтована на гарантоване відновлення не більше 4-х втрачених блоків з 12-ти ($n=12$) при використанні 10-ти резервних блоків ($m=10$) при відновленні 4-х втрачених інформаційних блоків ($h=4$) існує, в середньому, 6 ($q=6$) варіантів відновлення, які потребують транспортування від 10 до 12-ти непошкоджених блоків даних та від 15 до 28 обчислювальних операцій логічного додавання блоків. При використанні цієї ж матриці (4.1) для реконструювання 3-х втрачених ($h=3$) існує, в середньому 24 варіанти відновлення ($q=24$), які потребують доставки, в середньому від 8 до 12 непошкоджених блоків даних та від 6 до 16-ти обчислювальних операцій логічного додавання блоків. При відновлення пари втрачених блоків з використанням матриці (4.1) існує 3 варіанти відновлення, в яких число блоків, потрібних для реконструкції лежить в межах від 10 до 12, а число операцій – від 9 до 13. При реконструюванні одного втраченого блоку потрібно, в середньому транспортувати 8 блоків і виконувати 6 операцій логічного додавання блоків даних, доступ до яких не втрачено.

В таблиці 4.1 наведені експериментально отримані дані щодо середньої кількості варіантів відновлення різного числа втрачених блоків даних для матриць, які орієнтовані на гарантоване реконструювання до 4-х інформаційних блоків даних. В таблиці 4.1 наведені також дані щодо мінімальної та максимальної кількості непошкоджених блоків даних, які потрібно транспортувати для здійснення реконструкції втрачених блоків даних. Аналогічні дані наведені і для кількості операцій логічного додавання, що виконуються над блоками даних в процесі безпосереднього відновлення інформації.

Аналіз наведених в таблиці 4.1 даних показує, що за рахунок оптимізації вибору варіанту відновлення втрачених блоків за критеріями мінімуму кількості блоків, які потрібно транспортувати по глобальній мережі можна

прискорити процес відновлення даних, в середньому, на 28.4%, причому ефективність такої оптимізації зростає зі збільшенням кількості блоків даних, які зберігаються віддалено.

Таблиця 4.1

Параметри варіантів відновлення втрачених блоків для різної їх кількості (h) в залежності від параметрів матриці формування резервних блоків, орієнтованої на гарантовану реконструкцію до 4-х блоків (за експериментальними даними)

n	m	h	q	Кількість блоків, які потрібно доставити		Кількість операцій лог. додавання блоків	
				мінімум	максимум	мінімум	максимум
6	7	2	3	5	6	8	10
		3	7	5	6	11	12
		4	3	6	6	12	17
7	7	2	3	5	7	8	10
		3	6	5	7	12	16
		4	4	6	7	15	20
8	8	2	3	5	8	9	12
		3	15	6	8	12	17
		4	4	7	8	16	22
14	10	2	3	8	12	6	16
		3	24	10	12	9	18
		4	6	10	12	15	28
16	12	2	3	10	16	18	45
		3	36	12	16	21	52
		4	15	13	16	24	62
32	18	14	3	16	32	12	60
		3	38	22	32	28	72
		4	22	24	32	34	86

Інший важливий висновок за результатами проведених експериментальних досліджень, які часткового відображені в таблиці 4.1, полягає в тому, що число лінійних ортогональних систем відносно невелике і їх розв'язки доволі просто перебрати з оформленням результатів спеціальними таблицями. Це означає, що основні ресурси при реалізації відновлення втрачених блоків витрачаються на виділення самих систем ортогональних рівнянь.

Якщо є h втрачених блоків, то перше рівняння ортогональної системи може бути вибране 2^h-1 способами, друге рівняння має бути відмінним від першого вибраного, тобто існує 2^h-2 способів його вибору. Третє рівняння має бути відмінним від першого, другого на їх суми, тобто вкладатися в 2^h-3 варіанти, четверте рівняння має не співпадати з 2^3-1 лінійними комбінаціями перших трьох вибраних рівнянь. Таким чином, можна говорити, що загальна кількість K ортогональних бінарних рівнянь обчислюється у вигляді:

$$K = \frac{1}{h!} \cdot \prod_{j=1}^h (2^h - 2^j). \quad (4.2)$$

За формулою (4.2) для $h=3$ значення $K=28$, а для $h=4$ число ортогональних систем $K=840$. Наведені числа є відносно невеликими і це означає, що виявлення ортогональності підматриць для кожного конкретної конфігурації втрачених інформаційних блоків може бути реалізовано з використанням спеціальних таблиць, в яких зберігаються всі можливі види ортогональних підматриць для найбільш уживаних на практиці значень $h=3$ та $h=4$.

Оскільки виділення з матриці A ортогональної підматриці Θ та її подальше розв'язання потребує певних часових ресурсів, що не завжди є прийнятним для систем, що працюють в реальному часі, пропонується табличний спосіб відновлення втрачених пакетів.

Пропонований спосіб передбачає на етапі налаштування системи створити таблиці, які визначають для кожної комбінації втрачених блоків (інформаційних та резервних) перелік невтрачених блоків, потрібних для реконструювання та специфікацію, яка описує обчислювальні операції по відновленню втрачених блоків.

Відповідно, на етапі налаштування потрібно вибрати ту ортогональну матрицю, яка дозволяє оптимізувати процес відновлення за критеріями мінімуму блоків, що мають бути транспортованими для відновлення втрачених блоків та обчислювальної складності операцій реконструювання.

Перебір варіантів вибору ортогональних матриць потребує на етапі налаштування системи найбільше часу. Для його скорочення доцільно використовувати схеми неповного перебору [34]. Було експериментально досліджено декілька таких схем. Проведені дослідження показали, що найбільш ефективною є схема, яка передбачає таку послідовність дій:

1. Для заданого набору $\Omega = \{\eta_1, \eta_2, \dots, \eta_h\}$, $\forall l \in \{1, 2, \dots, h\}$: $h_l \in \{1, 2, \dots, n\}$ номерів втрачених інформаційних блоків з матриці A формується підматриця H' , яка складається зі стовпців матриці A , номери яких належать набору Ω .
2. З матриці H' видаляються рядки, номери яких співвідносяться з номерами резервних блоків даних, доступ до яких втрачено. В результаті отримується матриця H , в якій потрібно віднайти ортогональну матрицю Θ .
3. Обчислюється значення γ об'єму первинного перебору у вигляді: $\gamma = \sqrt{q}$.
Лічильник j первинного перебору встановлюється в нуль: $j = 0$.
4. Вибирається підматриця Λ розміром $h \times h$ з матриці H .
5. Здійснюється перевірка вибраної підматриці Λ за описаною вище методикою, яка дозволяє крім визначення ортогональності отримати розв'язання відповідної системи лінійних рівнянь. Якщо матриця Λ ортогональна, то лічильник віднайдених ортогональних систем збільшується на одиницю: $j = j + 1$. Інакше, перехід на п.8.
6. Для віднайденої ортогональної системи Θ_j за таблицями визначається математичні вирази, згідно з якими здійснюється процес відновлення. З виразів визначається кількість η_j інформаційних та резервних блоків, які потрібно транспортувати по глобальній мережі для відновлення втрачених блоків. Якщо $j = 1$ або кількість блоків, які підлягають доставці менша за максимальне значення: $\eta_j < \mu$, то $\mu = \eta_j$ і опис математичних виразів для відновлення втрачених блоків фіксується в поточній специфікації.
7. Якщо $j > \gamma$, тобто первинний перебір закінчено, то перехід на кінець.
8. Здійснюється повернення на повторне виконання п. 4.

Проведені експериментальні дослідження запропонованого алгоритму показали, що він в 92% випадків забезпечує віднаходження оптимального в сенсі мінімуму блоків даних, які потрібно доставляти, варіанту відновлення, при тому, що об'єм перебору варіантів зменшено практично в $2 \cdot \sqrt{q}$ рази.

Запропонований алгоритм реалізується, як вказувалося вище, на етапі налаштування системи.

Таким чином, для прискорення процесу відновлення втрачених блоків даних, пропонується всі зазначені вище допоміжні дії виконати на етапі налаштування системи для всіх можливих локалізацій втрачених пакетів. Отримані результати пропонується організувати у вигляді спеціальних таблиць, які, в залежності від локалізації втрачених пакетів, містять специфікацію операцій по відновленню втрачених даних, або інформацію про те, що втрачені пакети не можуть бути відновлені. Відповідно, вказані вище процедури трансформації матриці A , віднаходження в ній ортогональної підматриці Θ , складання та розв'язання системи лінійних рівнянь, можуть бути зведені до читання специфікації відновленні втрачених пакетів з табличної пам'яті. Таке рішення цілком дозволяє реалізувати вказаний перелік дій в режимі реального часу.

Іншими словами, запропонований спосіб прискореного відновлення втрачених даних полягає в тому, що на етапі налаштування системи виявляються всі можливі варіанти втрати пакетів, для кожного з цих варіантів здійснюється віднаходження ортогональної підматриці Θ , її розв'язання з фіксацією в табличній пам'яті формалізованого представлення специфікації дій по відновленню втрачених інформаційних блоків.

При використанні m резервних пакетів можливо відновити не більше, ніж m інформаційних блоків. Тобто, таблиця має надавати специфікацію відновлення втрачених пакетів, якщо їх кількість не перевищує m .

Важливим технологічним моментом використання таблиці передобчислень є розробка алгоритму її адресації по заданому коду L

локалізації втрачених блоків даних. Код L складається з $n+m$ бітів, кожен з яких співвідноситься з інформаційним або резервним блоком і дорівнює одиниці, якщо відповідний пакет втрачено.

Зрозуміло, що кількість δ_j можливих локалізацій втрат j пакетів (кількість можливих кодів L , що містить рівно j одиниць) дорівнює C_{n+m}^j , де $j \in \{1, 2, \dots, m\}$. Специфікація відновлення i -того пакету, $i \in \{1, 2, \dots, n+m\}$ є $(n+m)$ -бітовим кодом $C = \{c_1, c_2, \dots, c_{n+m}\}$, $\forall i \in \{1, 2, \dots, n+m\}$: $c_i \in \{0, 1\}$, одиничні компоненти якого вказують на пакети, сума яких дорівнює втраченому. Іншими словами, втрачений блок B_i може бути відновлено, з використанням специфікації у відповідності з наступною формулою:

$$B_{ic} = \bigoplus_{l=1}^n c_l \cdot B_l \oplus \bigoplus_{u=0}^m c_{n+u} \cdot R_u. \quad (4.3)$$

Кількість специфікацій визначається числом комбінацій втрачених інформаційних та резервних блоків з виключенням комбінацій втрат лише резервних блоків : при втраті u блоків з загальної кількості n основних і m резервних блоків, кількість комбінацій за участю інформаційних блоків дорівнює $C_{m+n}^u - C_m^u$. Для виправлення кожного інформаційного блоку потрібно, як було зазначено вище, $m+n$ біт. Відповідно, загальний об'єм пам'яті V_u , потрібний для зберігання специфікацій відновлення інформаційних блоків за умови втрати u (інформаційних та резервних) визначається наступною формулою:

$$V_u = \sum_{j=1}^u C_n^j \cdot C_m^{u-j} \cdot j \cdot (m+n). \quad (4.4)$$

Відповідно, загальна кількість N_c специфікацій відновлення втрачених основних блоків, що містяться в таблиці, за умови що їх кількість не перевищує k , визначається такою формулою:

$$N_c = \sum_{u=1}^k \sum_{j=1}^u C_n^j \cdot C_m^{u-j} \cdot j. \quad (4.5)$$

Відповідно, об'єм V пам'яті в бітах, яку займає таблиця специфікацій відновлення основних блоків даних, визначається формулою:

$$V = N_c \cdot (m + n) = (m + n) \cdot \sum_{u=1}^k \sum_{j=1}^u C_n^j \cdot C_m^{u-j} \cdot j. \quad (4.6)$$

Наприклад, при $n = 8$, для гарантованого відновлення інформаційних блоків, за умови, що загальна кількість втрачених блоків не перевищує 4-х ($k=4$) потрібно 8 резервних блоків $m=8$. Згідно з формулою (4.5) для табличного відновлення цих блоків за запропонованим табличним способом потрібно загалом створити 4608 специфікацій. Об'єм пам'яті для зберігання відповідної таблиці специфікацій становить у відповідності з (4.6) 72738 біт або 9216 байтів.

Дані про кількість специфікацій та потрібний для їх зберігання об'єм пам'яті для різної кількості інформаційних блоків за умови їх гарантованого відновлення при втраті не більше трьох блоків наведено в таблиці 4.2.

Таблиця 4.2

Залежність кількості специфікацій гарантованого відновлення всіх основних пакетів за умови втрати не більше трьох переданих пакетів

Кількість n основних пакетів	Мінімальна кількість m резервних пакетів	Число N специфікацій	Об'єм V пам'яті специфікацій, байт
7	5	469	703
15	6	3165	8308
31	7	21824	$103 \cdot 10^3$
63	8	156618	$139 \cdot 10^4$
127	9	$116 \cdot 10^4$	$198 \cdot 10^5$

Аналіз даних, наведених в таблиці 4.3 свідчить про те, що об'єми пам'яті таблиць специфікацій лежать у межах можливості технічної реалізації навіть з використанням обчислювальних платформ відносно невеликої потужності. Це доводить, що запропонований спосіб може бути ефективно використаний широким колом користувачів сервісу віддаленого зберігання інформації з використанням хмарних технологій.

Проведені експериментальні дослідження показали, що основний час процесу відновлення витрачається на транспортування блоків даних з віддалених сховищ. Ці блоки потрібні для безпосередньої реконструкції втрачених блоків.

Запропонований спосіб формування специфікацій на етапі налаштування системи може бути ілюстровано наступним прикладом. Нехай кількість інформаційних блоків становить $n = 8$, кількість резервних – $m = 4$. Матриця A , що описує формування резервних блоків має наступний вигляд:

$$A = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{vmatrix}$$

Відповідно, вектори формування резервних блоків з основних мають такий вигляд: $\lambda_1 = [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0]$, $\lambda_2 = [1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1]$, $\lambda_3 = [0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1]$, $\lambda_4 = [0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1]$. Це означає, що резервні блоки даних формуються наступним чином:

$$R_1 = B_1 \oplus B_2 \oplus B_3 \oplus B_7$$

$$R_2 = B_1 \oplus B_4 \oplus B_5 \oplus B_7 \oplus B_8$$

$$R_3 = B_2 \oplus B_4 \oplus B_6 \oplus B_7 \oplus B_8$$

$$R_4 = B_3 \oplus B_5 \oplus B_6 \oplus B_8$$

Для вектору L втрачених пакетів, що має такий вигляд: **$[0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ | \ 0 \ 0 \ 0 \ 1]$** , специфікація відновлення в рамках поточного прикладу формується наступним чином. Аналіз вектору L показує, що він відображає ситуацію втрати 3-х основних блоків B_3 , B_5 та B_8 , а також одного резервного блоку даних - R_4 . Тоді, з матриці A виділяється підматриця H , що складається зі стовпців, які співвідносяться зі втраченими інформаційними блоками даних:

$$H = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$

На наступному етапі з матриці H видаляється рядок, який співвідноситься з втраченим 4-м резервним блоком. В результаті отримується матриця H' , розмірністю 3×3 , яка являє собою ортогональну матрицю Q :

$$H' = Q = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix}$$

Таким чином, вектори $\gamma_1, \gamma_2, \gamma_3$, що відповідають логічній сумі тих інформаційних блоків, які втрачено і які входять до відповідного за індексом резервного пакету, можна записати у наступному вигляді:

$$\begin{cases} \gamma_1 = B_3 \\ \gamma_2 = B_5 \oplus B_8 \\ \gamma_3 = B_8 \end{cases}$$

Розв'язок наведеної вище системи лінійних булевих рівнянь відносно B_3, B_5 та B_8 має наступний вигляд:

$$B_3 = \gamma_1$$

$$B_5 = \gamma_2 \oplus \gamma_3$$

$$B_8 = \gamma_3$$

Після підстановки в $\gamma_1, \gamma_2, \gamma_3$, позначень тих інформаційних блоків, які не втрачено, вирази для реконструювання втрачених інформаційних блоків на основі невтрачених основних і резервних блоків може бути представлена у наступному кінцевому вигляді:

$$B_3 = R_1 \oplus B_1 \oplus B_2 \oplus B_7$$

$$B_5 = R_2 \oplus R_3 \oplus B_1 \oplus B_2 \oplus B_6$$

$$B_8 = R_3 \oplus B_2 \oplus B_4 \oplus B_6 \oplus B_7$$

Відповідно, специфікація для відновлення втрачених блоків даних має наступний вигляд:

$$s_1 = [1\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ |\ 1\ 0\ 0\ 0]$$

$$s_2 = [1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ |\ 0\ 1\ 1\ 0]$$

$$s_3 = [0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ |\ 0\ 0\ 1\ 0]$$

$$s_4 = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ |\ 0\ 0\ 0\ 0]$$

Сформована описаним вище способом специфікація зберігається в табличній пам'яті за визначеною адресою. Формування специфікацій здійснюється на етапі налаштування системи і не є критичним за часом обчислювальної реалізації. Сформовані в результаті специфікації зберігаються в пам'яті і використовуються для швидкого відновлення втрачених блоків.

За результатами експериментальних досліджень показано, що розроблений спосіб технологічної реалізації відновлення втрачених блоків при їх віддаленому зберіганні дозволяє на 10-15% прискорити обчислювальну реалізацію реконструювання втрачених блоків в порівнянні з відомими технологіями за рахунок:

- оптимізації вибору варіанту за критерієм мінімуму кількості блоків даних, які використовуються для реконструювання втрачених блоків;
- застосування передобчислень, що виключає з процесу безпосереднього відновлення обчислень, пов'язаних з розв'язанням систем рівнянь.

Суттєво новими елементами запропонованого способу відновлення блоків даних на основі таблиць специфікацій від відомих таблиць стандартного розташування є те, що таблиці специфікації дозволяють оптимізувати процедуру відновлення за критерієм мінімуму блоків, що транспортуються для відновлення втрачених блоків, що забезпечує мінімальний час реконструювання втрачених даних, а також використання perfect хеш-адресації таблиці, що також дозволяє скоротити час пошуку в таблиці потрібної специфікації.

4.3 Організація швидкого пошуку в таблиці специфікацій

Швидкість відновлення втрачених інформаційних блоків при застосуванні запропонованого способу значною мірою залежить від часу пошуку потрібної специфікації в таблиці. Для цього потрібно визначити ефективний спосіб адресації таблиці специфікацій реконструювання втрачених інформаційних блоків.

Адресацію таблиці специфікацій відновлення втрачених інформаційних блоків даних пропонується організувати таким чином. В якості заданої інформації для відновлення втрачених блоків розглядається код L бінарного вектору доступності блоків. Одиничні компоненти цього вектору вказують на блоки, доступ до яких втрачено.

Для заданого коду L визначається кількість одиниць в ньому – $E(L)$, а також порядковий номер $W(L)$ серед кодів, що містять $E(L)$ одиниць. Адресу A_L першої з специфікацій, що співвідносяться з заданим кодом L пропонується обчислювати у відповідності до формули:

$$A_L = B(E(L)) + W(L) \cdot E(L),$$

де $B(E(L))$ – зміщення початку специфікацій, що описують відновлення $E(L)$ втрачених пакетів. Наприклад, при $n = 8$ і $k = 4$; $B(1) = 0$, $B(2) = 12$, $B(3) = 12 + 66 \cdot 2 = 144$, $B(4) = 144 + 220 \cdot 3 = 804$.

Для обчислення зміщення адреси специфікацій в табличній пам'яті коду L потрібно виконати його трансформацію в порядковий номер $W(L)$ на множині $(n+m)$ -розрядних кодів, які містять $E(L)$ одиниць. Наприклад, при $n = 8$ і $k = 4$ код $L = 1111\ 0000\ 0000$ може бути трансформований в порядковий номер 0, код $1110\ 1000\ 0000$ – в порядковий номер 1. Відповідно, для коду $L = 0000\ 0000\ 1111$ код $W(L)$ порядкового номеру становить $W(L) = C_{12}^4 - 1 = 494$.

Для обчислення порядкового номеру $W(L)$ коду L , що містить $E(L)$ одиниць пропонується наступний алгоритм.

1. Номер i поточного біту коду L встановити в одиницю: $i = 1$, код r результату встановити в нуль: $r = 0$, змінній g присвоїти значення, що дорівнює кількості одиниць $E(L)$ в коді L : $g = E(L)$.

2. Якщо поточний біт l_i коду L дорівнює одиниці, то виконати декремент g : $g = g - 1$; інакше, якщо $l_i = 0$, додати до коду r результату C_{n+m-1}^{g-1} : $r = r + C_{n+m-1}^{g-1}$.

3. Зробити перехід на наступний біт коду L : $i = i + 1$. Якщо $i < n + k$ і при цьому $g > 0$, то здійснити перехід на повторне виконання п.2.

4. Кінець алгоритму: $W(L) = r$.

Робота запропонованого алгоритму може бути проілюстрована прикладом обчислення $W(L)$ для $L = \{0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1\}$. Діаграма значень змінних алгоритму при обчисленні $W(L)$ показана в таблиці 4.3.

Таблиця 4.3

Діаграма значень змінних алгоритму обчислення зміщення $W(L)$ для коду $L = \{0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1\}$

Номер i поточного біту коду L	Поточний біт коду L : l_i	Кількість g не оброблених одиниць коду L	Результат r
1	0	4	$0 + C_{11}^3 = 165$
2	0	4	$165 + C_{10}^3 = 165 + 120 = 285$
3	1	3	285
4	0	3	$285 + C_8^2 = 285 + 28 = 313$
5	1	2	313
6	0	2	$313 + C_6^1 = 313 + 6 = 319$
7	0	2	$319 + C_6^1 = 319 + 6 = 325$
8	1	1	325
9	0	1	$325 + C_3^0 = 325 + 1 = 326$
10	0	1	$326 + C_2^0 = 326 + 1 = 327$
11	0	1	$327 + C_1^0 = 327 + 1 = 328$
12	1	0	328

Числові коди факторіалів C_{n+k-1}^{g-1} для всіх можливих значень g та i можуть бути обчислені на етапі налаштування зі збереженням результатів в

табличній пам'яті, що адресується конкатенацією кодів g та i . Для $n = 8$ і $k = 4$ потрібно зберігати $11 \cdot 4 = 44$ значення факторіалів.

У рамках розглянутого прикладу $W(L) = r = 328$. Це означає, що специфікація, яка визначає процедуру відновлення втрачених інформаційних блоків B_3 , B_5 і B_8 зберігається в пам'яті, починаючи з адреси $804 + 328 = 1132$.

В таблиці 4.4 наведено підсумкові характеристики організації зберігання специфікацій для відновлення основних блоків даних за умови відновлення не більше 3-х із них. В таблиці 4.4 прийняті наступні позначення: U – загальна кількість втрачених при передачі блоків, X – кількість втрачених основних блоків, Y – кількість втрачених резервних блоків, $U=X+Y \leq 3$, z – адреса початку зони пам'яті, i_1 – номер першого втраченого основного блоку, i_2 – номер другого втраченого основного блоку, i_3 – номер третього втраченого основного блоку, j_1 – номер першого втраченого резервного блоку, j_2 – номер другого втраченого резервного блоку.

Таблиця 4.4

Характеристики розміщення в пам'яті таблиці специфікацій для відновлення втрачених інформаційних блоків та формули обчислення адрес специфікацій

Тип врат пакетів			Зона	Кількість специфікацій в зоні	Початкова адреса зони z	Зміщення специфікації для відновлення i_1 -го пакету відносно початку зони
U	X	Y				
1	1	-	1	n	0	$i_1 - 1$
2	1	1	2	$n \cdot k$	n	$(j_1 - 1) \cdot n + i_1 - 1$
	2	-	3	$n \cdot (n - 1)$	$n \cdot (k + 1)$	$2 \cdot (n \cdot (i_1 - 1) - (i_1 - 1) - \frac{(i_1 - 1) \cdot (i_1 - 2)}{2} + i_2 - 1)$
3	1	2	4	$k \cdot n \cdot \frac{k - 1}{2}$	$n \cdot (k + n)$	$((k - 1) \cdot (j_1 - 1) - \frac{(j_1 - 1) \cdot (j_1 - 2)}{2} + (j_2 - 1)) \cdot n + i - 1$
	2	1	5	$k \cdot n \cdot (n - 1)$	$n \cdot (n + k \cdot \frac{k + 1}{2})$	$2 \cdot (i_2 - i_1 + (j - 1) \cdot \frac{n \cdot (n - 1)}{2} + n \cdot (i_1 - 1) - \frac{(i_1 - 1) \cdot (i_1 - 2)}{2})$
	3	-	6	$n \cdot (n - 1) \cdot \frac{(n - 2)}{2}$	$n \cdot (n + k \cdot \frac{k + n - 1}{2})$	$3 \cdot (\sum_{q=1}^{i_1-1} (n - q - 1) \cdot \frac{n - q}{2} + \sum_{g=i_1+1}^{i_2-1} (n - g - 1) \cdot \frac{n - g}{2} + i_3 - 1)$

Аналіз запропонованого алгоритму адресації табличної пам'яті специфікацій показує, що час його роботи визначається кількістю бітів вектору L доступності інформаційних та резервних блоків, тобто визначається значенням суми $n+m$. Причому запропонований алгоритм використовує, на відміну від інших технологій пошуку, зокрема бінарного, лише одне звернення до пам'яті (тобто всі передбачені алгоритмом дії виконуються на процесорі).

Фактично, запропонована процедура адресації специфікацій являє собою форму хеш-адресації, оскільки розташування специфікацій в табличній пам'яті залежить від коду вектору L доступності інформаційних та резервних блоків. Використання розробленої схеми хеш-адресації таблиці специфікацій дозволяє досягти того, що час доступу до даних фактично не залежить від об'єму самої таблиці. В порівнянні з класичним бінарним пошуком, запропонований варіант адресації дозволяє зменшити час доступу до потрібної для відновлення даних специфікації в ν раз, причому чисельне значення коефіцієнту ν прискорення пошук визначається формулою:

$$\nu = \log_2 N = \log_2 \sum_{u=1}^k \sum_{j=1}^u C_n^j \cdot C_m^{n-j} \cdot j. \quad (4.7)$$

Зокрема, при $n=127$ і $m=9$ значення коефіцієнта прискорення пошуку в таблиці специфікацій дорівнює $\nu=20$.

За наявності на обчислювальній платформі користувача вбудованого криптопроцесора та певних резервів пам'яті, доступ до специфікацій може бути прискорено за рахунок використання класичної хеш-адресації без колізій (perfect hash-addressing).

Висновки до розділу 4

В результаті досліджень, направлених на створення алгоритмів та програмних засобів для синтезу матриць формування резервних блоків, а також засобів для побудови таблиць специфікацій відновлення втрачених блоків, які складають четвертий розділ дисертаційної роботи можна зробити наступні висновки.

1. Запропоноване ефективне технологічне рішення обчислювальної реалізації створених методів у вигляді способу відновлення втрачених інформаційних блоків на основі попередньо створених таблиць специфікацій, який за рахунок оптимізації вибору варіанту реконструювання за критерієм мінімуму кількості блоків даних, які використовуються для цього, а також за рахунок застосування передобчислень, що разом виключають з процесу безпосереднього відновлення ті обчислення, які пов'язані з розв'язанням систем рівнянь, дозволяє на 10-15% прискорити обчислювальну реалізацію реконструювання втрачених блоків в порівнянні з відомими технологіями.

2. Суттєво новими елементами запропонованого способу відновлення блоків даних на основі таблиць специфікацій від відомих таблиць стандартного розташування, які використовуються в завадостійких кодах є те, що таблиці специфікації дозволяють оптимізувати процедуру відновлення за критерієм мінімуму блоків, що транспортуються для відновлення втрачених блоків, що забезпечує мінімальний час реконструювання втрачених даних, а також використання perfect хеш-адресації таблиці, що також дозволяє скоротити час пошуку в таблиці потрібної специфікації. Принциповою відмінністю запропонованих таблиць специфікацій від таблиць стандартного розташування є те, що на відміну від останніх, які містять в собі скореговані коди даних, специфікації описують математичні операції, які потрібно здійснити для того, щоб отримати відновлені коди втрачених інформаційних блоків при їх віддаленому зберіганні чи втрачених інформаційних пакетів при їх відновленні на стороні приймача.

3. Розроблено програмні засоби для реалізації синтезу матриць формування резервних блоків за розробленими методами, а також алгоритми та програми для побудови таблиць специфікацій відновлення втрачених блоків.
4. Експериментальні дослідження програмних засоби для практичної реалізації запропонованих в дисертаційному дослідженні методів відновлення втрачених при віддаленому зберіганні блоків даних та втрачених в процесі передачі по глобальним мережам пакетам практично довели працездатність розроблених методів за умови довільних конфігурацій втрат інформаційних та резервних блоків.
5. З використанням розроблених програмних засобів проведено експериментальне дослідження ефективності запропонованих методів резервування та відновлення даних, яке, в цілому, підтвердило отримані теоретично результати, зокрема реальне прискорення 10-15% обчислювальних процедур реконструювання втрачених блоків в порівнянні з відомими технологіями за рахунок: оптимізації вибору варіанту за критерієм мінімуму кількості блоків даних, які використовуються для реконструювання втрачених блоків; застосування передобчислень, що виключає з процесу безпосереднього відновлення обчислень, пов'язаних з розв'язанням систем рівнянь, а також за рахунок використання хеш-адресації при зверненні до створеної таблиці специфікацій.
6. Проведені експериментальні дослідження запропонованих методів відновлення інформації при її віддаленому зберіганні та при передачі по мережам показали наявність резервів подальшого підвищення ефективності цих важливих процесів в умовах динамічного розвитку технологій віддаленого зберігання даних користувачів та довели доцільність проведення подальших досліджень по практичному використанні цих резервів.

ВИСНОВКИ

В дисертаційній роботі виконано теоретичне обґрунтування і одержано нове вирішення наукової задачі підвищення ефективності резервування та відновлення даних в розподілених системах зберігання інформації, а також пакетів даних в глобальних мережах.

Основні наукові і практичні результати полягають у наступному.

1. Виконано аналіз сучасного стану та перспектив розвитку технологій розподіленого віддаленого зберігання інформації та транспортування пакетів даних по глобальним мережам, обрано критерії ефективності засобів резервування та відновлення втрачених даних в віддалених сховищах і при передачі по мережам. Показано, що в сучасних умовах зростає значимість часу відновлення втрачених даних. Виявлено, що дієвим резервом підвищення ефективності резервування та відновлення даних є урахування особливостей організації їх віддаленого зберігання в реальних системах.
2. Розроблено метод прискорення відновлення втрачених блоків даних, який дозволяє, за рахунок збільшення надлишковості резервування, зменшити час доставки по глобальній мережі інформаційних та резервних блоків для реконструювання втрачених блоків, а також зменшити кількість потрібних для цього обчислювальних операцій, що забезпечує важливе для багатьох застосувань прискорення відновлення даних.
3. Теоретично обґрунтовано, розроблено та досліджено метод відновлення інформаційних блоків при їх розподіленому зберіганні не більш ніж по r на кожному з віддалених сховищ, який базується на використанні для формування резервних блоків матриці, що є ортогональною в межах суміжних r стовпців, а також будь-які три стовпці якої містять ортогональну підматрицю, що гарантує реконструкцію всіх r блоків при втраті доступу до одного сховища, на якому вони зберігаються, а також трьох блоків, які зберігаються на різних сховищах. Метод використовує меншу кількість

резервних блоків, тобто має нижчий рівень надлишковості резервування в порівнянні з відомими методами, орієнтованими на відновлення будь-яких r втрачених блоків.

4. Теоретично обґрунтовано, розроблено та досліджено метод відновлення втрачених при передачі в глобальних мережах пакетів даних, який відрізняється використанням системи пріоритетів при виборі компонентів матриці формування обмеженої кількості резервних пакетів з урахуванням статистичних характеристик втрат пакетів та затримок, що дозволило на 7-10% підвищити ймовірність можливості реконструювання втрачених чи затриманих понад критичний час пакетів в порівнянні з відомими методами.

5. Запропоноване ефективне технологічне рішення обчислювальної реалізації створених методів у вигляді способу відновлення втрачених інформаційних блоків на основі попередньо створених таблиць специфікацій, який за рахунок оптимізації вибору варіанту реконструювання за критерієм мінімуму кількості блоків даних, які використовуються для цього, а також за рахунок застосування передобчислень, що разом виключають з процесу безпосереднього відновлення ті обчислення, які пов'язані з розв'язанням систем рівнянь, дозволяє на 10-15% прискорити обчислювальну реалізацію реконструювання втрачених блоків в порівнянні з відомими технологіями.

6. Розроблено програмні засоби для реалізації синтезу матриць формування резервних блоків за розробленими методами, а також алгоритми та програми для побудови таблиць специфікацій відновлення втрачених блоків. З використанням розроблених програмних засобів проведено експериментальне дослідження ефективності запропонованих методів резервування та відновлення даних, яке, в цілому, підтвердило отримані теоретично результати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gomez, L.A.B.,. Distributed diskless checkpoint for large scale systems. / L.A.B. Gomez, N. Maruyama, F. Cappelto, S. Matsuoka // Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing. CCGRID '10, IEEE Computer Society , Melbourne, Australia.- 2010.- P. 63–72.
2. Yuchong H. Proxy-Assisted Regenerating Codes With Uncoded Repair for Distributed Storage Systems. / H. Yuchong, P.C. Patric, W.S. Kenneth // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No. 4.- P. 2512-2527.
3. Танненбаум,Э. Распределенные системы. Принципы и парадигмы / Э. Танненбаум, М. Ван Стеен. - СПб. : Питер. 2003. - 877 с.
4. Youssefi A.E., Alageel V. A Framework for Secure Cloud Computing // IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.- PP.487-500.
5. Hu Y. Cooperative recovery of distributed storage systems from multiple losses with network coding./ Y. Hu, Y. Xu, X. Wang., C. Zhan, P. Li // IEEE Journal Sel/Areas Commun.- 2010.-Vol.28.- No.2, - P.268-27.
6. Blaum M. Partial MDS Codes and Their Application to RAID Type of Architectures / M. Blaum, J. L.Hafner, S.Hetzler // IEEE Transaction on Information Theory.- 2012.- Vol. 59.- No. 7.- P. 4510-4519.
7. Im S. Flash-aware RAID techniques for dependable and high-performance flash memory SSD/ S.Im, D.Shin // IEEE Trans. Comput.-2011. - Vol.C-60, - No.1,- P. 80-92.
8. Li M. C-codes: Cyclic lower-density MDS array codes constructed using starters for RAID-6 / M. Li, J. Shu // IBM New York USA. Res. Report RC25218.- 2011.- 273 P.

9. Lin S. Error Control Codes 2-th edition / S.Lin, J. Shu // NY: Englewood Cliffs NY USA: Prentice-Hall.-2004.- 344 P.
- 10.Габидулин Э.М. Теория кодов с максимальным ранговым расстоянием // Э.М. Габидулин // Проблемы передачи информации-1985.- Том.21. – Вып.1.- С.3- 16.
- 11.Коляда К.В. Метод відновлення даних при їх розподіленому зберіганні на віддалених сховищах / К.В. Коляда, В.О. Романкевич, М.М. Орлова, О.П. Марковський // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – № 40 – 2020. – С.44-50.
- 12.Rhea S. Maintence-free global data storage, IEEE Internet Comput. – 2011.- Vol. 5,-No.5,- P. 40-49.
- 13.Bardis N. Method for Cloud Storage Data Recovery with Limited Loss of Acces. / N. Bardis, O.P. Markovskyi // Proc. of 4-th International Conference on Mathematics and Computers in Sciences and Industry, MCSI-17, - 24-26 August 2017, Corfu, Greece, - P.55-61.
- 14.Rashmi K.V. Information-Theoretically Secure Erasure Codes for Distrubute Storage / K.V.Rashmi, B. Nihar, K.Ramchandran // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No. 3.- P. 1621-1645.
- 15.Kai X. A Construction of New MDS Symbol-Pair Codes / X.Kai., S.Zhu, P. Li // IEEE Transaction on Information Theory.- 2015.- Vol. 61.- No.11.- P. 5828-5834.
- 16.Vaushampayan V.A. Reability of Erasure Codes Storage Systems: A Combinatorial-Geometric Approach / V.A. Vaushampayan, A. Campello // IEEE Transaction on Information Theory.- 2015.- Vol. 61.- No.11.- P. 5795-5809.
- 17.Марковський О.П. Метод резервування та прискореного відновлення даних в системах їх віддаленого зберігання / О.П.Марковський, М.М.

- Великий // Вісник Національного технічного університету України "КПІ"
Інформатика, управління та обчислювальна техніка, – Київ: БЕК+ – 2015.
– № 63. - С.65-71.
18. Bardis Nikolaos G. Effective method to restore data in distributed data storage systems / Nikolaos G. Bardis, Nikolaos Doukas, Oleksandr P. Markovskyi. // Proceeding of International Conference MILCOM-15, 14-20 Oct.-2015.- USA. P.1101-1109.
 19. Kangwook L. The MDS Queue: Analysing the Latency Performance of Erasure Codes / L.Kangwook, B.S. Nihar, H.Longbo, R. Kannar // IEEE Transaction on Information Theory.- 2017.- Vol. 63.- No.5.- P. 2822-2842.
 20. Коляда К.В. Применение обобщенного модульного кода Хемминга в компьютерных системах / К.В. Коляда, И.А. Дичка // Міжнародна науково-практична конференція "Проблеми інформатики та комп'ютерної техніки" (ПІКТ – 2013), Чернівецький національний університет імені Юрія Федьковича: Тези доповідей – Чернівці, 27-31 травня 2013 р. – С. 86-88.
 21. Дичка И.А. Применение обобщенного кода Хемминга для обеспечения помехоустойчивости информационных систем / И.А. Дичка, К.В. Коляда, Е.С. Сулема // Тези доповідей 3-ї Української конференції з автоматичного керування "Автоматика-96". – Севастополь: СевГТУ, 1996. – Ч. II, С. 165-166.
 22. Leong D. On coding real-time streaming under packet erasure / D.Leong, A. Qureshi, T. // Proc. IEEE International Symposium Information Theory (ISIT).- Vienna. Austria. Jul. 2013.- P.1012-1016.
 23. Plank J. S. On Practical Use of LDPC Erasure Codes for Distribute Storage Application: Technical Report UT-CS-03-510.- Department of Computer Science, University of Tennessee.-2004. - 288 P.

- 24.Марковський О.П. Метод резервування та прискореного відновлення даних в системах їх віддаленого зберігання/ О.П.Марковський, Д.Г. Іванов, М.М. Великий, М.В. Невдащенко // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка, – Київ: БЕК+ – 2014 – № 60. С.46-54.
- 25.Leong D. Erasure coding for real-time streaming / D/ Leong, T. Ho // Proceeding IEEE International Symposium Information Theory (ISIT).- Parma. Italy. Jul. 2012.- P.282-293.
- 26.Sohn J.Y. Capacity of Clustered Distributed Storage / J.Y. Sohn, B.Choi, S.W. Yoon, J. Moon // IEEE Transaction on Information Theory.- 2019.- Vol. 65.- No. 1.- P. 81-107.
- 27.Chen H.C.H. NCCloud: A network coding based storage systems in cloud-of-cloud / H.C.C. Chen, Y.Hu, P.P.C. Li, Y. Tang // IEEE Transaction on Computers.- 2014.- Vol.63.-No.1.- P.31-44.
- 28.Stones R. J. K-Plex 2-Erasure Codes and Blackburn Partial Latin Squares / R. J. Stones // IEEE Transactions on Information Theory. – 2020.-vol. 66.- № 6.- P.3704-3713.
- 29.Ермилов Д.М. Свойства полиномиальных генераторов с выходной последовательностью наибольшего периода над кольцом Галуа / Д.М. Ермилов, О.А. Козлитин // Математические вопросы криптографии. - 2015.- том.6. – № 1.- С.52-61.
- 30.Suh Changho. Exact-Repair MDS Code Construction Using Interference Alignment / Changho Suh, Kannan Ramchandran // IEEE Transaction on Information Theory.- 2011.- Vol.57,- No. 3, - PP. 1425-1442.
- 31.Стіренко С.Г. Забезпечення безперервного відтворення потокового відео в однорангових мережах з використанням erasures кодів / С.Г. Стіренко, А.В., Габінет, Ю.В. Костенко // Вісник НТУУ "КПІ". Інформатика,

- управління та обчислювальна техніка: збірник наукових праць. – К.: "Бек+", 2015. – № 62. – С. 105–110.
32. Johnny M. A Multi-Level Encoding and Decoding Strategy for Binary Erasure Channel / M. Johnny, M.R.Aref // *IEEE Transaction on Information Theory*.- 2019.- Vol. 65.- No. 7.- P. 4143-4151.
 33. Calder B. Windows Azure Storage: A Highly Available Cloud Storage Service with Strong Consistency / B. Calder // *ACM SOSP*.- 2011.- № 2. - P.62-70.
 34. Lakshman A. Cassandra: A decentralized structured storage system./ A. Lakshman, P, Malik // *SIGOPS Oper. Syst. Rev.*- 2010.- № 44. - P. 35–40.
 35. Иванов Д.Г. Метод организации защищенных файловых систем на основе криптографических примитивов контроля доступа / Луцкий Г.М., Волокита А.Н., Иванов Д.Г. // *Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка*, – Київ: БЕК+ – 2010. – № 52. - С.115-119.
 36. Blaum M. Array Codes With Local Properties / M. Blaum, S. R. Hetzler // *IEEE Transactions on Information Theory*. – 2020.-vol. 66.- № 6.- P.3675 - 3690
 37. Ivanov D. Self-reconfigurable cryptographic coprocessor for real-time system // *Abstracts of 21-st International CODATA Conference. October 5-8, 2008. Kyiv, Ukraine.*- К. - 2008. – P.69.
 38. Ivanov D. Paladin: Secure and redundant cloud storage / Heuert U., Ivanov D. // *Herald of the Merseburg University of Applied Sciences*. - Merseburg: Elbe Drucketei Wittenberg GmbH.- 2011. - № 8.- S.220-228.
 39. Иванов Д. Г. Организация резервирования в системах распределенного хранения данных // *Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка*, – Київ: БЕК+ – 2012. – № 56. - С.160-164.

40. Bardis N. A Method for Cloud Storage Data Recovery with Limited Loss of Acces / N. Bardis, O. Markovskiy // Proceeding of 4-th International Conference on Mathematics and Computers in Sciences and Industry MCSI-17. 24-26 August 2017, Corfu, Greece. P.55-61.
41. Tang H. Circular-Shift Linear Network Coding / H.Tang, Q.T. Sun, Z.Li, X.Yang, K.Long // IEEE Transaction on Information Theory.- 2019.- Vol. 65.- No. 1.- P. 65-80.
42. Ye M. Cooperative Repair Construction of Optimal MDS Codes for All Admissible Parameters / M. Ye, A.Bard` // IEEE Transaction on Information Theory.- 2019.- Vol. 65.- No. 3.- P. 1639-1656.
43. Ghemawat S. The Google file system / S.Ghemawat, H/Gobioff, S.T. Leunh // Proceeding of ACM Symposium on Operating Systems Principles (SOSP). October 19–22, 2003, Bolton Landing, New York, USA.– 2003.- P.29-43.
44. Czap L. Secure Network Coding with Erasures and Feedback./ L. Czap, C. Fragouli, V. Phabhakaran, S. Diggavi // IEEE Transaction on Information Theory.- 2015.- Vol. 61.- No. 4.- P. 1667-1686.
45. Gluesing-Luessen H. Symbol Erasure Correction in Random Network with Spread Codes / H. Gluesing-Luessen, A.L. Horlemann-Trautmann // IEEE Transaction on Information Theory.- 2019.- Vol. 65.- No. 4.- P. 2075-2091.
46. Fan X. Variable Packet-Error Coding / X.Fan, O.Kosut, A.B. Wagner // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No. 3.- P. 1530-1547.
47. Mortuza A., Parametric Approach to List Decoding of Reed-Solomon Codes Using Interpolation / A. Mortuza, M. A. Kuijper // IEEE Transactions on information theory. - Vol.57.- № 10.- 2011.- P.6718-6728.
48. Wing Q. End-to-End Error-Correcting Codes on Networks with Wors-Case Bit Errors / Q. Wing, S. Jaggi // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No. 6.- P. 4467-4479.

- 49.Тормасов,А. Г. Модель распределенного хранения данных с регулируемой избыточностью / А. Г. Тормасов, М. А. Хасин, Ю. И. Пахомов // Электронный журнал «Исследовано в России». 2001.- С.14-22.
- 50.Дичка И.А. Способ коррекции модульных ошибок в запоминающих устройствах / И.А. Дичка, К.В. Коляда, А.Н. Наконечный // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1990. – № 27. - С. 51-54.
- 51.Дичка И.А., Коляда К.В. Сравнительный анализ надежности запоминающих устройств с аппаратурной и кодовой избыточностью / И.А. Дичка, К.В. Коляда // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1990. – № 27. С. 35-38.
- 52.Vrable M. Cumulus: Filesystem backup to the cloud / M. Vrable, S. Savage and G. Voelker // ACM Trans. on Storage (ToS), -2009. - Vol. 54.- № 12, - P.11-17.
- 53.Fan, B. Diskreduce: Raid for data-intensive scalable computing./ B.Fan, W.Tantisiriroj, L. Xiao, G. Gibson // In: PDSW '09: Proceedings of the 4th Annual Workshop on Petascale Data Storage. - 2009.- ACM, Portland, USA.- P. 6–10.
- 54.Ташков П. А. Восстанавливаем данные на 100 %. - СПб.: Питер, - 2010.- 208 с.
- 55.Дичка И.А. Сравнительный анализ надежности ЗУ с использованием различных корректирующих кодов / И.А. Дичка, Е.Ф. Колесник, К.В. Коляда // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1989. – № 26.- С. 46-50.
56. Li J. A Generic Transformation to Enable Optimal Repair in MDS Codes for Distribution Storage Systems. / J. Li, X.Tang, C. Tian // IEEE Transaction on Information Theory.- 2019.- Vol. 65.- No. 9.- P. 6257-6267.

57. Huang C/ Erasure coding in windows azure storage / C. Huang // Proceeding USENIX annu.Tech/Conf.- Jun.2012.- Boston. MA,USA.- 2012.- P.2-8.
58. Yehezkeally Y. and Schwartz M. (2020) Reconstruction Codes for DNA Sequences With Uniform Tandem-Duplication Errors / Y.Yehezkeally, M. Schwartz // IEEE Transaction on Information Theory.- 2020.- Vol. 66.- No. 5.- P. 2658-2669.
59. Lee Kangbook. The MDS Queue: Analysing the Latency Performance of Erasure Codes / Kangwook Lee, B.S. Nihar, H.Longbo, R. Kannar // IEEE Transaction on Information Theory.- 2017.- Vol. 63.- No. 5.- P. 2822-2842.
60. Adler N. Burs-Erasure Correcting Codes with Optimal Average Delay / N.Adler, Y.Cassuto // IEEE Transaction on Information Theory.- 2017.- Vol. 63.- No. 5.- P. 2848-2865.
61. Таненбаум Э. Компьютерные сети. СПб: Питер.- 2018. – 960 с.
62. Mladenov T. ; Krieger U. Raptor Codes for P2P Streaming / T. Mladenov, U. Krieger U. // Parallel, Distributed and Network-Based Processing . – Feb. 2012, P. 327 – 332.
63. Bardis N.G. Usage of Linear Erasure Codes for Increasing Reliability and Efficiency of Information Delivery on the Internet / Nikolaos G. Bardis, Oleksandr P. Markovskiy and Kostiantyn V. Koliada // International Journal of Circuits, System and Signal Processing. Vol. 13. – 2019.- P. 585-592.
64. Коляда К.В. Метод резервування та відновлення втрачених даних в глобальних мережах / К.В. Коляда, О.П. Марковський, В.Г. Саверченко, А.І. Торошанко// Телекомунікаційні та інформаційні технології. – № 1 (66). – 2020. – С.4-14.
65. Wang Q. End-to-end Error-Correcting Codes on Networks With Worst-Case Bit Errors / Q.Wang, S. Jaggi // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No. 6.- P. 4467-4479.

66. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера - 2005.- 319 с.
67. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Издательский дом "Вильямс".- 2004.- 1104 с.
68. Fong S.L. Optimal Streaming Erasure Codes Over Three Node Relay Network / Silas L. Fong, Ashish Khisti, Baochun Li, Wan-Tian Tan Li, Xiaoqing Zho // IEEE Transaction on Information Theory.- 2020.- Vol. 66.- No.5.- P. 2696-2712.
69. Fan X. Variable Packet-Error Coding / X.Fan, O. Kosut // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No.3.- P. 1637-1644.
70. Guang X. Linear Network Error Correction Coding / X.Guang, Z.Zhan // Springer-Verlag: N.Y.-2014.- 107p.
71. Seung-Hwa Chung. Detection and analysis of packet loss on underutilized enterprise network links / Seung-Hwa Chung, Y.J. Won, D. Agrawal, Seong-Cheol Hong, James Won-Ki Hong, Hong-Taek Ju // IEEE Workshop on End-to-End Monitoring Techniques and Services. Nice, France. 15-15 May 2005.- 2005.- P.68-74.
72. Suh T. How to estimate the impact of burst packet loss on speech quality in packet network of Electric Power Utility / T. Suh, A. Lebk, D. Mitic // Przegląd elektrotechniczny.- Vol. 89.- No, 8.- 2013.- P. 130-138.
73. Prakash N. The Storage Versus Repair Bandwidth Trade-off for Clustered Storage System./ N. Prakash., V. Abdrashitov, M.N. Megard // IEEE Transaction on Information Theory.- 2018.- Vol. 64.- No. 8.- P. 5783-5807.
74. Huang P. Multi Erasure Locally Recoverable Codes over Small Fields: A Tensor Product Approach P. Huang, E. Yaakobi, P.H.Siegel // IEEE Transaction on Information Theory.- 2020.- Vol. 66.- No.5.- P. 2609-2624.

- 75.Иванов Д.Г. Метод восстановления данных на основе скошенных матриц в системах распределенного хранения / Д.Г. Иванов, Г.М.Луцкий // Известия высших учебных заведений. Проблемы полиграфии и издательского дела. Информационные технологии. - М.:УПИПК МГУП им. И.Федорова. - 2013 - № 2. - С.47-52.
- 76.Николайчук Я.М. Коды полів Галуа: теорія і застосування. Тернопіль.- Вид-во ТНУ.-2012.- 576 с.
- 77.Wickers S.B., Bhargava V.K. Reed-Solomon Codes and Their Applications. IEEE Press. Piscataway, New Jersey.-1983.- p.433
- 78.Klove T. Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems / T. Klove, V. Korzhik // Norwell, MA: Kluwer, 1995. – 433 p.

ДОДАТОК А. Лістинг програми

```

#include<stdio.h>
#include<fstream.h>
#include<conio.h>
#include<iostream.h>
#include<dos.h>
#include<snap.h>
#include<math.h>

int ORTA(int*,int);
int ORTA_1(int*,int);
int TATA(int*);

int main()
{
    unsigned long n,m,h,k,j,i,q,d,u,r,t,w,v,f,l,y,r1,r2,r3,r4;
    int B[4][7] = { { 1,1,1,0,1,0,0 },
                    { 1,0,1,0,0,1,1 },
                    { 0,1,1,1,0,0,1 },
                    { 0,0,1,1,1,0,1 } };
    int D[4][4];
    int N[4][4];
    // 4 -var
    k=0; f=0; d=0; n=0;
    for(v=1; v<6; v++)
    for(l=v+1;l<7; l++)
    for(t=l+1;t<8; t++)
    for(h=t+1;h<16;h++)
    {
        w=v; u=0; for(q=0;q<3;q++) { D[0][q]=w&1; u+=w&1; w>>=1; }
        w=l;      for(q=0;q<3;q++) { D[1][q]=w&1; u+=w&1; w>>=1; }
        w=t;      for(q=0;q<3;q++) { D[2][q]=w&1; u+=w&1; w>>=1; }
        w=h;      for(q=0;q<4;q++) { D[3][q]=w&1; u+=w&1; w>>=1; }
        r1=D[0][0]+2*D[1][0]+4*D[2][0];
        r2=D[0][1]+2*D[1][1]+4*D[2][1];
        r3=D[0][2]+2*D[1][2]+4*D[2][2];
        r4=2020;
        r4=D[0][3]+2*D[1][3]+4*D[2][3]+8*D[3][3];
        d++;
    }
    //
    if((r1!=r2)&&(r1!=r3)&&(r1!=r4)&&(r2!=r3)&&(r2!=r4)&&(r3!=r4))
        if(1)
        {
            n++;
            if(u&1)
            {
                k++;
                N[0][0]=D[0][0]; N[0][1]=D[0][1]; N[0][2]=D[0][2];
                N[1][0]=D[1][0]; N[1][1]=D[1][1]; N[1][2]=D[1][2];
                N[2][0]=D[2][0]; N[2][1]=D[2][1]; N[2][2]=D[2][2];
            }
        }
}

```

```

        m=ORTA(&N[0][0],3);   cout<<"\n                m="<<m;
        if(m==1) f++;
        else
        {
            cout<<"\n k= "<<k<<"   f= "<<f<<"   u="<<u<<"   ORT=
"<<ORTA(&D[0][0],3);
            cout<<"\n "<<D[0][0]<<"   "<<D[0][1]<<"   "<<D[0][2];// <<"
"<<D[0][3];
            cout<<"\n "<<D[1][0]<<"   "<<D[1][1]<<"   "<<D[1][2];// <<"
"<<D[1][3];
            cout<<"\n "<<D[2][0]<<"   "<<D[2][1]<<"   "<<D[2][2]; //<<"
"<<D[2][3];
            // cout<<"\n "<<D[3][0]<<"   "<<D[3][1]<<"   "<<D[3][2]<<"
"<<D[3][3];
        }
    }
    else cout<<"\n    EE "<<v<<"   "<<l<<"   "<<t;
}
cout<<"\n  d= "<<d<<"   n= "<<n<<"   k= "<<k<<"   f= "<<f;
N[0][0]=1; N[0][1]=1; N[0][2]=0;
N[1][0]=0; N[1][1]=1; N[1][2]=1;
N[2][0]=1; N[2][1]=1; N[2][2]=1;
cout<<"\n ORTA = "<<ORTA(&N[0][0],3);

/*
w=v; u=0; while(w>0) { u+=w&1; w>>=1; }
if(u==4)
{
    l=0; w=v; k++;
    for(j=0;j<7;j++)
    {
        if(w&1) { for(i=0;i<4;i++) D[i][1]=B[i][j]; l++; }
        w>>=1;
    }
    m=ORTA(&D[0][0],4);
    if(m) f++; else for(i=0;i<4;i++)
        for(j=0;j<4;j++) N[i][j]=D[i][j];
}
}
cout<<"\n k= "<<k<<"   f= "<<f;
cout<<"\n "<<N[0][0]<<"   "<<N[0][1]<<"   "<<N[0][2]<<"
"<<N[0][3];
cout<<"\n "<<N[1][0]<<"   "<<N[1][1]<<"   "<<N[1][2]<<"
"<<N[1][3];
cout<<"\n "<<N[2][0]<<"   "<<N[2][1]<<"   "<<N[2][2]<<"
"<<N[2][3];
cout<<"\n "<<N[3][0]<<"   "<<N[3][1]<<"   "<<N[3][2]<<"
"<<N[3][3];

```

```

/*
ofstream FA("KORFU_76.TXT",ios::out);
n=0;
for(v=0;v<128;v++)
{
    w=v; u=0;
    while(w>0) { u+=w&1; w>>=1; }
    if (u==4) { A[n]=v;n++; }
}
cout<<"\n Total = "<<n;
cout<<"\t "<<hex<<A[n-1];
h=0; f=1; y=0;
for(j=0;j<n;j++)
{
    m=1; B[0]=A[j];
    for(k=1;k<n;k++)
    { //2
        q=0;
        w=B[0]^A[(k+j)%n];
        while(w>0) { u+=w&1; w>>=1; }
        if((u<3)||(u>6)) q=1;
        if(q==0) { B[1]=A[(k+j)%n]; m=2; }
        for(l=2; l<n; l++)
        { //3
            q=0;
            for(v=0;v<m;v++)
            {
                w=B[v]^A[(l+j)%n]; u=0;
                while(w>0) { u+=w&1; w>>=1; }
                if((u<3)||(u>6)) q=1;
            }
            if ( q==0)
            { B[m]=A[(l+j)%n]; m++; }
        } // 3
    } // 2
    f=1;
    for(k=2;k<127;k++)
    {
        w=k; u=0;
        while(w>0) { u+=w&1; w>>=1; }
        if ( u==3)
        {
            w=k; r=1; l=0;
            for(v=0;v<7;v++)
            {
                if((w&r) !=0 )
                { for(i=0;i<7;i++) E[i][l]=B[i]&r; l++; }
                r<<=1;
            }
            t=0;
            for(v=0;v<7;v++)
            if ((E[v][0]+E[v][1]+E[v][2])==1) t=1;
        }
    }
}

```



```

/* Forming D
for(i=1;i<128;i++)
{
    w=i; l=0;
    while(w>0) { l+=w&1; w>>=1; }
    if(l==3)
    {
        w=i; r=1; l=0;
        for(v=0;v<7;v++)
        {
            if((w&r) !=0 )
            {
                D[l][0]=E[v][0]; D[l][1]=E[v][1]; D[l][2]=E[v][2];
                if((D[l][0]+D[l][1]+D[l][2])==1) t=1;
                l++;
            }
            r<<=1;
        }
    }
}
if(t==0) f=0;
}
if(m==7)
{
    y++; r=1;
    for(v=0;v<7;v++)
    {
        FA<<"\n ";
        for(i=0;i<7;i++)
        { if((B[i]&r)==0) d=0; else d=1; FA<<" "<<d; }
        r<<=1;
    }
    FA<<"\n          "<<dec<<y;
    /*
}

    if(m>h) { h=m; for(i=0;i<m;i++) C[i]=B[i]; }
}
/* B[8]=0xB5; B[9]=0xCB;
for(v=0;v<m;v++)
{
    w=B[v]^B[9]; u=0;
    while(w>0) { u+=w&1; w>>=1; }
    if(u<3) { q=1; cout<<"\n EWA v= "<<v<<" u="<<u; }
}
cout<<"\n q="<<q;

    cout<<"\n y="<<dec<<y;
    FA<<"\n n="<<n;
FA.close();
*/

```

```

    return 0;
}

int TATA(int *h)
{
    int f,i,j,s;
    f=0;
    for(i=0;i<5;i++)
    {
        s=0;
        for(j=0;j<5;j++) s+=*(h+ 5*j +i);
        if((s==1)|| (s==4)) f=1;
    }
    for(i=0;i<5;i++)
    {
        s=0;
        for(j=0;j<5;j++) s+=*(h+5*i+j);
        if((s==1)|| (s==4)) f=1;
    }
    return f;
}

int ORTA_1(int *h,int n)
{
    int A[4]; int i,j, k;
    for(i=0;i<=n; i++)
    {
        k=0;
        for(j=0;j<=n;j++)
            if(j!=i) A[k++]=*(h+j);
        k=ORTA(&A[0],n);
        if(k) return 1;
    }
    return 0;
}

int ORTA(int *h, int n)
{
    int i,j,k,f,z,cj;
    int A[20]={0};
    k=1; for(i=0;i<n;i++)
    {
        for(j=0;j<n;j++) A[j]+=*(h+n*j +(n-1-i))*k;
        k*=2;
    }
    f=1;
    for(j=1;j<k;j++)
    {
        z=0; cj=j;
        for(i=0;i<n;i++)
        {
            if(cj&1) z^=A[i];
            cj>>=1;
        }
    }
}

```

```
    }  
    if(z==0) return 0;  
  }  
  return 1;  
}
```

ДОДАТОК Б. Перелік наукових публікацій за темою дисертації

1. Коляда К.В. Метод відновлення даних при їх розподіленому зберіганні на віддалених сховищах / К.В. Коляда, В.О. Романкевич, М.М. Орлова, О.П. Марковський // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – № 40. – 2020. – С.44-50.
2. Коляда К.В. Метод резервування та відновлення втрачених даних в глобальних мережах / К.В. Коляда, О.П. Марковський, В.Г. Саверченко, А.І. Торошанко// Телекомунікаційні та інформаційні технології. – № 1 (66). – 2020. – С.4-14.
3. Koliada K.V. Usage of linear erasure codes for increasing reliability and efficiency of information delivery on the internet / K.V. Koliada, N.G. Bardis, O.P. Markovskiy // International Journal of Circuits, Systems and Signal Processing – 2019 – Vol.13. – P.585-592.
4. Дичка И.А. Сравнительный анализ надежности запоминающих устройств с аппаратурной и кодовой избыточностью / И.А. Дичка, К.В. Коляда // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1990. – № 27. – С. 35-38.
5. Дичка И.А. Способ коррекции модульных ошибок в запоминающих устройствах / И.А. Дичка, К.В. Коляда, А.В. Наконечный // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1990. – № 27. – С. 51-54.
6. Дичка И.А. Сравнительный анализ надежности ЗУ с использованием различных корректирующих кодов / И.А. Дичка, Е.Ф. Колесник, К.В. Коляда // Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1989. – № 26. – С. 46-50.

7. Коляда К.В. Организация структур ПЗУ с сжатием данных / К.В.Коляда, И.А.Дичка //Вестн. Киевского политехн. ин-та. Сер. Автоматика и электроприборостроение. – К., 1988. – № 25. – С. 30-34.
8. Коляда К.В. Применение обобщенного модульного кода Хемминга в компьютерных системах / К.В. Коляда, И.А. Дичка // Міжнародна науково-практична конференція "Проблеми інформатики та комп'ютерної техніки" (ПІКТ – 2013), Чернівецький національний університет імені Юрія Федьковича: Тези доповідей – Чернівці, 27-31 травня 2013 р. – С. 86-88.
9. Дичка И.А. Применение обобщенного кода Хемминга для обеспечения помехоустойчивости информационных систем / И.А. Дичка, К.В. Коляда, Е.С. Сулема // Тези доповідей 3-ї Української конференції з автоматичного керування "Автоматика-96". – Севастополь: СевГТУ, 1996. – Ч. II, С. 165-166.