ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до магістерської кваліікаційної роботи

на тему: **«МЕТОДИ РЕЗЕРВУВАННЯ І ВІДНОВЛЕННЯ ДАНИХ В РОЗПОДІЛЕНИХ СИСТЕМАХ ЗВ'ЯЗКУ»**

Виконав: студент 6 курсу, групи ТСДМ-61
спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Авраменко О.Ю.
(прізвище та ініціали)

Керівник Варфоломеєва О.Г.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормконтроль _____
(прізвище та ініціали)

Київ – 2019

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти магістр
Спеціальність підготовки 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Телекомунікаційних систем та мереж
_____ В.Ф.Заїка
“____” _____2019 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Авраменку Олексію Юрійовичу

1.Тема роботи: Методи резервування і відновлення даних в розподілених системах зв’язку,
керівник роботи: Варфоломеєва О.Г. к.т.н., доцент,
затверджені наказом вищого навчального закладу від 22.10. 2019 року № 54

2. Строк подання студентом роботи 24.12. 2019 року

3. Вихідні дані до роботи:
1. Моделі і методи орієнтовані на локальну оптимізацію характеристик доступності інформаційних ресурсів
2. Методика комплексного оцінювання варіантів системи захисту центру обробки даних
3. Стратегії резервування та відновлення даних в розподілених системах
4. Науково-технічна література з питань, пов'язаних з оптимізацією збереження та доступності інформаційних ресурсів в розподілених системах

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити):
1. Досліджено особливості побудови розподілених системах, проведено аналіз основних чинників, що призводять до порушення збереження і доступності інформації.
2. Аналіз методів резервування та відновлення інформації, орієнтовні на успішне вирішення підвищення надійності віддаленого зберігання даних в розподілених системах.

3. Побудова систем резервування та управління даними Практична реалізація запропонованого комплексу методів.

5. Перелік демонстраційного матеріалу
   1. Мета та завдання
   2. Актуальність
   3. Особливості побудови розподілених систем обробки даних
   4. Доступність інформаційних ресурсів
   5. Причин зниження доступності інформації та методи їх підвищення
   6. Види та стратегії резервування
   7. Аналіз стратегій резервування
   8. Методи відновного резервування
   9. Рівні систем резервування та управління даними
   10. Організація розподілених центрів обробки даних
   11. Практична реалізація
   12. Висновок
   13. Апробація результатів

6. Дата видачі завдання 18.10.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір технічної літератури.		
2	Аналіз існуючих методів забезпечення доступності інформаційних ресурсів в розподілених системах обробки даних		
3	Дослідження особливостей підвищення надійності віддаленого зберігання даних в розподілених системах		
4	Розробка методів оптимізації підсистеми забезпечення доступності інформаційних ресурсів в розподілених системах обробки даних.		
5	Висновки по роботі		
6	Розробка демонстраційних матеріалів.		

Студент _____ Авраменко О.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Варфоломеєва О.Г.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина дипломної роботи 89 с., 37 рис., 11 табл., 17 джерел.

Об'єкт дослідження- розподілені системи зберігання та обробки даних

Предмет дослідження- моделі та методи резервування і відновлення даних

Мета роботи- дослідження моделей і методів оптимізації збереження та доступності інформаційних ресурсів в розподілених системах обробки даних.

Методи дослідження. У роботі використовувалися методи, засновані на положеннях загальної теорії зв'язку, теорії ймовірності, теорії графів, теорії аналізу ризику, теорії комплексного оцінювання багатовимірних об'єктів.

У дипломній магістерській роботі досліджено особливості побудови розподілених системах, проведено аналіз основних чинників, що призводять до порушення збереження і доступності інформації. Виконано аналіз методів резервування та відновлення інформації, орієнтовні на успішне вирішення підвищення надійності віддаленого зберігання даних в розподілених системах. Проведено класифікацію та аналіз основних стратегій оперативного резервування інформаційних масивів і програмних модулів, які використовуються в вузлах обчислювальних мереж. Розглянуто методи відновного резервування інформаційних масивів і програмних модулів розподілених систем, проводиться їх класифікація та аналіз. Проаналізована методика вибору оптимального рівня захисту центру обробки даних від аварій і катастроф на основі методу векторної стратифікації. Розроблено методи оптимізації підсистеми забезпечення доступності інформаційних ресурсів в розподілених системах обробки даних, та проведена практична реалізація запропонованого комплексу методів.

ІНФРАСТРУКТУРА, КОРПОРАТИВНА МЕРЕЖА, ПРОВАЙДЕР, VPN, ОПЕРАТОР, ТЕРИТОРІАЛЬНО-РОЗПОДІЛЕНА, АУТЕНТИФІКАЦІЯ, ЗАПИТ, АЛГОРИТМ, ПРОТОКОЛ, СТРАТЕГІЯ, ДОСТУПНІСТЬ, РЕЗЕРВ, ЦЕНТР ОБРОБКИ ДАНИХ, СХОВИЩЕ, РЕЗЕРВУВАННЯ, ВІДНОВЛЕННЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВЛ - Високовольтних лініях

ВОЛЗ- Волоконно-оптичні лінії зв'язку

ВР – Відновний ресурс

ЕЦП - Електронного цифрового підпису

ІТ – Інформаційні технології

КС - Кабельні системи;

ОР- Оперативний резерв

ПК- Персональний комп’ютер

РРЛ - Радіорелейний зв'язок

СЗ- Супутниковий зв'язок;

СУБД - Система управління базами даних

ЦОД – Центр обробки даних

DOO (Degraded Operations Objective) - Допустиме уповільнення виконання операцій системою

DWDM (Dense Wavelength Division Multiplexing)- Технологія ущільнення оптичних каналів.

IBP (Internet Backbone Provider) - Інтернет-магістральний постачальник

IP(Internet Protocol)- Інтернет протокол

ISP (Internet Service Provider)- Інтернет сервіс-провайдери

LAN (Local Area Network) –Локальна мережа

NRO (Network Recovery Objective) - Мінімальна смуга пропускання мережі

OSI (open systems interconnection basic reference model) - Базовая цільова модель взаємодії відкритих систем

RPO (Recovery Point Objective) - Цільова точка відновлення

RTO (Recovery Time Objective) – Час відновлення

TCP (Transmission Control Protocol)- Протокол управління передачею

VPN (Virtual Private Network) - Віртуальна приватна мережа

WAN (Wide Area Network) - Глобальна комп'ютерна мережа

ВСТУП

Актуальність дослідження. Прискорений розвиток засобів телекомунікацій, локальних та глобальних комп'ютерних мереж стимулює в останнє десятиліття інтенсивний розвиток технологій зберігання та обробки даних. В той же час вимагає різкого зниження витрат на виконання виробничих функцій, мобільності персоналу, можливості доступу до необхідної інформації і роботи з нею в будь-якій точці світу, підвищення ефективності інвестицій в інформатизацію організацій і підприємств забезпечується багатьма факторами, одним з яких є підвищення рівнів збереження і доступності інформаційних ресурсів (інформаційних масивів, баз знань і програмних модулів) і ефективне управління ними.

В умовах ринкової економіки і конкуренції, ефективність корпоративних розподілених систем обробки даних все більше зв'язується із забезпеченням безперервності підтримуваних ними бізнес- процесів. При цьому автоматизована система повинна забезпечувати певний рівень збереження і доступності інформаційних ресурсів при обмеженнях на вартість створення і експлуатації даної системи.

При збільшенні масштабів розподілених систем, організації доступу до корпоративних інформаційних ресурсів, наявності віддалених мобільних користувачів, збільшується ризик руйнування ІР, втрати доступу до ІР через вихід з ладу апаратного забезпечення і каналів зв'язку. Це призводить до появи ряду нових загроз для інформаційної безпеки систем, зниження ефективності підтримуваних системою виробничих процесів. З іншого боку, використання інфраструктури глобальних мереж, створює можливості застосування нових і модифікації вже відомих методів підвищення збереження і доступності інформаційних масивів, баз знань і програмних модулів. Комплексне вирішення завдань підвищення збереження і доступності ІР в розподільних системах може бути забезпечено розробкою і широким застосуванням формалізованих моделей і прикладних методів аналізу і синтезу механізмів підвищення катастрофо- і

відмовостійкості розподілених систем, що використовують канали зв'язку глобальної мережі Інтернет.

Існуючі в даний час моделі і методи в основному орієнтовані на локальну оптимізацію окремих характеристик доступності IP і підтримуючої інфраструктури (апаратного забезпечення, каналів зв'язку і т.д.), а також збереження IP і не забезпечують належного комплексного, взаємопов'язаного рішення з оптимізації рівнів доступності та збереження IP при проектуванні розподілених систем зберігання даних.

У зв'язку з цим обрана тема дипломної роботи є вельми актуальною.

Ступінь наукової розробки. У магістерській роботі розроблена комплексна методика оптимізації рівнів збереження і доступності інформаційного ресурсу в розподілених системах, що дозволяє створювати економічно обґрунтовані підсистеми захисту. В результаті проведених наукових досліджень, аналізу сучасних вимог були отримані наступні результати:

- сформульовані вимоги до створення відмовостійкої розподіленої системи, що забезпечує необхідні рівні збереження і доступності інформаційних ресурсів для авторизованих користувачів;

- проведено аналіз основних факторів і характеристик, що визначають доступність і збереження інформаційних ресурсів в розподілених системах;

Практичне значення одержаних результатів. Розглянуті в роботі моделі і методи формують науково-методичне забезпечення ефективних засобів підвищення рівнів збереження і доступності інформаційних ресурсів в розподілених системах.

Розроблені методи, алгоритми та інструментальні засоби можуть бути використані при розробці комерційних розподілених систем широкого класу і призначення в науково-дослідних, проектних організаціях і обчислювальних центрах, комерційних організаціях.

Публікації. Результати проведених наукових досліджень у магістерській роботі, доповідалися на 2-х наукових конференціях, опубліковано 1 статтю.

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ В РОЗПОДІЛЕНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

1.1 Особливості побудови розподілених систем обробки даних

В даний час IT-інфраструктура багатьох великих компаній значно ускладнилася і перетворилася в географічно розподілену глобальну структуру. Цей процес в силу об'єктивних причин зачіпає все більше число компаній. Подібна IT-інфраструктура поступово стає погано керованою і погано синхронізованої з центральним офісом, що вимагає при цьому значних витрат на її підтримку [1].

При проектуванні сучасних розподілених систем обробки даних зазвичай керуються вимогами, висунутими бізнесом підприємства. Вони, незалежно від розмірів компанії, потрапляють в 4 категорії [1], [2]:

1. Консолідація систем зберігання - перехід від розрізнених, фрагментованих систем до централізованих систем, що дозволяє консолідувати витрати, підтримку і висококваліфікований персонал в центрах обробки даних. Безліч систем зберігання розглядається як один ресурс, динамічно виділяється в залежності від актуальних потреб. При цьому знижуються витрати на підтримку і супровід, з'являється можливість централізованого контролю за системами. Чим вище рівень централізації управління, тим менше витрат йде на інсталяцію та підтримку функціонування цієї інфраструктури (Наприклад, за рахунок відмови від підтримки в віддалених офісах функціоналу з резервного копіювання/відновлення даних, поштових серверів і ін.). Якщо розвивати цю аналогію далі, віддалені офіси перетворюються в тонких клієнтів замість робочих станцій в клієнт-серверній архітектурі.

2. Спільне використання даних дозволяє знизити час відгуку мережі, доступність інформації, програмного забезпечення, зменшити дублювання даних, а також організувати множинний доступ до даними за технологією SAN, здійснювати балансування навантаження, зменшити необхідний ресурс зберігання

даних, спростити резервування даних і знизити витрати на інфраструктуру зберігання.

3. Резервування даних і сервісів. Зростання цінності даних тягне за собою необхідність забезпечення їх збереження і доступності. Системним методом вирішення даного завдання є використання додаткових ресурсів (копій або передісторій інформаційних масивів і програмних модулів, каналів зв'язку і т.д.) для резервування, що дозволяє значно зменшити вплив руйнують ці елементи факторів на ефективність функціонування системи в цілому.

4. Аварійне відновлення даних. Втрата доступності до важливих даних через аварії і катастроф може обійтися компанії в величезну суму.

Організаційно-технічні заходи щодо захисту від катастроф дозволяють піти від єдиної точки втрати даних, яка виникає завдяки консолідації зберігання і обробки даних в єдиному центрі. При це процес обробки даних повинен бути відновлений за мінімальну час. Для відновлення процесу обробки даних після аварії або катастрофи повинні бути відновлені як інформаційні масиви і програмні модулі, так і інфраструктура (Сервера, мережа передачі даних, живлення, кондиціювання і т.д.), необхідні для роботи автоматизованої системи. Загальна схема типовою розподіленої IT-інфраструктури наведена на рис. 1.1.

Розподілена корпоративна IT-інфраструктура є накладену мережу зв'язку, яка об'єднує локальні мережі філій компанії. При цьому дана накладена мережа будується поверх транспортної мережі, що складається із сукупності власних, орендованих і загальнодоступних WAN каналів (в т.ч. каналів зв'язку мережі Інтернет).

В якості каналів зв'язку на фізичному рівні використовуються:

- Волоконно-оптичні лінії зв'язку (ВОЛЗ);
- Радіорелейний зв'язок (РРЛ);
- Супутниковий зв'язок;
- Кабельні системи;
- ВЧ зв'язок по високовольтних лініях (ВЛ).

Розподілена IT-інфраструктура організації призначена для вирішення наступних основних завдань:

- формування єдиного телекомунікаційного простору організації;

- побудова універсальної транспортної середовища для підключення призначених для користувача мереж;

- забезпечення реалізації технологічних і бізнес-процесів організації;

- надання доступу до інформаційних ресурсів організації зацікавленим державним і приватним особам;

- забезпечення сучасного рівня управління та моніторингу телекомунікаційних ресурсів організації.

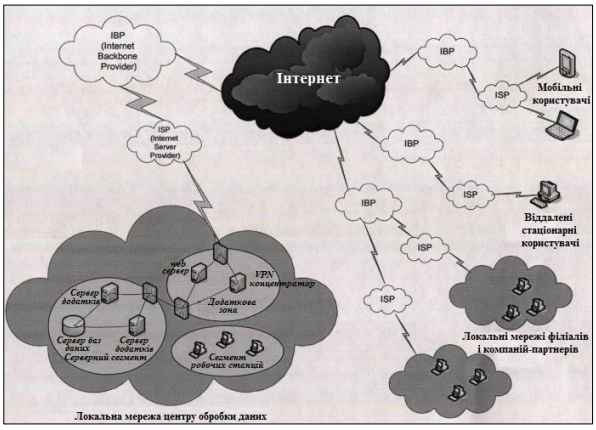

Рис.1.1. Загальна схема розподіленої корпоративної мережі, побудованої з використанням каналів мережі Інтернет

Вимоги, які пред'являлися розробникам при створенні мережі Інтернет, дають ключ до розуміння принципів її побудови, структури і особливостей функціонування.

Мережа Інтернет - це глобальна мережа, що складається з автономних систем, використовують для передачі стек протоколів TCP/IP, і з'єднаних між собою маршрутизаторами, званими граничними шлюзами [3]. В

Як автономних систем можуть виступати опорні мережі, регіональні мережі та мережі користувачів. Автономна система - це мережа, яка перебуває під незалежним управлінням, така як мережа університету або комерційної компанії.

Структурна схема сучасної мережі Інтернет представлена на рис.1.2. Основу мережі Інтернет складають високошвидкісні магістральні опорні мережі, з'єднані між собою через точки обміну трафіком - хаби в термінології SFN - моделі [4]. Регіональні мережі, як правило, підключені до пунктів обміну трафіком, сполученим з декількома опорними мережами. Кінцевими користувачами послуг Інтернет називаються юридичні або фізичні особи, які споживають або навмисні спожити інтернет-послуги, що не припускають використовувати ці послуги для безпосередній перепродажу третім особам.

Провайдером (оператором інтернет-доступу) називається оператор зв'язку, надає послуги доступу до мережі Інтернет, тобто послуги передачі даних між кінцевим обладнанням користувача або мережею передачі даних іншого оператора зв'язку і будь-який інформаційно-обчислювальної мережею (системою) або окремої ПК, підключеної до мережі Інтернет.

Провайдер інтернет-доступу, що надає іншого провайдера інтернет-доступу можливість забезпечення своїм клієнтам доступу до ресурсів мережі Інтернет, що знаходяться поза мережею даного оператора, називається UpStream провайдером.

Провайдери інтернет-доступу за функціонально-географічною ознакою поділяються на такі типи:

- магістральні оператори (Internet Backbone Provider - IBP) - оператори міжрегіональних IP-мереж, що забезпечують перенесення інтернет-трафіку між регіонами країни і за кордон;

- кінцеві провайдери (інтернет сервіс-провайдери - ISP), діючі на регіональному або локальному рівні (відповідно - регіональні ISP і локальні ISP) - оператори регіональних або локальних IP-мереж, що забезпечують надання інтернет-послуг кінцевим користувачам.

Визначальними ознаками IBP є:

- наявність як мінімум трьох високопродуктивних вузлів мережі передачі даних IP-вузлів), розташованих в різних суб'єктах країни і пов'язаних між собою високошвидкісними каналами зв'язку (власними або орендованими);

- можливість підключення IP-мереж інших операторів інтернет-послуг на швидкості 2 Мбіт/с і вище;

- безпосередню взаємодію з мережами найбільших світових UpStrcam провайдерів;

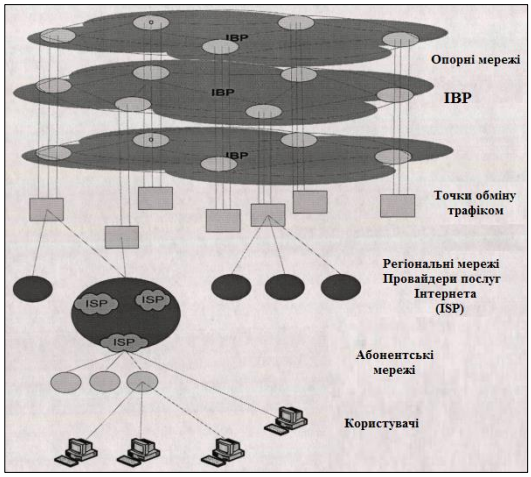

Рис. 1.2. Структурна схема мережі Інтернет.

- забезпечення клієнтам зв'язності з українським сегментом мережі інтернет і світовим Інтернетом.

Визначальними ознаками ISP є:

- наявність вузла (вузлів) доступу для підключення кінцевих користувачів за допомогою різних технічних рішень і мереж доступу (dial up, виділена лінія, мережі передачі даних і т. д.);

- підключення до мережі Upstream провайдера.

Інтернет сервіс-провайдери (ISP) об'єднуються в регіональну мережу.

Абонентські мережі користувачів підключаються до провайдерів послуг доступу до мережі Інтернет.

Українським сегментом мережі Інтернет називаються мережі передачі даних, що входять в мережу Інтернет, і контент-ресурси (інформація або служби, послуги, доступні через мережу) мережі Інтернет, що функціонують на території Украіни [7]. Структурна схема сегмента мережі Інтернет представлена на рис.1.3.

Регіональні мережі (WAN - Wide Area Network) з точки зору архітектури і протоколів практично не відрізняються від світових. В регіональних мережах

зазвичай не використовуються трансокеанські кабелі, але це відмінність не може розглядатися як принципове. Регіональні мережі вирішують проблему формування з LAN (локальних мереж) мереж регіонів і цілих країн і навіть наднаціональних мереж (наприклад, E-BONE для Європи). Як правило, ці мережі будуються з використанням протоколів SDH, ATM, ISDN, Frame Relay або X.25. Архітектурно такі мережі формуються з каналів зі схемою точка-точка і потужних комутаторів-мультиплексорів.

З таких фрагментів формуються і опорні мережі (BackBone), які дозволяють скоротити число кроків від вузла до вузла. У цих мережах в основному використовуються оптоволоконні транспортні системи, а там де це нерентабельно, супутникові або радіорелейні канали.

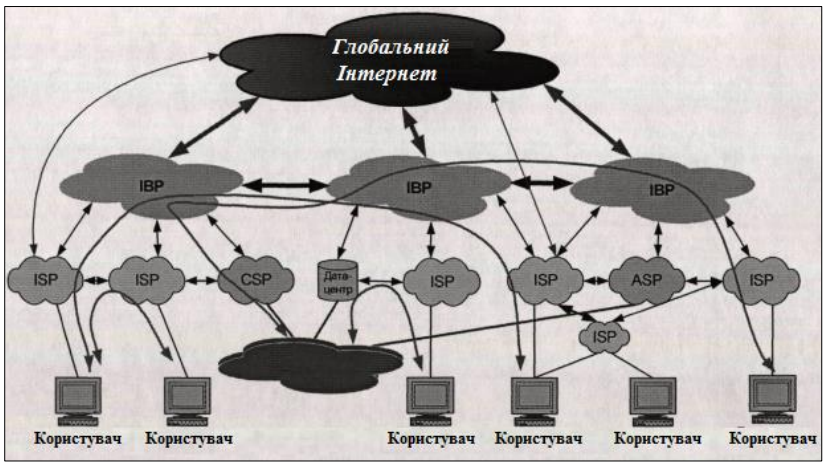

Рис. 1.3. Сегмент мережі Інтернет країни.

З появою корпоративних мереж типу Інтранет поняття локальної та регіональної мереж стали частково перекриватися. для користувача

Інтранет все вузли такої мережі є локальними, хоча і можуть відстояти на сотні або навіть тисячі кілометрів один від одного. По суті мережі інтранет є накладеними мережами по відношенню до регіональних мереж (WAN). Інтернет також слід віднести до числа накладених мереж по відношенню до WAN [2],[5].

В якості особливостей територіально-розподілених IT-інфраструктур сучасних компаній, найбільш істотних з точки зору інформаційної безпеки, можна вказати наступні:

- розподілена гетерогенна 1Т-інфраструктур включає в себе локальні мережі з різними периметрами безпеки, канали зв'язку глобальних мереж, як знаходяться в власності компанії, так і орендовані;

- канали зв'язку виходять за межі контрольованої зони;

- для передачі даних використовуються канали зв'язку мереж загального користування, в тому числі канали мережі Internet;

- територіально-розподілена корпоративна мережа може мати кілька точок підключення до мережі Internet;

- на кількох виробничих майданчиках можуть перебувати критично важливі сервера, в доступі до яких можуть потребувати співробітники, що працюють на інших майданчиках, мобільні користувачі, співробітники інших організацій; використання віддаленого мобільного доступу до ресурсів корпоративної мережі;

- багато критично важливі бізнес-процеси орієнтовані на використання інформаційних систем, тому до доступності інформаційних сервісів висуваються жорсткі вимоги; не вся територіально-розподілена IT-інфраструктура може контролюватися мережевими і/або системними адміністраторами організації.

Таким чином, використання в складі IT-архітектури організації загальнодоступною мережевої середовища, подібної Інтернет, робить вкрай актуальними питання забезпечення безпеки інформаційних ресурсів і IT-сервісів. Для успішного протистояння загрозам потрібна організація системи захисту, що складається з декількох рівнів і що включає в себе засоби захисту периметра, організації захищених приватних мереж VPN (Virtual Private Network - Віртуальна приватна мережа), антивірусного ПО, засоби аутентифікації і авторизації [2].

Відкриті канали зв'язку на базі протоколу TCP/IP мають досить серйозні проблеми з точки зору інформаційної безпеки.

Ігнорування цих проблем може призвести до тяжких наслідків для незахищених мереж. Помилки при проектуванні сервісів TCP/IP, складність конфігурації хостів, вразливі місця, що з'явилися в ході написання програм і ряд інших причин в сукупності роблять непідготовлені мережі відкритими і вразливими для діяльності зловмисників. Ряд служб TCP і UDP погано

забезпечують безпеку в сучасному середовищі в мережі Інтернет. При мільйонах користувачів, підключених до мережі Інтернет, залежність від мережі Інтернет багатьох організацій і промислових підприємств, недоліки в мережевих службах, широка доступність вихідного коду і автоматизованих засобів проникнення в системи створюють серйозні проблеми із забезпеченням безпеки. Сполучені з Інтернетом мережі зазнають значного ризику атак з боку зловмисників. На рівень ризику впливають наступні фактори:

- число систем в мережі;
- ефективність функціонування служб, які використовуються в мережі;
- спосіб з'єднання мережі з Інтернетом;
- профіль мережі або інформація про її існування
- ступінь готовності організації до вирішення проблем безпеки.

На рис. 1.4. представлений типовий варіант розподіленої корпоративної IT-інфраструктури, побудованої з використанням резервування інформаційних ресурсів і обладнання, розміщених в центрі обробки даних, а також каналів глобальних мереж зв'язку, що з'єднують дані інформаційні ресурси з кінцевими користувачами.

Незважаючи на використання надмірності, представлена на рис.1.4. схема має єдину точку відмови - корпоративний центр обробки даних.

При виході з ладу всієї площадки доступність інформаційних ресурсів для кінцевих користувачів може бути порушена на тривалий термін.

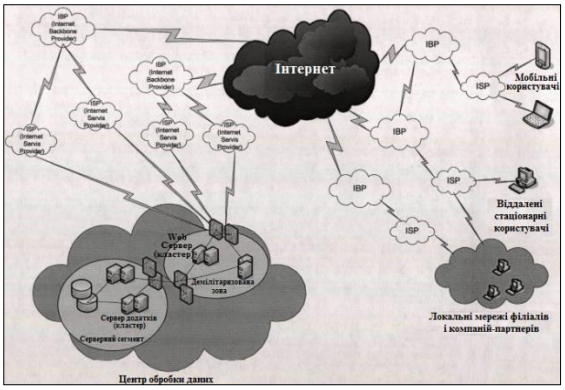

Рис. 1.4. Розподілена корпоративна IT-інфраструктура

Щоб уникнути подібного розвитку подій, використовують резервні центри обробки даних. На рис.1.5. представлений фрагмент типовою схеми організації корпоративної IT- інфраструктури, побудованої з резервуванням центрів обробки даних.

Аналіз показує, що об'єднання інформаційних ресурсів розрізнених підрозділів в єдину систему забезпечує певні переваги, проте перешкодою на цьому шляху є висока вартість організації та підтримки власних «безпечних» каналів зв'язку, за якими має йти обмін інформацією. Виходом з цього стали розробка і впровадження способів з'єднання комп'ютерів, при якому інформація, передана по загальнодоступних каналах зв'язку, виявлялася захищеної від перехоплення і декодування третіми особами.

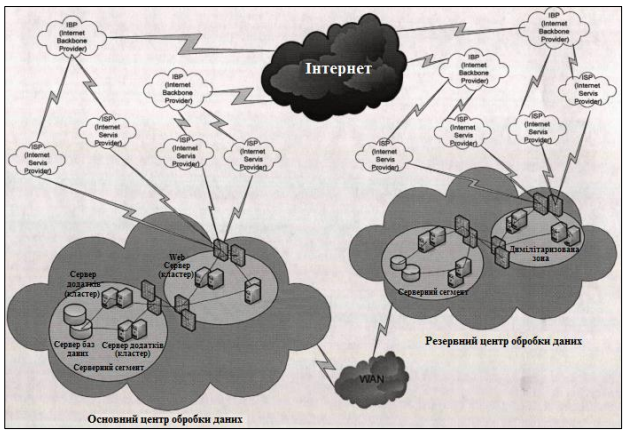

Рис.1.5. Схеми організації корпоративної IT- інфраструктури

Сукупність мережевих сполук, що використовуються для встановленн з'єднання між приватними (private) мережами за допомогою громадських (Public) каналів, отримала назву віртуальних приватних мереж (Virtual Private Network, VPN). При цьому захист інформаційних потоків, переданих через відкриті канали зв'язку, забезпечується за рахунок рішення наступних основних завдань [6]:

- Взаємна аутентифікація сторін при встановленні мережного з'єднання. Аутентифікація здійснюється на основі багаторазових і одноразових паролів, цифрових сертифікатів, протоколів суворої аутентифікації, і забезпечує встановлення VPN-з'єднання тільки між повноважними мережевими об'єктами.

- Авторизація та управління доступом. авторизація передбачає надання сторонам, вже довели свої повноваження, певних видів обслуговування, зокрема, різних способів фільтрації і шифрування їх трафіку.

- Забезпечення конфіденційності та достовірності передаваної інформації. Конфіденційність забезпечується за допомогою алгоритмів симетричного і асиметричного шифрування.

Достовірність даних, що передаються забезпечується за допомогою технології електронного цифрового підпису (ЕЦП).

- Реалізація політики безпеки організації. забезпечується за рахунок централізованого управління засобами захисту (VPN- агентами).

Схема взаємодії двох сегментів корпоративної мережі через відкриті канали мережі Інтернет за допомогою VPN - з'єднання представлена на рис.1.6.

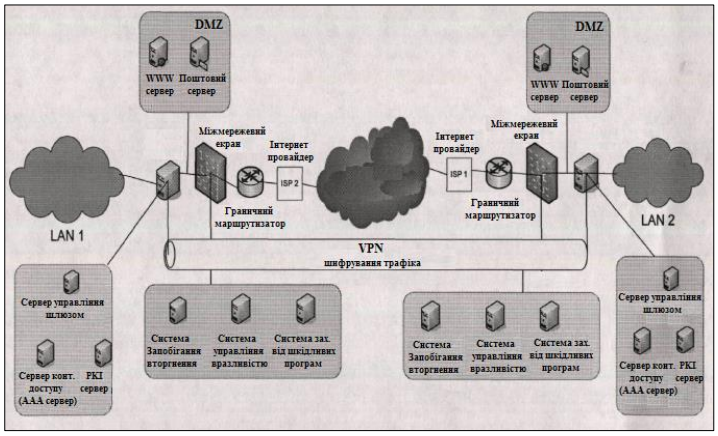

Рис. 1.6. Схема взаємодії двох сегментів корпоративної мережі через відкриті канали мережі Інтернет за допомогою VPN

В цьому випадку для протистояння загрозам, що виникають при використанні загальнодоступних каналів зв'язку, потрібна організація системи захисту, що складається з декількох рівнів і включає в себе засоби захисту периметра, організації захищених приватних мереж VPN (Virtual Private Network) - Віртуальна приватна мережа), антивірусного ПО, засобів аутентифікації і авторизації. Один з типових варіантів підключення локальної мережі до мережі Інтернет представлений на рис.1.7. Можна виділити три основні завдання, пов'язані із захистом периметра локальної мережі:

- забезпечення захисту інформаційних ресурсів локальної мережі від загроз з боку зовнішніх мереж;

- забезпечення надійного і безпечного інформаційного обміну між вузлами локальної мережі і віддаленими мережними об'єктами (Віддалені мобільні користувачі, мережі філій організації і т.д.);

- припинення зловживання користувачами локальної мережі популярними Інтернет-службами, перш за все електронною поштою і WWW.

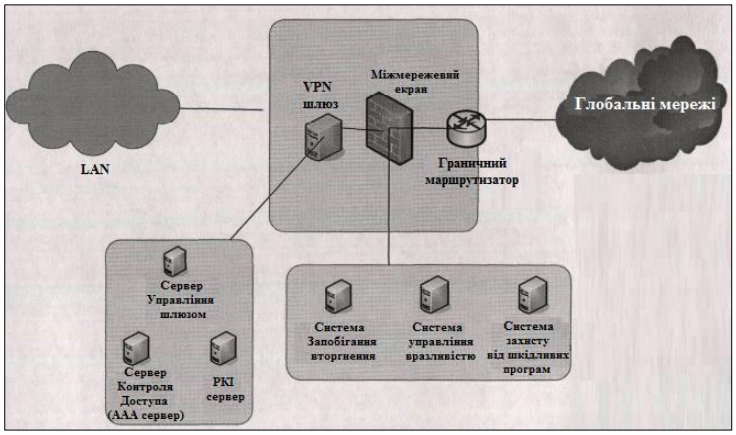

Рис.1.7. Варіант підключення локальної мережі до мережі Інтернет

При побудові системи захисту кожен її рівень вносить додаткові тимчасові затримки в передачу даних по каналах зв'язку, збільшує вартість системи і може служити додатковою точкою виникнення відмов. Тому слід строго витримувати баланс між цінністю захищаються ресурсів і міцністю створюваної системи захисту.

Узагальнена схема обміну даними між двома вузлами з використанням каналів зв'язку глобальних мереж наведена на рис.1.8. виникнення відмов можливо на кожному з наведених рівнів.

Нехай ймовірність відмови кожного з зображених одинадцяти елементів дорівнює $q_1 \ldots q_{11}$ відповідно. При відсутності резервування кожен з елементів буде представляти собою точку відмови. Тому резервування є необхідним заходом. Показники надійності при цьому розраховуються відомими методами.

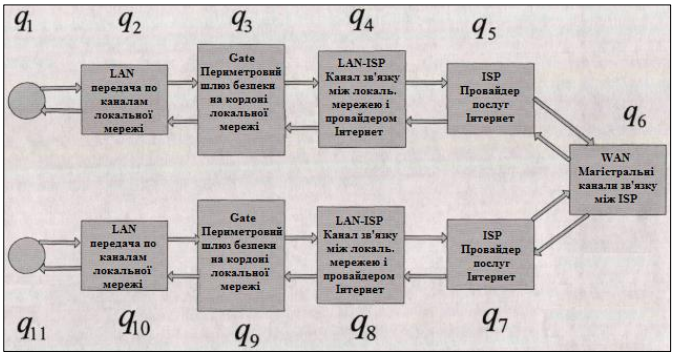

Рис.1.8. Узагальнена схема обміну даними між двома вузлами з використанням каналів зв'язку глобальних мереж

Слід зазначити, що існують два типи мережевих вузлів: кінцеві вузли та комунікаційні вузли. Прикінцеві вузли створюють або споживають інформацію, передану по мережі. Через комунікаційні вузли інформація проходить, але вони не створюють і не споживають її. Прикінцеві (Термінальні) вузли виконують і деякі комунікаційні функції.

Традиційні мережі і телекомунікаційні канали утворюють фізичний рівень мережі. Реальна топологія мережі може динамічно змінюватися, хоча его і відбувається зазвичай непомітно для учасників. При роботі мережі використовуються десятки протоколів. У будь-яких комунікаційних протоколах важливе значення мають операції, орієнтовані на встановлення зв'язку (connection-oriented) і операції, які не потребують зв'язку (Connectionless - "безладні", ISO 8473). Інтернет використовує обидва типи операцій [5]. При першому типі користувач і мережу спочатку встановлюють логічний зв'язок і тільки потім починають обмін даними.

Причому між окремими пересилаються блоками даних (пакетами) підтримується взаємодія. "Нескладні" операції не передбачають встановлення будь-якого зв'язку між користувачем і мережею (наприклад, протокол UDP) до початку обміну. Окремі блоки переданих даних в цьому випадку абсолютно незалежні і не вимагають підтвердження отримання.

Пакети можуть бути втрачені, задубліровани або доставлені не в порядку їх відправки, причому ні відправник, ні одержувач будуть про це оповіщені. Саме до

цього типу належить базовий протокол Інтернет – IP протокол, який буде намагатися надіслати пакети за призначенням, але не дає ніяких гарантій доставки. Пакети можуть бути втрачені на своєму шляху в

Внаслідок перевантаження каналів або маршрутизаторів, або канал може просто повністю вийти з ладу. Помилки при передачі також можуть пошкодити пакет. Для забезпечення працездатності мережі у вузла-джерела повинен бути спосіб повторювати доставку пакетів до тих пір, поки вони не будуть доставлені без спотворень. Це завдання вирішує протокол TCP (Transmission control protocol) - протокол управління передачею. До завдань протоколу TCP також входить управління швидкістю передачі щоб уникнути перевантажень в каналах і маршрутизаторах. Протокол TCP є механізм, який функціонує на комп'ютерах джерела і адресата повідомлень. Протокол TCP (transmission control protocol, RFC-793, -1323) на відміну від протоколу UDP здійснює доставку дейтаграм, званих сегментами, у вигляді байтових потоків з встановленням з'єднання.

Передбачається, що одержувач пакета практично завжди посилає відправнику пакет-відгук. Відправник може послати черговий пакет, що не чекаючи отримання від одержувача підтвердження про прийом попереднього пакету. Таким чином, може бути послано до пакетів, перш ніж буде отриманий відгук на перший пакет (протокол "ковзного вікна "). У протоколі TCP" ковзне вікно "використовується для регулювання трафіку і перешкоди переповнення буферів.

Розмір вікна в сегментах визначається співвідношенням:

window > RTT*B/MSS,

де **B** смуга пропускання каналу в біт/с,

MSS - максимальний розмір сегмента в бітах, а window - в сегментах,

RTT час подорожі пакету до адресата і назад.

Кінцевою метою регулювання трафіку є встановлення відповідності між темпом передачі і можливостями прийому. Причиною перевантаження може бути не тільки обмеженість розміру буфера, але і недостатня пропускна здатність якоїсь ділянки каналу.

Розглянемо передачу великої послідовності пакетів від комп'ютера S до комп'ютера S. Для управління процесом передачі, Про підтверджує прийом кожного вірно прийнятого пакета квитированием цього пакета для S.

Протокол комп'ютера S містить лічильник і таймери. Лічильник використовується для того, щоб S, після відправки N пакетів, на які ніхто не почув підтвердження, більше пакетів не передавав. Наприклад, S може послати N пакетів і чекати підтвердження отримання першого пакету, перш ніж відправити (N + 1) - ий пакет, і т.д. Якщо N мало і якщо у S між відправкою пакету і отриманням підтвердження (квітірованія) пройде T секунд, і, отже, за T секунд S отруює приблизно N пакетів. Таким чином, змінюючи N, комп'ютер S може змінювати швидкість передачі і коригувати навантаження на маршрутизаторах. Ідея TCP полягає в тому, що S зменшує N, коли S вважає, що в мережі наступила перевантаження, і збільшує N в іншому випадку. S може виявити виникнення перевантаження по затримці приходу квитирующего повідомлень (тобто за часом T). Збільшення T, таким чином, вказує на перевантаження і є приводом для того, щоб зменшити N.

Визначимо середнє число сеансів зв'язку, необхідних для безпомилкової передачі пакета інформації через мережу, що використовує стек протоколів TCP/IP. Для вирішення даного завдання використовуємо регенеративний метод [3]. Нехай передавач посилає приймача пакети. передача може виявитися невдалою (містити помилки) і вимагати повторення з ймовірністю q. Необхідно визначити середнє число сеансів зв'язку, необхідних для безпомилкової передачі пакета інформації. Граф станів системи представлений на рис. 1.9.

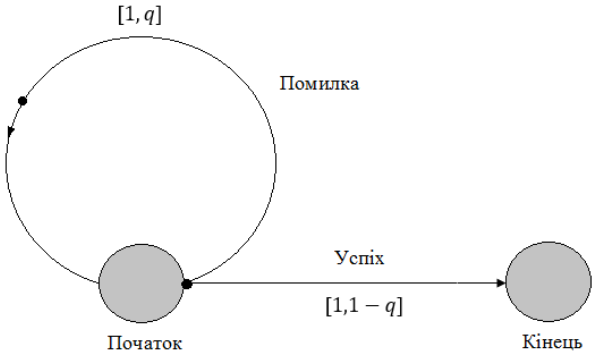

Рис.1.9. Граф станів системи

Одним із способів вирішення цього завдання є розрахунок розподілу числа необхідних сеансів зв'язку X [3]. тут по визначенню, випадкова величина має геометричний розподіл з параметром p ∈ [0, 1], тобто

$$P\{X = n\} = q^{n-1}(1-q),\ n = 1,2,\ldots\ldots,$$ де n - число сеансів зв'язку

Звідси випливає, що

$$E\{X\} = \frac{1}{1-q} \tag{1.1}$$

Даний метод важко застосовувати в ряді більш складних ситуацій.

Розглянемо інший підхід до вирішення поставленого завдання [3]. Нехай випадкова величина X дорівнює 1 з ймовірністю 1-ц, якщо перший сеанс зв'язку буде успішним. Тоді X дорівнює 1 + Y з ймовірністю q, коли розподіл Y відповідає розподілу X. Дійсно, перший невдалий сеанс зв'язку відбудеться з вірогідністю ц, після чого необхідно повторити передачу, так що число сеансів, що залишилися після першого невдалого, статистично еквівалентно випадкової величини X. Таким чином, можна записати, що

$$X = \begin{Bmatrix} 1 + Y \textit{ із ймовірістю } q \\ 1 \textit{ з ймовірністю } (1-q) \end{Bmatrix}$$

Y не залежить від результату першого сеансу зв'язку. отже,

$E\{X\} = (1-q) + q[1 + E\{Y\}]$

$E\{Y\} = E\{X\}$, *так як X і Y* статистично еквівалентні. Звідси випливає, що

$E\{Y\} = (1-q) + q + qE\{X\} = 1 + qE\{X\}$

Вирішуючи дане рівняння щодо E {X}, отримаємо

$$E\{X\} = \frac{1}{1-q}$$

Розглянемо модель передавача і приймача, які здійснюють обмін пакетами через обчислювальну мережу, що існує на основі стека протоколів TCP / IP [3]. Нехай успішна передача займає T одиниць часу. Якщо передача закінчилася невдачею, то необхідно затратити T + a одиниць часу, щоб зрозуміти, що передача

не пройшла (а - час, необхідне для прийому негативного підтвердження). нехай необхідно визначити середній час, який потрібен для успішної передачі. Граф станів системи представлений на рис. 1.10.

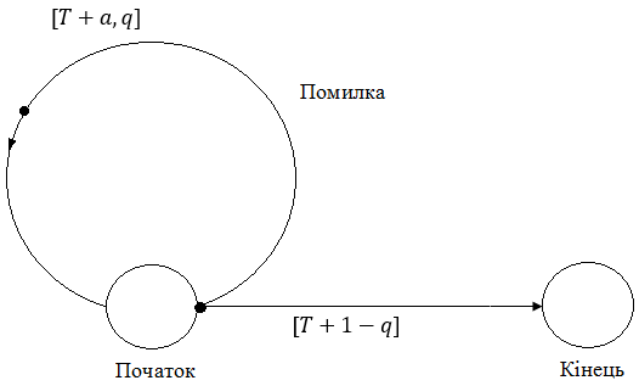

Рис. 1.10. Граф станів системи

Нехай τ - час, що минув до першого вдалого сеансу зв'язку. Тоді можна записати:

$$E\{\tau\} = (1-q)T + q[T + \alpha + E\{\tau\}]$$

Вирішивши рівняння щодо Е $\{\tau\}$, отримаємо – $E\{\tau\} = \frac{T+a(1-p)}{p}$

Дана модель може бути застосована і в більш складних ситуаціях. Припустимо, що пакет необхідно без помилок передати через три послідовно з'єднані ланки лінії. Передача по кожній ланці вимагає Т секунд, а ймовірність правильної передачі становить 1-р. Якщо перша, друга або третя передачі невдалі, передавач виявить це, відповідно, через Т + а, Т + 2а, або Т + 3а інтервалів часу. Граф станів системи в цьому випадку представлений на рис. 1.11.

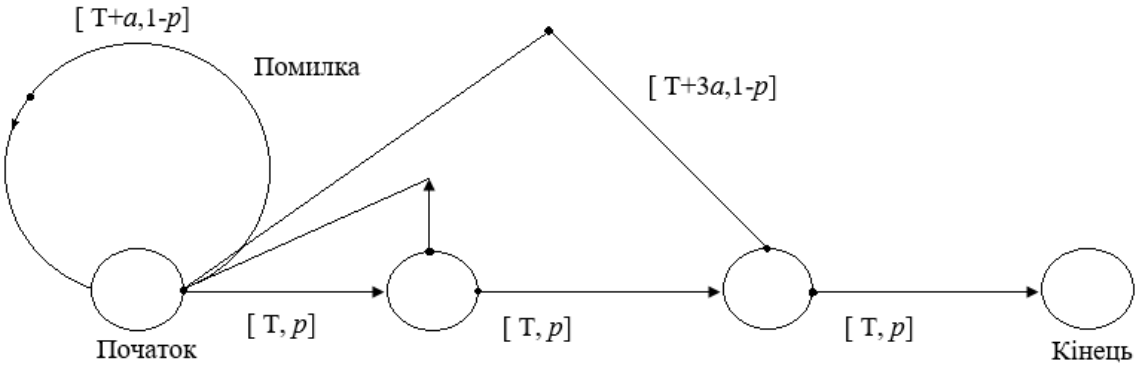

Рис.1.11.Граф станів системи [T+a,1-p] Помилка

Позначивши через τ загальний час передачі, за яке передається пакет надійде в пункт призначення без помилок, отримаємо:

$$E\{\tau\} = (1-p)(T + a + E\{\tau\}) + p[T + T_1]$$

$$T_1 = (1-p)(T + 2a + E\{\tau\}) + p[T + T_2]$$

$$T_2 = (1-p)(T + 3a + E\{\tau\}) + pT.$$

Рішення даної системи рівнянь дозволяє визначити E $\{\tau\}$.

Розглянемо основні характеристики каналу зв'язку між географічно розподіленими об'єктами IT-інфраструктури, використовує мережі, що функціонують на основі стека протоколів TCP/IP.

Для оцінки якості такого каналу необхідно отримати оцінки як мінімум для трьох його основних характеристик [1, 3, 4]:

- доступність каналу зв'язку, тобто ймовірність пересилки необхідного обсягу даних (напр., запиту до масиву і відповіді на запит) за максимально допустимий час;

максимальна продуктивність при передачі запитів/відповідей заданого типу (пропускна здатність, біт/с);

- середній час реакції (середній час отримання квитанції про успішну передачі пакета від передавача до приймача).

Дані показники розраховуються на основі наступних параметрів каналу зв'язку:

- середній час успішної передачі пакету даних від передавача до приймача;

- середній час затримки при передачі пакета по каналу зв'язку в кожну сторону;

- ймовірність втрати пакета при передачі;

- джиттер (різні затримки при передачі пакетів одного повідомлення через мережу - різні пакети можуть йти різними маршрутами);

- ширина вікна - число пакетів, які можна передати без підтвердження прийому.

Розглянемо більш докладно основні параметри каналу зв'язку [1,3, 5].

Затримка - це проміжок часу між прибуттям пакета на мережевий інтерфейс джерела і досягненням ним вузла призначення. В сучасних TCP/IP мережах середній час затримки при передачі пакета від вузла А до вузла Вів зворотну сторону від вузла В до вузла А може істотно відрізнятися. Затримка містить чотири компоненти: час перебування в черги, час доступу до середовища, час передачі, час поширення.

Час доступу до середовища - це час, який готовий до відправки пакет змушений очікувати до того моменту, коли вузол зможе його передати. В випадку використання протоколу Ethernet час доступу до середовища - це час, який буде потрібно до того моменту, поки вузлу вдасться здійснити передачу після деякого випадкового кількості конфліктів і передач інших вузлів. Час передачі дорівнює числу біт в пакеті, поділеній на швидкість передачі. Наприклад, в Ethernet тому пакети мають розміри від 500 до 12000 бітів, час передачі коливається в межах від 0,05 мс до 1,2 мс при швидкості 10 Мбіт / с і стає в 10 разів менше при швидкості 100 Мбіт/с. Час перебування в черзі - це час, який пакет очікує початку своєї передачі. Це час, необхідне для передачі інших пакетів, які прибули на мережевий інтерфейс раніше. Середній час перебування в черзі зазвичай в кілька разів більше часу передачі і залежить від завантаження мережі.

Час поширення - це час, який потрібен сигналу для поширення по середовищі передачі. Час поширення одно відношенню довжини каналу до швидкості поширення сигналу. Швидкість поширення становить близько 3х108 м/с в кручений парі і 2х108 м/с в оптичному волокні. Дані швидкості поширення відповідають затримок на 3,3 мкс/км в кручений парі і 5 мкс/км в оптичному волокні.

Таким чином, за час, який потрібен сигналу для подолання 200 м, передавач може передати приблизно біт, якщо швидкість передачі становить R Мбіт/с.

У разі, якщо канал зв'язку включає в себе кілька мережевих сегментів (Локальні мережі, мережі первинних провайдерів, мережі магістральних провайдерів), то загальний час затримки дорівнюватиме сумі затримок для кожного мережевого сегмента.

Для підвищення якості мережевого обслуговування застосовують кілька прийомів:

- Забезпечення надлишкової продуктивності мережі;

- Використання в вузлах мережі обладнання з пріоритезацією трафіку.

При цьому пакети, що відносяться до різних потоків, утворюють в буферної пам'яті окремі черги, які обслуговуються по різних алгоритмах з урахуванням пріоритету і відносного «ваги» того або іншого додатка. Метою такого маніпулювання чергами є зменшення затримок і втрат пакетів для додатків реального часу. Застосування в маршрутизаторах технологій комутації потоків (Tag switching, MPLS) також призводить до зменшенню затримок і втрат пакетів.

- Застосування набору протоколів для забезпечення необхідного рівня обслуговування в IP-мережах. Маються на увазі такі протоколи, як RTP, RSVP (протокол резервування ресурсів).

Використання механізмів QoS (забезпечення заданої якості обслуговування) на канальному рівні.

1.2 Аналіз причин зниження доступності інформації та методи їх підвищення

Перелік факторів, що впливають на безпеку інформаційних ресурсів, наведено в ГОСТ «Захист інформації, фактори що впливають на інформацію». Даний стандарт встановлює класифікацію впливають на захищається інформацію чинників, підлягають врахуванню при організації захисту інформації (забезпечення її конфіденційності, достовірності і доступності).

Основні фактори, що викликають тривалу відсутність або втрату інформаційних масивів і програмних модулів, перераховані нижче:

- Нехтування резервним копіюванням перед виконанням таких системних робіт, як перевстановлення або оновлення операційної системи, зміна конфігурації дискової пам'яті, установка нових периферійних пристроїв.

- Нехтування періодичним резервним копіюванням даних або помилки при складанні графіка копіювання.

- Прорахунки при розробці технології обробки та зберігання даних.

- Помилки при використанні системних утиліт, що змінюють структуру розділів диска, а також програмні помилки в цих утиліти.

- Випадкове видалення файлів і каталогів в процесі звичайної роботи.

- "Звісно" операційної системи.

- Серйозні перебої електроживлення системного блоку комп'ютера.

- Відмова контролера диска або дискового масиву.

- Відмова жорсткого диска.

- Вплив комп'ютерних вірусів, хробаків, троянів.

- Атака хакерів через Інтернет.

- Помилки в системному і прикладному програмному забезпеченні.

- Відмова змінних носіїв даних, що використовуються для резервного копіювання інформації (магнітних стрічок, магнітооптичних дисків, звичайних диску '!' і дискет ZIP і т. п.).

- Несумісність жорсткого диска з дисковим контролером, системною платою комп'ютера і драйвером ОС.

- Несправність кабелю, що з'єднує жорсткий диск з дисковим контролером, або ненадійне підключення цього кабелю до роз'ємів диска і контролера.

- Несправності системної плати і дискового контролера, викликані пилом.

- Пошкодження жорсткого диска в результаті падіння.

- Вихід комп'ютера з ладу при раптовому збільшенні напруги в електромережі (несправності в мережах електропостачання, робота зварювальних апаратів, влучення блискавки і т. д.).

- Дії зловмисників, в тому числі співробітників компанії.

- Пожежа в будівлі, де знаходиться комп'ютер, стихійне лихо, викраденню або диска, терористичний акт ".

Як показали результати детального аналізу, основним засобом підвищення відмовостійкості системи є внесення надмірності в конфігурацію апаратних і

програмних засобів, що підтримує інфраструктури та персоналу, резервування технічних засобів і інформаційних ресурсів (інформаційних масивів і програмних модулів)[7].

Розрізняють три основних види надмірності:

- програмну
- тимчасову (процеси відновлення і дампірованія)
- структурну (інформаційну та апаратну)

Таким чином, відмовостійкість забезпечується в основному використанням інформаційної (зберігання резервних даних), тимчасової (Процеси дампірованія і відновлення) і апаратної (наявність додаткових пристроїв і каналів зв'язку) видами надмірності.

Заходи щодо забезпечення відмовостійкості можна розділити на локальні і розподілені. Локальні заходи спрямовані на досягнення "живучості" окремих комп'ютерних систем або їх апаратних і програмних компонентів (в першу чергу з метою нейтралізації внутрішніх відмов автоматизованих систем). Прикладом подібних заходів є використання кластерних конфігурацій як платформи критичних серверів або "гаряче" резервування активного мережевого обладнання з автоматичним перемиканням на резерв. Якщо в число розглянутих ризиків входять серйозні аварії підтримуючої інфраструктури, що призводять до виходу з ладу на тривалий термін цілої виробничої площадки організації, слід передбачити розподілені заходи забезпечення живучості, наприклад, створення або оренда резервного обчислювального центру. У цьому випадку крім дублювання і / або тиражування ресурсів, необхідно передбачити засоби автоматичного або швидкого ручного переконфігурування компонентів автоматизованої системи, для перемикання з основної майданчики на резервну.

Одним з основних умов, необхідних для успішної розробки і реалізації заходів забезпечення високої доступності, є їх повнота і систематичність. Доброю практикою є складання і підтримка в актуальному стані карти автоматизованої системи організації, в якій фігурують все критично важливі об'єкти, їх стан, зв'язку між ними, процеси, асоційовані з об'єктами і зв'язками. За допомогою подібної

карти зручно формулювати намічені заходи, контролювати їх виконання, аналізувати стан автоматизованої системи. При виборі методів забезпечення високої доступності слід прагнути до забезпечення збалансованості між цінністю зберігається інформації, вартістю її зберігання з урахуванням витрат на підтримку надмірності та витратами на відновлення.

Збереження програм і даних забезпечується в основному використанням інформаційної надмірності (зберігання резервних даних), тимчасової (процеси відновлення і дампірування) і апаратної (наявність додаткових накопичувачів, серверів і т.д.) видами надмірності.

Метод резервування передбачає наявність ідентичною (при зберіганні копій) або неідентичних (при зберіганні передісторій) надмірності в системі [7]. При цьому розрізняють:

1. Оперативне резервування. Додаткові ресурси використовуються тільки для вирішення системою необхідних завдань. Відновлення що вийшли з ладу ресурсів не передбачено.

2. Відновне резервування. Частина резерву використовується тільки для відновлення зруйнованих робочих копій або передісторій, призначених для вирішення поточних завдань.

3. Оперативне резервування для вирішення системою необхідних завдань і відновне - для відновлення зруйнованих копій, використовуваних при оперативному резервування.

4. Резервування з метою забезпечення тривалого і надійного архівного зберігання програмних модулів і інформаційних масивів. Воно включає в себе як завдання визначення необхідного числа копій або передісторій модулів і масивів з урахуванням можливості їх руйнування при зберіганні, так і завдання організації функціонування архівів магнітних носіїв.

У ряді робіт [7] виділяють три основні стратегії резервування:

Стратегія 1. Застосовується для масивів постійних даних, в тому числі для програмних модулів. Полягає у створенні та використанні копій основного масиву.

У разі його руйнування використовується перша копія, при її руйнуванні - наступна і т.д.

Стратегія 2. Замість копій інформаційного масиву зберігаються його передісторії - попередні покоління масиву і відповідні їм масиви змін. При руйнуванні поточного масиву відбувається його відновлення по передісторії за допомогою програми оновлення.

Стратегія 3. Змішана стратегія, що передбачає зберігання як копій, так і передісторій. Резервування інформації проводиться методом поступового заміщення. Змінені частини масиву поміщаються в копію оригіналу. Оригінал видаляється лише після повного завершення оновлення і його підтвердження. Дві і більше копій є тільки під час оновлення.

Реалізація резервування даних здійснюється або шляхом створення прикладними програмами додаткових запитів записи даних на резервні пристрої пам'яті, або автоматичним дублюванням (тріорування) записи, що здійснюється на фізичному рівні, тобто або на рівні додатків, або на рівні пристроїв зберігання.

При експлуатації автоматизованих систем часто виникає необхідність в зберіганні великого обсягу даних в спеціалізованих архівах магнітних (або магнітооптичних) носіїв. При цьому використовуються дві основні стратегії резервування інформаційних масивів:

Стратегія А-1.

Робочі копії отримують з дубліката рівня т (в архіві зберігається основний масив-оригінал і т рівнів дублікатів. Якщо він руйнується, то його відновлюють з дубліката рівня (m-1) або при m=1 - з оригіналу, після чого знову робиться спроба отримання робочої копії. При цьому отримані раніше копії в якості дублікатів не використовуються.

Стратегія Л-2.

Робочі копії отримують з дублікатів рівня m, але при його руйнуванні дублікат може бути відновлений з будь-якої раніше отриманої робочої копії.

Метод дампірування поточної інформації передбачає періодичне зняття копії окремих інформаційних масивів (або всієї бази даних) на допоміжне пристрій з метою відновлення поточної інформації в разі її руйнування. У проміжках між

Зняття дампів ведеться системний журнал, званий «контрольним слідом », в якому реєструється послідовність дій, модифікують масиви, або значення записів до і після модифікації.

Системний журнал є основним засобом забезпечення збереження при використанні колективних даних. Головні цілі ведення системного журналу - відновлення поточного стану масивів шляхом послідовного здійснення операцій з ними, починаючи з останнього дампа, а також вилучення невірних результатів шляхом здійснення зворотного обробки.

Неможливість відновлення зруйнованої інформації в разі втрати системного журналу, що неприпустимо в більшості систем реального часу, вимагає резервування системного журналу декількома копіями.

1.3 Показники якості забезпечення доступності інформаційних ресурсів

Розглянемо докладніше, що ж входить в поняття доступності.

Інформаційна система надає своїм користувачам певний набір послуг (сервісів). Необхідний рівень доступності цих сервісів забезпечений, якщо такі показники знаходяться в заданих межах [8]:

- Ефективність послуг. Ефективність послуги визначається в термінах максимального часу обслуговування запиту, кількості підтримуваних користувачів і т.п. Потрібно, щоб ефективність не знижувалася нижче заздалегідь встановленого порога.

- Час недоступності. Якщо ефективність інформаційної послуги не задовольняє накладеним обмеженням, послуга вважається недоступною.

Потрібно, щоб максимальна тривалість періоду недоступності і сумарний час недоступності (сума періодів недоступності) за деякий проміжок часу не перевищували заздалегідь заданих меж.

Як правило, потрібно, щоб інформаційна система працювала з необхідної ефективністю. Для деяких критично важливих систем (наприклад, систем управління технологічними процесами, телекомунікаційних систем) час недоступності має мінімізуватися. У такому випадку ймовірність виникнення недоступності не повинна перевищувати заданої величини. Для вирішення даного завдання створюються відомовості системи, вартість яких значно перевищує вартість звичайних систем. До переважної більшості комерційних систем пред'являються менш жорсткі вимоги, однак сучасна ділова життя накладає досить жорсткі обмеження. Якщо кількість обслуговуваних користувачів досить велике, час відгуку не повинно перевищувати декількох секунд. При цьому час недоступності становить кілька годин в рік. Середня вартість години простою автоматизованої системи для різних галузей приведена в таблиці 1.1.

Таблиця 1.1.

Середня вартість години простою автоматизованої системи для різних галузей

Галузь	Додаток	Середня вартість години простою
Фінанси	Брокерські операції	$6500000
Фінанси	Продажі по кредитам к-м	$2600000
Медіа	Платежі за перегляд	$1150000
Роздрібна торгівля	Придбання за телевізор	$113000
Роздрібна торгівля	Продаж по каталогам	$90000
Транспорт	Резервування авіабілетів	$89500

З наведеної таблиці видно, що найбільша вартість години простою автоматизованої системи в даний час спостерігається серед компаній фінансового сектора. Згідно з опитуванням, проведеним компанією Eagle Rock Alliance серед

компаній фінансового сектора, втрати можуть бути настільки значні (див. рис.1.12), що більше 40% компаній припиняють існування вже при 72-годинному простої IT-сервісів. Жоден з провідних банків не може дозволити собі і цих трьох діб.

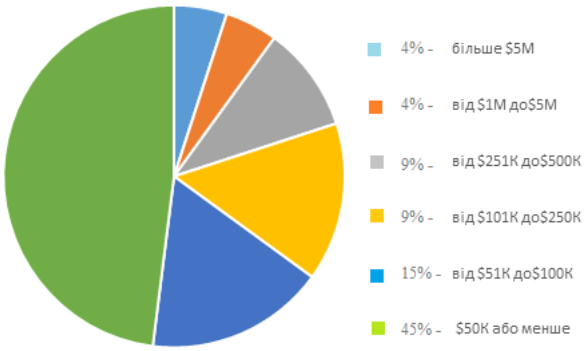

Рисунок 1.12- Фінансові втрати від однієї години простою IT-сервісу

У загальному випадку доступність системи досягається [8] за рахунок застосування трьох груп заходів, спрямованих на підвищення:

- безвідмовності - мінімізація ймовірності виникнення будь-якого відмови;

- відмовостійкості (живучості) - збереження доступності системи незважаючи на відмову будь-яких компонентів;

- обслуговуваемості - мінімізація часу непрацездатності відмовили компонентів, а також мінімізація негативного впливу ремонтних робіт на ефективність інформаційних сервісів).

Ключовими характеристиками, які визначають вимоги бізнесу до доступності IT-сервісів, є наступні параметри:

- RPO - Recovery Point Objective - (цільова точка відновлення) - інтервал часу, що передує аварії, на якому допускається втрата даних. Іншими словами, цей параметр показує, наскільки стан системи може відкотитися назад при надзвичайній ситуації;

- RTO - Recovery Time Objective - (цільове час відновлення) - інтервал часу після аварії, необхідний для відновлення IT- сервісів;

- DOO - Degraded Operations Objective - допустиме уповільнення виконання операцій системою, обумовлене перекладом обробки даних на резервні майданчики;

- NRO - Network Recovery Objective - мінімальна смуга пропускання мережі, яка належна бути відновлена для забезпечення можливості продовження виконання операцій.

Доступність системи для використання, як показник її надійності для кінцевого користувача, також можна виразити в процентному співвідношенні між працездатним станом системи і часом її простою по будь-якої причини, в тому числі і плановими простоями (до них відносяться профілактичні роботи, реконфігурації, зміна версій програмного забезпечення, модернізація обладнання і т.п.) [8].

Для оцінки доступності інформаційних ресурсів вводять поняття коефіцієнта готовності [7].

Значення коефіцієнта готовності можна отримати за формулою

$$K_Г = \frac{t_p}{T} \times 100\% \quad (1.2)$$

де t_p- тривалість перебування системи в робочому стані за зазначений період;

Т - сумарний час доступу до системи за вказаний період (включаючи час відновлення після збою).

Залежно від рівня доступності автоматизованої системи для використання виділяють чотири рівні надійності системи, перераховані в Таблиці 1.2.

Виділяють також такі показники, як ймовірність виникнення стану недоступності, максимальна тривалість періоду недоступності (час відновлення), число періодів вимушеної недоступності за аналізований період експлуатації системи (Сумарний час недоступності).

Для типового сучасного сервера величина доступності для використання становить 99,0%. Практика показує, що при ретельній налаштування операційної системи і продуманому системному адмініструванні надійність звичайного сервера можна довести до рівня 99,5% і навіть до 99,8%. Однак при досягненні 99,5% -ної доступності основну роль серед причин простою системи починають грати так

звані зовнішні причини (помилки в програмному забезпеченні, некваліфіковані дії персоналу і т.д.), від яких функціонування звичайного сервера не застраховане. Кластерна технологія дозволяє забезпечити рівень доступності системи для використання в 99,9% і вище, що на практиці означає менше 8 годин простою в рік.

Таблиця 1.2.

Рівні надійності системи

Рівень готовності % значення коефіцієнта готовності	Макс. час простою	Тип системи
99,0	3,5 дня в рік	Звичайна
99,9	8,5 годин в рік	Висока надійність
99,99	1 год в рік	Відмовостійка
99,999	5 хв. В рік	Безвідмовна

Для сучасних територіально-розподілених автоматизованих систем, побудованих за технологією клієнт/сервер, завдання забезпечення високої доступності необхідно вирішувати комплексно.

Це означає, що захисту потребує весь ланцюжок - від користувачів (Можливо, віддалених) до критично важливих серверів (в тому числі серверів безпеки).

Для забезпечення високої доступності інформаційних ресурсів в систему вводять надмірність для продовження роботи в разі відмови одного з компонентів системи. Наприклад таких, як руйнування інформаційного масиву або програмного модуля, а також виходу з ладу процесора, жорсткого диска, мережевої карти, каналу зв'язку та інших відмовах і збоях апаратного і програмного забезпечення. Якщо така відмова відбувається, система переносить робоче навантаження на резервні пристрої або навіть на інший вузол. Але в деяких випадках і такий захист не зможе забезпечити достатній рівень надійності. У разі повного краху майданчики, на якій розташований центр обробки даних, для підтримки безперервності функціонування системи обробки даних необхідне рішення, що забезпечує роботу при множинних відмовах.

Незважаючи на досить високу надійність сучасного обладнання та застосовуваних технологій резервування і відновлення даних, зберігається можливість недоступності системи для користувачів протягом тривалого часу в разі виникнення надзвичайної ситуації (пожежа, затоплення, тривалий відключення електроживлення і.т.д.), зачіпає майданчик, на якій проводиться обробка даних. В цьому випадку всі інформаційні ресурси, розміщені на даній майданчику, виявляться недоступними для користувачів на досить тривалий проміжок часу. Крім цього зберігається можливість безповоротної втрати даних, резервні копії яких не були зроблені, або були знищені. Тому останнім часом в світі активно розвивається напрямок по створенню катастрофостійкої систем.

Катастрофостійкостю називається можливість системи відновити працездатність додатків і даних, що забезпечують безперервність основних виробничих процесів, протягом прийнятного періоду часу після катастрофи. При цьому під катастрофами маються на увазі не тільки такі лиха як пожежа, потоп, землетрус та інші природні або техногенні катастрофи, а й можливі непередбачені збої в роботі служб, руйнування даних або пошкодження всього центру обробки в

Внаслідок різних причин, наприклад, розрив телекомунікаційних ліній в результаті проведення ремонтних робіт, навмисної диверсії або саботажу, різні соціальні чинники (страйки, громадські заворушення, військові дії тощо), що ведуть до неможливості продовжувати обробку даних в наявному центрі обробки. Таким чином, в даному контексті катастрофою можна вважати будь-яку подію, що веде до зупинці сервісу, що забезпечує безперервність бізнесу, або до втрати даних. Захистом від катастроф (Disaster Recovery) називається розробка заходів, що забезпечують здатність організації відновити обробку даних на іншому майданчику, якщо катастрофа зруйнувала основну площадку або іншим чином привела її в непрацездатний стан. Це одна з компонент загального плану забезпечення безперервності бізнесу (Business Continuity Plan) [9].

2 ПІДВИЩЕННЯ НАДІЙНОСТІ ВІДДАЛЕНОГО ЗБЕРІГАННЯ ДАНИХ В РОЗПОДІЛЕНИХ СИСТЕМАХ

2.1 Аналіз існуючих стратегій резервування

Для підвищення рівня доступності інформаційних масивів і програмних модулів в межах одного вузла обчислювальної мережі традиційно виділяють три стратегії резервування [7]. При цьому у ролі вузла можуть розглядатися окремий сервер, серверний кластер, територіально-розподілений кластер, центр обробки даних.

Традиційно виділяють наступні основні стратегії резервування:

Стратегія 1. Використовується певна кількість копій масиву. якщо основний масив зруйнувався, то використовується перша його копія. Якщо і вона зруйнувалася, то використовується наступна копія і т.д.

Стратегія 1 може використовуватися для масивів постійних і поточних даних.

Стратегія 2. При використанні цієї стратегії замість копій інформаційного масиву зберігаються його передісторії – попередні покоління масиву і відповідні їм масиви змін. При руйнуванні поточного масиву відбувається його відновлення по передісторії за допомогою програми оновлення.

Стратегія 3. Змішана стратегія, що передбачає зберігання як копій, так і передісторій. Резервування інформації проводиться методом поступового заміщення. Змінені частини масиву поміщаються в копію оригіналу. Оригінал видаляється лише після повного завершення оновлення і його підтвердження. Дві і більше ідентичні копії є тільки у час оновлення.

Розглянемо зазначені стратегії більш докладно:

Основними характеристиками стратегій резервування є:

P_j - ймовірність успішного вирішення завдання за одиничний проміжок часу при використанні j- стратегії резервування (j = 1,2,3);

M [$T^у$] - середній час виконання завдання за умови її успішного вирішення;

M[$T^р$] - середній час до руйнування масиву і його копій і (або) передісторій;

M [T] - середній час виконання завдання або плановане час доступу до ресурсів системи;

Отримаємо аналітичні вирази для визначення основних тимчасових і імовірнісних характеристик різних стратегій резервування для випадку, коли моделлю виникнення помилок є схема незалежних випробувань [7].

Стратегія 1. (Використовується певна кількість копій масиву. Якщо основний масив зруйнувався, то використовується перша його копія. Якщо і вона зруйнувалася, то використовується наступна копія і т.д.). Граф станів системи при використанні стратегії 1 представлений на рис. 2.1.

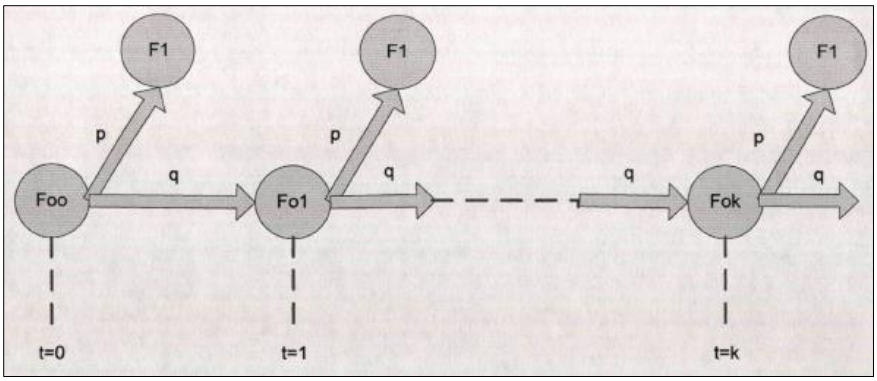

Рис. 2.1. Граф станів системи при використанні стратегії 1

Основний масив F_{00} резервується K копіями $\{F_{0r}\}$, $r = \overline{1,k}$. Нехай мовірність того, що масив не буде зруйноване за одиничний інтервал часу при його використанні, дорівнює $P_{исп}$. Відповідно, ймовірність руйнування масиву при його використанні за одиничний інтервал часу буде $q_{исп}= 1-P_{исп}$. Можливість руйнування масиву під час зберігання за одиничний інтервал часу приймається рівною $q_{хран}$.

Таким чином, ймовірність того, що масив не буде зруйноване за одиничний інтервал часу, буде $p=1-(q_{исп} + q_{хран})$.

Імовірність того, що масив зруйнується за одиничний проміжок часу буде:

$q = q_{исп} +q_{хран}=1-(p_{исп}+p_{хран}) =1-p$

Якщо копія F_{0r}, $r = \overline{1,k-1}$ руйнується в заданий одиничний інтервал часу, наступна копія F_{0r+1} використовується в наступний одиничний інтервал часу для закінчення виконання завдання і т.д. визначимо ймовірність успішного вирішення

завдання при наявності k копій основного масиву. Імовірнісний процес функціонування системи при рішенні завдання може бути представлений у вигляді:

$$p + pq + pq^2 + ... + pq^k + q^{k+1} = 1.$$

Імовірність успішного вирішення завдання $P_1 = 1 - q^{k+1}$ (Індекс I позначає використання першої стратегії резервування).

Визначимо оптимальне число копій масиву - £. Для визначення оптимальної величини £ використовуються статистичний або детермінований підходи.

Для апріорі великих k для оцінки £ може бути використана центральна гранична теорема. В цьому випадку можна записати:

$$Bep\{M(x) - d \le \bar{x} \le M(x) + d\} = 1 - \alpha$$

Звідки £ може бути визначено у вигляді £=$\{d^{-1}\sigma t\}^2$

Де $\sigma = \sqrt{qp^{-2}}$

M (x) =qp^{-1}

де: 2d - допустимі межі зміни k для заданої ймовірності негативної події α;

t - стандартний нормальний відхилення.

Детермінована оцінка k визначена за умови, що величина σ мала при заданій величині $P_1=\gamma$. Вирішивши рівняння $P_1= 1 – q^{k+1}$, отримаємо

$$k = \frac{\ln(1-\gamma)}{\ln q} - 1.$$

Розглянемо тимчасові характеристики процесу використання оперативного резерву при використанні стратегії I.

Нехай $M[T_1^{(1)}] = k\tau$, де τ - час створення однієї копії.

Тоді середній час вирішення завдання при наявності до копій і за умови, що задача вирішена успішно, визначається у вигляді

$$M\left[T_1^{(2)}\right] = \theta p^{-1}\left\{1 - q^{k+1}\left[1 + (k+1)p\right]\right\},$$

Де θ- час виконання завдання.

Середній час, витрачений на вирішення завдання, незалежно від того, буде вона вирішена успішно чи ні, визначається виразом:

$$M\left[T_I^{(3)}\right] = \theta p^{-1}(1-q^{k+1})$$

Отже, плановане середній час доступу до ПК при використанні стратегії I буде

$$M[T_I] = M\left[T_I^{(1)}\right] + M\left[T_I^{(3)}\right]$$

Стратегія 2. Зберігаються передісторії - попередні покоління масиву і відповідні їм масиви змін. При руйнуванні поточного масиву відбувається його відновлення по передісторії за допомогою програми оновлення. Граф станів системи при використанні стратегії 2 представлений на рис. 2.2.

Для отримання аналітичних виразів для даної стратегії скористаємося моделлю, що застосовуються при вирішенні класичної завдання про розорення.

Резервування масивів формується наступним чином:

Нехай в початковий момент в системі є до передісторій і масивів змін основного масиву F_{00}, тобто $F_{-1}, F_{-2}, \ldots, F_{-k}$, які використовуються для вирішення деякої задачі. потрібно створити оновлений масив.

Нехай за фіксоване (одиничне) час оновлений масив може бути створений з ймовірністю p, з ймовірністю q =p-1 масив може бути зруйнований.

Робота системи триває до тих пір, поки масив F_{00} і до його передісторій ні зруйновані, або не буде створено оновлений масив.

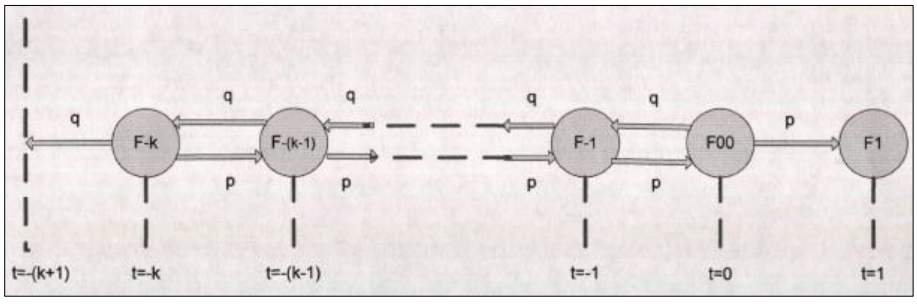

Рис.2.2. Граф станів системи при використанні стратегії 2

При використанні даної стратегії резервування основними характеристиками системи будуть:

- ймовірність руйнування масиву і k його передісторій;
- тривалість роботи ПК до поновлення масиву;
- тривалість роботи ПК до руйнування всіх передісторій;

- середній час функціонування ПК.

Результати поновлення масивів можна уявити як переміщення точки по осі Z. У момент t = 0 точка знаходиться в положенні z= k + 1, а в момент t = 1,2, ... Вона переміщається на один крок вліво або вправо в залежності від успіху або невдачі відповідного оновлення, тобто здійснює випадкові блукання. Положення точки в довільний момент часу ξ визначає кількість незруйнованих передісторій після закінчення ξ -й спроби оновлення. Робота закінчується, коли точка потрапляє в одне з поглинаючих станів. (z = 0 або z= k+ 2).

Нехай q_z - ймовірність того, що масив F_{00} і до його передісторій будуть зруйновані, а p_z - ймовірність того, що масив буде оновлено. В термінах випадкових блукань q_z і p_z означають ймовірність того, що точка, що виходить зі стану z, буде поглинена екранами z= 0 або z= k + 2 відповідно.

Якщо система знаходиться в стані'у то після першої спроби поновлення вона перейде в стан z-1 або z + 1, тому для 1 <z <k + 1

$$q_z = pq_{z+1} + qq_{z-1}.$$

Відомо, що для z = 1 q = q2p+q,

а для z = k +1 q_{k+1}=qq_k,

При граничних умовах $q_0 = 1$ і $q_{k+2}= 0$, а також при $q \neq p$ рішення рівняння має вигляд:

$$q_z = \left[qp^{k+2} - 1\right]^{-1}\left[qp^{k+2} - (q/p)^z\right]$$

Звідси, враховуючи, що початковий стан системи z = k + 1, визначаємо

ймовірність руйнування масиву F_{00} всіх його передісторій:

$$q_{k+1} = [q^{k+2} - p^{k+2}]^{-1}[q^{k+1}(q-p)]$$

Це рішення не має сенсу при p = q = 1/2, але практично завжди p> q.

Визначимо ймовірність успішного оновлення масиву F_{00} використанні стратегії II, яка вийде з виразу для визначення q_z заміною p, q і z на q, p і k + 2-z відповідно, тобто

$$P_2 = P_{k+1} = p[p^{k+2} - q^{k+2}]^{-1}[p^{k+1} - q^{k+1}]$$

Визначимо детерміновану оцінку $\hat{k}$ для $p_и = \gamma$:

$$\hat{k} = \left\{ [\ln(p/q)]^{-1} \ln[1-(1-\gamma)^{-1}(1-p/q)] \right\} - 2.$$

Статистична оцінка до може бути визначена аналогічно її визначенню для стратегії I.

Розглянемо тимчасові характеристики процесу при використанні стратегії II. Для визначення середньої тривалості роботи ПК до поновлення масиву F_{00} і до руйнування цього масиву і до його передісторій застосуємо метод виробляють функцій. Дане завдання аналогічне завданню визначення тривалості випадкового блукання точки з вихідного стану при наявності поглинаючих екранів при z = k + 2 і z = 0. Так само як і раніше, вихідним положенням точки є z (0 <z <k + 2).

Нехай $u_{z,\xi}$ - ймовірність того, що процес закінчиться на ξ кроці перед екраном z = 0. Після першої спроби поновлення система потрапляє або в точку z + 1, або в точку z-1 і при 1 <z <k + 1 і $\xi > 1$ можна записати:

$$u_{z,\xi+1} = pu_{z+1,\xi} + qu_{z-1,\xi}$$

Дане рівняння є різницевим і залежить від двох змінних: z і ξ.

Граничні умови мають вигляд:

$u_{z,\xi} = u_{k+2,\xi} = 0$ при $\xi \geq 1$ и $u_{00} = 1$, $u_{z,0} = 0$ при z>0, $\forall z$, 0<z<k+2 и $\xi \geq 0$.

Введемо виробляє функцію

$$U_z(s) = \sum_{\xi=0}^{\infty} U_{z,\zeta} s^{\zeta}$$

Ця виробляє функція ймовірності руйнування масиву F_{00} всіх його-передісторій на кроці (поглинання біля екрану z = 0) може бути представлена у вигляді:

$$U_l(s) = (qp^{-1})^z \left[\lambda_1^{k+2}(s) - \lambda_2^{k+2}(s)\right]^{-1} \left[\lambda_1^{k+2-z}(s) - \lambda_2^{k+2}(s)\right], \qquad (2.1)$$

де

$$\lambda_1(s) = (2ps)^{-1}\left[1 + \left(1 - 4pqs^2\right)^{1/2}\right];$$

$$\lambda_2(s) = (2ps)^{-1}\left[1 - \left(1 - 4pqs^2\right)^{1/2}\right] \quad \text{для} \quad 0 < s < 1.$$

Тоді математичне очікування часу до руйнування масиву і всіх його передісторій M ($T_{d,z}$) за умови, що процес функціонування почався в точці z, може бути визначено як

$$dU_z(s)/ds\big|_{s\to 1} = M\left(T_{d,z}\right).$$

Можна показати, що для z=k +1 маємо

$$M(T_{d,k+1}) = (qp^{-1})^{k+1} \times C\left(A^{K+2} - B^{K+2}\right)^{-2}\eta,$$

Де

$$\eta = (\kappa+2)(A^{k+2}+B^{k+2})(A-B) - (A^{k+2}-B^{k+2})(A+B);$$

$$A = \lambda_1(s)\big|_{s\to 1}, \quad B = \lambda_2(s)\big|_{s\to 1},$$

$$C = (1-4pq)^{1/2}$$

Виробляє функція ймовірності успішного оновлення масиву F_{00} (успішного вирішення завдання) на ξ -му кроці має вигляд:

$$F_z(s) = (pq^{-1})^{k+2-z}\left[\lambda_1^{k+2}(s) - \lambda_2^{k+2}(s)\right]^{-1}\left[\lambda_1^{z}(s) - \lambda_2^{z}(s)\right] \qquad (2.2)$$

Математичне сподівання часу до успішного закінчення рішення задачі M($Tq_{q,z}$) за умови, що процес почався в точці z, визначимо як

$$dF_z(s)/ds\,|_{s\to 1} = M(T_{q,z}).$$

Можна показати, що при z = k +1

$$M\left[T_z^y\right] = M(T_{q,k+1}) = (qp^{-1})^1 \times C\left[\left(A^{k+2} - B^{k+2}\right)^{-2}\eta\right],$$

де

$$\eta = (k+2)(A^{k+2}+B^{k+2})(A^{k+1}-B^{k+1}) - (k+1)(A^{k+2}+B^{k+2})(A^{k+1}+Bk+1);$$

$$A = \lambda_1(s)\big|_{s\to 1}, \quad B = \lambda_2(s)\big|_{s\to 1}, \quad C = (1-4pq)^{1/2}.$$

Виробляє функцією тривалості функціонування ПК до поновлення масиву Г0 () або до руйнування всіх масивів буде сума виробляють функцій (2.3.2) і (2.3.3). Однак, якщо тривалість функціонування має кінцеве математичне очікування, q ≠p і процес починається в стані z, для визначення середньої тривалості функціонування ПК можна застосувати більш простий метод. Розмірковуючи так

само, як при виводі рівняння (2.2), отримаємо $D_z=pD_{z+1}+qD_{z-1}+1$ при $0<z<k+2$ і граничних умовах $D_0=0$, $D_{k+2}=0$.

Враховуючи на те що z= k +1 і q < отримаємо:

$$M[T_2]=\theta D_{k+1}=\left[\frac{\theta}{q-p}\right]\left[k+1=(k+2)\times\frac{1-(qp^{-1})^{k+1}}{1-(qp^{-1})^{k+2}}\right].$$

Відзначимо, що при q →> 1/2, D_z =z (a - z) і при z = k +1

$$M[T_2]=\theta D_{k+1}=\theta(k+1),\ \text{где}\ a=k+2.$$

Стратегія 3. (Змішана стратегія - зберігаються як копії, так і передісторії.

Резервування інформації проводиться шляхом поступового заміщення. Змінені частини масиву поміщаються в копію оригіналу.

Оригінал видаляється лише після повного завершення оновлення та його підтвердження. Дві і більше копій є тільки під час оновлення.)

Процес функціонування системи при використанні стратегії 3 представлений на рис. 2.3.

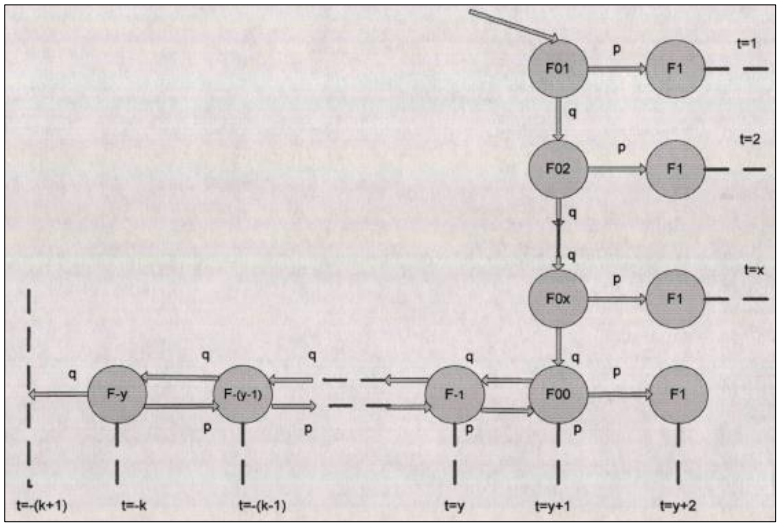

Рис. 2.3. Процес функціонування системи при використанні стратегії 3

Використовуючи результати, отримані для стратегій I і II, отримуємо ймовірність успішного вирішення завдання при застосуванні масиву F_{00} (успішного оновлення) у вигляді

$$P_3 = 1 - q^x\left[\frac{q^{y+1}(q-p)}{q^{y+2}-p^{y+2}}\right]$$

Спростимо цей вислів, використовуючи співвідношення к = х + у,

Де x - число копій масиву F_{00} і y - число його передісторій.

При цьому

$$P_3 = 1 - \left[q^{y+2} - p^{y+2}\right]^{-1}\left[q^{k+2}(q-p)\right]$$

Детермінована оцінка £ може бути знайдена з цього рівняння при заданих значеннях γі y і відповідних значеннях x =1,23,, (л - у).

Визначимо тимчасові характеристики процесу при використанні даної стратегії. Математичне сподівання планованої тривалості функціонування ПК при цьому визначимо з виразу:

$$M[T_3] = M\left[T_3^{(1)}\right] + M\left[T_3^{(2)}\right]$$

де

$$M\left[T_3^{(1)}\right] = x\tau + \theta p^{-1}(1-q^x),$$

$$M\left[T_3^{(2)}\right] = \frac{\theta q^x}{q-p}\left[(y-1) - \frac{(y+2)\left[1-(qp^{-1})^{y+1}\right]}{1-(qp^{-1})^{y+2}}\right].$$

Таким чином

$$M[T_3] = x\tau + \theta p^{-1}(1-q^x) + \frac{\theta q^x}{q-p}\left[(y-1) - \frac{(y+2)\left[1-(qp^{-1})^{y+1}\right]}{1-(qp^{-1})^{y+2}}\right].$$

Результати дослідження стратегій резервування представлені в табл. 2.1.

Таблиця 2.1.

Результати дослідження резервування

№ Стра-тегії	Характеристики	
	P_j-ймовірність успішного рішення задачі за одиничний проміжок часу при використанні j-ї стратегії резервування (j=1,2,3)	$M[T_j]$-середній час рішення задачі чи плануючий час доступу до ресурсів системи при використанні j=ї стратегії резервування (j=1,2,3)
1	$P_1 = 1 - q^{k+1}$	$[T_1] = \theta p^{-1}(1-q^{k+1}) + k\tau$

2	$P_2 = p[p^{k+2} - q^{k+2}]^{-1} \times [p^{k+1} - q^{k+1}]$	$M[T_2] = \left[\frac{\theta}{q-p}\right] \times [k+1 = (k+2) \times \frac{1-(qp^{-1})^{k+1}}{1-(qp^{-1})^{k+2}}$
3	$P_3 = 1 - [q^{y+2} - p^{y+2}]^{-1} \times [q^{k+2}(q-p)]$	$M[T_3] = x\tau + \theta p^{-1}(1-1^3) + \frac{\theta q^2}{q-p}[(y-1) - \frac{(y+2)[1-(qp^{-1})^{y+1}]}{1-(qp^{-1})^{y+2}}$

2.2 Використання методів організації резервування, орієнтованих на успішне вирішення функціональних задач

Розглянемо особливості розрахунку імовірнісних, тимчасових і вартісних характеристик для основних схем оперативного резервування інформаційних масивів і IT-сервісів в територіально розподілених IT-інфраструктурах з виділеними центрами обробки даних. При використанні схем 1.1 і 1.2 вся обробка даних зосереджена в єдиному ЦОД. При цьому в рамках локальної мережі ЦОД-а можливо як централізоване (рис. 2.4.), Так і децентралізоване (рис.2.5.) розміщення резерву, а також використання різних стратегій оперативного резервування в вузлах локальної мережі.

При цьому для розрахунку основних характеристик використовуваної схеми резервування можна використовувати аналітичні вирази, наведені в таблицях 2.2, 2.3 та 2.1., враховуючи ймовірність виходу з ладу всієї виробничої площадки ЦОД в розглянутий одиничний проміжок часу - $Q^{цод}$ і можливість резервування каналів зв'язку, а також окремих складових підсистеми інформаційної безпеки.

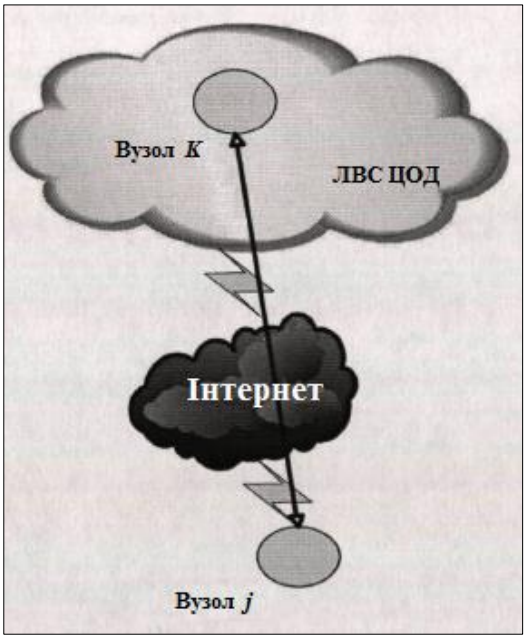

Рис.2.4. Централізоване розміщення резерву

У таблиці 2.2. наведені вирази для розрахунку характеристик оперативного резерву, розташованого в єдиному ЦОД, при централізованому зберіганні резерву в одному вузлі. При цьому значення $t_з$ і r_{jk} розраховуються за формулами, значення $P_к(x_к)$ і $M_к(x_к)$ - за формулами, наведеними в табл. 2.1.

Таблиця 2.2.

Вирази для розрахунку характеристик оперативного резерву

$p_j t_j, Z, ZP$
$p_j = (1 - Q^{ЦОД}) r_{jk} P_k(x_k) r_{kj}$
$z = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j + V_j) y_k \, Z_{jk}(x_k) = 2(1 - r_{jk}) D_{jk} + [1 - P_k(x_k)] M_k(x_k) h_k$
$t_j = 2t_з(1 - y_j) + \sum_{k+1}^{N} M_k(x_k) y_k$
$ZP = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j + V_j) y_k \, ZP_{jk}(x_k).;\ ZP_{jk}(x_k) = 2D_{jk} + M_k(x_k) h_k$

У разі розміщення оперативного резерву в єдиному ЦОД, при децентралізованому зберіганні резерву в К різних вузлах в межах даного ЦОД-а

(рис. 2.3.), основні характеристики оперативного резерву для різних дисциплін обробки запитів наведені в таблиці 2.3.

При цьому значення $t_з$ і r_{jk} до розраховуються за формулами, значення $P_к$ ($x_к$) і $M_к$ ($x_к$) - за формулами, наведеними в табл. 2.1.

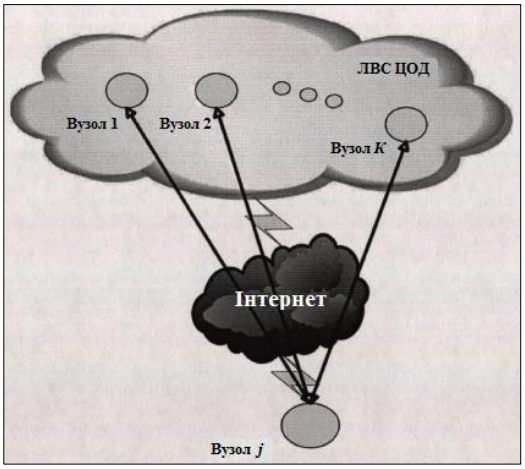

Рис. 2.5. Децентралізоване розміщення резерву

При обробці даних в основному ЦОД можуть використовуватися різні дисципліни обробки запитів і стратегії оперативного резервування, основні характеристики яких розраховуються на основі аналітичних виразів, наведених в таблицях 2.2. і 2.3. Особливості відновного резервування будуть розглянуті в главі

3. У резервному ЦОД також можуть використовуватися різні стратегії оперативного резервування і дисципліни обробки запитів. При використанні розглянутих схем оперативне резервування в резервному ЦОД-і буде актуальним у разі виходу з ладу основного ЦОД-а і перекладу обробки даних в резервний ЦОД. Для розрахунку основних характеристик оперативного резервування, здійснюваного в резервному ЦОД, також можуть використовуватися вирази, наведені в табл. 2.2. і 2.3.

При використанні схем, які передбачають оперативне резервування основного ЦОД-а одним або декількома резервними ЦОД-ами, оперативне резервування здійснюється як всередині кожного з ЦОД-ів, так і на рівні глобальної мережі зв'язку. При цьому ЦОД-ди розглядаються в якості вузлів глобальної

мережі (рис. 2.6.). Слід виділити схеми з використанням синхронної і асинхронної реплікації даних на резервні майданчики.

Таблиця 2.3.

Характеристики оперативного резерву для різних дисциплін обробки запитів

№ Дисципліни обробки запитів	$p_j t_j, Z, ZP$
1	$p_j = (1 - Q^{ЦОД}) \sum_{k=1}^{N} r_{jk} P_k r_{kj} \psi_{jk};$
	$z = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j \psi_{jk} + V_j y_k) Z_{jk};\ Z_{jk} = 2(1 - r_{jk}) D_{jk} + [1 - P_k] M[T_k] h_k$
	$t_j = 2t_3(1 - \psi_{jj}) + \sum_{k+1}^{N} M[T_k] \psi_{jk}$
	$ZP = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j \psi_{jk} + V_j y_k) ZP_{jk};\quad ZP_{jk} = 2D_{jk} + M[T_k] h_k$
2	$p_j = (1 - Q^{ЦОД})(1 - \prod_{k=1}^{N} [1 - r_{jk} P_k r_{kj} \psi_{jk}]);$
	$ZP = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j \psi_{jk} + V_j y_k) Z_{jk};\quad Z_{jk} = 2(1 - r_{jk}) D_{jk} + [1 - P_k] M[T_k] h_k$
	$t_j = max\{2t_3 + max M[T_k] M[T_j] \psi_{jj}\};$
	$ZP = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j \psi_{jk} + V_j y_k) ZP_{jk};\ ZP_{jk} = 2D_{jk} + M[T_k] h_k$
3	$p_j = (1 - Q^{ЦОД}) \sum_{n=1}^{k} r_{jj} P_j r_j \prod_{I=2}^{n} [1 - P_{j_{i-1}}] r_{j_{i-1} j_i};$ $j_i \in N, i = \overline{1, K};$
	$Z = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j \psi_{jk} + V_j y_k) Z_{jk};\quad Z_{jk}(x_k) = 2(1 - r_{jk}) D_{jk} + [1 - P_k] M[T_k] h_k$
	$ZP = \sum_{j=1}^{N} \sum_{k=1}^{N} (U_j \psi_{jk} + V_j y_k) Z_{jk};\quad ZP_{jk} = 2D_{jk} + M[T_k] h_k$

	$t_j = (K+1)t_3 \sum_{k=1}^{N} M[T_k]\psi_{jk} - B;$
	$B = \begin{cases} t_3, \text{ при } n(j,j) = 1 \text{ або } n(j,j) = K; \\ 0, \text{ в інших випадках} \end{cases}$
3	$p_j = (1 - Q^{ЦОД}))(1 - \prod_{k=1}^{N}[1 - r_{jk}M[T_k]r_{kj}\psi_{jk}]);$
	$Z = \sum_{j=1}^{N}\sum_{k=1}^{N}\left\{U_j \prod_{I=1}^{n(j,k)-1}[1 - r_{jj_i}P_j r_{j,j}] + V_j y_k\right\} Z_{jk},$ $j_i \in N, i = \overline{1,K};$
	$t_j = 2t_3(K - \psi_{jj}) + \sum_{k=1}^{N} M[T_k]\psi_{jk};$
	$ZP = \sum_{j=1}^{N}\sum_{k=1}^{N}\left\{U_j \prod_{I=1}^{n(j,k)-1}[1 - r_{jj_i}P_j r_{j,j}] + V_j y_k\right\} ZP_{jk},$
	$Z_{jk} = 2(1 - r_{jk})D_{jk} + [1 - P_k]M[T_k]h_k;$
	$ZP_{jk} = 2D_{jk} + M[T_k]h_k;$
	$U_{ik} = \begin{cases} \sum_{j=1}^{N} \psi_n \psi_{jk} U_{jk}^{(j)} \text{ при } n(j,i)+1 \\ 0, \text{ в інших випадках} \end{cases}$ $U_{jk}^{(j)} = U_j \prod_{I=1}^{n(j,k)-1} r_{j_{a-1}j\alpha}[1 - P];$ $j_0 = j;\ j_0 \in N;$

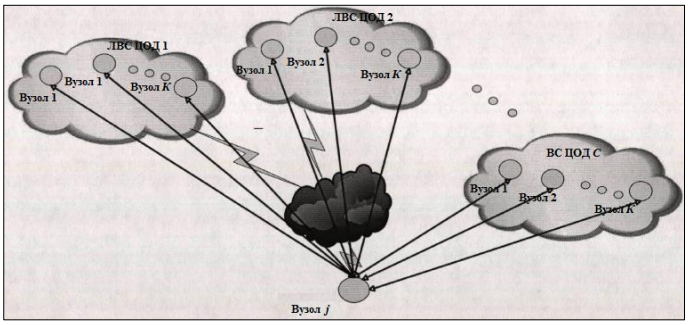

Рис.2.6. Приклад ЦОД-ів в якості вузлів глобальної мережі

При резервуванні ЦОД-ів, які передбачають розподілену обробку, (кожен ЦОД використовується у виробничій діяльності), окремо розглянемо основні використовувані схеми. Розподілений ЦОД з синхронної реплікації з точки зору використання різних схем резервування та дисциплін обробки запитів можна прирівняти до єдиного ЦОД, всі вузли якого знаходяться в одній локальній мережі. При цьому розрахунок основних характеристик буде проводитися на основі аналітичних виразів, наведених в таблицях 2.2. і 2.3.

У разі розподіленої обробки з асинхронної реплікації для відповідальних додатків організовується перехресне резервування, при якому основний і резервний сервери і сховища даних розташовуються на різних майданчиках. З точки зору розрахунку основних характеристик дана схема аналогічна асинхронної реплікації в резервний ЦОД.

2.3 Аналіз існуючих методів відновного резервування

Відновлювальних резервуванням є створення і зберігання однієї або декількох резервних копій і (або) передісторій, призначених для відтворення поточної версії масиву і копій оперативного резерву в разі їх руйнування. На відміну від розглянутого раніше методу оперативного резервування, відновний резерв призначений не для вирішення поточного завдання (поновлення, розрахунку і т. п.), а для відтворення зруйнованого основного масиву і його оперативного резерву. У циклі відновного резервування можливе використання носіїв інформації різних типів і вартості (жорстких дисків різного типу, магнітооптичних дисків, DVD - дисків, магнітних стрічок, машинних роздруківок первинних документів і т. п.). У багатьох випадках застосування відновного резервування є єдиним способом збереження працездатності системи обробки даних. Наприклад, в разі помилок оператора, помилок в програмі або введенні невірних даних, в внаслідок яких була порушена достовірність основного масиву і всіх копій оперативного резерву [7]. У разі чималих допустимих значень RPO (Recovery Point Objective - цільова точка відновлення - інтервал часу, що передує аварії, за який допускається втрата даних)

і RTO - Recovery Time Objective - цільове час відновлення - інтервал часу після аварії, необхідний для відновлення IT-сервісів), на випадок виходу з ладу всього Центру обробки даних (ЦОД) можна передбачити використання тільки відновного резервування, тому що його організація набагато дешевше організації оперативного. Так, відповідно до семирівневої класифікацією систем віддаленого резервування даних, що зберігаються в ЦОД, яка була розроблена в 1992 р користувальницької групою SHARE за підтримки компанії IBM, для рівнів з 1 по 3 на випадок виходу з ладу всієї виробничої площадки передбачено тільки відновне резервування даних ЦОД з зовнішнім зберіганням резервних копій. Для рівнів з 4 по 7, мають більш жорсткі обмеження на час PRO і RTO, передбачається також створення оперативного резерву на віддаленій майданчику.

Відповідно до пропонованої в даній роботі класифікацією, яка описує 10 найбільш поширених в даний час схем організації резервування інформаційних масивів і IT-сервісів в територіально-розподілених 1T-інфраструктурах з виділеними центрами обробки даних, для схем 1.1, 1.2, 2.1 відновлення даних у разі виходу з ладу всієї площадки ЦОД забезпечується тільки за рахунок відновного резервування (процедур резервного копіювання та відновлення масивів даних і програмних модулів). Решта схеми, описані в даній класифікації, на випадок відновлення даних ЦОД в разі катастрофи крім відновного передбачають також використання оперативного резерву. У всіх описаних схемах резервування додатково до оперативного як на основний, так і на резервній майданчиках може також використовуватися відновний резерв для відновлення даних у разі руйнування основного масиву і його оперативного резерву (наприклад, для забезпечення можливості відновлення в разі реплікації невірних даних в усі копії оперативного резерву).

Розглянемо загальну модель функціонування автоматизованої системи з використанням відновного резерву. Припустимо, що моделлю виникнення помилок в системі є схема незалежних випробувань [7].

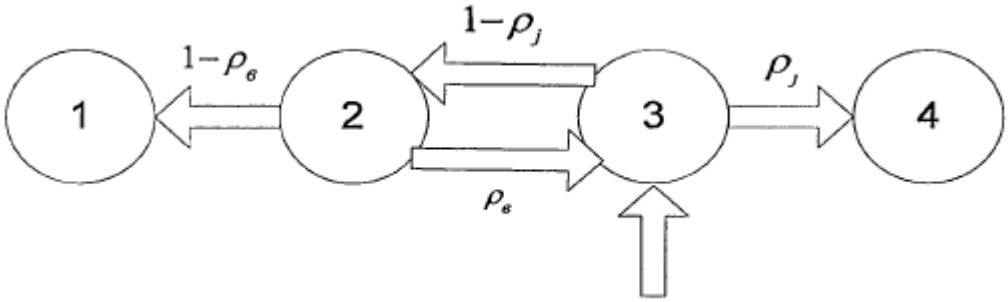

Рис. 2.7. Загальна модель функціонування автоматизованої системи

Нехай у вихідному стані (стан 3 па рис. 2.7.) В системі є k копій і (або) передісторій оперативного резерву. В разі руйнування оперативного резерву система переходить в стан 2. З цього стану система може перейти в початковий стан 3 з використанням відновного резерву. У разі успішного відновлення основного масиву і його оперативного резерву знову робиться спроба вирішення завдання.

При відтворенні оперативного резерву можливе руйнування відновного, що означає повну або часткову втрату даних в системі. В цьому випадку система переходить в поглинаючий стан 1.

Поглинаючий стан 4 відповідає успішному вирішенню завдання.

Імовірність успішного вирішення завдання з використанням відновного резерву можна визначити наступним чином:

$$\rho_j^в = \sum_{i=0}^{\infty} \rho_j P_в^i (1-\rho_j)^i = \frac{\rho_j}{1-(1-\rho_j)P_в}, \qquad (2.3)$$

де:

p_j - ймовірність успішного вирішення завдання при використанні стратегії j (j = I,II, III) оперативного резервування, розраховується за допомогою аналітичних виразів;

$P_в$ - ймовірність успішного відновлення оперативного резерву.

Загальний час доступу до автоматизованої системи з урахуванням її відновлення в разі можливого руйнування ІМ і ПМ (при функціонуванні цієї системи) можна визначити у вигляді [7]:

$$M[T_j^e] = \rho_j \sum_{i=1}^{\infty} (1-\rho_j)^i P_e^i [M[T_j](i+1) + T_e i] + (1-P_e) \sum_{i=0}^{\infty} (1-\rho_j)^{i+1} P_e^i [T_e(i+1) + M[T_j](i+1)] =$$
$$= (1-(1-\rho_j)P_e)^{-2} [M[T_j](\rho_j + (1-P_e)(1-\rho_j)) + T_e(1-\rho_j)(1-P_e(1-\rho_j))].$$

$M[T_j]$ - середній час виконання завдання з використанням оперативного резерву (вираження для розрахунку $M[T_j]$ наведені в таблиці 2.2.);

$T_в$ - час відновлення оперативного резерву.

Проведемо аналіз доцільності використання методів відновного резервування в системі обробки даних з точки зору різних критеріїв. Б якості розглянутих критеріїв приймемо наступні:

Критерій 1 - максимальна ймовірність успішного вирішення завдання;

Критерій 2 - мінімальний час вирішення завдання;

Критерій 3 - мінімум експлуатаційних витрат при функціонуванні системи.

Проведемо аналіз ефективності використання методів відновного резервування з точки зору оптимізації кожного з перерахованих вище критеріїв.

Розглянемо ефективність використання відновного резервування з точки зору максимізації ймовірності успішного вирішення завдання. Для цього порівняємо ефективність використання останньої копії або передісторії масиву в оперативному і відновному резервах [7]. Якщо все k копій і (або) передісторій використовуються в циклі оперативного резервування, то ймовірність виконання завдання p_j (*k*) при використанні j – й стратегії резервування визначається відповідно до таблиці 2.3.1.

Визначимо ймовірність успеншого поновлення масиву при використанні в циклі відновного резервування останньої копії або передісторії.

Нехай в оперативному резервування використовується *k*-1 копій і (або) передісторій, а *k*-я копія або передісторія використовується в циклі відновного резервування. В цьому випадку вираз (2.3) для ймовірності успішного вирішення завдання набуде вигляду:

$$\rho_j^n(k) = \frac{\rho_j(k-1)}{1 - P_e[1-\rho_j(k-1)]},$$

Де $P_в$- ймовірність успішного відновлення масиву і його копій і (Або) передісторій. Використання відновного резервування доцільно, якщо виконується співвідношення:

$$\rho_j^в(k) \geq \rho_j(k).$$

Звідси отримуємо:

$$P_в \geq \frac{\rho_j(k) - \rho_j(k-1)}{\rho_j(k)[1 - \rho_j(k-1)]} \qquad (2.4)$$

Тобто відновне резервування ефективно, якщо ймовірність успішного відновлення перевищує деякий рівень, який визначається характеристиками системи.

При використанні стратегії I вираз (2.4) приймає вид:

$$P_в \geq p(1 - q^{k+1})^{-1}$$

Діаграми ефективності використання методів відновного резервування наведені на рис. 2.8.

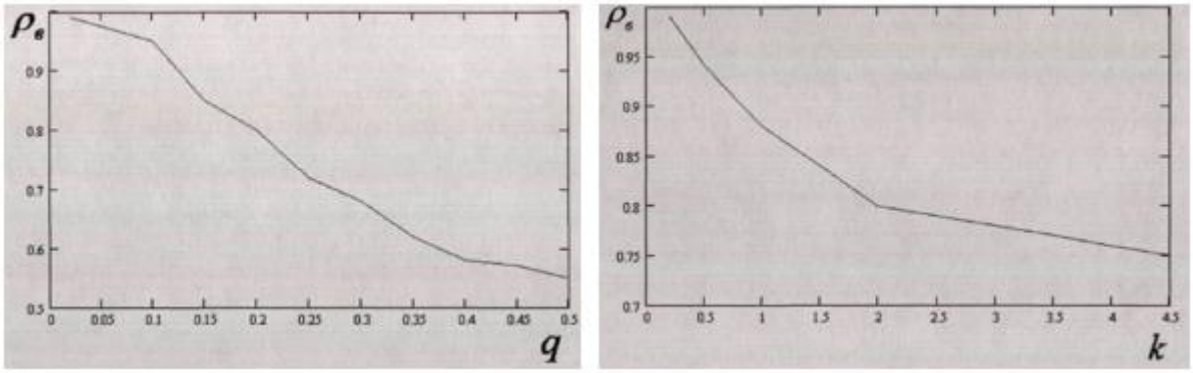

Рис.2.8. Діаграми ефективності використання методів відновного резервування

Аналіз даних діаграм показує, що відновне резервування найбільш ефективно на етапах налагодження і дослідної експлуатації системи, коли велика ймовірність руйнування зарезервованого масиву даних через помилки і збоїв в програмному забезпеченні або помилок оператора.

Одним з основних параметрів, що характеризують доступність автоматизованої системи для авторизованих користувачів, є коефіцієнт готовності.

Застосування відновного резервування дозволяє збільшити значення коефіцієнта готовності системи обробки даних за рахунок зменшення часу, необхідного на відновлення зруйнованих масивів даних. Коефіцієнт готовності системи можна представити у вигляді [7]:

$$K_z = \frac{M[T_j(n)]}{M[T_j(k)] + (1-\rho_j)t_в},$$

Де: M [T_j, (k)] - середній час доступу до системи за умови вирішення завдання і використанні стратегії резервування j (створюється k копій або передісторій основного масиву);

ρ_j - ймовірність успішного вирішення завдання при використанні стратегії j;

$t_в$ - час відновлення зруйнованих масивів.

Під відмовою будемо розуміти руйнування основного масиву і п його копій або передісторій (n≤k), використовуваних в циклі оперативного резервування.

Нехай m = k +1 - n - число інформаційних масивів, використовуваних в циклі відновного резервування. Тоді умова доцільності використання відновного резервування можна представити у вигляді:

$$K_Г(m=1) > K_Г(m=0)$$

Приклад розрахунку коефіцієнта готовності системи обробки даних в залежності від кількості масивів, використовуваних в циклі відновного резервування, наведено на рис. 2.9. (При m = 0 відновне резервування відсутня).

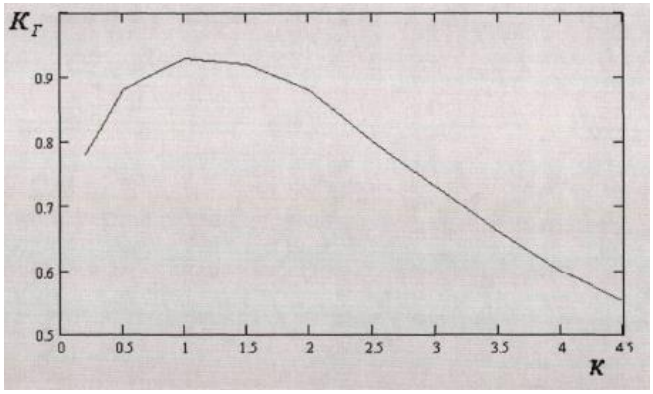

Рис.2.9. Приклад розрахунку коефіцієнта готовності системи обробки даних

Аналіз даної діаграми показує, що при великих значеннях часу відновлення зруйнованих масивів найбільш ефективним є використання однієї копії масиву в циклі відновного резервування (передбачається, що ймовірність руйнування масиву при копіюванні значно нижча ймовірності руйнування при оновленні).

У ряді випадків можливе використання схеми функціонування з проміжним відновленням. В цьому випадку при руйнуванні оперативного резерву він відновлюється в повному обсязі, тобто відновлюються x копій і (Або) передісторій $0 \leq k \leq x$, після чого робиться спроба вирішення завдання і в випадку її успішного вирішення закінчується відновлення оперативного резерву.

Часткове відновлення доцільно при оновленні масиву, коли після виконання завдання в будь-якому випадку доводиться отримувати до копій першої версії при прийнятій структурі резервування. У режимі використання часткове відновлення виправдано лише в тому випадку, коли існують обмеження на час отримання результатів рішення задачі.

Визначимо оптимальне число відновлюваних копій, забезпечують мінімум середнього часу виконання завдання при $P_в \to 1$.

Середній час вирішення завдання визначається у вигляді:

$$M[T_в] = \theta p^{-1}(1-q^k) + q^k \left\{ t_n + x\tau + \theta p^{-1}(1q^x) + (1-q^x)^{-1}\left[t_n + x\tau + \theta p^{-1}(1-q^x) \right] \right\}$$

Оптимальне значення x визначається з рівняння:

$$dM[T_в]/dx = 0$$

Після ряду перетворень вираз приводиться до вигляду:

$$(q^x + 1)\tau + q^x \ln q(t_n + x\tau) = 0$$

Цей вираз дозволяє розрахувати оптимальне значення x.

Наприклад, при τ = 10 хв, t_n= 25 хв, j = 0.01 оптимальним є x = 1, тобто доцільно відновлювати масив і одну його копію.

При оцінці за критерієм мінімізації експлуатаційних витрат використання відновного резервування є доцільним, якщо воно дозволяє зменшити експлуатаційні витрати.

Нехай для деякого інформаційного масиву створено оперативний резерв, до якого входять до копій і (або) передісторій зарезервованого масиву. Визначимо умови доцільності введення замість одного з носіїв оперативного резерву циклу відновного резервування.

Витрати системи можна записати у вигляді:

$$R = R_A + R_B + R_C,$$

де R_A - математичне очікування втрат системи від руйнування масиву, його оперативного і відновлювального резерву;

R_B - вартість часу роботи системи, витраченого на рішення задач

R_C- вартість носія інформації.

Якщо використовується тільки оперативний резерв, витрати системи визначаються у вигляді:

$$R_i^o = vT\{(1-\rho_i)Z_n + M[T_j]Z_M\} + (k+1)Z_{м.н}$$

де v - щільність потоку звернень до масиву;

Т- період часу, протягом якого досліджується поведінка системи;

p_j - ймовірність успішного оновлення масиву при використанні j–й стратегії резервування;

Z_N - вартість відновлення інформації, втраченої від руйнування масиву і його копій і (або) передісторії;

M [T_j] середнє час поновлення масиву;

Z_M- вартість використання одиниці машинного часу системи;

$Z_{Н.И.О.}$ - вартість носія інформації, що використовується при оперативному резервуванні.

При використанні відновного резервування вираз набуває вигляду:

$$R_i^в = vT\{(1-\rho_i^в)Z_n + M[T_j^в]Z_M\} + kZ_{Н.И.О.} + Z_в'$$

Тут $\rho_i^в$- ймовірність успішного вирішення завдання (поновлення масиву);

M [$T_j^в$] - середній час доступу до системи при вирішенні поточної завдання з урахуванням використання відновного резерву;

Z_B - вартість носія відновного резерву.

Якщо в циклі відновного резервування застосовується носій разового використання, то вираз для витрат $R_j^в$ набуде вигляду:

$$R_i^в = vT\{(1-\rho_i^в)Z_п + M[T_j^в]Z_M + Z_в\} + kZ_{Н.И.О.}$$

Нехай для резервування масиву використовується стратегія 1. На рис. 2.10. показано відміну оперативного резервування а) від відновного б). У разі відновного резервування копія F_k використовується не для оновлення основного масиву, а для відновлення версії F_{00} всіх копій F_1- F_{k-1}.

Умова доцільності використання відновного резервування можна записати у вигляді $R_I^0 > R_I^в$.

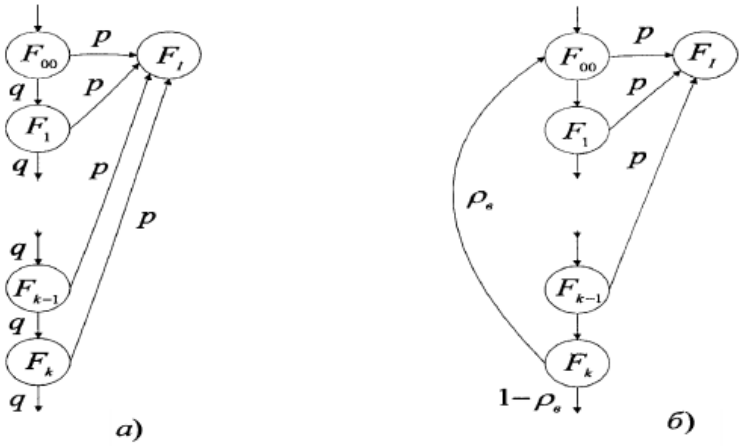

Рис. 2.10. Відмінність оперативного резервування а) від відновного б).

Якщо ймовірність відновлення зруйнованого масиву вище ймовірності успішного оновлення, то з використанням виразів для витрат системи при оперативному та відновлювальне резервування R_j^0 і $R_j^в$, отримаємо:

$$vT\{(1-\rho_1)Z_п + Z_м[M[T_I] - M[T_I^в]]\} + Z_{Н.И.О.} - Z_в > 0,$$

де:

$\rho_I = 1-q^{k+1}$;

$M[T_I] = \theta p^{-1}(1-q^{k+1})$;

При $P_в \to 1$ вираз

$$M[T_j^e] = \rho_j \sum_{i=1}^{\infty} (1-\rho_j)^i P_e^i [M[T_j](i+1) + T_e i] + (1-P_e) \sum_{i=0}^{\infty} (1-\rho_j)^{i+1} P_e^i [T_e(i+1) + M[T_j](i+1)] =$$
$$= (1-(1-\rho_j)P_e)^{-2} [M[T_j](\rho_j + (1-P_e)(1-\rho_j)) + T_e(1-\rho_j)(1-P_e(1-\rho_j))]$$

набуває вигляду:

$$M[T_i^в] = \theta p^{-1}(1-q^k) + (1-q^k)^{-1} q^k [T_в + \theta p^{-1}(1-q^k)];$$

де:

q - ймовірність руйнування масиву;

в - час оновлення;

$T_в$ - час відновлення масиву і його копій.

Використовуючи отримані раніше вирази, умова доцільності використання відновного резервування можна записати у вигляді:

$$T_b < Z_M^{-1}(1-q^k)[q(Z_П - Z_M \theta p^{-1}] + \frac{Z_{Н.И.О.} - Z_B}{vTq^k} \quad (2.5)$$

Таким чином, відновне резервування доцільно, якщо час відновлення системи оперативного резервування менше деякого значення, що визначається характеристиками системи.

Аналіз виразу (2.5) показує, що ефективність відновного резервування тим вище, чим більше втрати *Zn* які несе система від руйнування інформації, що міститься в масиві.

Це дозволяє зробити висновок про те, що даний метод найбільш ефективний при резервуванні масивів великого об'єму або містять дані, відновлення яких вимагає значних витрат часу і ресурсів або взагалі неможливо, внаслідок чого руйнування таких масивів завдає значної шкоди системі і призводить до великих втрат.

На рис. 2.11. приведена діаграма ефективності використання відновного резервування в сенсі критерію (2.5). Як видно з діаграми, область ефективного використання відновного резервування досягає найбільшої ширини в стаціонарному режимі функціонування (при q→0) або при значній імовірності руйнування програмних модулів і інформаційних масивів.

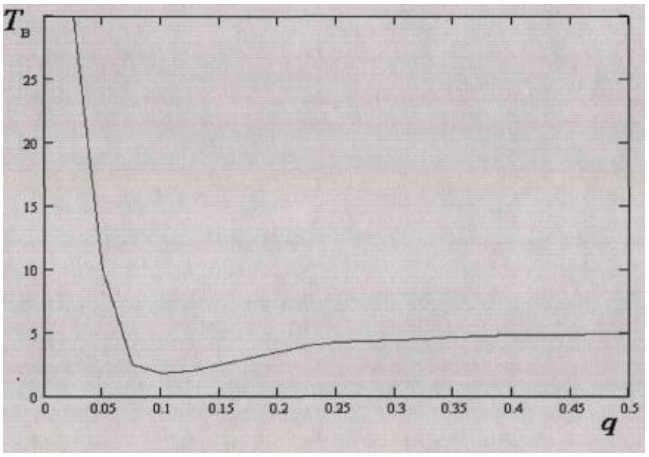

Рис. 2.11. Діаграма ефективності використання відновного резервування

В першому випадку ефективність розглянутого методу пояснюється тим, що при малих ймовірності руйнування масиву, коли витрати машинного часу системи, пов'язані з використанням резерву, і частота звернення до нього малі, досягається значний виграш від використання в циклі відновного резервування більш дешевих носіїв інформації, а при великих можливостях руйнування (т. з. в перехідному режимі) ефект досягається від значного зниження математичного очікування втрат від руйнування модулів і масивів при відновлювальному резервування.

При проміжних значеннях ймовірності руйнування масивів область ефективності відновного резервування кілька звужується, так як в даному випадку середні втрати від руйнування знижуються незначно, а додаткові витрати часу системи, яких вимагає даний метод резервування, зростають.

Якщо в якості носія інформації відновного резерву використовується носій, однотипний з носіями оперативного резерву, то вираз (2.5) набуває вигляду:

$$T_в < Z_M^{-1}(1-q^k)\left\lfloor q\left(Z_n - Z_M \theta p^{-1}\right)\right\rfloor \qquad (2.6)$$

На рис.2.12. представлені області ефективності відновного резерву в сенсі умови (2.6). З даних діаграм випливає, що метод відновного резервування кращий в випадку q→ 1/2, що в реальних умовах відповідає етапам впровадження і дослідної експлуатації системи обробки даних.

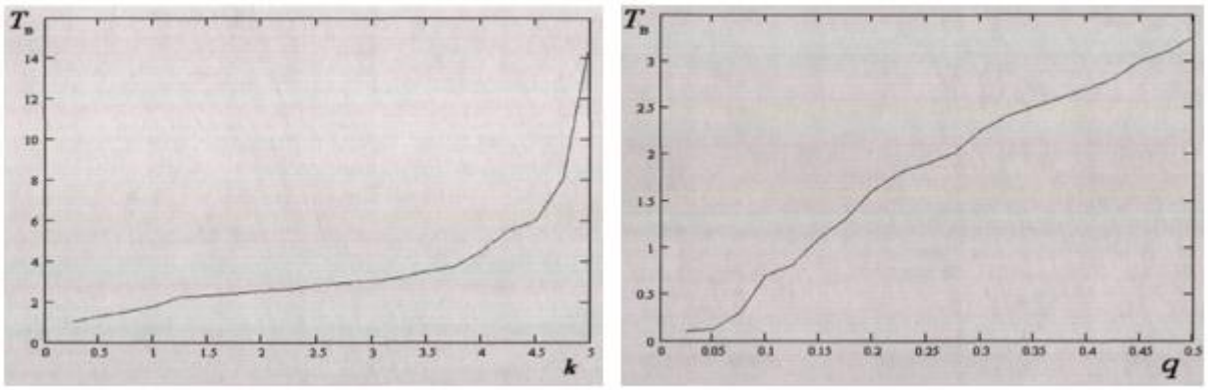

Рис.2.12. Області ефективності відновного резерву

Якщо ймовірність успішного отримання копії масиву значно вище ймовірності успішного оновлення, то вираз (2.6) запишеться у вигляді:

$$t_П < \sum_M^{-1} k^{-1}(1-q^k)\left[q(Z_n - Z_M\theta p^{-1}) + \frac{Z_{М.Н.}-Z_B}{vTq^k}\right] - (k-)\tau \qquad (2.7)$$

де:

$t_П$ - час введення даних відновного резерву (перенесення на магнітний носій);

τ - час отримання однієї копії масиву;

$T_в = t_П + (k-1)\tau$ - час відновлення.

Якщо в циклі відновного резервування використовується носій інформації, однотипний використовуваним при оперативному резервування, то умова (3.4.) з урахуванням витрат часу на копіювання набуде вигляду:

$$\tau < \sum_M^{-1} k^{-1}(1-q^k)[q(Z_П - Z_M\theta p^{-1})] \qquad (2.8)$$

Нехай для резервування масиву використовується стратегія II. На рис. 2.13. і 2.14. показано відміну використання передісторії F_{-k} в циклі оперативного резервування від відновного резервування.

Основна відмінність полягає в тому, що при руйнуванні передостанній передісторії F_{-k+1} остання передісторія (зберігається в циклі відновного резервування) F_{-k} спочатку копіюється, а потім вже відбувається її оновлення. Надалі схема функціонування аналогічна схемі оперативного резервування.

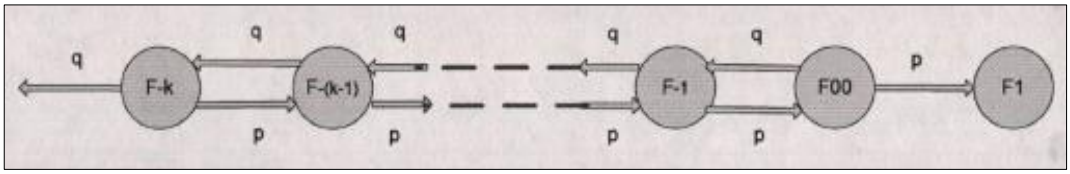

Рис. 2.13. Відмінність використання передісторії F_{-k} в циклі оперативного резервування від відновного резервування

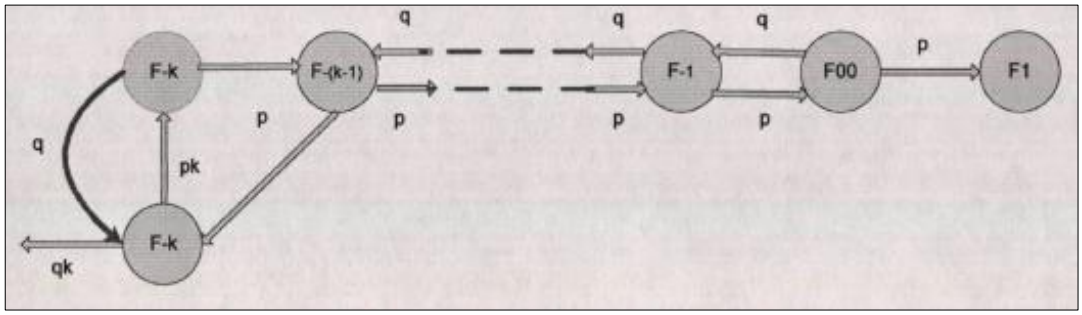

Рис. 2.14. Відмінність використання передісторії F_{-k} в циклі оперативного резервування від відновного резервування

Розглянемо умови доцільності використання останньої передісторії в циклі відновного резервування. якщо ймовірність успішного копіювання останньої передісторії або її перенесення на магнітний носій близька до одиниці ($\rho_k \to 1$), то умова доцільності використання відновного резервування має вигляд:

$$t_П < (1-\rho_{II}(k-1))^{-1}\rho^{*}_{II}\left\{Z_M^{-1}\left[(1-\rho_{II}(k))Z_П + Z_M M[T_{II}(k)] + \frac{Z_{M.H.}-Z_H}{\sqrt{T}}\right] - \frac{M[T^{*}_{II}][1-\rho_{II}(k-1)]}{\rho^{*}_{II}}\right\}$$

Де

$$M[T^{*}_{II}] = \frac{\theta}{q-p}\left\{1 - \frac{(k+2)[1-(qp^{-1})^{k+1}]}{1-(qp^{-1})^{k+2}}\right\}$$

$$\rho^{*}_{II} = \frac{(p/q)^{k+2} - (p/q)^{k+1}}{(p/q)^{k+2} - 1}$$

Аначітіческіе вираження для ρ_u і M[$T_и$] наведені в таблиці 2.2.

При використанні стратегії II в циклі відновного резерву доцільно зберігати останню передісторію. В іншому випадку при руйнуванні оперативного резерву все передісторії будуть втрачені для системи.

Умова доцільності використання відновного резервування для стратегії III має вигляд:

$$T_{Ш} < (1-\rho_{Ш}(y-1))^{-1}\rho_{Ш}(y-1)\left\{Z_M^{-1}\left[(1-\rho_{Ш}(y))Z_П + Z_M \mathrm{M}[\mathrm{T_Ш}(y)]\right] + \frac{Z_{M\,н.} - Z_в}{\nu T} - M[T_{Ш}(y-1)]\right\}$$

Вирази для $\rho_ш$ і M[$T_ш$] наведені в таблиці 2.1,

$$T_в = x\tau\left[\frac{(p/q)^{y+2} - (p/q)^{y+1}}{(p/q)^{y+1} - 1}\right] + t_п + \frac{\theta}{q-p}\left(1 - \frac{(y+2)(1-(q/p)^{y+1})}{1-(q/p)^{y+2}}\right)$$

Наведені нерівності визначають області ефективного застосування відновного резервування в порівнянні з оперативним. їх аналіз показує, що поліпшення імовірнісних характеристик системи тягне за собою погіршення тимчасових характеристик, що обумовлює необхідність економічної оцінки ефективності відновного резервування.

2.4 Використання методів відновного резервування в глобальних мережах

Територіальна розподіленість мереж ПК і особливості їх функціонування дозволяють виділити два основні варіанти відновлення оперативного резерву ІМ і ПМ, зруйнованого в одному з вузлів мережі.

1) Як відновного резерву використовується незруйнованим оперативний резерв, розташований в найближчому вузлі (в разі децентралізованого зберігання оперативного резерву в мережі).

2) Як відновного резерву використовується спеціальний резерв ІМ і ПМ - архів магнітних носіїв, розміщений в одному або декількох вузлах мережі і призначений для тривалого і надійного зберігання модулів і масивів і обробки запитів на відновлення зруйнованого оперативного резерву (ОР).

Відновлення ЗР з копій відновного резерву ІМ і ПМ здійснюється відповідно до однієї з двох основних стратегій відновного резервування [10,11]:

Стратегія В1:

З відновного резерву (ВР) послідовно відновлюють всі копії, необхідні для відновлення ОР.

Стратегія В2:

При одержанні чергової копії, необхідної для відновлення ОР, використовуються і все раніше отримані копії ІМ і ПМ.

Для відновлення ОР, що містить передісторії ІМ і ПМ, можна, використовуючи ВР, отримати і переслати в вузол зі зруйнованим ЗР дублі всіх, декількох або тільки останньої передісторії. Надалі будемо вважати, що зруйнований ЗР містить тільки копії ІМ і ПМ.

Розглянемо процес відновлення ОР, що складається з п копій. нехай в якості ВР використовується незруйнованим ОР, створений відповідно до стратегією І оперативного резервування з т копій ІМ або ПМ.

Визначимо основні характеристики стратегії В-1.

Нехай кожна чергова копія, яка використовується для відновлення зруйнованого ОР, знімається з останньої т-й копії ВР, при цьому вона з ймовірністю $\gamma = 1 - \beta$ може бути зруйнована. її відновлення проводиться шляхом копіювання з (m-1) - й копії ВР, яка, в свою чергу, може бути зруйнована. Даний процес може бути описаний з використанням моделі випадкового блукання частинки по цілочисельним точкам дійсній прямій з двома поглинаючими екранами в точках x = 0 і x = m + 1. Точка x = 0 відповідає руйнуванню копій B_1 ,….., B_m відновного резерву, а точка x = m + 1 - успішному отриманню з відновного резерву черговий копії, призначеної для відновлення оперативного резерву.

Відповідно до моделі випадкового блукання частка з початкової точки x = z може потрапити в точку x = 0 (відповідну руйнування всіх копій відновного резерву) з ймовірністю:

$$q_z = \left(b^{m+1} - b^z\right)\left(b^{m+1} - 1\right)^{-1}, \qquad (2.9)$$

де b = γ/β;

$\gamma = 1 - \beta$ - ймовірність руйнування масиву відновного резерву в процесі отримання копії оперативного резерву.

Ймовірність влучення з точки x = z в точку x = m + 1 дорівнює:

$$p_z = 1 - q_z = \left(1 - b^z\right)\left(1 - b^{m+1}\right)^{-1} \tag{2.10}$$

У розглянутому нами випадку z=m тому ймовірність отримання однієї копії для відновлення оперативного резерву буде:

$$P_1^I = \left(1 - b^m\right)\left(1 - b^{m+1}\right)^{-1} \tag{2.11}$$

Імовірнісний процес функціонування системи при отриманні всіх n копій зруйнованого оперативного резерву можна описати рівнянням:

$$\left(P_1^I\right)^n + \left(P_1^I\right)^{n-1} Q_1^I + \ldots + P_1^I Q_1^I + Q_1^I = 1, \tag{2.12}$$

де

$$Q_1^I = 1 - P_1^I$$

Відповідно до моделі випадкового блукання середній час отримання однієї копії E_1^Iв термінах випадкового блукання - середній час переходу частки з x = m в x = m + 1) можна представити у вигляді наступного виразу:

$$E_1^I = C_1\left[(m+1)\left(1 + b^{m+1}\right)\left(1 - b^m\right) - m\left(1 - b^{m+1}\right)\left(1 + b^m\right)\right]\tau \tag{2.13}$$

де:

τ - середній час копіювання;

$$C_1 = (\beta - \gamma)\left(1 - b^{m+1}\right)^{-2}$$

Середній час до руйнування відновного резерву при отриманні однієї копії можна представити у вигляді:

$$\overline{E}_1^I = C_1 b^m\left[(m+1)\left(1 + b^{m+1}\right)(1 - b) - \left(1 - b^{m+1}\right)(1 + b)\right]\tau \tag{2.14}$$

Використовуючи вирази (2.12) - (2.14) можна отримати аналітичні вираження для основних характеристик стратегії В-1:

ρ_{B-1}^I- ймовірності успішного отримання n копій для відновлення зруйнованого оперативного резерву;

E_{B-1}^I- середній час успішного отримання n копій для відновлення зруйнованого оперативного резерву;

σ_{B-1}^{I} - ймовірність руйнування відновного резерву при отриманні п копій для відновлення зруйнованого оперативного резерву;

$\bar{E}_{B-1}^{I}$- середній час до руйнування відновного резерву при отриманні п копій для відновлення зруйнованого оперативного резерву;

T_{B-1}^{I} - середній час функціонування системи при отриманні п копій.

Основні характеристики стратегії відновлення В-1 (відповідно до якої з відновного резерву (ВР) послідовно відновлюють всі копії, необхідні для відновлення ОР) наведені в табл. 2.4.

Отримаємо вирази для розрахунку характеристик стратегії В-2 (при отриманні чергової копії, необхідної для відновлення ОР, використовуються і все раніше отримані копії ІМ і ПМ). Процес функціонування системи також опишемо за допомогою моделі випадкового блукання точки на відрізку. Початковою точкою є точка z= m.

Попадання в точку x=m+n відповідає успішному отриманню всіх п копій, необхідних для відновлення зруйнованого оперативного резерву.

Замінивши z і m + 1 на m і m + n відповідно, з виразу (2.10) можна отримати вираз для розрахунку ймовірності отримання п копій ρ_{B-2}^{I}.

Значення E_{B-2}^{I}- середнього часу до успішного отримання n копій - виходить з (2.13) заміною m + 1 і C_1, на m + n і $C_2 = (\beta - \gamma)^{-1}$, $(1\text{-}b^{m+n})^{-2}$

Значення $\bar{E}_{B-2}^{I}$ - середнього часу до руйнування відновного резерву виходить з (2.14) шляхом заміни m+ 1, b і C_1 на m + n, b^n і C_2 відповідно і поставивши коефіцієнт п у від'ємника в квадратних дужках.

Отримані аналітичні вирази для розрахунку характеристик стратегії В-2 в розглянутому випадку наведені в табл. 2.4.

Налітичні вирази для розрахунку характеристик стратегій відновного резервування В-1 і В-2 для випадку, коли в якості ВР використовується незруйнованим ОР,

Таблиця 2.4.

Основні характеристики стратегії відновлення

B-1	B-2
$\rho^{I}_{B-1} = \left\lfloor \frac{1-b^{m}}{1-b^{m+1}} \right\rfloor$, $\sigma^{I}_{B-1} = 1-\rho^{I}_{B-1}$, $E^{I}_{B-1} = n\mathrm{E}^{I}_{1}$, $\overline{E}^{I}_{B-1} = \overline{E}^{I}_{1} + E^{I}_{1}P^{I}_{1}\left(\sigma^{I}_{1}Q^{I}_{1}\right)^{-1} \times \times\left[1-\left(P^{I}_{1}\right)^{n-1}\left(1+(n-1)Q^{I}_{1}\right)\right]$, $T^{I}_{B-1} = \left(E^{I}_{1}P^{I}_{1} + \overline{E}^{I}_{1}Q^{I}_{1}\right)\sigma^{I}_{B-1}\left(Q^{I}_{1}\right)^{-1}$	$\rho^{I}_{B-2} = \left(1-b^{m}\right)\left(1-b^{m+n}\right)^{-1}$, $\sigma^{I}_{B-2} = 1-\rho^{I}_{B-2}$, $E^{I}_{B-2} = C_2[(m+n)\left(1+b^{m+n}\right)\left(1-b^{m}\right)- -m\left(1-b^{m+n}\right)\left(1+b^{m}\right)]\tau$, $\overline{E}^{I}_{B-2} = C_2 b^{m}[(\mathrm{m}+\mathrm{n})\left(1+b^{m}\right)\left(1-b^{n}\right)- -n\left(1-b^{m+n}\right)\left(1+b^{n}\right)]\tau$, $T^{I}_{B-2} = \rho^{I}_{B-2}E^{I}_{B-2} + \sigma^{I}_{B-2}\overline{E}^{I}_{B-2}$

Таблиця 2.5.

Отримані вирази

B-1	B-2
$\rho^{II}_{B-1} = \left[\beta\left(1-\gamma P^{II}_{B-1}\right)^{-1}\right]^{n}$, $\sigma^{II}_{B-1} = 1-\rho^{II}_{B-1}$, $E^{II}_{B-1} == nE^{II}_{1}$,	$\rho^{II}_{B-2} = P_c\left(1-Q_c P^{II}_{b}\right)^{-1}$, $\sigma^{II}_{B-2} = 1-\rho^{II}_{B-2}$, $E^{II}_{B-2} = E_c + \left(\overline{E}_b + E^{II}_{b}\right)\times \times Q_c P^{II}_{b}\left(1-Q_c P^{II}_{b}\right)^{-1}$,
$\overline{E}^{II}_{B-1} = \overline{E}^{II}_{1} + E^{II}_{1}P^{II}_{1}\left(\sigma^{II}_{1}Q^{II}_{1}\right)^{-1} \times \times\left[1-\left(P^{II}_{1}\right)^{n-1}\left(1+(n-1)Q^{II}_{1}\right)\right]$, $T^{II}_{B-1} = \left(E^{II}_{1}P^{II}_{1} + \overline{E}^{II}_{1}Q^{II}_{1}\right)\sigma^{II}_{1}\left(Q^{II}_{1}\right)^{-1}$	$\overline{E}^{II}_{B-2} = \overline{E_c} + \overline{E}^{II}_{b} + \left(\overline{E}_c + E^{II}_{B}\right)\times \times Q_c P^{II}_{b}\left(1-Q_c P^{II}_{b}\right)^{-1}$, $T^{II}_{B-2} = \rho^{II}_{B-2}E^{II}_{B-2} + \sigma^{II}_{B-2}\overline{E}^{II}_{B-2}$

створений відповідно до стратегією II оперативного резервування з ш передісторій ІМ або ПМ визначаються аналогічним чином на основі моделі випадкового блукання точки на відрізку. Отримані вирази наведені в таблиці 2.5.

Таблиця 2.6.

Отримані вирази

В-1	В-2
$\rho_{B-1}^{III} = P_1^n,$ $\sigma_{B-1}^{III} = 1 - \rho_{B-1}^{III},$ $T_{B-1}^{III} = \left[E_1 P_1 + E_1 \bar{Q}_1 \right] \times \sigma_{B-1}^{III} \times Q_1^{-1},$ $E_{B-1}^{III} = nE_1,$ $\bar{E}_{B-1}^{III} = \bar{E}_1 + E_1 P_1 \left(\sigma_{B-1}^{III} Q_1 \right)^{-1} \times$ $\times \left[1 - P_1^{n-1} \left(1 + (n-1) Q_1 \right) \right]$	$\rho_{B-2}^{III} = P_C \left(1 - Q_C P_b \right)^{-1},$ $\sigma_{B-2}^{III} = 1 - \rho_{B-2}^{III},$ $T_{B-2}^{III} = E_{B-2}^{III} \rho_{B-2}^{III} + \bar{E}_{B-2}^{III} \sigma_{B-2}^{III},$ $E_{B-2}^{III} = E_C + \left(\bar{E}_C + E_b \right) \times$ $\times Q_C P_b \left(1 - Q_C P_b \right)^{-1},$ $\bar{E}_{B-2}^{III} = \bar{E}_C + \bar{E}_b + \left(\bar{E}_C + E_b \right) \times$ $\times Q_C P_b \left(1 - Q_C P_b \right)^{-1}$
$P_1 = P_C \left(1 - Q_C P_b \right)^{-1},$ $Q_C = 1 - P_1,$ $P_C = \left(1 - b^x \right) \left(1 - b^{x+1} \right)^{-1},$ $Q_C = 1 - P_C,$ $E_1 = E_C + \left(\bar{E}_C + E_b \right) \times$ $\times Q_C P_b \left(1 - Q_C P_b \right)^{-1},$ $\bar{E}_1 = \bar{E}_C + \bar{E}_b + \left(\bar{E}_C + E_b \right) \times$ $\times Q_C P_b \left(1 - Q_C P_b \right)^{-1},$ $E_C = C_1 \left[(x+1) \left(1 + b^{x+1} \right) \left(1 - b^x \right) - \right]$ $[- x \left(1 - b^{x+1} \right) \left(1 + b^x \right)] \tau,$ $\bar{E}_C = C_1 b^x [(x+1) \left(1 + b^{x+1} \right) (1 - b) -$ $- \left(1 - b^{x+1} \right) (1 + b)] \tau$	$P_C = \left(1 - b^x \right) \left(1 - b^{x+n} \right)^{-1},$ $Q_C = 1 - P_C,$ $E_C = C_2 [(x+n) \left(1 + b^{x+n} \right) \left(1 - b^x \right) -$ $- x \left(1 - b^{x+n} \right) \left(1 + b^x \right)] \tau$ $\bar{E}_C = C_1 b^x [(x+n) \left(1 + b^{x+n} \right) \left(1 - b^n \right) -$ $- n \left(1 - b^{x+n} \right) \left(1 + b^n \right)] \tau,$ $C_2 = (\beta - \gamma)^{-1} \left(1 - b^{x+n} \right)^{-2}$
$P_b = D_1 \left[1 - U_1 D_2 \right]^{-1},$ $D_1 = (1 - b) \left(1 - b^{x+1} \right)^{-1},$ $U_1 = 1 - D_1,$ $E_b = E_b^I + Q_C^I P_b^I \left(1 - Q_C^I P^I \right)^{-1} \times$ $\times \left(\bar{E}_C^I + E_b^I \right),$ $E_C^I = C_1 [(x+1) \left(1 + b^{x+1} \right) (1 - b) -$ $- \left(1 - b^{x+1} \right) (1 + b)] \tau,$ $E_b^I = W [y \left(1 + a^y \right) \left(1 - a^{y-1} \right) -$ $- (y-1) \left(1 - a^y \right) \left(1 + a^{y-1} \right)] \theta,$ $C_1 = (\beta - \gamma)^{-1} \left(1 - b^{x+n} \right)^{-2},$ $W = (\rho - q)^{-1} \left(1 - a^y \right)^{-2}$	$D_2 = P_b^I = \left(1 - a^{y-1} \right) \left(1 - a^y \right)^{-1},$ $Q_C^I = b \left(1 - b^x \right) \left(1 - b^{x+1} \right)^{-1},$ $\bar{E}_b = \bar{E}_C^I + \bar{E}_b^I + \left(\bar{E}_C^I + E_b^I \right) \times$ $\times Q_C^I P_b^I \left(1 - Q_C^I P_b^I \right)^{-1},$ $E_C^I = C_1 b [(x+1) \left(1 + b^{x+1} \right) \left(1 - b^x \right) -$ $- x \left(1 - b^{x+1} \right) \left(1 + b^x \right)] \tau,$ $\bar{E}_b^I = W a^{y-1} [y \left(1 + a^y \right) (1 - a) -$ $- \left(1 - a^y \right) (1 + a)] \theta$

Аналогічно виходять вирази для розрахунку характеристик стратегій відновного резервування В-1 і В-2 при використанні як ВР незруйнованим ОР, створеного відповідно до стратегії III оперативного резервування з x копій і y передісторій (x+y =m). Отримані вирази наведені в таб. 2.6.

Якщо в якості відновного резерву (ВР) використовується архів магнітних носіїв (АМН), то для розрахунку характеристик стратегій В-1 і В-2 без будь-яких змін можна застосовувати формули з таблиці 2.4., так як АМН являє собою деяку кількість копій ІМ і ПМ.

Розглянемо особливості розрахунку імовірнісних, тимчасових і вартісних характеристик для основних схем відновного резервування інформаційних масивів і 1Т-сервісів в територіально розподілених ГГ-ііфраструктурах з виділеними центрами обробки даних.

При використанні схем 1.1 і 1.2 при розрахунку часу відновлення слід також враховувати час відновлення процесу обробки даних

- відновлення пошкодженої майданчика або розгортання обробки даних з нуля на новому майданчику. Повний час відновлення процесу автоматизованої обробки даних буде визначатися за формулою:

$$M[T_{\text{обр}}] = M[T_{\text{шифр}}] + M[T_j],$$

де М [$T_{\text{інфр}}$] - час, необхідний на відновлення після аварії підтримуючої інфраструктури центру обробки даних або розгортання обробки даних на новому майданчику;

М [Tj] - час, необхідний для відновлення основного масиву і його оперативного резерву з відновного резерву.

При використанні схеми 1.1 слід враховувати ймовірність руйнування відновного резерву, що зберігається в межах основного ЦОД, в випадку виникнення надзвичайної ситуації, що виводить з ладу основний масив і його оперативний резерв. Для схеми 2.1. необхідно враховувати вартість організації регулярного вивезення резервних копій в окреме захищене приміщення, періодичність вивезення резервних копій. При розрахунку часу відновлення слід враховувати час доставки резервних копій з місця зберігання на майданчик резервного ЦОД. Також береться до уваги можливість втрати частини даних, введених в проміжку між вивезенням резервних копій в місце зовнішнього зберігання.

Для схеми 2.1. слід брати до уваги вартість використання каналів зв'язку для організації резервного копіювання на майданчик резервного ЦОД.

Нехай d_{jk} - вартість передачі по каналах зв'язку одного біта інформації з вузла j в вузол k. Тоді вартість передачі по каналах зв'язку даних резервного копіювання об'ємом X буде D_{jk} (X) = d_{jk}*x при використанні схеми 2.1.можлива втрата даних, введених після останнього резервного копіювання. Проміжок часу, за який можлива втрата даних, визначається періодичністю резервного копіювання по мережі. При атом ймовірність успішного відновлення даних в межах допустимого проміжку часу перед аварією залежить також від імовірності успішної передачі даних останнього резервного копіювання по каналах зв'язку (тобто працездатності каналу зв'язку на протязі часу, відповідному вікна резервного копіювання).

3 МЕТОДИ ОПТИМІЗАЦІЇ РІВНЯ ДОСТУПНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ В РОЗПОДІЛЕНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

3.1 Розподіл засобів зберігання і обробки даних як метод захисту інформаційних ресурсів і елементів інфраструктури від аварій

В даний час інформаційні технології надають все більш значний вплив на діяльність сучасних підприємств різного рівня. Мережі передачі даних, безліч додатків і сервісів складають обов'язкову частину інформаційних ресурсів сучасного підприємства. Порушення або збої в їхній роботі негативно позначаються на безперервності бізнес-процесів підприємства, що є неприпустимим.

Великі корпорації почали цілеспрямовано впроваджувати технології забезпечення безперервності бізнесу в непередбачених ситуаціях (BCP - business continuity planning). Використання каналів глобальних мереж зв'язку дозволяє територіально рознести вузли з резервом ІМ і ІМ, що істотно підвищує ймовірність збереження доступності даних при різних катастрофічних ситуаціях (пожежі, землетруси, повені і т.п.), в разі виникнення яких можуть бути знищені (або виведені з ладу на тривалий термін) все локально розташовані копії ІМ і ПМ (як основні, так і резервні) і/або елементи підтримуючої інфраструктури. При використанні каналів глобальних мереж зв'язку і децентралізованому зберіганні резерву можливо швидке відновлення роботи при виході з ладу одного з вузлів, що містить робочі інформаційні масиви і програмні модулі, і/або які обслуговують його каналів зв'язку.

Залежність фінансових втрат, які несе організація через недоступності IT-сервісів, від часу їх недоступності приведена на рис. 3.1. Тут же наведена залежність вартості створення системи високої доступності від величини допустимого часу простою. Величина фінансових втрат, як правило, зростає

нелінійно, нелінійна залежність спостерігається і у величини витрат на заходи щодо забезпечення безперервності IT-сервісів від гарантованого часу відновлення.

Оптимальне рішення зазвичай лежить в області, яка на рисунку позначена як вікно співвідношень «ціна/час відновлення».

Основними технологіями, що забезпечують захист даних в надзвичайних ситуаціях, є:

- про резервне копіювання та архівування даних на віддаленій майданчику (Crossite backup) з розміщенням їх на стрічкових накопичувачах.

Для значень RTO (цільове час відновлення) порядку декілька годин або навіть декількох хвилин, використовуються різні варіанти кластерних комплексів, у яких вузли тим чи іншим способом розносяться на віддалені площадки. Перемикання додатки з одного вузла на інший відбувається автоматично або вручну. Деякі простої, пов'язані з недоступністю додатків, мають місце і в кластерних конфігураціях, але вони незрівнянно нижча, ніж в разі одиночних систем. для кластерів типовий коефіцієнт готовності Кг = 99,98 (близько 1 години на рік).

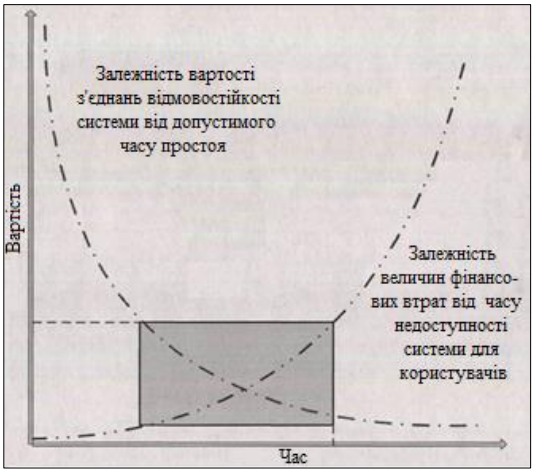

Рис.3.1. Залежність фінансових втрат, які несе організація через недоступності IT-сервісів, від часу їх недоступності

Надмірність обчислювальних ресурсів, за рахунок якої досягається висока доступність, має на увазі ускладнення обчислювального комплексу і вимагає додаткових витрат на управління, так як відповідні технологічні рішення повинні

супроводжуватися розробкою і впровадженням організаційних заходів та процедур, що забезпечують швидке і передбачуване відновлення IT-сервісів на резервному майданчику.

В даний час прийнято виділяти 7 рівнів (0 - 6) побудови систем резервування та управління даними. Семирівнева класифікація систем резервування даних була розроблена ще в 1992 р користувальницької групою SHARE за підтримки компанії IBM. В

Відповідно до цієї класифікації виділяють наступні сім основних рівнів стратегій відновлення в разі аварії або катастрофи, зачіпає центр обробки даних:

1) Рівень «О» - відсутність стратегії відновлення. наприклад, відсутність резервного копіювання, або резервне копіювання даних з зберіганням копій в тому ж приміщенні / будинку, де проводиться обробка даних. Наслідки можуть бути такі, що в разі катастрофи (пожежа, повінь, прорив труб і т.д.) відновлення даних буде неможливо і інформація буде безповоротно втрачено. час відновлення непередбачувано.

2) Рівень «1» - регулярне резервне копіювання даних з зберіганням копій в окремому приміщенні/будинку. Метод носить назву «Pickup Truck Access Method (ротами)». Дані на видобутих носіях регулярно вивозяться на зберігання в окреме захищене приміщення/будинок.

Час відновлення після повного виходу з ладу центру обробки даних - від тижня до місяця. Можлива втрата частини даних, введених після останнього резервного копіювання. Час відновлення в основному залежить від часу відновлення засобів обробки і підтримуючої інфраструктури (відновлення пошкодженої майданчики центру обробки даних або створення нового центру обробки даних).

3) Рівень «2» - комбінація PTAM + резервний центр. метод носить назва «PTAM + hostsite». Дані на видобутих носіях регулярно вивозяться на зберігання в окреме захищене приміщення. додатково, в законсервованому стані існує резервний центр. Після аварії резервні копії витягуються з сховища, проводиться запуск резервного центру і відновлення даних на резервному майданчику. Час

відновлення - кілька днів. Можлива втрата частини даних, введених після останнього резервного копіювання.

4) Рівень «3» - комбінація ротами + резервний центр + використання засобів зв'язку для віддаленого копіювання найбільш критичних даних. Метод називається «Electronic Vaulting». Метод удосконалить «ротами + hostsite» тим, що резервний центр не законсервований повністю, а здійснює через мережу регулярне копіювання найбільш часто оновлюваних і найкритичніших для бізнесу даних. Час відновлення - кілька днів. Можлива втрата даних, введених після останнього резервного копіювання. Проміжок часу, за який можлива втрата даних, визначається періодичністю резервного копіювання по мережі.

5) Рівень «4» - резервний ЦОД. Метод називається «Electronic vaulting to hotsite»; відрізняється від «Electronic Vaulting» тим, що дані по мережі регулярно копіюються на повністю розгорнутий резервний центр в асинхронному режимі (з невеликим запізненням). Час відновлення - кілька годин (визначається часом перемикання додатків на резервний ЦОД). Можлива втрата частини даних, введених перед аварією. Проміжок часу, за який може спричинити втрату даних, визначається часом затримки при асинхронної передачі даних.

6) Рівень «5» - дзеркальний ЦОД. Метод називається «Two-site, two-phase commit ». Даний метод відрізняється від «Electronic vaulting to hotsite» тим, що дані по мережі регулярно копіюються на повністю розгорнутий резервний центр в синхронному режимі, тобто операція запису в основному ЦОД закінчується одночасно із записом даних в резервному ЦОД. Час відновлення від декількох хвилин до декількох годин (визначається процедурою перемикання на резервний ЦОД).

7) Рівень «6» - розподілене ЦОД. Метод називається «Zero data loss ». Відрізняється від методу «Two-site, two-phase commit» тим, що перемикання користувачів проводиться автоматично так, що жодне натискання клавіші користувачем не втрачається. Перераховані вище рівні побудови систем резервування та управління даними наведено на рис. 3.2. На даному рисунку

показана залежність вартості створення систем резервування та управління даними різного рівня в залежності від цільового часу відновлення.

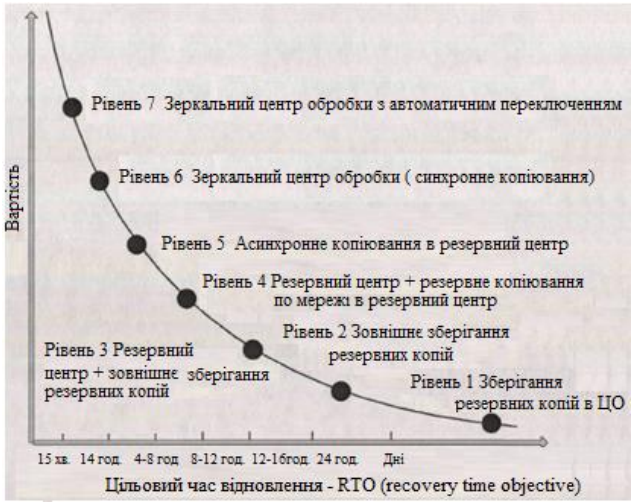

Рис. 3.2. Рівні побудови систем резервування та управління даними

Зазначені рівні побудови систем резервування та управління даними можна умовно розділити на 3 сегмента [12]:

1. «Резервне копіювання/відновлення». У перший сегмент входять рівні з 1 по 3 включно. Даний сегмент характеризується використанням коштів резервного копіювання/відновлення з зберіганням даних на резервному майданчику (рівні 2 і 3). У разі виходу з ладу основного майданчика час відновлення може варіюватися від декількох тижнів до декількох днів або навіть годин, що визначається використовуваним регламентом резервного копіювання.

2. «Швидке відновлення обробки даних». У другій сегмент входять рівні з 4 по 6 включно. Даний сегмент характеризується використанням територіально-розподілених кластерів і реплікацій даних на резервний майданчик. У разі виходу з ладу основний майданчики час відновлення може варіюватися від декількох годин до декількох хвилин, що визначається використовуваними технологіями реплікації і застосовуваними кластерними технологіями.

3. «Завжди готовий». Третій сегмент складається з одного 7-го рівня готовності і передбачає використання територіально розподіленого кластера з використанням синхронної реплікації даних на резервний майданчик і автоматичне

перемикання призначених для користувача додатків на резервний майданчик в разі виходу з ладу основний.

Розподіл рівнів побудови систем резервування та управління даними на сегменти зображено на рис. 3.3.

Рис. 3.3. Розподіл рівнів побудови систем резервування та управління даними на сегменти

Можна виділити наступні стратегії, пов'язані із забезпеченням безперервності 1Т-сервісів в разі аварій і катастроф:

1. Відсутність спеціальних заходів на випадок виходу з ладу виробничої площадки.

Надія покладається на те, що в разі виникнення надзвичайної ситуації буде досить часу і ресурсів для виконання необхідних кроків по відновленню працездатності пошкодженого обладнання.

Такий підхід виправданий, якщо діяльність компанії дозволяє практично безболісно для бізнесу переривати функціонування ІТ-сервісів на час, необхідний для виконання відновлювальних робіт.

2. Створення максимально захищеного центру обробки даних - "Побудова фортеці"

Даний варіант знижує ймовірність реалізації зовнішніх загроз до прийнятного рівня. Прикладом рішень такого роду можуть служити різні сейфи і

саркофаги, надійно захищають обладнання від зовнішніх впливів, фізичний захист по периметру будівлі, відео-моніторинг приміщень і т.д.

3. Розгортання IT-сервісів на резервному майданчику (continuous processing)

Стратегія цього підходу полягає в створенні резервний майданчик, розгортанні на ній резервних систем і комунікаційних каналів, повністю ідентичних продуктивної середовищі. При цьому перемикання на альтернативний майданчик надаються інформаційною системою сервісів відбувається тільки в разі надзвичайної ситуації. ця стратегія використовується в різних варіантах - організація альтернативної «Холодної», «теплою» або «гарячої» резервний майданчик. "Холодна" альтернативний майданчик - місце для розміщення нового обладнання, з проинсталлировать оточенням (опорної інфраструктурою), які дозволяють запустити сервіси на альтернативному майданчику, не допускаючи значної перерви в функціонуванні сервісів.

"Тепла" альтернативний майданчик - серверне приміщення з опорної інфраструктурою і комплектами основного серверного обладнання з проінсталювати критичними додатками. На майданчику є все необхідне обладнання, і в разі надзвичайної ситуації для відновлення обробки можуть знадобитися лише роботи по відновленню даних.

"Гаряча" альтернативний майданчик забезпечує ефективне дублювання сервісів з продуктивністю, достатньою для обслуговування бізнесу. На ній є все необхідне для цього обладнання, здійснюється реплікація даних по мережі на резервний майданчик і в разі надзвичайної ситуації можуть знадобитися лише роботи з переключення резервної майданчики в режим основної. Можливість організації швидко перевести обробку даних на альтернативну робочу площадку значно підвищує її життєздатність. Висока вартість такого рішення обумовлена вартістю високопродуктивних резервних систем, в штатної ситуації знаходяться в режимі очікування і, отже, в виробничої діяльності не беруть участь.

Таблиця 3.1.

Рішення для захисту даних і для відновлення сервісів

Рішення	Капітальні затрати	Експлуата-ційні затрати	Надій-ність	Скла-дність	Продук-тив-ність	Тех. Пригод-ність	Загальна оцінка
RRO~ 0 годин-захист від фізичного руйнування							
Синхронна реплкація даних з використанням томів	4,8	3,8	3,0	4,1	3,2	2,9	21,8
Синхронна реплікація даних під управління хост-системи	2,6	3,1	2.7	2,9	2,1	2,9	16,2
Синхронна реплікація даних на базі дискового масиву	2,2	3,4	4,0	3,6	3,9	4,6	21,7
RRO~ 0 годин-захист від логічного руйнування							
«Розчеплення зеркала» з використанням технології масивів	2,6	3,4	5,0	2,9	4,9	4,0	22,7
«Розчеплення зеркала» під управлінням хост-комп'ютера	2,9	4,2	3,9	3,4	3,6	3,6	21,6
Миттєві копії з використанням технологій копіювання при записі	3,6	4,0	3,1	3,0	3,6	3,6	21,1
PRO< 24 години							
Перехресне резервне копіювання з використанням мережі зберігання даних	3,0	3,5	3,7	4,3	3,5	4,5	22,5

4. Розподілена обробка (distributed processing) Стратегія розподіленої обробки характеризується розміщенням IT- сервісів на кількох альтернативних майданчиках. Завдяки цьому ймовірність виходу з ладу одночасно всіх систем

навіть у випадку катастрофи, що виводить з ладу цілу виробничу площадку, досить мала. Більш того, окремі сервіси можна задублювати на двох майданчиках, забезпечуючи додаткову гарантію життєздатності інформаційної системи.

Таблиця 3.2.

Рішення для захисту даних і для відновлення сервісів

Рішення	**Капітальні затрати**	**Експлуатаційні затрати**	**Надійність**	**Складність**	**Продуктивність**	**Тех. Пригодність**	**Загальна оцінка**
RTO< 4 години							
Автоматичне Аварійне перемикання на «гарячий» резерв в кластерній конфігурації з виділеними ресурсами	1,7	3,5	4,0	3,0	4,8	5,0	22,0
RTO< 24 години							
Автоматичне відновлення на серверах із заданою зарання конфігураціюєю	2,0	3,9	4,0	2,9	4,4	3,8	20,7
Ручне відновлення додатків з використанням альтернативних завантажуючих пристроїв	4,4	2,6	2,4	2,3	2,4	2,4	16,8
Ручне відновлення додатків з автоматичним розгортанням серверів	2,7	3,0	2,6	2,3	1,9	3,2	16,8

Технології зеркалирования і реплікації, що використовуються для захисту від фізичного руйнування даних, не захищають від ризиків логічного спотворення даних, які, "як є", копіюються на віддалені вузли, тобто в випадку помилки оператора або логічного збою в програмному забезпеченні помилкові дані будуть реплікуються в усі віддалені вузли. Тому технології захисту від фізичного руйнування даних зазвичай комбінуються з технологіями забезпечення

достовірності даних. В якості засобів використовуються технології резервного копіювання, що дозволяють отримувати достовірну інформацію.

При побудові систем резервування та управління даними крім технологій захисту даних також необхідно використовувати технології, що дозволяють за відведений цільовий час (RTO) відновити процес надання IT-сервісів.

Нижче в табл. 3.1., 3.2. наведені різні рішення для захисту даних і для відновлення сервісів. За кожним критерієм технічним рішенням було присвоєно експертна оцінка від 1 (найгірше) до 5 (Краще).

3.2 Організація розподілених центрів обробки даних

Як було показано вище, створення резервного обчислювального центру (РОЦ) є одним з рішень, спрямованих на забезпечення доступності даних і інформаційних сервісів. РОЦ гарантує безперервність роботи IT-інфраструктури в разі виходу з ладу основного обчислювального центру, коли час його відновлення перевищує допустимий час недоступності інформаційної системи.

Всі резервні центри організовані схожим чином – вибирається майданчик, розташована на безпечній відстані від основного центру, і на ній встановлюється обладнання, необхідне для роботи основних додатків і IT-сервісів. Основний і резервний центри з'єднуються каналом зв'язку для передачі даних додатків. Коли відбувається аварія в основному центрі, в резервному актуальні дані додатків переводяться в стан, придатний для здійснення обробки (відновлення з резервних копій або переклад в робочий режим наявних реплік) і здійснюється запуск додатків на ресурсах резервного центру. Після запуску додатків в резервному центрі користувальницькі додатки переключаються на ресурси резервного центру, і їх діяльність поновлюється.

Типова схема організації резервування з використанням резервного центру представлена на рис. 3.4.

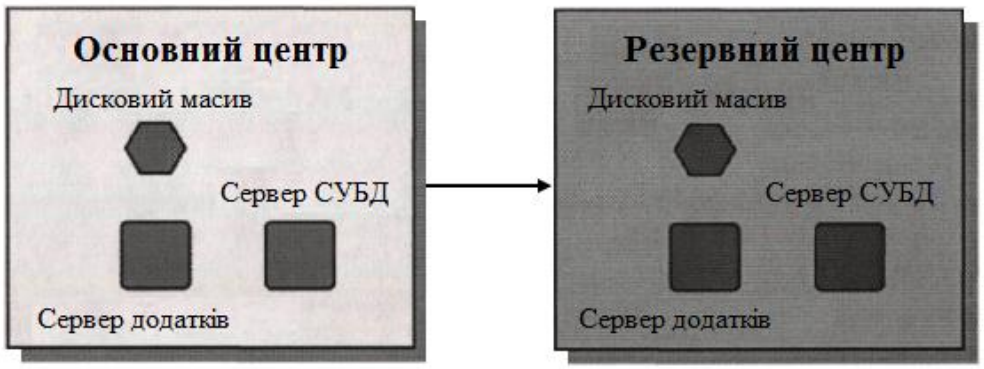

Рис. 3.4. Типова схема організації резервування з використанням резервного центру

При створенні резервного центру використовують з'єднання з мережею з пропускною здатністю, що задовольняє вимогам NRO (Network Recovery Objective-мінімальна смуга пропускання мережі, яка повинна забезпечити продовження виконання операцій. Всі зміни, що відбуваються в основному центрі обробки даних, потрібно відображати в резервному, щоб він повністю відповідав важливість справ.

За останні 10 років відбулися серйозні зміни в технологіях зв'язку, істотні характеристики яких представлені в табл. 3.3.

Таблиця 3.3.

Характеристики змін характеристик технологій зв’язку

Технологія	1996-і роки	2018 рік
Мережа	-OC-3(155 Mbit) -OC-12(622 Mbit)	-10 Gigabit Ethernet
Ввід-вивід	- SCSI, ESCON (200 Mbit)	- 4 Gigabit Fibre Channel - 10 Gigabit Fibre Channel
Лінії зв’язку	- 1 пара оптоволокна-1 лінія зв’язку	- DWDM- до 32 ліній зв’язку в одній парі оптоволокна - CWDM – 8 ліній зв’язку в одній парі оптоволокна

Аналіз показує, що при розміщенні майданчиків усередині одного міста потрібні оптоволоконні комунікації протяжністю максимум 35-40 км. Майданчики з'єднуються продуктивними каналами зв'язку з пропускною спроможністю в

десятки гігабіт. Якщо майданчики знаходяться в одному місті, і відстань між ними не перевищує 50 км, то з декількох майданчиків можна створити єдиний обчислювальний центр, розглядаючи їх просто як різні кімнати в одній будівлі. На рис. 3.5. представлена приблизна схема розподіленого обчислювального центру.

Локальні мережі (LAN) і мережі зберігання даних (SAN) всіх майданчиків пов'язані між собою. Сегменти локальних мереж, до яких підключені сервери, об'єднані в домени другого рівня моделі OSI, і це дозволяє прозоро для додатків переміщати IP-адреси серверів з майданчика на майданчик.

Завдяки об'єднанню SAN всіх майданчиків, сервери можуть використовувати ресурси зберігання даних на будь-який з них.

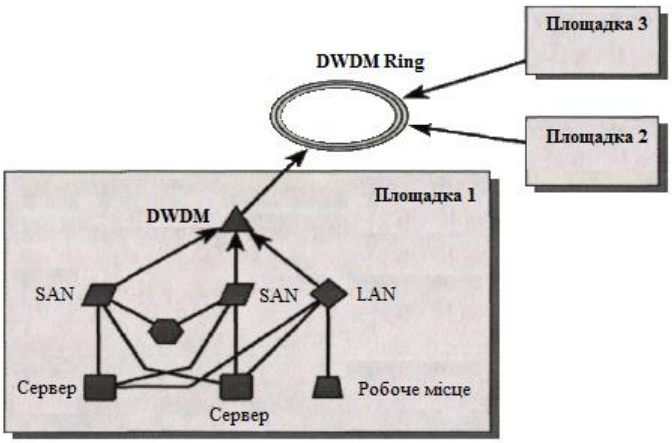

Рис. 3.5. Схема розподіленого обчислювального центру

Майданчики об'єднані за допомогою технології DWDM. Для надійності з'єднання використовується схема "кільце" (DWDM Ring).

Устаткування DWDM забезпечує захист каналів зв'язку на фізичному рівні - імпульси світла можуть передаватися між двома точками на кільці по двом різним маршрутам (умовно назвемо їх "короткий", коли відстань між точками на кільці мінімально, і "довгий"). В разі розриву кільця між двома майданчиками "короткий" маршрут стає недоступним, але світлові імпульси продовжують передаватися по "Довгому" маршруту і зв'язок між майданчиками не губиться [13]. При правильної конфігурації обладнання локальної мережі та мережі передачі даних розрив кільця і зміна маршруту передачі світлових імпульсів між майданчиками не призводять до втрати інформації і відбуваються прозоро для обладнання SAN і LAN. Прозорий

доступ між майданчиками дозволяє використовувати замість схеми "Резервний центр" більш прості способи локального резервування: сервери, резервують один друга, можуть перебувати на різних майданчиках, а дані розташовуються на "Дзеркалі" з двох дискових масивів, також розташованих на різних майданчиках. Локальні схеми резервування передбачають набагато більше варіантів, ніж схема резервного центру.

Між кожною парою майданчиків за допомогою двох пар оптоволокна і мультиплексорів / демультіплексорів CWDM проводяться 16 каналів зв'язку.

Це можуть бути канали Gigabit Ethernet і 2 Gigabit Fibre Channel. Такого кількості каналів повинно вистачити для створення розподіленого обчислювального центру в компанії середнього розміру [13].

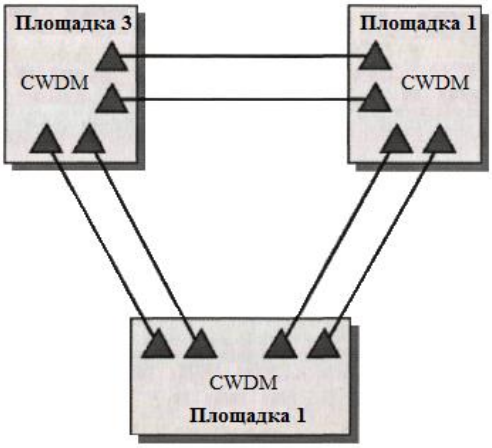

Рис. 3.6. Варіант з'єднання трьох майданчиків з використанням CWDM

Для з'єднання майданчиків буде потрібно 12 мультиплексорів/ демультіплексорів CWDM і 96 приймачів CWDM з 8-ма різними довжинами хвилі. Але все одно ціна рішення виходить значно нижче, ніж в разі DWDM. З'єднання чотирьох майданчиків зазначеним чином буде виглядати вже складно, а ось для з'єднання двох майданчиків CWDM - майже ідеальний варіант (див. рис. 3.7.).

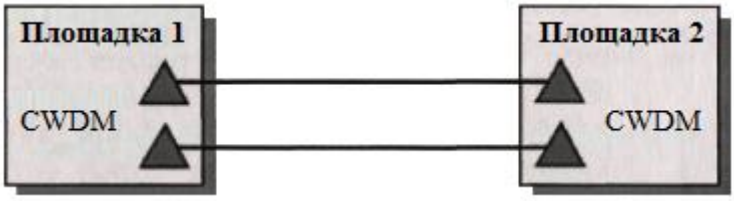

Рис. 3.7. Варіант з'єднання двох майданчиків CWDM

IT-система підприємства або організації централізованою теж повинна бути кілька територій. 1Т-система, яка обслуговує представлена на рис. 3.8. [13].

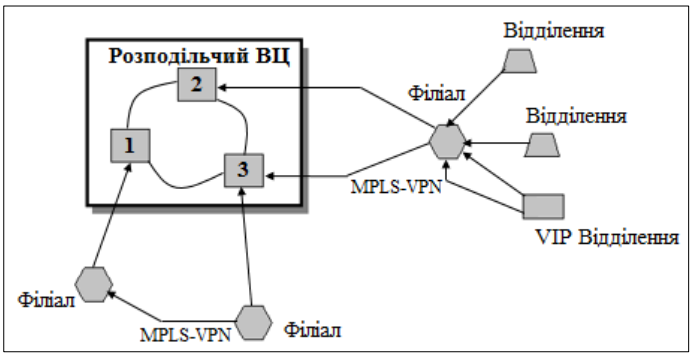

Рис.3.8. IT-система підприємства

IT - архітектура в цьому випадку спирається на сильний центр і базується на наступних принципах:

- зосередити в центрі найбільш значущі функції IT;

- винести на периферію функції 1Т, розміщення яких в центрі призводить до непотрібних витрат;

- зосередити в центрі все складні рішення, периферійні конструкції максимально стандартизувати.

Такий підхід дозволяє зосередити в центрі системи рішення по підвищення продуктивності і надійності. 1Т-інфраструктура має три рівня ієрархії - центральний офіс, філія і відділення; відділення підключені до своїм філіям, у центрального офісу можуть бути свої відділення, необхідні для роботи компанії в центрі.

Засоби підтримки основних додатків - сервери СУБД і додатків - розташовуються тільки в центральному офісі, що забезпечує необхідну продуктивність і доступність додатків, а також впровадження нових функціональних додатків.

Резервні канали можуть бути організовані за двома схемами.

1. Основний і резервний канали з'єднують філія і центральний офіс і належать різним провайдерам. Такий варіант використовується для філій, розташованих в центральній частині Росії, де існують розвинена мережа каналів зв'язку і кілька телекомунікаційних провайдерів зі своєю інфраструктурою.

2. Резервний канал з'єднує філія з іншим філією, розташованим в сусідньому регіоні, що обслуговується іншим телекомунікаційним провайдером. Так, наприклад, простіше отримати канал від Вінниці до

Львова, ніж другий незалежний канал від Вінниці до Києва. Філія-сусід буде пропускати через себе транзитний графік в разі відмови основного каналу. Резервний канал може бути організований по ешевшою технології, ніж основний. Основний канал від філії до центрального офісу реалізований по виділеній лінії, а резервний, зв'язує філії, - за технологією MPLS VPN, широко застосовуваної зараз телекомунікаційними провайдерами України.

Відділення підключаються до філій по нерезервовані каналам зв'язку місцевих телекомунікаційних провайдерів. Для відділень класу VIP може бути передбачено резервування каналу зв'язку з філією шляхом організації VPN-з'єднання через Інтернет. В цьому випадку не гарантується пропускна здатність каналу, але зберігається можливість роботи відділення.

Якщо на підприємстві вся діяльність з обробки даних зосереджена в єдиному центрі обробки даних, то деякі з клієнтів такого підприємства неминуче виявляться "далеко" від додатків в сенсі часу проходження повідомлень, що призведе до збільшення часу відгуку на запити подібних клієнтів і уразливості підприємства перед "локальними" конкурентами. На рис. 3.9. зображені два сайти (Сайт I і Сайт II). Кожен з цих сайтів є набором з'єднаних між собою кластерів, причому принаймні один з цих кластерів є для даного сайту головним (site master); весь набір кластерів (сайт) підключений до іншої частини глобальної системи кластерів. Програмне забезпечення головного кластера сайту можна конфігурувати таким чином, щоб відмови серверів виявлялися і оброблялися локально. На рис. 3.9. сервер C-2 кластера 3 є головним для Сайту I, а сервер E-2 - головним для Сайту II.

У глобальній системі кластерів інформація про копіях на сайті передається через головний сервер.

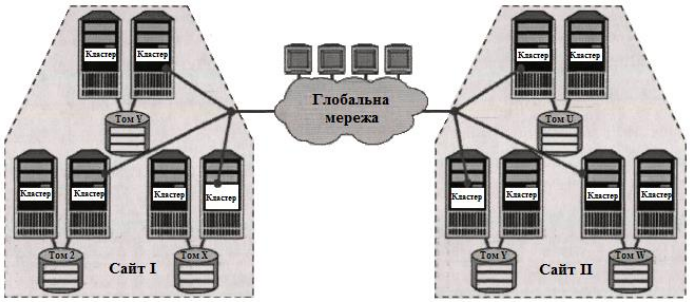

Рис. 3.9. Представлення інформації

У глобальному електронному бізнесі пік активності переміщається по регіонах циклічно, відповідно до настанням робочих годин у даному регіоні. Електронний бізнес найбільш ефективний в тих випадках, коли така інформація обробляється "недалеко" від клієнта в сенсі часу передачі даних по мережі, тобто з мінімальним часом затримки, обумовленої передачею з глобальних мереж зв'язку.

На рис.3.10. представлений сценарій відновлення систем після аварії, в якому поєднуються реплікація даних і глобальна кластеризація.

Рис.3.10. Сценарій відновлення систем після аварії

Зображені на рис.3.10. кластери P і Q перебувають один від одного на відстані в кілька тисяч кілометрів. Дані з томи X кластера P реплікуються на тому Y кластера Q через глобальну обчислювальну мережу.

Група прикладних сервісів P1 може виконуватися на будь-якому з серверів кластера P, а в разі відмови цього сервера їх виконання можна перенести на будь-який інший сервер цього кластера.

Аналогічно, група прикладних сервісів Q_1 може виконуватися на будь-якому з серверів кластера Q, а в разі відмови цього сервера їх виконання можна перенести

на будь-який інший сервер цього кластера. додаток Q_1 складається з наступних компонентів:

- сценарій для зупинки реплікації, відключення томи У як допоміжної репліки даних і його повторного монтування як локального томи читання / запису для використання додатком;

- сценарій або програма для перевірки цілісності всіх використовуваних додатком даних, яку необхідно провести до того, як можна буде перезапустити образи додатка P1;

- файли програм, що використовуються прикладним сервісом P_1.

Обидва розглянутих кластера входять до складу глобальної кластерної системи. Головні сервери сайтів обмінюються між собою періодичними контрольними повідомленнями для перевірки стану глобального кластера. Механізми глобального кластера починають діяти тоді, коли відбувається збій в обміні контрольними повідомленнями між двома сайтами, що вказує на відмову всього сайту. В цьому випадку, відповідно до вказаної політикою глобальний кластер починає виконання групи прикладних сервісів Q1. агент DNS глобального кластера вступає у взаємодію з DNS-ссрвером мережі, щоб перепризначити доменні імена додатки IP-адресами кластера Q.

Для оптимізації використання ресурсів зазвичай застосовуються схеми взаємного перенесення виконання додатків на альтернативні сервери в випадку відмови, тобто для одних додатків продуктивні сервера розташовуються на одному першому сайті, а резервні на другому, а для інших - навпаки.

При проектуванні IT-інфраструктури сучасних територіально розподілених автоматизованих систем в даний час зазвичай використовуються архітектури, що передбачають створення одного або декількох центрів обробки даних (ЦОД), іноді знаходяться на значній відстані один від одного. Прийнявши за основу описану вище 7- ми рівневу (0 ...- 6) класифікацію побудови систем резервування та управління даними, розроблену ще в 1992 р користувальницької групою SHARE за підтримки IBM [12], і допрацювавши її на основі українського і міжнародного досвіду побудови територіально-розподілених IT- архітектур з виділеними

центрами обробки даних [3,8,13,14], пропонується виділити 10 найбільш поширених схем організації резервування інформаційних масивів і IT-сервісів в територіально-розподілених IT- інфраструктурах з виділеними центрами обробки даних.

При резервуванні інформаційних масивів і IT-сервісів в територіально-розподілених IT-інфраструктурах з виділеними центрами обробки даних можна виділити наступні основні схеми, об'єднані в 3 групи (рис.3.11.):

1. Централізована обробка даних в одному єдиному ЦОД. Ризики виходу з ладу всієї площадки знижуються шляхом різних захисних заходів. Резервні майданчика не передбачені.

1.1. Проводиться регулярне резервне копіювання ІМ і ПМ з зберіганням резервних копій в тому ж приміщенні/будинку. В разі катастрофи (пожежа, повінь, прорив труб і т.д.) існує ризик повної втрати даних.

1.2. Проводиться регулярне резервне копіювання зі зберіганням резервних копій в окремому приміщенні/будинку. Метод носить назву «Pickup Truck Access Method (ротами)». Дані на видобутих носіях регулярно вивозяться на зберігання в окреме захищене приміщення/будинок. У разі виходу з ладу основного ЦОД необхідний час на ліквідацію наслідків аварії в ЦОД (або організацію нового майданчика, закупівлю обладнання і т.д.) і на відновлення даних з резервних копій.

2. Створюється майданчик резервного ЦОД. У штатному режимі обладнання резервного ЦОД не використовується в процесі виробничої діяльності (резервний ЦОД задіюється тільки в надзвичайній ситуації).

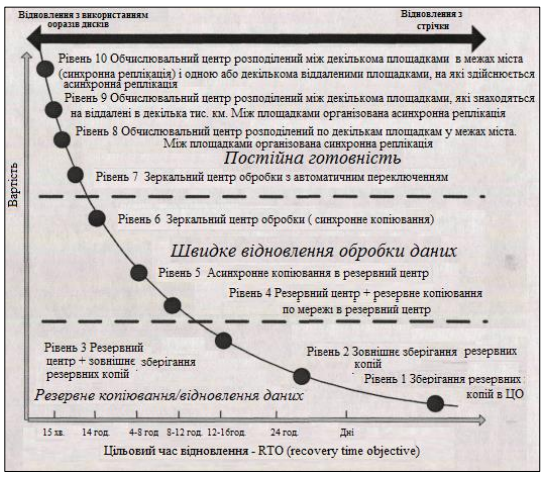

Рис.3.11. Класифікація рівнів побудови систем резервування та управління даними

2.1. Використовується відновне резервування (територіально віддалений резерв використовується тільки для відновлення на резервній майданчику основних ІМ і ПМ і їх копій, які використовуються потім для рішення задачі).

2.1.1. Конструктор резервного копіювання та архівування даних на резервний майданчик (комбінація РТАМ + Резервний центр). Метод носить назву «РТАМ + hostsite». Дані на видобутих носіях регулярно вивозяться на зберігання в окреме захищене приміщення. Додатково, в законсервованому стані існує резервний центр. Після аварії резервні копії витягуються з сховища, проводиться запуск резервного центру та відновлення даних на резервній майданчику. Час відновлення - кілька днів. Можлива втрата частини даних, введених після останнього резервного копіювання.

2.1.2. Конструктор резервного копіювання та архівування найбільш критичних даних на резервний майданчик але каналам зв'язку (комбінація РТАМ + резервний центр + використання засобів зв'язку для віддаленого копіювання найбільш критичних даних). Метод називається «Electronic Vaulting».

Резервний центр не законсервований повністю, а здійснює по мережі регулярне копіювання найбільш часто оновлюваних і самих критичних для бізнесу даних. Час відновлення – кілька днів. Можлива втрата даних, введених після останнього резервного копіювання. Проміжок часу, за який можлива втрата даних, визначається періодичністю резервного копіювання по мережі.

2.2. Використовується оперативне резервування (територіально віддалений резерв використовується для вирішення завдання в разі недоступності основних ІМ і ПМ і їх копій, що знаходяться в основному ЦОД). Режим швидкого відновлення сервісів. Конструктор реплікації даних на резервний майданчик.

Як правило, використовуються різні варіанти кластерних комплексів, у яких вузли тим чи іншим способом розносяться на віддалені площадки.

2.2.1. Реплікація даних на резервний майданчик в асинхронному режимі (з невеликим запізненням). Метод називається «Electronic vaulting to hotsite ». Перемикання додатків на резервну майданчик здійснюється в ручному режимі. Час відновлення - кілька годин (визначається часом перемикання додатків на резервний ЦОД). Можлива втрата частини даних, введених перед аварією. Проміжок часу, за який можуть бути втрачені даних, визначається часом затримки при асинхронної передачі даних.

2.2.2. Реплікація даних на резервний майданчик в синхронному режимі. Перемикання додатків на резервний майданчик здійснюється в ручному режимі. Метод називається «Two-site, two- phase commit ». Даний метод відрізняється від «Electronic vaulting to hotsite »тим, що дані по мережі регулярно копіюються на повністю розгорнутий резервний центр в синхронному режимі, тобто операція запису в основному ЦОД-е вважається завершеною одночасно з отриманням квитанції про записи даних в резервному ЦОД-і. Час відновлення від декількох хвилин до декількох годин (визначається процедурою перемикання на резервний ЦОД).

2.3. Оперативне резервування. Режим постійної готовності.

Реплікація даних на резервний майданчик здійснюється в синхронному режимі. Використовуються різні варіанти кластерних комплексів, у яких вузли тим чи іншим способом розносяться на віддалені площадки. Перемикання додатків на резервну майданчик в разі аварії проводиться автоматично. Метод називається «Zero data loss». Відрізняється від методу «Two-site, two-phase commit »тим, що перемикання користувачів проводиться автоматично так, що ні одне натискання клавіші користувач не втрачається.

3.Розподілена обробка даних в декількох ЦОД. всі майданчики використовуються в процесі виробничої діяльності.

Використовуються різні варіанти кластерних комплексів, у яких вузли тим чи іншим способом розносяться по різним майданчикам.

3.1. Обчислювальний центр розподілений по декількох майданчиках, знаходяться на відстані не більше 50 км (в межах одного міста). В цьому випадку з

декількох майданчиків можна створити єдиний обчислювальний центр, розглядаючи їх просто як різні кімнати в одній будівлі. Використовуються кластерні комплекси, у яких вузли розносяться по різних майданчиках. Між вузлами організована синхронна реплікація (тобто операція запису в будь-яку з реплицируемой копій вважається завершеною при отриманні повідомлень про запис даних в усі інші реплицируемой копії на інших майданчиках). У разі аварії жодна транзакція не буде втрачена.

3.2. Обчислювальний центр розподілений по декількох майданчиках, знаходяться на істотному видаленні (в кілька тисяч кілометрів). Використовуються кластерні комплекси, у яких вузли розносяться по різних майданчиках. Між вузлами організована асинхронна реплікація (з невеликим запізненням). Можлива втрата частини даних, введених перед аварією. Проміжок часу, за який може спричинити втрату даних, визначається часом затримки при асинхронної передачі даних.

3.3. Обчислювальний центр складається з декількох майданчиків, розташованих в межах одного міста, плюс одна або кілька майданчиків на істотному видаленні (в іншому регіоні). Між майданчиками в межах міста організована синхронна реплікація, на віддалені площадки здійснюється асинхронна реплікація.

3.3 Комплекс методів вирішення задачі оптимізації підсистеми забезпечення доступності інформаційних ресурсів автоматизованих системах обробки даних в розподілених системах.

Для сучасних територіально-розподілених автоматизованих систем, побудованих з використанням каналів глобальних мереж передачі даних, завдання забезпечення високої доступності необхідно вирішувати комплексно. Це означає, що в захисті потребує весь ланцюжок - від користувачів (можливо, віддалених) до критично важливих серверів (в тому числі серверів безпеки), а також будівель і приміщень з усією необхідною інфраструктурою, де функціонують дані сервера. При цьому ймовірність відмови буде визначатися ймовірністю відмови найслабшої

ланки в цьому ланцюжку. Для забезпечення високої доступності інформаційних ресурсів в систему вводять достатню надмірність для продовження роботи в разі відмови одного з компонентів системи. Наприклад, таких, як руйнування інформаційного масиву або програмного модуля, а також виходу з ладу процесора, жорсткого диска, мережевої карти, каналу зв'язку та інших відмовах і збоях апаратного і програмного забезпечення. Якщо така відмова відбувається, система переносить робоче навантаження на резервні пристрої або навіть на інший вузол. За в деяких випадках такий захист не зможе майданчики, на якій розташований центр обробки даних, для підтримки безперервності функціонування системи обробки даних необхідне рішення, що забезпечує роботу при множинних точках відмови. В результаті аналізу викладених в попередніх розділах моделей і методів, пропонується методика рішення комплексної задачі оптимізації рівнів збереження і доступності інформаційних ресурсів в АСОД, використовують канали глобальних мереж передачі даних. Методика полягає у вирішенні чотирьох етапну завдання послідовної оптимізації. При цьому на першому етапі здійснюється вибір варіанта захисту центру обробки даних від аварій і катастроф на основі методу цілеспрямованого вибору варіанту захисту інформаційних ресурсів і елементів інфраструктури від аварій і катастроф (на основі методу векторної стратифікації). На другому етапі, для варіанта захисту від аварій і катастроф, обраного на етапі 1, проводиться оптимізація процесу реплікації даних в територіально-розподіленої автоматизованої паспортної системи з використанням моделей і протоколів несуперечності при організації реплікації між віддаленими центрами обробки даних в АСОД (на реплікації між віддаленими центрами обробки даних в АСОД. На третьому етапі здійснюється вибір оптимального варіанту організації резервування з метою вирішення поточної функціональної завдання в структурі, сформованої на етапах 1 і 2. Вибирається оптимальна дисципліна обробки запитів і оптимальна стратегія оперативного резервування. Для обраної стратегії розраховується оптимальне число копій або передісторій. На останньому, четвертому етапі, здійснюється вибір оптимальної схеми організації відновного резервування в структурі, сформованої на етапах 1, 2 і 3.

3.4. Результати практичної реалізації запропонованих методів

У роботі розглянуто підхід оцінки ефективності запропонованого комплексу заходів підвищення доступності. В якості критерію ефективності розглядається коефіцієнт ефективності заходів щодо підвищення доступності, що є відношенням між зниженням ризику порушення доступності (в грошовому вираженні) і додатковими капітальними і експлуатаційними витратами, необхідними для зниження ризику на зазначену величину. Величина сумарного ризику порушення доступності інформаційних ресурсів при відсутності заходів щодо підвищення доступності розраховується за наступною формулою:

$$R_{\sum} = \sum_i Q_i W_i , \qquad R_n = \sum_i Q_{ni} W_{ni}$$

Де Q_i ймовірність реалізації небезпек стосовно *i*-й трупи об'єктів небезпеки; W_i - збиток в разі реалізації небезпек в відношенні *i*-ї групи об'єктів небезпеки. Відповідно кожній групі об'єктів небезпеки буде відповідати ризик $R_t=Q_tW_t$

Розрахунок значень ризику R_n для кожного з варіантів підвищення доступності, отриманого при використанні чотирьохетапну методики оптимізації, здійснюється наступним чином:

$$R_n = \sum_i Q_{ni} W_{ni} ,$$

де n - номер варіанта; *i* - номер групи небезпек, що впливають на певну групу об'єктів небезпек.

Виділено 4 групи небезпек, заходи протидії яким розглядаються на кожному з етапів даної методики, тоді:

$$R_n = Q_n^{\text{ЦОД}} W_n^{\text{ЦОД}} + Q_n^{\text{НП}} W_n^{\text{НП}} + Q_n^{OP} W_n^{\text{ОР}} + Q_n^{\text{ВР}} W_n^{\text{ВР}} ,$$

Для кожного з розглянутих варіантів обчислюються величини зниження ризику в порівнянні з величинами ризиків, розрахованих для випадку відсутності заходів захисту:

$$\Delta R_n = R_{\sum} - R_n$$

Розрахунок витрат C_n на реалізацію кожного варіанту заходів підвищення доступності здійснюється наступним чином:

$$C_n = \sum_i C_{ni},$$

де n - номер аналізованого варіанта; *i*- стаття витрат.

Коефіцієнт ефективності обраного комплексу заходів підвищення доступності інформаційних ресурсів визначається наступним чином:

$$K_E = \frac{\Delta R_n}{C_n}$$

В процесі роботи в дипломній роботі комплексної методики підвищення доступності інформаційних ресурсів були досягнуті значення коефіцієнта $К_э$ порядку 0,2-0,3.

ВИСНОВОК

Використання інфраструктури глобальних мереж, створює можливості застосування нових і модифікації вже відомих методів підвищення збереження і доступності інформації, баз знань і програмних модулів. Комплексне вирішення завдань підвищення збереження і доступності ІР в розподільних системах може бути забезпечено розробкою і широким застосуванням формалізованих моделей, прикладних методів аналізу і синтезу механізмів підвищення катастрофо- і відмовостійкості розподілених систем.

Існуючі в даний час моделі і методи в основному орієнтовані на локальну оптимізацію окремих характеристик доступності ІР і підтримуючої інфраструктури, а також збереження ІР і не забезпечують належного комплексного, взаємопов'язаного рішення з оптимізації рівнів доступності та збереження ІР при проектуванні розподілених систем зберігання даних.

У дипломній роботі виконано дослідженння особливості побудови розподілених систем, проведено аналіз основних чинників, що призводять до порушення збереження і доступності інформації. Виконаний аналіз методів резервування та відновлення інформації, які орієнтовні на успішне вирішення функціональних завдань в розподілених системах. Розроблено методи оптимізації підсистеми забезпечення доступності інформаційних ресурсів в розподілених системах обробки даних.

Запропоновані в роботі моделі і методи формують науково методичне забезпечення ефективних засобів підвищення рівнів збереження і доступності інформаційних ресурсів в АСОД, використовують канали мережі Інтернет. Використання цих коштів дозволяє зменшити витрати на розробку необхідних інструментальних засобів на 30-50%, знизити витрати на забезпечення заданих рівнів збереження і доступності інформаційних ресурсів не менше, ніж в 3-5 разів. При заданих витратах дані рівні підвищуватися не менше, ніж на 30%.

Розроблені методи, алгоритми та інструментальні засоби можуть бути використані при розробці комерційних АСОД широкого класу і призначення в

науково-дослідних, проектних організаціях і обчислювальних центрах, комерційних організаціях, які розробляють і впроваджують системи даного класу.

Отримані результати можуть використовуватись в ході проектування ряду корпоративних підсистем інформаційної безпеки, пов'язаних з резервуванням і відновленням IP, що робить обрану тему роботи вельми актуальною.

ПЕРЕЛІК ПОСИЛАНЬ

1. В. Кастрюков Когда WAN быстрее LAN, или способы консолидации WAN- офисов М: - “Storage News” № 1 (26), 2006.

2. Кульба В.В., Павельев С.В., Микрин Е.А. Методы обеспечени доступност программного и информационного обеспечения территориально-распределенных системах обработки данных, построенных с использованием инфраструктуры глобальных сетей передачи данных. -М., 2008 (Научное издание/Институт проблем управления им. В.А. Трапезникова РАН)

3. Дж. Уолрэнд Телекоммуникационные и компьютерные сети. Вводный курс. Москва: Постмаркет, 2001. - 480 с.

4. Jan Matlis, “Scale-Free Networks”, (Computerworld'). November 04, 2002

5. Семенов Ю.А. "Сети Интернет. Архитектура и протоколы" (Сиринъ, М. 1998)

6. Павельев С.В. Методы обеспечения сохранности информаци пользователей в сети Интернет. // Теория активных систем / Труды международной научно-практической конференции (17-19 ноября 2003 г., Москва, Россия). Общая редакция -В.Н.Бурков, Д.А.Новиков. Том 2. -М.: ИЛУ РАН, 2003.

7. Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. Издание второе. Серия «Информационные технологии». - М.: СИ1 [ТЕГ, 2003, 500 с.

8. В.Галатенко, И.Дорошин Доступность как элемент информационной безопасности, М:- «Jet Info», №2(33), 1997.

9. C. Brooks, M. Bedemjak, I. Juran, J. Merryman Disaster Recovery Strategies with Tivoli Storage Management International Technical Support Organization IBM Redbooks SG24-6844-01 November 2002.

10. Шелков А.Б., Сомов С.К., Коробко В.Б. Восстановительно резервировани программных модулей и информационных массивов в сетях ЭВМ.// Анализ и синтез оптимальных модульных СОД: Сборник трудов Института проблем управления. М.: ИЛУ, 1984.

11. Шелков А.Б., Сомов С.К. Резервирование программ и данных в системах коллективного пользования// Теоретические и прикладные задачи оптимизации. М.: Наука, 1985.

12. C. Warrick, C. Beretta, R. Ghem, L. Hilliard, S. Kamonthipsukon, S. Rolandi, J. Sing, G. J. Tarella, C. Lcung IBM Total Storage Business Continuity Solutions Guide, International Technical Support Organization, IBM Redbooks SG24-6547-02, August 2005.

13. Д.Л. Голубев Распределенные центры обработки данных М:- «Jet Info» , №5 (156), 2006.

14. Р. Третау, Э. Андал, Р. Батталья, Д. Эдвардс, Х. Спе Управление хранением данных IBM Tivoli Storage Management IBM Redbooks SG24-4877-03, в переводе, Москва, КУДИЦ-ОБРАЗ, 2006.

15. Э. Таненбаум, М. Ван Стен Распределенные системы. Принципы и парадигмы. — СПб.: Питер, 2003. - 877 с.: ил.

16. Stumm, M., Zhou, S.: “Algorithms Implementing Distributed Shared Memory.”Computer, vol. 23, no. 5, pp. 54-64, 1990.

17. Комер Д. Принципы функционирования Интернета. - СПб.: Питер, 2002.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ