МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

СИГИДЕНКО Микола Михайлович

Модель захисту інформації на основі ресурсів мультисервісних мереж / Information Protection Model Based on Multi-Service Network Resources

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -22
М.М. Сигиденко

_____

Науковий керівник
д.т.н., професор В.В.Яцків

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
СИГИДЕНКО МИКОЛА МИХАЙЛОВИЧ

1. Тема кваліфікаційної роботи:
Модель захисту інформації на основі ресурсів мультисервісних мереж / Information Protection Model Based on Multi-Service Network Resources

керівник роботи д.т.н., професор В.В. Яцків
затверджені наказом по університету від «__» _____ 2022 року № _____
2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– сучасного стану забезпечення конфіденційності, цілісності і доступності інформації в мультисервісних мережах зв'язку;
– дослідження можливості використання багаторазового асиметричного шифрування;
– розробка методу та імітаційне моделювання для забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку;
– розробка узагальненої функціональної моделі маршрутизації в мультисервісних мережах зв'язку;
– розробка методик захисту інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку.

5. Перелік графічного матеріалу у роботі:
– схема пошуку маршруту «Логічним» методом;
– градієнтний і дифузний вибір вихідних ТПП;
– пошук маршруту «Локально-хвильовим» методом;
– концепція методики забезпечення цілісності інформації;
– концепція методики забезпечення доступності інформації;
– концепція методики забезпечення конфіденційності інформації;

– схема розшифрування повідомлення.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз сучасних підходів для забезпечення конфіденційності, цілісності та доступності інформації	12.2022 р. – 03.2023 р.	
2	Розроблення методів захисту інформації з використанням ресурсів мультисервісних мереж зв'язку	03.2023 р. – 05.2023 р.	
3	Розроблення методик захисту інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку	05.2023 р. – 11.2023 р.	

Студент _____ Сигиденко М.М.
(підпис)

Керівник роботи _____ д.т.н., професор В.В.Яцків

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Модель захисту інформації на основі ресурсів мультисервісних мереж” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 78 сторінок і містить 18 ілюстрацій, 2 таблиці, 1 додаток та 30 джерел за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка моделі захисту інформації на основі ресурсів мультисервісних мереж.

Методи дослідження. Математичні методи моделювання, методи дослідження мереж, методи маршрутизації..

Результати дослідження. Здійснено аналіз сучасного стану забезпечення конфіденційності, цілісності і доступності інформації в мультисервісних мережах зв'язку, що дало змогу обгрунтувати і дослідити можливості використання багаторазового асиметричного шифрування. Розроблено метод забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку та проведено його імітаційне моделювання, що дозволило встановити критерії вибору ресурсів мультисервісних мереж зв'язку для забезпечення цілісності та доступності інформації. Розроблено узагальнену функціональну модель маршрутизації в мультисервісних мережах зв'язку, що дозволило встановити методи формування плану розподілу інформації в мультисервісних мережах зв'язку. Розроблено методики забезпечення цілісності, доступності та конфіденційності інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку, а також узагальнену методику захисту інформації в мультисервісних мережах.

Результати роботи можуть успішно застосовуватися для захисту інформації на основі ресурсів мультисервісних мереж.

КЛЮЧОВІ СЛОВА: МУЛЬТИСЕРВІСНА МЕРЕЖА, РЕСУРСИ МЕРЕЖІ, ЗАХИСТ ІНФОРМАЦІЇ, МОДЕЛЬ, КОНФІДЕНЦІЙНІСТЬ.

ABSTRACT

The graduate work on the topic „Information Protection Model Based on Multi-Service Network Resources” for Master’s degree on speciality 125 "Cybersecurity " is written on 78 pages and contains 18 illustrations, 2 tables, 1 suplement and 30 references.

The aim of graduate work is to develop a model of information protection based on the resources of multi-service networks.

Research methods. Mathematical modeling methods, network research methods, routing methods.

Results of the study. An analysis of the current state of ensuring confidentiality, integrity and availability of information in multi-service communication networks was made, which made it possible to substantiate and investigate the possibilities of using multiple asymmetric encryption. A method of ensuring the integrity of information at the network level of multi-service communication networks was developed and its simulation modeling was carried out, which made it possible to establish criteria for the selection of resources of multi-service communication networks to ensure the integrity and availability of information. A generalized functional model of routing in multi-service communication networks was developed, which made it possible to establish the methods of forming an information distribution plan in multi-service communication networks. Methods for ensuring the integrity, availability and confidentiality of information at the expense of network resources of a multi-service communication network have been developed, as well as a generalized method of protecting information in multi-service networks.

The results of the work can be successfully applied to protect information based on the resources of multi-service networks..

Keywords: MULTISERVICE NETWORK, NETWORK RESOURCES, INFORMATION PROTECTION, MODEL, PRIVACY.

ЗМІСТ

ВСТУП

Сучасний стан та розвиток телекомунікаційних систем [1-4] характеризується прагненням виробників та провайдерів послуг до надання користувачам (через єдину точку доступу) необмеженого спектру додатків із гарантованою якістю обслуговування (Quality of Service, QoS) [5-7]. Слід зазначити, що вирішення цієї проблеми має власну історію. У середині XX століття було висловлено ідею створення єдиної автоматизованої мережі зв'язку (ЄАМЗ). Мета ЄАМЗ – максимально об'єднати, уніфікувати та автоматизувати засоби зв'язку, що дозволило б значно скоротити фінансові та організаційні ресурси на підготовку кадрів, проектування, будівництво та обслуговування телекомунікаційних систем. Однак реалізація цієї програми спочатку була утруднена через використання аналогових форм подання інформації під час її передачі через ЄАМЗ.

Наприкінці XX століття, з появою нових форм представлення інформації та методів управління в телекомунікаційних системах, ідея об'єднання та уніфікації різних служб електрозв'язку знайшла своє відображення у створенні цифрових мереж інтегрального обслуговування (ЦМІО). Спочатку передбачалося, що ЦМІО надаватиме користувачу можливість передачі інформації у цифровому форматі з швидкістю $64\times N$ кбіт/с. В результаті такі мережі отримали назву вузькосмугові ЦСІО. Однак це рішення виявилося не здатним підтримувати високошвидкісні служби електрозв'язку, що функціонують у реальному масштабі часу.

З появою технології асинхронного методу передачі (Asynchronous Transfer Mode, ATM), що фундаментально відрізняється від інших телекомунікаційних технологій, з'явилася можливість створення транспортного механізму передачі всіх видів інформації з QoS. У в результаті такі телекомунікаційні системи отримали назву широкосмугові ЦСІО (рекомендації МСЕ-Т, серія I.700-799) [8-9].

Конкуренція виробників та провайдерів послуг у боротьбі за користувачів телекомунікацій активізувала подальший розвиток технології інтернет-протоколів (Internet Protocol, IP)[10-11]. Як наслідок, робочою групою, яка проектувала IP (Internet Engineering Task Force, IETF), були розроблені технології MPLS (Multiprotocol Label Switching – мультипротокольна комутація за мітками) та IP v.6.0, що дозволяють надати користувачеві необмежений спектр додатків та QoS.

В результаті IP/MPLS і ATM стали базовими технологіями мультисервісних мереж зв'язку (ММЗ) [12-14], які мають відмінності, але мають і багато спільного:

– будь-яка користувальницька та службова інформація перетворюється на єдину форму - цифрові блоки певної довжини (пакети);

– до кожного цифрового блоку додається заголовок з даними про маршрут, який попередньо визначено та гарантує підтримку необхідних імовірнісно-часових характеристик (швидкість передачі інформації, затримка в часі, часовий джиттер, ймовірність неправильного прийому на повідомлення/пакет/символ, ймовірність відмови в обслуговуванні) інформації, що передається;

– передача користувальницьких та службових пакетів здійснюється шляхом асинхронного мультиплексування у відповідні користувацькі та службові цифрові тракти та канали;

– у пункті призначення пакети об'єднуються, перетворюються на первісну форму і передаються користувачеві для подальшої обробки.

Таким чином, подання всіх видів інформації у єдиному цифровому форматі та виділення необхідних ресурсів мережі, що гарантують QoS, перед початком передачі користувальницької інформації є обов'язковими компонентами для технологій IP/MPLS та ATM [15-16].

Природно, що за унікальної можливості мультисервісних мереж зв'язку надавати користувачам необмежений спектр додатків у реальному масштабі часу виникає проблема захисту інформації. Архітектура безпеки поділяє всі ресурси

телекомунікаційних систем (канали зв'язку, програмно-апаратні комплекси, додатки тощо) на незалежні модулі захисту [17-19]. Кожен модуль характеризується параметрами інформаційної безпеки, підтримка яких є актуальною задачею.

Мета роботи. Метою даної роботи є розробка моделі захисту інформації на основі ресурсів мультисервісних мереж.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– сучасного стану забезпечення конфіденційності, цілісності і доступності інформації в мультисервісних мережах зв'язку;

– дослідження можливості використання багаторазового асиметричного шифрування;

– розробка методу та імітаційне моделювання для забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку;

– розробка узагальненої функціональної моделі маршрутизації в мультисервісних мережах зв'язку;

– розробка методик захисту інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку.

Об’єкт дослідження. Процес захисту інформації на основі ресурсів мультисервісних мереж.

Предмет дослідження. Методи і засоби захисту інформації на основі ресурсів мультисервісних мереж.

Методи дослідження. Математичні методи моделювання, методи дослідження мереж, методи маршрутизації.

Наукова новизна одержаних результатів.

1. Здійснено аналіз сучасного стану забезпечення конфіденційності, цілісності і доступності інформації в мультисервісних мережах зв'язку, що дало змогу обгрунтувати і дослідити можливості використання багаторазового асиметричного шифрування.

2. Розроблено метод забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку та проведено його імітаційне моделювання,

що дозволило встановити критерії вибору ресурсів мультисервісних мереж зв'язку для забезпечення цілісності та доступності інформації.

3. Розроблено узагальнену функціональну модель маршрутизації в мультисервісних мережах зв'язку, що дозволило встановити методи формування плану розподілу інформації в мультисервісних мережах зв'язку.

Практичне значення отриманих результатів. Розроблено методики забезпечення цілісності, доступності та конфіденційності інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку, а також узагальнену методику захисту інформації в мультисервісних мережах.

Публікації та апробація КР.

1. Сигиденко М.М., Казьмірчук Н.В., Войтенко О.О. Аналіз захищеності інформації в мультисервісних мережах. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.77-79 [20].

2. Сигиденко М.М., Басістий В.П. Метод захищеної маршрутизації в мультисервісних мережах. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.171-173 [21].

.

1 АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ, ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ ІНФОРМАЦІЇ

1.1 Аналіз сучасного стану забезпечення конфіденційності, цілісності і доступності інформації у мультисервісних мережах зв'язку

Основними міжнародними стандартами в області інформаційної безпеки є стандарти, що визначають:

– архітектуру безпеки взаємозв'язку відкритих систем;

– концепції інформаційної безпеки відкритих систем;

– основні складові забезпечення інформаційної безпеки (ITU-T Recommendation X.810 ÷ 815, ISO/IEC 10181-2 ÷ 7) [22].

Для мультисервісної мережі зв'язку, орієнтованої на надання користувачам необмеженого спектру програм з QoS, важливим документом, що визначає її архітектуру безпеки, є ITU-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications (Архітектура безпеки для систем, що забезпечують зв'язок межи кінцевими пристроями) [23].

Архітектура безпеки (рисунок 1.1) поділяє всі ресурси телекомунікаційних систем (ТКС) (програмно-апаратні комплекси, канали зв'язку, додатки тощо) на незалежні:

1) функціональні площини захисту:

– контролю - для передачі службової інформації для моніторингу стану ресурсів ТКС;

– управління – для передачі службової інформації для поточного управління ресурсами ТКС;

– користувача – для передачі інформації від користувача;

2) рівні захисту:

– додатків – весь спектр додатків (електронна комерція, пошукові служби, відкритий доступ до інститутів управління державою, відеоконференції, дистанційне навчання, виховання, реклама, розваги і так далі);

– сервісів – весь спектр послуг ТКС, які провайдери надають своїм користувачам (доступ до Інтернету, служби динамічної конфігурації хостів, імен доменів, послуги телефонії, QoS, служби позиціонування тощо);

– інфраструктури – структуроутворюючі елементи ТКС (лінії зв'язку, каналоутворююча апаратура, маршрутизатори, комутатори, сервери тощо).

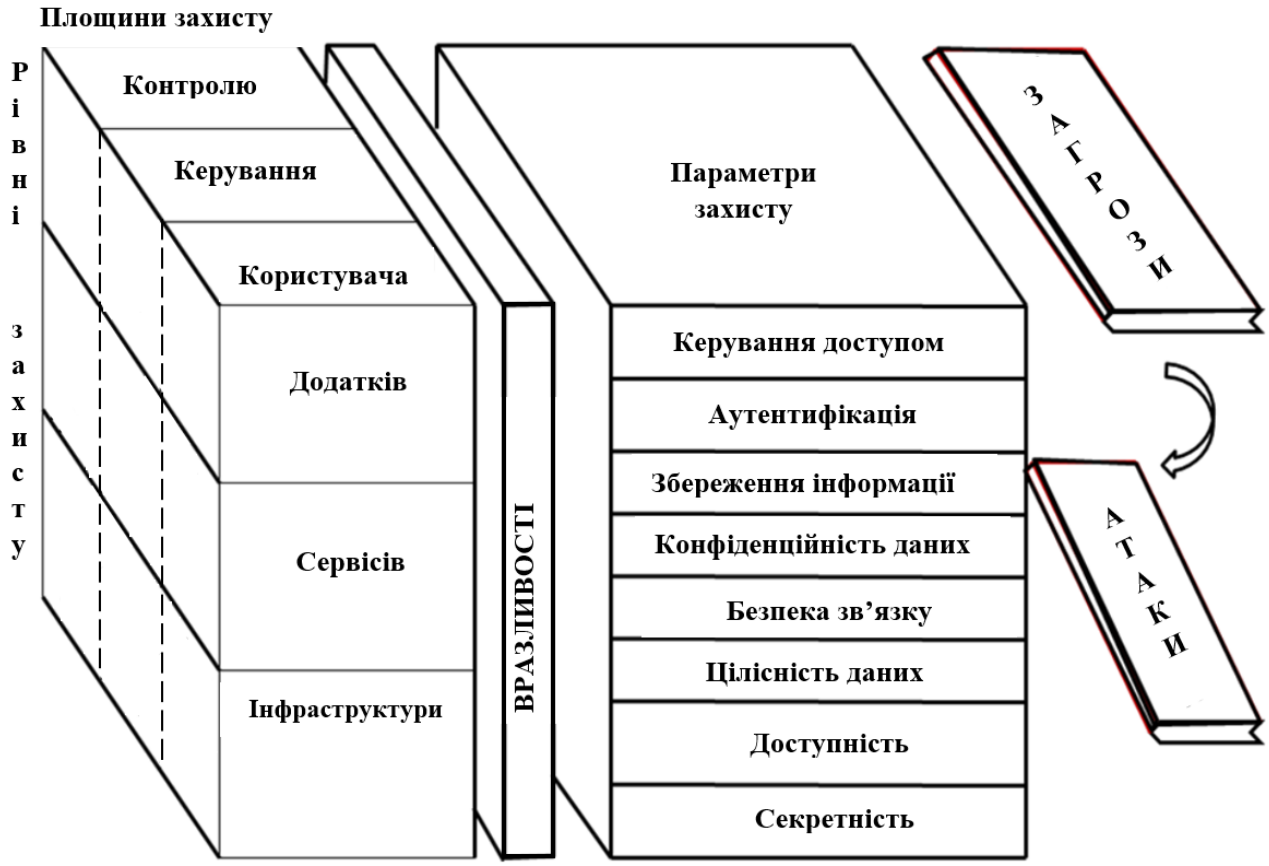


Рисунок 1.1 - Архітектура безпеки ТКС

На перетині площин та рівнів формується дев'ять незалежних модулів захисту ТКС. Кожен модуль, що містить відповідні програмно-апаратні засоби, характеризується вісьмома параметрами (вимірюваннями) захисту:

– управління доступом;

– аутентифікація;

– конфіденційність даних;

– збереження інформації;

– цілісність даних;
– безпека зв'язку;
– секретність
– доступність.

Таким чином, можна стверджувати наступне – для захисту інформації від загроз та атак порушників, спрямованих на:

– знищення інформації;
– спотворення чи зміну інформації;
– крадіжку, видалення або втрату інформації;
– розкриття інформації;
– переривання обслуговування,

необхідно виконати вимоги 72-х параметрів (вимірювань) захисту (9 модулів, кожен із яких містить 8 параметрів захисту).

Базовими параметрами (вимірюваннями) захисту інформації прийнято вважати конфіденційність, цілісність та доступність [24-26].

Конфіденційність даних – властивість інформації бути недоступною та закритою для неавторизованого індивідуума, логічного об'єкта або процесу або стан інформації, при якому доступ до неї здійснюють лише суб'єкти, які мають на нього право.

Доступність інформації – це стан інформації, за якого суб'єкти, які мають право доступу, можуть реалізувати їх безперешкодно.

Цілісність інформації – це стан інформації, за якого відсутня її будь-яка зміна чи здійснюється зміна навмисно тільки суб'єктами, які мають на нього право.

1.2 Аналіз основних підходів по забезпеченню конфіденційності інформації

Забезпечення конфіденційності ґрунтується на криптографічних способах захисту інформації [27-29]. Існує два принципові підходи:

– шифрування з одним (секретним) ключем (симетричні алгоритми шифрування);

– шифрування з двома (відкритим та секретним) ключами (асиметричні алгоритми шифрування).

У першому випадку, як правило, час шифрування/розшифрування прямо пропорційний довжині ключа та складності алгоритмів шифрування. Недоліком цього підходу є наявність закритого каналу зв'язку доставки користувачам секретного сеансового ключа. В асиметричних криптосистемах цей недолік відсутній. Однак залежність часу шифрування $t_{ш}$ від довжини ключа L_k має нелінійний характер і в загальному випадку визначається як

$$t_{ш} = A * L_k^c + B,$$

де A, B і c - постійні, значення яких визначаються криптографічними алгоритмами.

За великих значень L_k час шифрування різко зростає, що є неприйнятним для високошвидкісних додатків, які функціонують в реальному масштабі часу. Тому на практиці застосовують "гібридну" систему шифрування. Асиметричні криптоалгоритми використовуються для організації закритого каналу зв'язку (для доставки користувачам сеансових секретних ключів симетричних алгоритмів шифрування). Симетричні алгоритми використовують безпосередньо для шифрування даних між користувачами.

У цього підходу є недолік. Користувачі володіти повинні певними знаннями в галузі захисту інформації та мати спеціальне додаткове програмно-апаратне криптографічне забезпечення, застосування якого може бути обмежене внаслідок часових, технологічних, фінансових чи інших витрат.

Основна ідея полягає в поділі повідомлення M на кілька частин n за секретною схемою з подальшим відправленням цих частин за n незалежними маршрутами до одержувача інформації. Таким чином, якщо навіть якась

невелика кількість маршрутів буде піддана атакам з боку порушників, то секретне повідомлення загалом не буде розсекречено.

На сьогодні відомо кілька класів порогових схем поділу секрету:

– Шаміра (на основі степеневого многочлена);
– на еліптичній кривій;
– Блеклі (використання точок багатовимірного простору);
– Карнін-Грін-Геллмана (на основі скалярного добутку);
– Асмута-Блума (з використанням простих чисел).

Порогові схеми поділу секрету знайшли широке застосування при розв'язанні багатьох задач:

– розділене зберігання даних;
– безпечний колективний підпис;
– керування ключами в протоколах, що містять велику кількість учасників і в багатьох інших.

У даному випадку вирішується завдання динамічного розподілу даних по мережі із метою забезпечення конфіденційності інформації.

Основне призначення мультисервісних мереж зв'язку полягає в наданні користувачам необмеженого спектра додатків, зокрема високошвидкісних, що функціонують в реальному масштабі часу. Ця обставина накладає на реалізацію механізму порогової схеми поділу секрету тимчасове обмеження - алгоритмічну складність.

Переваги та недоліки основних підходів, що забезпечують конфіденційність інформації, наведено в таблиці 1.1.

"Гібридна" система для шифрування (асиметричні криптосистеми використовуються для організації таємного каналу зв'язку, а безпосередньо симетричні – вже для шифрування інформації) цілком є прийнятною у мультисервісних мережах зв'язку. Оскільки є можливість для користувачів скористатися високошвидкісними додатками, які функціонують в реальному масштабі часу, із забезпеченням конфіденційності.

До недоліків "гібридної" системи шифрування відносять такі:

– користувачі мають володіти знаннями в галузі захисту інформації;

– у своєму розпорядженні мати спеціальне криптографічне апаратно-програмне забезпечення.

Таблиця 1.1 - Результати аналізу основних підходів, що забезпечують конфіденційність інформації

<table>
<tr><th>№ п/п</th><th>Спосіб забезпечення конфіденційності</th><th>Переваги</th><th colspan="2">Недоліки</th></tr>
<tr><td>1</td><td>Симетрична система шифрування</td><td>Висока швидкість шифрування
$t_ш = A * L_k + B$</td><td>Наявність закритого каналу зв'язку</td><td rowspan="3">Користувачі повинні мати спеціальне додаткове криптографічне апаратно-програмне забезпечення</td></tr>
<tr><td>2</td><td>Асиметрична система шифрування</td><td>Відсутність закритого каналу зв'язку</td><td>Низька швидкість шифрування
$t_ш = A * L_k^c + B$</td></tr>
<tr><td>3</td><td>"Гібридна" система шифрування</td><td>1. Відсутність закритого каналу зв'язку.
2. Висока швидкість шифрування:
$t_ш = A * L_k + B$
3. Забезпечується QoS додатків користувача.</td><td></td></tr>
<tr><td>4</td><td>Багатоколійна маршрутизація з пороговою схемою поділу повідомлення</td><td>1. Користувачі не повинні мати спеціального додаткового криптографічного апаратно-програмного забезпечення.
2. Забезпечується QoS додатків ММЗ.</td><td colspan="2">1. Чутливість до зміни частин секретного повідомлення.
2. Необхідність реалізації незалежних маршрутів з однаковими ймовірно-часовими характеристиками.</td></tr>
</table>

Метод багатошляхової маршрутизації із пороговою схемою розподілу повідомлення дає змогу збільшити пропускну спроможність мережі, забезпечити

конфіденційність інформації, зменшити ризик щодо перевантаження мережі, що впливає позитивно на QoS застосунків мультисервісних мереж зв'язку.

Недоліком при використанні методу багатоколійної маршрутизації із пороговою схемою розподілу повідомлення є чутливість до зміни частин секретного повідомлення та необхідність при організації незалежних маршрутів, які володіють однаковими часово-ймовірнісними характеристиками (швидкість передавання інформації, часовий джиттер, час затримки, імовірність помилкового приймання на пакет, символ тощо).

1.3 Аналіз основних підходів щодо забезпечення цілісності та доступності інформації

На рисунку 1.2 наведено основні підходи, які забезпечують цілісність інформації [30], - криптографічні методи із дублюванням інформації і методи, що використовують резервування інформації.

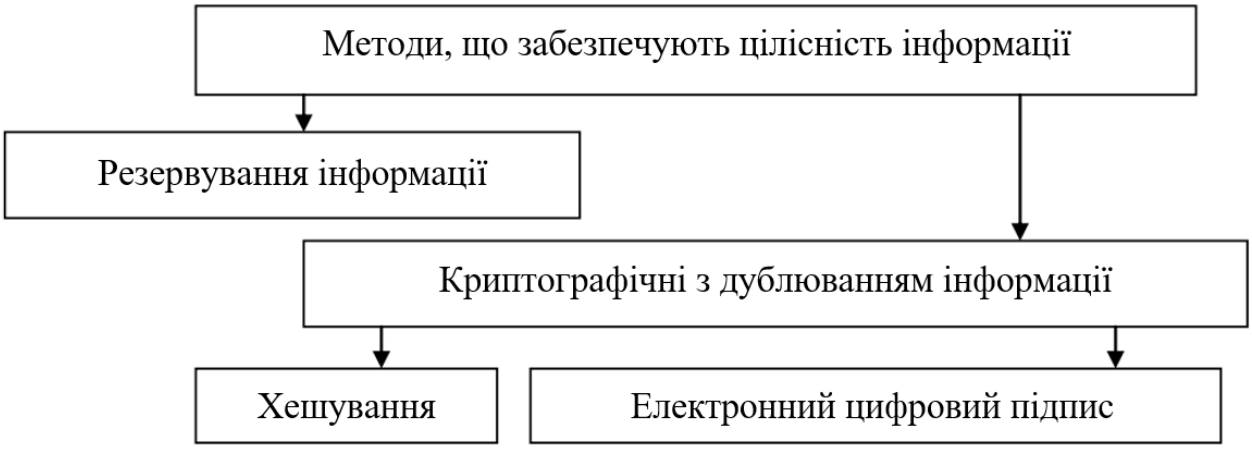


Рисунок 1.2 - Основні методи, що забезпечують цілісність інформації в ТКС

Криптографічний метод (хешування, електронний цифровий підпис) має на увазі введення в повідомлення, що передається, надмірності - перевірної комбінації, яку обчислюють за певними алгоритмами, і яка є "індикатором" для порушення цілісності інформації.

В результаті зробити можна висновок, що криптографічний метод контролює тільки цілісність інформації. В разі її модифікації джерелу зробити необхідно повторну передачу повідомлення. Ця процедура повторюватиметься доти, доки не буде забезпечена цілісність інформації. У цьому разі між віддаленими користувачами організувати необхідно канал зворотного зв'язку та канал для повторної передачі повідомлення, тобто багаторазове дублювання інформації виконати, що впливає значно на час затримки.

Таким чином, застосування у ММЗ криптографічного методу із дублюванням інформації з метою забезпечення цілісності є обмеженим для високошвидкісних додатків, які функціонують в реальному масштабі часу.

Метод резервування інформації для забезпечення цілісності має на увазі одночасне паралельне передавання інформації за кількома маршрутами та ухвалення рішення про цілісність інформації на приймальній стороні. У такий спосіб час затримки передавання інформації зменшується та забезпечується QoS високошвидкісних додатків, які функціонують в реальному масштабі часу.

Основні методи забезпечення доступності інформації такі:

– дублювання інформації, доступ до якої здійснюється;

– резервування для каналів зв'язку (КЗ).

Забезпечення доступності інформації зводяться до завдань іззабезпечення живучості і надійності мереж зв'язку.

Таким чином, аналіз основних підходів при забезпеченні базових параметрів захисту інформації (цілісність, доступність та конфіденційність) в мультисервісних мережах зв'язку виявив такі проблеми:

1) для забезпечення конфіденційності, доступності і цілісності інформації користувачі мультисервісної мережі зв'язку у своєму розпорядженні мають мати актуальне спеціалізоване (постійно оновлюване) апаратно-програмне забезпечення та володіти знаннями в галузі захисту інформації;

2) застосування основних підходів для захисту інформації у мультисервісних мережах зв'язку обмежене. Це пов'язано із збільшенням часу

затримки при передачі інформації, що критично є для додатків мультисервісної мережі, які на великих швидкостях функціонують і у реальному масштабі часу.

Вирішуються перераховані проблеми за рахунок залучення ресурсів мультисервісної мережі зв'язку (канальних, криптографічних та інших) під кожну заявку користувача при передачі захищеної інформації.

В зв'язку із цим виникає необхідність у розробленні, дослідженні нових методик, способів, методів і алгоритмів (методології), що дають змогу розв'язувати задачі забезпечення базових параметрів для захисту інформації (цілісність, доступність та конфіденційність) з підтримкою QoS додатків у мультисервісній мережі зв'язку.

1.4 Дослідження можливості використання багаторазового асиметричного шифрування

В асиметричних криптосистемах із відкритим ключем відсутній закритий канал зв'язку, що значно спрощує проблему разових сеансових секретних ключів. Однак такі алгоритми мають особливості. По-перше, для досягнення аналогічної криптостійкості із симетричними алгоритмами шифрування потрібен довший ключ. У таблиці 1.2 наведено значення довжин симетричних і відкритих ключів.

Таблиця 1.2 - Відповідність криптостійкості алгоритмів шифрування

Алгоритми	Довжини ключів				
Симетричні	56	64	80	112	128
Асиметричні	384	512	768	1792	2304

По-друге, залежність часу шифрування від довжини ключа L_k нелінійний характер.

Обидва фактори значно обмежують застосування асиметричних криптосистем у ММЗ. Це пов'язано із тим, що збільшення довжини ключа до критичного значення $L_{\text{k кр}}$ призведе до неприпустимого збільшення часу

затримки на шифрування ($t_ш$) інформації (рисунок 1.3), що позначиться на зниженні QoS високошвидкісних додатків, які функціонують в масштабі реального часу.

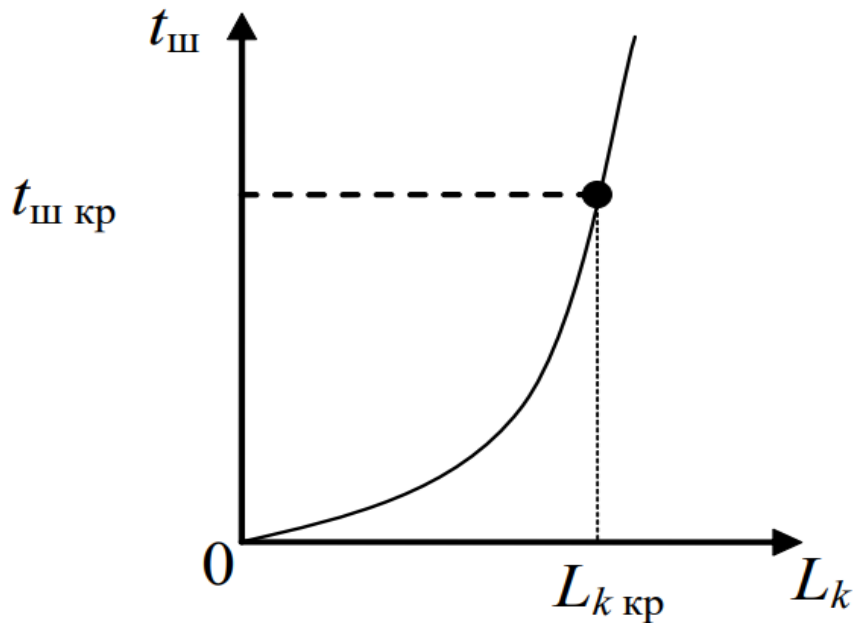


Рисунок 1.3 - Залежність часу на шифрування від довжини ключа

Водночас асиметричне багаторазове шифрування з ключами меншої довжини дає змогу розв'язати безліч проблем. Рисунок 1.4 демонструє цей підхід.

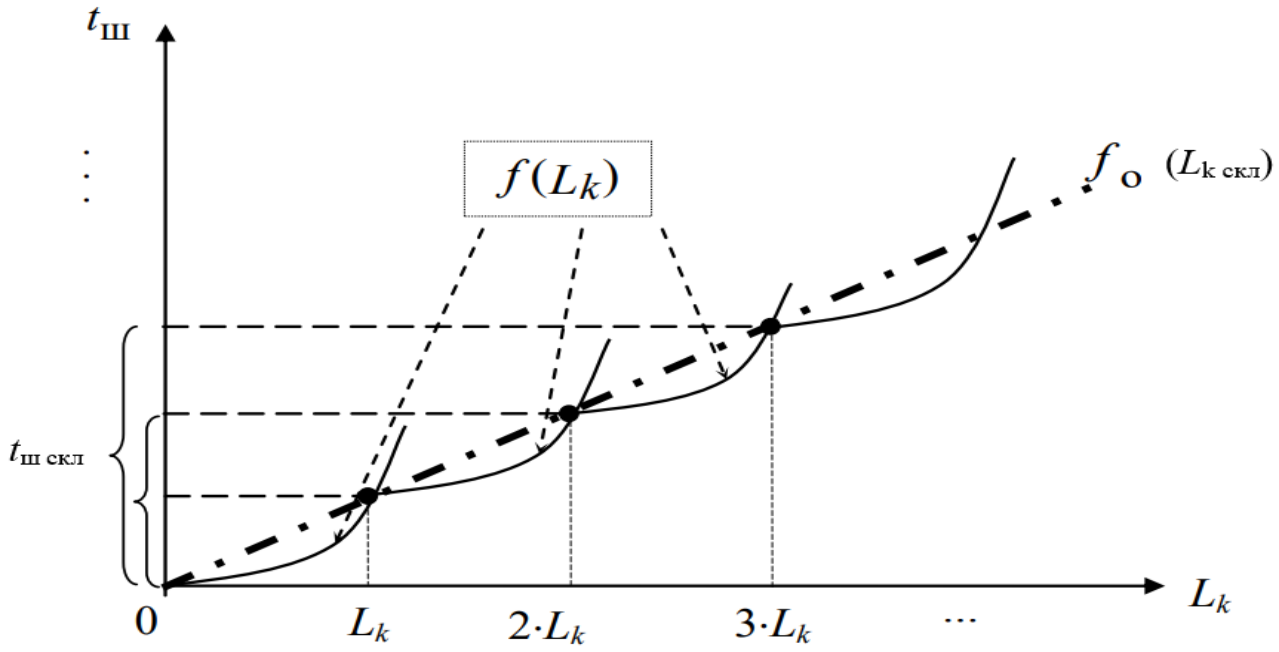


Рисунок 1.4 - Залежності часу шифрування від довжини складеного ключа

Зазначимо, що багаторазове шифрування широко використовується в симетричних криптографічних алгоритмах з метою уніфікації шифрування/розшифрування та збільшення довжини секретного ключа.

Введемо такі позначення:

$$y = E_{k^{(o)}}(M), M = D_{k^{(c)}}(y)$$

відповідно функції шифрування інформації M із використанням відкритого ключа ключа $k^{(o)}$ і розшифрування закритої інформації у c за допомогою секретного ключа $k^{(c)}$. Припустимо, що довжини всіх відкритих і секретних ключів однакові та рівні між собою, тобто:

$$L_{k_i^{(o)}} = L_{k_i^{(c)}} = L_k; i = \overline{1,l},$$

тоді загальна довжина складеного ключа багаторазового шифрування визначається виразом:

$$L_{k_{скл}} = \sum_{i=1}^{l} L_{k_i}; L_{k_i} = const.$$

Функція $t_ш = f(L_{k\ скл})$ (рисунок 1.5) являє собою складну криву, що складається з ділянок функціональних залежностей:

$$t_ш = f(L_{k\ скл}) = f\{f(L_k); \ldots; f(L_k); \ldots\}.$$

Замінимо функцію $t_ш = f(L_{k\ скл})$ на лінійну ($f_o(L_{k\ скл})$), оскільки відповідні перші похідні дорівнюють.

На рисунку 1.5 представлено експериментальні результати шифрування алгоритмом *RSA* блоку даних обсягом 1 кБ за зміни довжини ключа від 256 біт до 2048 біт і використання складеного 256-бітного ключа (багаторазове асиметричне шифрування).

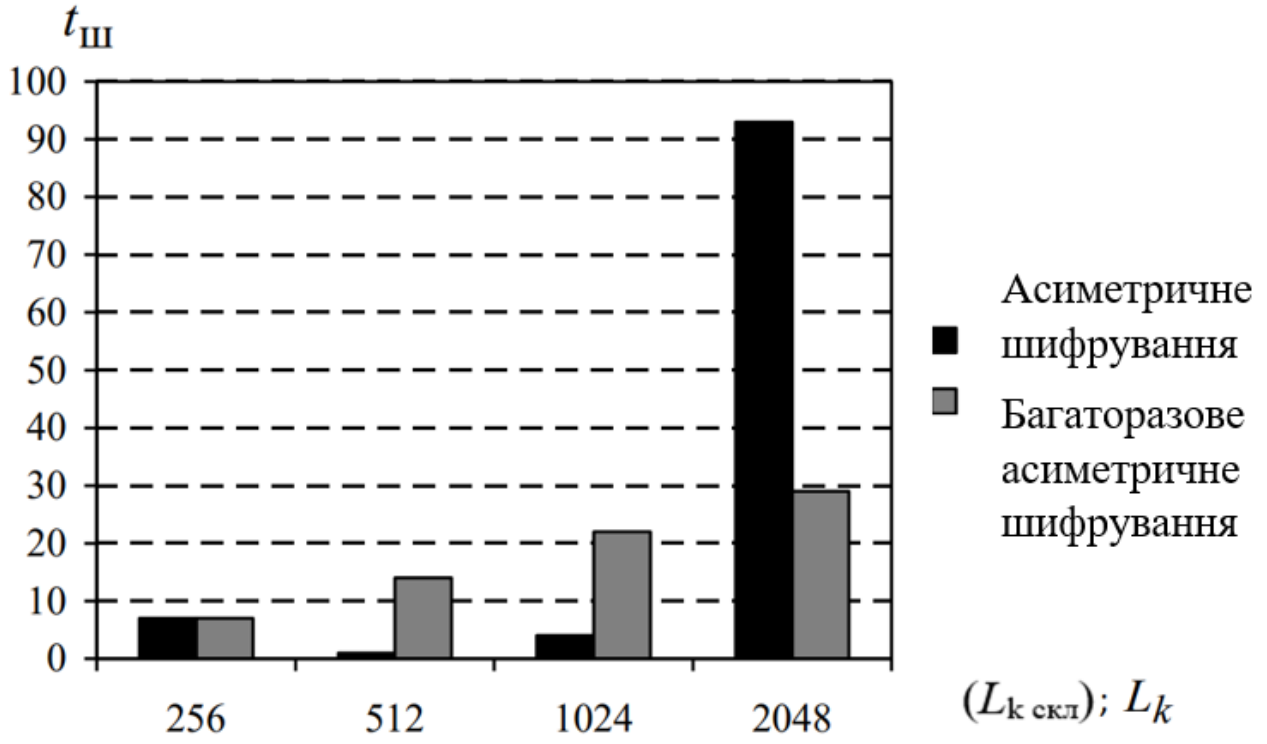


Рисунок 1.5 - Порівняння часу при асиметричному шифруванні та при багаторазовому асиметричному шифруванні

Реалізація паралельного передавання та оброблення інформації в точці приймання є одним із ефективних методів, що забезпечують надійність обчислювальних і телекомунікаційних систем. Цей підхід доцільно застосувати для забезпечення цілісності інформації з підтриманням відповідних показників QoS високошвидкісних додатків ММЗ, що функціонують у масштабі реального часу.

1.5 Терміни та визначення предметної області "Маршрутизація в мережах зв'язку"

Маршрут - список елементів мережі зв'язку (ліній зв'язку (ЛЗ), вузлів комутації (ВКЗ), каналів зв'язку (КЗ), трактів передавання повідомлень (ТПП), що починається з ВД передаваної інформації і закінчується в ВО.

Маршрутизація - набір процедур, що дають змогу визначити й установити оптимальний за заданими параметрами маршрут на мережі зв'язку між ВД та ВО.

У МВВС функції маршрутизації покладено на третій - мережевий рівень. Цей рівень зручно представити у вигляді підрівнів (Рисунок 3.1). На другому, верхньому підрівні проводиться моніторинг стану мережі зв'язку і формування таблиць маршрутизації (ТМ).

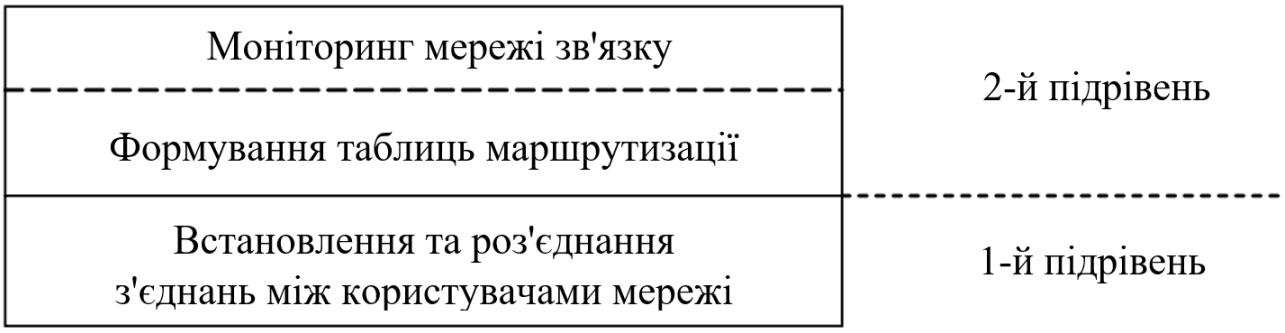


Рисунок 1.6 - Підрівні мережевого рівня моделі ВВС

Основне завдання моніторингу полягає у визначенні імовірнісно-часових характеристик (ІЧХ) елементів мережі зв'язку: швидкість передавання інформації; час затримки передавання інформації; надійність та інші. Ця інформація є підставою для визначення маршрутів із необхідними ІЧХ між усіма ВК аналізованої мережі зв'язку. Сформовані маршрути прописуються в ТМ у ранжированому порядку за переважністю вибору.

У процесі функціонування мережі зв'язку, сформовані ТМ, використовуються процедурами першого підрівня для встановлення з'єднань між користувачами.

Протоколи, що беруть участь у 2-му підрівні (формують ТМ), заведено називати протоколами маршрутизації.

Протоколи, що виконують функції встановлення і роз'єднання з'єднань, зазвичай називають протоколами сигналізації.

У сукупності протоколи 2-го і 1-го підрівнів є службовими протоколами, які забезпечують можливість передавання користувацької інформації з необхідною якістю обслуговування.

Зауважимо, що в системах телекомунікацій мережевий рівень МВВС може бути реалізований у двох варіантах:

– наявність тільки протоколів маршрутизації (тільки другий підрівень мережевого рівня МВВС);

– наявність протоколів маршрутизації та сигналізації (другий і перший підрівні мережевого рівня МВВС).

Кажуть, що в першому випадку в мережі зв'язку реалізується технологія комутації пакетів у режимі дейтаграм. Відомо, що ця технологія не підтримує QoS додатків, що функціонують у мережах зв'язку.

У другому випадку в мережі реалізується технологія комутація пакетів із попереднім встановленням з'єднань, яка гарантує QoS, що є необхідною умовою для мультисервісних мереж зв'язку. Тому надалі ми будемо аналізувати тільки другий варіант.

Користувач мережі, що викликає, через кінцеве обладнання ініціює пакет виклику на встановлення з'єднання з користувачем, що викликається. Пакет виклику містить таку інформацію:

– адреса ВД;

– адреса ВО;

– додаток ММЗ (телефонія, телебачення, відеоконференція тощо), що братиме участь під час передавання користувацької інформації (фактично визначаються вимоги до ІЧХ інформації, що передається, - час затримки, швидкість передавання інформації, вірогідність помилкового приймання на символ і так далі).

Система сигналізації:

– приймає цей пакет виклику;

– звертається до ТМ, які сформовані на другому підрівні (протоколами маршрутизації) для зазначеного в пакеті виклику додатка;

– обирає перший у ранжированому списку маршрут - визначає вихідні ТПП і наявність у них вільних каналів з необхідними ІЧХ;

– встановлює за обраним маршрутом з'єднання між заданими користувачами (за наявності вільних каналів з необхідними ІЧХ).

У результаті інформація встановленого з'єднання фіксується в таблицях комутації (ТК) відповідних ВК.

Фактично це означає, що ММЗ виділила необхідні ресурси (КЗ, ТПП) для цього виклику і готова для передавання користувацької інформації з необхідною якістю обслуговування обраного застосунку.

Якщо з якихось причин перший у ранжируваному списку маршрут недоступний, то обирається наступний за перевагою маршрут. І так доти, доки маршрут не буде реалізовано у вигляді з'єднання між парою користувачів. В іншому разі користувачеві буде дано відмову в обслуговуванні.

По завершенню передачі повідомлення інформація в ТК стирається. Це означає, що виділені ресурси (КЗ, ТПП) для передання користувацької інформації звільнилися і можуть бути використані мережею зв'язку для передання іншої інформації.

Для того, щоб була можливість визначати маршрути між будь-якою парою ВК, необхідно побудувати ТМ у кожному вузлі мережі.

Сукупність ТМ у всіх ВК мережі називається планом розподілу інформації (ПРІ) на мережі зв'язку. Вважається, що ПРІ на мережі задано, якщо визначено ТМ для кожного ВК.

На практиці таблиці маршрутизації можуть бути реалізовані у двох варіантах: покрокові ТМ; ТМ від джерела.

Спочатку (під час проектування або модифікації мережі зв'язку) ПРІ формується адміністрацією. Однак ІЧХ елементів мережі (надійність; час затримки передавання інформації; швидкість передавання інформації та інші) є випадковими функціями від часу *t* і залежать від багатьох причин:

– виду та інтенсивності користувацького трафіку в мережі;

– умов навколишнього середовища під час експлуатації обладнання мережі;

– технічного стану обладнання мережі;

– втручання третіх осіб (порушників) у процес функціонування телекомунікаційної системи та інших причин.

Тому в процесі експлуатації мереж зв'язку можуть виникнути ситуації, за яких необхідно скоригувати ТМ і тим самим переформувати ПРІ. Як правило, формування та корекція ТМ (дія протоколів маршрутизації) відбувається у фіксовані моменти часу t і з інтервалом Δt (рисунок 1.7). Причому Δt може бути як постійною, так і змінною величиною. Однак заявки на встановлення з'єднань надходять у мережу зв'язку в довільні моменти часу. Отже, інформація в ТМ принципово не може відображати реальну ситуацію,що склалася на мережі в момент установлення з'єднань. Тому процедура першого підрівня (дія протоколів сигналізації) призначена для уточнення вибору маршруту з відповідними ІЧХ і його реалізації у вигляді з'єднання.

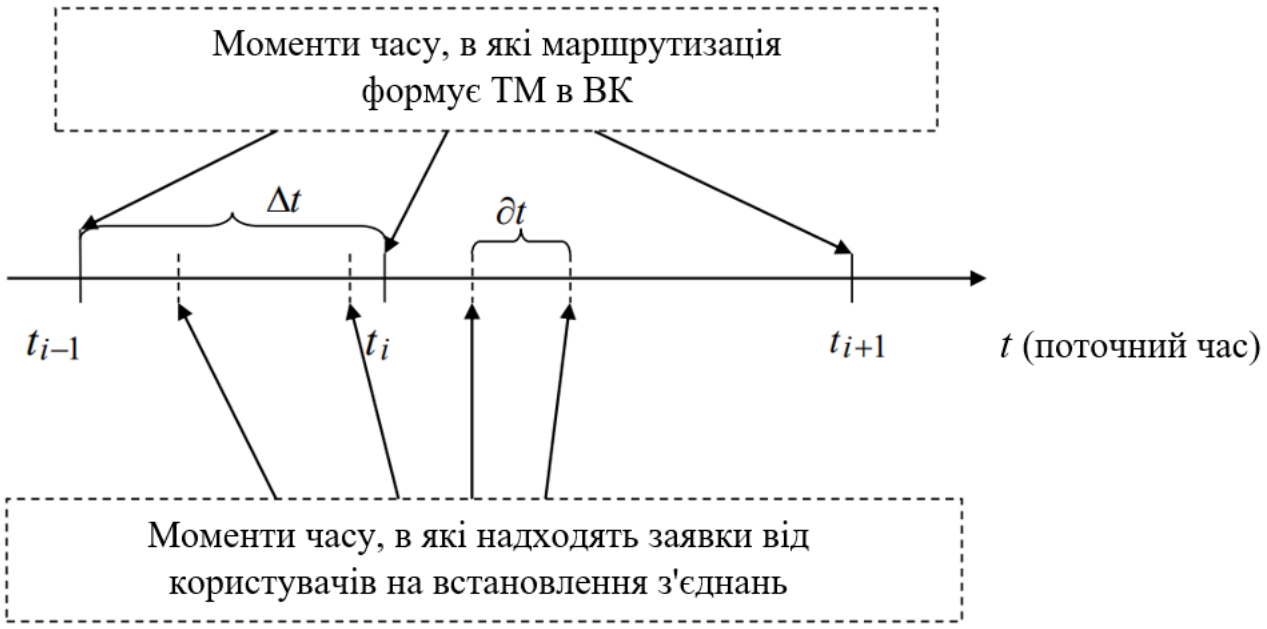


Рисунок 1.7 - Причини невідповідності інформації, що зберігається в ТМ, реальній ситуації в мережі на момент встановлення з'єднання

Якщо в процесі експлуатації мереж зв'язку відбувається автоматичне переформування ПРІ (без участі адміністрації мережі), то такий метод формування ПРІ називають динамічним. В іншому випадку метод формування ПРІ буде статичним.

Частота корекції ПРІ Δt залежить від багатьох факторів:

– використання статичних або динамічних методів маршрутизації;

– набору статистики (за певний період часу Т) про стан елементів мережі зв'язку (ІЧХ);

– ступеня централізації пристроїв управління мережею зв'язку (централізовані, децентралізовані або комбіновані методи управління);

– можливості адміністрації мережі зв'язку впливати на процес управління мережею зв'язку;

– наявність постійних (не комутованих) з'єднань між користувачами мережі зв'язку та інших факторів.

2 РОЗРОБЛЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ РЕСУРСІВ МУЛЬТИСЕРВІСНИХ МЕРЕЖ ЗВ'ЯЗКУ

2.1 Розробка методу забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку

Нехай у ММЗ між вузлом-джерелом (ВД) та вузлом-отримувачем (ВО) передається повідомлення, що являє собою собою бітовий потік $M = \{M_1, M_2\}$ з відповідними ймовірностями $P(M_1)$ і $P(M_2)$.

Повідомлення передається від ВД до ВО по n паралельних з'єднаннях через m транзитних вузлів (ТВ) у кожному з'єднанні (рисунок 2.1).

Нехай $P_м^{(i)}$ - імовірність модифікації повідомлення $M = \{M_1, M_2\}$ внаслідок атаки порушника у відповідному i-му з'єднанні $(i = \overline{1,n})$.

У цьому разі цілісність інформації досягається за рахунок ухвалення рішення в УО за n прийнятими символами $x = (x_1,\ldots,x_i,\ldots,x_n)$. У результаті, значення M^* на виході вирішувального пристрою (ВП) відповідатиме переданому значенню M_1 або M_2.

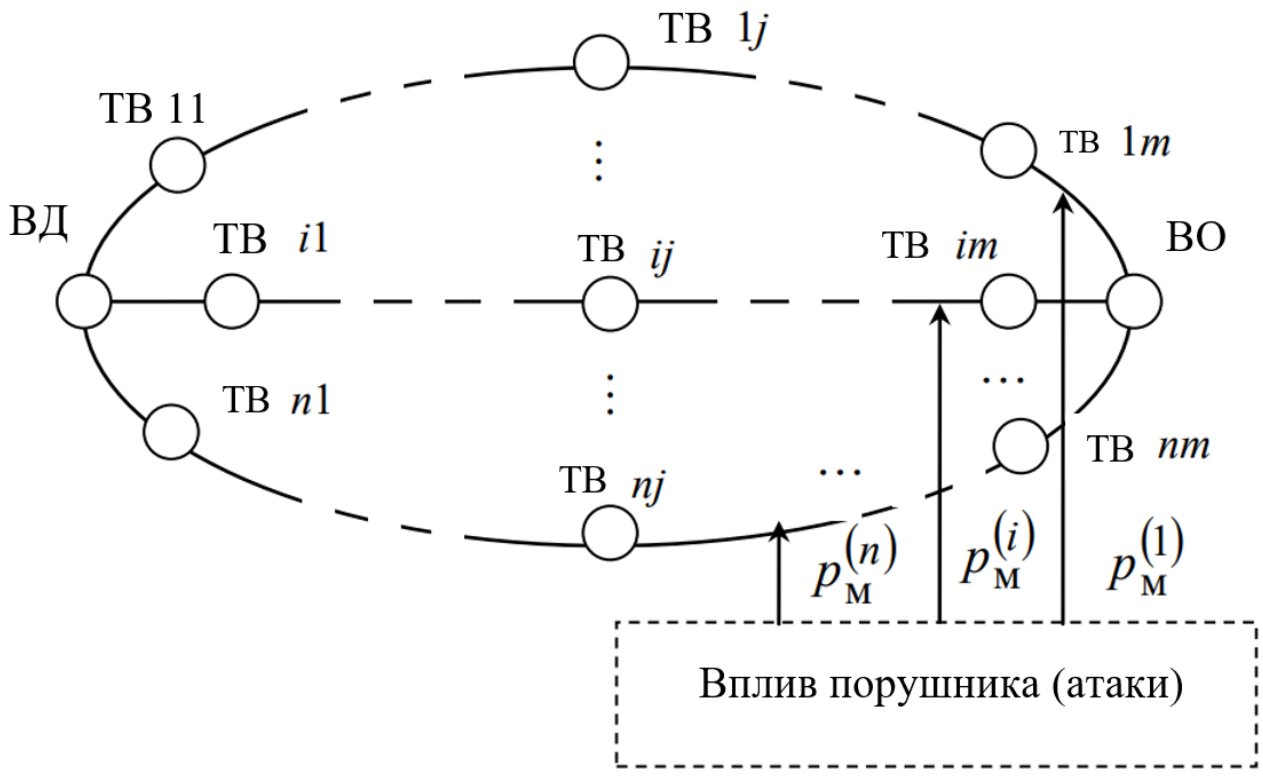


Рисунок 2.1 - Організація паралельних з'єднань

Введемо такі обмеження:

– ймовірності модифікації $M = \{M_1, M_2\}$ по всіх з'єднаннях між ВД та ВО рівні, тобто $P_м = P_м^{(i)}; i = \overline{1,n}$ (Рисунок 2.4) і незалежні;

– кількість паралельних з'єднань n між ВД та ВО непарна і $n \geq 3$.

Тоді ймовірність цілісності інформації визначається виразом:

$$P_{цВП} = 1 - \sum_{i=0}^{(n-1)/2} C_n^{(n+1+2*i)/2} * (1 - P_м)^{(n-1-2*i)/2} * P_м^{(n+1+2*i)/2}, \quad (2.1)$$

де $C_n^{(n+1+2*i)/2}$ - число поєднань $(n+1+2*i)/2$ з n.

На рисунку 2.2 наведено результати оцінки цілісності інформації, розраховані за формулою (2.1).

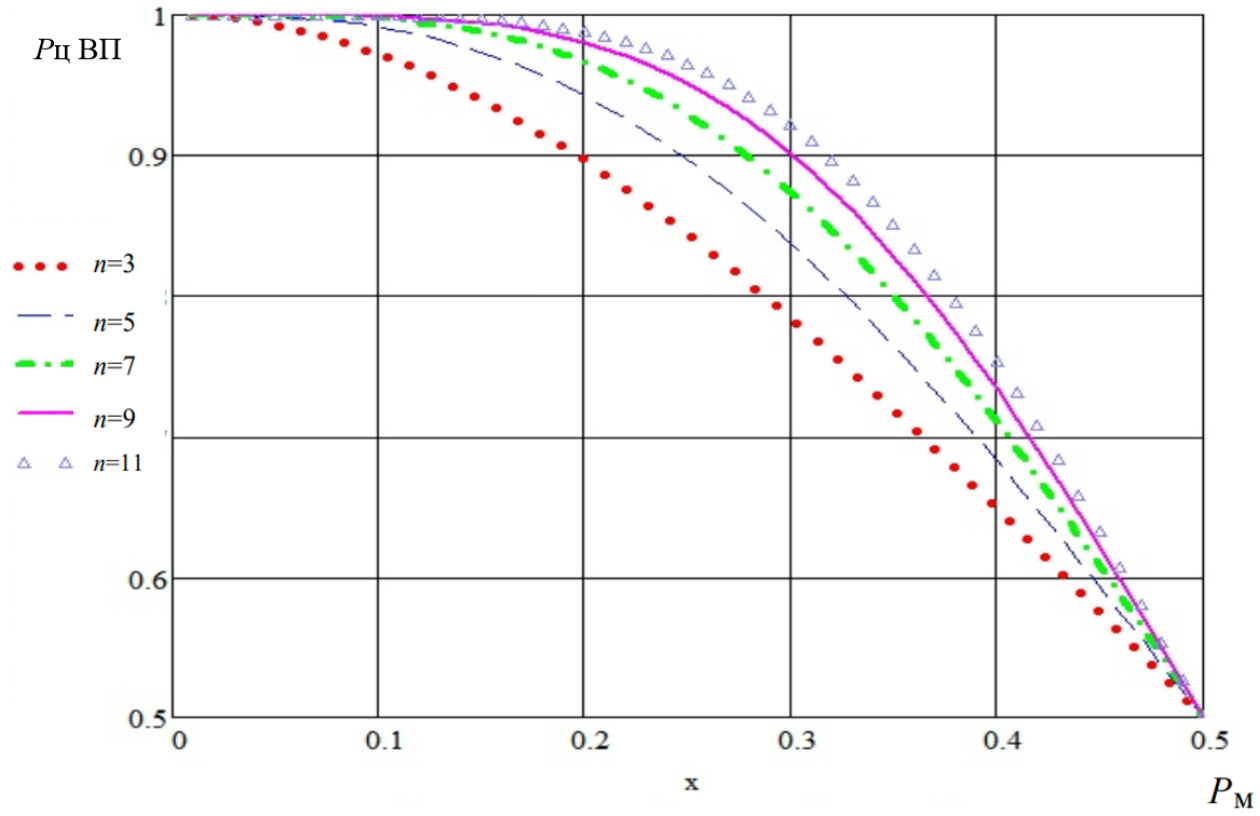


Рисунок 2.2 - Результати теоретичного розрахунку $P_{ц\,ВП} = f(P_м)$ для різних значень n

2.2 Імітаційне моделювання забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку

Апробація функціонування ВП на діючій мережі зв'язку пов'язана з фінансовими, організаційними та часовими витратами. У зв'язку з цим для підтвердження теоретичних результатів оцінювання ймовірності цілісності інформації на виході ВП скористаємося методом статистичного моделювання, суть якого зводиться до такого (рисунок 2.3).

Вихідними даними алгоритму моделювання є:

- $P(M_1)$; $P(M_2)$ - апріорні ймовірності появи $M = \{M_1, M_2\}$ на виході ВД, за умови $P(M_1)+P(M_2)=1$;

- n - кількість з'єднань між ВД та ВО;

- $P_{м}^{(i)}; i = \overline{1,n}$ ймовірності модифікації бітового потоку $M = \{M_1, M_2\}$ в кожному з n з'єднань між ВД та ВО;

- N_o - кількість переданих значень $M = \{M_1, M_2\}$ між ВД та ВО (кількість незалежних випробувань при статистичному моделюванні).

2.3 Розроблення критерію вибору ресурсів мультисервісних мереж зв'язку для забезпечення цілісності та доступності інформації

Резервування каналів зв'язку і дублювання самої інформації є базовими методами забезпечення доступності інформації ТКС. Стосовно ММЗ цей підхід реалізується за рахунок організації паралельних з'єднань між ВД та ВО (рисунок 2.1). У цьому разі необхідно визначити критерій вибору з'єднань між ВД та ВО, що забезпечує необхідний рівень доступності або цілісності інформації користувача.

Уведемо такі позначення. Нехай: c_i - вартість i-ого з'єднання між ВД та ВО (рисунок 2.1), що бере участь у забезпеченні доступності або цілісності інформації; p_i - імовірність забезпечення доступності або цілісності i-го з'єднання ($i = \overline{1,n}$).

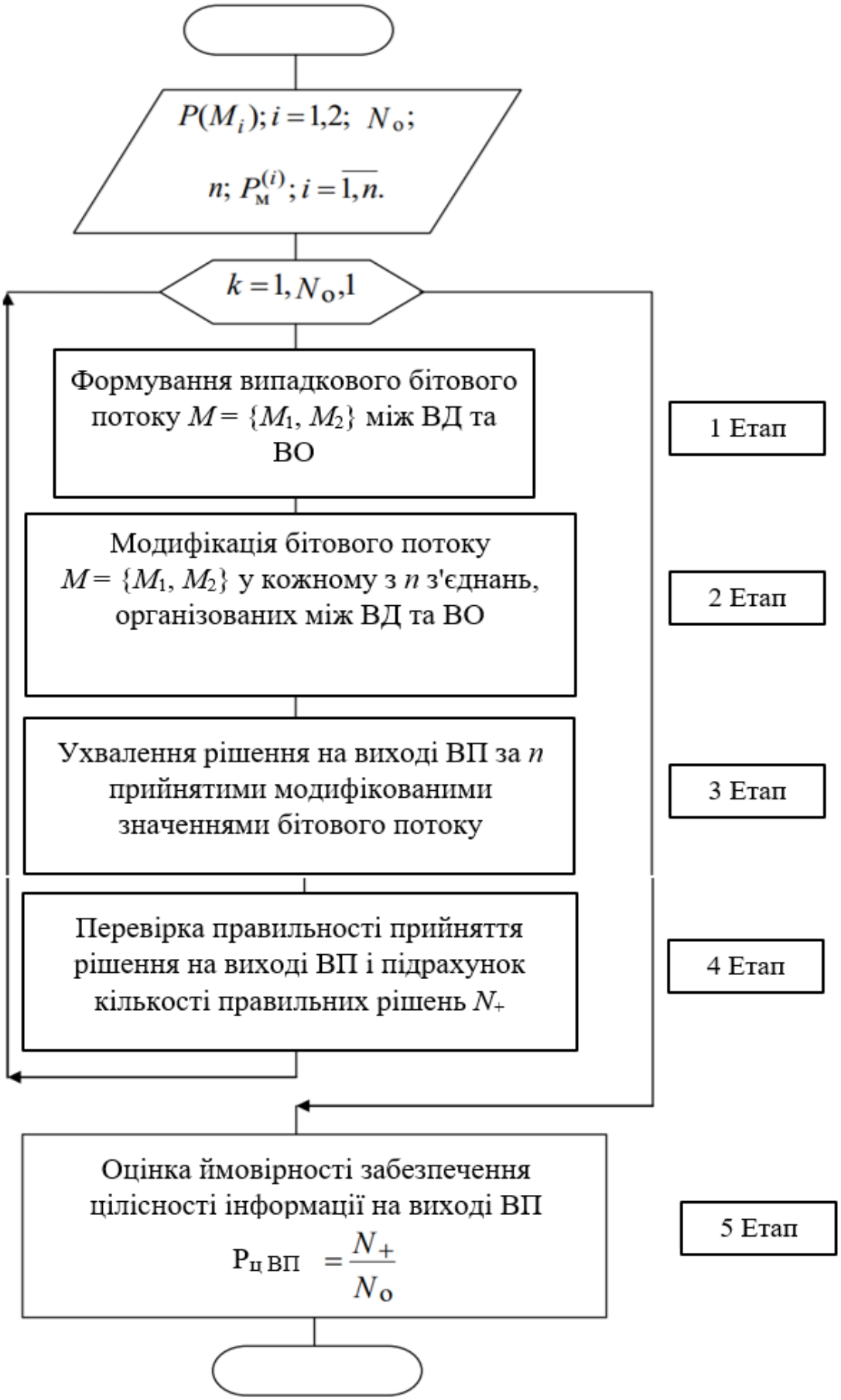


Рисунок 2.3 - Основні етапи оцінки цілісності інформації на виході ВП методом статистичного моделювання

Тоді загальна вартість організації *n* паралельних з'єднань становитиме:

$$C_o = \sum_{i=1}^{n} c_i. \qquad (2.2)$$

Нехай впливи порушників на кожне з'єднання є незалежними подіями. У цьому разі результуючу (загальну) ймовірність забезпечення доступності або цілісності інформації можна визначити:

$$P_{рез} = 1 - \prod_{i=1}^{n} (1 - p_i). \qquad (2.3)$$

Введемо позначення:

$$Q_{рез} = 1 - P_{рез}; q_i = 1 - p_i; i = \overline{1, n.}$$

Припустимо, що всі *n* з'єднань (рисунок 2.1) однакові за вартістю та ймовірністю забезпечення доступності або цілісності інформації.

Тоді:

$$C_o = n * c_i; i = \overline{1, n;} \qquad (2.4)$$

$$Q_{рез} = q_i^n; i = \overline{1, n.} \qquad (2.5)$$

Прологарифмуємо вираз (2.5):

$$\ln Q_{рез} = n * \ln q_i; i = \overline{1, n.}$$

і розділимо на (2.4). У результаті отримаємо:

$$\frac{\ln Q_{рез}}{C_o} = \frac{\ln q_i}{c_i}; i = \overline{1, n.}$$

Враховуючи, що

$$\frac{\ln Q_{рез}}{C_o} = \frac{\ln q_i}{c_i} \le 0; i = \overline{1, n,}$$

то приймемо:

$$\left|\frac{\ln Q_{рез}}{C_o}\right| = \left|\frac{\ln q_i}{c_i}\right|; i = \overline{1, n.} \qquad (2.6)$$

Із (2.6) випливає висновок. Для забезпечення доступності або цілісності інформації за рахунок організації n паралельних незалежних з'єднань між ВД і ВО необхідно вибирати ті з'єднання, у яких відношення

При організації *n* паралельних з'єднань між ВД і ВО необхідно вибирати ті маршрути, у яких:

$$\max\left\{a_i = \left|\frac{\ln(1-p_i)}{c_i}\right|; i = \overline{1, n}\right\}. \qquad (2.7)$$

Отже, багаторазове асиметричне шифрування з ключами меншої довжини забезпечить конфіденційність інформації за меншого часу її шифрування.

Паралельні з'єднання між вузлом-джерелом та вузлом-одержувачем, які враховують імовірнісно-вартісні параметри, дають змогу за сукупності прийнятих символів паралельно передану інформацію відновити, забезпечити тим самим її цілісність та зменшити час затримки передавання інформації (порівняно з відомими методами, що використовують контроль модифікації для переданої інформації та запит на її повторне передавання).

Формування незалежних паралельних з'єднань відповідно критерію при виборі мережевих ресурсів, який враховує імовірнісно-вартісні параметри при з'єднанні, забезпечує доступність та цілісність інформації у мультисервісних мережах зв'язку.

Застосування методу інформаційного резервування та резервування елементів інфраструктури дає змогу забезпечити захист інформації із QoS.

Процедури, що беруть участь в моніторингу інфраструктури мультисервісної мережі зв'язку, виборі оптимального маршруту і встановленні з'єднань, дають змогу не тільки забезпечити QoS-додатки, а й необхідний рівень для інформаційної безпеки.

У зв'язку із цим виникає необхідність у розробленні, дослідженні нових методів для маршрутизації, здатних розв'язувати задачі захисту інформації із підтримкою QoS додатків для мультисервісної мережі зв'язку.

2.4 Розроблення узагальненої функціональної моделі маршрутизації в мультисервісних мережах зв'язку

Аналіз вищевикладеного матеріалу дає змогу виробити узагальнену функціональну модель маршрутизації в ММЗ ,яка зображена на рисунку 2.4.

Узагальнена модель маршрутизації в ММЗ містить два рівні:

– рівень формування ПРІ виконує функції формування та корекції баз даних (БД) про стан елементів мережі;

– рівень сигналізації виконує функції виділення та резервування ресурсів мережі для кожної заявки викликів.

Основним продуктом рівня формування ПРІ є ТМ для кожного додатка ММЗ $\varepsilon = \overline{1, E}$. При цьому застосовуються відповідні методи формування та корекції баз даних (БД), які за ступенем централізації можна класифікувати на централізовані, розподілені та комбіновані.

Рівень сигналізації, використовуючи методи вибору вихідних ТПП, за сформованими ТМ формує в усіх транзитних ВО, починаючи з ВД:

– таблиці комутації для кожної заявки на встановлення з'єднання з необхідними ІЧХ;

– структуру з'єднань захисту з метою виконання вимог користувачів до ступеня захищеності переданої інформації.

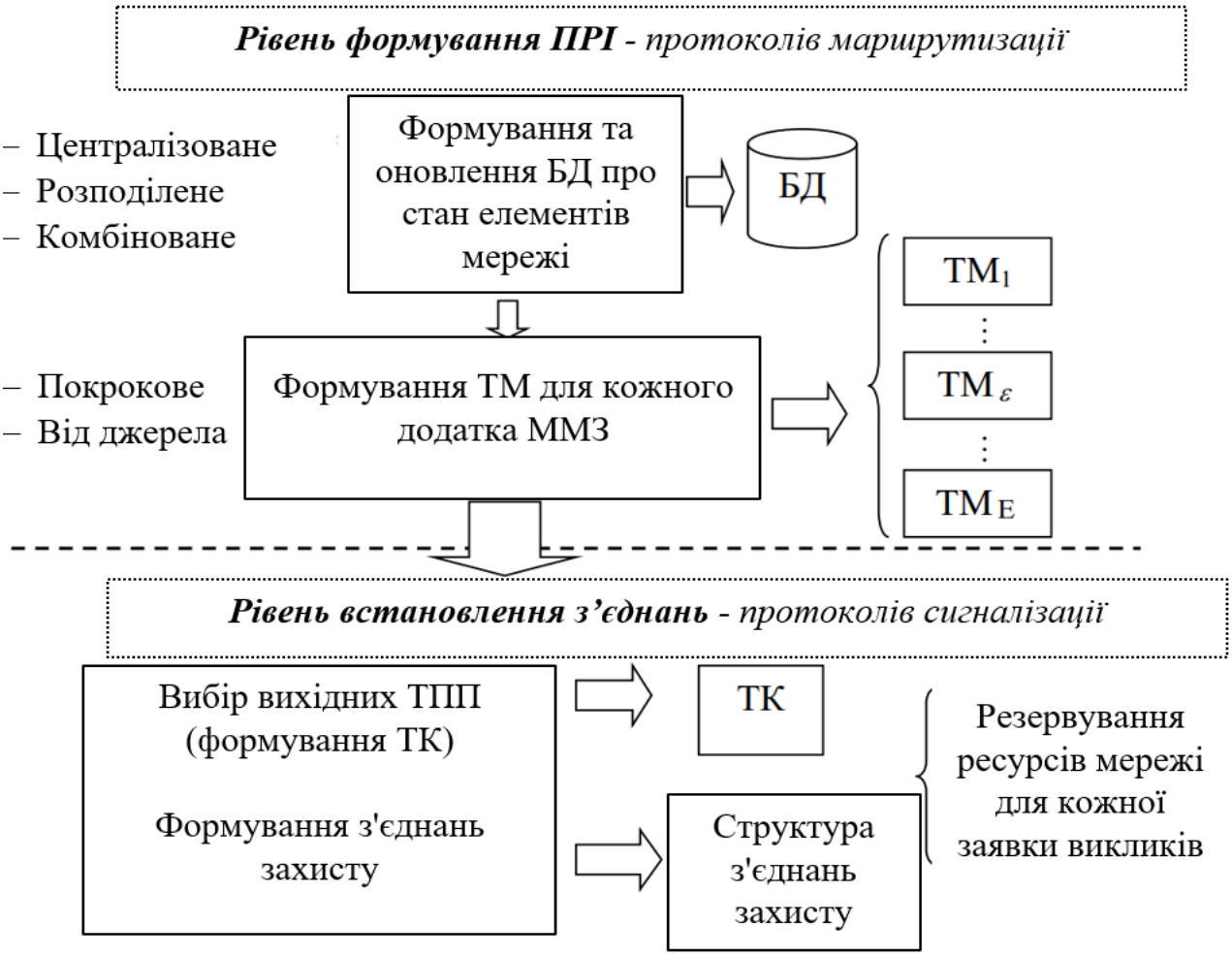


Рисунок 2.4 - Узагальнена функціональна модель маршрутизації в ММЗ

Передача повідомлень користувачів здійснюється за встановленими з'єднаннями, відповідно до таблиць комутації.

2.5 Методи формування плану розподілу інформації в мультисервісних мережах зв'язку

"Лавинний" метод формування ПРІ на мережі полягає в такому. В кожному ВК через певний час Δt =constant генеруються зонд-сигнали, які пересилаються

до всіх суміжних вузлів. У суміжних ВК ця процедура повторюється. Таким чином, зонд-сигнали потрапляють в усі вузли мережі. У міру просування мережею зонд-сигнали аналізують ІЧХ усіх елементів мережі (ВК, ЛЗ, ТПП, КЗ тощо). Після закінчення зондування мережі сигнали повертаються у вихідні ВК. Зібрана інформація про ІЧХ елементів мережі записується в бази даних ВК, аналізується і використовується для розрахунку ТМ.

Основним недоліком "Лавинного" методу формування ПРІ є необхідність виділення певного ресурсу мережі (КЗ, ТПП) для передавання зонд-сигналів.

"Лавинний" метод реалізовано в технології АТМ і IP усіх версій, а саме: PNNI (Private Network - to - Network Interface), RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Extended IGRP), IS-IS (Intermediate System - to - Intermediate System), OSPF (Open Shortest Path First).

"Статистичний", або "Ігровий" метод передбачає формування ПРІ за накопиченою статистикою встановлення з'єднання між заданою парою ВК.

У процесі експлуатації мережі формується (коригується) оптимальний ПРІ зі змінним інтервалом $\Delta t = \partial t$ (рисунок 1.7). Критерієм оптимальності в цьому разі є результат організації маршрутів у попередні моменти часу.

Якщо розглядати вагові коефіцієнти $p_{iv}^{(j)}$ як імовірності вибору відповідних вихідних ТПП $m_{iv}^{(j)}$, то можна припустити, що "Статистичний" метод формування ПРІ має ітеративний характер і розв'язує задачу глобальної оптимізації ПРІ на мережі зв'язку за критерієм - вірогідність установлення з'єднання між парами ВО та ВД.

Необхідність передачі мінімальної кількості службової інформації для формування ПРІ на мережі є безсумнівною перевагою "Статистичного" методу. Однак цей метод має інерційність. Дійсно, у разі виходу елементів мережі зв'язку з ладу знадобиться певний період часу для переформування ПРІ на мережі.

Іншим недоліком "Статистичного" методу є невизначеність вибору початкового ПРІ в разі введення нових ВК в експлуатацію.

Зазначимо, що цей метод було реалізовано в технології MPLS.

"Логічний" метод формування ПРІ на мережі зв'язку полягає в процедурі, яку виконують у кожному транзитному ВК, починаючи з ВД, і яка дає змогу визначити вихідний ТПП, максимально близький до геометричного напрямку на ВО. Для цього мережа зв'язку вкладається в систему координат (наприклад, у прямокутну). Кожному вузлу мережі відповідно до системи координат *(X, Y)* присвоюється власна адреса (рисунок 2.5).

У кожному транзитному ВК (X_i,Yj), починаючи з ВД (X_R,Y_L), проводиться аналіз адреси ВО зіставленням її з власною. У результаті обчислюється геометричний напрямок з даного вузла на ВО. Потім визначається той вихідний ТПП, який має найбільший збіг з раніше розрахованим геометричним напрямком на ВО. Якщо найближчий за напрямком ТПП недоступний, то підбирається черговий за перевагою вихідний ТПП.

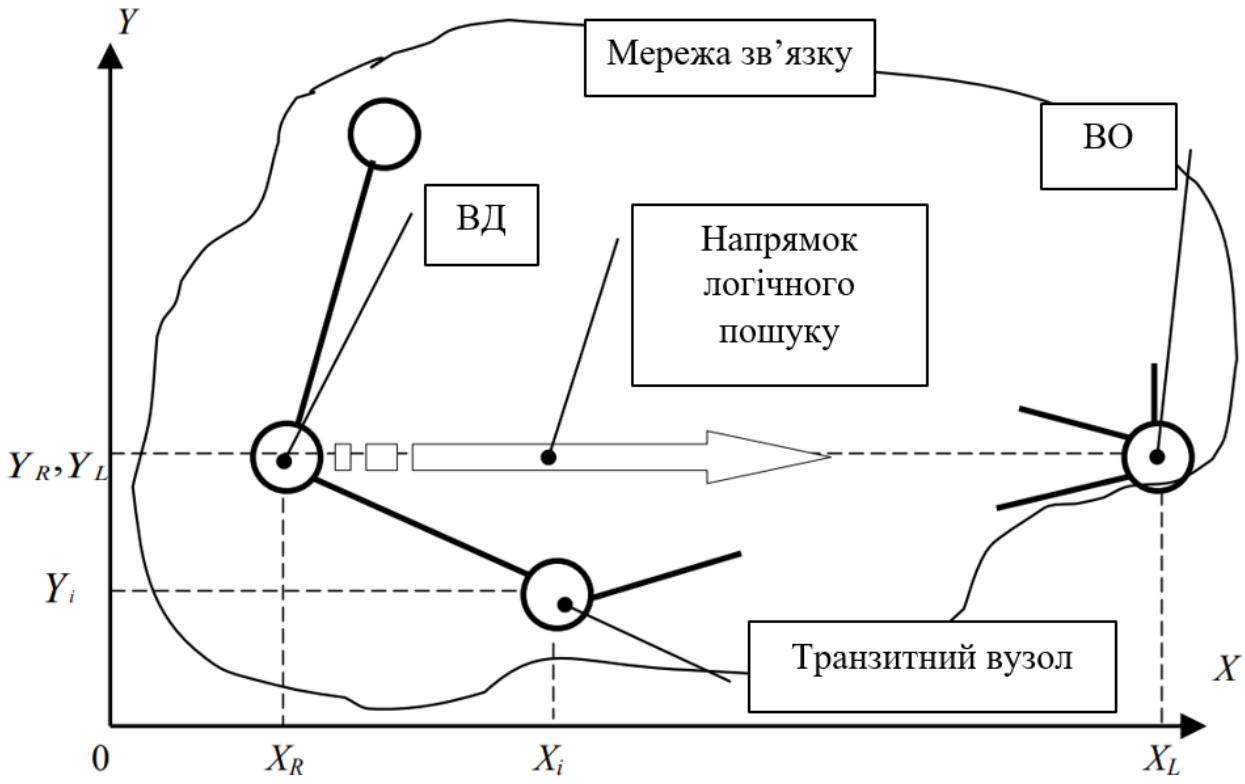


Рисунок 2.5 - Пошук маршруту "Логічним" методом

Безсумнівною перевагою цього методу є простота і відсутність необхідності передавання службової інформації мережею. Застосування простого алгоритму обчислення вихідного ТПП у кожному ВК дає змогу

відмовитися від ТМ, що значно скорочує об'єм оперативної пам'яті ВК, спрощує процедуру маршрутизації та введення в експлуатацію нових вузлів. Водночас цей метод не є динамічним і не розв'язує завдання глобальної оптимізації ПРІ.

2.6 Методи вибору вихідних трактів у вузлах комутації мультисервісних мереж зв'язку

Залежно від кількості одночасно встановлюваних маршрутів між ВД та ВО розрізняють послідовний або паралельний (багатошляховий) вибір вихідних ТПП.

Послідовний вибір вихідних ТПП полягає в тому, що в кожному ВК, починаючи з ВД, здійснюється вибір тільки одного вихідного ТПП. В результаті на мережі формуватиметься один маршрут, що складається з послідовного нарощування комутаційних ділянок з ВО до ВД.

Відмітна особливість алгоритмів із паралельним вибором вихідних ТПП полягає в тому, що пошук маршруту між ВО та ВД здійснюється одночасно за всіма вихідними ТПП у певній зоні мережі зв'язку.

Залежно від характеру поширення на мережі процесу пошуку маршруту виокремимо три основні класи послідовних алгоритмів вибору вихідних ТПП: градієнтний, дифузний і градієнтно-дифузний.

Градієнтний полягає в тому, що в кожному транзитному вузлі, починаючи з ВК, у процесі вибору вихідного ТПП беруть участь не всі вихідні ТПП, а лише частина (найкращі). Якщо в одному з ВК вихідні ТПП, що беруть участь у виборі, не доступні, то цій заявці на формування маршруту дається відмова.

У результаті градієнтного вибору маршрут формуватиметься вздовж геометричного напрямку з ВО на ВД (рисунок 2.6).

Збільшення кількості вихідних ТПП, що беруть участь у виборі, призведе до можливого відхилення маршруту від геометричного напряму з ВО на ВД, зокрема й у бік протилежний від ВО.

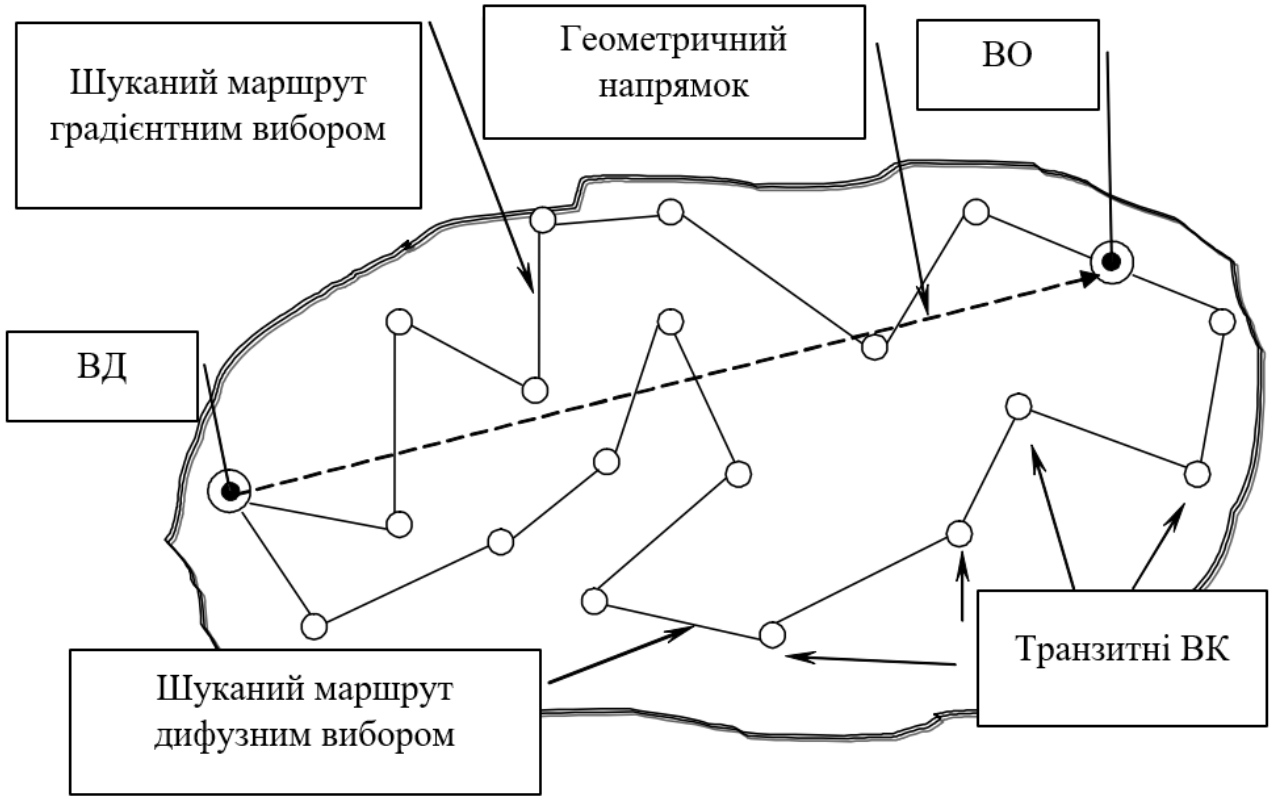


Рисунок 2.6 - Градієнтний і дифузний вибір вихідних ТПП

Вибір ТПП, за якого шуканий маршрут формується і в протилежний бік від ВО, називатимемо дифузним.

Таким чином, дифузний вибір вихідних ТПП допускає можливість вибору будь-якого доступного вихідного ТПП.

Градієнтно-дифузний метод є комбінацією перших двох.

Реалізація градієнтних алгоритмів вибору вихідних ТПП дає змогу організувати найкоротші маршрути (за кількістю транзитних ВК).

Дифузні володіють великою гнучкістю при обходах пошкоджених ділянок мережі, проте середня довжина маршруту в рівних з градієнтним умовах буде більшою.

Своєю чергою процедура вибору вихідного ТПП у кожному ВК може бути детермінованою та стохастичною. У першому випадку вибір вихідного ТПП здійснюється однозначно за максимальним значенням одного з елементів вектора. У другому випадку вибір вихідного ТПП здійснюється в результаті

випадкового розіграшу. При цьому вихідні ТПП, що мають великі значення $m_{iv}^{(j)}$, отримують більшу ймовірність вибору.

Можливий і комбінований спосіб вибору вихідних ТПП, який містить як імовірнісну, так і детерміновану компоненти.

З огляду на перелічені градації, можна вказати безліч варіантів послідовних алгоритмів вибору вихідних ТПП в ВК (наприклад, "Дифузний імовірнісний" або "Градієнтно-дифузний детермінований").

2.7 "Логіко-статистичний" метод формування плану розподілу інформації

"Логіко-статистичний" метод для формування ПРІ є узагальненням "Логічного" і "Статистичного". Цей метод увібрав у себе позитивні властивості двох методів:

– відсутність необхідності передавання службової інформації в мережі під час формування (під час уведення ВК у експлуатацію) і переформування (в процесі експлуатації ВК) ТМ;

– розв'язання задачі для глобальної оптимізації ПРІ в мережі зв'язку за накопиченою статистикою встановлення з'єднання між заданою парою ВК.

Суть "Логіко-статистичного" методу формування ПРІ зводиться до такого. За аналогією з "Логічним" методом мережа зв'язку вкладається у прямокутну систему координат, відповідно до якої кожному вузлу мережі присвоюється власна адреса *(X, Y)*. У кожному *j*-му ВК є розширена матриця:

$$p'^{(j)} = \left\| p'^{(j)}_{i,v} \right\|_{(S^{(j)}-1),(X_j+3);} v = \overline{1, X_j}; i, j = \overline{1, S}; i \neq j, \qquad (2.8)$$

яка містить (S - 1) рядків і (X_j + 3) стовпці. Один стовпець відводиться для номерів ВО, представлених у загальновизнаній нумерації (№ ВО), і два стовпці для номерів у прямокутній системі координат (*X, Y*).

На момент уведення вузла в експлуатацію матриця містить тільки інформацію про суміжні номери ВК з даними, виражену в прямокутній системі координат.

У міру функціонування мережі зв'язку матриця $p'^{(j)}$ коригується, заповнюється і Визначення вихідних ТПП здійснюється "Логічним" методом, а заповнення і коригування матриці $p'^{(j)}$ методом здійснюється "Статистичним"

Тим самим під час формування (під час введення в експлуатацію ВК) та переформування (в процесі експлуатації ВК) ТМ відпадає необхідність передавання службової інформації мережею. Накопичення інформації в ТМ про формування маршрутів дає змогу розв'язати задачу глобальної оптимізації ПРІ на мережі зв'язку.

2.8 "Локально-хвильовий" метод маршрутизації

Розглянемо "Локально-хвильовий" метод, який є узагальненням "Лавинного" і "Логічного" методів формування плану розподілу інформації на мережі зв'язку. "Локально-хвильовий" метод маршрутизації залежно від організації вибору вихідного ТПП може бути віднесено до паралельних (багатоколійних) і до паралельно-послідовних (комбінованих) методів. Водночас спосіб вибору зони, в якій здійснюється пошук маршруту, у "Локально-хвильовому" методі може бути ймовірнісним, детермінованим і комбінованим.

"Локально-хвильовий" метод маршрутизації полягає в тому, що для знаходження оптимального маршруту в мережі між парою вузлів з вузла-джерела організовується "Лавинний" пошук, але не в усіх напрямках, а лише в бік вузла-одержувача. Хвиля пошуку поширюється в деякій зоні у вигляді смуги, що охоплює пару з'єднуваних вузлів (рисунок 2.7). Ширина і форма смуги залежно від пріоритету користувача, стану елементів мережі (ВК, ТПП) і вимог додатків ММЗ до якості обслуговування може встановлюватися в різних межах. На рисунку 2.7 показано "Локально-хвильовий" пошук на мережі від ВД до ВО у деякий момент часу, що відповідає приблизно половині шляху між парою

вузлів. З малюнка видно, що пошукова хвиля - це рухома вузька зона, усі вузли в межах якої охоплені процесом "Лавинного" пошуку.

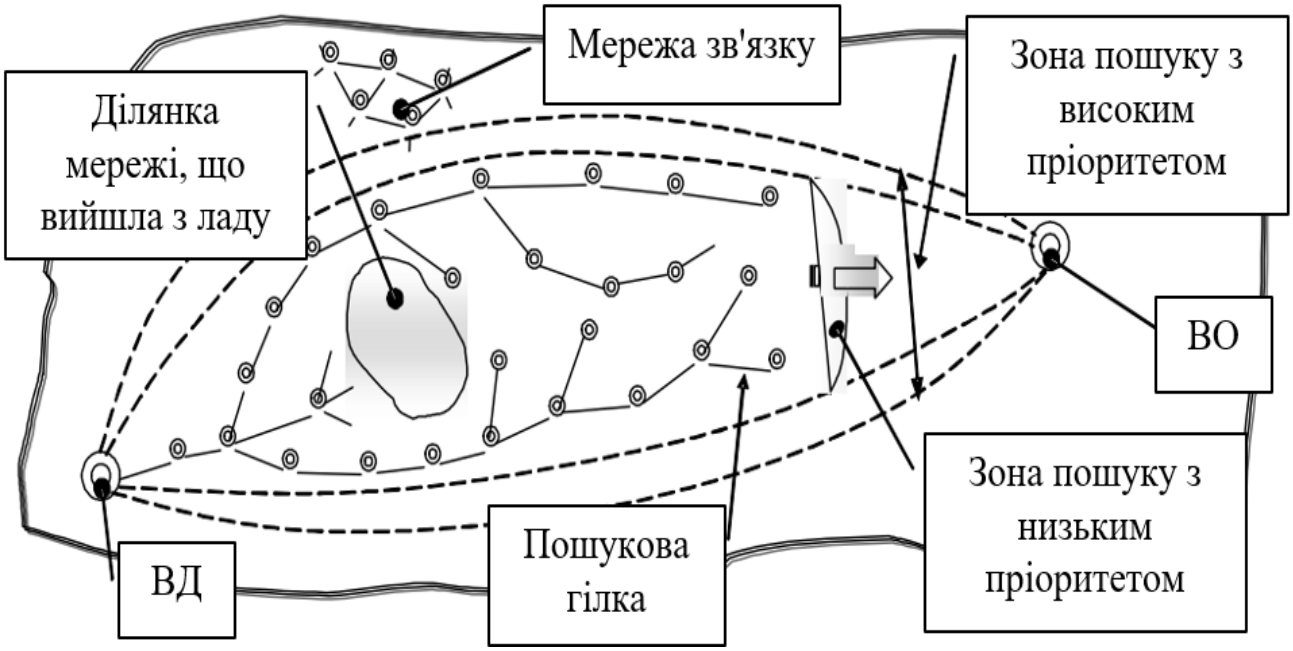


Рисунок 2.7 - Пошук маршруту "Локально-хвильовим" методом

Що вищий пріоритет користувача або вимоги додатків ММЗ до якості обслуговування (QoS), то більше можливостей є для встановлення з'єднання. Таким чином, за "Локально-хвильового" методу в кожному вузлі визначають вихідні з цього вузла ТПП до суміжних ВК, які найближче збігаються з геометричним напрямком на шуканий вузол. Обрані вихідні ТПП розташовуються в ряд за ступенем переважності. При цьому в поняття переважності може вкладатися не тільки ступінь близькості до зазначеного напрямку на ВО, а також ІЧХ елементів мережі зв'язку.

Кількість приєднаних ТПП, а отже, і ширина пошукової хвилі визначаються пріоритетом користувача, що викликає, або вимогами додатків ММЗ до якості обслуговування (QoS).

Для користувачів нижчої категорії кількість обраних трактів передавання повідомлень може не перевищувати одного, тоді пошук перетворюється на послідовний.

Для користувачів вищих пріоритетів пошуки можуть відрізнятися не тільки шириною хвилі пошуку, а й комбінуванням послідовного пошуку з розщепленням на "Локально-хвильовий" у тих вузлах, де послідовний пошук зустрічає перешкоду.

Для організації в мережі "Локально-хвильового" методу маршрутизації необхідно забезпечити виконання таких вимог.

У хвилі пошуку мають бути виключені замкнуті петлі, тобто один і той самий вузол комутації не повинен підключатися до процесу пошуку більше одного разу.

В області пошуку не повинно бути неохоплених хвилею вузлів, крім тих, які повністю завантажені або вийшли з ладу.

У разі зайнятості ВО, неможливості доступу до нього або його пошкодження поширення хвилі пошуку повинно бути призупинено, а всі обрані хвилею ТПП повинні саморозпастися.

Доступ до ВО має бути забезпечений з усіх ТПП, що входять до нього.

Усередині області, охопленої пошуковою хвилею, окремі тупикові маршрути повинні саморозпастися ще до завершення процесу пошуку.

Набрані таким чином маршрути (маршрут) фіксуються на весь час сеансу передання користувацької інформації між заданою парою вузлів комутації. Після закінчення сеансу передачі користувацької інформації маршрути (маршрут) розпадаються.

Організація "Локально-хвильового" методу маршрутизації може бути такою. Адресація вузлів комутації на мережі допускається довільною, що забезпечує, однак, єдиність номера кожного вузла комутації. У запам'ятовуючому пристрої блока керування кожного ВК міститься ТМ, число рядків якої дорівнює (S-1). Таблиця запам'ятовується до моменту запуску в роботу даного вузла.

Таблиця може заповнюватися і коригуватися в міру розширення мережі і появи нових вузлів комутації, ТПП, зміни режиму роботи вузла, зміни адрес і пріоритетів.

Для цього ВК у *Т*-му рядку таблиці міститься така інформація.

1) перелік вихідних з даного вузла трактів передачі повідомлень, що починається з найбільш близького до геометричного напрямку на ВО і далі в спадному порядку;

2) перелік тих вихідних ТПП, за якими має поширюватися в середовище хвиля пошуку з цього вузла до ВО для кожного з прийнятих у мережі визначених пріоритетів. Чим вищий пріоритет, тим більшою буде кількість можливих вихідних ТПП одночасно, які братимуть участь у поширенні хвилі пошуку;

3) час існування цього пошуку, що побічно відображає відстань між цим вузлом і ВО. Для вищих пріоритетів час пошуку може бути збільшено;

4) далі розглядатиметься тільки процес встановлення з'єднання між ВД і ВО у мережі. Процедура підключення користувача, що викликає, тут не розглядається. Передбачається, що користувач, який викликає, отримавши доступ до мережі, передав, а ВД прийняв і зафіксував адресу ВО і пріоритет користувача, який викликає;

5) процес організації в мережі "Локально-хвильового" пошуку маршруту ініціюється ВД. У ВД при цьому формується пошукова посилка, до складу якої входять:

– номер вузла одержувача;

– номер вузла джерела та індекс, що відрізняє цей пошук від інших, які одночасно виходять з одного і того ж ВД;

– пріоритет пошуку;

– абсолютний час, до якого дозволяється існування цього пошуку;

6) пошукова посилка в ВД піддається відповідному аналізу - визначаються з урахуванням визначеного пріоритету ті ТПП, якими має поширюватися в середовище ця хвиля пошуку. Якщо в цих ТПП є якісь вільні канали, то тоді вони резервуються цим пошуком. Цими ж каналами (або спеціально виділеними службовими каналами) на суміжні ВК передається

пошукова посилка. В усіх суміжних вузлах системи ця посилка піддається такому ж самому аналізу, і тоді також резервуються відповідні вільні канали в обраних ТПП. На всіх наступних ВК процес повторюється аналогічно описаному.

3 РОЗРОБЛЕННЯ МЕТОДИК ЗАХИСТУ ІНФОРМАЦІЇ ЗА РАХУНОК МЕРЕЖЕВИХ РЕСУРСІВ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

3.1 "Гібридний" метод маршрутизації

Розроблені в попередніх розділах методи забезпечення базових параметрів захисту інформації (конфіденційність, доступність і цілісність), а також паралельні (багатошляхові) методи маршрутизації і проведені дослідження методів маршрутизації в мультисервісних мережах зв'язку в умовах зовнішніх деструктивних впливів дають змогу виробити методики захисту інформації завдяки залученню територіально-розподілених ресурсів у мультисервісних мережах зв'язку (каналів зв'язку, криптографічних програмно-апаратних комплексів, баз даних тощо). Метою цих методик є захистити інформацію під час її передавання ММЗ.

Користувачеві з боку ММЗ (оператора ММЗ) надають не тільки вибір додатка (відео, телефонія, телеметрія, відеоконференція тощо) для передавання інформації, а й тарифний план, що забезпечує захист інформації. Тарифний план може бути представлений у декількох варіантах, наприклад у вигляді:

– кількісних оцінок параметрів інформаційної безпеки (ймовірності забезпечення цілісності, доступності та конфіденційності);

– якісних параметрів інформаційної безпеки ("Високий","Низький" або "Середній" ступінь захищеності).

Користувач визначає свій профіль захисту інформації для обраного додатка. Система управління, провівши моніторинг вільних ресурсів мультисервісної мережі зв'язку, реалізує не тільки з'єднання, що підтримує QoS для обраного додатка, а й заявлений користувачем профіль у вигляді структури з'єднань захисту інформації.

Для прикладу, "Гібридний" або "Логіко-лавинно-статистичний" метод маршрутизації є узагальненням "Логічного", "Лавинного" і "Статистичного", суть якого зводиться до такого. За аналогією з "Логічним" методом мережа зв'язку вкладається в прямокутну систему координат, відповідно до якої

кожному вузлу комутації мережі присвоюється власна адреса *(X, Y)*. У кожному *j*-му ВК є матриця (2.8).

На момент уведення вузла в експлуатацію матриця містить тільки інформацію про суміжні номери ВК з даними і виражені в прямокутній системі координат.

У міру функціонування мережі зв'язку матриця (2.8) заповнюється і коригується. Визначення вихідних ТПП здійснюється "Логічним" методом, а заповнення і коригування матриці (2.8) здійснюється "Статистичним" методом. Тим самим під час формування (під час введення ВК в експлуатацію) і переформування (у процесі експлуатації ВК) ТМ відпадає необхідність передавання службової інформації мережею. Накопичення інформації в ТМ про формування маршрутів дає змогу розв'язати завдання глобальної оптимізації ПРІ на мережі зв'язку.

У разі зовнішніх деструктивних впливів на елементи ММЗ (ВК, ЛЗ) формування ПРІ здійснюється "лавинним" методом. При цьому вибір вихідних ЛЗ у ВК, починаючи від ВД до ВО, може бути послідовним, паралельним (багатошляховим) або комбінованим. Цей підхід дає змогу скоротити обсяг переданої службової інформації на мережі під час: введення вузлів комутації в експлуатацію; штатної експлуатації мережі, завдяки накопиченій раніше статистиці встановлення з'єднання між заданою парою ВК; зовнішніх деструктивних впливів на елементи ММЗ.

Таким чином, цей метод увібрав у себе позитивні властивості трьох методів "Логічного", "Лавинного" і "Статистичного":

– відсутність необхідності передавання службової інформації на мережі під час формування (під час уведення ВК в експлуатацію) і переформування (у процесі експлуатації ВК) ТМ;

– визначення оптимальних маршрутів і встановлення з'єднань, що підтримують QoS додатків в умовах зовнішніх деструктивних впливів на елементи ММЗ;

– розв'язання задачі глобальної оптимізації ПРІ на мережі зв'язку за накопиченою раніше статистикою встановлення з'єднання між заданою парою ВК.

В підсумку, узагальнена функціональна модель маршрутизації враховує резервування мережевих ресурсів для забезпечення комплексного захисту користувацької інформації користувача та підтримання якості обслуговування додатків мультисервісної мережі зв'язку.

Класифікація методів маршрутизації для мереж зв'язку враховує незалежні процедури: формування плану розподілу інформації на мережі; вибір вихідних ліній, трактів, каналів зв'язку у вузлах комутації. Ця класифікація дає змогу:

– виявити безліч варіантів реалізації як послідовних, так і паралельних (багатошляхових) методів маршрутизації;

– провести цілеспрямований аналіз і синтез тих методів маршрутизації, які будуть найефективніше функціонувати в передбачуваних мережах зв'язку і в заданих умовах.

"Гібридний" метод маршрутизації залежно від ступеня і характеру зовнішніх деструктивних впливів на елементи мережі використовує для формування таблиць маршрутизації "Логічний", "Статистичний" або "Лавинний" методи формування таблиць маршрутизації.

"Лавинний" методи формування ПРІ дає змогу скоротити обсяг переданої службової інформації на мережі під час:

– введення вузлів комутації в експлуатацію;

– штатної експлуатації мережі, за рахунок накопиченої раніше статистики встановлення з'єднання між заданою парою ВК;

– зовнішніх деструктивних впливів на елементи мережі.

Для визначення межі використання "Логічного", "Статистичного" і "Лавинного" методів формування ПРІ необхідно провести дослідження функціонування ММЗ в умовах зовнішніх деструктивних впливів на елементи мережі.

3.2 Розроблення методики забезпечення цілісності інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку

Суть методики забезпечення цілісності інформації за рахунок мережевих ресурсів ММЗ представлена на рисунку 3.1 у вигляді алгоритму послідовності дій. Використано такі позначення:

- $\overline{\mu_{(\varepsilon)i}^{(j)}}$ ранжований за переважністю список маршрутів із *j*-го ВД до *i*-го ВО при передаванні інформації *i*- му ВО під час передавання інформації ε-го додатка ММЗ;

- $\left\langle \mu_{(\varepsilon)iv}^{(j)} \right\rangle$ маршрут (список елементів мережі) *v*-го за переважністю вибору з *j*-го ВД до *i*-го ВО під час передавання інформації ε-го додатка ММЗ;

- m_j - кількість маршрутів у ранжованому списку з *j*-го ВД до *i*-го ВО.

Досягнення заданої користувачем цілісності переданої інформації $(P_Ц^{(П)})$ (оператор 01 алгоритму концепції методики (рисунок 3.1)) забезпечується за рахунок реалізації n паралельних з'єднань між ВД та ВО (рисунок 2.1) і в ВО прийняття рішення.

Для цього необхідно, щоб протоколи маршрутизації (методи формування плану розподілу інформації) здійснили моніторинг ММЗ і сформували бази даних параметрів (швидкість передавання інформації, час затримки, ймовірність помилкового приймання на символ тощо) стану елементів мережі (оператор 02 рисунка 3.1).

У результаті формуються таблиці маршрутизації (наприклад, від джерела) для кожного додатка мультисервісної мережі зв'язку.

На наступному етапі (оператор 03 рисунка 3.1) необхідно для кожного маршруту з таблиць маршрутизації обчислити відповідне значення та відповідно до нього сформувати новий ранжований спадаючий за перевагою список маршрутів з *j*-го ВД до *i*-го ВО для кожного ε-го додатка ММЗ.

Для c_i - замість вартості $\left\langle \mu'^{(j)}_{(\varepsilon)iv} \right\rangle$-го маршруту можна використовувати кількість транзитних ВК між ВД та ВО. Як p_i можна використовувати:

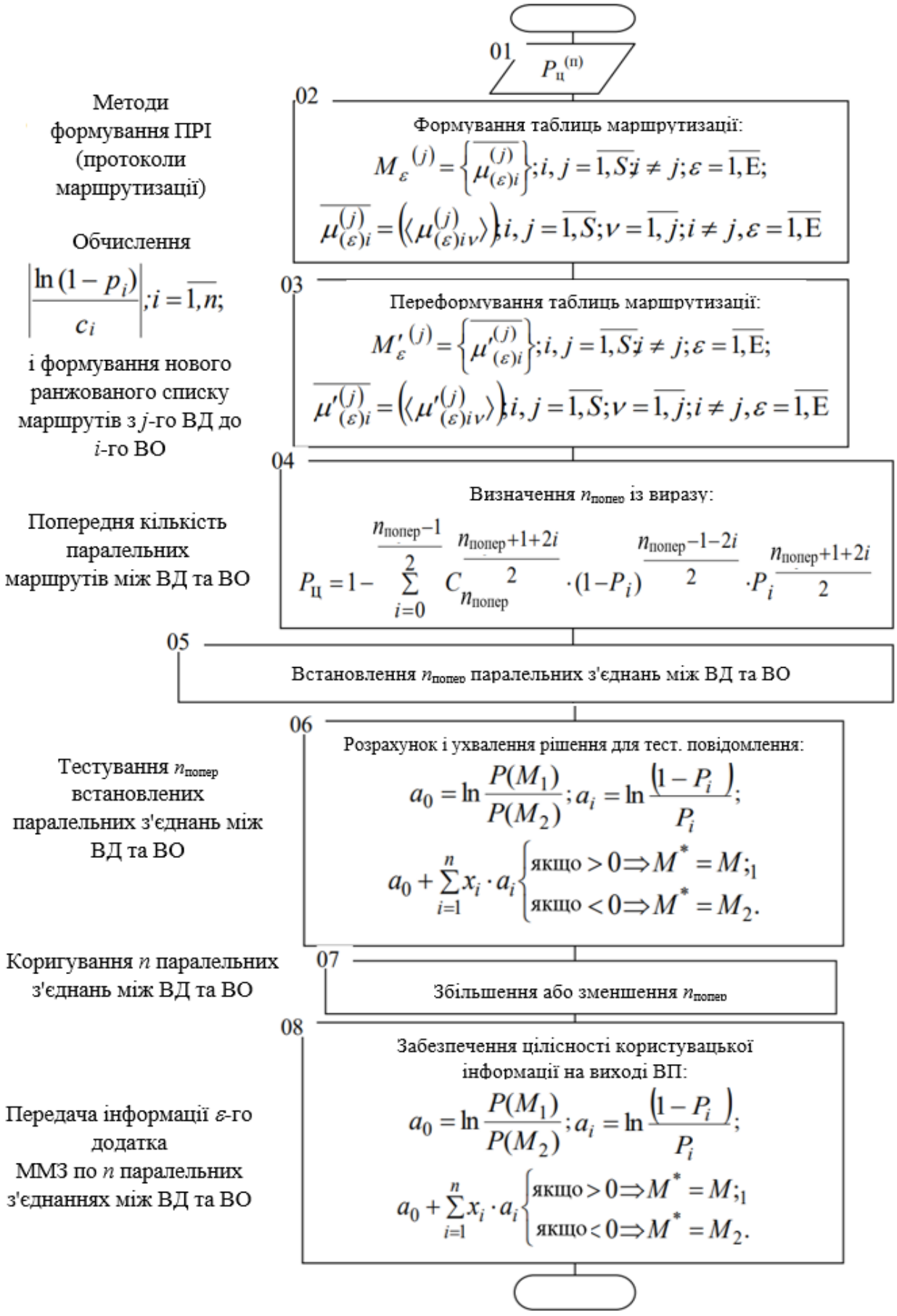


Рисунок 3.1 - Концепція методики забезпечення $(P_{Ц}^{(П)})$ цілісності інформації

– надійність $\left\langle \mu'^{(j)}_{(\varepsilon)iv} \right\rangle$-го маршруту, виражену в імовірнісних величинах;

– (1-$p_{\text{ош}i}$), де $p_{\text{ош}i}$ - ймовірність помилкового приймання символу, пакета, повідомлення тощо під час передавання інформації за $\left\langle \mu'^{(j)}_{(\varepsilon)iv} \right\rangle$-м маршрутом;

– (1-$p_{\text{м}i}$) тут $p_{\text{м}i}$ - ймовірність модифікації інформації, переданої по $\left\langle \mu'^{(j)}_{(\varepsilon)iv} \right\rangle$ -м маршрутом.

Оператори 04 ÷ 07 алгоритму (рисунок 3.1) визначають і встановлюють паралельні з'єднання між ВД та ВО.

Математичний вираз, який дає змогу визначити величину n, отримано за умови, що модифікації $M=\{M_1,M_2\}$ на всіх з'єднаннях (рисунок 2.1) є незалежними подіями, а їхні ймовірності рівні між собою, тобто $P_{\text{М}} = P_{\text{М}}^{(i)}; i = \overline{1,n}$. Тому визначення кількості паралельних з'єднань складається з двох етапів - попереднього (оператори 04, 05 і 06) та остаточного (оператор 07).

На попередньому етапі, використовуючи значення графіків $P_{\text{ц ВП}}=f(P_{\text{м}})$ (рисунок 2.2), визначається $n_{\text{попер}}$ (оператор 04). Далі система управління ММЗ, застосовуючи протоколи сигналізації (методи вибору вихідних ТПП), установлює між ВД та ВО $n_{\text{попер}}$ з'єднань (оператор 05).

Остаточне визначення величини n полягає в:

– тестуванні встановлених ппредв паралельних з'єднань (оператор 06);

– ухваленні рішення в ВО (оператор 06);

– коригуванні n (збільшенні або зменшенні $n_{\text{попер}}$) (оператор 07).

Після встановлення n паралельних з'єднань (цю процедуру реалізують методи вибору вихідних ТПП - протоколи сигналізації), вважається, що на ММЗ сформовано структуру з'єднань захисту інформації, що забезпечує її цілісність. Далі, використовуючи правило прийняття, представлене оператором 08, вирішальний пристрій, розташований в ВО, реалізує цілісність інформації.

3.3 Розроблення методики забезпечення доступності інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку

Концепцію методики забезпечення доступності інформації за рахунок мережевих ресурсів ММЗ представлено на рисунку 3.2.

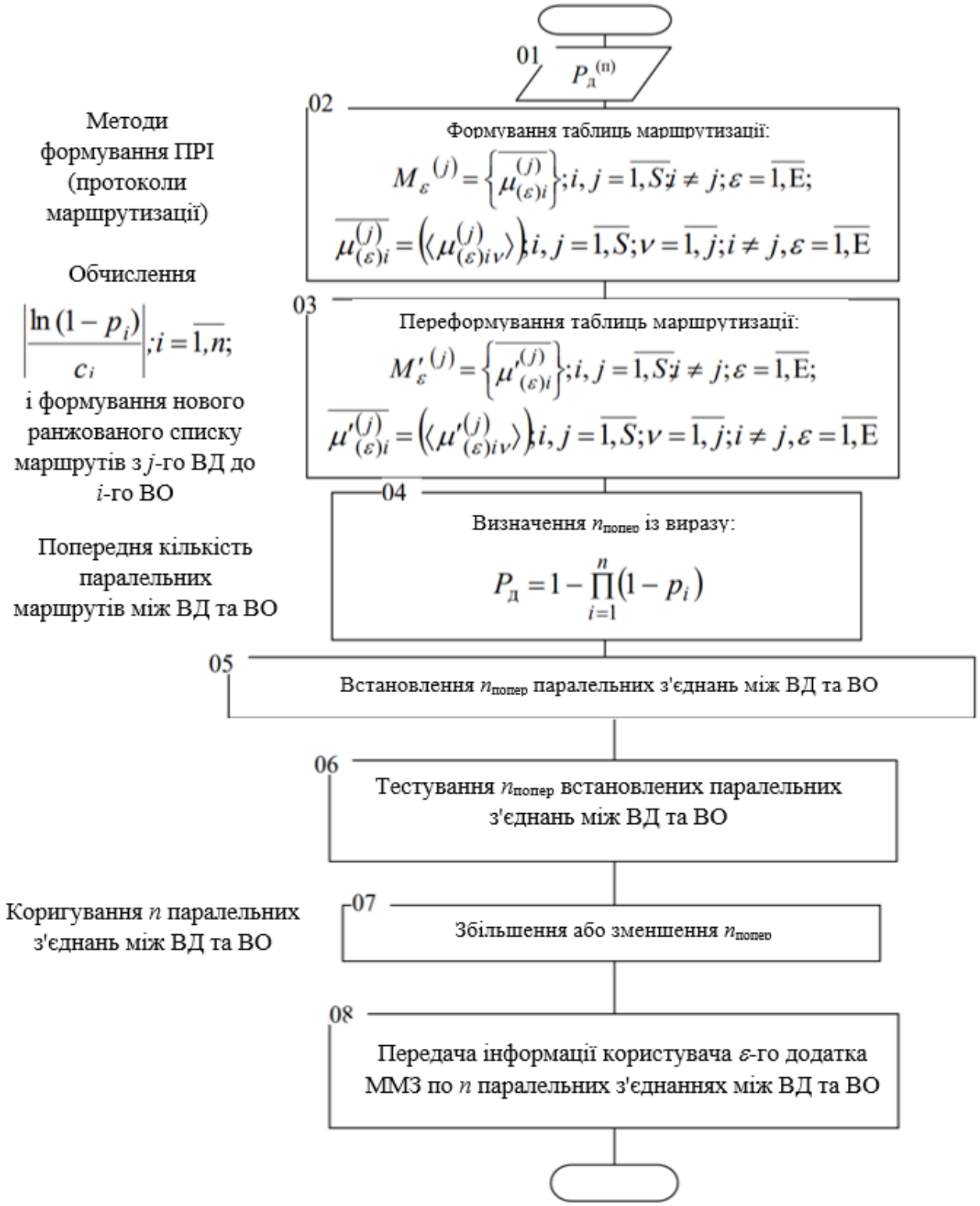


Рисунок 3.2 - Концепція методики забезпечення $P_д^{(П)}$ доступності інформації

Досягнення заданої користувачем параметра доступності переданої інформації $(P_{Д}^{(П)})$ (оператор 01), за аналогією з концепцією забезпечення цілісності, забезпечується за рахунок організації *n* паралельних з'єднань між ВД та ВО (рисунок 2.1).

Протоколи маршрутизації здійснюють моніторинг ММЗ і формують таблиці маршрутизації для кожного додатка мультисервісної мережі зв'язку $(\varepsilon = \overline{1,E})$ (оператор 02).

На наступному етапі (оператор 03) формується новий ранжований, спадний за перевагою список маршрутів (4.3) з *j*-го ВД до *i*-го ВО для кожного ε -го додатка ММЗ.

Оператори 04 ÷ 07 визначають і встановлюють n паралельних з'єднань між ВД та ВО.

Після встановлення *n* паралельних з'єднань вважається, що на ММЗ сформовано структуру з'єднань захисту інформації, яка забезпечує її доступність.

3.4 Розроблення методики забезпечення конфіденційності інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку

Цю методику можна застосувати в ММЗ для випадку забезпечення високого ступеня конфіденційності інформації під час використання високошвидкісних застосунків, критичних до затримок, наприклад відеоконференції.

В основу цієї методики закладено механізм багаторазового асиметричного шифрування відкритої інформації в ВД та розшифрування закритої інформації в ВО. Демонстрацію багаторазового асиметричного шифрування представлено на рисунку 1.4.

Концепцію методики забезпечення конфіденційності інформації представлено на рисунку 3.3.

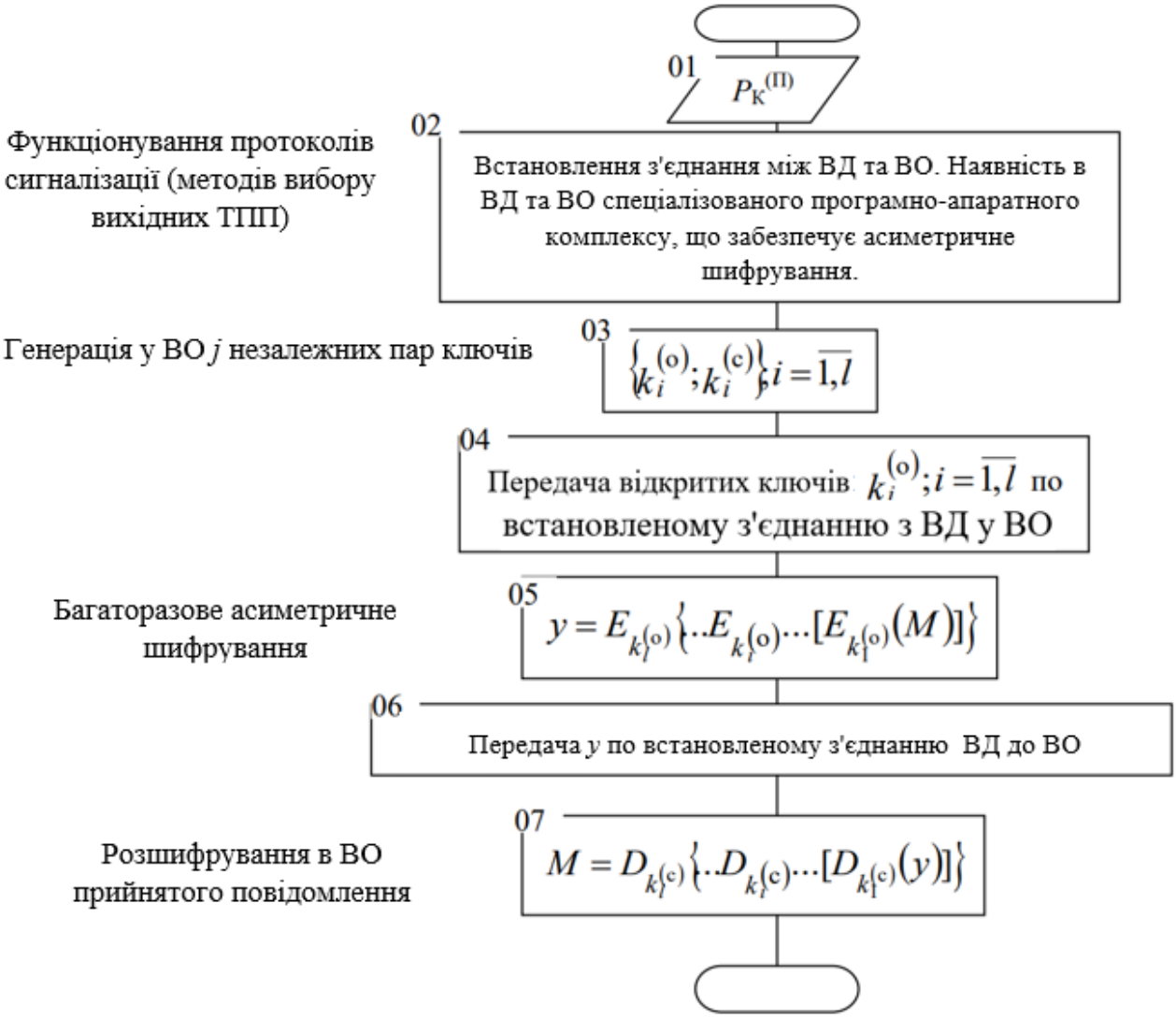


Рисунок 3.3 - Концепція методики забезпечення $P_К^{(П)}$ конфіденційності інформації

Для досягнення заданої користувачем конфіденційності $P_К^{(П)}$ переданої інформації (оператор 01) необхідна наявність (оператор 02):

– встановленого протоколами сигналізації (методами вибору вихідних ТПП) з'єднання між ВД та ВО;

– в ВД та ВО відповідного спеціалізованого програмно-апаратного комплексу, що забезпечує асиметричне шифрування.

У ВО генерується l незалежних пар відкритих $k_i^{(o)}$ і $k_i^{(c)}$ секретних ключів (оператор 03):

$$\{k_i^{(o)}; k_i^{(c)}\}; i = \overline{1,l}.$$

Відкриті ключі $k_i^{(o)}; i = \overline{1,l}$ за встановленим з'єднаннямпередаються з ВД в ВО (оператор 04).

У ВД виконується процедура багаторазового асиметричного шифрування (оператор 05).

Зашифроване повідомлення *y* передається по встановленому з'єднанню з ВД в ВО (оператор 06), а прийняте у ВО повідомлення розшифровується (оператор 07).

3.5 Розроблення методики захисту інформації за рахунок мережевих ресурсів мультисервісних мереж зв'язку

Концепція методики захисту інформації в ММЗ містить у собі послідовне застосування розроблених методик забезпечення доступності, конфіденційності, цілісності та представлена на рисунку 3.4. Досягнення заданих користувачем параметрів захисту переданої інформації, що передається $\left(P_Д^{(П)}, P_К^{(П)}, P_Ц^{(П)} \right)$ (оператор 01), забезпечується за рахунок організації структури з'єднань захисту, що являє собою *n* паралельні з'єднання між ВД та ВО.

З цією метою протоколи маршрутизації здійснюють моніторинг ММЗ і формують у всіх ВК таблиці маршрутизації (наприклад, від джерела) (оператор 02) для кожного додатка мультисервісної мережі зв'язку $\left(\varepsilon = \overline{1,E}\right)$, де:

- $\overline{\mu_{(\varepsilon)i}^{(j)}}$ - ранжований за переважністю список маршрутів з *j*-го ВД до *i*-го ВО під час передавання інформації ε -го додатка ММЗ;

- $\left\langle \mu'^{(j)}_{(\varepsilon)iv} \right\rangle$ маршрут (список елементів мережі) *V*-го за переважністю вибору з *j*-го ВД до *i*-го ВО під час передавання інформації ε - го додатка ММЗ;

- m_j - кількість маршрутів у ранжованому списку з *j*-го ВД до *i*-го ВО.

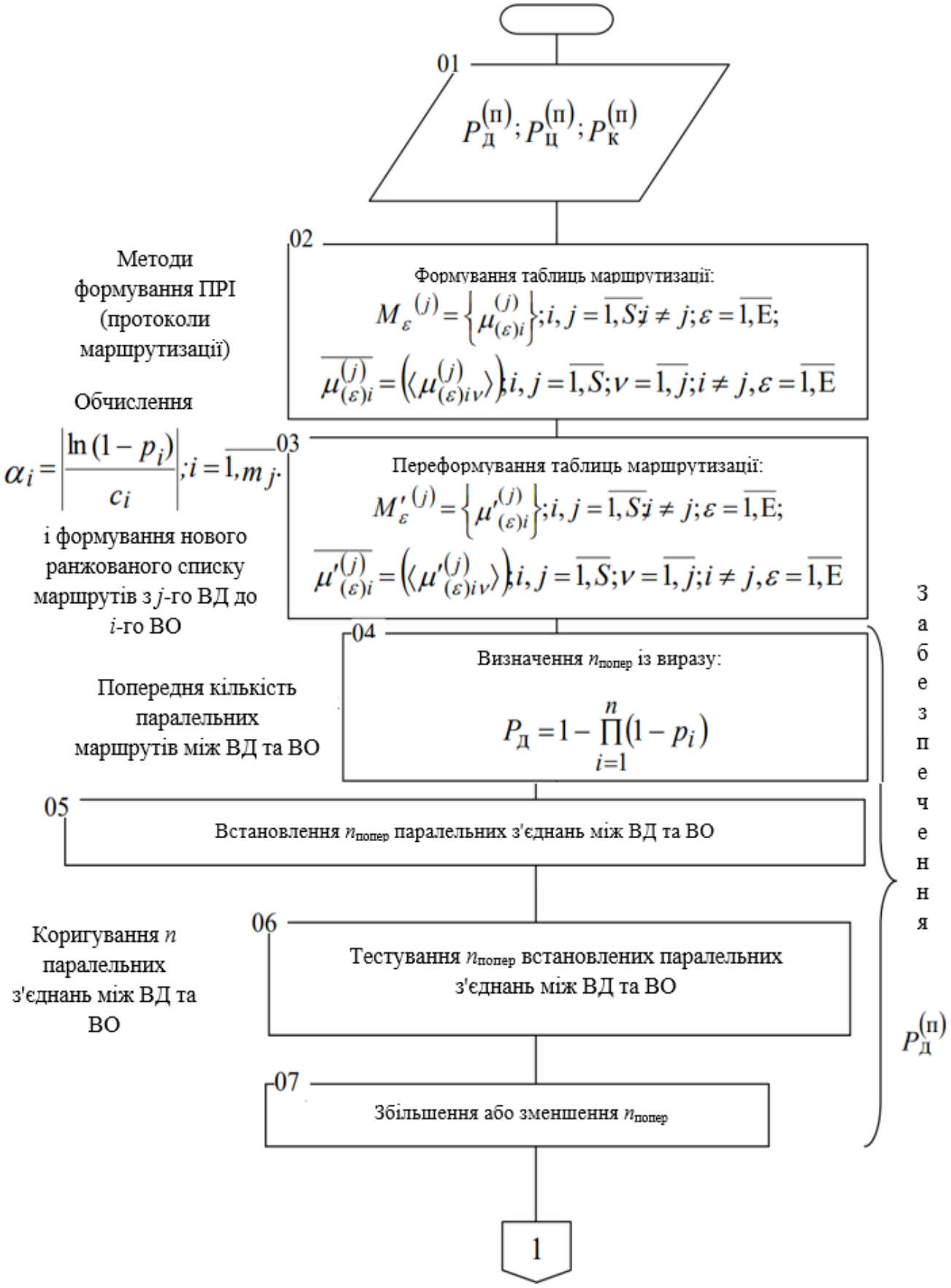
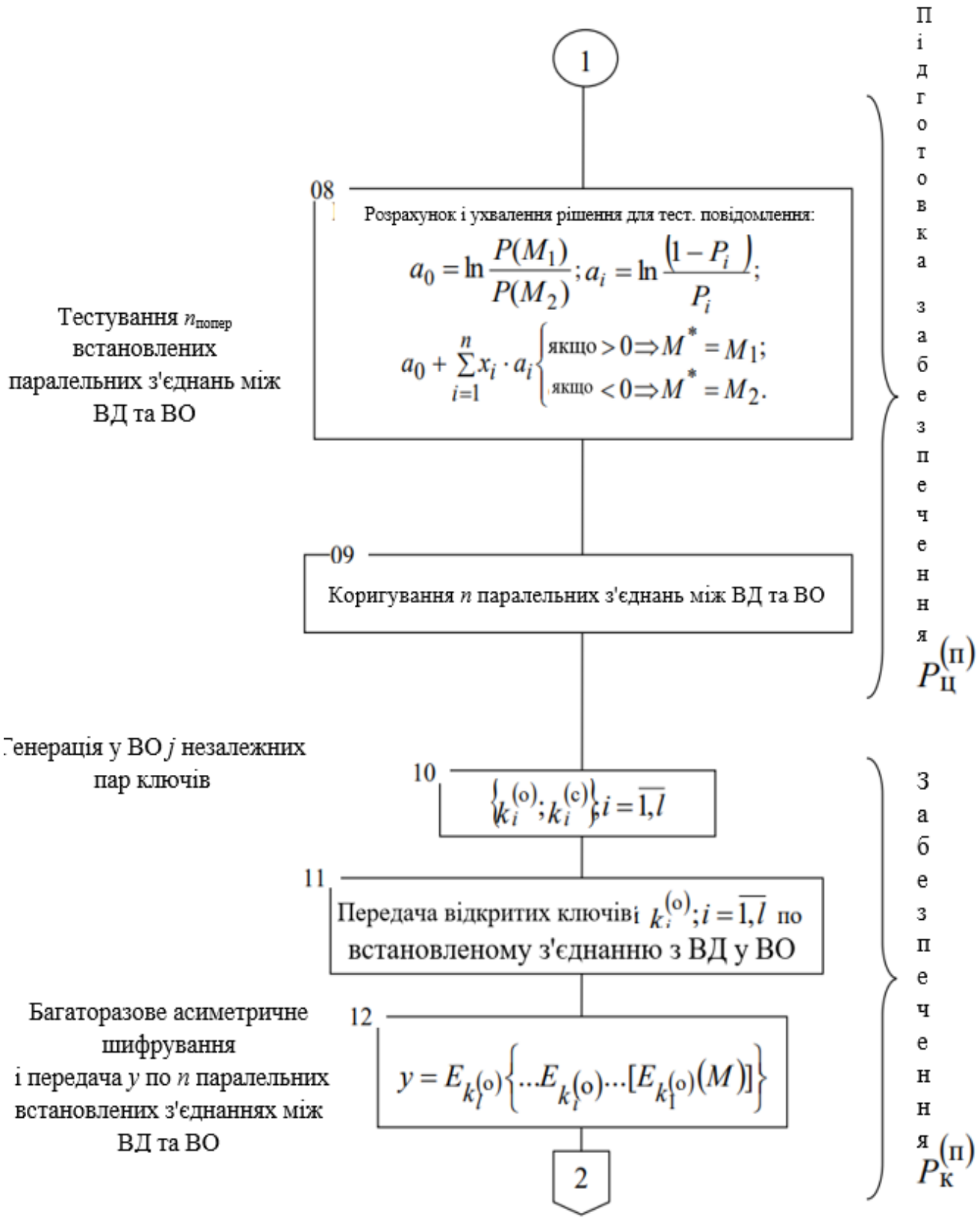
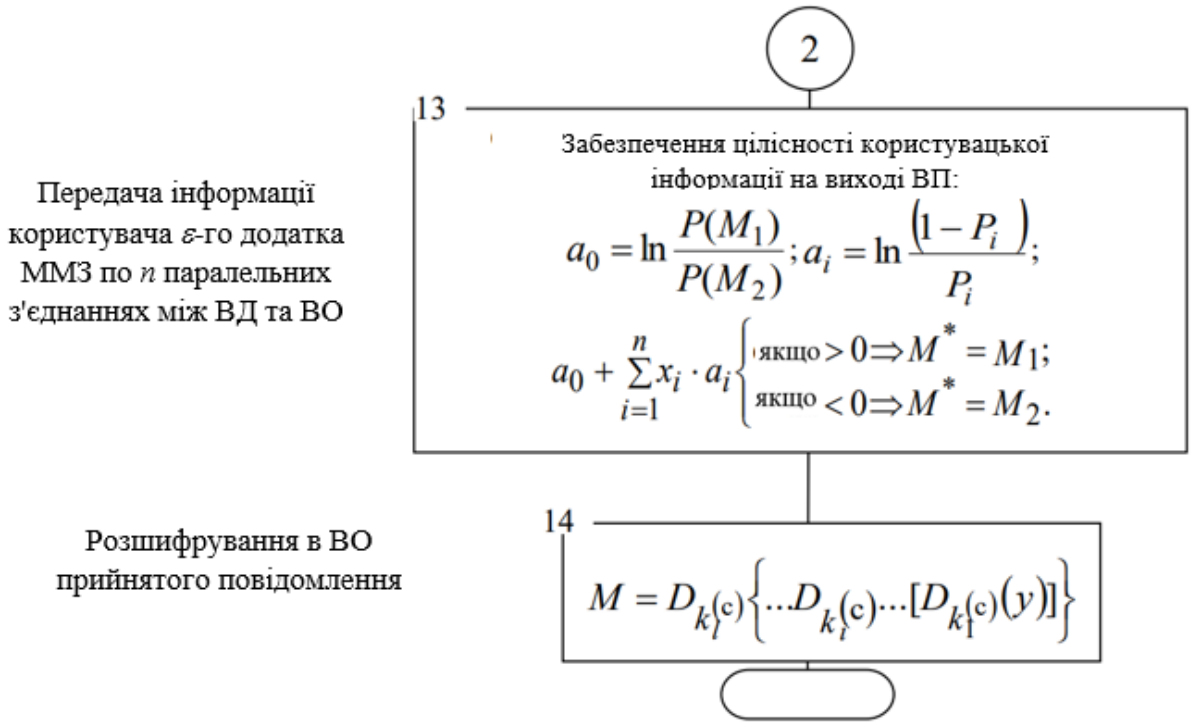


Рисунок 4.4 - Концепція методики захисту інформації



Продовження рисунка 4.4 - Концепція методики захисту інформації - процедура відновлення прийнятого тест-сигналу за правилом порівняння прийнятого тест-сигналу з переданим



Продовження рисунка 4.4 – Розшифрування повідомлення

На наступному етапі (оператор 03) послідовно виконуються процедури:

1) розрахунок для кожного маршруту $\langle \mu'^{(j)}_{(\varepsilon)iv} \rangle$ значення:

$$a_i = \left| \frac{\ln(1-p_i)}{c_i} \right|; i = \overline{1, m_j}.$$

Тут як змінні c_i і p_i можна використовувати наступні. Для c_i - замість вартості $\langle \mu'^{(j)}_{(\varepsilon)iv} \rangle$=го маршруту можна використовувати кількість транзитних ВК між ВД та ВО.

Як p_i можна використовувати:

– надійність $\langle \mu'^{(j)}_{(\varepsilon)iv} \rangle$-го маршруту, виражену в імовірнісних величинах;

– ($1-p_{\text{оші}}$), де $p_{\text{оші}}$ - імовірність помилкового приймання символу, пакета, повідомлення тощо під час передавання інформації по $\langle \mu'^{(j)}_{(\varepsilon)iv} \rangle$-му маршруту;

– ($1-p_{\text{Мі}}$), тут $p_{\text{мі}}$ - ймовірність модифікації інформації під час передання за $\langle \mu'^{(j)}_{(\varepsilon)iv} \rangle$-м маршрутом.

2) перестановка маршрутів у новий ранжированій убуваючий за перевагою список. Переважнішим є той маршрут, у якого $\alpha i; i = \overline{1, mj}$ є більшим значенням.

У результаті для кожного ε-го додатка ММЗ формуються таблиці маршрутизації.

Оператори 04 ÷ 07 визначають і встановлюють n паралельних з'єднань між ВД та ВО для забезпечення доступності $\left(P_{Д}^{(П)}\right)$ інформації в ММЗ.

Визначення кількості паралельних з'єднань складається з двох етапів: попереднього (оператори 04 ÷ 06) та остаточного (оператор 07).

На попередньому етапі визначається $n_{\text{попер}}$ (оператор 04). Далі система управління ММЗ, використовуючи протоколи сигналізації, встановлює між ВД та ВО $n_{\text{попер}}$ попередніх паралельних з'єднань (оператор 05).

Остаточне визначення величини n полягає в:

– тестуванні попередньо встановлених попередніх паралельних з'єднань (оператор 06);

– коригуванні n (збільшенні або зменшенні $n_{\text{попер}}$) (оператор 07). Після закінчення встановлення n паралельних з'єднань вважається, що на ММЗ сформовано структуру з'єднань захисту інформації, що забезпечує її доступність.

Наступним етапом методики є визначення необхідної кількості паралельних з'єднань між ВД та ВО для забезпечення цілісності інформації в ММЗ (оператори 08 і 09).

Визначення кількості паралельних з'єднань складається з двох етапів: попереднього (оператор 08) і остаточного (оператор 09).

На попередньому етапі з боку ВД в бік ВО надсилається тест-сигнал. Передача тест-сигналу здійснюється за заздалегідь встановленими паралельними з'єднаннями для забезпечення доступності інформації користувача.

У разі недостатнього значення величини $P_{Ц}^{(П)}$ приймається рішення про додавання додаткових паралельних з'єднань між ВД та ВО.

Після закінчення встановлення вибраних *n* паралельних з'єднань (дану процедуру реалізують методи вибору вихідних ТПП або ж використані протоколи сигналізації) вважається, що на ММЗ уже сформована структура з'єднань захисту інформаційних потоків, що забезпечує їх доступність та цілісність.

Для досягнення заданої користувачем конфіденційності інформації, що передається $P_K^{(П)}$ в ВО генерується l незалежних пар відкритих $k_i^{(o)}$ і $k_i^{(c)}$ секретних ключів (оператор 10).

Відкриті ключі $k_i^{(o)}; i = \overline{1,l}$, за встановленими з'єднаннями передаються з ВО в ВД (оператор 11).

На цьому етапі вважається, що структура захисту інформації між ВД та ВО сформована. ММЗ готова:

– передавати інформацію з QoS обраного користувачем додатка;

– реалізувати заявлений користувачем (за тарифним планом) профіль захисту інформації ($P_Д^{(П)}, P_K^{(П)}, P_Ц^{(П)}$).

У ВД виконується процедура багаторазового асиметричного шифрування (оператор 12).

Зашифроване повідомлення *y* передається через *n* паралельних установлених з'єднань з ВД у ВО.

Прийняте у ВО повідомлення обробляється вирішувальним пристроєм. Тим самим реалізується цілісність інформації. Далі повідомлення *y* розшифровується (оператор 14). У результаті забезпечується конфіденційність інформації.

Після закінчення кожного сеансу зв'язку структура захисту інформаційних потоків між ВД та ВО розформовується. Усі використані мережеві ресурси, які були задіяні в цьому сеансі зв'язку, для захисту і передачі інформації з QoS, вивільняються.

Запропоновані у роботі методики дають змогу в принципі забезпечити прийнятний ступінь захисту інформаційних потоків у мультисервісних комп’ютерних мережах зв'язку без зниження QoS у випадку високошвидкісних

додатків, які функціонують в системі у реальному масштабі часу (критичних до затримок).

Методики орієнтовані на розробників у сфері інформаційної безпеки телекомунікаційних систем, а також на операторів мультисервісних мереж зв'язку.

ВИСНОВКИ

1. Здійснено аналіз сучасного стану забезпечення конфіденційності, цілісності і доступності інформації в мультисервісних мережах зв'язку, що дало змогу обгрунтувати і дослідити можливості використання багаторазового асиметричного шифрування.

2. Розроблено метод забезпечення цілісності інформації на мережевому рівні мультисервісних мереж зв'язку та проведено його імітаційне моделювання, що дозволило встановити критерії вибору ресурсів мультисервісних мереж зв'язку для забезпечення цілісності та доступності інформації.

3. Розроблено узагальнену функціональну модель маршрутизації в мультисервісних мережах зв'язку, що дозволило встановити методи формування плану розподілу інформації в мультисервісних мережах зв'язку.

4. Розроблено методики забезпечення цілісності, доступності та конфіденційності інформації за рахунок мережевих ресурсів мультисервісної мережі зв'язку, а також узагальнену методику захисту інформації в мультисервісних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О. Телекомунікаційні системи та мережі наступного покоління, 2019. 315с.
2. Cisco AVVID Network Infrastructure Overview [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/web/offer/CAT4500/toolkit/comin_ov.pdf
3. Яцишин О.В. Дослідження технологій безпроводових сенсорних мереж з інфокомунікаційними наземними вузлами у зоні надзвичайної ситуації. https://ela.kpi.ua/bitstream/123456789/28112/1/Yatsishin_bakalavr.pdf
4. Kizza J. M. Guide to Computer Network Security. Chattanooga: Springer, 2015. 550 p.
5. Fuller R., Roberts J.W. Engineering for Quality of Service. [Електронний ресурс], 2008. Режим доступу: http://reference.kfupm.edu.sa/content/e/n/ engineering_for _quality_of_service__454802.pdf
6. Durand B., Sommerville J., Buchmann M. Administering Cisco QoS in IP networking. NY.: Syngress, 2003. 535 p.
7. Building the Carrier-Class IP Next-Generation Network. [Електронний ресурс], 2003. – Режим доступу: http://www.cisco.com/en/US/prod/collateral/ routers/ps5763/prod_white_paper090 0aecd802e2a52_ns573_Networking_ Solutions_White_Paper.html
8. Рекомендації ITU – T [Електронний ресурс]. Режим доступу до ресурсу: https://www.itu.int/ITU-T/recommendations/index.aspx?ser=H .
9. ITU-R Recommendation E.800 Terms and definitions, related to Quality of Services and network performance including dependability.
10. Бельков Д. В. Дослідження мережевого трафіка. Інформатика, кібернетика та обчислювальна техніка ДонНТУ, Донецьк, 2009. № 10. С. 38-49.
11. Willinger W., Willinger W., Taqqu M.S., and Erramilli A. A bibliographical guide to self-similar traffic and performance modeling for modern high-speed networks. Stochastic Networks: Theory and Applications. In Royal

Statistical Society Lecture Notes Series, Oxford University Press, 1996. Vol.4, P.339–366.

12. Бараш Л. Архітектура мультисервісних мереж. Комп'ютерне дослідження. Київ. 2002. № 14. С.93-99.

13. Побудова мультисервісної мережі [Електронний ресурс]. Режим доступу до ресурсу: http://ea.donntu.edu.ua/bitstream/123456789/2845/1/%D0%9F%D0%BE%D0%B1%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%20%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D1%81%D0%B5%D1%80%D0%B2%D1%96%D1%81%D0%BD%D0%BE%D1%97%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96.pdf .

14. Піневич Т.О. Стандартизація інфокомунікаційних мереж та систем. Інформаційно-керуючі системи на залізничному транспорті 2018 №6. С. 41-58.

15. Бовда Е.М., Сальник В.В. Методи забезпечення якості обслуговування в сучасних телекомунікаційних мережах військового призначення. Збірник наукових праць Харківського національного університету Повітряних Сил. 2017. № 2(51). С. 85-94.

16. QoS [Електронний ресурс]. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/QoS.

17. Tanenbaum A.S., Wetherall D.J. Computer Networks, 5th Ed. Prentice Hall, Cloth, 2011. 960 pp.

18. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. - Pearson Education, Inc., Old Tappan, New Jersey, 2016. 538 pp.;

19. Kurose J.F. Computer Networking: A Top-Down Approach, 7th Ed. Pearson Education, Inc., 2017. 864 pp.

20. Сигиденко М.М., Казьмірчук Н.В., Войтенко О.О. Аналіз захищеності інформації в мультисервісних мережах. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.77-79.

21. Сигиденко М.М., Басістий В.П. Метод захищеної маршрутизації в мультисервісних мережах. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.171-173.

22. ITU-T Recommendation P.862: "Perceptual evaluation of Speech Quality (PESQ), an objective method for End to end speech quality assessment of narrowband telephone networks and speech codecs".

23. Рекомендації ETSI [Електронний ресурс]. Режим доступу до ресурсу: https://www.etsi.org/ .

24. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. К. : НІСД, 2016. 528 с.

25. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.

26. Дузь-Крятченко О. П., Грицай П. М., Грищенко В. П., Клименко В. С. та ін. Основи стратегії національної безпеки та оборони держави: підруч. К. : НУОУ ім. Івана Черняховського, 2015. – 620 с.

27. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 с.

28. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. К.: ДУТ, 2015. 288 с.

29. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В. Захист інформації в автоматизованих системах управління: посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

30. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.

ДОДАТОК А

Копії публікацій