

## ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

### Магістр

(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Розроблення методики системи захисту комп'ютерної мережі з використанням серверів Stanford University Networks

Виконав: студент (ка) 6 курсу, групи СНмз-61  
спеціальності (напряму підготовки) 122  
Комп'ютерні науки  
(шифр і назва спеціальності (напряму підготовки))

Ядельський В.І.  
(підпис) (прізвище та ініціали)

Керівник Щербак Л.М.  
(підпис) (прізвище та ініціали)

Нормоконтроль Мацюк О.В.  
(підпис) (прізвище та ініціали)

Рецензент Кареліна О.В.  
(підпис) (прізвище та ініціали)



## АНОТАЦІЯ

Протоколи маршрутизації: дослідження та порівняння їх безпекових характеристик // Дипломна робота ОР «Магістр» // Ядельський Віктор Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНмз-61 // Тернопіль, 2019 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: МЕРЕЖА, ДАНІ, ПРОТОКОЛ, МАРШРУТИЗАЦІЯ, ДОСЛІДЖЕННЯ, АЛГОРИТМ, ДИНАМІЧНИЙ, АЛГОРИТМ, ЗБІЖНІСТЬ.

В першому розділі описано поняття маршрутизації. Проаналізовано основні компоненти маршрутизації. Наведено основні алгоритми маршрутизації, зокрема, звернуто увагу на мету розробки алгоритму маршрутизації. Однією із цілей алгоритмів маршрутизації є збіжність.

В другому розділі проведено аналіз протоколів маршрутизації. У сучасних мережах протокол RIP не саме краще рішення для вибору в якості протоколу маршрутизації, оскільки його можливості поступаються сучаснішим протоколам, таким як EIGRP, OSPF. Обмеження на 15 переходів не дозволяє застосовувати його у великих мережах. Перевага цього протоколу – простота конфігурації. Тому, якщо мережа невелика, то протокол RIP цілком прийнятний як протокол маршрутизації.

Недоліком протоколу EIGRP, являється те, що він обмежений кількістю вузлів – 100 і є закритим, тобто може бути реалізований на обладнанні компанії Cisco Systems.

Властивості збіжності включають швидкість поширення маршрутною інформації і обчислення оптимальних шляхів. Протоколи маршрутизації можуть бути оцінені на основі швидкості збіжності; чим швидша збіжність, тим

кращий протокол маршрутизації. Зазвичай, RIP не поспішає сходитися, тоді як EIGRP і OSPF в цьому плані швидші.

В третьому розділі проведено дослідження динамічного протоколу OSPF. Недоліком алгоритмів маршрутизації з врахуванням стану каналів є те, що вони можуть викликати значний трафік керуючих пакетів, що поширюється по всій мережі, наприклад, якщо в мережі виникає деяка подія і інформацію про ці події необхідно розіслати по всій мережі. Основною проблемою в сучасних мережах є те, що їх подальше зростання може привести до збільшення об'єму такої лавинної розсилки. Крім того, алгоритми маршрутизації з врахуванням стану каналів вимагають складніших обчислень в порівнянні з алгоритмами дистанційно-векторної маршрутизації і витрачають в порівнянні з ними більше ресурсів процесора і оперативної пам'яті. Але в міру подальшого підвищення оброблювальної здатності маршрутизаторів гострота цієї проблеми знижується.

*Метою дипломної роботи є дослідження динамічних протоколів маршрутизації.*

*Об'єктом дослідження є комп'ютерна мережа.*

*Предметом дослідження є динамічні протоколи маршрутизації RIP, EIGRP, OSPF.*

*Основні результати:* розроблено інструкцію початкового налаштування маршрутизації для обладнання компанії Cisco Systems протоколів маршрутизації OSPF та EIGRP.

## ABSTRACT

Routing information protocols: study and comparison of their safety characteristics // Diploma work degree "Master" // Yadelskyi Viktor // Ternopil Ivan Pul'uj National Technical University, Faculty of computer-information systems and software engineering, Department of computer science, a group SNmz-61 // Ternopil, 2019 // P. , Fig. - , Table. - , Draws. - , Add. - , Ref. - .

Modern engineering firms and organizations include information infrastructure that combines software, PC, assignment and cable networks. Most downtime assignment is for cable fault components. Understandably, users create maximum cable system perfectly. Reliability of information infrastructure as a whole depends on the reliability of its weakest component - cable system. Therefore, only the structured cabling system (SCS) - the basis of the information actually normal-computable network building and organization.

According to the "LAN Technology" simple information network are a consequence of failure network (on average 20 times a year), and by the fault of poor quality cable networks there is a 70% downtime.

Unfortunately, the failure of the cable system is not the only cause of downtime. Almost 40% of employees annually transported within the building along with their workstations. This leads to the need to consider the term MAC (Move, Add, Change - move, add, change (SW)). In unstructured SW cable networks can lead to serious work, that simple information online businesses and institutions.

In some areas of the building undesirable and even impossible to re-laying of the cable, because it entails a very expensive repair facilities. The best way to reduce the amount of downtime - refuse to use unstructured and structured cabling systems. The fact that the ease of use of cross-connections in the SCS allows you to perform the SW is much faster and cheaper than laying new segments structured cabling system.

Successfully working cable infrastructure data-processing systems (ITS) should address not only the present but also the future challenges ITS for years to come.

Experts estimate the life cycles (the "major" repair) components of information networks are: Software - 1 year, personal computers (CPU generations) - 2 years, mainframe - 10 years, structured cabling system - 16 years (without alterations and costs), frame building - 50 years. Economically important to design and install such a cable system, which will be the most durable of the potential for the introduction of any (even future) network equipment with no new costs for cable system. Structured Cabling Systems ITS not only today transmit signals efficiently informational video systems and cable television, language and computer data at speeds up to 100 megabits per second, but also serve as a basis for future multi-functional and efficient networks, such as for the long-awaited multimedia (at of 100 Mbps to sec. and faster) network ATM.

It is estimated that the cost of creating the various components of an information network infrastructure in building optimal if the cable system consumes 5% of the infrastructure in general, equipment assignment - 7% for workstations (equipment jobs) - 34%, and finally, software (total, including, for example, MS DOS, MS Windows, etc.) - 54%.

What is a high-quality cable jumper and switching equipment? They should be made to the producers recognized worldwide brands.

These materials must meet the quality standards of ISO-9000 International Organization for Standardization (Switzerland). Besides all components must have the manufacturer's warranty.

But the network is important not only equipment, but the principles of their work - protocols.

The first section describes the concept of routing. The basic components of routing. The basic routing algorithms, in particular, referred to the aim of developing routing algorithm. One of the goals of routing algorithms is convergence.

The second chapter analyzes routing protocols. Modern network protocol RIP is not the best solution to choose as routing protocol because the possibility of giving more modern protocols such as EIGRP, OSPF. Limit 15 transitions can not use it in larger networks. The advantage of this protocol - easy configuration. Therefore, if the network is small, the RIP protocol is acceptable as the routing protocol.

The downside protocol EIGRP, is that it is limited to the number of units - 100 and is closed, that can be implemented on equipment company Cisco Systems.

Properties include the convergence speed of propagation of routing information and calculation of optimal routes. Routing protocols can be evaluated on the basis of the rate of convergence; The faster convergence, the better routing protocol. Typically, RIP no hurry to converge, while EIGRP and OSPF in this regard faster.

In the third chapter the research of dynamic protocol OSPF. The downside of routing algorithms taking into account the state of channels is that they can cause considerable traffic control packets distributed throughout the network, for example, if a network event and there is some information about these events should send across the network. The main problem in modern networks is that their further growth could increase the volume of this avalanche distribution. In addition, the routing algorithms taking into account the state of channels require more complex calculations than with distance vector algorithms routing and spend compared to their more CPU and RAM. However, with further increase manufacturing capacity routers acuteness of the problem is reduced.

The aim of the thesis is to study dynamic routing protocols.

To fulfill our purpose, to perform the following tasks:

- analyze the concept of routing;
- to analyze the dynamic routing protocols and conduct their comparison;
- form the initial configuration of routers based on research protocols to ensure fast convergence of the network.

Object is a computer network.

The object of the study is dynamic routing protocols RIP, EIGRP, OSPF.

Main results: A manual for initial setup routing equipment company Cisco Systems routing protocols OSPF and EIGRP.

Keywords: NETWORK, DATA, PROTOCOLS, ROUTING, RESEARCH, ALGORITHMS, DYNAMIC, ALGORITHM, CONVERGENCE.



## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКРОЧЕНЬ І ТЕРМІНІВ**

AD – Advertised distance;

ANSI – American National Standards Institute (Національний інститут стандартизації США);

AS – Autonomous System (автономні системи);

ASBR – Autonomous System Boundary Router (граничні маршрутизатори автономної системи);

ATM – Asynchronous Transfer Mode (асинхронний режим передачі);

BDR – backup designated router (запасний виділений маршрутизатор);

BGP – Border Gateway Protocol;

CLNP – Connectionless Network Protocol;

DEC – Digital Equipment Corporation;

DR – designated router (виділений маршрутизатор);

DUAL – Diffusing Update Algorithm;

ES – кінцеві системи;

ES-IS – End System-to-intermediate System (протокол передачі маршрутної інформації від кінцевої системи до проміжної системи);

FC – Feasible Condition;

FD – Feasible distance;

FDDI – Fiber Distributed Data Interface (розподілений інтерфейс передачі даних по волоконно-оптичних каналах)

FS – Feasible Successor;

IANA – Internet Assigned Numbers Authority;

IDRP – InterDomain Routing Protocol (міждоменний маршрутизуючий протокол);

IPX – Internetwork Packet Exchange (міжмережевий пакетний обмін);

IS – проміжні системи;

LSA – Link - State Advertisement;

LSDB – Link-State DataBase (базі даних про стан каналів);  
MAC – Move, Add, Change;  
NBMA – NonBroadcast MultiAccess (неширокомовна мережа з множинним доступом);  
NSSA – Not-So-Stubby Area (не повністю тупикові області);  
RIP – Routing Information Protocol;  
RTMP – Routing Table Maintenance Protocol (протокол супроводу таблиць маршрутизації)  
RTP – Reliable Transport Protocol (надійний транспортний протокол);  
SKIP – Simple Key management for Internet Protocol (просте керування ключами для IP-протоколу).  
SPF – Shortest Path First (пошуку найкоротших шляхів);  
ІОС – інформаційно-обчислювальних систем;  
ПДЗ – переміщення, додавання, зміна;  
СКС – структурована кабельна система.

## ЗМІСТ

ВСТУП.....	14
1 АНАЛІЗ ПРОБЛЕМАТИКИ ДОСЛІДЖЕННЯ.....	17
1.1 Компоненти маршрутизації .....	17
1.1.1 Визначення маршруту.....	18
1.1.2 Комутація .....	19
1.2 Алгоритми маршрутизації .....	21
1.3 Типи алгоритмів.....	24
2 АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ.....	30
2.1 Протокол маршрутизації на базі вектору відстаней .....	30
2.2 Протокол маршрутизації на основі стану каналу.....	33
2.3 Вдосконалений протокол маршрутизації на базі вектору відстаней.....	36
2.4 Загальна характеристика внутрішніх протоколів маршрутизації.....	39
2.5 Зовнішній протокол маршрутизації.....	40
3 ДОСЛІДЖЕННЯ ДИНАМІЧНОГО ПРОТОКОЛУ OSPF .....	44
3.1 Маршрутизуючий протокол .....	44
3.1.1 Основні принципи функціонування маршрутизуючого протоколу ....	46
3.1.2 Порівняння протоколів маршрутизації з врахуванням стану каналів і протоколів дистанційно-векторної маршрутизації.....	49
3.2 Вибір відповідного маршрутизуючого протоколу.....	52
3.3 Огляд алгоритму SPF.....	53
3.3.1 Опис алгоритму SPF у дії .....	53
3.4 Ієрархія маршрутизації OSPF .....	60
3.4.1 Методи проектування ієрархічних мереж .....	61
3.4.2 Маршрутизації в мережі OSPF .....	62
3.4.3 Области OSPF .....	63
3.5 Експлуатаційне середовище OSPF.....	65
3.5.1 Типи маршрутизаторів OSPF .....	66
3.5.2 Типи мереж OSPF.....	67

3.5.3 Ідентифікація маршрутизатора .....	68
3.5.4 Сусідні пристрої .....	69
3.5.5 Стосунки суміжності.....	70
4 ПРАКТИЧНА РЕАЛІЗАЦІЯ ДОСЛІДЖЕНЬ.....	71
4.1 Особливості маршрутизаторів Cisco Systems .....	71
4.2 Налаштування маршрутизаторів Cisco.....	72
5 СПЕЦІАЛЬНА ЧАСТИНА.....	78
5.1 Протокол SKIP .....	78
5.2 Протокол IPSec.....	83
6 ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ.....	85
6.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР .....	85
6.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи ..	86
6.3 Розрахунок матеріальних витрат.....	89
6.4 Розрахунок витрат на електроенергію.....	90
6.5 Розрахунок суми амортизаційних відрахувань .....	90
6.6 Обчислення накладних витрат на дослідження та аналіз динамічних протоколів маршрутизації.....	91
6.7 Складання кошторису витрат та визначення собівартості .....	92
6.8 Розрахунок ціни дослідження та аналізу динамічних протоколів маршрутизації.....	93
6.9 Визначення економічної ефективності і терміну окупності капітальних вкладень .....	94
7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ .....	96
7.1 Охорона праці.....	96
7.1.1 Принципи професійного відбору операторів ВДТ .....	96
7.1.2 Працездатність операторів ВДТ .....	99
7.2 Безпека в надзвичайних ситуаціях.....	102
7.2.1 Міжнародний тероризм .....	102
7.2.2 Структура системи БЖД.....	104

7.2.3 Елементи теорії, що відповідають моделі безпеки життєдіяльності .	108
8 ЕКОЛОГІЯ .....	111
8.1 Вимоги до приміщень для експлуатації моніторів і ПЕОМ. Шляхи дотримання цих вимог.....	111
8.2 Статистичний аналіз екологічності виробництва .....	112
ВИСНОВКИ.....	115
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	117

## ВСТУП

Техніка сучасних фірм і організацій включає інформаційну інфраструктуру, що об'єднує в собі ПЗ, ПК, ЛКМ і кабельні мережі. Більшість простоїв ЛКМ відбувається за виною кабельних компонентів. Зрозумілим є бажання користувачів створити кабельну систему максимально безвідмовною. Надійність інформаційної інфраструктури в цілому залежить від надійності найслабшого її компонента – кабельної системи. Тому тільки структурована кабельна система (СКС) – основа дійсно нормальної роботи інформаційно-обчислюваної мережі будівлі, і організації в цілому.

Згідно з даними “LAN Technology” простої інформаційної мережі бувають в наслідок відмови мережі (в середньому 20 разів на рік), причому за виною неякісних кабельних мереж виникає 70% простоїв.

Нажаль, відмови кабельної системи не єдина причина простоїв. Майже 40% службовців щорічно переміщуються в межах будівлі разом зі своїми робочими станціями. Це призводить до необхідності враховувати термін MAC (Move, Add, Change – переміщення, додавання, зміна (ПДЗ)). В неструктурованих кабельних мережах ПДЗ можуть призводити до серйозних порушень роботи, тобто простої інформаційної мережі підприємства, установи.

На деяких ділянках будівлі небажана і навіть неможлива повторна прокладка кабеля, тому що вона тягне за собою дуже дорогі ремонти приміщень. Найкращий спосіб знизити кількість простоїв – відказ від неструктурованих і використання структурованих кабельних систем. Справа в тому, що простота використання крос-з'єднань в СКС дозволяє виконувати ПДЗ набагато швидше і дешевше ніж прокладання нових сегментів неструктурованої кабельної системи.

Успішно працюючі кабельні інфраструктури інформаційно-обчислювальних систем (ІОС) повинні вирішувати не тільки сьогоднішні, але й майбутні проблеми ІОС на багато років вперед.

За оцінками експертів життєві цикли (до “капітального” ремонту) компонентів інформаційних мереж такі: програмного забезпечення – 1 рік, персональних комп’ютерів (покоління процесорів) - 2 роки, мейнфреймів – 10 років, структурованої кабельної системи – 16 років (без переробок і затрат), каркасу будівлі – 50 років. Економічно важливо спроектувати і інсталиувати таку кабельну систему, яка стане максимально довговічною з потенціалом для впровадження будь-якого (навіть майбутнього) мережевого обладнання без нових витрат на кабельну систему. Структуровані кабельні системи ІОС не тільки вже сьогодні якісно передають сигнали інформаційних відеосистем та кабельного телебачення, мову та комп’ютерні дані зі швидкістю до 100 Мбіт на секунду, але й послужать основою для багатофункціональних та продуктивних майбутніх мереж, наприклад, для довгоочікуваної мультимедійної (зі швидкістю передачі 100 Мбіт на сек. та швидше) мережі АТМ.

Підраховано, що витрати на створення різноманітних компонентів інфраструктури інформаційної мережі в будівлі оптимальні, якщо на кабельну систему витрачається 5% від вартості інфраструктури в цілому, на обладнання ЛКМ – 7%, на робочі станції (обладнання робочих місць) – 34%, й, насамкінець, на програмне забезпечення (сумарне, включаючи, наприклад, MS DOS, MS Windows і т.п.) – 54%.

Що таке якісний кабель, кросове та комутаційне обладнання? Вони повинні бути виготовлені виробниками із визнаними в усьому світі торговими марками.

Ці матеріали повинні відповідати стандартам якості ISO-9000 Міжнародної організації по стандартизації (Швейцарія). Окрім того всі комплектуючі повинні мати гарантії виробника.

Але в роботі мережі важливим є не тільки обладнання, а принципи їх роботи – протоколи.

Метою роботи є дослідження динамічних протоколів маршрутизації.

Для виконання мети роботи потрібно виконати наступні завдання:

- проаналізувати поняття маршрутизації;

– здійснити аналіз динамічних протоколів маршрутизації та провести їх порівняння;

– розробити початкові налаштування маршрутизаторів на основі досліджених протоколів для забезпечення швидкої збіжності мережі.

Новизна: методи дослідження, використані в роботі, сформульовані в таких стандартах, як RFC, і являють собою методи роботи протоколів маршрутизації EIGRP та OSPF, що дозволяють аналізувати, вивчати й оцінювати об'єкт дослідження – комп'ютерну мережу.



# 1 АНАЛІЗ ПРОБЛЕМАТИКИ ДОСЛІДЖЕННЯ

В загальнодоступному значенні слова маршрутизація означає пересування інформації від джерела до пункту призначення через об'єднану мережу. При цьому, як правило, на шляху зустрічається принаймні один вузол. Маршрутизація часто протиставляється об'єднанню мереж за допомогою моста, яке, в популярному розумінні цього способу, виконує такі самі функції. Основна відмінність між ними полягає в тому, що об'єднання за допомогою моста має місце на рівні 2 еталонної моделі ISO, тоді як маршрутизація зустрічається на рівні 3. Цією різницею пояснюється те, що маршрутизація і об'єднання за мостовою схемою використовують різну інформацію в процесі її переміщення від джерела до місця призначення. Результатом цього є те, що маршрутизація і об'єднання за допомогою моста виконують свої завдання різними способами; фактично, є декілька різних видів маршрутизації і об'єднання за допомогою мостів.

Тема маршрутизації висвітлювалася в науковій літературі про комп'ютери більше 2-х десятиліть, проте з комерційної точки зору маршрутизація отримала популярність тільки в 1970 рр. Впродовж цього періоду мережі були досить простим, гомогенним оточенням. Великомасштабне об'єднання мереж стало популярним тільки останнім часом.

## 1.1 Компоненти маршрутизації

Маршрутизація включає два основні компоненти: визначення оптимальних трактів маршрутизації і транспортування інформаційних груп (що зазвичай називаються пакетами) через об'єднану мережу. Комутація відносно проста. З іншого боку, визначення маршруту може бути дуже складним процесом.

### 1.1.1 Визначення маршруту

Визначення маршруту може базуватися на різних показниках (величинах, результуючих з алгоритмічних обчислень по окремій змінній – наприклад, довжина маршруту) або комбінаціях показників. Програмні реалізації алгоритмів маршрутизації враховують показники маршруту для визначення оптимальних маршрутів до пункту призначення.

Для полегшення процесу визначення маршруту, алгоритми маршрутизації ініціалізуються і підтримують таблиці маршрутизації, в яких міститься маршрутна інформація. Маршрутна інформація змінюється залежно від використовуваного алгоритму маршрутизації.

Алгоритми маршрутизації заповнюють маршрутні таблиці деякою множиною інформації. Асоціації "Пункт призначення/наступна пересилка" повідомляють роутеру, що певний пункт призначення може бути оптимально досягнутий шляхом відправки пакету в певний роутер, що представляє "наступну пересилку" на шляху до кінцевого пункту призначення. При прийомі пакету роутер, що поступає, перевіряє адресу пункту призначення і намагається асоціювати цю адресу з наступною пересилкою. На рисунку 1.1 наведений приклад маршрутної таблиці "місце призначення/наступна пересилка".

To reach network:	Send to:
27	Node A
57	Node B
17	Node C
24	Node A
52	Node A
16	Node B
26	Node A
.	.
.	.
.	.

Рисунок 1.1 – Destination/Next Hop Routing Table

В маршрутних таблицях може міститися також і інша інформація. "Показники" забезпечують інформацію про бажаність якого-небудь каналу або тракту. Маршрутизатори порівнюють показники, щоб визначити оптимальні маршрути. Показники відрізняються один від одного залежно від використаної схеми алгоритму маршрутизації.

Маршрутизатори з'єднуються один з одним (і підтримують свої маршрутні таблиці) шляхом передачі різних повідомлень. Одним із видів таких повідомлень є повідомлення про "оновлення маршрутизації". Оновлення маршрутизації зазвичай включають всю маршрутну таблицю або її частину. Аналізуючи інформацію про оновлення маршрутизації, що поступає від усіх маршрутизаторів, будь-який з них може побудувати детальну картину топології мережі. Іншим прикладом повідомлень, якими обмінюються маршрутизатори, є "об'ява про стан каналу". Об'ява про стан каналу інформує інші маршрутизатори про стан каналів відправника. Канальна інформація також може бути використана для побудови повної картини топології мережі. Після того, як топологія мережі стає зрозумілою, маршрутизатори можуть визначити оптимальні маршрути до пунктів призначення.

### **1.1.2 Комутація**

Алгоритми комутації порівняно прості і в основному однакові для більшості протоколів маршрутизації. У більшості випадків головна обчислювальна машина визначає необхідність відправки пакету в іншу головну обчислювальну машину. Отримавши певним способом адресу маршрутизатора, головна обчислювальна машина-джерело відправляє пакет, адресований спеціально у фізичну адресу маршрутизатора (рівень MAC), проте з адресою протоколу (мережевий рівень) головної обчислювальної машини пункту призначення.

Після перевірки адреси протоколу пункту призначення пакету маршрутизатор визначає, знає він або ні, як передати цей пакет до наступного маршрутизатора. В другому випадку (коли маршрутизатор не знає, як

переслати пакет) пакет, як правило, ігнорується. В першому випадку маршрутизатор посилає пакет до наступного маршрутизатора шляхом заміни фізичної адреси пункту призначення на фізичну адресу наступного маршрутизатора і подальшої передачі пакету.

Наступна пересилка може бути або не бути головною обчислювальною машиною остаточного пункту призначення. Якщо ні, то наступною пересилкою, як правило, являється інший маршрутизатор, який виконує такий же процес прийняття рішення про комутацію. В міру того, як пакет просувається через об'єднану мережу, його фізична адреса міняється, проте адреса протоколу залишається незмінною. Цей процес наведено на рисунку 1.2.

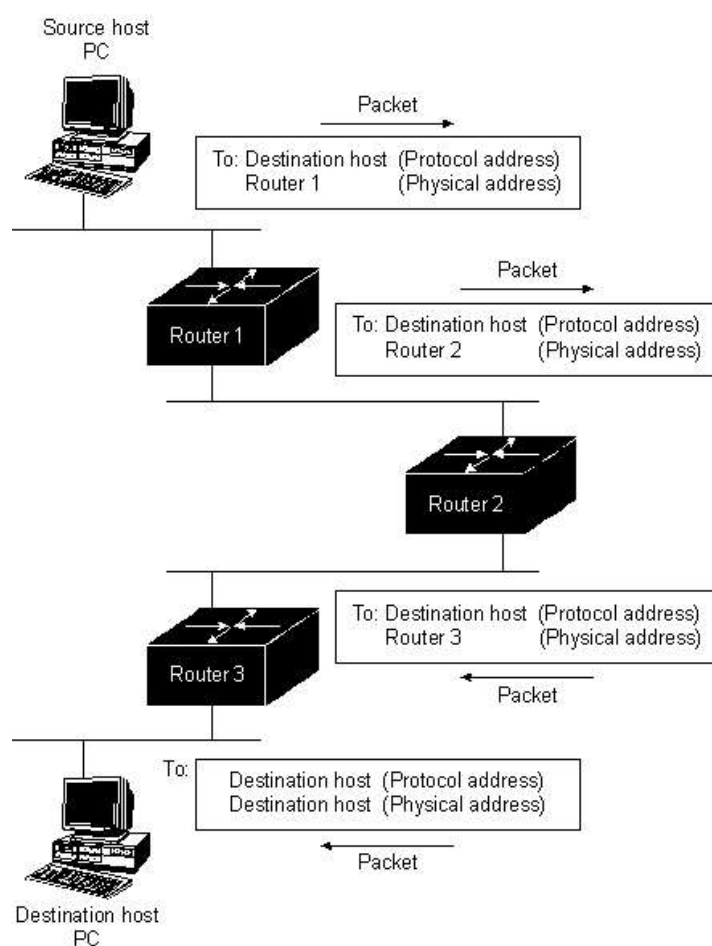


Рисунок 1.2 – Процес перемикування

Вище розглянута комутація між джерелом і системою кінцевого пункту призначення. Міжнародна Організація по Стандартизації (ISO) розробила ієрархічну термінологію, яка може бути корисною при описі цього процесу.

Якщо користуватися цією термінологією, то пристрої мережі, що не мають здатності пересилати пакети між підмережами, називаються кінцевими системами (ES), тоді як пристрої мережі, що мають таку здатність, називаються проміжними системами (IS). Проміжні системи далі поділяються на системи, які можуть повідомлятися в межах "доменів маршрутизації" ("внутрішньодоменні" IS), і системи, які можуть повідомлятися як в межах домена маршрутизації, так і з іншими доменами маршрутизації ("міждоменні IS"). Зазвичай вважається, що "домен маршрутизації" – це частина об'єднаної мережі, що знаходиться під загальним адміністративним керуванням і регульованої певним набором адміністративних керуючих принципів. Домени маршрутизації називаються також "автономними системами" (AS). Для певних протоколів домени маршрутизації можуть бути додатково поділені на "ділянки маршрутизації", проте для комутації як всередині ділянок, так і між ними також використовуються внутрішньодоменні протоколи маршрутизації.

## **1.2 Алгоритми маршрутизації**

Алгоритми маршрутизації можна диференціювати, ґрунтуючись на декількох ключових характеристиках. По-перше, на роботу результуючого протоколу маршрутизації впливають конкретні завдання, які вирішує розробник алгоритму. По-друге, існують різні типи алгоритмів маршрутизації, і кожен з них по-різному впливає на мережу і ресурси маршрутизації. І нарешті, алгоритми маршрутизації використовують різні показники, які впливають на розрахунок оптимальних маршрутів.

### *Мета розробки алгоритмів маршрутизації*

При розробці алгоритмів маршрутизації часто переслідують одну або декілька з перерахованих нижче цілей:

1. Оптимальність.
2. Простота і низькі непродуктивні витрати.
3. Живучість і стабільність.

4. Швидка збіжність.

5. Гнучкість.

*Оптимальність.* Оптимальність, ймовірно, є самою спільною метою розробки. Вона характеризує здатність алгоритму маршрутизації вибрати "найкращий" маршрут. Найкращий маршрут залежить від показників і від "ваги" цих показників, використовуваних при проведенні розрахунку. Наприклад, алгоритм маршрутизації міг би використати декілька пересилок з певною затримкою, але при розрахунку "вага" затримки може бути ним оцінений як дуже значний. Природно, що протоколи маршрутизації повинні строго визначати свої алгоритми розрахунку показників.

*Простота і низькі непродуктивні витрати.* Алгоритми маршрутизації розробляються як можна простішими. Іншими словами, алгоритм маршрутизації повинен ефективно забезпечувати свої функціональні можливості, з мінімальними витратами програмного забезпечення і коефіцієнтом використання. Особливо важлива ефективність в тому випадку, коли програма, що реалізовує алгоритм маршрутизації, повинна працювати в комп'ютері з обмеженими фізичними ресурсами.

*Живучість і стабільність.* Алгоритми маршрутизації повинні мати живучість. Іншими словами, вони повинні чітко функціонувати у випадку неординарних або непередбачених обставин, таких як відмови апаратури, умови високого навантаження і некоректні реалізації. Оскільки маршрутизатори розташовані у вузлових точках мережі, їх відмова може викликати значні проблеми.

Часто найкращими алгоритмами маршрутизації виявляються ті, які витримали випробування часом і довели свою надійність в різних умовах роботи мережі.

*Швидка збіжність.* Алгоритми маршрутизації повинні швидко сходиться. Збіжність - це процес угоди між усіма маршрутизаторами по оптимальних маршрутах. Коли яка-небудь подія в мережі призводить до того, що маршрути або відкидаються, або стають доступними, маршрутизатори

розсилають повідомлення про оновлення маршрутизації. Повідомлення про оновлення маршрутизації пронизують мережі, стимулюючи перерахунок оптимальних маршрутів і, зрештою, змушуючи всі маршрутизатори прийти до угоди по цих маршрутах. Алгоритми маршрутизації, які сходяться повільно, можуть привести до утворення петель маршрутизації або виходів з ладу мережі.

На рисунку 1.3 зображена петля маршрутизації. В даному випадку, в момент часу  $t_1$  до маршрутизатора 1 прибуває пакет. Маршрутизатор 1 вже був оновлений і тому він знає, що оптимальний маршрут до пункту призначення вимагає, щоб наступною зупинкою був маршрутизатор 2. Тому маршрутизатор 1 пересилає пакет в маршрутизатор 2. Маршрутизатор 2 ще не був оновлений, тому він вважає, що наступною оптимальною пересилкою має бути маршрутизатор 1.

Тому маршрутизатор 2 пересилає пакет назад в маршрутизатор 1. Пакет продовжуватиме скакати назад і вперед між двома маршрутизаторами до тих пір, поки маршрутизатор 2 не отримає коригування маршрутизації, або доки число комутацій цього пакету не перевищить допустимого максимального числа.

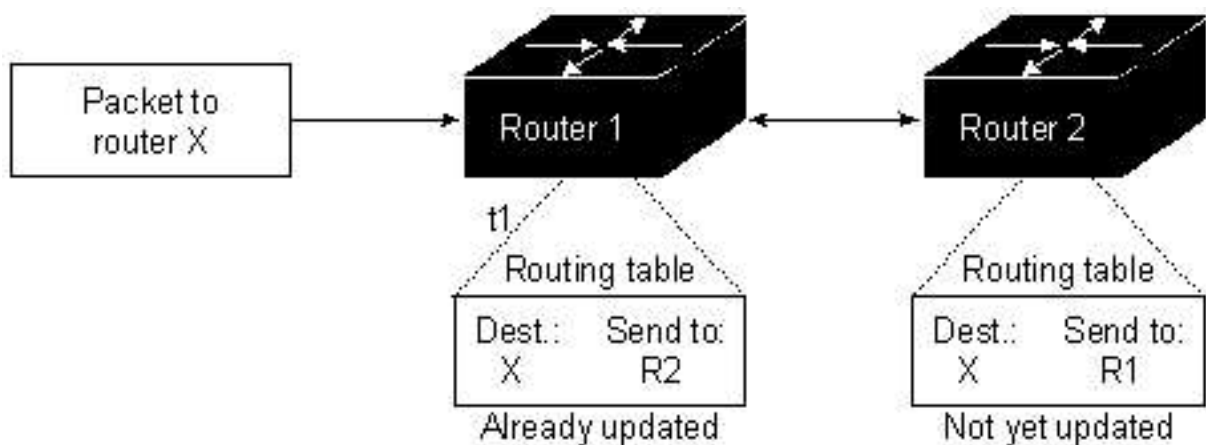


Рисунок 1.3 – Повільна збіжність і зациклення маршрутизації

*Гнучкість.* Алгоритми маршрутизації мають бути також гнучкими. Іншими словами, алгоритми маршрутизації повинні швидко і точно

адаптуватися до різноманітних обставин в мережі. Наприклад, припустимо, що сегмент мережі знехтуваний. Багато алгоритмів маршрутизації, після того, як вони дізнаються про цю проблему, швидко вибирають наступний найкращий шлях для всіх маршрутів, які зазвичай використовують цей сегмент. Алгоритми маршрутизації можуть бути запрограмовані так, щоб вони могли адаптуватися до змін смуги пропускання мережі, розмірів черги до маршрутизатора, величини затримки мережі і інших змінних.

### 1.3 Типи алгоритмів

Алгоритми маршрутизації можуть бути класифіковані по типах. Наприклад, алгоритми можуть бути:

1. Статичними або динамічними.
2. Одномаршрутними або багатомаршрутними.
3. Однорівневими або ієрархічними.
4. З інтелектом в головній обчислювальній машині або в маршрутизаторі.
5. Внутрішньодоменними і міждоменними.
6. Алгоритмами стану каналу або вектору відстаней.

#### *Статичні або динамічні алгоритми.*

Статичні алгоритми маршрутизації взагалі навряд чи є алгоритмами. Розподіл статичних таблиць маршрутизації встановлюється адміністратором мережі до початку маршрутизації. Він не міняється, якщо тільки адміністратор мережі не змінить його. Алгоритми, що використовують статичні маршрути, прості для розробки і добре працюють в оточенні, де трафік мережі відносно передбачуваний, а схема мережі відносно проста.

Оскільки статичні системи маршрутизації не можуть реагувати на зміни в мережі, вони, як правило, вважаються непридатними для сучасних великих, постійно змінюваних мереж. Більшість домінуючих алгоритмів маршрутизації 1990 р. – динамічні.



Динамічні алгоритми маршрутизації підлаштовуються до обставин мережі, що змінюються, в масштабі реального часу. Вони виконують це шляхом аналізу повідомлень, що поступають, про оновлення маршрутизації. Якщо в повідомленні вказується, що мала місце зміна мережі, програми маршрутизації перераховують маршрути і розсилають нові повідомлення про коригування маршрутизації. Такі повідомлення пронизують мережу, стимулюючи маршрутизатори наново проганяти свої алгоритми і відповідним чином змінювати таблиці маршрутизації. Динамічні алгоритми маршрутизації можуть доповнювати статичні маршрути там, де це доречно. Наприклад, можна розробити "маршрутизатор останнього звернення" (тобто маршрутизатор, в який відсилаються всі невідправлені по певному маршруту пакети). Такий роутер виконує роль сховища невідправлених пакетів, гарантуючи, що всі повідомлення будуть хоч би певним чином оброблені.

*Одномаршрутні або багатомаршрутні алгоритми.* Деякі складні протоколи маршрутизації забезпечують безліч маршрутів до одного і того ж пункту призначення. Такі багатомаршрутні алгоритми роблять можливою мультиплексну передачу трафіку по численних лініях; одномаршрутні алгоритми не можуть робити цього. Переваги багатомаршрутних алгоритмів очевидні – вони можуть забезпечити значно велику пропускну спроможність і надійність.

*Однорівневі або ієрархічні алгоритми.* Деякі алгоритми маршрутизації оперують в плоскому просторі, тоді як інші використовують ієрархії маршрутизації. У однорівневій системі маршрутизації всі роутери рівні по відношенню один до одного. В ієрархічній системі маршрутизації деякі роутери формують те, що складає основу (backbone - базу) маршрутизації. Пакети з небазових роутерів переміщуються до базових роутерів і пропускаються через них до тих пір, поки не досягнуть загальної області пункту призначення. Починаючи з цього моменту, вони переміщуються від останнього базового роутера через один або декілька небазових роутерів до кінцевого пункту призначення.

Системи маршрутизації часто встановлюють логічні групи вузлів, що називаються доменами, або автономними системами (AS), або областями. В ієрархічних системах одні роутери якого-небудь домена можуть з'єднуватися з роутерами інших доменів, тоді як інші роутери цього домену можуть підтримувати зв'язок з роутером тільки в межах свого домена. В дуже великих мережах можуть існувати додаткові ієрархічні рівні. Роутери найвищого ієрархічного рівня утворюють базу маршрутизації.

Основною перевагою ієрархічної маршрутизації є те, що вона імітує організацію більшості компаній і отже, дуже добре підтримує їх схеми трафіку. Велика частина мережевого зв'язку має місце в межах груп невеликих компаній (доменів). Внутрішньодоменим роутерам необхідно знати тільки про інші роутери в межах свого домена, тому їх алгоритми маршрутизації можуть бути спрощеними. Відповідно може бути зменшений і трафік оновлення маршрутизації, залежний від використовуваного алгоритму маршрутизації.

*Алгоритми з інтелектом в головній обчислювальній машині або в роутері.* Деякі алгоритми маршрутизації припускають, що кінцевий вузол джерела визначає весь маршрут. Зазвичай це називають маршрутизацією від джерела. В системах маршрутизації від джерела роутери діють просто як пристрої зберігання і пересилки пакету, без будь-яких роздумів посилаючи його до наступної зупинки.

Інші алгоритми припускають, що головні обчислювальні машини нічого не знають про маршрути. При використанні цих алгоритмів роутери визначають маршрут через об'єднану мережу, базуючись на своїх власних розрахунках. В першій системі, розглянутій вище, інтелект маршрутизації знаходиться в головній обчислювальній машині. В системі, розглянутій в другому випадку, інтелектом маршрутизації наділені роутери.

Компроміс між маршрутизацією з інтелектом в головній обчислювальній машині і маршрутизацією з інтелектом в роутере досягається шляхом зіставлення оптимальності маршруту з непродуктивними витратами трафіку. Системи з інтелектом в головній обчислювальній машині частіше

вибирають найкращі маршрути, оскільки вони, як правило, знаходять усі можливі маршрути до пункту призначення, перш ніж пакет буде дійсно відісланий. Потім вони вибирають найкращий маршрут, ґрунтуючись на визначенні оптимальності цієї конкретної системи. Проте акт визначення усіх маршрутів часто вимагає значного трафіку пошуку і великого об'єму часу.

*Внутрішньодоменні або міждоменні алгоритми.* Деякі алгоритми маршрутизації діють тільки в межах доменів; інші - як в межах доменів, так і між ними. Природа цих двох типів алгоритмів різна. Тому зрозуміло, що оптимальний алгоритм внутрішньодоменної маршрутизації не обов'язково буде оптимальним алгоритмом міждоменної маршрутизації.

*Алгоритми стану каналу або вектору відстані.* Алгоритми стану каналу (відомі також як алгоритми "першочерговості найкоротшого маршруту") направляють потоки маршрутної інформації в усі вузли об'єднаної мережі. Проте кожен роутер посилає тільки ту частину маршрутної таблиці, яка описує стан його власних каналів. Алгоритми вектору відстані (відомі також як алгоритми Белмана-Форда) вимагають від кожного роутера посилення всієї або частини своєї маршрутної таблиці, але тільки своїм сусідам. Алгоритми стану каналів фактично направляють невеликі коригування по всіх напрямках, тоді як алгоритми вектору відстаней посилають більші коригування тільки в сусідні роутери.

Відрізняючись швидшою збіжністю, алгоритми стану каналів дещо менше схильні до утворення петель маршрутизації, ніж алгоритми вектору відстані. З іншого боку, алгоритми стану каналу характеризуються складнішими розрахунками порівняно з алгоритмами вектору відстаней, вимагаючи більшої процесорної потужності і пам'яті, ніж алгоритми вектору відстаней. Внаслідок цього, реалізація і підтримка алгоритмів стану каналу може бути дорожчою. Незважаючи на їх відмінності, обидва типи алгоритмів добре функціонують при найрізноманітніших обставинах.

*Показники алгоритмів (метрики)*

Маршрутні таблиці містять інформацію, яку використовують програми комутації для вибору найкращого маршруту. Чим характеризується побудова маршрутних таблиць? Яка особливість природи інформації, яку вони містять? Проаналізуємо яким чином алгоритм визначає перевагу одного маршруту в порівнянні з іншими.

В алгоритмах маршрутизації використовується багато різних показників. Складні алгоритми маршрутизації при виборі маршруту можуть базуватися на множині показників, комбінуючи їх таким чином, що в результаті виходить один окремих (гібридний) показник. Нижче перераховані показники, які використовуються в алгоритмах маршрутизації :

1. Довжина маршруту.
2. Надійність.
3. Затримка.
4. Ширина смуги пропускання.
5. Навантаження.
6. Вартість зв'язку.

*Довжина маршруту.* Довжина маршруту є найбільш загальним показником маршрутизації. Деякі протоколи маршрутизації дозволяють адміністраторам мережі призначати довільні ціни на кожен канал мережі. В цьому випадку завдовжки тракту являється сума витрат, пов'язаних з кожним каналом, який був траверсований. Інші протоколи маршрутизації визначають "кількість пересилок", тобто показник, що характеризує число проходів, які пакет повинен вчинити на шляху від джерела до пункту призначення через спроби об'єднання мереж (такі як роутери).

*Надійність.* Надійність, в контексті алгоритмів маршрутизації, відноситься до надійності кожного каналу мережі (зазвичай описуваною в термінах співвідношення біт/помилка). Деякі канали мережі можуть відмовляти частіше, ніж інші. Відмови одних каналів мережі можуть бути усунені легше або швидше, ніж відмови інших каналів. При призначенні оцінок надійності можуть бути враховані будь-які чинники надійності. Оцінки надійності

зазвичай призначаються каналам мережі адміністраторами мережі. Як правило, це довільні цифрові величини.

*Затримка.* Під затримкою маршрутизації зазвичай розуміють відрізок часу, необхідний для пересування пакету від джерела до пункту призначення через об'єднану мережу. Затримка залежить від багатьох чинників, включаючи смугу пропускання проміжних каналів мережі, черги в порт кожного роутера на шляхи пересування пакету, перевантаженість мережі на всіх проміжних каналах мережі і фізичну відстань, на яку необхідно перемістити пакет. Оскільки тут має місце конгломерація декількох важливих змінних, затримка є найбільш загальним і корисним показником.

*Смуга пропускання.* Смуга пропускання відноситься до наявної потужності трафіку якого-небудь каналу. При інших рівних показниках, канал Ethernet 10 Mbps краща будь-якої орендованої лінії із смугою пропускання 64 Кбайт/сек. Хоча смуга пропускання є оцінкою максимально досяжної пропускнуої спроможності каналу, маршрути, що проходять через канали з більшою смугою пропускання, не обов'язково будуть кращі за маршрути, що проходять через менш швидкодіючі канали.

## 2 АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

### 2.1 Протокол маршрутизації на базі вектору відстаней

Одним з найбільш поширених протоколів маршрутизації на базі вектору відстаней, являється протокол RIP.

Основні характеристики протоколу RIP [1]:

- дистанційно-векторний протокол маршрутизації;
- метрика – число переходів;
- максимальне число переходів – 15;
- ширококомовна розсилка оновлень маршрутизації по замовчуванню – 30 секунд.

Еволюція протоколу RIP полягала в переході від класового протоколу маршрутизації (RIPv1) до безкласового протоколу (RIPv2). Відповідно до цих RIPv2 [1]:

- підтримує маску змінної довжини;
- відправляє маску підмережі разом з оновленням маршрутизації;
- групова розсилка (RIPv1 – ширококомовна розсилка);
- підтримка сумування маршрутів вручну;
- підтримка аутентифікації (процедура перевірки достовірності).

У чому полягає основна відмінність класової маршрутизації від безкласової. Існує таке поняття як маска підмережі – «набір біт, який визначає, яка частина в IP-адресі» показує адресу мережі, а яка показує адресу вузла в цій мережі. Набір є безперервною послідовністю одиниць і нулів.

Класова адресація потрібна для розділення мереж на підмережі, при цьому використовуються «стандартні» маски.

Для мереж класу А – маска «255.0.0.0», для мереж класу В – маска «255.255.0.0», для мереж класу С – маска «255.255.255.0» [2].

```

IP Адреса - хоста    13.14.49.121
      13      14      49      121
      00001101.00001110.00110001.01111001
Маска
      255      255      255      0    = /24
      11111111.11111111.11111111.00000000
      └──────────────────┬──────────┘
                мережа      хости
Компактний запис
IP Адреса - хоста    13.14.49.121/24
IP Адреса - мережі   13.14.49.0

```

Оскільки маленьких мереж набагато більше, ніж представлено в класі С, ввели безкласову адресацію. Для організації такої адресації використовують маски змінної довжини [2].

```

IP Адреса - хоста    13.14.49.121
      13      14      49      121
      00001101.00001110.00110001.01111001
Маска
      255      255      255      192  = /26
      11111111.11111111.11111111.11000000
      └──────────────────┬──────────┘
                мережа      хости
IP Адреса - мережі
      13      14      49      121
      00001101.00001110.00110001.01111001
      00001101.00001110.00110001.01000000
      13      14      49      64
Компактний запис
IP Адреса - хоста    13.14.49.121/26
IP Адреса - мережі   13.14.49.64

```

Враховуючи це, можна сказати, що протокол RIPv2 з підтримкою безкласової маршрутизації має більше можливостей.

Принцип роботи протоколу RIP. Маршрутизатори обмінюються повідомленнями про маршрутизацію тільки зі своїми сусідами (пряме підключення). Оновлення ці відбуваються періодично, незалежно змінилася

топология мережі або ні, і включають повну таблицю маршрутизації. Отримавши таблицю, маршрутизатор вносить певні зміни у свою таблицю.

Існує ряд проблем, що виникають з роботою протоколу RIP.

Наприклад, є три маршрутизатори, які з'єднані послідовно (див. рисунок 2.1). У кожного маршрутизатора вже складена своя таблиця маршрутизації до кожної мережі. Несподівано, мережа №4 відмовила в доступі, відповідно маршрутизатор №3 припиняє відправляти пакети в цю мережу. Але маршрутизатори №1 і №2 не знають про відмову мережі №4 [2].

Маршрутизатор №1 бачить, що мережа доступна через маршрутизатор №2, тобто в таблиці маршрутизації вказана мережа №4 з метрикою 2.

Відповідно ця мережа так само записується на другому маршрутизаторі, як відома. Таблиця маршрутизації видається маршрутизатору №3, і він вважає, що він має доступ до мережі №4 через маршрутизатор №2.

Таким чином, метрика буде рости по колу до безкінечності. Ця проблема вирішується шляхом задання максимуму, у випадку з протоколом RIP цей максимум дорівнює 16 переходам [2].

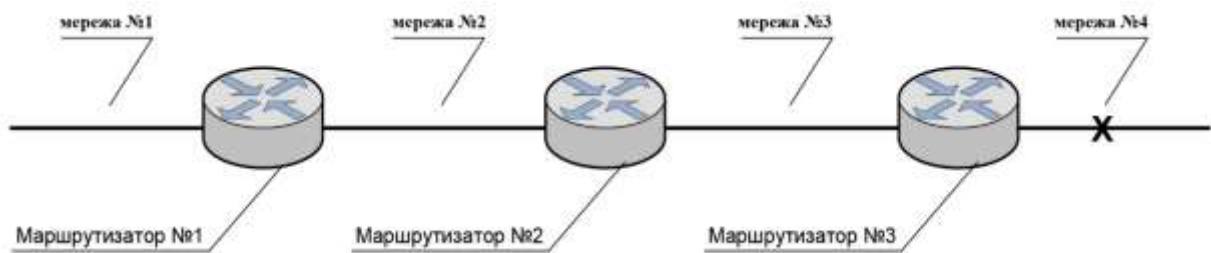


Рисунок 2.1 – Приклад послідовного з'єднання маршрутизаторів

Іноді в мережах, що використовують протокол RIP, виникають петлі. З розглянутого прикладу видно, що при відмові мережі №4 посланий пакет з мережі №1 нескінченно блукатиме між маршрутизаторами №2 і №3, тобто утворюється петля. Є декілька методів, які не допускають утворення петель:

1. Split Horizon. Суть методу полягає в тому, що маршрутизатор не відправлятиме дані про маршрут у зворотний бік.



2. Route Poisoning. При відмові мережі №4 маршрутизатор №3 привласнює каналу в цьому напрямку метрику 16 переходів (тобто мережа недоступна). Завдяки цьому маршрутизатор не сприйматиме оновлення (інформація, що мережа доступна), що поступають, від інших маршрутизаторів.

3. Таймери утримання. Таймер утримання інформації дозволяє запобігти петлям, проте збільшує час збіжності мережі. Стандартний час утримання в протоколі RIP складає 180 секунд. Цей час можна змінювати. Ідеальним рішенням є встановлення цього періоду дещо більшим максимального часу оновлення маршрутів цієї мережі.

Так, якщо відмовила мережа №4, відразу ж на маршрутизаторі №3 запускається таймер утримання, і маршрут до мережі №4 відзначається як недоступний. Якщо від сусідніх маршрутизаторів прийде оновлення з кращою метрикою, то мережа стане доступна, і таймер буде видалений. В іншому випадку оновлення ігноруватимуться. Завдяки цьому збільшиться час, щоб розповсюдити оновлення про зміну мережі.

## **2.2 Протокол маршрутизації на основі стану каналу**

Одним з поширених протоколів на основі стану каналу є протокол OSPF. Технологія роботи протоколу полягає у відстежуванні стану каналів і пошуку найкоротших шляхів, використовуючи алгоритм Дейкстри.

Стан каналу в цьому протоколі має на увазі опис інтерфейсу (наприклад, IP-адресу, маску, тип мережі і тому подібне) і його відношення із сусідніми маршрутизаторами. На основі вище вказаних описів інтерфейсів формується база даних стану каналів.

База даних заповнюється завдяки отриманню повідомлень про стан каналу («Link – State Advertisement – LSA») [3], які розсилаються регулярно або ж відразу після зміни топології мережі, або при яких-небудь змінах на маршрутизаторах. Ці повідомлення є невеликими пакетами. У LSA міститься інформація про підключені інтерфейси, метрики і інші параметри.

На основі отриманих повідомлень LSA маршрутизатор використовує алгоритм SPF, який будує дерево найкоротших маршрутів. Алгоритм проводить розрахунок над базою даних топології мережі, видаляючи зайві гілки (гілки – усі можливі шляхи). Отримані маршрути заносяться в таблицю маршрутизації.

Протокол OSPF – внутрішній протокол маршрутизації і працює всередині однієї автономної системи. Її можна розбити на зони (області), які є логічними розділами автономної системи.

Розглянемо дворівневу мережеву ієрархію, в якій у всіх маршрутизаторів свій принцип роботи.

На рисунку 2.2 представлена одна автономна система, яка має один пограничний маршрутизатор (марш. №0), що служить для зв'язку із зовнішньою мережею (наприклад, з іншою автономною системою).

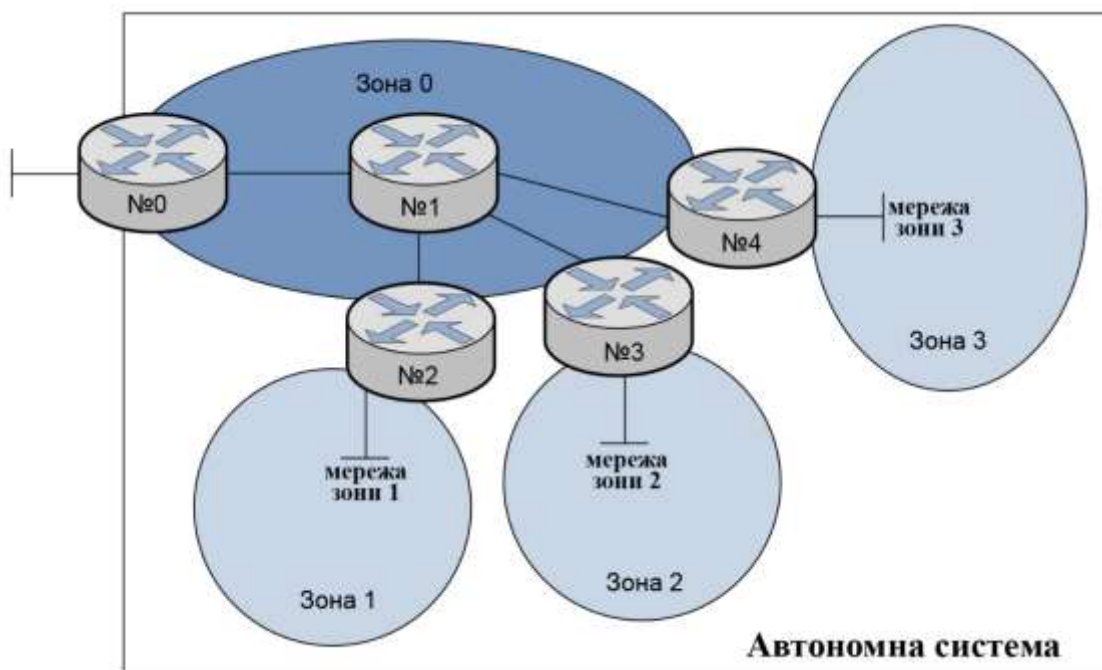


Рисунок 2.2 – Дворівнева мережева ієрархія

Автономна область включає [3]:

– зону 0 – область, що відповідає за з'єднання усіх областей, іноді її називають як магістральна область. Маршрутизатор №1 в цій області називають магістральним;

- зони 1-3 – маршрутизатори в цих областях називаються не магістральні. Це маршрутизатори, які знають топологію області, в яких вони знаходяться, і ведуть базу цих станів каналів тільки своїх областей;

- на стику зони 0 і зон 1-3 знаходяться пограничні маршрутизатори №2-4. Ці маршрутизатори ведуть базу цих станів каналів усіх областей, до яких вони підключені;

- маршрутизатор №0 так само є пограничним, але вже для автономної системи.

OSPF виконує наступні функції [3]:

- формує стосунки з сусідами;
- розсилає LSA для формування на кожному маршрутизаторі бази даних;

- запускає SPF для розрахунку найкращих маршрутів до всіх одержувачів;

- заповнює таблиці маршрутизації найкращими маршрутами до всіх одержувачів.

Протокол OSPF формує стосунки з сусідами таким чином. Два маршрутизатори, тобто маршрутизатори-сусіди, які працюють по протоколу OSPF, повинні «бачити» один одного в мережі, перш ніж обмінюватимуться інформацією. Цей процес реалізується за допомогою протоколу Hello. Маршрутизатори, в яких реалізований протокол OSPF, з усіх інтерфейсів розсилають hallo-пакети (багатоадресна розсилка – 224.0.0.6), які містять наступну інформацію [3]:

- «Router ID» – ідентифікатор маршрутизатора – 32-х бітний унікальний номер для маршрутизатора. По замовчуванню вибирається найбільша IP-адреса активного інтерфейсу. Ця ідентифікація важлива для встановлення сусідських стосунків і усунення неполадок в них, а також для координації обміну даними маршрутизації;

– Hello і Dead інтервали – інтервали вітання і простою. Інтервал вітання визначає період відправки hello-пакетів маршрутизатором (за умовчанням – 10 секунд). Інтервал простою – цей час, впродовж якого маршрутизатор чекає hello-пакет від сусіднього маршрутизатора, перш ніж оголосити його несправним (по замовчуванню інтервал простою в чотири рази перевищує інтервал вітання). Ці інтервали мають бути однаковими на сусідніх маршрутизаторах, в іншому випадку сусідські стосунки не будуть реалізовані;

– Neighbors – сусіди, в цьому полі перераховані всі сусідні маршрутизатори, з якими встановлено двостороннє з'єднання;

– Area ID – ідентифікатор області. Для взаємодії між собою, маршрутизатори повинні знаходитися в одному сегменті і їх інтерфейси повинні належати до однієї області OSPF в цьому сегменті. Так само, сусідні вузли повинні використати однакову підмережу і маску;

– Authentication password – пароль для аутентифікації, якщо аутентифікація включена. Пароль на всіх маршрутизаторах має бути однаковий;

– Stub area flag – прапор тупикової області. Тупикова область – особлива область середовища OSPF. Два маршрутизатори повинні погоджувати прапор тупикової області в hello-пакетах.

Для формування сусідства поля hello-пакету – повинні співпадати.

### **2.3 Вдосконалений протокол маршрутизації на базі вектору відстаней**

Вдосконаленим протоколом маршрутизації на базі вектору відстаней є протокол EIGRP. Він був розроблений компанією Cisco Systems, отже, часто використовується в обладнанні цієї компанії.

Протокол має наступні якості [4]:

– швидша збіжність порівняно з іншими протоколами на базі вектору відстаней, яка досягається завдяки алгоритму DUAL. Алгоритм складає

таблицю топологій, в якій вказано два кращі шляхи до мережі призначення (основний і резервний). На обох цих маршрутах не виникають петлі;

- зниження споживання смуги пропускання досягається за рахунок того, що при будь-кому зміні на мережі, алгоритм DUAL відправляє тільки нові оновлення, а не всю таблицю маршрутизації;

- підтримка багатьох протоколів мережевого рівня (IP, IPX, AppleTalk);

- безкласовий протокол маршрутизації.

- використання багатоадресної (224.0.0.10) і одноадресної розсилки, замість широкомовної. Завдяки цьому оновлення маршрутизації не зачіпають не потрібні маршрутизатори.

Принцип роботи протоколу EIGRP [4].

1. Протокол EIGRP спочатку повинен виявити своїх сусідів, для цього він використовує протокол Hello, який у свою чергу розсилає hello пакети (по замовчуванню кожні 5 секунд). Для відправки пакетів використовується багатоадресна розсилка. Поки hello-пакети приходять від сусіда, маршрутизатор визначає його як він функціонує. Якщо впродовж певного часу (по замовчуванню 15 секунд) від сусіда не прийшов hello-пакет, він вважається недоступним.

2. Після того, як сусіди встановлені, відбувається обмін інформацією. Спочатку пересилається інформація про повну топологію мережі між маршрутизаторами. А далі, при зміні на мережі, маршрутизатори обмінюються наступними пакетами:

- пакет оновлення маршрутів (Update). В цих пакетах зберігається інформація про зміну маршрутів. Пакети можуть пересилатися по багатоадресній або одноадресній розсилці;

- пакет запитів (Query). Цей пакет потрібний, коли маршрутизатор перераховує який-небудь маршрут, і в нього немає резервного. Маршрутизатор відправляє запит сусідам. Якщо у сусідів є маршрут, то вони відповідають

шляхом посилки пакету відповіді на запит (Reply). Якщо маршруту немає, то вони відправляють запит вже своїм сусідам;

– окрім цього, при отриманні вище вказаних пакетів (update, query, reply), у відповідь посилається пакет підтвердження (Acknowledgment).

Для гарантованої доставки відправлених пакетів протокол EIGRP використовує надійний транспортний). Протокол повторно пересилає маршрутну інформацію, якщо повідомлення було втрачене. За рахунок використання протоколу RTP зменшується ймовірність виникнення петель.

3. Далі відбувається вибір найкращого шляху. Маршрутизатори аналізують топологічну таблицю і вибирають з неї шлях з найменшою метрикою. Протокол рахує її за допомогою вагових коефіцієнтів («по замовчуванню  $K1=1$ ;  $K2=0$ ;  $K3=1$ ;  $K4=0$ ;  $K5=0$ »), а також смуги пропускання (bandwidth) і затримки (delay).

Формула для розрахунку смуги пропускання виглядає так:

$$\langle \text{bandwidth} = 10000000 / \text{bandwidth}(m) * 256 \rangle$$

bandwidth(m) – це мінімальна пропускна спроможність каналу на всьому шляху дотримання до мережі призначення.

Формула для розрахунку затримки виглядає так:

$$\langle \text{delay} = \text{delay} (s) * 256 \rangle$$

delay(s) – це сумарна затримка на всіх маршрутизаторах по дорозі дотримання до мережі призначення.

Якщо коефіцієнти залишити по замовчуванню, то:

$$\langle \text{Metric} = K1 * \text{bandwidth} + K3 * \text{delay} \rangle$$

У таблиці топологій знаходяться всі відомі маршрутизатори шляху.

Successor – це маршрутизатор, через який проходить оптимальний маршрут в мережу.

FD (Feasible distance) – це метрика, яку використовуватиме маршрутизатор. В даному випадку вона рівна 156160.

10.0.0.1 – IP-адреса сусіда. 128256 теж метрика, називається вона Advertised distance (AD) і показує метрику маршруту в мережу для того маршрутизатора, який оголошує про цей маршрут.

Так само в таблиці топологій можуть зустрітися наступні поняття:

FS (Feasible Successor) – це резервний маршрутизатор, через який можна потрапити в деяку мережу, якщо вийде з ладу сенсор.

«Feasible Condition (FC)». Щоб маршрутизатор міг стати резервним для якогось маршруту, необхідно, щоб значення Advertised distance (AD) для цього маршрутизатора було менше, ніж «Feasible distance (FD)». Таким чином, маршрутизатори, які працюють на основі протоколу EIGRP, підтримують три таблиці [3-5]:




- таблиця сусідів, в якій вказані всі сусіди;
- таблиця топології, в якій ведуться записи маршрутів до кожного місця призначення, відомі маршрутизатору;
- таблиця маршрутизації, куди заносяться кращі маршрути.

## **2.4 Загальна характеристика внутрішніх протоколів маршрутизації**

Порівняємо основні характеристики внутрішніх протоколів. В таблиці 2.1 показано [6]:

Можна зробити висновок (див. таблицю 2.1): кращими внутрішніми протоколами маршрутизації є OSPF і EIGRP. Особливо у застосуванні до великих і складних мереж. Але так само ці протоколи, не дивлячись на широкий спектр позитивних якостей, мають і свої мінуси. Протокол OSPF має високі вимоги до ресурсів маршрутизації через занадто складний обчислювальний розрахунок найкоротших шляхів. Хоча протокол EIGRP виграє в цьому плані, він все ж є закритим. Його реалізація можлива тільки на обладнанні Cisco Systems. Але в наш час в мережах застосовується обладнання різноманітних фірм.

Таблиця 2.1 – Порівняння внутрішніх протоколів маршрутизації

Протокол маршрутизації	RIPv2	OSPF	EIGRP
Алгоритм	Вектор відстаней (Белмана-Форда)	Стан каналу (Дейкстри)	Комбінований (DUAL)
Оновлення маршрутної інформації	Вся таблиця	Тільки зміни	Тільки зміни
Безкласовий	так	так	так
Максимальна кількість маршрутизаторів в мережі	15	–	255
Відкритий стандарт	так	так	ні
Метрика	Одна основна	Одна основна	Комбінована
Планування мережі	ні	так (вибір зон)	ні
Балансування навантаження	ні	Однакові метрики	Різні метрики
Складність конфігурації			

Тому у великих мережах вигідніше застосовувати протокол OSPF.

## 2.5 Зовнішній протокол маршрутизації

Протокол функціонує поверх протоколу транспортного рівня («TCP, порт 179») між автономними системами.

Як сказано вище, автономна система – це сукупність мереж із загальним управлінням, тобто набір маршрутизаторів, що мають єдині правила маршрутизації. В кожній автономній системі є свій номер. Організація, яка привласнює їх, називається «Internet Assigned Numbers Authority (IANA)». Номер є 16 бітною комбінацією, тобто номер від 1 до 65535. З них номери від 64512 до 65535 зарезервовані для приватного користування [6].



Маршрутизатори, які працюють на BGP, обмінюються інформацією про мережеву доступність будь-якої мережі, що складається із атрибутів шляху, щось на кшталт метрик для внутрішніх протоколів маршрутизації. Ці атрибути включають список всіх автономних систем, які необхідно пройти до мережі призначення. Так само включають IP-адреси наступної автономної системи і позначення, як мережа в кінці шляху була додана.

Протокол маршрутизації BGP дотримується правил про маршрутизацію тільки на рівні автономної системи. Внаслідок чого маршрутизатор, який працює на цьому протоколі, може передавати сусідній автономній системі тільки ті шляхи, які використовує сам.

Наприклад, у нас є декілька автономних систем (див. рисунок 2.3).

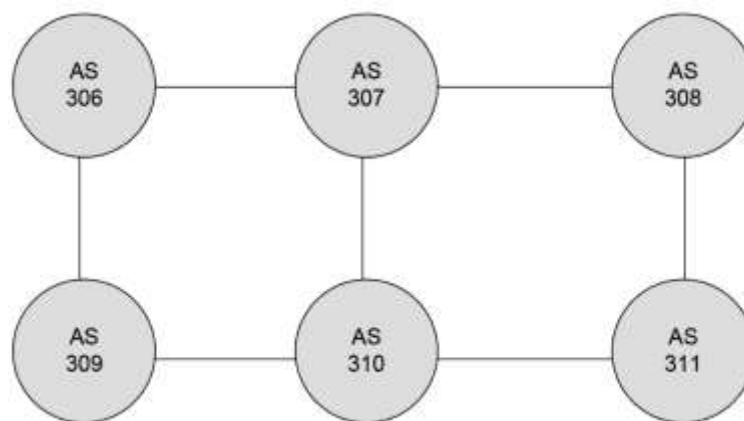


Рисунок 2.3 – Приклад декількох автономних систем

Необхідно відправити інформацію з автономної системи 306 в автономну систему 311, і є декілька варіантів шляхів [7]:

- «306-307-308-311»;
- «306-307-310-311»;
- «306-309-310-311»;
- «306-309-310-307-308-311».

Автономна система 306 не бачитиме всі ці варіанти, їй будуть видні тільки ті маршрути до системи 311, які передадуть автономні системи 307 і 309, причому найкращі маршрути. Наприклад, для маршрутизатора 307 кращий

маршрут «307-308-311». Автономна система 306 при зверненні до 307 бачитиме і відправлятиме трафік тільки по маршруту «306-307-308-311».

Автономна система 306 вибере найкращий варіант для відправки трафіку до 307 або 309 автономній системі за правилами, прийнятими у своїй автономній системі. Такий вид передачі даних, називається маршрутизація «крок за кроком».

Принцип взаємодії протоколу BGP між автономними системами і всередині однієї системи відрізняється. Якщо маршрутизатори належать одній автономній системі, то вони працюють по Internal BGP (IBGP), а якщо вони знаходяться в різних АС, то працюють по External BGP (EBGP).

На початку своєї роботи маршрутизатори, які працюють на основі протоколу BGP, формують TCP-з'єднання з кожним своїм сусідом, відправляючи повідомлення open. Це повідомлення має бути підтверджене повідомленням keepalive. Потім встановлюється з'єднання. «Стосунки» з сусідом підтримуються шляхом відправки повідомлень keepalive з періодичністю в 60 секунд [7].

Після встановлень «стосунків» маршрутизатори обмінюються кращими маршрутами, які зберігаються в їхніх же таблицях маршрутизації. Далі кожен маршрутизатор збирає ці маршрути від кожного сусіда і поміщає їх у базу даних топології BGP. Кращі маршрути для кожної мережі вибираються з бази даних топології процесом вибору маршруту BGP і записуються в таблицю маршрутизації. Зовнішні BGP маршрути мають адміністративну відстань 20, а внутрішні 200.

Після складання таблиці маршрутизації маршрутизатори обмінюються тільки оновленнями (повідомлення Update) при змінах на мережі. Так само маршрутизатори обмінюються повідомленнями про помилки і іншою службовою інформацією («notification messages»).

Розглянемо протокол BGP слід використати в тих випадках, коли [8-9]:

– автономна система є транзитною, через яку проходять пакети, призначені для інших автономних систем;

- автономна система має декілька підключень до інших автономних систем;
- політика маршрутизації між автономними системами має бути керованою, якщо потрібно вплинути на вибір шляху для вхідного та вихідного трафіку.

Протокол BGP не слід використовувати в тих випадках, коли:

- мережа має одне підключення до мережі Інтернет або до іншої автономної системи;
- недостатньо ресурсів процесора і пам'яті на граничному маршрутизаторі для застосування BGP маршрутизації;
- політика маршрутизації, використовувана в автономній системі, сумісна з політикою в автономній системі провайдера.

## 3 ДОСЛІДЖЕННЯ ДИНАМІЧНОГО ПРОТОКОЛУ OSPF

Враховуючи вищенаведене, протокол OSPF є найбільш практичним у використанні при проектуванні комп'ютерних мереж. Таким чином проаналізуємо його більш детально.

### 3.1 Маршрутизуючий протокол

Розробка будь-якого маршрутизуючого протоколу ведеться в рамках певного процесу проектування. У основі такого процесу лежать документи, відомі під назвою запитів на коментарі («Request For Comments – RFC»). Після випуску такого документа з пропозиціями про створення маршрутизуючого протоколу розглядаються письмові коментарі, що поступили, за запропонованою технологією, що дозволяє зрештою забезпечити її стандартизацію. Прикладом стандартного маршрутизуючого протоколу, розробленого вказаним чином, може служити OSPF, який визначений в документі RFC 2328.

Призначення OSPF можна коротко визначити таким чином, що цей протокол дозволяє успішно передавати пакети з одного хоста на інший по мережі. Цей процес, що виконується за допомогою маршрутизаторів, можна розглядати як таким, що складається з двох описаних нижче етапів – перенаправлення і маршрутизації [9]:

– *Перенаправлення.* Так називається процес здобуття маршрутизатором пакету через один інтерфейс, а потім визначення, через який інтерфейс необхідно передати цей пакет, аби він продовжував свій рух до одержувача. Але успішне виконання операції перенаправлення повністю залежить від того, чи має маршрутизатор інформацію про те, куди має бути відправлений пакет; якщо маршрутизатор не має такої інформації, він знищує цей пакет.

– *Маршрутизація*. Для того, щоб маршрутизатор міг визначити, через який інтерфейс необхідно перенаправити пакет, йому потрібна схема маршрутів (або доріг), на якій показана вся дорога від відправника до одержувача. Такий маршрут може бути сформований в результаті або статичною, або динамічного налаштування конфігурації; в даний момент нас цікавить лише динамічний аспект маршрутизації. OSPF – це динамічний маршрутизуючий протокол, і якщо маршрутизатор діє під управлінням протоколу OSPF, то динамічно виробляє маршрути до всіх одержувачів в мережі. З цими маршрутами можна ознайомитися, переглядаючи таблицю маршрутизації маршрутизатора.

Нижче перераховані основні типи протоколів з точки зору маршрутизації [10]:

– Протоколи, що маршрутизуються. Протоколи, за допомогою яких передавані дані перенаправляються через маршрутизатори. Для того, щоб маршрутизатор міг функціонувати належним чином, він має бути здатний правильно інтерпретувати інформацію про логічну мережу, яка вказана маршрутизованим протоколом. «До найбільш широко відомих маршрутизованих протоколів належить міжмережевий протокол (Internet Protocol – IP)»; іншими прикладами таких протоколів є протоколи мереж AppleTalk и DECnet. Для передачі даних по локальній або розподіленій мережі маршрутизовані протоколи використовують засоби, що надаються маршрутизуючими протоколами.

– Динамічні маршрутизуючі протоколи. Протоколи, що здійснюють динамічну маршрутизацію за допомогою алгоритму маршрутизації. Динамічний маршрутизуючий протокол підтримує маршрутизуючий протокол і забезпечує супровід таблиць маршрутизації. Динамічно маршрутизуючий протокол дозволяє маршрутизаторам динамічно обмінюватися інформацією про маршрути або топологію мережі за рахунок поширення маршрутної інформації по мережі. «Як приклади динамічних маршрутизуючих протоколів можна

назвати «OSPF, IGRP і RIP» («Routing Information Protocol – протокол маршрутної інформації»).

Протоколи, що маршрутизуються, такі як IP, використовуються як засіб обміну даними між окремими пристроями по мережі. Із застосуванням вибраного маршрутизуючого протоколу, такого як OSPF, який підтримується протоколом, що маршрутизується, таким як IP, можна створити мережу, що забезпечує обмін даними між будь-якими пристроями. Наприклад, як було вказано вище, IP є протоколом, що маршрутизується, який може використовувати в якості маршрутизуючого протоколу OSPF або RIP.

Динамічний маршрутизуючий протокол можна коротко визначити як набір стандартизованих правил, що дозволяють маршрутизаторам визначати маршрути. За допомогою маршрутизуючого протоколу формуються таблиці маршрутизації, що дозволяють маршрутизаторам вибирати оптимальні маршрути до одержувачів. Маршрутизуючі протоколи передбачають можливість для визначення оптимальних маршрутів (інколи названих шляхами) порівнювати між собою числові значення, названі метриками. Метрики – це числові значення, які представляють характеристики конкретних маршрутів. Метрики можуть розглядатися як вартості, тому їх числове значення часто визначають як вартість проходження пакету по каналу. Інформація про значення метрик зберігається в таблиці маршрутизації і використовується маршрутизатором при визначенні оптимального маршруту до мережі одержувача [11].

### **3.1.1 Основні принципи функціонування маршрутизуючого протоколу**

Розглянемо приклад маршрутизатора, конфігурація якого була спочатку налаштована на роботу з двома мережами, до яких він безпосередньо підключений. На перших порах в таблиці маршрутизації даного маршрутизатора є інформація лише про ці дві мережі. Але відомості про інші мережі, що виходять за межі перших двох, не введені в таблицю маршрутизації,

оскільки ці мережі не підключені до маршрутизатора безпосередньо. Яким же чином маршрутизатор може отримати інформацію про всі інші мережі, якщо йому потрібно буде передати в них пакети? Це завдання може бути вирішене за допомогою описаних нижче способі

– *Статична маршрутизація*. Визначення і введення в маршрутизатор вручну інформації про маршрут як про єдину дорогу до даного конкретного отримувача. Маршрутизація такого типу вимушує маршрутизатор вибирати той маршрут до одержувача, який вказаний в таблицях маршрутизації. Окрім того, маршрути такого типу розглядаються як переважніші в порівнянні з маршрутами, вибраними за допомогою динамічних маршрутизуючих протоколів. На рисунку 3.1 наведений приклад того, як ввести в таблицю маршрутизації статичний маршрут і як його використовувати. Статична маршрутизація не може застосовуватися як ефективне автономне рішення по забезпеченню маршрутизації в мережах середніх і великих розмірів, оскільки при цьому об'єм роботи, необхідний для забезпечення успішного функціонування мережі, інколи стає дуже великим. Найчастіше статичні маршрути використовуються в тупикових мережах (див. рис. 3.1). В таких умовах статичні маршрути дуже добре діють у поєднанні з динамічними маршрутизуючими протоколами, такими як OSP [12]:

– *Маршрутизація з використанням стандартного маршруту (default route)*. Стандартним (або вживаним за умовчанням) називається маршрут, вручну введений в таблицю маршрутизації маршрутизатора для використання в якості маршруту, по якому вирушають пакети, якщо маршрут одержувача невідомий. Маршрутизатор, якому передаються ці пакети, відомий також як маршрутизатор або шлюз, вживаний в безвихідних ситуаціях («gateway of last resort»). На рисунку 3.2 показано, що використання стандартного маршруту дозволяє спростити маршрутизацію.



Рисунок 3.1 – Приклад використання статичних маршрутів

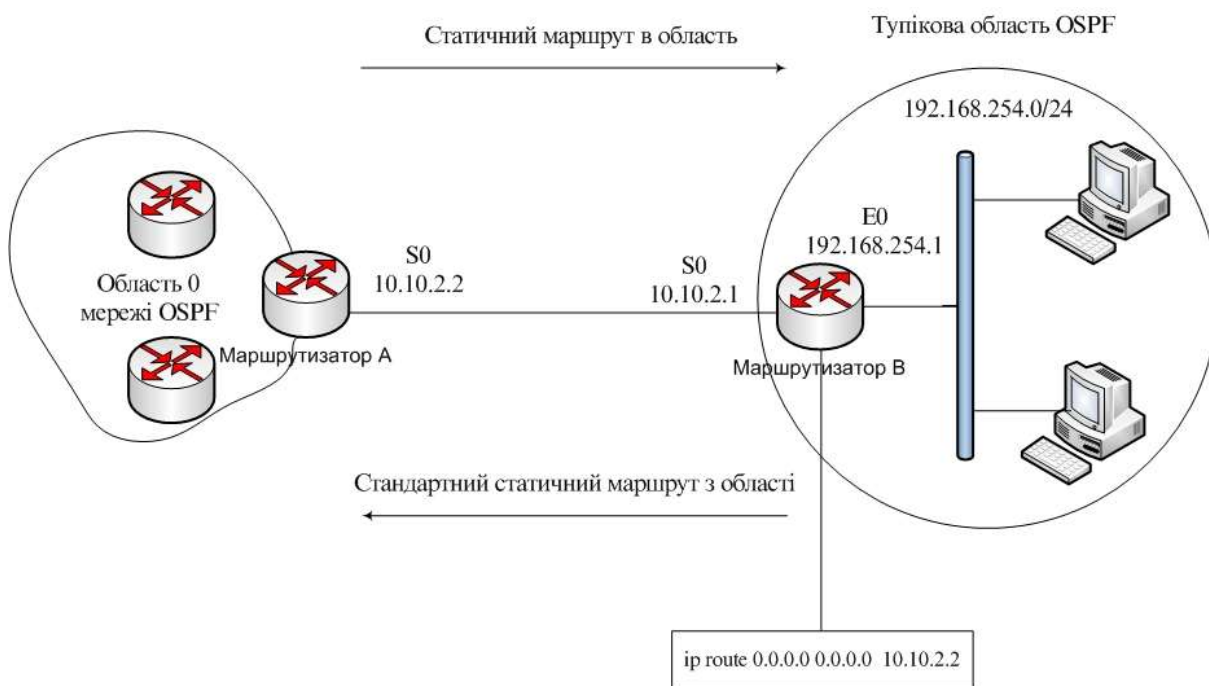


Рисунок 3.2 – Приклад використання стандартного маршруту

Як показано на рис. 3.2, весь трафік, отриманий маршрутизатором В і що не відноситься до мережі E0 з адресою 192.168.254.0/24, перенаправляється в інтерфейс S0 маршрутизатор

– *Динамічна маршрутизація*. Це спосіб маршрутизації, в якому використовуються алгоритми маршрутизації для аналізу вхідних повідомлень з



оновленнями маршрутів, що поступають від одного або декількох маршрутизуючих протоколів, в цілях визначення оптимального маршруту до отримувача. Найбільшою перевагою способу маршрутизації такого типу є те, що він дозволяє автоматично пристосовуватися до змін в топології мережі.

### **3.1.2 Порівняння протоколів маршрутизації з врахуванням стану каналів і протоколів дистанційно-векторної маршрутизації**

Опишемо два найширше вживаних і загально визнаних маршрутизуючих протоколи, призначених для використання у поєднанні з набором протоколів «TCP/IP, – RIP і OSPF». У дискусіях з приводу того, які алгоритми маршрутизації (що враховують стан каналів або дистанційно-векторні) є найкращими, остання крапка ще не поставлена.

Найпростіше можна зрозуміти, як діє технологія, в якій враховується стан каналів, якщо уявити собі, що мережа – це велика мозаїка; кількість фрагментів в цій мозаїці залежить від розмірів мережі. На кожному фрагменті мозаїки змальований лише один маршрутизатор або одна локальна мережа. Кожен маршрутизатор "малює" себе на фрагменті мозаїки, показуючи на ньому стрілки, які ведуть до інших маршрутизаторів і локальних мереж. Після цього такі фрагменти з інформацією тиражуються і розсилаються по мережі від одного маршрутизатора до іншого (за допомогою анонсів LSA) до тих пір, поки кожен маршрутизатор не отримує повну і точну копію кожного фрагмента мозаїки. Потім кожен маршрутизатор збирає в своїй пам'яті ці фрагменти за допомогою алгоритму SPF.

Основний принцип маршрутизації коли всі маршрутизатори, що належать до однієї області, підтримують ідентичні копії схеми топології мережі. На основі цієї схеми кожен маршрутизатор виконує ряд обчислень для визначення оптимальних маршрутів. Інформація про топологію мережі міститься в базі даних про стан каналів кожен запис якої представляє інформацію про канали до конкретного вузла в мережі.

Кожен запис містить перераховану нижче інформацію [13-14].

- Ідентифікатор інтерфейсу.
- Номер каналу.
- Дані про метрику, в яких враховується стан каналу.

Володіючи цією інформацією, кожен маршрутизатор може швидко обчислити, найкоротші маршрути, які починаються з нього і проходять до всіх інших маршрутизаторів.

Алгоритм SPF дозволяє визначити, яким чином складаються один з одним різні фрагменти мозаїки. На рисунку 3.3 показано, як в цілому діють всі ці компоненти протоколу маршрутизації з врахуванням стану каналів.

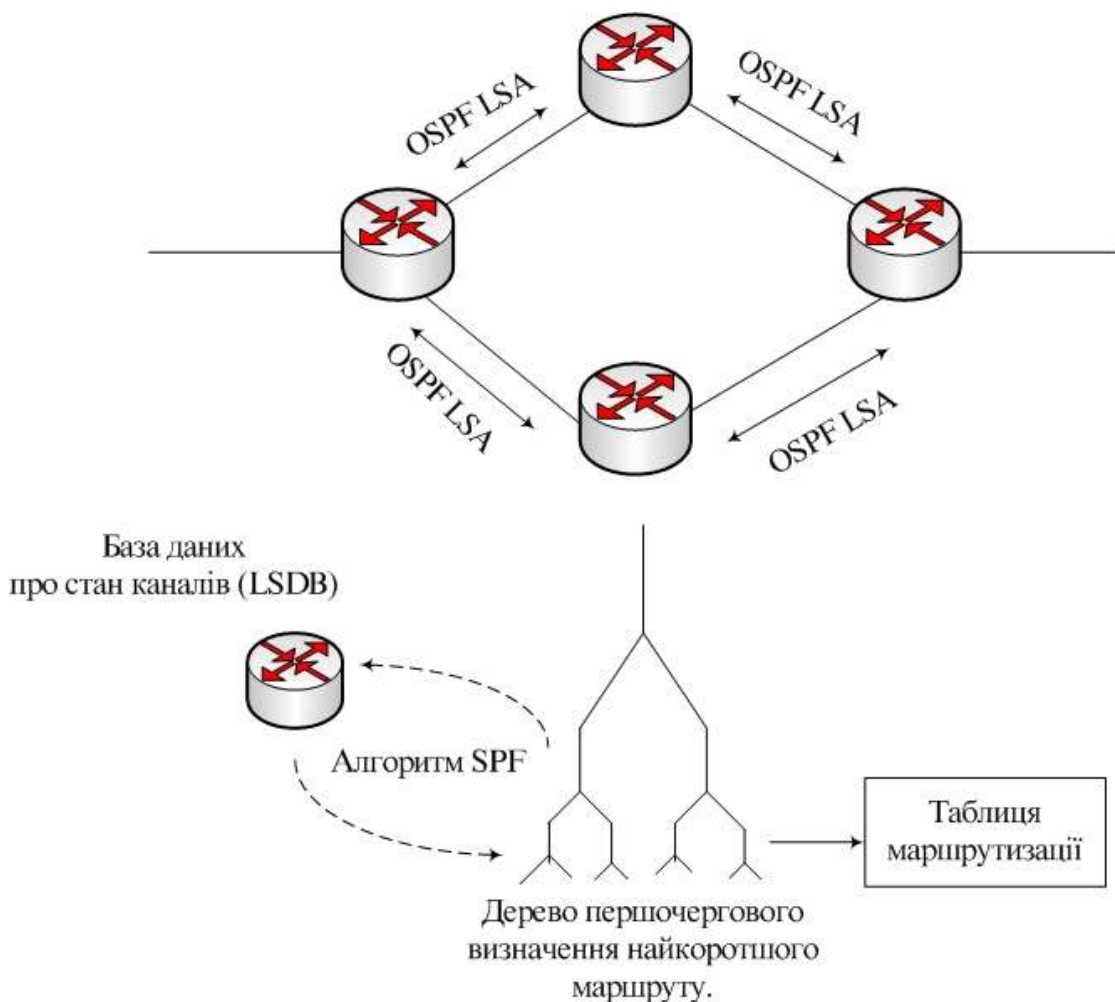


Рисунок 3.3 – Принципи функціонування протоколу маршрутизації з врахуванням стану каналів

Такі як OSPF, передбачають лавинну розсилку маршрутизаторами маршрутної інформації у вигляді пакетів з даними про стан каналів відразу після їх переходу в активний стан. А в мережі, що знаходиться в сталому стані, за допомогою пакетів з даними про стан каналів передаються лише невеликі оновлення.

На рисунку 3.4, кожна зміна в мережі викликає передачу таблиці маршрутизації від одного сусіднього пристрою іншому для того, щоб мережа знову перейшла в сталий стан у відповідь на важливу подію в мережі (таке як зупинка однієї з мереж). Але на цьому рисунку не показано, що у відповідності з цим протоколом сусідні маршрутизатори періодично передають один одному свої таблиці маршрутизації; такий механізм забезпечує подвійний контроль над тим, аби маршрутна інформація в кожному маршрутизаторі була дійсною [15].

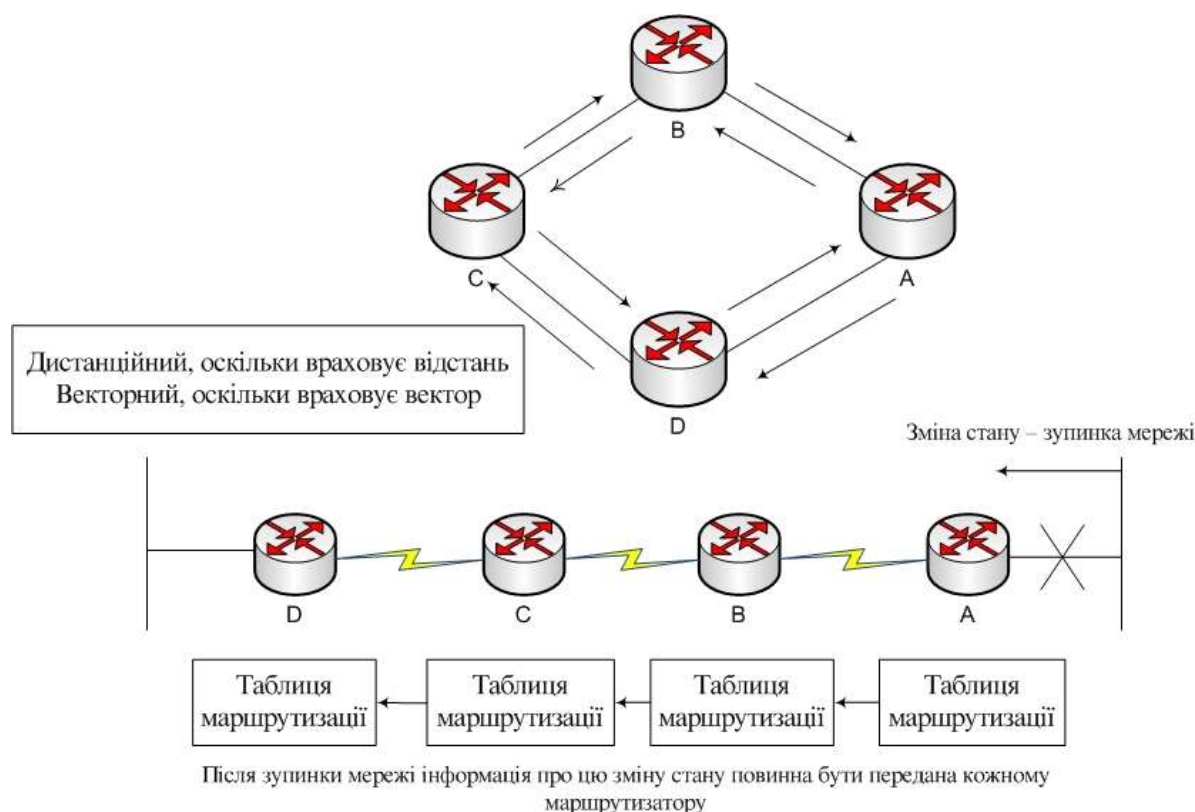


Рисунок 3.4 – «Принципи функціонування дистанційно-векторного протоколу маршрутизації»

### *Характеристики протоколу маршрутної інформації*

Протокол RIP версії 1 – це дистанційно-векторний протокол, розроблений в Берклі (Berkeley) в кінці 1960-х років, який все ще широко застосовується і у наш час. У цьому протоколі передбачено, що маршрутизатор обмінюється тільки маршрутною інформацією, отриманою від підключених до нього сусідніх пристроїв. Основні характеристики протоколу RIP полягають в наступному:

- протокол передбачає розсилку ширококомовних повідомлень через кожні 30 секунд для підтримки цілісності мережі;
- протокол регламентує вживання таблиць маршрутизації, що містять дані про кількість транзитних переходів між маршрутизаторами, і обмежує їх кількість 15 транзитними переходами;
- маршрутизатор, що діє по протоколу RIP, передає всю таблицю маршрутизації кожному безпосередньо підключеному до нього сусідньому маршрутизатору, про яке йому відомо.

### **3.2 Вибір відповідного маршрутизуючого протоколу**

Мережевим проектувальникам і інженерам часто доводиться вирішувати проблему вибору маршрутизуючого протоколу для створюваної ними мережі. Проведемо порівняння двох протоколів маршрутизації з врахуванням стану каналів, – IS-IS і OSPF. Перш ніж приступати до вибору маршрутизуючого протоколу, необхідно розглянути приведені нижче питання.

- Експлуатаційні вимоги. Ці вимоги дозволяють встановити, чи з часом не ускладнюватиметься завдання управління мережею. Експлуатаційні вимоги визначають здатність протоколу адаптуватися до змін, зводити до мінімуму негативні дії на роботу мережі і забезпечувати усунення порушень в роботі.

- Технічні вимоги. Ці вимоги дозволяють визначити, чи здатний даний протокол забезпечити виконання ряду конкретних вимог до мережі.
- Функціональні вимоги. Визначені як регламент і правила функціонування мережі, від яких залежать вирішення по проектуванню мережі. Вимоги такого типу можуть бути пред'явлені будь-яким підрозділом компанії і часто стають ключем до успішного створення мережі [17].

### **3.3 Огляд алгоритму SPF**

#### **3.3.1 Опис алгоритму SPF у дії**

В мережі ARPAnet використовувався також один з перших дистанційно-векторних маршрутизуючих протоколів. Розвиток цього протоколу привів до створення RIP – протоколу, який застосовується і в даний час. Але в міру зростання мереж, в яких використовується протокол RIP, виявляються серйозні обмеження. Тому виникла необхідність в створенні нового протоколу, здатного функціонувати в межах окремої автономної системи і володіє здатністю охоплювати всю більшу кількість хостів (масштабування мережі, що надає можливість) для створення крупної мережі, що складається з багатьох маршрутизаторів і мережевих каналів.

В рамках цієї тенденції була розроблена версія 1 протоколу OSPF, опублікована у вигляді документа RFC 1131 в жовтні 1989 року робочою групою OSPF Working Group організації IETF. В протоколі OSPF був застосований знаменитий алгоритм Дейкстри. Цей алгоритм не був новим і не розроблявся спеціально для вирішення тієї задачі, яка стала перед всім мережевим співтовариством. Дейкстрі спочатку розробив свій математичний алгоритм в 1956 році, за 30 років до того, як почалося створення протоколу OSPF, для демонстрації можливостей комп'ютера ARMAC

Едсгер В. Дейкстра (Edsger W. Dijkstra) народився в 1930 році в Роттердаме, Голландія. Його сім'я надавала велике значення заняттям наукою, тому Едсгер, володіючи неабиякими здібностями, швидко досяг перших успіхів

і в 1959 році отримав ступінь доктора філософії по комп'ютерних науках в Амстердамському університеті. У віці 32 років Дейкстра вже обіймав в Ейндховенському університеті посаду професора по математиці, що має докторську ступінь. Його досягнення залишаються надзвичайно вражаючими і в наші дні.

Дейкстрі вніс великий вклад до розвитку комп'ютерних наук, але самим цікавим його досягненням з'явився алгоритм, особливо алгоритм обчислення короткого маршруту. В той час Дейкстра не розглядав розроблений ним алгоритм як заслуговуючий особливої уваги, тому пройшло багато років, перш ніж він був опублікований. В даний час алгоритм Дейкстри застосовується в дорожньому будівництві, в маршрутизації трафіку зв'язку і в організації повітряного руху. Одна з модифікацій цього алгоритму застосовується навіть для визначення найменш дорогої схеми прокладки дротів в комп'ютері. Як було початково вказано в статті Едсгера Дейкстри з описом цього алгоритму, призначення алгоритму обчислення найкоротшого маршруту полягає в пошуку найкоротшого маршруту між двома точками через ряд вузлів. Але в маршрутизації під терміном вузол мається на увазі маршрутизатор.

Для опису в основних рисах роботи першочергового вибору найкоротшого маршруту розглянемо наступний приклад.

Передбачимо, що потрібно знайти маршрут між містами Ролі і Бостон, який потребує менше всього часу. Між цими містами є ряд інших міст (які розглядаються як аналоги проміжних маршрутизаторів), де може бути отримана інформація про найкращий місцевий маршрут до кінцевого пункту призначення [18].

Передбачимо, що в даному прикладі необхідно визначити найкоротший (що має мінімальну вартість) маршрут, який потрібний для переміщення в Бостон, шляхом вивчення в процесі цього пошуку кожної автодороги (аналог каналу зв'язку), що виходить з кожного нового міста. Як відомо, деякі дороги (канали) кращі за інших. Їх перевагою може бути те, що вони допускають рух з вищою швидкістю, мають більше смуг або менш завантажені. Для визначення

найкоротшої (що дозволяє найшвидше добратися до місця призначення) дороги (маршруту) від Ролі ка Бостона привласнимо кожній автодорозі (каналу) числове значення, яке характеризує швидкість проходження відповідної нею ділянки маршруту.

Оскільки комп'ютери оперують лише цифрами і не можуть враховувати особисті побажання відносно вибору того або іншого маршруту, аби забезпечити функціонування алгоритму, необхідно привласнити відповідні значення ділянкам дороги вручну. Зокрема, маршрутизатор може керуватися тим, що маршрут із вартістю 50 є ефективнішим, ніж маршрут з вартістю 100.

В даному прикладі йдеться про використання протоколу OSPF, тому припустимо, що для збору всієї інформації про канали, необхідної для визначення короткого маршруту від Ролі ка Бостона, застосовується протокол OSPF. Потім за допомогою алгоритму SPF обчислюється найкоротший маршрут (рисунок 3.5). Нижче описана процедура вибору маршруту, що характеризується мінімальним значенням часу (найкоротшого маршруту).

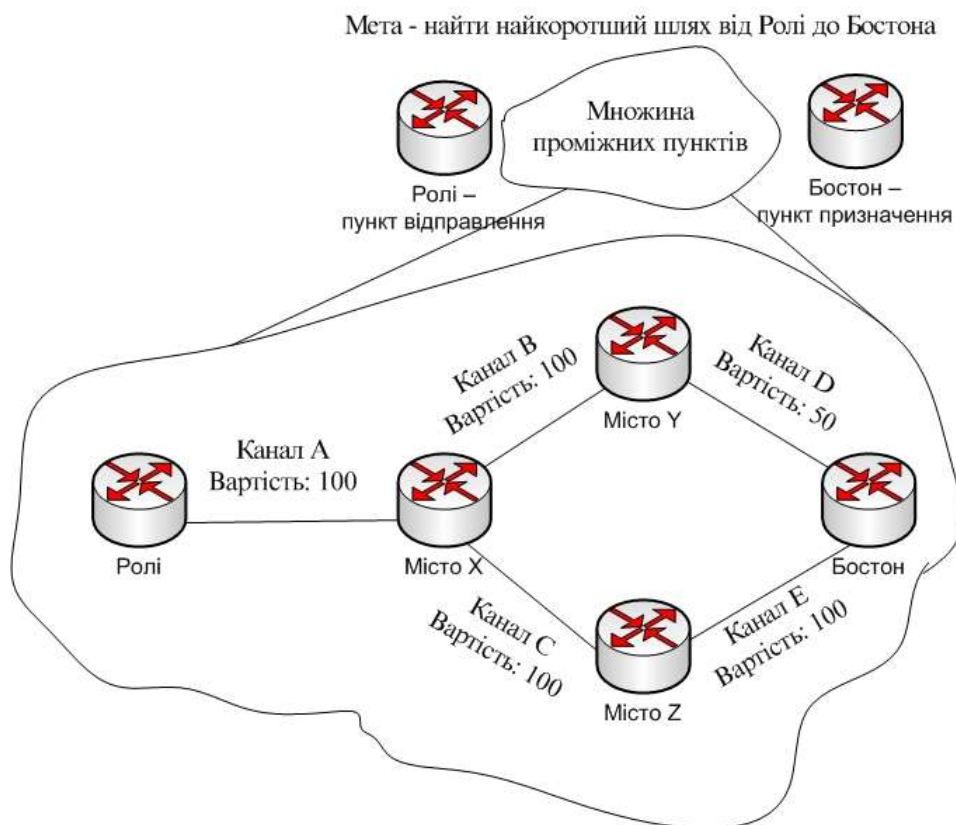


Рисунок 3.5 – Приклад використання алгоритму SPF

1. Почати з міста, що є відправною точкою маршруту (Ролі). Час (вартість маршруту), необхідний для досягнення міста Ролі, рівний 0 (оскільки ми в ньому вже знаходимося).

2. В маршруті (Ролі) отримана (за допомогою протоколу OSPF) інформація про те, що до Бостона веде єдине з'єднання з іншим містом. Це з'єднання з містом X має вартість 100, оскільки воно відповідає хорошій дорозі з двома смугами руху. Помістимо цю інформацію про канал в базу даних для майбутніх довідок, як показано нижче [29].

Канал A; вартість 100; веде в місто X; канал знаходиться в робочому стані.

3. Маршрутизатор, що знаходиться в місті X, повідомляє, що з цього міста виходять дві дороги. Після перевірки відповідних каналів по протоколу OSPF отримана наступна інформація [29]:

Канал A; вартість 100; веде в місто Y; канал знаходиться в робочому стані.

Канал C; вартість 100; веде в місто Z; канал знаходиться в робочому стані.

Ці два записи поміщаються в базу даних, і продовжується пошук маршруту, ведучого в Бостон.

4. Маршрутизатор, що знаходиться в місті Y, повідомляє, що у нього є з'єднання з Бостоном через нову швидкісну автомагістраль; ця інформація також поміщається в базу даних, як показано нижче.

Канал D; вартість 50; веде в Бостон; канал знаходиться в робочому стані.

5. До цього моменту стало також відомо, що один канал до Бостона є і в місті Z.

Канал E; вартість 100; веде в Бостон; канал знаходиться в робочому стані.

6. Оскільки до Бостона ведуть два канали, алгоритм SPF повинен обчислити, який з них відповідає найкоротшому маршруту.



7.Маршрутизатор OSPF звертається до своєї бази даних. (Оскільки в цій базі даних накопичується інформація про багато каналів, у тому числі про їх вартості і про стан, зокрема про те, чи є кожен з них работоздатним або зупиненим, її прийнято називати базою даних про стан каналів, або базою даних про топологію.)

8.Маршрутизатор OSPF виявив два маршрути, ведучих в Бостон, а тепер повинен визначити, який з них повинен використовуватися. За інформацією, яка є в базі даних, не можна безпосередньо визначити найкоротший маршрут. Але таке завдання дозволяє вирішити алгоритм SPF, який застосовується в маршрутизаторі OSPF.

9.На даному етапі маршрутизатор OSPF викликає на виконання алгоритм SPF і формує схему всіх каналів від Ролі до Бостона. Цю схему можна розглядати як дерево, в якому Ролі є коренем (знаходиться в основі дерева), а вітки (канали) ведуть до багатьох міст (одержувачам).

Але комп'ютер не розглядає красиве зображення дерева, а виконує математичні розрахунки по обробці представленої з його допомогою інформації.

Після цього, відповідно до алгоритму SPF, ці два значення порівнюються для визначення того, який з них є найкоротшим, аби по ньому можна було відправитися в Бостон (передати туди пакет). Алгоритм SPF показує, що має бути вибраний маршрут 1, оскільки він має нижчу загальну вартість в порівнянні з маршрутом 2.

9. Формулюється вивід, що найкоротшим є маршрут 1.

10. Після цього маршрут 1 вводиться в пам'ять комп'ютера автомобіля (у таблицю маршрутизації), аби водій міг визначити, як дістатися до Бостона (або відправити пакет) по найкоротшому зі всіх можливих маршрутів.

Цей приклад наочно показує, чому алгоритм SPF носить таку назву. Ще одним важливим аспектом його функціонування є те, що він забезпечує перехід мережі з одного сталого стану в інший. Зокрема, якби в умовах попереднього прикладу вийшов з ладу канал між містом X і Бостоном, то умови передачі

трафіку в мережі змінилися б корінним чином. Алгоритм SPF дозволяє це врахувати і перенаправити трафік (пакети) по іншому маршруту, через місто Z. Процес, в ході якого формуються маршрути, відповідні поточному стану мережі, називається переходом мережі в сталий стан.

По суті, перехід мережі в сталий стан при використанні протоколу OSPF відбувається в середньому протягом  $O(M \cdot \log M)$  ітерацій, де M- кількість каналів. Такі показники набагато кращі в порівнянні з дистанційно-векторним алгоритмом Беллмана-Форда, який забезпечує «перехід мережі в сталий стан протягом  $O(N \cdot M)$  ітерацій, де N- кількість вузлів» [20].

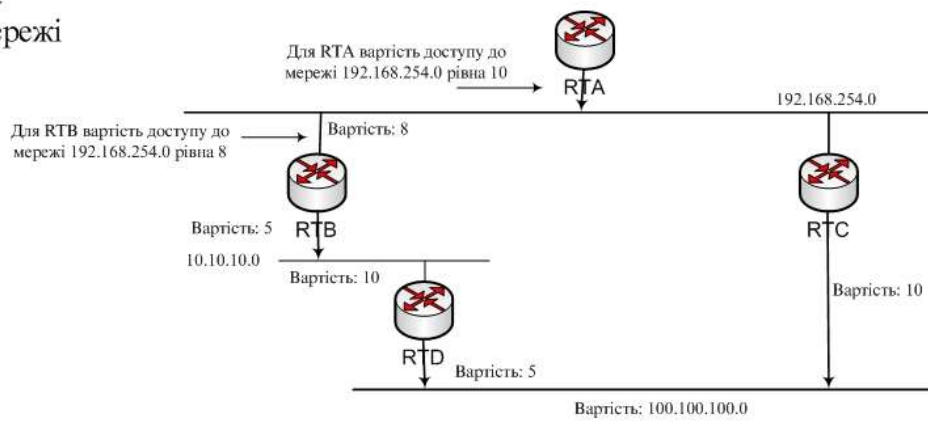
#### *Призначення алгоритму SPF.*

Передбачимо, що є мережа (див. рисунок 3.6) з вказаними вартостями інтерфейсів. Аби сформувати дерево найкоротших маршрутів для маршрутизатора RTA, необхідно зробити його коренем дерева і обчислити мінімальну вартість маршруту до кожного одержувача.

На рис. 3.6 показано, як виглядає мережа, що розглядається з позицій маршрутизатора RTA. Звернемо увагу на напрям стрілок з позначенням вартості. Наприклад, вартість інтерфейсу маршрутизатора RTB до мережі «192.168.254.0» не грає ролі при обчисленні вартості інтерфейсу до мережі «10.10.10.0». Маршрутизатор RTA може передати пакет в мережу «10.10.10.0» через RTB по маршруту з вартістю 15 (10+5). Крім того, RTA може передати пакет в мережу 100.100.100.0 по маршруту через маршрутизатор RTC, з вартістю 20 (10+10), або через маршрутизатор RTB, із вартістю 20 (10+5+5). В тому випадку, якщо до одного і тому ж одержувача ведуть маршрути з однаковою вартістю, в реалізації OSPF компанії Cisco передбачено розподіл навантаження по таких маршрутах, кількість яких може досягати шести.

Після формування дерева найкоротших маршрутів маршрутизатор приступає до підготовки відповідної цьому дереву таблиці маршрутизації. Безпосередньо підключені мережі є досяжними за допомогою метрики (вартості), рівної 0, а інші мережі можна досягти по маршруту з вартістю, обчисленою на основі дерева.

## Фізична топологія мережі



## Логічне представлення дерева SPF

Для RTB вартість доступу до цієї мережі рівна 15

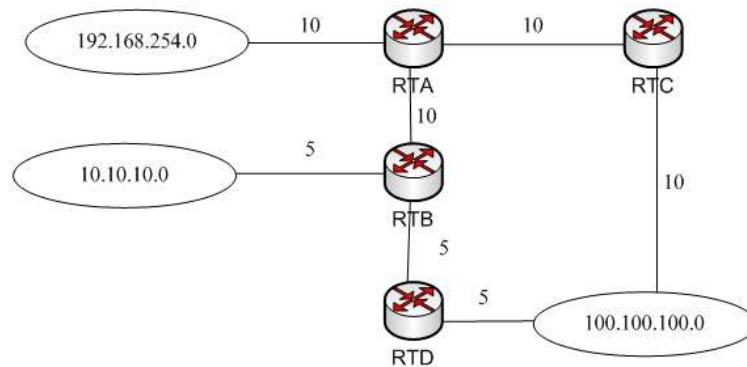


Рисунок 3.6 – Приклад, що показує, в чому полягає призначення алгоритму SPF

Історія створення протоколу OSPF описана нижче, але перш ніж приступити до опису цієї теми, необхідно розглянути основні особливості протоколу OSPF. Спочатку необхідно відзначити, що цей протокол відомий під багатьма назвами і має багато характеристик, які коротко перераховані нижче і можуть служити введенням до опису складніших понять.

*Повні і часткові обчислення по алгоритму SPF [21].*

Реалізація алгоритму SPF, передбачена компанією Cisco Systems, дозволяє використовувати прискорені способи обчислення маршрутів. Така можливість привела до появи двох типів обчислень по алгоритму SPF – повного і часткового.

Повні обчислення по алгоритму SPF виконуються лише за наявності змін в топології, представлених у вигляді анонса стану каналів (LSA), переданого маршрутизатором, а не сумарного анонса LSA. Сумарні анонси LSA викликають виконання часткового обчислення по алгоритму SPF.

В протоколі OSPF передбачено, що часткові обчислення по алгоритму SPF відносяться лише до змін, виражених в зовнішніх і сумарних анонсах LSA. По суті, часткові обчислення по алгоритму SPF здійснюються, лише якщо происходять мимовільні зміни маршруту до мережі, які відбиваються в зовнішніх або сумарних анонсах LSA. Іншими словами, часткові обчислення по алгоритму SPF відбуваються, якщо топологія області не змінюється, але відбувається самовипадкова зміна деякого префікса IP.

Зміна префікса IP всередині області викликає повне повторне обчислення по алгоритму SPF.

#### *Перевірка функціонування алгоритму SPF*

Як було описано вище, в мережі може виникати необхідність контролювати лавинну розсилку, що виконується за допомогою протоколу OSPF. Справа в тому, що повторне обчислення по алгоритму SPF може статися після здобуття будь-якого анонса LSA. Роботу протоколу OSPF можна проконтролювати, викликавши на виконання команду «show ip ospf process id». Ця команда може використовуватися для визначення кількості випадків виконання алгоритму SPF. Вона також показує значення тайм-ауту оновлення інформації про стан каналів, який застосовується за умови, що відсутні зміни в топології.

Крім того, для контролю за виконанням часткового обчислення по алгоритму SPF можна використовувати команду «debug ip ospf spf inter або debug ip ospf spf external», оскільки при цьому розглядаються лише зміни, викликані сумарними або зовнішніми анонсами LSA. Може бути також вказаний список доступу для перегляду лише тих обчислень, які відносяться до анонса LSA з конкретним ідентифікатором LSA.

### **3.4 Ієрархія маршрутизації OSPF**

Однією з найважливіших переваг протоколу OSPF є його здатність використовувати ієрархічну структуру маршрутизації. Вивчаючи особливості

застосування протоколу OSPF в ієрархічній структурі такого типу, необхідно враховувати наступні його характеристики [27]:

- для правильного функціонування OSPF повинна існувати або бути створена структура;
- інформація, задана у вигляді явної топологічної структури, вважається більш важливою, ніж задана за допомогою адресації.

Будь-яка автономна система є групою областей, в яких застосовується загальна стратегія маршрутизації, що відносяться до загального домена адміністрування. Автономні системи позначаються унікальним номером. Номери автономних систем можуть бути відкритими або закритими, залежно від потреби конкретної мережі. Номери автономних систем привласнюються організаціями ARIN в Північній Америці, RIPE – в Європі і APNIC – в Азії. Для використання OSPF номер автономної системи не потрібний, оскільки підприємство, що має єдиний вихід в Internet, розглядаються як частина автономної системи провайдера Internet, до якої вони примикають.

#### **3.4.1 Методи проектування ієрархічних мереж**

При створенні мережі OSPF використовуються перераховані нижче критерії якості проекту, які обґрунтовані сучасними теоріями проектування мереж:

- підхід, що передбачає використання трирівневої опорної мережі, «забезпечує швидкий перехід мережі» в стані перебування і зменшення відносно кількості хостов на кожному рівні.
- кількість проміжних транзитних переходів між маршрутизаторами в будь-якому маршруті від відправника до одержувача не повинно перевищувати шести.
- кількість маршрутизаторів в кожній області повинно знаходитися в межах від 30 до 100. (Ці цифри можуть змінюватися залежно від перерахованих нижче чинників.)

– окрім з'єднання з областю 0, будь-який «граничний маршрутизатор області (ABR)» не повинен мати з'єднання більше ніж з двома областями. В протилежному випадку кількість баз даних з інформацією про стан каналів, за якими повинен стежити маршрутизатор ABR, буде дуже велике [27].

### 3.4.2 Маршрутизації в мережі OSPF

В мережі OSPF можуть використовуватися маршрути наступних трьох типів [27]:

- внутріобласні;
- міжобласні;
- зовнішні.

Загальні описи маршрутів цих типів приведені нижче.

#### *Внутріобласна маршрутизація.*

Внутріобласними називаються маршрути до одержувачів, що знаходяться в межах тієї ж логічної області OSPF, де знаходяться відправники. Інформація про внутріобласні маршрути OSPF передається за допомогою анонсів LSA, що відносяться до маршрутизаторів (анонсів типу 1) і до мережі (анонсів типу 2). У лістингах команд, які виводять таблиці маршрутизації OSPF на зовнішній пристрій, внутріобласні маршрути позначені буквою "o".

#### *Міжобласна маршрутизація.*

Міжобласними називаються маршрути, які проходять між двома або декількома областями OSPF. Інформація про маршрути цих типів передається в сумарних анонсах LSA, які відносяться до мережі (анонсах типу 3). При маршрутизації пакетів між двома областями, відмінними від опорної, використовується опорна область. Це означає, що в процесі міжобласної маршрутизації частково застосовується внутріобласна маршрутизація, як показано нижче.

1. Для передачі пакету від маршрутизатора відправника до граничного маршрутизатора області використовується внутріобласний маршрут.

2.Для прокладки маршруту від області відправника до області одержувача використовується опорна область.

3.Для передачі пакету від граничного маршрутизатора області одержувача до маршрутизатора одержувача використовується внутріобласний маршрут.

Міжобласний маршрут створюється в результаті з'єднання всіх цих трьох маршрутів. Безумовно, алгоритм SPF забезпечує визначення маршруту з мінімальною вартістю між цими двома точками. В лістингах команд, які виводять таблиці маршрутизації OSPF на зовнішній пристрій, маршрути цього типу позначені буквами "O IA".

Типи зовнішніх маршрутів, використовуваних в протоколі OSPF, перераховані нижче.

– Маршрути E1. Вартості маршрутів E1 дорівнюють сумі внутрішньої і зовнішньої (віддаленої автономної системи) метрик OSPF. Наприклад, якщо пакет призначений для іншої автономної системи, для маршруту E1 береться метрика віддаленої автономної системи і з нею складаються всі внутрішні вартості OSPF. Ці маршрути в таблиці маршрутизації OSPF позначаються як E1.

– Маршрути E2. Маршрути E2 є зовнішніми маршрутами, які застосовуються для OSPF за умовчанням. У них не передбачено складання з внутрішніми метриками OSPF; використовується лише метрика віддаленої автономної системи, незалежно від того, де вони проходять в даній автономній системі. Наприклад, якщо пакет призначений для іншої автономної системи, із значеннями метрики маршрутів E2 складаються лише значення метрики відповідного маршруту від автономної системи одержувача, по якому пакет передається до одержувача.

### **3.4.3 Области OSPF**

Области аналогічні підмережам в тому, що дозволяють легко підсумовувати інформацію про маршрути, що відносяться до них, і мережі.

Іншими словами, області є суміжними логічними сегментами мережі. Якщо в протоколі OSPF використовуються області, мережею стає простіше управляти і спостерігається помітна скорочення трафіку маршрутизації. Ці переваги досягаються завдяки тому, що топологія області стає невидимою для інших маршрутизаторів, що знаходяться за межами цієї області [27-29].

Як правило, в міру розширення мережі і збільшення в ній кількості вузлів протокол OSPF втрачає свої переваги. Зокрема, в результаті збільшення розмірів мережі і зростання кількості маршрутизаторів збільшуються розміри «бази даних про стан каналів», і настає такий момент, що робота протоколу OSPF стає неефективною.

Крім того, лавинна розсилка анонсів LSA багаточисельними маршрутизаторами може також викликати проблеми, пов'язані із заторможеністю. Для вирішення цих проблем після достатнього збільшення автономних систем їх необхідно сегментувати на декілька областей. При цьому, групуючи маршрутизатори по областях, слід враховувати, що число маршрутизаторів в області належить знаходитися в певних межах. При дотриманні цієї вимоги база даних про стан каналів, в якій представлена інформація про кожен маршрутизатор області, матиме розумні розміри, що сприяє істотному підвищенню ефективності мережі OSPF.

Області NSSA можуть застосовуватися в тих випадках, якщо в мережі відсутній транзитний канал Internet і в тупиковій області доводиться поширювати інформацію про традиційну мережу RIP, але все ще є єдина точка виходу в інші області OSPF. Області NSSA знаходять широке поширення, оскільки багато пристроїв не підтримують (або погано підтримують) OSPF, але здатні працювати під управлінням протоколу RIP.





Рисунок 3.7 – Приклад топології мережі з областю NSSA

Типова топологія мережі з областю NSSA приведена на рисунку 3.7.

### 3.5 Експлуатаційне середовище OSPF

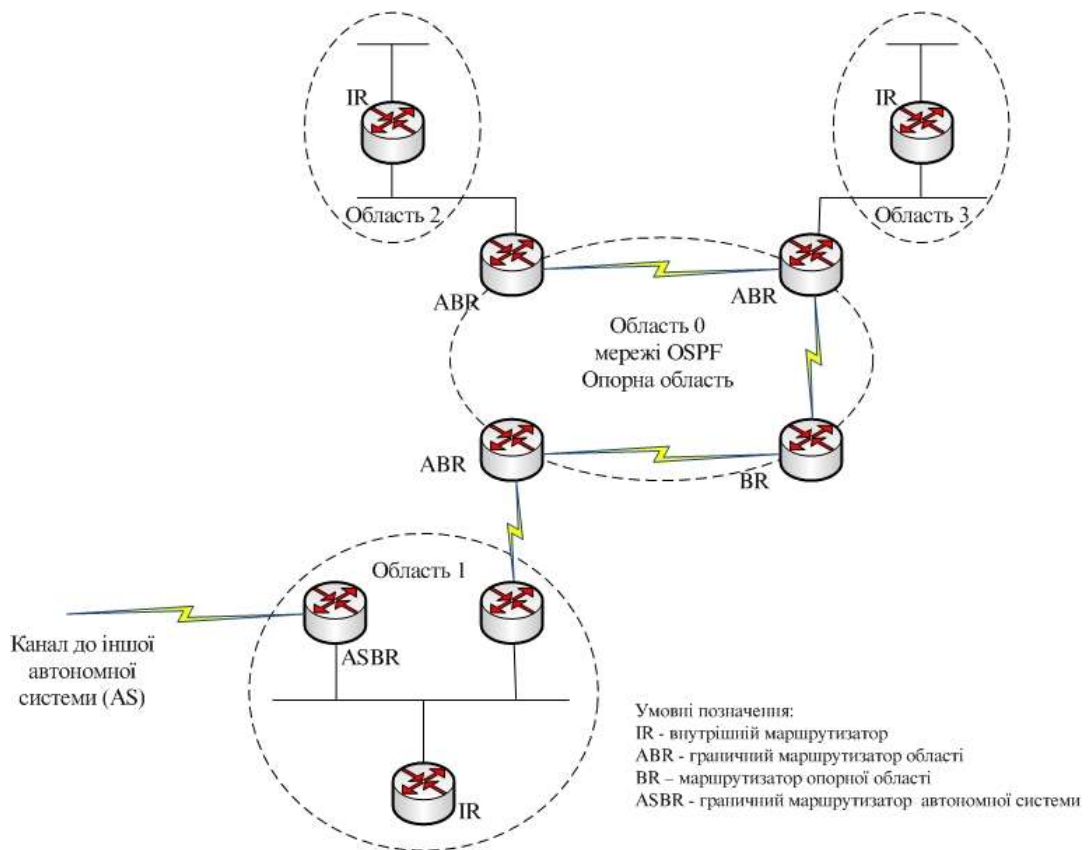
Опишемо основні характеристики і засоби експлуатаційного середовища OSPF. Середовище, в якому діє протокол OSPF, визначається можливостями і характеристиками його експлуатації і проектування. Іншими словами, експлуатаційне середовище OSPF можна визначити як мережеву архітектуру, в якій цей протокол може функціонувати належним чином.

В документі «RFC 1793, Extending OSPF to Support Demand Circuits», наведений приклад того, які складнощі доводиться долати, реалізуючи за допомогою OSPF можливість експлуатувати в мережі канали, що активізуються на вимогу. До того як був опублікований і реалізований цей документ RFC, протокол OSPF не діяв належним чином стосовно таких каналів, як ISDN. Тепер, після внесення в протокол доповнень, що забезпечують його правильне функціонування стосовно каналів, що активізуються на вимогу, функціональне середовище цього протоколу значно розширилося [29].

### 3.5.1 Типи маршрутизаторів OSPF

Чотири різні типи маршрутизаторів OSPF відповідають ієрархічній структурі маршрутизації, вживаної в OSPF. Кожен маршрутизатор в цій ієрархії виконує унікальну роль і володіє набором властивих лише йому характеристик. На рисунку 3.9 показана типова мережа OSPF, в якій декілька областей містять маршрутизатори OSPF різних типів.

Загальний опис маршрутизаторів OSPF чотирьох типів приведений нище.



Рсиунок 3.8 – Типи маршрутизаторів OSPF

Кожен маршрутизатор в автономній системі має відомості про те, як звернутися до кожного маршрутизатора ASBR в цій автономній системі. В маршрутизаторах ASBR одночасно експлуатуються протокол OSPF і інший маршрутизуючий протокол, такий як RIP або BGP. Маршрутизатори ASBR повинні знаходитися в області OSPF, відмінній від тупикової.

Маршрутизатори ASBR обробляють інформацію про зовнішні маршрути. Один із способів налаштування конфігурації або активізації в OSPF маршрутизатора ASBR полягає у використанні команди «redistribute static або redistribute connected в процесі маршрутизації OSPF».

Маршрутизаторами опорної області (Backbone Router – BR) називаються маршрутизатори, інтерфейси яких сполучають їх лише з опорною областю.

### **3.5.2 Типи мереж OSPF**

На рисунку 3.9 показано чотири різних типи мереж, в яких застосовується протокол OSPF [29].

Характеристики типів мереж OSPF (рис. 3.9) перераховані нижче.

– «Широкомовна мережа». Стосунки сусідства формуються з використанням вітальних повідомлень OSPF.

– «Неширокомовна мережа з множинним доступом» (NBMA). В мережах NBMA широкомовна розсилка не дозволена за умовчанням. До мереж такого типу відносяться Frame Relay, АТМ і Х.25. В мережах NBMA також можуть встановлюватися багаточисельні стосунки суміжності, але оскільки не у всіх мережах такого типу вирішується використання широкомовної розсилки, вони не можуть гарантувати правильне формування таких стосунків.

– Багатоточкова мережа. Дозволяє експлуатувати протокол OSPF таким чином, неначебто маршрутизатори були сполучені двоточковими каналами, а не через мережу NBMA. В такій конфігурації не застосовуються «маршрутизатори DR або BDR», оскільки кожен канал розглядається як двоточковий.

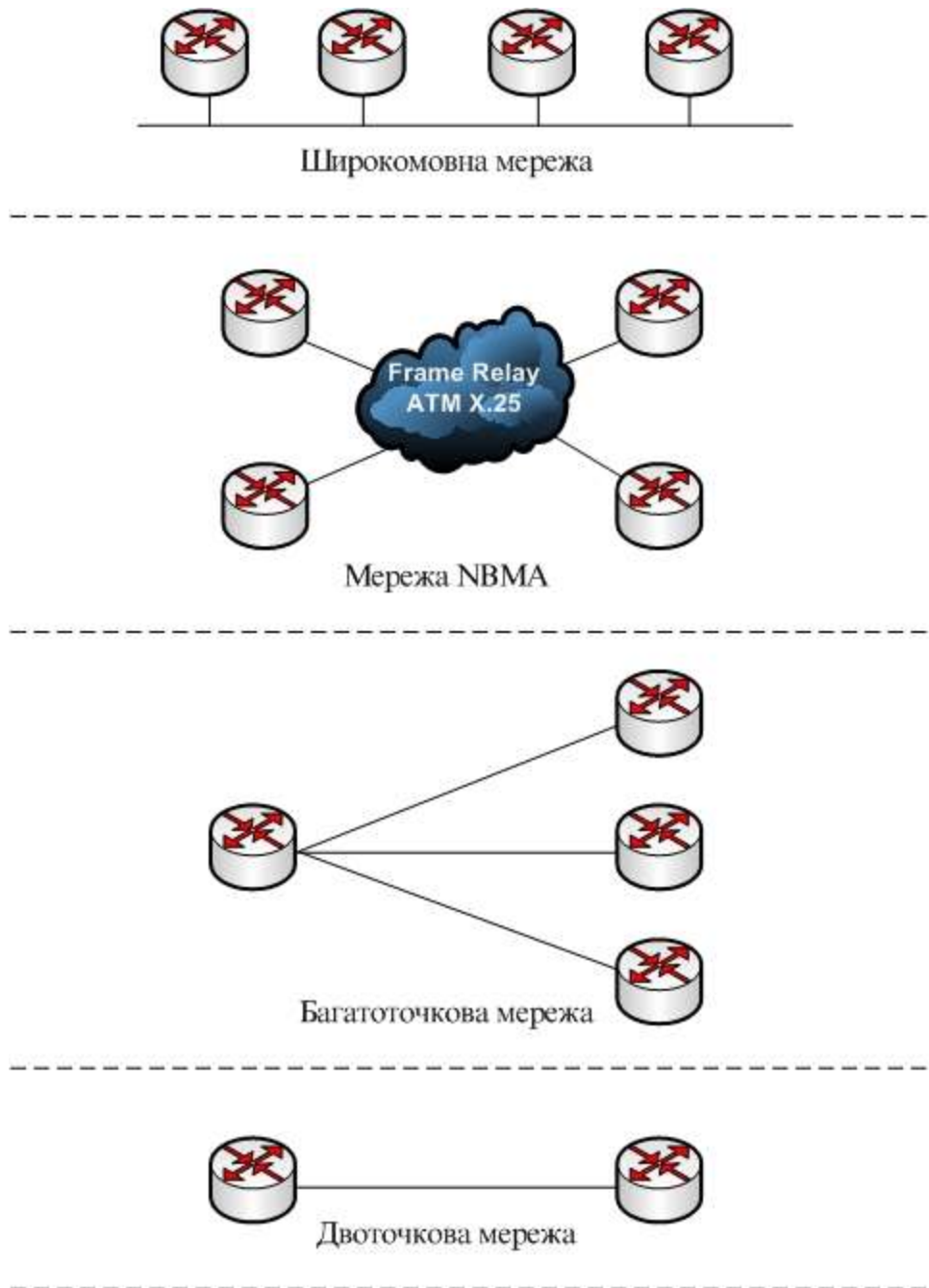


Рисунок 3.9 – Типи мереж OSPF

Введення в конфігурацію інформації про тип мережі OSPF здійснюється на рівні інтерфейсу маршрутизатора.

### 3.5.3 Ідентифікація маршрутизатора

Цей ідентифікаційний номер є унікальним для кожного маршрутизатора OSPF. Мережевий інженер може використовувати декілька методів для

визначення того, яким чином в мережі повинні призначатися ідентифікатори RID OSPF.

Для визначення значення RID в мережі OSPF застосовується описаний нижче процес [28].

«Крок 1. Перевірити, чи не був RID встановлений вручну за допомогою команди `ospf router-id`. В разі негативної відповіді перейти до кроку 2.»

«Крок 2. Якщо є інтерфейси петлі зворотного зв'язку, застосувати самий більший з використовуваних IP-адресів інтерфейсів петлі зворотного зв'язку. Якщо є лише одна адреса інтерфейсу петлі зворотного зв'язку, застосувати цей IP-адрес. Якщо інтерфейс петлі зворотного зв'язку відсутній, перейти до наступного кроку.»

«Крок 3. Встановити як ідентифікатор RID найбільшу IP-адресу зі всіх адрес активних інтерфейсів маршрутизатора.»

#### **3.5.4 Сусідні пристрої**

Відповідно до специфікації OSPF два маршрутизатори, що мають інтерфейси інтерфейси, які знаходяться в загальній мережі, називаються сусідніми пристроями. Для маршрутизатора OSPF першим етапом здобуття інформації про мережу, до якої він підключений, і формування таблиці маршрутизації є виявлення своїх сусідніх пристроїв. Процес такого виявлення починається з того, що маршрутизатор нагромаджує зведення про ідентифікаційні номери своїх сусідніх пристроїв за допомогою многоадресатних вітальних пакетів.

Вітальні пакети передаються через кожні 10 секунд в інтерфейсах ширококомовної або двоточнової мережі і через кожні 30 секунд в інтерфейсах мережі NBMA. Вітальні пакети передаються за багатоадресною адресою 224.0.0.5 (яка умовно позначається як `AllSPFRouters` – для всіх маршрутизаторів SPF); це дозволяє всім маршрутизаторам, що діють під управлінням протоколу OSPF, отримувати і обробляти такі вітальні пакети.

Процес встановлення стосунків сусідства починається з того, що один з двох маршрутизаторів, що обмінюються вітальними пакетами, виявляє свій власний ідентифікатор RID у вітальних пакетах іншого маршрутизатора і приступає до узгодження.

### **3.5.5 Стосунки суміжності**

Для формування стосунків суміжності маршрутизатор OSPF повинен спочатку виявити свої сусідні пристрої. Стосунки суміжності формуються для обміну маршрутною інформацією. Стосунки суміжності формують не всі сусідні маршрутизатори. Нижче перераховані різні умови, при дотриманні яких маршрутизатори OSPF формують стосунки суміжності [27].

Стосунки суміжності дозволяють управляти процесом розподілу оновлень маршрутів, оскільки інформацію про оновлення обробляють лише маршрутизатори, суміжні стосовно того маршрутизатора, який відправив це оновлення.

## 4 ПРАКТИЧНА РЕАЛІЗАЦІЯ ДОСЛІДЖЕНЬ

Враховуючи вищенаведене, найкращі параметри щодо збіжності мережі мають протоколи OSPF та EIGRP. В даному розділі опишемо практичне використання маршрутизаторів компанії Cisco, враховуючи, що дані протоколи в основному використовуються обладнанням цієї компанії.

### 4.1 Особливості маршрутизаторів Cisco Systems

Опишемо компоненти маршрутизаторів компанії Cisco Systems [29]:

1. Оперативна пам'ять (ОЗП, RAM). Її основні функції – зберігання таблиць маршрутизації, кеш протоколу ARP (протокол канального рівня, призначений для визначення відповідності між MAC і IP-адресою). Забезпечує зберігання пакетів на інтерфейсах, поки вони ще не почали оброблятися центральним процесором (наприклад, черга захоплених пакетів).

2. «Енергонезалежна пам'ять – NVRAM». Містить резервну або стару копію файлу конфігурації (startup – config). Після виключення живлення або перезавантаження вміст пам'яті НЕ стирається.

3. Flash – пам'ять. Стирана перепрограмовувана пам'ять. Дозволяє оновлювати ПЗ без видобування чіпа на процесорі.

4. «Постійний запам'ятовуючий пристрій (ПЗП, RAM)». Містить мікрокод для початкового завантаження і обслуговування маршрутизатора, тобто ПЗП перевіряє внутрішню цілісність маршрутизатора: процесор, пам'ять і так далі, які є присутніми в модулі; визначає, в якому порядку і звідки завантажити операційну систему. Так само в ПЗП зберігається частина операційної системи Cisco, яка використовується для відновлення файлу образу операційної системи (наприклад, якщо її видалили із flash-пам'яті).

5. Інтерфейс – мережеве з'єднання, через які дані поступають і передаються з пристроєм.

6. Центральний процесор (ЦП). Процесор забезпечує швидку обробку запитів застосувань і служб безпеки.

При включенні живлення на маршрутизаторі Cisco виконуються наступні функції:

1. Перевіряється працездатність усіх компонентів маршрутизатора. Аналогічно перевіряється склад обладнання. Перевірка відбувається на основі команд з ПЗП.

2. Завантаження і виконання коду завантаження (код використовується для подальших дій). Код завантаження є мікрокомандою ПЗП.

3. Код завантаження визначає місцезнаходження ПЗ операційної системи, що запускається. Часто образ ПЗ повинен зберігатися на flash-пам'яті.

4. Далі код завантаження розпаковує ПЗ в ОЗП і запускає його. На деяких маршрутизаторах ПЗ читається відразу із flash-пам'яті, без завантаження в ОЗП, оскільки бракує пам'яті ОЗП.

5. Пошук конфігурації. По замовчуванню (strtp – config) знаходиться в енергозалежній пам'яті.

6. Завантаження конфігурації.

7. Запуск налагодженого ПЗ операційної системи.

Основні функції маршрутизаторів:

1. Читання заголовків пакетів мережевих протоколів, які приймаються у буфер по кожному порту маршрутизатора;

2. Прийняття рішень про подальший маршрут прямування;

3. Підключення локальних мереж до глобальної мережі.

## **4.2 Налаштування маршрутизаторів Cisco**

Маршрутизатори Cisco можна налаштовувати через інтерфейс командного рядка на консолі або віддаленому терміналі.

На маршрутизаторі можна працювати в декількох режимах.



Користувацький режим. В цьому режимі зазвичай перевіряється стан маршрутизатора. Для виходу використовують команду exit.

```
«RouterX>>
```

Привілейований режим. В цьому режимі маршрутизатор налаштовується. Для входу вводиться команда enable, а так само пароль, якщо він є. Для виходу використовують команду disable [29].

```
«RouterX> RouterX>password RouterX>enable RouterX# RouterX#disable RouterX>>
```

Для перегляду списку команд в будь-якому режимі можна ввести знак питання. Так само Cisco IOS дозволяє не вводити команди повністю, наприклад, писати не повністю enable, а enab. Якщо немає іншої команди з таким початком, маршрутизатор відразу зрозуміє команду.

Існує режим глобальної конфігурації, який надає доступ до спеціальних режимів конфігурації маршрутизатора (наприклад, конфігурація інтерфейсу, лінії, протоколу і так далі).

```
«RouterX> RouterX>enable RouterX#configure terminal RouterX(config)#>
```

Приклад налаштування інтерфейсу на маршрутизаторі [29]:

```
«RouterX>>
«RouterX>enable»
«RouterX#configure terminal»
«RouterX(config)#interface fa 0/0 - налаштування певного»
«інтерфейсу»
«RouterX(config - if)#ip address - привласнення IP-адреси і»
«маски»
«192.168.1.1 255.255.255.0»
«RouterX(config - if)#no shutdown - включення інтерфейсу»
```

Для перегляду налаштування на маршрутизаторі існує команда show interface.

При налаштуванні локальної мережі необхідно кожному комп'ютеру в цій мережі присвоїти IP -адрес. Це можна здійснити вручну, але частіше для цього застосовують протокол DHCP. Сам протокол працює за принципом клієнт-сервер. DHCP -сервер виділяє IP -адреса хостам автоматично (привласнює постійну адресу клієнтові), динамічно (адреса виділяється на якийсь проміжок часу) або вручну [29].

```
«RouterX(config)# service dhcp - включення dhcp-сервера»
```

```
«RouterX(config)# ip dhcp pool LAN - оголошуємо пул»
«RouterX(config - pool)# network 192.168.20.0 255.255.255.0»
«RouterX(config - pool)# default - router - вказування шлюзу по»
«замовчуванню 192.168.20.1»
```

Виключення IP-адрес з наданого пулу адрес [29].

```
«RouterX(config - pool)# ip dhcp - виключення однієї адреси»
«excluded - addresses 192.168.0.2»
«RouterX(config - pool)# ip dhcp - виключення діапазону адрес»
«excluded - addresses 192.168.0.128 192.168.0.255»
```

Враховуючи, що краща збіжність притаманна протоколам EIGRP, OSPF, опишемо налаштування маршрутизаторів саме для цих протоколів.

*Налаштування статичної маршрутизації.*

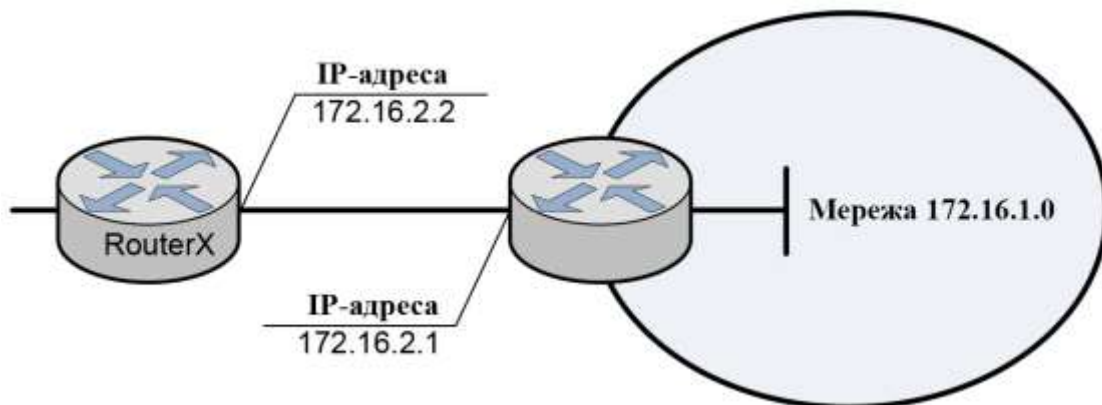


Рисунок 4.1 – Налаштування статичної маршрутизації

```
«RouterX(config)#ip route» – статичний маршрут
«172.16.1.0» – адреса статичного маршруту до мережі
                призначення
«255.255.255.0» – маска підмережі
«172.16.2.1» – адреса наступного переходу
```

*Налаштування протоколу OSPF (див. рисунок 4.2).*

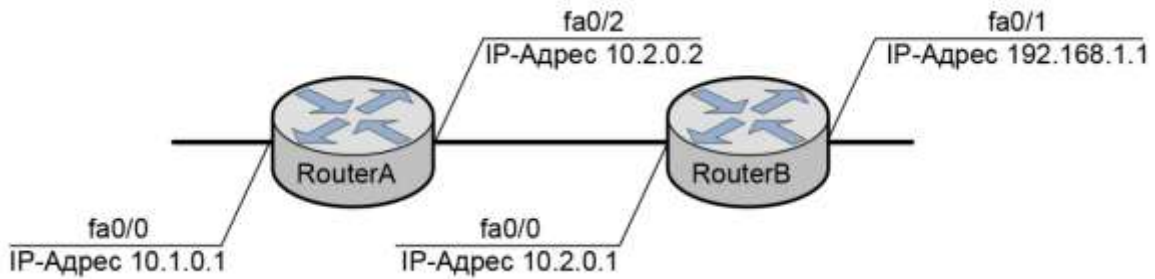


Рисунок 4.2 – Налаштування протоколу OSPF

101 – ідентифікатор процесу маршрутизації, випадковий номер;

10.2.0.1 – адреса інтерфейсу (так само може бути записана адреса мережі або підмережі);

0.0.0.0 – wildcard mask, зворотна маска, яка показує, яка частина (скільки біт) IP -адреса можуть мінятися. 0.0.0.0 – всі біти фіксовані;

Area 0 – ідентифікатор області.

Далі відображається сама таблиця маршрутизації. В ній вказуються усі записи про всі відомі мережі, які так само позначаються буквою коду. У записах з віддаленою мережею, так само є поля з вказуванням адміністративної відстані джерела даних, метрики маршруту, адреси наступного переходу, часу, що пройшов з моменту останнього оновлення, а так само інтерфейсу, через який можна отримати доступ до віддаленої мережі.

```

RouterB#show ip route
...
R   10.1.0.0    [120/1]   via 10.2.0.2    00:00:08, fa0/2
↓
RIP
↓
адмін.від./Метрика
↓
адреса віддаленої мережі
↓
адреса маршруту наступного переходу

```

Рисунок 4.3 – Приклад виведення таблиці маршрутизації

```
«RouterB(config - router)#ip ospf cost cost»
```

Налаштування вартості (метрика від 1 до 65535) маршруту (для цього інтерфейсу) маршрутизації. За відсутності цієї команди вартість для цього інтерфейсу розраховується виходячи з його пропускної спроможності [29].

*Налаштування протоколу EIGRP (рисунок 4.4).*

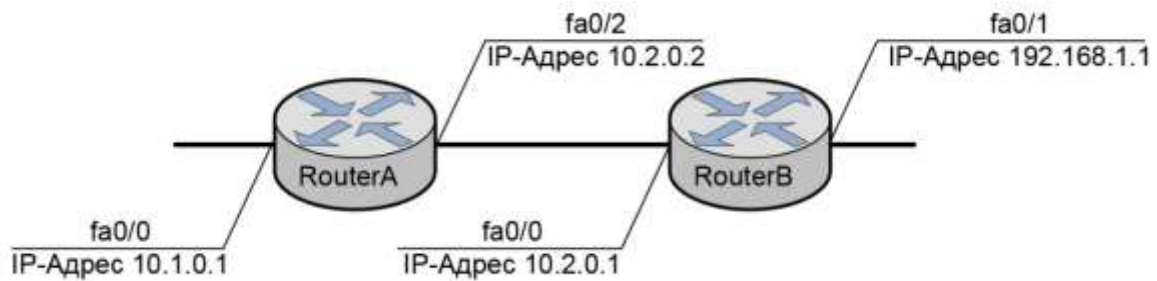


Рисунок 4.4 – Налаштування протоколу EIGRP

100 – номер автономної системи. Номер автономної системи може бути зареєстрованим або приватним. Всі маршрутизатори, які працюють в одній автономній системі, повинні використати один номер автономної системи для обміну інформацією.

По замовчуванню EIGRP виконує балансування навантаження між 4 маршрутами з однаковою метрикою. Для того, щоб відключити балансування навантаження, потрібно встановити кількість маршрутів рівним 1. Зміна кількості маршрутів, між якими виконується балансування навантаження:

```
«RouterX(config - router)# maximum - paths 6»
```

Залежно від того, як маршрутизатор обробляє пакет балансування навантаження, виконується per – packet (для кожного пакету) або perdestination (для кожного адресата).

Балансування навантаження по адресатові призначення означає, що маршрутизатор розподіляє пакети на основі адреси призначення. За наявності двох шляхів доступу до однієї мережі, всі пакети для призначення 1 в цій мережі пересилаються по першому шляху, а усі пакети для призначення 2 в цій

мережі пересилаються по другому шляху і так далі. При цьому зберігається порядок пакетів з потенційно нерівномірним використанням каналів.

Балансування навантаження по пакетах означає, що маршрутизатор відправляє один пакет для призначення 1 по першому шляху, а другий пакет для цього ж призначення 1 по другому шляху і так далі. Балансування навантаження по пакетах гарантує рівномірний розподіл навантаження між усіма каналами. Проте існує ймовірність порушення порядку дотримання пакетів, коли вони досягають адресата призначення, через можливе існування диференціальної затримки в мережі.

EIGRP може розподіляти трафік між декількома маршрутами з різною метрикою. Це регулюється завданням `variance` [29]:

```
«RouterX(config - router)# variance 2»
```

Значення `variance` може бути від 1 до 128. Це множник, на який множитиметься FD поточного маршруту для визначення `feasible` маршрутів.

Балансування навантаження може виконуватися тільки між `feasible routes`, коли вони потраплять в таблицю маршрутизації.

Маршрут вважається `feasible` при виконанні двох умов [29]:

- FD кращого маршруту більше ніж AD, який анонсує сусідній маршрутизатор. Іншими словами, наступний маршрутизатор на шляху має бути ближчий до `destination`, ніж локальний маршрутизатор (для запобігання створенню петель маршрутизації);
- FD кращого маршруту, помножене на `variance`, повинно бути більше, ніж FD альтернативного маршруту.

## 5 СПЕЦІАЛЬНА ЧАСТИНА

Дипломна робота ОР “Магістр” присвячена дослідження динамічних протоколів маршрутизації, проте не потрібно забувати і про захист даних. В даному розділі опишемо алгоритми захисту даних на мережевому рівні.

На мережевому рівні застосовуються два основні алгоритми: SKIP і IPSec. Відмінність в алгоритмах, головним чином, полягає в способі генерації і передачі ключів для шифрування вмісту пакетів.

### 5.1 Протокол SKIP

Протокол SKIP (Simple Key management for Internet Protocol – просте керування ключами для IP-протоколу) розроблений компанією Sun Microsystems в 1994 році. Основними його властивостями є: апаратна незалежність, прозорість для застосувань і незалежність від системи шифрування. Останнє дуже важливе з огляду на те, що в більшості країн світу, включаючи і нас, існують обмеження на вживані в цій країні стандарти шифрування передаваних даних. Таким чином, при реалізації алгоритму в кожній країні може бути застосований свій стандарт шифрування, зокрема у нас застосовується симетричний алгоритм ГОСТ 28147-89.

В основі алгоритму лежить система відкритих ключів Діффі-Хелмана. В цій системі передбачається наявність у кожного з користувачів пари ключів. Кожен користувач системи захисту інформації має секретний ключ  $K_s$ , відомий тільки йому, і відкритий ключ  $K_o$ . Відкриті ключі можуть бути викладені на будь-якому загальнодоступному сервері.

Особливістю схеми є те, що відкритий ключ  $K_o$  обчислюється з секретного ключа  $K_s$ . Обчислення здійснюється таким чином:  $K_o = g^{K_s} \bmod n$ , де  $g$  і  $n$  – деякі заздалегідь вибрані досить довгі прості цілі числа.

При цьому якщо вузол  $J$  встановлює з'єднання з вузлом  $I$ , то вони легко можуть сформувати спільний ключ для симетричного алгоритму шифрування

даних, скориставшись можливістю обчислення спільного для них розділюваного секрету  $K_{ij}$ :

$$K_{ij} = K_{oj} * K_{ci} = (gK_{cj}) * K_{ci} \bmod n = (gK_{ci}) * K_{cj} \bmod n = K_{oi} * K_{cj} = K_{ij}.$$

Іншими словами, відправник і одержувач пакету можуть вичислити розділюваний секрет на підставі власного секретного ключа і відкритого ключа партнера.

Отриманий ключ  $K_{ij}$  є довготривалим секретом, що розділяється, для будь-якої пари абонентів  $I$  і  $J$  і не може бути вичислений третьою стороною, оскільки секретні ключі  $K_{ci}$  і  $K_{cj}$  в мережевому обміні не беруть участь і третій стороні не доступні.

Таким чином, секрет, що розділяється, не вимагається передавати по лінії зв'язку для організації з'єднання, і він придатний як ключ для симетричного алгоритму шифрування. Проте на практиці для шифрування окремих пакетів застосовують так званий пакетний ключ, який поміщають в заголовок SKIP-пакету і зашифровують за допомогою розділюваного секрету.

Далі отриманий пакет доповнюється новим IP-заголовком, адресами в якому є адреси тунелюючих вузлів (див. рисунок 5.1).

Перевагами такого рішення є, по-перше, додатковий захист розділюваного секрету оскільки він використовується для шифрування малої частини трафіку (тільки пакетного ключа) і не дає вірогідному противнику матеріал для статистичного криптоаналізу у вигляді великої кількості інформації, зашифрованої ним; по-друге, у разі компрометації пакетного ключа збиток складе лише невелика група пакетів, зашифрованих ним.

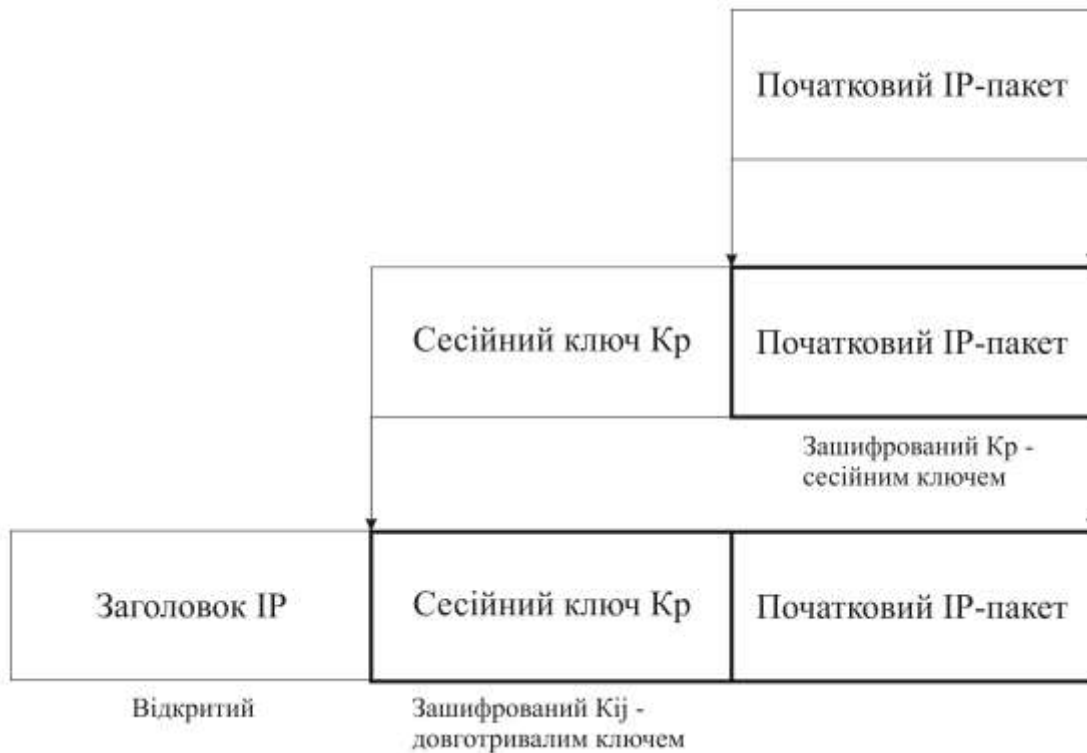


Рисунок 5.1 – Схема створення SKIP-пакета

У тому випадку, коли відсутня необхідність шифрування або підписування даних, відповідні елементи, а саме пакетний ключ і ЕЦП пакету, можуть бути відсутніми. Необхідність шифрування і/або підписки вказується при установці параметрів SKIP-з'єднання. Так, в прикладі налаштувань SKIP-протоколу в СЗІ "Застава", приведеному на рисунку 5.2 (у нижній частині рисунку), вказано на необхідність шифрування цих пакетів з використанням алгоритму DES, вимога аутентифікації, тобто застосування ЕЦП пакету, відсутня.

Технологія, що застосовує протокол SKIP, не вільна від ряду організаційних проблем:

- необхідно забезпечити безпечне зберігання секретних ключів  $K_s$  і кешування розділюваних секретів  $K_{ij}$ ;
- необхідно забезпечити безпечний спосіб генерації і зберігання (на протязі відносно короткого часу життя) пакетних ключів  $K_p$ ;
- забезпечити сертифікацію відкритих ключів.



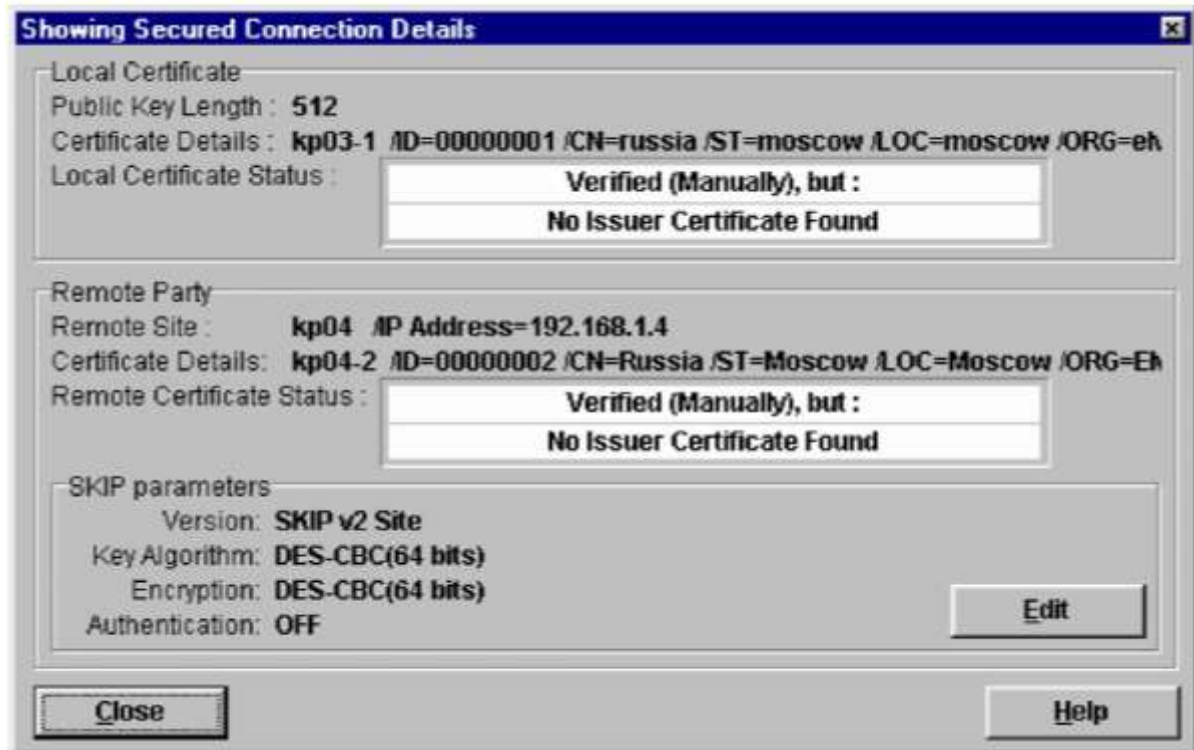


Рисунок 5.2 – Налаштування параметрів протоколу SKIP

Проблема забезпечення сертифікації відкритих ключів виникає внаслідок можливості проведення відомої атаки “man - in - the - middle”. В якості захисту від подібної атаки застосовується сертифікація відкритих ключів. Сенс сертифікації полягає в створенні електронного документу – сертифікату відкритого ключа. В цьому документі окрім самого електронного ключа повинна знаходитися інформація про того, кому цей сертифікат виданий, який термін його дії, ким виданий, і, найважливіше, має бути присутнім ЕЦП відкритого ключа, згенерована організацією, видавщою сертифікат. Знаючи цю організацію, будь-який користувач, що бажає перевірити достовірність сертифікату, може отримати її відкритий ключ і перевірити ЕЦП, що зберігається в сертифікаті.

Передбачається, що розподілом відкритих ключів повинна займатися заслуговуюча довіри сторона. В зарубіжній літературі для подібного органу використовується термін Certificate Authority ("Нотаріус"), в наших документах він іменується Центром сертифікації (ЦС).

Як вже говорилося, сертифікат - файл певного формату. Найбільшого поширення набув формат сертифікату, встановлений Міжнародним телекомунікаційним союзом ITU Rec. X.509. Електронний сертифікат стандарту X.509 містить: ім'я видавця сертифікату; ім'я власника сертифікату; відкритий ключ власника; термін дії відкритого (секретного) ключа видавця і власника; доповнення; списки відкликаних сертифікатів.

Приклад сертифікату відкритого ключа у форматі X.509 приведений в таблиці 5.1.

Таблиця 5.1 – Приклад сертифікату відкритого ключа

Поле	Приклад значення
Версія сертифікату	1, 2, 3
Серійний номер сертифікату	40:00:00:00:00:00:00:ab:38:1e:8b:e9:00:31:0c:60
Ідентифікатор алгоритму ЕЦП	ГОСТ Р 34.10-94
Ім'я видавця сертифікату	C=RU, ST=Moscow, O=PKI, CN=Certification Authority
Термін дії сертифікату	Дійсний з: Листопада 2 06:59:00 1999 GMT Дійсний по: Листопад 6 06:59:00 2004 GMT
Ім'я власника сертифікату	C=RU, ST=Moscow, O=PKI, CN=Sidorov
Відкритий ключ власника	тип ключа : Відкритий ключ ГОСТ довжина ключа : 1024 значення: AF: ED :80:43
Унікальний ідентифікатор видавця	
Унікальний ідентифікатор власника	
ЕЦП Центру сертифікації	

Протокол SKIP містить механізми захисту від наступних видів атак.

– атаки з мережі на сервіси ОС і на прикладні програми, підключення неавторизованих вузлів до мережі. Механізм: в захищену мережу або комп'ютер пропускаються пакети тільки від власника секрету, що розділяється.

– прослуховування трафіку. Механізм: передавані пакети можуть бути прочитані тільки власником секрету, що розділяється.

– повторення пакетів. Механізм: в аутентифікуючу частину заголовка SKIP-пакета перед обчисленням криптосуми пакету підставляється, зокрема, поточний час.

– підміна/маскарад. Механізм: всі пакети і їх адресна інформація аутентифікуються і захищаються від підробки криптосумою по пакету, розділюваному секрету і поточному часу.

– перехоплення сесій. Механізм: в мережу може увійти тільки власник розділюваного секрету.

– атака Man - in - the - middle. Механізм: підписані сертифікати ЦС.

– аналіз топології мережі. Механізм: топологія мережі повністю ховається тунелюванням усіх пакетів, що виходять з мережі.

– криптоаналіз. Механізм: велика довжина пакетних ключів (до 256 біт); часта зміна пакетних ключів - через кожних 5-10 IP - пакетів; відсутність даних для криптоаналізу розділюваного секрету, - він не використовується безпосередньо для криптообробки.

– атака: відмова в обслуговуванні. Механізм: нейтралізується для всіх DoS атак, що ведуться на рівні вище, ніж IP. В мережу пропускаються пакети тільки від власника розділюваного секрету.

В той же час, захист від ряду атак протоколом не реалізується:

– здійснюється захист лише частини трафіку, наприклад спрямованого у віддалену філію. Інший трафік (наприклад, до web-серверів) проходить через VPN-пристрій без обробки;

– немає захисту від дій користувачів, що мають санкціонований доступ в корпоративну мережу.

## **5.2 Протокол IPSec**

Протокол IPSec дозволяє здійснювати дві найважливіші функції мережевого захисту – здійснювати криптографічний захист трафіку і

виконувати фільтрацію вхідних/вихідних пакетів. Протокол реалізований в ОС Windows 2000/XP. Протокол забезпечує аутентифікацію учасників мережевого обміну (протокол IKE - Internet Key Exchange), захист цілісності (заголовок аутентифікації AH - Authentication Header) і шифрування (ESP - Encapsulating Security Payload).

Аутентифікуючий заголовок (AH) виконує захист від атак, пов'язаних з несанкціонованою зміною утримуваного пакету. Для цього особливим чином застосовується алгоритм MD5: в процесі формування AH послідовно обчислюється хеш-функція від об'єднання самого пакету і деякого заздалегідь узгодженого ключа, потім від об'єднання отриманого результату і перетвореного ключа.

Заголовок ESP служить для забезпечення конфіденційності даних, припускає можливість використання будь-якого симетричного алгоритму шифрування.

Протокол обміну ключами IKE відповідає за первинний етап встановлення з'єднання, спосіб ініціалізації захищеного каналу, процедури обміну секретними ключами, вибір методу шифрування. Припускає три різні способи аутентифікації: технологію "виклик-відповідь" з використанням хеш-функції із спільним секретним ключем, застосування сертифікатів відкритих ключів і використання протоколу Керберос.

## 6 ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від дослідження збіжності мережі на базі динамічних протоколів маршрутизації, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільність впровадження відповідної розробки.

Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції, що мала місце при проведенні наукових досліджень.

### 6.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 6.1.

Таблиця 6.1 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Витрати праці на підготовку опису задачі	інженер	10
2.	Витрати праці на розробку проекту	інженер	16
3.	Витрати праці на розробку структури системи	інженер	20
4.	Витрати праці на створення системи по вибраному проекту та структурі	інженер	55
5.	Витрати праці на підготовку документації	інженер	12

1	2	3	4
6.	Витрати праці на відлагодження роботи зпроектованої системи при комплексній відладці	інженер	40
<b>Разом</b>			153

Сумарний час на проведення науково-дослідної роботи становить 153 години.

## **6.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи**

Відповідно до Закону України «Про оплату праці» заробітна плата – це «винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу».

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці. Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку [ ].

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Рекомендовані тарифні ставки: керівник проекту – 40,5..50,5 грн./год., інженер – 30,25..40,5 грн./год., консультант – 25,75..37 грн./год., технік – 22,0..35,0 грн./год., лаборант – 20,0..30,5 грн./год.

Основна заробітна плата розраховується за формулою:

$$Z_{осн} = T_c \cdot K_z, \quad (6.1)$$

де  $T_c$  – тарифна ставка, грн.;

$K_z$  – кількість відпрацьованих годин.

Оскільки всі види робіт в даному дослідженні виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою:

$$Z_{осн} = 38 \cdot 153 = 5814 \text{ грн.}$$

Додаткова заробітна плата становить 10-15 % від суми основної заробітної плати.

$$Z_{дод} = Z_{осн} \cdot K_{додл.}, \quad (6.2)$$

де  $K_{додл.}$  – коефіцієнт додаткових виплат працівникам, 0,1-0,15 (візьмемо його рівним 0,15).

$$Z_{дод} = 5814 \cdot 0,15 = 872,1 \text{ грн.}$$

Звідси загальні витрати на оплату праці ( $B_{о.п.}$ ) визначаються за формулою:

$$B_{o.n.} = Z_{ocn.} + Z_{dod.} \quad (6.3)$$

$$B_{o.n.} = 5814 + 872,1 = 6686,1 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи: єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%, військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{c.z.} = \Phi O П \cdot 0,235, \quad (6.4)$$

де  $\Phi O П$  – фонд оплати праці, грн.

$$B_{c.z.} = 6686,1 \cdot 0,235 = 1571,23 \text{ грн.}$$

Таблиця 6.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	інженер	38	153	5814	872,1	1571,23	8257,33

Проведені розрахунки витрат на оплату праці наведено у таблиці 6.2.

Згідно з проведеним аналізом та розрахунками загальна сума витрат на оплату праці складається з фактично нарахованої заробітної плати, додаткової заробітної плати та нарахування на ФОП і становить суму 8257,33 грн.



### 6.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{Bi} = q_i \cdot p_i, \quad (6.5)$$

де:  $q_i$  – кількість витраченого матеріалу  $i$ -го виду;

$p_i$  – ціна матеріалу  $i$ -го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Z_{м.в.} = \sum M_{Bi}. \quad (6.6)$$

Таблиця 6.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Програмне забезпечення різного рівня	комплект	–	2413,75	2413,75
2	Папір формату А1	шт.	9	25	225
Разом			9	2438,75	2638,75

Проведені розрахунки на матеріальні витрати наведено у таблиці 6.3.

## 6.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання, що використане для даного дослідження визначаються за формулою:

$$Z_e = W_i \cdot T \cdot S, \quad (6.7)$$

де  $W$  – необхідна потужність, кВт;

$T$  – кількість годин роботи обладнання;

$S$  – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (1,68 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 2,01 грн [ ].

Потужність комп'ютера – 450 Вт, кількість годин роботи обладнання згідно таблиці 6.1 – 153 години, тоді,

$$Z_e = 0,45 \cdot 153 \cdot 2,01 = 138,38 \text{ грн.}$$

## 6.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі дослідження є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів.

Для цієї групи річна норма дорівнює 60 % (квартальна – 15 %).

$$A = \frac{B_B \cdot H_A}{100\%}, \quad (6.8)$$

де  $A$  – амортизаційні відрахування за звітний період, грн.;

$B_B$  – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$H_A$  – норма амортизації, %.

Під час дослідження та аналізу динамічних протоколів маршрутизації засобом праці є комп'ютер. Його ціна становить 12000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{12000 \cdot 5\%}{100\%} = 720 \text{ грн.}$$

Оскільки робота виконувалась 153 години, то амортизаційні відрахування будуть становити:

$$A = \frac{720 \cdot 153}{153} = 720 \text{ грн.}$$

## **6.6 Обчислення накладних витрат на дослідження та аналіз динамічних протоколів маршрутизації**

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20-60 % від суми основної та додаткової заробітної плати працівників [ ].

$$H_B = B_{o.p.} \cdot 0,2..0,6, \quad (6.9)$$

де  $H_B$  – накладні витрати.

Отже, накладні витрати на дослідження:

$$H_B = 8257,33 \cdot 0,2 = 1651,46 \text{ грн.}$$

## 6.7 Складання кошторису витрат та визначення собівартості

Результати проведених вище розрахунків зведено у таблицю 6.4.

Таблиця 6.4 – Кошторис витрат на розробку

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	8257,33	55,7
Відрахування на соціальні заходи	1571,23	10,5
Матеріальні витрати	2638,75	17,6
Витрати на електроенергію	138,38	0,92
Амортизаційні відрахування	720	4,8
Накладні витрати	1651,46	11,02
Собівартість	14977,15	100

Собівартість ( $C_B$ ) дослідження розраховується за формулою:

$$C_B = B_{o.n.} + B_{c.z.} + Z_{m.v.} + Z_e + A + H_e. \quad (6.1)$$

0)

Отже, собівартість дослідження дорівнює:

$$C_B = 8257,33 + 1571,23 + 2638,75 + 138,38 + 720 + 1651,46 = 14977,15 \text{ грн.}$$

## 6.8 Розрахунок ціни дослідження та аналізу динамічних протоколів маршрутизації

Ціну дослідження можна визначити за формулою:

$$Ц = \frac{СВ \cdot (1 + P_{рен}) + К \cdot B_{н.і.}}{К} \cdot (1 + ПДВ), \quad (6.11)$$

де  $P_{рен.}$  – рівень рентабельності, 30 %;

$K$  – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$  – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

$ПДВ$  – ставка податку на додану вартість, (20 %). Оскільки розроблюваний продукт не є прикладним, то для розрахунку його ціни не потрібно вказувати коефіцієнти  $K$  та  $B_{н.і.}$ .

Тоді, формула для обчислення ціни буде мати вигляд:

$$A = СВ \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (6.12)$$

Звідси ціна:

$$Ц = 14977,15 \cdot (1 + 0,3) \cdot (1 + 0,2) = 23364,35 \text{ грн.}$$

## 6.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність дослідження – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ( $E_p$ ) полягає у відношенні дослідження до затрачених ресурсів:

$$E_p = \frac{\Pi}{C_B}, \quad (6.13)$$

де  $\Pi$  – прибуток;

$C_B$  – собівартість.

Плановий прибуток ( $\Pi_{пл}$ ) знаходиться за формулою:

$$\Pi_{пл} = Ц - C_B. \quad (6.14)$$

Плановий прибуток складатиме:

$$\Pi_{пл} = 23364,35 - 14977,15 = 8387,2 \text{ грн.}$$

Отже, формула для визначення економічної ефективності дослідження набуде вигляду:

$$E_p = \frac{\Pi_{пл}}{C_B}. \quad (6.15)$$

Тоді,

$$E_p = \frac{8387,2}{14977,15} = 0,56.$$

Поряд із економічною ефективністю розраховується термін окупності капітальних вкладень ( $T_p$ ):

$$T_p = \frac{1}{E_p}, \quad (6.16)$$

)

Термін окупності дослідження дорівнює:

$$T_p = \frac{1}{0,56} = 1,8 \text{ років.}$$

Отже, дане дослідження може бути впроваджене та мати подальший розвиток, оскільки воно є економічно вигідним за всіма основними техніко-економічними показниками.

## **7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ**

### **7.1 Охорона праці**

#### **7.1.1 Принципи професійного відбору операторів ВДТ**

На сучасному етапі розвитку НТП надійність та продуктивність функціонування комп'ютеризованих систем значною мірою залежить від правильного відбору та навчання фахівців. Завдання професійного вибору є визначення людей, які здатні найефективніше виконувати відповідні професійні завдання, використовуючи при цьому певні технічні засоби.

Для операторів ВДТ основним змістом роботи є складний комплекс розумової діяльності з невеликими елементами фізичної праці. В основі взаємодії оператора з апаратурою є приймання, опрацювання інформації, прийняття та реалізація рішення.

Важливою особливістю людини-оператора є те, що оптимальне, опрацювання інформації, яка надходить до нього, відбувається у тому випадку, коли вона за обсягом узгоджена з його можливостями сприйняття та не є занадто великою і занадто малою. При великому навантаженні оператори не встигають виконувати задані функції, але коли навантаження є зменшується, то оператори втрачають активність. Аналіз праці операторів ВДТ показує, що коли до цього виду діяльності залучаються люди, які не мають достатніх здібностей до такої роботи, то вони не лише значно довше та з більшими труднощами оволодівають цією спеціальністю, але й частіше роблять помилки та прорахунки. Тому при професійному відборі необхідно ретельно перевірити відповідність психофізіологічних властивостей кандидата до вимог, що пред'являються до операторської діяльності.

Професійний відбір може здійснюватися наступними методами: стихійним, медичним, конкурсним та інженерно-психологічним.



Під час стихійного відбору кандидати на посаду оператора призначаються з групи претендентів без врахування їх індивідуальних здібностей.

Під час медичного відбору враховується лише один фактор – стан здоров'я. За заключенням медичної комісії про придатність до роботи відібрані кандидати можуть призначатися на посади.

Під час конкурсного відбору кандидати на посади операторів відбираються за результатами перевірки їх індивідуальних здібностей шляхом проведення іспитів або конкурсу документів.

Найбільше відповідаю потребам професійного вибору інженерно-психологічний метод. В цьому випадку кандидати на посаду оператора вибираються з повним врахуванням антропометричних, фізіологічних, психологічних та інших даних. В основі інженерно-психологічного методу лежать два основних принципи: активність та етапність відбору.

Під активністю відбору розуміють не лише факт визначення кандидатів на посади операторів, але й удосконалення методів навчання, а також органів керування. Основні напрями: максимальне пристосування органів керування та робочого Місця оператора до функціональних характеристик людини, раціональна автоматизація керування; розробка алгоритмічних систем навчання, оптимізація режимів тренувань, застосування засобів покращення функціональних характеристик людини згідно з особливостями окремого кандидата на професію.

Під етапністю відбору розуміють послідовність проведення цієї роботи. Найбільш широко застосовується три етапний відбір.

Перший етап – відбір за висновками медичних комісій. Його основне завдання полягає в тому, щоб виключити осіб, які за станом здоров'я не можуть виконувати ті чи інші функціональні обов'язки оператора.

Під час другого етапу з'ясовується ступінь придатності тої чи іншої людини до виконання даних професійних обов'язків.

Третій етап вибору є контролюючим. В його завдання входять:

– своєчасне виявлення між працюючими спеціалістами і тими, що навчаються, осіб, які не можуть ефективно виконувати свої функціональні обов'язки;

– розробка методики навчання, адаптованої до даного, кандидат (групи кандидатів).

Розглянемо детальніше порядок вибору операторів на другому та третьому етапі. Завданням цих двох етапів є Відбір кандидатів в оператори, які:

– мають здобуті до початку роботи операторами навички, що впливають на оволодіння спеціальністю оператора;

– характеризуються потрібною швидкістю отримання навичок оператора.

При цьому завдання другого етапу полягає в тому, щоб звести до мінімуму контингент осіб, яких залучають до відбору на оператора.

Завдання третього етапу полягає в тому, щоб з високим ступенем імовірності вирішити питання придатності до праці існуючої спеціальності кандидатів, які пройшли другий етап відбору.

На другому етапі відбір кандидатів для роботи за даною спеціальністю проводиться за наслідками обстеження за допомогою психофізіологічних тестів. Залежно від якості виконання кожного тесту кандидат отримує окремий бал. Сума балів, одержаних при виконання усіх тестів є критерієм можливості використання кандидата для роботи за спеціальністю.

На третьому етапі основною є оцінка діяльності кандидатів за результатами їх праці в ситуаціях, характерних для реальних умов праці. На цьому етапі і фіксуються дані, які дозволяють зробити кінцевий за можливостями кандидата в отриманні необхідних знань.

З цією метою знаходять коефіцієнт навчання кандидата та початковий рівень підготовки до роботи за даною спеціальністю.

Усі кандидати проходять короткий курс навчання на місцях праці. Вони знайомляться з особливостями робочого місця, обов'язками, порядком роботи

та правилами безпеки. Після короткочасного навчання проводиться контрольний іспит, за результатами якого і робляться; висновки.

При необхідності формування бригади чи зміни, доцільно підбирати кандидатів із врахуванням психологічної сумісності, яка передбачає оптимальне об'єднання людей. В основу покладено спільність мети, смаків, звичок, подібність динамічної спрямованості емоційно-вегетативних реакцій та ін. Професійна сумісність передбачає зарахування до складу групи осіб, на підготовку яких потрібні майже однакові витрати часу та засобів.

Психологічна сумісність передбачає встановлення між особами групи відносин, які базуються на взаємодопомозі та увазі один до одного. Добра психологічна сумісність індивідумів у колективі досягається, як правило, в тому випадку, коли рівень психомоторної та розумової діяльності у них достатньо великий і рівнозначний. Задовільна психологічна сумісність є також при сумісній діяльності осіб, які мають високу швидкість думки та слабке моторне реагування, з особами, які мають лише швидке моторне реагування. Для формування емоційної стійкості у колективі при розподілі функціональних обов'язків між операторами за ступенем відповідальності потрібно призначати на відповідальні посади тих операторів, які мають вищу емоційну стійкість. Доцільно у складі групи мати декілька операторів з високою емоційною стійкістю, які могли б при виникненні стресової ситуації і психологічної нестійкості частини операторів зберігати здатність до правильного прийняття рішення та оперативного втручання. Правильне та розумне виконання вимог щодо професійного добору дозволяє відібрати та навчити спеціалістів, які спроможні забезпечити найвищу працездатність та необхідну надійність роботи.

### **7.1.2 Працездатність операторів ВДТ**

Працездатність відображає здатність людини виконувати роботу певної важкості та напруженості з необхідною якістю за встановлений період часу. В процесі роботи працездатність людини змінюється. На рисунку 7.1 показана

найбільш типова крива, яка характеризує зміну працездатності оператора за робочий цикл (зміну).

Як видно з рисунку 7.1 працездатність має відповідну протяжність у часі та фазний характер зміни періодів. Виділяють чотири періоди працездатності: період втягування в роботу (I);

- період стійкої працездатності (II);
- період субкомпенсації (III);
- період втоми (IV).

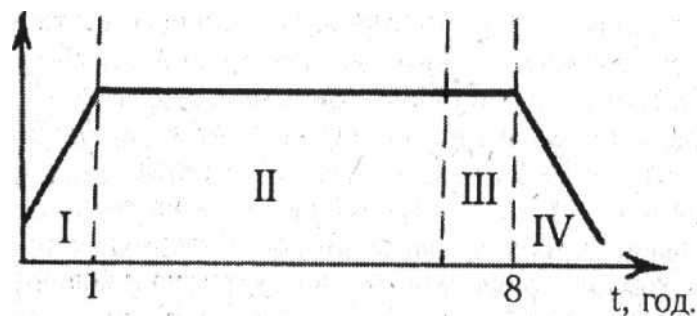


Рисунок 7.1 – Зміна працездатності оператора за робочий цикл (зміну)

Період втягування в роботу, який може тривати до години і більше, виражається у поступовому підвищенні працездатності. Важливою умовою високої працездатності є поступовість втягування в трудовий процес, причому людина повільніше включається в розумову роботу, ніж у фізичну. Значного скорочення періоду втягування в роботу можна досягти за рахунок попередньої підготовки працівника до роботи (адаптації зору, слуху, виконання фізичних вправ) та шляхом попереднього розумового навчання. Суть останнього полягає в тому, що оператор перед початком роботи проводить вирішення одного чи кількох ситуаційних завдань. Оператор за аналогією з спортсменами проводить попередню розминку ("розігрівається").

Другий період характеризується високою та стійкою працездатністю. В цей час усі зміни фізіологічних функцій адекватні робочому навантаженню і перебувають у межах фізіологічних норм. Тривалість періоду залежить від інтенсивності роботи. Чим більше навантаження, тим коротший другий період.

Період субкомпенсації розглядається як початок розвитку втоми. В цей період продуктивність праці ще зберігається на високому рівні, але завдяки вольовим зусиллям та за рахунок перенапруження відповідних систем організму.

Період втоми характеризується зниженням продуктивності праці при дальшому погіршенні функціонального стану оператора. Почуття втоми стрімко наростає, а у фізіологічних системах настає зміна показників. Швидше настають зміни в тих органах і системах, які забезпечують виконання конкретної роботи. В операторів ВДТ у цей період частіше всього появляються болі та різь в очах, головний біль, судоми м'язів кисті, ниючий біль спини й шиї та ін. Якщо в цей період не припинити роботи, то втома перейде в перевтому. При перевтомі період Відновлення працездатності (відпочинок) збільшується, а в організмі порушуються відповідні психофізіологічні процеси. При наявності хронічної перевтоми, можуть настати функціональні і навіть паталогічні зміни.

Однією з особливостей праці операторів є виражена післядія – мимовільний напружений стан центральної нервової системи вже теля-фактичного припинення роботи. Мозок на якийсь час продовжує "працювати" у попередньому режимі та ритмі, хоча нова інформація вже не надходить. Це призводить до того, що частина часу Відведеного для відпочинку не використовується за прямим призначенням. Тобто зрозуміло, що короткочасні перерви в цих умовах не ефективні. Час відпочинку повинен бути збільшений на той проміжок, протягом якого центральна нервова система подолає труднощі й організм почне повноцінно відпочивати, відновлюючи свій вихідний до робочий стан.

Працездатність оператора залежить від цілої низки факторів, які можна умовно поділити на зовнішні і внутрішні.

До зовнішніх факторів належать: кількість та форма отриманої інформації, зручність робочого місця, санітарно-гігієнічні умови, характер взаємовідносин в колективі, моральні та матеріальні стимули тощо.

До внутрішніх факторів належать: рівень підготовки, стаж роботи, тренуваність, стан здоров'я, емоційна стійкість, вік та ін.

## **7.2 Безпека в надзвичайних ситуаціях**

### **7.2.1 Міжнародний тероризм**

Терор (лат. *terror* – страх, жах) – має ознаку «усувати», «закривати». Ця обставина і визначає терор як особливу форму політичного насильства, що характеризується жорстокістю, цілеспрямованістю й уявленою ефективністю. Ці особливості визначили широке використання терору упродовж людської історії як засобу політичної боротьби в інтересах держави, організацій чи окремих угруповань. Безпосередньо сам факт привселюдної страти кримінальних чи політичних злочинців, чи процес «аутодафе» в період середньовікової інквізиції, є класичною формою терору в інтересах держави чи католицької церкви.

Правовою основою боротьби з міжнародним тероризмом є «Декларація про заходи для ліквідації міжнародного тероризму», що затверджена на 49-й сесії Генеральної асамблеї ООН (резолюція 49/60 від 9 грудня 1994 р.)

Цей документ встановлює принципи відносин світової спільноти і програму заходів з метою ліквідації такого огидного суспільного явища, як міжнародний тероризм, а також встановлює подальше співробітництво між державами для невідкладної ліквідації будь-яких форм і проявів терористичної діяльності. Характерним для розвитку світової спільноти є те, що наявність лідера (провідної країни чи провідної сили) народжує відповідну реакцію – формування нижчого за рангом (рівнем) іншого лідера (іншої країни чи іншої провідної сили). Має місце формування біполярності, виникають реалії антагонізму на різних рівнях світового суспільства, в т.ч. суперечності на рівні «держава»↔«держава», «держава»↔«внутрішня організація» (організація зовнішня), «держава»↔«партія» та ін. Крім того, у світовій практиці мають місце комбіновані види із вищезгаданих «пар», з яких формуються інші групи

(сили), в т.ч. політичні, злочинні та ін. відповідні сили чи угруповання. На другому етапі формування ці сили (групи) шукають собі відповідні «ніші» існування; економічну, політичну, наукову та інші види підтримок; формують свої озброєні сили, відповідні професійні кадри, джерела озброєння, територію знаходження тощо. При цьому використовуються всі «блага» цивілізації особистого розвитку і поширення впливу на світову спільноту.

Міжнародний тероризм, створюючи свій плацдарм, може викликати кризи (системні) в світовій, моральній, політичній, економічній системі відносин і зруйнувати та усунути всі передумови розвитку світової спільноти.

В Україні, за даними служби безпеки, за останні два роки скоєно понад 560 злочинів терористичного характеру, внаслідок цього 90 осіб (із них 15 представників владних структур) загинуло. В Україні зростає активність міжнародних терористичних організацій, насамперед із країн Близького Сходу («Хезболах», «Абу Ніджаль», «Хамас», «Брати мусульмани»), які прагнуть використати територію України для транзиту своїх бойовиків до країн західної Європи, підготовки терористичних акцій.

Головними принципами попередження та боротьби з міжнародним тероризмом має стати постійне удосконалення відповідної законодавчої бази, співробітництво з правоохоронними організаціями, консолідація з іншими країнами й організація напрямів запобігань поширенню будь-яких терористичних організацій і угруповань.

Терористичний акт не має безпосередніх можливостей досягнення оголошеної кінцевої мети і звичайно складається з таких елементів: насильницька дія у різноманітних її формах, політичний мотив в основі здійснення самого терористичного акту; сам акт спрямовано проти осіб, організацій, націй, національностей і меншин, державних інститутів чи їх представників з метою їх залякування чи виконання окремих вимог. Терор щодо націй, етнічної, расової чи релігійної групи, що здійснюється для її повного чи часткового усунення, розглядається світовою спільнотою вже як акт геноциду.

Варіанти комбінацій за спрямованістю суб'єкт—об'єкт здійснення терористичного акту багатоспрямовані, тому важко дати універсальне визначення «терору». Проте деякі критерії певної класифікації можна встановити:

- індивідуальний, організований терор і терор як політика держави;
- терор як метод внутрішньополітичної боротьби і терористичні акти міжнародного характеру.

### **7.2.2 Структура системи БЖД**

Поняття «життєдіяльність» стосується тільки людини. Людина живе і працює в безпосередньому зв'язку з навколишнім середовищем.

Життєдіяльність (ЖД) – це складна фізіологічна система, яка має назву «система ЖД».

Системою називають сукупність взаємозв'язаних елементів, функціонування яких спрямоване на досягнення певної загальної мети.

Система ЖД складається із взаємопов'язаних елементів: життя, діяльності людини, навколишнього середовища, – і має підтримувати комфортне та безпечне існування людини, забезпечити сталий розвиток людства.

Розглянемо характеристики елементів системи ЖД.

Життя – це форма існування матерії, яка характеризується обміном речовин, здатністю до розмноження і розвитку, вмінням пристосовуватись до навколишнього середовища.

Людина – вища форма розвитку живої матерії, і її існування – дуже складний процес, що не тільки підтримує її фізіологічний стан, але й задовольняє духовні потреби. Крім того, на життя людини суттєво впливають умови проживання та праці, медичний догляд і багато інших факторів, що виникають завдяки діяльності самих людей.

Діяльність – це специфічна форма ставлення людей до навколишнього середовища та одне до одного, яка має задовольняти потреби та інтереси



людини. Це соціальна категорія, нерозривно зв'язана із суспільством. Тільки завдяки діяльності людини створено всі блага, які має людство.

Основні види діяльності такі:

- виробнича;
- наукова;
- мистецька;
- освітня.

Однією із специфічних форм діяльності людини є праця – перша й основна умова існування людини (людства).

Праця – цілеспрямована діяльність людини, у процесі якої вона впливає на природу і використовує її з метою виробництва матеріальних та інших благ, необхідних для задоволення своїх потреб.

Потреби – це необхідність для людини того, що забезпечує її існування і самозабезпечення (фізіологічне, матеріальне, соціальне, духовне та ін.).

Навколишнє середовище (довкілля) або середовище існування – це все, що оточує людину впродовж її життя. Навколишнє середовище, у свою чергу, поділяють на такі види:

- природне середовище;
- штучне середовище.

Природне середовище (біосфера) – це частина Землі і простору навколо неї, де зосереджено все живе. Біосфера включає:

- атмосферу (газоподібна частина);
- гідросферу (рідка водна частина);
- літосферу (тверда частина).

На ЖД людей найбільше впливає частина біосфери від поверхні Землі вглиб на 15–20 км і до висоти 20–22 км, де починається озоновий шар. Природне середовище є джерелом природних ресурсів для існування людини: повітря, води, деревини, корисних копалин, ґрунту та ін.

Штучне середовище – це складова довкілля, створена людством за тривалий час його існування. Штучне середовище умовно можна поділити на два види:

- виробниче середовище;
- побутове середовище.

Виробничим називають середовище, в якому людина реалізує свою трудову діяльність (підприємства, установи, навчальні заклади тощо).

Побутовим є середовище, де люди мешкають або проводять вільний час. Воно охоплює сукупність житлових будинків, комунально-побутових об'єктів, місця відпочинку та ін.

Організм людини може нормально функціонувати тільки тоді, коли умови (параметри) зовнішнього середовища відповідають оптимальним. Якщо умови середовища змінюються, стають несприятливими, то на протидію їм організм людини включає спеціальні механізми, які зберігають постійність параметрів внутрішнього середовища (всередині організму) чи змінюють їх у межах допустимого.

Можливість функціонування організму в середовищі, параметри якого постійно змінюються, забезпечується завдяки механізму, який називають адаптацією.

Адаптація (лат. *adapto* – пристосування) – динамічний процес пристосування організму до мінливих умов зовнішнього середовища, який спостерігається в будь-якому виді діяльності щоразу, коли виникають значні зміни в системі «людина – середовище». Адаптація може бути фізіологічною, психологічною, соціальною.

Отже, для функціонування системи ЖД середовище має обов'язково відповідати природним параметрам. Відхилення можливі в межах допустимого, коли організм людини здатний адаптуватися, захистити себе, підтримувати існування. Усе, що існує за цими межами, становить загрозу життю, тому виникає потреба захисту ЖД людей. Отже, безпека – важлива складова системи ЖД.

Розглядаючи систему ЖД як взаємодію людей з навколишнім середовищем, слід зауважити, що вона завжди підпорядкована певним принципам, правилам, умовам життя, природним умовам, традиціям тощо.

Система ЖД має такі характерні ознаки:

- її функціонування підпорядковане об'єктивним законам природи;
- це динамічна система, яка розвивається, удосконалюється, пристосовується до змін умов існування;
- тяжіє до сталого розвитку, вживаючи заходів захисту від впливу негативних факторів.

Основні принципи забезпечення ЖД такі:

- своєчасність, достатність, якість забезпечення людей необхідними для життя засобами високої якості і заходами в потрібний час у належній кількості;
- безпека ЖД (захист ЖД від впливу негативних факторів, що виникають унаслідок як природних явищ, так і діяльності людей).

Рівень реалізації цих принципів значною мірою залежить від способів забезпечення ЖД. Виходячи із сказаного, можна визначити такі головні способи забезпечення ЖД:

1. Організація ефективної трудової діяльності людей в суспільстві з максимальним залученням усіх ресурсів (створення робочих місць, упровадження високопродуктивного виробництва і технологій, нормування праці тощо).
2. Організація та удосконалення освіти і підготовка кадрів, розвиток науки відповідно до вимог часу.
3. Розвиток сфери послуг (комунальних, транспортних, торговельних, побутових і т. ін.).
4. Розширення мережі культурних, спортивних, розважальних установ.

5. Проведення заходів щодо збереження здоров'я людей (диспансеризація, оздоровлення, кваліфіковане медичне обслуговування і лікування, санітарно-епідеміологічний стан).

6. Розроблення законодавчих і нормативно-правових актів із забезпечення прав, свобод і захисту людей і суспільства в цілому.

Залежно від того, якою мірою реалізуються принципи та способи забезпечення ЖД, визначається рівень життя людей окремих країн і загальний розвиток людства.

### **7.2.3 Елементи теорії, що відповідають моделі безпеки життєдіяльності**

Модель у широкому розумінні – це предмет, явище, система (опис, схема, знак, графік, план, макет та ін.), які за певних умов відіграють роль замітника або представника будь-якого іншого предмета, явища чи системи.

З точки зору науки модель – це матеріальна чи уявна система, що відображає чи імітує принципи внутрішньої організації, функціонування, певні властивості чи характеристики об'єкта дослідження, безпосереднє вивчення якого неможливе. Модель може замінити цей об'єкт у пізнавальному процесі з метою отримання нових знань про нього. Таким чином, відношення «модель—оригінал» не природне, а зумовлене процесом пізнання, і питання про їх співвідношення, ступінь їх подібності, адекватності – одне з найважливіших і найскладніших у процесі використання моделей у науковому пізнанні.

Сам процес моделювання – це непрямий, опосередкований метод наукового дослідження об'єктів пізнання на їх моделях, коли з певних причин безпосереднє їх вивчення неможливе.

Моделі в дисципліні «Безпека життєдіяльності» можна систематизувати за об'єктом зв'язків. Усі моделі можна умовно поділити на дві множини залежно від обсягу зв'язків, які вони демонструють.

Перша множина об'єднує моделі, що характеризуються структурою зв'язків.

Друга множина об'єднує моделі парних зв'язків. Певна умовність щодо цієї множини пов'язана з тим, що запровадження глибокого аналізу дозволяє уявити механізми реалізації цих зв'язків діючих великих систем.

Для характеристики довкілля на глобальному, державному і регіональному рівні використовують поняття структури зв'язків (на світовому рівні – навіть загальної). Відповідно до визначеної послідовності рівнів (за територією, від світового до регіонального) зменшується кількість таких зв'язків – з одного боку, а з іншого – збільшується рівень їх деталізації.

Під державним рівнем у цьому випадку розуміють сукупність діючих галузей виробництва як джерел забруднення і географічні чинники території, що одержує це забруднення. Відповідно до двох визначених рівнів подано моделі, що формують уявлення про стан світового довкілля і держави (на прикладі сільськогосподарської галузі). На регіональному рівні модель, що формує стан довкілля, може бути представлена у вигляді взаємодій комплексу діючих (діючого) підприємств із середовищем виробництва.

Для визначення умов роботи підприємства найбільшу увагу для застосування привертають моделі, що відображають зв'язки:

- 1) «регіональний природно-виробничий комплекс – середовище виробництва»;
- 2) «виробниче підприємство – довкілля»;
- 3) «виробниче середовище виробничого підприємства (середовище робочого місця) – людина».

Здобуття найбільш деталізованої інформації за взаємодії можливе на рівні парних (взаємодій) у вигляді: забруднювач середовища (джерелом є підприємство) – елемент довкілля. Таким чином, необхідно розробити відповідні моделі парної взаємодії.

До таких моделей (як зразок) належать:

- а) модель розповсюдження елемента забруднення в середовищі (елементи довкілля – атмосфера, гідросфера, літосфера);
- б) моделі обігу елемента забруднення в елементах довкілля;

- в) моделі обігу елементів середовища;
- г) моделі взаємних впливів на елементи довкілля;
- д) моделі взаємодій екологічних компонентів і організації екосистем;
- е) моделі впливів небезпечних і шкідливих чинників;
- ж) моделі ієрархії екосистем та ін.

У рамках пари «виробниче середовище – людина» певний зміст взаємодій реалізується на базі спрощення уявлення «виробниче середовище» і представлення його як «технологічний процес, обладнання, види господарських робіт тощо».

В період виконання «технологічного процесу...» виникають небезпеки. Це може бути ініційовано як з боку «технологічного процесу, обладнання, видів господарських робіт», так і з боку – «людини». Виходячи з цього, у схемі розгляду нещасного випадку необхідно йти двома шляхами відносно:

- технологічного процесу, обладнання, видів господарських робіт та ін.;
- «людини» як джерела небезпек.

Розвиток подій вивчають за допомогою ступеневих логіко-імітаційних моделей. Характер ступеневої суті моделі визначає перехід від події до події. Події і переходи за змістом формуються трьома складовими: 1) технологічний процес, його операції й елементи; 2) конструкція обладнання; 3) стан охорони праці при їх взаємодії.

За наявності небезпечних обставин під час виконання будь-яких робіт людина сприяє, усвідомлює, приймає і реалізує відповідні рішення в послідовності.

Обидві моделі в межах поєднання свого змісту дають змогу усвідомити комплексний розвиток подій, причини аварій та ін., сприяють створенню безпечних умов праці і запобіганню травматизму.

## 8 ЕКОЛОГІЯ

### 8.1 Вимоги до приміщень для експлуатації моніторів і ПЕОМ.

#### Шляхи дотримання цих вимог

При використанні ПЕОМ з відео моніторами слід притримуватись вимог наведених нижче.

Відеотермінали, ПЕОМ, спеціальні периферійні пристрої ПЕОМ та устаткування для обслуговування, ремонту та налагодження ПЕОМ повинні відповідати вимогам чинних в Україні стандартів, нормативних актів з охорони праці.

Площа, виділена для одного робочого місця з відеотерміналом або ПЕОМ, повинна складати не менше 6 кв. м, а обсяг – не менше 20 куб.м. Робочі місця з відеотерміналами відносно світлових прорізів повинні розміщуватися так, щоб природне світло падало збоку, переважно зліва.

При розміщенні робочих місць з відеотерміналами та персональними ЕОМ необхідно дотримуватись таких вимог:

- робочі місця з відеотерміналами та персональними ЕОМ розміщуються на відстані не менше 1 м від стін зі світловими прорізами;
- відстань між бічними поверхнями відеотерміналів має бути не меншою за 1,2 м;
- відстань між тильною поверхнею одного відеотермінала та екраном іншого не повинна бути меншою 2,5 м;
- прохід між рядами робочих місць має бути не меншим 1 м.

Вимоги цього пункту щодо відстані між бічними поверхнями відеотерміналів та відстані між тильною поверхнею одного відеотермінала та екраном іншого враховуються також при розміщенні робочих місць з відеотерміналами та персональними ЕОМ в суміжних приміщеннях, з урахуванням конструктивних особливостей стін та перегородок.

Якщо у приміщенні одночасно експлуатується більше п'яти персональних ПЕОМ, на помітному та доступному місці має бути встановлено аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

ПЕОМ, периферійні пристрої ПЕОМ та устаткування для обслуговування, ремонту та налагодження ПЕОМ, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники тощо), електропроводи та кабелі за виконанням та ступенем захисту мають відповідати класу зони за ПВЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

## **8.2 Статистичний аналіз екологічності виробництва**

Еколого-економічний аналіз виробництва підприємств-забруднювачів ґрунтується на системі показників та інформації, необхідних для прийняття оптимальних управлінських рішень у сфері раціоналізації природокористування й охорони навколишнього середовища, екологізації та екологічності виробництва.

Екологізація – процес послідовного впровадження нової техніки і технології, нових форм організації виробництва, виконання управлінських та інших рішень, які дають змогу підвищити ефективність використання природних ресурсів з одночасним збереженням природного середовища та його поліпшення на різних рівнях. Екологізація економіки - цілеспрямований процес перетворення економіки, пов'язаний зі зниженням інтегрального екодеструктивного впливу виробництва і споживання товарів і послуг у розрахунку на одиницю сукупного суспільного продукту. Екологічність виробництва характеризує частку екологічних витрат у сукупних витратах виробництва конкретного виду продукції. Важливим показником екологізації виробництва виступає екологоемність продукції, тобто сукупність екологічних витрат в одиниці вартості продукції.



Загальна класифікація еколого-економічних показників з метою оцінки й аналізу екологічності виробництва (ЕВ) у промисловості може бути подана за такими ознаками: за змістом, за рівнем визначення, за часовим інтервалом, за об'єктом оцінки, за характером використання:

– за змістом еколого-економічних показників: натуральні – показники екологічності (екобезпеки) технологічних процесів, техніки (включаючи природоохоронне устаткування), виробничо-господарської діяльності в цілому та її окремих складових. Наприклад, ступінь очищення промислових викидів, комплексність використання сировини (ресурсна ефективність виробництва), обсяги викидів (скидів) шкідливих речовин у навколишнє середовище та ін.;

– натурально-вартісні – еколого-економічний збиток у розрахунку на одиницю товарної продукції в натуральному вираженні, збиткоємність маси викиду (скиду), екологічний результат у розрахунку на одну гривню капітальних вкладень;

– вартісні – розмір економічного збитку в розрахунку на одиницю продукції у вартісному вираженні, повні екологічні витрати виробництва, екологічні платежі за забруднення довкілля;

– локальні – показники вимірюють окремий параметр ЕЕРВ і можуть бути основою формування інтегральних показників, а також використовуватися для аналізу впливу екологічних чинників (показників) на узагальнюючі результати виробничо-господарської діяльності;

– узагальнюючі – показники є головною, підсумковою і регулюючою оцінкою еколого-економічної ефективності технологічних процесів, забезпеченості підприємства основними природоохоронними фондами, рівня впливу виробництва на навколишнє природне середовище і т.д.

За рівнем визначення:

– народногосподарський рівень – аналізуються макроекономічні показники екологічної спрямованості;

– галузевий рівень – галузь розглядається в основному як сукупність підприємств, які об'єднуються за схожими характерними організаційно-технічними ознаками, оскільки сьогодні в основному відсутній дієвий галузевий організаційно-адміністративний розподіл матеріального виробництва;

- регіональний рівень - область, район;
- мікрорівень - підприємство;
- рівень внутрішньовиробничих підрозділів підприємств.

За часовим інтервалом:

- ретроспективні, поточні;
- фактичні, оперативні;
- прогнозні, планові.

За об'єктом оцінки:

– виробництво в цілому, окремі етапи відтворювальних процесів (виробничо-технологічні, переробні, організаційні, природоохоронні, ресурсозбережні та ін.);

- виробництво конкретних видів продукції (послуг);
- види (складові) виробничо-господарської діяльності підприємств (виробнича, інвестиційна та ін.).

За характером використання:

– регулюючі (дієві) – це показники, що безпосередньо застосовуються в процесі регулювання (управління) екологічності виробництва і якості навколишнього середовища, а також стану екосистем у процесі використання;

– індикаторні – показники, за допомогою яких може здійснюватися узагальнююча характеристика ЕВ у процесі аналізу;

– допоміжні показники забезпечують розрахунок комплексних, узагальнюючих еколого-економічних показників; можуть відігравати допоміжну роль при прийнятті складних, управлінських рішень.

## ВИСНОВКИ

В ході виконання завдань дипломної роботи було виконано ряд наступних робіт:

1. Описано поняття маршрутизації. В цілому маршрутизація – пересування інформації від джерела до пункту призначення через об'єднану мережу. Проаналізовано основні компоненти маршрутизації. Наведено основні алгоритми маршрутизації, зокрема, звернуто увагу на мету розробки алгоритму маршрутизації. Однією із цілей алгоритмів маршрутизації є збіжність.

2. Сформовано основні алгоритми маршрутизації.

3. Проведений аналіз і порівняння внутрішніх протоколів маршрутизації. Наведено їх характеристики. Розглянуто протокол зовнішньої маршрутизації.

4. Проведено дослідження динамічного протоколу маршрутизації OSPF. Протокол OSPF має ряд переваг:

- маршрути, обчислені протоколом OSPF, не можуть бути циклічними;
- протокол забезпечує масштабованість для великих мереж;
- швидке перенастроювання при зміні топології мережі.

До недоліків же відноситься:

- ієрархічна топологія;
- відсутній розподіл навантаження при нееквівалентних шляхах;
- метрика використовує тільки вартість маршруту.

Властивості збіжності включають швидкість поширення маршрутної інформації і обчислення оптимальних шляхів. Протоколи маршрутизації можуть бути оцінені на основі швидкості збіжності; чим швидша збіжність, тим кращий протокол маршрутизації.

5. Розроблено початкові налаштування маршрутизації для обладнання компанії Cisco Systems протоколів маршрутизації OSPF та EIGRP.

В розділі «Спеціальна частина» описано використання протоколів SKIP і IPSec, які використовуються для захисту даних на мережевому рівні.

В розділі «Обґрунтування економічної ефективності» здійснено економічні розрахунки, спрямовані на визначення економічної ефективності від дослідження збіжності мережі на базі динамічних протоколів маршрутизації, а також прийнято рішення щодо подальшого розвитку.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» опрацьовано наступні питання: принципи професійного відбору операторів ВДТ, працездатність операторів ВДТ, міжнародний тероризм, структура системи БЖД, елементи теорії, що відповідають моделі безпеки життєдіяльності.

В розділі «Екологія» проаналізовано вимоги до приміщень для експлуатації моніторів і ПЕОМ та розглянуто шляхи дотримання цих вимог, також було проведено статистичний аналіз екологічності виробництва.

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. RFC 1131. OSPF Specification Version 1 (J. Moy, Oct. 1989).
2. RFC 1245. OSPF Protocol Analysis (J. Moy, July 1991).
3. RFC 1246. Experience with the OSPF Protocol (J. Moy, July 1991).
4. RFC 1247. OSPF Version 2 [obsoletes 1131] (J. Moy, July 1991).
5. RFC 1248. OSPF Version 2 Management Information Base (F. Baker & R. Coltun, July 1991).
6. RFC 1252. OSPF Version 2 Management Information Base [obsoletes 1248] (F. Baker & R. Coltun, July 1991).
7. RFC 1253. OSPF Version 2 Management Information Base [obsoletes 1252] (F. Baker & R. Coltun, Aug. 1991).
8. RFC 1364. BGP OSPF Interaction [obsoletes 1247 and 1267] (K. Varadhan, Sept. 1992; IAB; L. Chapin, Oct. 1992).
9. RFC 1370. Applicability Statement for OSPF (IAB; L. Chapin, Oct. 1992).
10. RFC 1371. Choosing a "Common IGP" for the IP Internet (\ESG; P. Gross, Oct. 1992).
11. RFC 1403. BGP OSPF Interaction [obsoletes 1364] (K. Varadhan, Jan. 1993).
12. RFC 1583. OSPF Version 2 [obsoletes RFC1247] (J. Moy, March 1994).
13. RFC 1584. Multicast Extensions to OSPF (L Moy, March 1994).
14. RFC 1585. MOSPF: Analysis and Experience (J. Moy, March 1994).
15. RFC 1586. Guidelines For Running OSPF Over Frame Relay Networks (O. deSouza and M. Rodriguez, March 1994).
16. RFC 1587. The OSPF NSSA Option (V. Fuller & R. Coltun, March 1994).
17. RFC 1745. BGP4/IDRP for IP-OSPF Interaction (K. Varadhan, S. Hares, Y. Rekhter, Dec. 94).
18. RFC 1765. OSPF Database Overflow (L Moy, March 1995).

19. RFC 1793. Extending OSPF to Support Demand Circuits (J. Moy, April 1995).
20. RFC 1850. OSPF Version 2 Management Information Base [obsoletes 1253] (F. Baker & R. Coltun, Nov. 1995).
21. RFC 2178. OSPF Version 2 [obsoletes 1583](L Moy, July 1997).
22. RFC 2328. OSPF Version 2 [obsoletes 2178] (J. Moy, April 1998).
23. RFC 2370. The OSPF Opaque ISA Option (R. Coltun, July 1998).
24. RFC 2676. QoS Routing Mechanisms and OSPF Extensions (G. Apostolopoulos,  
25. D. Williams, S. Kamat, R. Guerin, A. Orda, T. Przygienda, August 1999).
26. RFC 2740. OSPF for IPv6 (R. Coltun, D. Ferguson, J. Moy, December 1999).
27. RFC 2844. OSPF over ATM and Proxy PAR (T. Przygienda, P. Droz, R. Haas, May 2000).
28. OSPF // Википедия. Свободная энциклопедия. – Режим доступа: [ru.wikipedia.org/wiki/OSPF](http://ru.wikipedia.org/wiki/OSPF). – Дата доступа: октябрь 2019 года. – Заглавие с экрана.
29. OSPF Design Guide // CISCO. – Режим доступа: [www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html](http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html). – Дата доступа: листопад 2019 року. – Заголовок з екрану.
30. В.Г. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / Олифер В.Г., Олифер Н.А. – СПб.: Питер, 2010. – 944 с. – ISBN: 978-5-49807-389-7
31. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. – Екатеринбург: Изд-во Урал. Ун-та, 2003. – 328 с. : ил.
32. Жуков І. А., Дрововозов В. І., Масловський Б. Г. Експлуатація комп'ютерних систем та мереж. Навч. Посібник. – К.: НАУ.2007.-368с.

33. Запечников, С.В. Основы построения виртуальных частных сетей [Текст]: Учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. – М.: Горячая линия-Телеком, 2003. – 249 с. ; 20 см. – 3000 экз. – ISBN 5-93517-139-2.

34. Збіжність // Всесвітні енциклопедичні знання. – Режим доступу: [http://uk.swewe.net/word\\_show.htm/?20332\\_3&%D0%97%D0%B1%D1%96%D0%B6%D0%BD%D1%96%D1%81%D1%82%D1%8C](http://uk.swewe.net/word_show.htm/?20332_3&%D0%97%D0%B1%D1%96%D0%B6%D0%BD%D1%96%D1%81%D1%82%D1%8C). – Дата доступу: листопад 2019 року. – Заголовок з екрану.

35. Зегжда Д. П. Как построить защищенную информационную систему. Технология создания безопасных систем [Текст] / Д. П. Зегжда, А. М. Ивашко ; под научн. ред. П. Д. Зегжды, В. В. Платонова. – СПб.: Мир и Семья-95, Интерлайн, 1998. – 256 с. : ил. ; 20 см. – 500 экз.

36. Олгри, Терри. Модернизация и ремонт сетей, 4-е издание. / Терри Олгри; пер. с англ. И.В. Берштейна, Л.М. Ильичевой, Е.Л. Полонской, А.П. Сергеева, Т.А. Шамренко; [глав. Ред. С.Н. Тригуб] – М.: Издательский дом „Вильямс”, 2005. – 1328 с. – ISBN: 5-8459-0688-1.

37. Методичні вказівки до виконання дипломної роботи ОКР “Магістр” для студентів спеціальності 8.05010101– Інформаційні управляючі системи та технології / Укладачі: О. В. Маєвський, О.В. Мацюк, М.В. Приймак, Г.В. Шимчук – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2014. – 196 с.

38. Сходимость сети // [marshrutizatsiia.ru](http://marshrutizatsiia.ru). – Режим доступу: <http://marshrutizatsiia.ru/sxodimost-seti.html>. – Дата доступу: ноябрь 2019 года. – Заглавие с экрана.

39. Тарасова В.В. Екологічна статистика (з блочно-модульною формою контролю знань). Підручник. / В.В. Тарасова – К.: Центр учбової літератури, 2008. – 392 с. – ISBN 978-966-364-669-5.

40. Томас, Том М. II Структура и реализация сетей на основе протокола OSPF, 2-е изд. : Пер. с англ. – М.: Издательский дом "Вильямс", 2004. – 816с.: ил.

41. Цапко В.Г. Безпека життєдіяльності: Навч. посіб. / За ред. В.Г. Цапка. - 3-тє вид., стер. - К.: Знання, 2004. - 397 с. – ISBN 966-8148-39-8.