АНОТАЦІЯ

Дослідження маршрутизація в межах автономної системи // Дипломна робота ОР «Магістр» // Панчук Віктор Васильович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНм–61 // Тернопіль, 2019 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА, МАРШРУТИЗАЦІЯ, ВІРТУАЛІЗАЦІЯ МЕРЕЖЕВИХ РЕСУРСІВ, ПРОГРАМНО КОНФІГУРОВАНА МЕРЕЖА, СЕРВІСИ, ПРОТОКОЛ, МОДЕЛІ ВІРТУАЛІЗАЦІЇ МАРШРУТИЗАЦІЇ.

У дипломній роботі проведено дослідження методів маршрутизації в межах автономної системи, віртуалізації мережевих ресурсів та запропоновано різні моделі використання в залежності від вхідних вимог.

В першому розділі дипломної роботи розглянуто актуальність питання маршрутизації в автономних системах, віртуалізації мережевих ресурсів та проведено аналіз такої реалізації через використання технології SDN. У результаті такого аналізу виявлено ряд труднощів при вирішенні специфічних задач з використанням цієї технології. Проведено порівняльний аналіз збільшення продуктивності при впровадженні SDN у порівнянні з технологією MPLS, що показало суттєвий приріст у продуктивності. Формування SDN кластерів з різними вхідними вимогами до маршрутизації та зменшення операційних витрат можливе через застосування технології NFV, що дало змогу визначити шляхи розвитку мережевих архітектур з гнучкими функціональними можливостями. За результатами дослідження визначено використання різних архітекур доступних для організації

маршрутизації в автономних системах, що в своїй основі об’єднують традиційну статичну та динамічну маршрутизацію з можливістю впровадження SDN рішень.

В другому розділі дипломної роботи описано вимоги до розроблюваної маршрутизації, що повинна функціонувати в межах автономної системи, а також проаналізовано ризики пов’язані з її порушенням. Здійснено аналіз можливостей застосування статичної маршрутизації для організації обміну даними. Детально визначено ситуації при яких відповідні протоколи, які динамічно визначають маршрути повинні бути застосовані.

В третьому розділі дипломної роботи на основі проведених досліджень запропоновано модель віртуалізації маршрутизації в автономній системі через резервування мережевих ресурсів з врахуванням потоків інформації та аналізом вимог до роботи. На основі запропонованої моделі визначено два варіанти віртуалізації, що дає змогу вирішувати поставлені завдання з ефективним розподілом ресурсів.

Метою роботи є аналіз і дослідження методів маршрутизації в автономній системі, що дасть змогу збільшити ефективність функціонування, підвищить надійність, продуктивність, гнучкість та визначить необхідні заходи для забезпечення роботи комп’ютерних мереж. Для досягнення поставленої мети необхідно виконати наступні завдання: провести аналіз наукових публікацій, результатів науково-дослідних робіт щодо організації маршрутизації в автономній системі, що дасть змогу надати рекомендації для вибору відповідних архітектурних рішень маршрутизації в залежності від вхідних вимог; проаналізувати вимоги до мережевих дизайнів з використанням віртуалізації мережевих ресурсів, що дасть змогу розробити вдосконалений дизайн з врахуванням вимог та специфіки бізнес процесів організації.

Об’єкт дослідження – процес маршрутизації даних у комп’ютерних мережах гетерогенної структури.

Предмет дослідження – теорія зв’язку у комп’ютерних мережах, теорія проектування мереж.

ANNOTATION

Routing study within an isolated system // Diploma thesis Master degree // Panchuk Viktor V. // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2019 // P. , Tables – , Fig. – , Diagrams – , Annexes. – , References – .

In the thesis work the research of routing methods within the autonomous system were conducted, virtual measurement resources and various options were used in the input requirements.

In the first section of the thesis, actual issues of routes in autonomous systems, virtualization of resources were provided and analysis of SDN usage was carried out. As a result, a number of difficulties for specific tasks of all these technologies was found. A comparative analysis of performance in the study of SDN compared with MPLS technology, which showed a significant increase in productivity. Formation of SDN clusters with different input views on routing and reduction of operational capabilities to use through NFV technology, which allows to change ways of development of measuring architectures with flexible functionalities was displayed. As the results of the study, different architectures available for routing in autonomous system that are known for traditional static and dynamic routing with addition of the use of an SDN deployment are explored.

Second section of the thesis describes the requirements for created routing that operate within the autonomous system, and analyzes the necessary conditions that exist with its requirements. The analysis performed reflect the use of statistical routes to organize data exchange. Understanding in detail the response of protocols that dynamically make routes was conducted.

In the third section of the thesis on base of prepared results the model of virtual routing in the autonomouse system is offered with ability of reserve amount of measured resources with the accounted flows of information and analytically

required work. As the result there are two virtualization options that can be used to deliver results with effective distributed resources.

The purpose of the work is to analyze and explore the methods of routing in the autonomous system that allows to achieve effective functionality, while maintaining reliability, productivity, the need for work and the necessary responsibilities to work in the computer networks. In order to achieve this goal, the following tasks must be accomplished: research the analysis of scientific publications, the results of research that carried out routing in an autonomous system, which can provide guidance of the choice of modern architectural routing with the ability of including the input requirements; provide analyzis of requirements for mixed designs with virtualization of routing resources that allows to develop advanced designs that take into account the necessary and specific involved business processes.

The object of research - the process of routing data in autonomouse system of computer networks of a heterogeneous structure.

The subject of research - the theory of communication in computer networks, the theory of network design.

Keywords: COMPUTER NETWORK, ROUTING, NETWORK RESOURSES VIRTUALIZATION, SOFTWARE DEFINED NETWORK, SERVICE, PROTOCOL, MODELS OF ROUTING VIRTUALIZATION.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SDN – Software Defined Network

NFV – Network Function Virtualization

MPLS – Multi Protocol Label Switching

QoS – Quality of Service

RFC – Request For Comments

BGP – Border Gateway Protocol

IP – Internet Protocol

QoE – Quality of Experience

HSRP – Hot Standby Router Protocol

RIP – Routing Information Protocol

OSPF – Open Shortest Path First

EIGRP – Enhanced Interior Gateway Routing Protocol

IETF – Internet Engineering Task Force

IGP - Interior Gateway Protocol

DR – Designated Router

BDR – Backup Designated Router

ПКМ – Програмно Конфігурована Мережа

ЗМІСТ

ВСТУП

Актуальність роботи полягає у необхідності дослідження методів маршрутизації в межах автономної системи.

Одним з найбільш актуальних наукових завдань у галузі телекомунікацій є передавання трафіку з дотриманням низки вимог щодо якості обслуговування. Це пов’язано із тим, що множина потоків даних передається по мережі, ресурси якої необхідно розподілити між цими потоками за певною пропорцією. Оскільки дані, які підлягають передаванню, різні за своєю природою та важливістю, то необхідно мати механізми, які дають змогу розв’язувати задачу розподілу ресурсів оперативно, у відповідності до властивостей тих потоків, які передаються у конкретний момент часу через конкретні телекомунікаційні вузли. Такі механізми повинні базуватись на удосконалених методах розподілу ресурсів, що мають високу масштабованість, швидкодію, гнучкість, низьку операційну складність та ресурсоємність.

Для підвищення якості обслуговування (QoS) переданого мережевого трафіку актуальним є пошук гнучких методів управління мережними ресурсами для забезпечення їхнього збалансованого завантаження й гарантованої якості обслуговування різнорідного трафіку користувачів у мультисервісних мережах.

Таким чином, розширення спектру послуг, масштабування інфраструктури та обсяги трафіку, що постійно зростають спонукають до розв’язання наукового завдання покращення якості обслуговування трафіку в мультисервісних мережах за рахунок впровадження нових методів маршрутизації чи вдосконалення існуючих.

Мета і задачі дослідження. Метою роботи є аналіз і дослідження методів маршрутизації в межах автономної системи, що дасть змогу збільшити ефективність функціонування, підвищить надійність,

продуктивність, гнучкість та визначить необхідні заходи для забезпечення роботи комп'ютерних мереж. Для досягнення поставленої мети необхідно виконати наступні завдання: провести аналіз наукових публікацій, результатів науково-дослідних робіт щодо організації маршрутизації в автономній системі, що дасть змогу надати рекомендації для вибору відповідних архітектурних рішень маршрутизації в залежності від вхідних вимог; проаналізувати вимоги до мережевих дизайнів з використанням віртуалізації мережевих ресурсів, що дасть змогу розробити вдосконалений дизайн з врахуванням вимог та специфіки бізнес процесів організації.

Об'єкт дослідження – процес маршрутизації даних у комп'ютерних мережах гетерогенної структури.

Предмет дослідження – теорія зв'язку у комп'ютерних мережах, теорія проектування мереж.

Практичне значення одержаних результатів. На основі отриманих результатів запропоновано методи маршрутизації в межах автономної системи, що базуються на аналізі потоків та вимог до функціонування.

Наукова новизна отриманих результатів: проведено аналіз реалізації маршрутизації в межах автономної системи через використання технології SDN. Проведено порівняльний аналіз збільшення продуктивності при впровадженні SDN у порівнянні з технологією MPLS. Формування SDN кластерів з різними вхідними вимогами до маршрутизації та зменшення операційних витрат можливе через застосування технології NFV, що дало змогу визначити шляхи розвитку мережевих архітектур з гнучкими функціональними можливостями. За результатами дослідження визначено використання різних архітекур доступних для організації маршрутизації в автономних системах, що в своїй основі об'єднують традиційну статичну та динамічну маршрутизацію з можливістю впровадження SDN рішень.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Порівняльний аналіз засобів маршрутизації в автономній системі

Проведений аналіз літературних джерел [1-30] дав змогу визначити ключові, на сьогоднішній день, методи маршрутизації, що використовуються або є перспективними для впровадження. В подальшому викладі матеріалу розглянуто основні характеристики, визначено переваги та недоліки вибраних технологій.

Окрім традиційних методів маршрутизації все більшої популярності набирають мережі створені на базі комутації міток або програмно конфігуровані мережі. Такі підходи суттєво спрощують впровадження нових технологій, оскільки вони є протокольно та технологічно незалежними і гнучкими в побудові та функціонуванні.

Для аналізу ефективності впровадження технології SDN у роботі проведено детальний аналіз побудови маршрутів у мережах, створених на основі технологій SDN та MPLS.

На контролері SDN створюються таблиці, в яких зберігається карта мережі. Найчастіше для їх створення використовують протокол OSPF (англ. Open Shortest Path First), тобто протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (Dijkstra's algorithm).

Оскільки алгоритм Дейкстри побудований на графах, то карту магістральної мережі розглядатимемо як граф з вершинами в точках встановлення мережевих пристроїв і ребрами, які відображають зв’язки між ними. Алгоритм Дейкстри на графах знаходить найкоротший шлях від однієї вершини графа до всіх інших вершин.

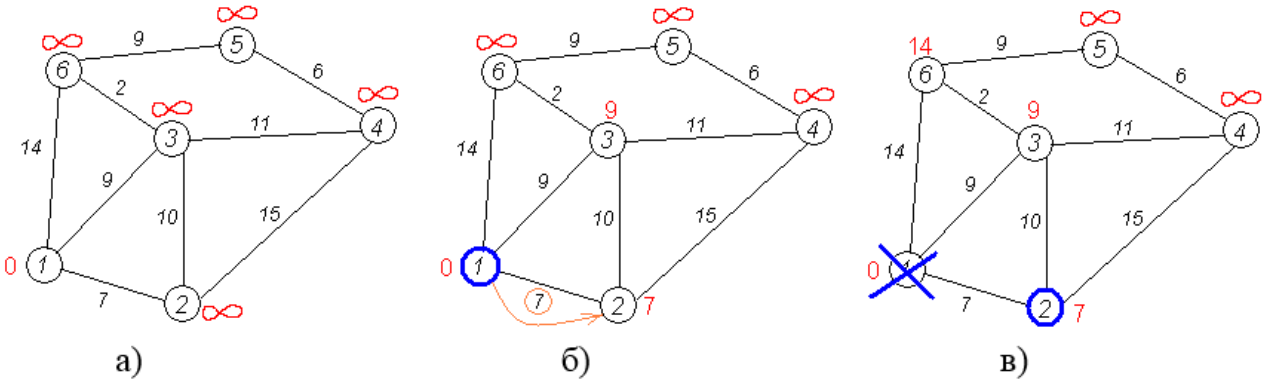

Рисунок 1.1 – Схематичне зображення алгоритму Дейкстри

Розглянемо конкретний приклад роботи алгоритму Дейкстри для графу, поданого на рисунку 1.1. Алгоритм використовує множину L, що містить вершини графа, для яких найкоротший шлях від вихідної вершини r уже знайдено. Він також використовує масив s[1..n] (де n – кількість вершин графа G), в якому для кожної вершини $v \in V$ зберігається поточне значення найкоротшого шляху. Опишемо послідовність алгоритму Дейкстри:

1. Ініціалізація. Відстань до всіх вершин графа V = ∞. Відстань до a = 0. Жодна вершина графа ще не опрацьована (див. рисунок 3.1(а)).

2. Знаходимо таку вершину (із ще не оброблених), поточна найкоротша відстань до якої мінімальна. В нашому випадку це вершина 1. Обходимо всіх її сусідів і, якщо шлях в сусідню вершину через 1 менший за поточний мінімальний шлях в цю сусідню вершину, то запам'ятовуємо цей новий, коротший шлях як поточний найкоротший шлях до сусіда.

3. Перший по порядку сусід 1-ї вершини — 2-а вершина. Шлях до неї через 1-у вершину дорівнює найкоротшій відстані до 1-ї вершини + довжина дуги між 1-ю та 2-ю вершиною, тобто 0 + 7 = 7. Це менше поточного найкоротшого шляху до 2-ї вершини, тому найкоротший шлях до 2-ї вершини дорівнює 7 (див. рис. 3.1(б)).

Кроки 4, 5. Аналогічну операцію виконуємо з двома іншими сусідами 1-ї вершини — 3-ю та 6-ю.

6. Всі сусіди вершини 1 перевірені. Поточна мінімальна відстань до вершини 1 вважається остаточною і обговоренню не підлягає (те, що це дійсно так, вперше довів Дейкстра). Тому викреслимо її з графа, щоб відмітити цей факт (див. рис. 3.1(в)).

7. Практично відбувається повернення до кроку 2. Знову знаходимо «найближчу» необроблену (невикреслену) вершину. Це вершина 2 з поточною найкоротшою відстанню до неї рівною 7. Знову намагаємося зменшити відстань до всіх сусідів 2-ої вершини, намагаючись пройти в них через 2-у. Сусідами 2-ої вершини є 1, 3, 4.

8. Перший (по порядку) сусід вершини № 2 — 1-а вершина. Але вона вже оброблена (або викреслена — див. крок 6). Тому з 1-ою вершиною нічого не робимо. Крок 8 (з іншими вхідними даними). Інший сусід вершини 2 — вершина 4. Якщо йти в неї через 2-у, то шлях буде = найкоротша відстань до 2-ої + відстань між 2-ою і 4-ою вершинами = 7 + 15 = 22. Оскільки $22 < \infty$, встановлюємо відстань до вершини № 4 рівним 22.

9. Ще один сусід вершини 2 — вершина 3. Якщо йти в неї через 2-у, то шлях буде = 7 + 10 = 17. Але 17 більше за відстань, що вже запам'ятали раніше до вершини № 3 і дорівнює 9, тому поточну відстань до 3-ої вершини не міняємо.

10. Всі сусіди вершини 2 переглянуті, заморожуємо відстань до неї і викреслюємо її з графа.

Кроки 11 — 15. По вже «відпрацьованій» схемі повторюємо кроки 2 — 6. Тепер «найближчою» виявляється вершина № 3.

Далі виконуємо те саме з вершинами, що залишилися (№ по порядку: 6, 4 і 5).

Завершення виконання алгоритму відбувається, коли викреслені всі вершини. Найкоротший шлях від 1-ої вершини до 2-ої становить 7, до 3-ої — 9, до 4-ої — 20, до 5-ої — 20, до 6-ої — 11 умовних одиниць.

Отже, у ході кожної нової ітерації алгоритму до множини L додається нова вершина u, така, що

$$s[u] = \min \{s[u] | V^{\in} (V - L\} \quad . \tag{1.1}$$

Після додавання вершини всі значення масиву s[v] оновлюються, якщо сума відстані до вершини u та ваги ребра менша, ніж поточна відстань до вершини. Алгоритм закінчує роботу, коли L=V.

Кожна операція додавання вершини до множини L та операція переходу до наступної вершини займає час O(1), а кожна операція пошуку мінімуму (s[u]=min{s[v]|v$^{\in}$ (V-L)}) O(V) (оскільки в ній виконується пошук по всьому масиву); в результаті повний час роботи алгоритму дорівнює $O(V^2)$. Використовуючи деякі швидші структури даних (наприклад, чергу з пріоритетом), можна пришвидшити цей алгоритм.

Тепер змоделюємо мережу, в якій є 200 мережевих пристроїв. В найгіршому випадку, коли немає жодної початкової інформації, тобто передається перший пакет, складність передачі буде рівна 40000 операцій (200^2). Крім того, для зчитування даних з отриманого пакету і заповнення всіх необхідних полів таблиці OpenFlow, необхідно ще 356 операцій. Отже, загалом для розпізнавання пакету і вибору оптимального маршруту, нам знадобиться 40356 операцій. Процесор з тактовою частотою 1 ГГц може виконати 10^8 операцій за секунду. Таким чином, весь цей процес займе приблизно 0,4мс. Так як оптимальний маршрут будується на основі ваг ребер, які можна легко змінювати в залежності від частоти використання каналу, завантаженості середовища, пропускної здатності і т.д., то це максимально спрощує використання статистичних методів при побудові маршрутів, які дадуть змогу максимально врахувати всі деталі даної мережі.

Проаналізуємо роботу мережі IP/MPLS. Як і SDN, мережа IP/MPLS перед початком передачі даних проводить пошук оптимального шляху за наперед прописаним алгоритмом. Він базується на тому, що кожен мережевий пристрій передає іншому спеціальне повідомлення, в якому вказується певне відносне значення ваги шляху. Таким чином кожен комутатор чи маршрутизатор зможе вибрати найкоротший шлях передачі даних. Лістинг 1.1 демонструє спрощений псевдокод побудови маршрутів у мережі MPLS.

Лістинг 1.1:

```
private void sending(int k)
{
    int j;
    for(j = 0; j < N; j++)                    } N^2
        if (j != k)
        {
            send_message(j);  //передача ваги шляху
            sending(j);
        }
}

    for (i = 0; i < N; i++)
    {
        send_query(i);    //запит на отримання ваг
шляхів
        sending(i);
    }
```

Загальна складність даного алгоритму становить O(N3), оскільки рекурсивна функція, складність якої O(N2), викликається в циклі N разів. Якщо повернутись до попереднього прикладу, де в мережі є 200 пристроїв, то мережа на основі IP/MPLS побудує маршрут за час 8 мс.

Занесемо отримані дані в таблицю для зручнішого їх порівняння.

Таблиця 1.1 – Порівняння швидкодії роботи технологій SDN та IP/MPLS при визначенні найкоротшого шляху.

Технологія управління	**Частота процесора**	**Кількість пристроїв**	**Час побудови маршруту**	**Врахування статистики**
IP/MPLS	1 ГГц	200	0,008 с	Неможливе
SDN	1 ГГц	200	0,0004 с	Можливе

Отже, як видно з таблиці 1.1, мережі, побудовані за технологією SDN, мають меншу затримку передачі даних і дають більше можливостей при побудові маршрутів. Проте, кожна з цих технологій має як переваги, так і недоліки.

1.2 Аналіз роботи SDN як перспективного методу організації маршрутизації

Стрімке зростання обсягів трафіку і зміна його структури, необхідність підтримки великої кількості користувачів, формування високопродуктивних кластерів для обробки великих обсягів даних і добре масштабованих віртуалізованих середовищ для надання хмарних сервісів – все це серйозно змінило вимоги до мережевих середовищ. І все частіше мережа перетворюється на обмежуючий фактор розвитку обчислювальної інфраструктури.

Головна проблема – традиційні мережі занадто статичні і тому не відповідають динаміці, що властива сучасним процесам обміну даними, на відміну від серверів – чим останні зобов'язані технологіям віртуалізації. Сьогодні додатки розподілені між безліччю віртуальних машин, які інтенсивно обмінюються даними. Для оптимізації завантаження серверів віртуальні машини часто мігрують, що змінює точки “прив’язки” трафіку. Традиційні схеми адресації, логічного поділу мереж і способи призначення

правил обробки трафіку в таких динамічних середовищах стають неефективні.

Схожі труднощі виникають і з реконфігурацією механізмів Quality of Service (QoS) при додаванні в мультисервісну мережу нового додатка, наприклад відеозв'язку. Занадто багато часу у великих мережах займають процедури зі зміни параметрів захисту, що не дозволяє оперативно реагувати на виникаючі загрози.

Впровадження технологій програмно-конфігурованих мереж та віртуалізації мережевих функцій може стати саме тим фактором, який дозволить вирішити існуючі проблеми і радикально змінити підхід до організації та керування мережею.

Під програмно-конфігурованою мережею (Software-defined Networking, SDN) розуміють мережу передачі даних, в якій рівень управління мережею відділений від пристроїв передачі даних і реалізується програмно, вона являє собою одну з форм віртуалізації обчислювальних ресурсів. Дані передаються відповідно до таблиць маршрутизації, що зберігаються на апаратних системах, як і згідно існуючих підходів. Але ці таблиці централізовано керуються віддаленою системою, у зв’язку з чим зникає необхідність змінювати таблиці на кожному комутаторі окремо. В ідеальному випадку всі мережеві компоненти повинні управлятися і налаштовуватися в ході однієї операції.

Спільна робота компонентів програмно обумовленої мережі може бути заснована на стандарті OpenFlow. Ключові принципи SDN – поділ процесів передачі та управління даними, централізація управління мережею за допомогою уніфікованих програмних засобів, віртуалізація фізичних мережевих ресурсів. Протокол OpenFlow, який реалізує незалежний від виробника інтерфейс між логічним контролером мережі і мережевим транспортом, є однією з реалізацій концепції програмно-конфігурованої мережі. Головна ідея SDN полягає у відділенні функцій передачі трафіку від

функцій управління (включаючи контроль як самого трафіку, так і пристроїв, що здійснюють його передачу). У традиційних комутаторах і маршрутизаторах ці процеси невіддільні один від одного і реалізовані в одній “коробці”: спеціальні мікросхеми мережевого обладнання забезпечують пересилання пакетів з одного порту на інший, а вищерозміщене програмне забезпечення визначає правила такого пересилання, виконує необхідний аналіз пакетів, виконує зміну службової інформації, що міститься в них і т. д. Для визначення маршруту передачі або недопущення зациклення трафіку пристрої, звичайно, обмінюються між собою даними, для чого розроблено безліч протоколів, таких як Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) і Spanning Tree, але при цьому кожен пристрій функціонує досить автономно.

Реалізація концепції SDN на практиці дозволить підприємствам і операторам зв’язку отримати вендоронезалежний контроль над всією мережею з єдиного місця, що значно спростить її експлуатацію. Що не менш важливо, конфігурування мережі сильно спроститься і адміністраторам не доведеться вводити сотні рядків коду окремо для різних комутаторів або маршрутизаторів. Характеристики мережі можна буде оперативно змінювати в режимі реального часу, відповідно, терміни впровадження нових додатків і сервісів значно скоротяться.

Основним елементом концепції SDN є протокол OpenFlow, який забезпечує взаємодію контролера з мережевими пристроями. Контролер надає програмні інтерфейси (Application Programming Interface, API), наявність яких дозволяє власнику мережі або стороннім розробникам створювати додатки для управління мережею. Такі програми можуть виконувати різноманітні функції в інтересах бізнес-завдань (наприклад, контролювати доступ, управляти пропускною здатністю і т. п.), причому їх розробникам не треба знати деталі функціонування конкретних мережевих пристроїв. Завдяки контролеру, вся мережа, що складається з безлічі

різнотипних пристроїв різних виробників, постає для програми як один логічний комутатор.

Як і випливає з назви, протокол OpenFlow при ідентифікації трафіку оперує поняттям “потоку”. Ключовим елементом комутатора, що підтримує цей протокол, є таблиця потоків (Flow Table). Група стовпців в лівій частині таблиці формує поля відповідності, де вказані характеристики потоків: це можуть бути різні параметри, включаючи Media Access Control (MAC) адреси і Intenet Protocol (IP) адреси відправника і одержувача, ідентифікатор Virtual Local Area Network (VLAN), номера протокольних портів Transmission Control Protocol (TCP) і User Datagram Protocol (UDP), а також інша інформація. Ці дані за допомогою протоколу OpenFlow записує в таблицю комутатора контролер, він же визначає пріоритет різних потоків: чим вище пріоритет, тим вище відповідний запис у таблиці потоків.

Вхідні пакети перевіряються на відповідність зазначеним у таблиці параметрам. Якщо відповідність виявлено, до пакетів застосовується дія, яка вказана в наступному стовпці таблиці. Типовою дією є пересилання пакета на один або кілька вихідних портів. Крім того, комутатор може змінити вміст службових полів пакету, скинути його, направити для аналізу контролеру і т.д. У разі, якщо збіг не знайдено, пакет відкидається або надсилається контролеру, який визначить, як слід обробляти даний потік, і додасть відповідний запис у таблицю. Статистика по трафіку - число пакетів, байтів і ін. розміщується у відповідних полях.

Використовуючи протокол OpenFlow, контролер додає, модифікує і видаляє записи в таблиці потоків. Крім того, він може запитувати у комутатора його характеристики і зібрану статистику, конфігурувати комутатор і його окремі порти. У більшості сучасних комутаторів Ethernet використовуються таблиці потоків, які описують, як найбільш ефективно доставити пакет від відправника до пункту призначення. У кожного постачальника таблиця потоків своя, проте можна виділити набір функцій,

загальних для більшості комутаторів старшого класу, наприклад якість обслуговування і звітність по трафіку. OpenFlow стандартизує цей загальний набір функцій.

OpenFlow відокремлює один від одного функції потоку даних і потоку управління, що традиційно реалізуються комутаторами.

Функціональність, що відноситься до потоку даних, як і раніше виконується на комутаторі, але за прийняття рішень про високорівну маршрутизацію в OpenFlow відповідає контролер, як правило організований на базі стандартного сервера. Комутатор і контролер спілкуються по протоколу OpenFlow Switching Protocol. Контролер може, наприклад, наказати коммутаторам ввести в дію правила для потоків мережевого трафіку. Такі правила можуть, зокрема, забезпечувати відправку даних по найшвидшим маршрутам або за маршрутами, які мають мінімум транзитних ділянок.

OpenFlow надає єдиний API, за допомогою якого адміністратори можуть програмувати роботу мережі, а також задавати правила маршрутизації пакетів, балансування навантаження та управління доступом. У цей API типово входять два основні компоненти: програмний інтерфейс для контролю пересилання пакетів через мережеві комутатори і набір глобальних інтерфейсів, на основі яких можна створювати високорозвинені інструменти управління.

Впровадження протоколу OpenFlow дає можливість отримати ряд важливих переваг. Так, завдяки зняттю з комутаторів навантаження по обробці тракту управління, OpenFlow дозволить цим пристроям спрямувати всі свої ресурси на прискорення переміщення трафіку. За рахунок віртуалізації управління мережею OpenFlow знижує витрати на побудову та супровід мереж. Також, програмні засоби OpenFlow дозволять адміністраторам додавати нову функціональність до наявної мережевої архітектурі. При цьому нові функції будуть працювати на багатьох

платформах – їх не доведеться реалізовувати заново у вбудованому програмному забезпеченні комутаторів кожного постачальника. Крім того, технологія OpenFlow обіцяє можливість створення віртуальних мережевих топологій – побудова в разі необхідності віртуальних локальних або глобальних мереж без фізичного зміни мережі. Для цього передбачена можливість створення централізованої віртуальної площині управління, що забезпечує функції мережевого адміністрування. Ця функція може бути особливо корисною для управління центрами обробки даних та при організації платформ віртуалізованих ресурсів. Тобто, дана технологія здатна забезпечити необхідний “хмарним” сервісам рівень “інтелектуальності” мереж, зокрема для оркестрування роботи значних груп комутаторів. Автоматизованих інструментів віртуалізації, що дозволяють оперативно виділяти мережеві сегменти, хмарні платформи більшості компаній досі не мають. Відсутність таких інструментів спонукає найбільш зацікавлені компанії при побудові та реконфігурації мереж звертатися до технологій SDN.

Фактори, що стимулюють віртуалізацію мереж, сильно відрізняються від факторів, що викликають віртуалізацію серверів. Наявні в компаніях обчислювальні ресурси, як правило, недозавантажені, тому вигідна їх консолідація. Мережам же недозавантаження не страшне – скоріше, навпаки. Тому, метою віртуалізації мереж є підвищення їх гнучкості та ємності. Все більш популярним стає підхід до мереж, орієнтований на потреби додатків. Компанії фокусують свою увагу на прискореному запуску нових послуг, а також полегшенні процесів виділення ресурсів, управлінням мережами та зміни їх конфігурації відповідно до вимог додатків. Ще однією важливою перевагою віртуалізації мереж є скорочення витрат на мережеву інфраструктуру. Наприклад, комутатори, що відповідають вимогам інфраструктури операторів зв'язку, досить дорогі. При цьому значна частина їх ціни припадає на програмне забезпечення, що реалізує безліч надлишкових

(у разі конкретних потреб) функцій. Завдяки перенесенню управління на рівень центрального контролера, компанії отримують можливість купувати недороге обладнання з мінімальною інтелектуальною складовою.

Порівняння традиційних архітектур з віртуалізованою мережею на основі технології SDN показано на рисунку 1.2.

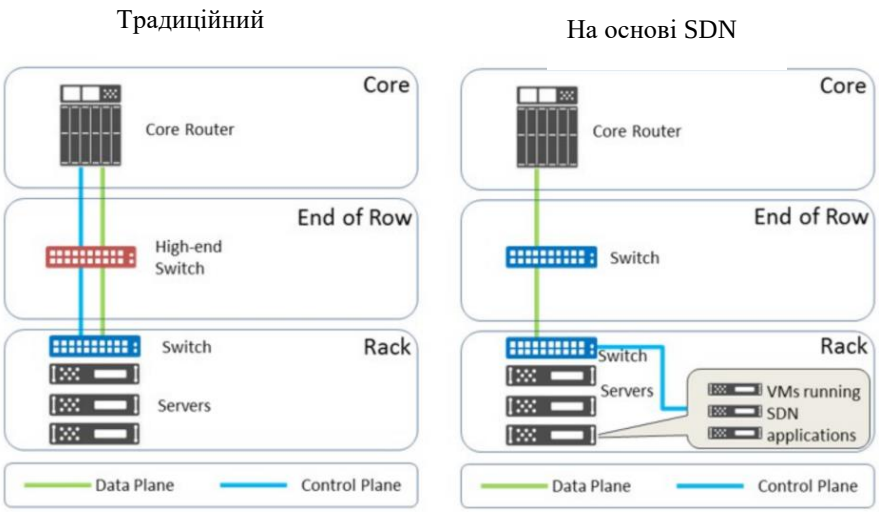

Рисунок 1.2 – Поріняння традиційного мережевого дизайну та на основі SDN

Як видно з поданого аналізу традиційний трирівневий дизайн може бути застосований при проектуванні мереж з сталими вимогами до використання та малими змінами в часі до вимог користувачів. При цьому потрібно розуміти, що зміна ситуації буде провокувати додаткові фінансові витрати та затримки пов’язані з впровадженням нових змін, а також може збільшувати операційні витрати.

1.3 Мережева архітектура на основі віртуалізації мережевих функцій

У переході до програмного управління мережами окрім технології SDN ключову роль грає технологія віртуалізації мережевих функції NFV. Ці технології доповнюють один одного в тому, що вони звертаються до різних

елементів забезпечення програмно-керованого рішення. SDN збільшує гнучкість мережі за допомогою цілісного управління мережею, дозволяє швидко впроваджувати інновації і знижує експлуатаційні витрати. NFV розробляється для того, щоб оператори могди зменшити експлуатаційні витрати Capital Expenditure (CAPEX) і Operational Expenditure (OPEX) за рахунок зниження витрат на устаткування і зниження енергоспоживання.

Окрім цього, NFV також зменшує складність і робить управління мережею і розгортання нових можливостей більш легким і швидшим. Віртуалізація мережевих функцій – це концепція мережевої архітектури, що пропонує використовувати технології віртуалізації для віртуалізації цілих класів функцій мережевих вузлів у вигляді складових елементів, які можуть бути з'єднані разом або пов'язані в ланцюжок для створення телекомунікаційних послуг (сервісів). NFV відрізняється від традиційних способів віртуалізації, що використовуються в інформаційних технологіях рівня підприємства. Функція мережі, що віртуалізується (virtualized network function, VNF) може включати одну або кілька віртуальних машин, що використовують різноманітне програмне забезпечення та процеси, на верхівці галузевих стандартів сервери, комутатори і сховища великого обсягу, або навіть інфраструктури хмарних обчислень, замість окремих апаратних рішень для кожної конкретної мережевої функції. Суть ідеї віртуалізація мережевих функцій в новому підході до побудови мережевої архітектури, при якому на уніфікованому фізичному середовищі працюють програмні додатки, що реалізують різні мережеві функції. Відповідно до цієї ідеї, NFV дозволяє операторам розгортати мережні рішення (Deep Packet Inspection (DPI), Network Address Translation (NAT), Firewall і т.д.) як програмні додатки, а не як окремі мережеві пристрої. Робота програм NFV і сама реалізація віртуальних функцій можлива на високопродуктивних мережевих платформах і серверах, розташованих у центрах обробки даних, мережевих вузлах і обладнанні клієнтів. Важливим позитивним чинником

розвитку NFV є зниження залежності оператора від вузькоспеціалізованих мережевих пристроїв на користь програмних інструментів, що в кінцевому рахунку радикально знижує операційні витрати на підтримку всього життєвого циклу мережевих послуг.

Взаємозв'язок з концепцією SDN полягає у тому, что загальним трендом обох технологій у галузі телекомунікацій є напрямок на віртуалізацію мережі і використання нових концепцій, в суті яких лежить програмне керування. Найважливішою відмінністю NFV від SDN є кінцева мета концепції. Якщо в NFV планується взяти конкретні мережеві функції і реалізувати їх програмно, а потім керувати ними як програмними об'єктами, то SDN – це ідеологія роботи всієї мережі, де все управління і відповідальність за прийняття рішень (маршрутизація, комутація і т.д.) винесені на окремий централізований рівень. Тобто, NFV – це конкретні програмні компоненти, що реалізують конкретні мережеві функції, а SDN – ідеологія роботи всієї мережі і взаємодії її функціональних рівнів. Основні архітектурні складові реалізації NFV (Architectural Framework) це:

1. Інфраструктура віртуалізації мережевих функцій (NFVI, Network Functions Virtualisation Infrastructure), яка забезпечує віртуальні ресурси, необхідні для підтримки виконання віртуалізованих мережевих функцій (VNF). Вона включає в себе апаратне забезпечення COTS (Commercial-OffThe-Shelf), компоненти прискорення в разі необхідності, і програмний шар, який віртуалізує базове устаткування.

2. Віртуалізована мережева функція (VNF, Virtualised Network Function) — це програмна реалізація мережної функції, яка здатна працювати на NFVI. Вона може супроводжуватися системою управління елементами (Element Management System, EMS), до тих пір, поки застосовується щодо конкретної функція, яка реалізує і виконує управління індивідуальною VNF і своїми особливостями. VNF — це об'єкт, який відповідає мережевим вузлам

традиційної архітектури, які планується реалізувати безпосередньо в програмному забезпеченні вільному від апаратної залежності.

3. NFV M&O (Management and Orchestration, Керування та оркестрація) охоплює адміністрування та управління життєвим циклом фізичних та/або програмних засобів, що підтримують інфраструктуру віртуалізації і управління життєвим циклом функцій VNF. NFV M&O фокусується на конкретних завданнях управління віртуалізації необхідних в рамках реалізації NFV. NFV M&O також взаємодіє із зовнішнім по відношенню до NFV зоною OSS/BSS, що дозволяє інтегрувати NFV у вже існуючі зони управління в масштабах цілої мережі.

Проект ETSI (European Telecommunications Standards Institute) пропонує конкретне бачення концепцій адміністрування NFV. Це проект зі створення архітектури управління віртуалізованою мережевою інфраструктурою, яка дозволяє “побачити” функціональні можливості NFV з експлуатаційних позицій оператора “хмарних” послуг. Метою запропонованої архітектури MANO (Management and Orchestration) є забезпечення можливості для оператора, що працює з хмарним ЦОД, об’єднувати і керувати всіма ресурсами (обчислювальними, мережевими, сховищами даних і віртуальними машинами). Даний проект вже встиг охопити питання вимог, архітектур і сценаріїв використання NFV. Ядро архітектури MANO складається з трьох функціональних блоків:

NFV Orchestrator, VNF Manager, Virtualised Infrastructure Manager (VIM). NFV Orchestrator відповідає за наступні функції:

– управління життєвим циклом мережевого сервісу (від інсталяції до термінування);

– високорівневе управління ресурсами, валідація та авторизація запитів до віртуальної інфраструктури.

VNF Manager дозволяє:

– керувати життєвим циклом віртуальних мережевих об'єктів;

– погоджувати взаємодію між віртуальною інфраструктурою і N/EMS.

VIM забезпечує:

– управління віртуальною інфраструктурою;

– управління продуктивністю і моніторинг подій.

NFV M&O (Management and Orchestration, Керування та оркестрація) охоплює адміністрування та управління життєвим циклом фізичних та/або програмних засобів, що підтримують інфраструктуру віртуалізації і управління життєвим циклом функцій VNF. NFV M&O фокусується на конкретних завданнях управління віртуалізації необхідних в рамках реалізації NFV. NFV M&O також взаємодіє із зовнішнім по відношенню до NFV зоною OSS/BSS, що дозволяє інтегрувати NFV у вже існуючі зони управління в масштабах цілої мережі. Вся система NFV приводиться в дію набором метаданих, що описують обслуговування, функції VNF і вимоги до інфраструктури, і таким чином NFV M&O може функціонувати відповідним чином. Ці інструкції разом з сервісами, віртуалізованими функціями та інфраструктурою можуть бути забезпечені різними компаніями галузі.

Компоненти архітектурної реалізації взаємодіють за допомогою певних опорних точок, так що різні об’єкти можуть бути чітко відокремлені, що сприяє відкритості та інноваційності екосистеми NFV. Опорні точки між VNF і NFVI (і так само між суб’єктами в NFVI) погоджені з абстракцією і віртуалізацією ресурсів та хостингом функцій VNF, так що функції VNFs можуть не просто бути перенесені тільки з однією інфраструктури NFVI до іншої, а й забезпечують той факт, що можуть підтримуватися різні варіанти базового обладнання. Опорні точки між NFV M&O і VNF а, також, між M&O і NFVI (а також між сутностями всередині M&O) погоджуються з керуванням і експлуатацією системи NFV. Відповідні базові блоки сконструйовані таким чином, що дозволяють повторне використання існуючих рішень (наприклад, системами «хмарного» адміністрування), а

також взаємодію з існуючим середовищем OSS/BSS, до якого необхідно під'єднувати систему NFV.

Коли провайдер послуг створює з'єднання з новим місцем, то є декілька пристроїв, що мають бути обов'язково інстальовані в мережі. Це керований маршрутизаторо та демаркаційний пристрій, який має ключову роль розділяючи мережу провайдера та клієнта. Крім стандратного обладнання провайдер змушений ставити деяке додадкове для вирішення певних бізнес задач. Як результат, закупка та підтримка такого набору стає дуже затратною і NFV вирішує ці питання.

Порівняльний аналіз традиційної архітектури та з використанням NFV показано на рисунку 1.2.

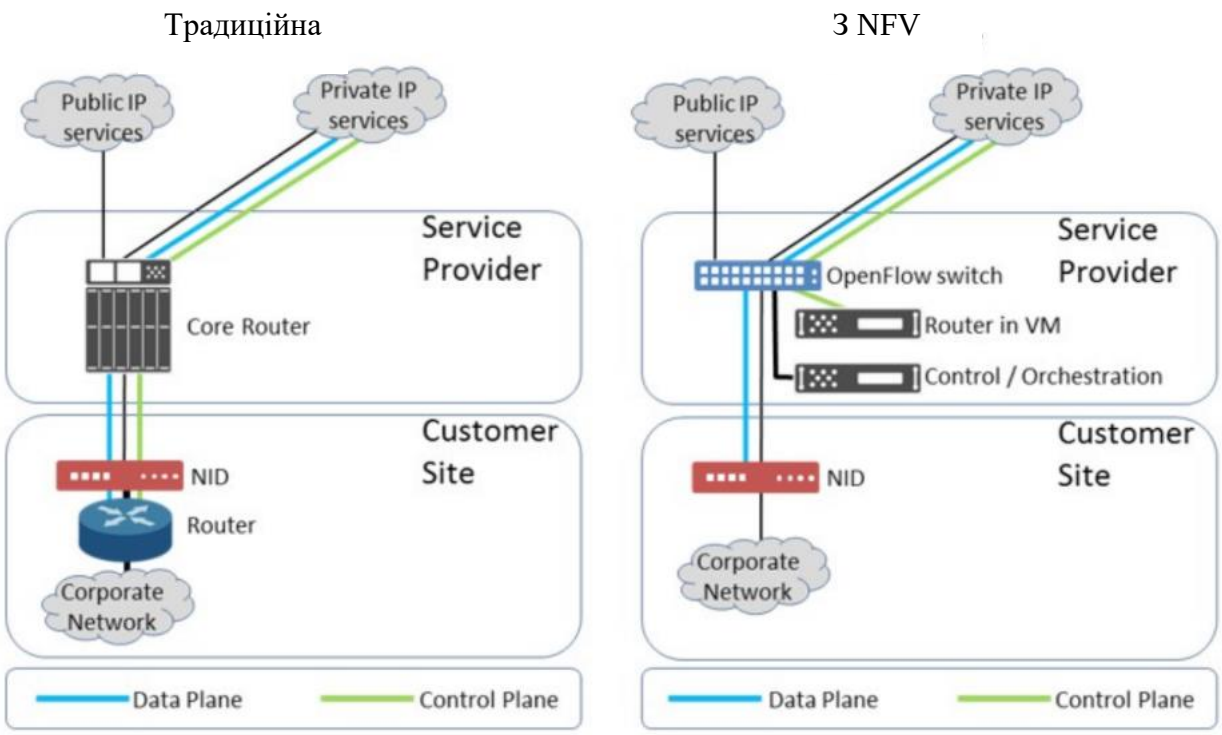

Рисунок 1.2 – Порівняльний аналіз архітектур: традиційної та NFV

Як видно з поданого аналізу впровадження та обслуговування нових сервісів та функцій суттєво спрощується при використанні та впровадженні технології NFV.

1.4 Огляд архітектур мереж, що формують автономні системи

Найкращим прикладом типової мережі є корпоративна мережа. Корпоративна мережа – це складний комплекс взаємозалежних і узгоджено функціонуючих програмних і апаратних компонентів, який забезпечує передачу інформації між різними віддаленими додатками й системами, що використовуються на підприємстві. Таким чином, корпоративна мережа – це мережа, що підтримує роботу підприємства, яке володіє даною мережею, і користувачами такої мережі можуть бути тільки співробітники конкретного підприємства.

Структура корпоративної мережі в цілому відповідає узагальненій структурі телекомунікаційної мережі. Але є й відмінності, наприклад, назви структурних одиниць корпоративної мережі, як правило, відбивають організаційну структуру підприємства. Залежно від масштабів підприємства розрізняють: мережі відділів і робочих груп, мережі будинків і кампусів і мережі масштабу підприємства. Мережа відділу створюється на основі будь-якої стандартної технології локальних мереж і охоплює всі приміщення, що належать відділу. Головне призначення такої мережі – поділ локальних ресурсів. Для такої мережі характерний один або максимум два типи операційних систем. Мережа відділу може входити до складу мережі будинку або мережі кампусу, а може являти собою мережу віддаленого офісу підприємства. У цьому випадку мережа офісу підключається до магістралі корпоративної мережі підприємства за допомогою однієї з технологій глобальних мереж (WAN). Мережа будинку поєднує мережі відділів у межах одного будинку, а мережа кампусу – однієї території. Для побудови таких мереж також використовуються технології локальних мереж. Найчастіше мережа будинку будується як ієрархічна, із власною магістраллю, організованою на основі технології Gigabit Ethernet або вище, до якої

приєднуються мережі відділів, що використовують, наприклад, технологію Fast Ethernet.

Мережі масштабу підприємства відрізняються масштабованістю й високим ступенем неоднорідності (різні типи комп'ютерів, декілька типів операційних систем, безліч різних додатків). І всі ці неоднорідні частини мережі повинні працювати як єдине ціле, надаючи користувачам простий і зручний доступ до всіх різноманітних ресурсів мережі. Корпоративну мережу корисно розглядати як складну ієрархічну систему, що складається з декількох взаємодіючих рівнів. У основі системи, що представляє корпоративну мережу, лежить рівень комп'ютерів – центрів зберігання й обробки інформації, і транспортна підсистема, що забезпечує надійну передачу інформаційних пакетів між комп'ютерами. Над транспортною системою працює рівень мережевих операційних систем, що організує роботу додатків у комп'ютерах і надає через транспортну систему ресурси свого комп'ютера у загальне користування. Над операційною системою працюють різні додатки, але через особливу роль систем керування базами даних, що зберігають в упорядкованому вигляді основну корпоративну інформацію, цей клас системних додатків виділяють в окремий рівень корпоративної мережі. На наступному рівні працюють системні сервіси, які, користуючись СУБД, як інструментом для пошуку потрібної інформації, надають кінцевим користувачам цю інформацію в зручній для ухвалення рішення формі, а також виконують деякі загальні для підприємств всіх типів процедури обробки інформації. До таких сервісів відносяться, наприклад, служба WorldWideWeb, система електронної пошти й багато інших. І, нарешті, верхній рівень корпоративної мережі представляють спеціальні програмні системи, які виконують завдання, специфічні для даного підприємства або підприємств даного типу. Прикладами таких систем можуть служити системи автоматизації банку, організації бухгалтерського

обліку, автоматизованого проектування, керування технологічними процесами й т.п.

Кінцева мета корпоративної мережі втілена саме в прикладних програмах верхнього рівня, але для їхньої успішної роботи абсолютно необхідно, щоб підсистеми інших рівнів чітко виконували свої функції. Транспортна система мережі (кабельна система та активне устаткування) створює основу для взаємозалежної роботи окремих комп'ютерів, тому її часто ототожнюють із самим поняттям "корпоративна мережа", вважаючи всі інші рівні й компоненти мережі просто надбудовою. У свою чергу, транспортна система корпоративної мережі складається з ряду підсистем і елементів. Відповідно до сучасних вимог бізнесу, мережева інфраструктура корпоративної мережі повинна надавати:

– високопродуктивні рішення з забезпечення високої доступності сервісів у межах мережі (HA - High Availability);

– можливість гнучкого нарощування портів із часом, наприклад у міру збільшення абонентів;

– подача живлення по мережевому кабелю (PoE - Power over Ethernet).

Велика й найчастіше зростаюча кількість комутаторів і інших пристроїв мережевого типу (маршрутизатори , міжмережеві екрани й т.п.) вимагає наявності єдиної системи керування й моніторингу всіх пристроїв мережі. Всі перераховані проблеми організації транспортної інфраструктури мережі можуть бути успішно вирішені, якщо керуватися стандартними моделями побудови таких мереж.

На даний час відомі два основних підходи побудови транспортної інфраструктури мережі: дворівнева модель і трирівнева. Історично першою була розроблена трирівнева модель, що передбачає наявність наступних компонентів:

– рівня доступу;

– рівня розподілу (агрегації);
– рівня ядра.

Рівень доступу відповідає за підключення користувальницьких пристроїв до мережі. На цьому рівні формується мережевий трафік, а також здійснюється контроль доступу до мережі. Рівень розподілу вирішує три задачі:

– ізоляція наслідків зміни топології;
– керування розміром таблиці маршрутизації;
– агрегація мережевого трафіка.

Розбиття мережевого дизайну на рівні дає змогу створити модульну структуру, що підвищує масштабування та дає змогу проводити зміни без руйнування початкового дизайну. Розподіл функцій дає змогу проводити вибір обладнання виходячи з потреб на кожному рівні, а також проводити агрегування функцій між рівнями.

Таким чином, на цьому рівні здійснюється маршрутизація між окремими підмережами, застосовуються політики безпеки, передача трафіка здійснюється у відповідності із заданими пріоритетами, працюють протоколи, що забезпечують відмовостійкість мережі. Рівень ядра призначений для високошвидкісної передачі мережевого трафіка й швидкісної комутації пакетів. Тому на мережевих пристроях цього рівня не вводяться додаткові технології, що відповідають за фільтрацію або маршрутизацію пакетів. Існують два типи ядра: вироджений тип ядра і ядро на основі базової мережі. Вироджений тип ядра використовується в невеликих корпоративних мережах і складається з одного маршрутизатора. Ядро на основі базової мережі складається із групи маршрутизаторів, зв’язаних швидкісними каналами зв’язку Загальна структура транспортної системи мережі у відповідності з такою моделлю представлена на рисунку 1.3.

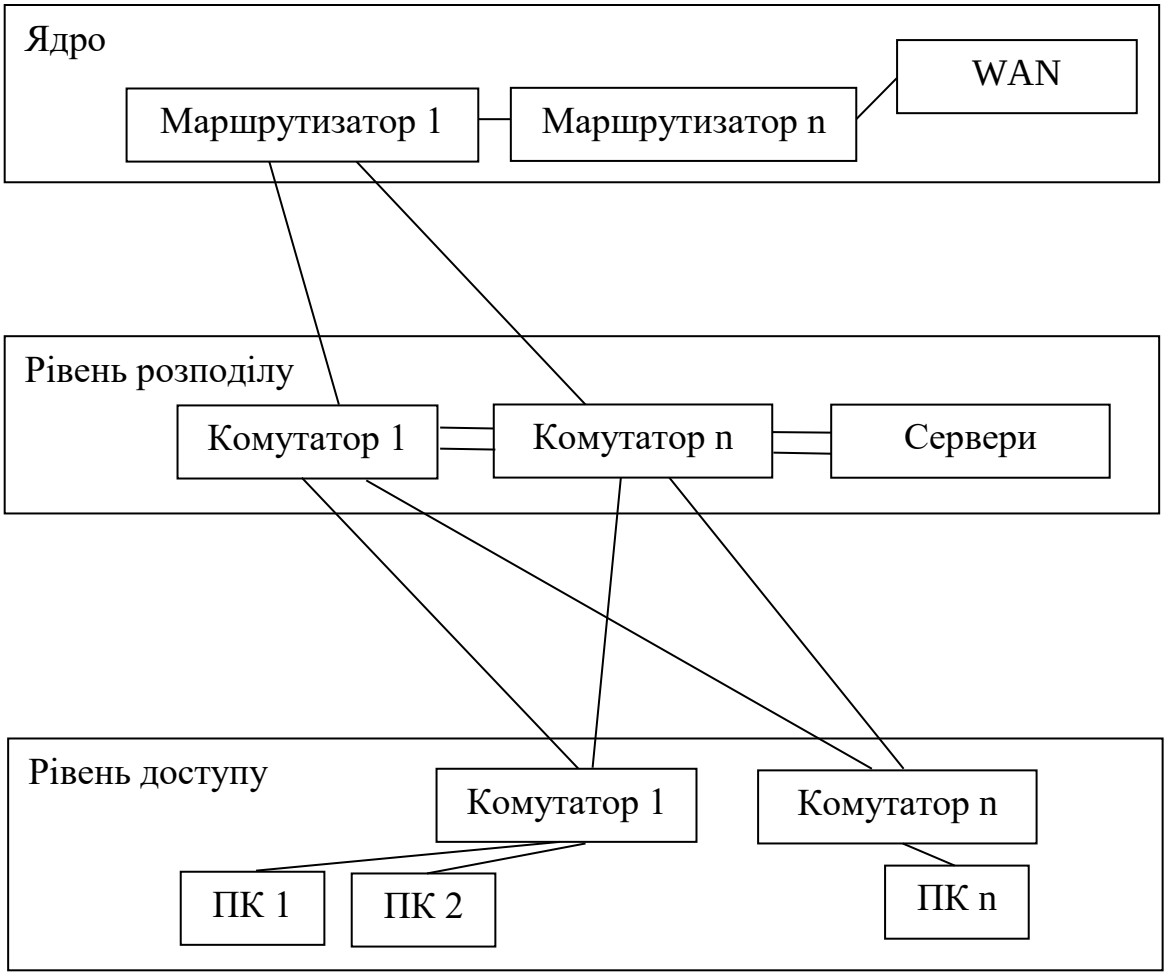

Рисунок 1.3 – Трирівнева модель дизайну мережі

Підвищення надійності дворівневої мережі може бути досягнуте за рахунок забезпечення відмовостійкості роботи ключових мережевих елементів і вузлів. Для цього найбільш відповідальне активне устаткування й канали можуть дублюватися або резервуватися. Крім того, можна перенаправляти трафік по альтернативних шляхах.

Наступним логічним етапом розвитку дизайну мережі стала дворівнева модель, у якій об’єднали рівень агрегації й рівень ядра мережі. Головним достоїнством цієї моделі вважається можливість істотно скоротити витрати на устаткування та обслуговування мережі у порівнянні із трирівневою моделлю (рисунок 1.4).

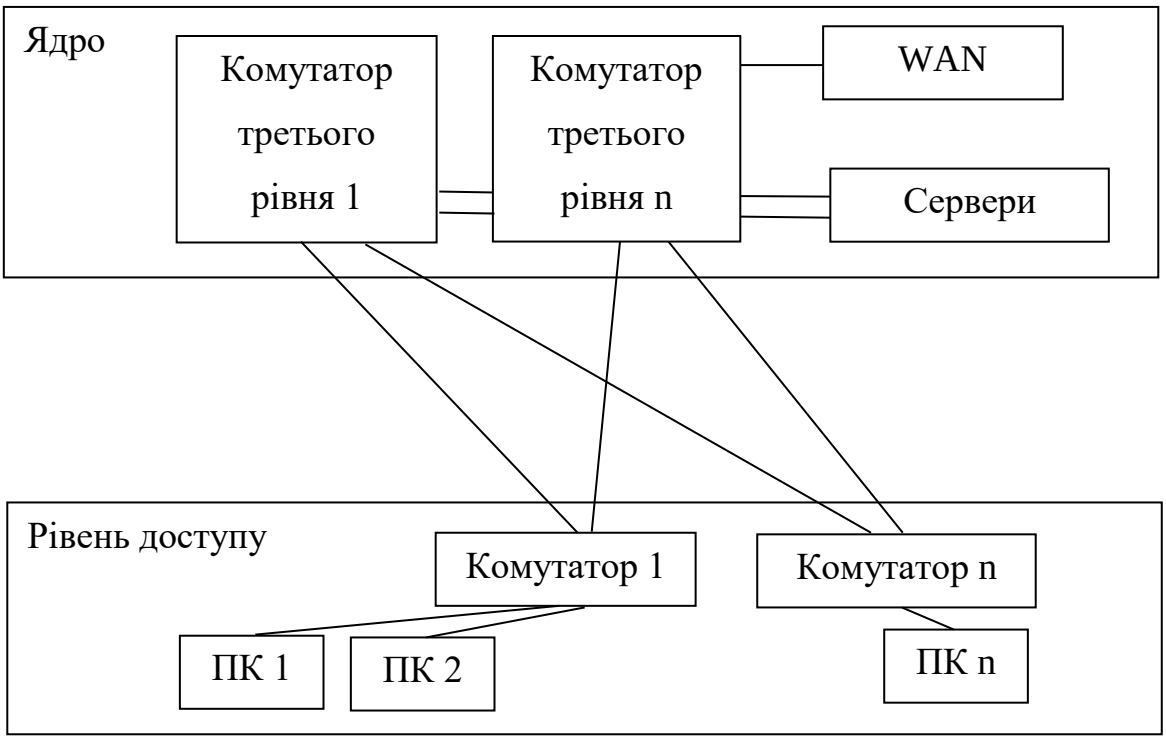

Рисунок 1.4 – Дворівнева модель дизайну мережі

Активне мережеве устаткування – це маршрутизуюче й/або комутуюче устаткування для створення інтелектуального прошарку в рамках всієї мережі. Саме це устаткування забезпечує ключовий параметр – механізм якості обслуговування, що дозволяє в рамках однієї мережі передавати різнорідний трафік. Активне мережеве устаткування необхідно вибирати відповідно до вимог проектованої мережі, з огляду на такі параметри, як величина трафіка, що передається, можливість нарощування мережі, сумісність устаткування. Крім того, необхідно враховувати тип устаткування – маршрутизатор або комутатор, і його характеристики. Пристрій повинен відповідати вимогам по кількості інтерфейсів і їхньому типу, по пропускній здатності, по протоколах, які ним підтримуються. Таким чином, тип пристрою обирається виходячи з його положення в мережі, з необхідними характеристиками, беручи до уваги рекомендації виробника. Основні тенденції розвитку й побудови сучасної інфраструктури корпоративних мереж сьогодні базуються на принципах централізації

сервісів. Такий підхід забезпечує цілий ряд переваг: скорочення витрат у віддалених офісах на обслуговування мережі й утримання персоналу, підвищення швидкості підключення нових офісів, наявність єдиних корпоративних політик. У випадку централізації всі віддалені офіси компанії в рамках великої корпоративної мережі підключаються до центрального офісу, а тому у центральному офісі необхідно забезпечити високу відмовостійкість і необхідну продуктивність.

1.5 Висновки до першого розділу

В даному розділі дипломної роботи розглянуто актуальність питання маршрутизації в автономних системах, віртуалізації мережевих ресурсів та проведено аналіз такої реалізації через використання технології SDN. У результаті такого аналізу виявлено ряд труднощів при вирішенні специфічних задач з використанням цієї технології. Проведено порівняльний аналіз збільшення продуктивності при впровадженні SDN у порівнянні з технологією MPLS, що показало суттєвий приріст у продуктивності. Формування SDN кластерів зрізними вхідними вимогами до маршрутизації та зменшення операційних витрат можливе через застосування технології NFV, що дало змогу визначити шляхи розвитку мережевих архітектур з гнучкими функціональними можливостями. За результатами дослідження визначено використання різних архітекур доступних для організації маршрутизації в автономних системах, що в своїй основі об’єднують традиційну статичну та динамічну маршрутизацію з можливістю впровадження SDN рішень.

2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ПЕРЕДАВАННЯ ДАНИХ В МЕЖАХ АВТОНОМНОЇ СИСТЕМИ

2.1 Обгрунтування областей реалізації маршрутизації в автономній системі

Для успішного функціонування будь-якої мережі маршрутизація є критично важливим елементом, тому її забезпечення можна розділити на три ключові області реалізації:

– надійність фізичних каналів;

– власне організація обміну даними через налаштовані маршрути;

– керування потоками даних з забезпеченням якості послуг.

При побудові мережі якість фізичних каналів опирається на ряд факторів:

– якість та надійність комплектуючих;

– мережевий дизайн з відповідними надлишковими характеристиками;

– швидкість відновлення від помилок та поломок.

Фізичне середовище обміну даними формує шляхи для передачі інформації і тому потребує особливо ретельного підходу до побудови та обслуговування. На основі правильно розробленої та впровадженої інфраструктури можна створювати сучасні логічні надбудови, які дають змогу проводити оновлення без втручання в початковий дизайн. Масштабування при цьому забезпечується методом реплікації модульних елементів, що мають однакову природу.

Поломка або відстуність плану відновлення можуть привести до великих фінансових витрат. При цьому такі витрати діляться на три категорії:

– безпосередні витрати – пов’язані з неможливість виконувати задану діяльність організації. Вони будуть включати вартість виявлення та виправлення інциденту, а також вартість зобов’язань перед партнерською стороною, якщо така існує;

– непрямі витрати – кількість часу, зусилля і інші організаційні витрати, що не входять у першу категорію. Це може бути відновлення втрачених даних, втрата продуктивності мережі для користувачів та ін.;

– вартість репутації – пов’язана з неможливістю клієнтами отримати доступ до ресурсів організації, несправністю використання IP телефонії та ін.

Для забезпечення фізичної надійності використовують обладнання та архітектури з надлишкою надійністю. При цьому вибираючи необхідні компоненти враховують вартість кінцевого проекту в порівнянні з цілями та можливостями організації. Обладнання повинне містити резервуючі елементи такі як блоки живлення, вентилятори охолодження, можливість гарячої заміни основних компонентів без зупинки роботи пристрою. Шляхи повинні дублюватись для організації альтернативних маршрутів.

З точки зору архітектури мереж, доцільно використати трирівневу модель мережевого дизайну. Рівень доступу у ній буде акумулювати обладнання для забезпечення портів під’єднання кінцевих користувачів та їх пристроїв, а на рівні розподілу та кореневому будуть зосереджені агрегуючі та маршрутизуючі пристрої. При такому підході реалізуться максимальна масштабованість та керованість.

2.2 Використання статичної маршрутизації

Забезпечення передавання даних в межах автономної системи потребує ретельного вибору методу маршрутизації “IP” пакетів даних між вузлами мережі. В залежності від складності та розмірів мережі доцільність

використання статичної маршрутизації може бути зменшена операційною вартістю. Налаштування великої кількості статичних маршрутів займає багато часу та загромаджує таблиці маршрутизації. Це в свою чергу збільшує час пошуку найкращого маршруту. Зміни в таких великих масивах записів можуть приводити до помилок, що важко знайти та виправити. Це збільшує час простою мережі та зменшує швидкість відновлення.

Проте, з точки зору надійності прийняття рішення та навантаження на мережеві ресурси такий підхід має ряд плюсів. Достеменно знаючи фізичну інфраструктуру своєї мережі адміністратор може направляти трафік за керунком, що є менш грошово вартісним чи забезпечувати доступ до мереж з єдиним виходом. Таким чином оптимізується використання мережевого обладнання не приводячи до зростання навантаження на інженерів.

До переваг статичної маршрутизації в автономних системах можна віднести можливість організації запасних маршрутів у комбінації з динамічною маршрутизацією. При цьому використовується параметр адміністративної віддалі, що в поєднанні з відповідним значенням протоколу динамічної маршрутизації створює запасний маршрут.

Для зменшення об’єму таблиць маршрутизації використовуються сумарні або супернет маршрути. Об’єднання декількох логічних мережевих адрес з спільною мережевою частиною та вихідним інтерфейсом дає змогу представляти одним мережевим числом набір мереж. Таке властиве для автономних систем, оскільки вони є у власності певної організації. Також, такий підхід збільшує захищеність мереж всередині автономної системи, оскільки вони представлені у вигляді комбінованого мережевого числа та спільної мережевої маски. Ззовні не є видимою внутрішня структура організації логічної адресації.

У випадку єдиного виходу з мережі можна використовувати маршрут за замовчуванням. Його конфігурують на граничному маршрутизаторі.

2.3 Методи маршрутизації пакетів з застосуванням протоколів динамічної маршрутизації

До протоколів, які мають можливість динамічно вивчати маршрутизацію, що працюють в автономних системах належать “RIP”, “RIPv2”, “OSPF”, “EIGRP”. Кожен з них має ряд переваг та недоліків, що потрібно проаналізувати для вибору правильного протоколу розгортання в автономній системі.

Протокол “RIP” незважаючи на свою давність залишається таким, що підтримується. Відносячись до відкритого стандарту він імплементований у багато операційних систем різних виробників мережевого устаткування, що дає змогу розгортати маршрутизацію в багатовендорному середовищі. Цей динамічний протокол використовує кількість вузлів у якості метрики для шляху. Його адміністративна віддаль рівна 120 і його програмний порт 520. Ця інформація потрібна маршрутизатору для визначення рівня довіри до маршруту у випадку використання декількох динамічних протоколів, а також мережевому адміністратору для контролю портів на активність.

Маршрутизація з “RIP” можлива у мережах де кількість вузлів не перевищує 15, оскільки єдиним методом боротьби з петлями є встановлення граничної віддалі рівної 16. Періодичний обмін таблицями маршрутизації займає користувацький трафік та ресурси пристрою, а відсилання методом широкомовної передачі впливає на інші отримувачі, які не призначені для таких даних. Повні таблиці маршрутів відсилаються і кожен надіється на інформацію отриману від сусіда.

Основним недоліком використання “RIP” в сучасних мережах є те, що він не підтримує безкласову маршрутизацію. Тобто маска під мережі не відсилається в оновленнях і тому не може бути коректно застосована до інформації про маршрут.

Використання часових таймерів також є ненадійним методом боротьби з помилками маршрутизації. Час оновлення інформації про зміни 30 секунд. Періодичність обміну таблиць створює додаткове навантаження на мережу. Час встановлення маршруту неправильним становить 180 секунд. Час затримки маршруту 180 секунд використовується для уникнення прийняття неправдивої інформації від іншого сусіда, а через 240 секунд маршрут видаляється з таблиці.

Протокол “RIPv2” є новішою версією, яка частково має покращені характеристики. Параметри метрики залишились незмінними, що створює ті самі проблеми та незручності як і при використанні свого попередника. Основною перевагою новішого зразка є відсилання оновлень методом групової передачі замість широкомовної. Це частково зменшує навантаження на пристрої, що обробляють дану інформацію.

Для розгортання маршрутизації з використанням обладнання виробника “Cisco” можна використовувати протокол “EIGRP”. Він є покращеною версією старішого “IGRP” і основна його превага – це безкласовість. Таким чином можна використовувати маски зімнної довжини та інші сучасні застосунки в мережах гетерогенної структури.

Важливою особливістю даного протоколу є швидка конвергенція – “EIGRP”в своїй основі має алгоритм “DUAL” для її підтримки. Якщо маршрут до мережі стає недоступний, тоді може бути використаний інший маршрут (можливий наступник), що зберігається в таблиці топології. Якщо маршруту до цієї мережі немає в таблиці топології, тоді повідомлення запиту відсилається широкомовним способом, щоб дізнатися альтернативний шлях до цієї мережі.

В порівнянні з іншими протоколами зменшене використання пропускної здатності – “EIGRP” не надсилає періодичні оновлення, як це робить інший протокол “RIP”. Будучи дистанційно-векторним протоколом “RIP”, надсилає повну таблицю маршрутизації протягом певного періоду

часу, тому споживає необхідну пропускну здатність без потреби, а “EIGRP” використовує часткові оновлення, якщо відбуваються якісь зміни в топології, тобто оновлення спрацьовує лише в тому випадку, якщо відбувається будь-яка подія. Також оновлення “EIGRP” передаються лише маршрутизаторам які цього вимагають.

Підтримка всіх протоколів і технологій зв’язку каналів передачі даних “LAN” та “WAN” – “EIGRP” підтримує мережі спільного доступу, наприклад “FDDI”, “Tocken Ring” тощо та всі топології WAN, такі як виділена лінія, з’єднання “точка-точка”. “EIGRP” не потребує додаткової конфігурації в протоколах 2-го рівня.

Підтримується автоматичний підсумок – у “EIGRP” автоматичне підбиття підсумків маршрутів увімкнено за замовчуванням. Автоматичне підсумовування – це функція, яка дозволяє протоколам маршрутизації автоматично підсумовувати свої маршрути до своїх класних мереж, тобто маршрутизатори отримуватимуть зведені маршрути автоматично.

Підтримується нерівномірне балансування витрат навантаження – в “EIGRP” можливе нерівномірне балансування витрат навантаження, змінивши значення дисперсії. За замовчуванням дисперсія становить 1, тому підтримує рівновагу балансування витрат навантаження, але якщо ми хочемо використовувати нерівномірне балансування витрат навантаження між нерівноцінними маршрутами, то ми можемо змінити значення дисперсії відповідно до кількості трафіку, який ми хочемо розділити на різні шляхи. Найкраща відстань множиться таким чином, що вона стає більшою, ніж величина можливої відстані наступника.

Комунікація через надійний протокол передачі “RTP” – “EIGRP” опирається на власний протокол “RTP” для управління зв’язком між маршрутизаторами, які обмінюються “EIGRP”. “EIGRP” використовує 224.0.0.10 як групову адресу. Для кожної багатоадресної групової передачі маршрутизатор готує та веде список маршрутизаторів (що мають спільний

“EIGRP”). Якщо не отримано підтвердження багатоадресної передачі, то ті самі дані передаються через 16 одноадресних повідомлень. Якщо підтвердження не отримано навіть після 16 одноразових спроб, таке повідомлення оголошується недіючим. Цей процес відомий як надійний багатоадресний пакет.

Найкращий вибір шляху за допомогою “DUAL” – “EIGRP” використовує алгоритм розширення оновлення “DUAL”, щоб знайти найкращий шлях, доступний для мережі. Маршрутизатори, що мають спільний “EIGRP” підтримують таблицю топології, в якій підтримуються всі маршрути до мережі. Якщо найкращий шлях (наступник) стає недоступним, то другий найкращий шлях (можливий наступник) використовується з таблиці топології. Якщо в таблиці топології немає шляху, він надсилає повідомлення запиту для отримання оновленої інформації.

Робота “EIGRP” базується на обслуговуванні 3 різних таблиць.

Таблиця сусідів: вона містить в собі інформацію про маршрутизатори, з якими було сформовано сусідство. Вона також містить значення кількості черги для привітальних повідомлень і які не розпізнаються. На основі привітальних повідомлень “EIGRP” відслідковує наявність каналу між ним і сусідом, що в свою чергу дає змогу підтримувати всі маршрути асоційовані з цим сусідом.

Топологічна таблиця: Вона містить усі маршрути до доступних мереж (наступників та можливих наступників). Такий підхід допомагає уникнути небажаних перезапускань алгоритму “DUAL”, що займає ресурси обладнання. Провівши розрахунки можливих шляхів, маршрутизатор зберігає їх в таблиці топології і використовує заміни при необхідності без перерахунку.

Таблиця маршрутизації: Вона містить усі маршрути, які використовуються для прийняття поточних рішень про маршрутизацію. Маршрути в цій таблиці розглядаються як наступний (найкращий) шлях.

При розрахунку метрики маршруту “EIGRP” може використовувати до 5 змінних, але за замовчуванням використовуються лише 2 (K1 і K3). Коефіцієнтами розрахунку метрики є: K1 (пропускна здатність); K2 (навантаження); K3 (затримка); K4 (надійність); K5 (максимальний розмір одиниці передавання “MTU”)

У формулі розрахунку метрики використовується найменша пропускна здатність, навантаження, затримка, надійність, “MTU” на шляху між джерелом і пунктом призначення.

Зазвичай для обчислення метрики за допомогою EIGRP використовуються лише значення k1 і k3. Значення для k1=1, k2=0, k3=1, k4=0, k5=0 відповідно.

Для формування “EIGRP”-сусідства повинні бути виконані такі критерії: k значення повинні відповідати між двома сусідами; номер автономної системи повинен відповідати; аутентифікація повинна відповідати (якщо застосовується); “EIGRP” підтримує лише автентифікацію MD5; маска підмережі повинна бути однаковою.

Таймери, що використовуються в “EIGRP” теж відіграють важливу роль: привітальний таймер – інтервал, протягом якого “EIGRP” надсилає привітальне повідомлення на інтерфейс. За замовчуванням це 5 секунд; Мертвий таймер – інтервал, протягом якого сусід буде оголошений мертвим, якщо він не в змозі надіслати привітальний пакет. За замовчуванням це 15 секунд.

Протокол відкриття мершого найкоротшого (“OSPF”) – це протокол маршрутизації стану каналу, який використовується для пошуку найкращого шляху між джерелом та маршрутизатором призначення, використовуючи свій власний алгоритм першого найкоротшого шляху (“SPF”). Протокол маршрутизації стану каналу використовує концепцію миттєвих оновлень, тобто, якщо в створеній таблиці маршрутизації спостерігаються зміни, то

оновлення спрацьовують лише для тих маршрутизаторів, що його потребують.

Спочатку процедура відкриття найкоротшого шляху (“OSPF”) розроблялась Інженерною робочою групою (“IETF”) як один із протоколів внутрішнього шлюзу (“IGP”), тобто протокол, який спрямований на переміщення пакету у великій автономній системі або домені маршрутизації. Це протокол мережевого рівня, який працює на порті номер 89 і використовує значення для адміністративної системи 110. “OSPF” використовує багатоадресову групову адресу 224.0.0.5 для звичайного зв’язку та 224.0.0.6 для оновлення призначеного маршрутизатора (“DR”) / резервного призначеного маршрутизатора (“BDR”).

Для формування сусідства в “OSPF” є критерії для обох маршрутизаторів: вони мають бути в одній області; ідентифікатор маршрутизатора повинен бути унікальним; підмережева маска – однаковою; значення таймерів – однаковим; аутинтифікація повинна співпадати, якщо застосовується.

“OSPF” та “EIGRP” є найбільш перспективними динамічними протоколами для розгортання в межах автономної системи, оскільки мають набори переваг, що роблять їх швидкими та надійними з точки вибору найкращого маршруту. Основним недоліком “EIGRP” буде його залежність від виробника, оскільки він є приватним протоколом виробника “Cisco” і тому у багатовендорному середовищі будуть складнощі з його використанням. Напротивагу цьому “OSPF” є відкритим стандартом може бути розгорнутий в таких умовах. Ще однією особливістю застосування цих протоколів є їх ресурсні вимоги до обладнання. Оскільки обидва обслуговують декілька таблиць та мають алгоритми розрахунку найкращих шляхів, то як наслідок, використовують достатньо багато оперативної пам’яті та процесора. На малопотужному обладнанні це приведе до суттєвих затримок і спровокує неналежну роботу мережі. Основним завданням будь

якої маршрутизації є передавання користувацьких даних. І коли протоколи будуть займати значну частину ресурсів на свою роботу, то наслідком можу бути унеможливлення їх використання.

2.4 Аналіз роботи таблиці маршрутизації в межах автономної системи

Таблиця маршрутизації – це набір правил, які часто переглядаються у форматі таблиці, що використовуються для визначення, куди будуть спрямовані пакети даних.

Таблиця маршрутизації містить інформацію, необхідну для пересилання пакету по найкращому шляху до місця призначення. Кожен пакет містить інформацію про його походження та призначення. Коли пакет приймається, мережевий пристрій вивчає пакет і шукає співпадання з ним у таблиці таблиці маршрутизації, забезпечуючи найкращу відповідність його призначенню. Потім у таблиці задано вказівки пристрою щодо відправлення пакета до наступного вузла на його маршруті по всій мережі.

Основна інформація в таблиці маршрутизації включає:

– місце призначення: “IP”-адреса кінцевого пункту призначення пакету;

– наступний вузол на шляху: IP-адреса, на яку пересилається пакет;

– інтерфейс – вихідний мережевий інтерфейс, який пристрій повинен використовувати під час пересилання пакету на наступний вузол або кінцевий пункт призначення

– метрика – призначає вартість кожному доступному маршруту, щоб можна було вибрати найбільш рентабельний шлях

– маршрути – включає прямі підключені підмережі, непрямі підмережі, які не прикріплені до пристрою, але до них можна отримати доступ через один або декілька вузлів, а також маршрути за замовчуванням,

які використовуватимуться для певного типу трафіку або коли бракує інформації.

В незалежності від способу отримання інформації для заповнення таблиць маршрутизації потрібно розуміти роботу самого маршрутизатора з ними. Існує два підходи до читання маршрутів. Якщо використовується класовий підхід, тоді кожен пристрій вважає, що в нього є повна інформація про мережі і при знаходження батьківської мережі він починає пошук конкретнішого маршруту в дочірніх. При відсутності співпадання в цьому каскаді вважається, що шляху до отримувача неіснує і пакет знищується. Це може не відопвідати дійсності, оскільки існують маршрути за замовчуванням, сумарні маршрути та супернети.

Безкласова маршрутизація передбачає читання повної інформації. Якщо у випадку співпадання з батьківською мережею у дочірніх співпадання не буде, то пошук продовжується на знаходження додаткової інформації. У випадку закінчення пошуку і незнаходження відповідника для отримувача – пакет буде знищено. В іншому випадку відбудеться розв’язування маршруту за адресою отримувача і передача пакету до відповідника.

2.5 Висновки до другого розділу

В другому розділі дипломної роботи описано вимоги до розроблюваної маршрутизації, що повинна функціонувати в межах автономної системи, а також проаналізовано ризики пов’язані з її порушенням. Здійснено аналіз можливостей застосування статичної маршрутизації для організації обміну даними. Детально визначено ситуації при яких відповідні протоколи, які динамічно визначають маршрути повинні бути застосовані.

3 МЕТОДИ ВДОСКОНАЛЕННЯ МАРШРУТИЗАЦІЇ В АВТОНОМНІЙ СИСТЕМІ

3.1 Віртуалізація шлюзів як метод підвищення надійності маршрутизації

Важливими компонентами, що потребують резервування у більшості локальних мереж, є шлюзи. Функції шлюзу можуть виконувати як прикордонні маршрутизатори, так і міжмережеві брандмауери екрани. З точки зору кінцевих користувачів потрібно, щоб методи та алгоритми резервування вищезгаданих пристроїв були максимально прозорими, тобто їх робота не вимагала додаткового програмного забезпечення та додаткових дій.

Необхідність віртуалізації критичних компонентів локальних мереж пов’язана з використанням цими елементами статичних фізичних і логічних адрес та підтримкою одночасного інформаційного обміну з багатьма вузлами мережі. З цього випливає, щоб резервний компонент міг виконувати функції основного, необхідно зробити таким чином, що його канальні та мережні адреси збігалися з адресами основного компонента, а це суперечить базовим принципам організації обміну інформації на канальному та мережному рівнях моделі “OSI”. Одним з методів розв’язання зазначеної суперечності є застосування спеціальних підходів, які повинні забезпечувати:

– можливість формування групи резервування пристроїв, яка складається з основного і резервного (резервних) одиниць обладнання;

– забезпечення колективного використання адрес членами групи резервування;

– організація створення та налагодження віртуального пристрою для забезпечення обміну потоками інформації з кінцевими абонентами різних мереж (виконання функцій шлюзу за замовчуванням);

– забезпечення постійного моніторингу стану основного пристрою в межах групи резервування.

Для реалізації вищеперерахованих функцій використовують додатки у вигляді програмних модулів, що підтримують роботу протоколів динамічного резервування на основному та резервному пристроях мережі.

Одними з найбільш поширених протоколів динамічного резервування елементів мереж в автономних системах (відомих як “FHRP, First Hop Redundancy Protocols”), що розгортаються в сучасних мережах є такі:

– “HSRP, Hot Standby Router Protocol (Cisco Systems Inc.)”;

– “VRRP, Virtual Router Redundancy Protocol”;

– “CARP, Common Address Redundancy Protocol”;

– “GLBP, Gateway Load Balancing Protocol (Cisco Systems Inc.)”;

– “IPSTB, IP Standby Protocol (DEC, Digital Equipment Corporation)”;

– “ESRP, Extreme Standby Router Protocol (Extreme Networks)”;

– “R-SMLT, Routed Split Multi-Link Trunking (Avaya)”;

– “NSRP, NetScreen Redundancy Protocol (Juniper Networks)”;

– “XRRP, XL Router Redundancy Protocol (Hewlett Packard)”.

Протокол “HSRP” є першим протоколом виробника мережевого обладнання, який був розроблений для динамічного резервування шлюзу у мережах, що побудовані на основі маршрутизаторів і багаторівневих комутаторів “Cisco”. Одним з подібних за функціями є відкритий протокол “VRRP”, який був розроблений “IETF” як альтернатива протоколу “HSRP”. Протокол “CARP” також розроблявся як відкритий протокол, але з обмеженим застосуванням, оскільки він був призначений лише для резервування серверів для “BSDподібних ОС”. Решта протоколів – це фірмові розробки відповідних виробників мережевого обладнання та програмного забезпечення. Одією з можливостей, окрім резервування, є

забезпечення балансування (розподілу) навантаження при передаванні трафіку та захист на канальному рівні.

Протокол “HSRP (Hot Standby Router Protocol)” є одним із перших протоколів динамічного резервування шлюзу. Цей протокол описаний у стандарті RFC-2281 „Cisco Hot Standby Router Protocol (HSRP)”, який опублікований IETF у березні 1998 року в категорії інформаційних стандартів. У розробці даного стандарту окрім представників фірми “Cisco” брали участь представники фірми “Juniper Networks”. Патент на протокол “HSRP” належить розробнику протоколу – організації “Cisco”. На даний момент існують дві версії протоколу “HSRP”: “HSRP Version 1” та “HSRP Version 2”, які мають певні внутрішні технічні відмітності реалізації. “” орієнтована на функціонування в “IP-мережах” версії 4, а “HSRP Version 2” орієнтована на функціонування в “IP-мережах” версій 4 та 6. У практиці побудови мереж широко використовується модифікація протоколу “HSRP”, відома як “MHSRP (Multiple HSRP)”, у якій наявна можливість реалізації статичного балансування навантаження. Стосовно моделі “OSI” протокол “” є протоколом мережевого рівня. Відповідно, стосовно стеку “TCP/IP” даний протокол є протоколом рівня міжмережевої взаємодії. Для передачі своїх повідомлень протокол “HSRP” використовує можливості протоколу “UDP” для забезпечення групової розсилки.

Робота протоколу “HSRP” пов’язана з використанням поняття маршрутизатор “HSRP (HSRP Router)” та група резервування “HSRP (HSRP Standby Group)”. Маршрутизатором “HSRP” є будь-який пристрій маршрутизатор (або багаторівневий комутатор), на одному з інтерфейсів якого активовано використання протоколу “HSRP”. До групи резервування “HSRP” входять активний маршрутизатор “HSRP (HSRP Active Router)” та резервний маршрутизатор “HSRP (HSRP Standby Router, HSRP Primary Backup Router)”. Резервних маршрутизаторів у одній групі може бути декілька. В такій ситуації обирається один резервний маршрутизатор, решта

маршрутизаторів залишаються запасними маршрутизаторами “HSRP (HSRP Backup Routers)”. Для решти вузлів мережі група резервування “HSRP” подається як один віртуальний маршрутизатор “HSRP (HSRP Virtual Router)”, якому відповідає одна віртуальна адреса мережевого рівня (“HSRP Virtual IPAddress”) та одна віртуальна адреса канального рівня (“HSRP Virtual MAC Address”). Таким чином віртуальний маршрутизатор “HSRP” є шлюзом за замовчуванням для всіх вузлів автономної системи. В реальній мережі функції віртуального маршрутизатора “HSRP” фактично виконує один пристрій, то фізична пересилка IP-пакетів до інших мереж здійснюється через активний маршрутизатор “HSRP”. Один реальний маршрутизатор може бути членом кількох груп резервування “HSRP”, де в одних групах він може бути активним, а в інших виконувати роль резервного. Така можливість використовується для реалізації схеми підключення локальних мереж, у яких необхідне статичне балансування навантаження.

Процес вибору активного та резервного маршрутизаторів “HSRP” відбувається на основі механізму пріоритетів (“Priority”). Пріоритет маршрутизатора “HSRP” може набувати значень у діапазоні від 0 до 255. Маршрутизатор із найбільшим пріоритетом вибирається як активний маршрутизатор “HSRP”, йому призначаються віртуальна “IPадреса” та віртуальна “MAC-адреса”, і на нього покладаються функції маршрутизації. Маршрутизатор із наступним пріоритетом в процесі виборів стає резервним маршрутизатором “HSRP”. Решта маршрутизаторів приймають роль запасних. Якщо пріоритети маршрутизаторів, які претендують на роль активного, однакові, то наступним критерієм порівняння є їх IP-адрес і маршрутизатор із найбільшою адресою стає активним маршрутизатором “HSRP”.

Для підтвердження свого статусу активний маршрутизатор групи резервування “HSRP” періодично (через інтервал “Hello Time”) розсилає решті маршрутизаторів повідомлення свого існування “HSRP Hello”. Якщо

резервний і запасні маршрутизатори не отримують повідомлення “HSRP Hello” через певний проміжок часу (проміжок часу “Hold Time”), то вони констатують, що активний маршрутизатор вийшов із ладу (або вимкнений адміністратором), відповідно резервний маршрутизатор стає активним і серед запасних маршрутизаторів обирається новий резервний. Маршрутизатор, який має намір стати активним, для інформування решти членів групи резервування “HSRP” розсилає повідомлення показуючи намір проведення перевиборів – повідомлення “HSRP Coup”. Якщо ж маршрутизатор не має наміру більше бути активним, він повинен розіслати повідомлення відмови від статусу активного маршрутизатора – повідомлення “HSRP Resign”.

У роботі протоколу “HSRP” використовуються три службові таймери: “Hello Timer”, “Active Timer”, “Standby Timer”. Таймер “Hello Timer” – це таймер, який застосовується для формування і розсилки повідомлень “HSRP Hello” активним та резервним маршрутизаторами “HSRP”. Цей таймер формується за допомогою значення інтервалу “Hello Time”. Таймер “Active Timer” – це таймер, який застосовується для контролю стану активного маршрутизатора “HSRP”. Цей таймер формується за допомогою значення інтервалу “Hold Time” для активного маршрутизатора “HSRP”. Таймер “Standby Timer” – це таймер, який застосовується для контролю стану резервного маршрутизатора “HSRP”. Цей таймер формується за допомогою значення інтервалу “Hold Time” для резервного маршрутизатора “HSRP”.

При виконанні операцій протоколу “HSRP” маршрутизатор групи резервування “HSRP” може знаходитися в одному з таких станів:

- стан ініціалізації (“Initial State”);
- стан навчання (“Learn State”);
- стан прослуховування мережі (“Listen State”);
- стан передавання повідомлень (“Speak State”);
- стан резервного маршрутизатора (“Standby State/Standby Router”);
- стан активного маршрутизатора (“Active State/Active Router”).

Після активації інтерфейсу (або зміни його параметрів) маршрутизатор перебуває у стані “Initial”. У цьому стані інтерфейс не бере участі в операціях протоколу “HSRP”. Якщо ж на інтерфейсі протокол “HSRP” налагоджено, то інтерфейс переходить у наступний стан навчання – “Learn State”. У стані навчання маршрутизатор “HSRP” знаходиться до отримання першого повідомлення “HSRP Hello” від активного маршрутизатора. З цього повідомлення він отримує віртуальну “IP-адресу” групи та значення таймерів.

Після отримання повідомлення “HSRP Hello” маршрутизатор “HSRP” переходить до стану прослуховування мережі – “Listen State”. У цьому стані маршрутизатор не є ні активним, ні резервним маршрутизатором. У стані “Listen State” маршрутизатор прослуховує повідомлення активного і резервного маршрутизаторів і може перейти до наступного стану передачі повідомлень – “Speak State” у тому разі, якщо має достатній пріоритет. Маршрутизатор “HSRP”, що знаходиться у стані передачі повідомлень, пересилає повідомлення “HSRP Hello” для участі у виборах, у результаті яких він стає активним або резервним маршрутизатором.

Надалі маршрутизатор “HSRP”, який став резервним, контролює стан активного маршрутизатора шляхом аналізу повідомлень “HSRP Hello”, які сформовані і розіслані активним маршрутизатором. Резервний маршрутизатор також формує власні повідомлення “HSRP Hello” для підтвердження свого стану решті маршрутизаторів групи резервування “HSRP”.

Особливістю протоколу “HSRP” є те, що в разі його застосування лише один із маршрутизаторів групи резервування “HSRP” – резервний маршрутизатор, – контролює стан активного маршрутизатора, а, отже, може його замінити при виході з ладу. Решта маршрутизаторів групи – запасні маршрутизатори, контролюють стан резервного маршрутизатора. При виході

з ладу резервного маршрутизатора його функції починає виконувати той запасний маршрутизатор, пріоритет якого є найбільшим.

Контроль працездатності активного маршрутизатора “HSRP” із використанням механізму розсилки повідомлень “HSRP Hello” не завжди є ефективним. Часто виникає ситуація, коли інтерфейс маршрутизатора, що бере участь у роботі протоколу “HSRP”, функціонує нормально, а зовнішній інтерфейс або канал зв’язку до сусіднього комунікаційного пристрою вийшов із ладу. У такому разі для вузлів локальної мережі стосовно доступності шлюзу за замовчуванням проблеми немає, а стосовно забезпечення пересилки “IP-пакетів” до зовнішніх мереж проблема існує.

Тому з метою підвищення надійності роботи у протоколі “HSRP” введені дві взаємозалежні та взаємопов’язані функції: “Interface Tracking” та “Preempt”. Функція “Interface Tracking” забезпечує контроль стану зовнішніх (щодо “HSRP”-інтерфейсу) інтерфейсів маршрутизатора та динамічну зміну пріоритету маршрутизатора. У разі виходу з ладу зовнішнього інтерфейсу (або виникнення проблем у каналі зв’язку) дана функція зменшує значення пріоритету “HSRP” маршрутизатора, а при відновленні роботи – збільшує. Функція “Preempt” забезпечує швидкі перевибори нових активного та резервного маршрутизаторів після змін пріоритетів пристроїв. Слід зазначити, що згадані функції використовуються одночасно.

Отже, створення групи маршрутизаторів, що будуть виконувати роль віртуального пристрою і прозоро працювати як шлюз мережі дасть змогу підвищити надійність та продуктивність. У випадку фізичного виходу з ладу одного пристрою інший прийме роль активного маршрутизатора в автоматичному режимі і процес передавачі даних буде відбуватись без збоїв.

На основі проведених досліджень можна провести класифікацію вимог до мережевих дизайнів з забезпеченням віртуалізації:

– віртуалізація окремих вузлів мережі;
– повна віртуалізація мережі автономної системи;

Модель віртуалізації мережі на основі аналізатора вимог та потоків показано на рисунку 3.1.

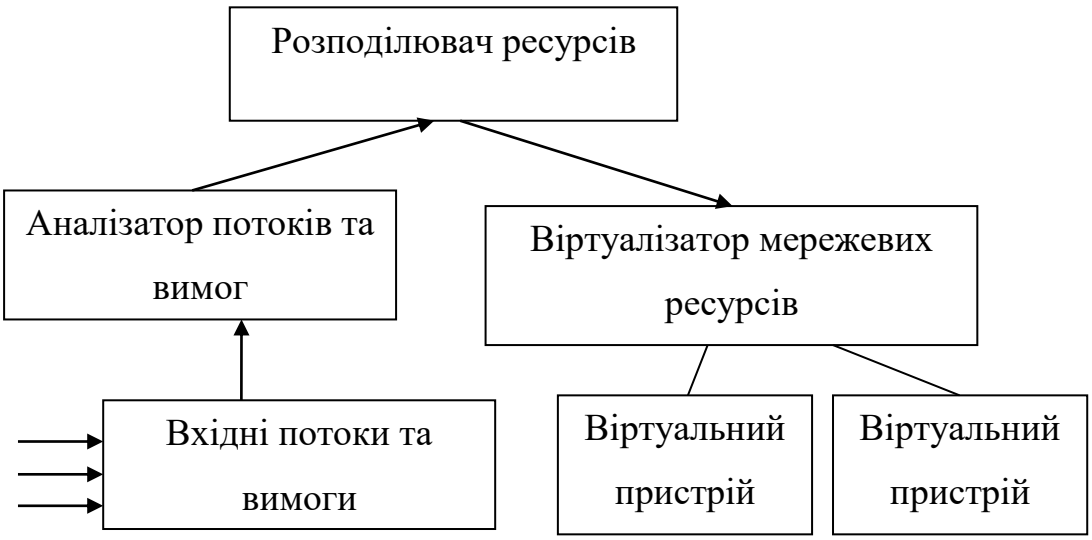

Рисунок 3.1 – Модель віртуалізації автономної системи

В залежності від задач які повинна вирішувати віртуалізація розроблена модель дає можливість вибирати один з попередніх варіантів дизайну. Якщо мережа з доволі статичними вимогами до мережевих ресурсів проте з підвищеними вимогами до надійності роботи, можна використати віртуалізацію окремих мережевих вузлів, при цьому впровадження більш про двинутих рішень буде дороговартісним та технічно складним для впровадження. Окремий віртуальний маршрутизатор чи набір таких буде більш раціональним вибором.

У випадку, коли мережа окремої організації потребує гнучкої реалізації вирішення поставлених завдань потрібно впроваджувати технологію тотальної віртуалізації. Такий підхід у віртуалізації дасть змогу на основі програмних додатків вирішувати завдання, при цьому набір сталих вимог в межах бізнес процесів одного суб’єкта господарювання забезпечить нормальну операційну діяльність.

3.2 Забезпечення маршрутизації в автономній системі засобами технології SDN

Сучасні мережеві архітектури на основі програмно конфігурованих мереж надають гнучкість управління специфічними задачами з передавання даних, що в свою чергу підвищує надійність послуг. Наприклад, в мережах “Розумного міста” часто виникає потреба налаштувати певні види сервісів і при цьому операційної системи обладнання не є достатньо для виконання таких завдань. Вирішення такого роду проблем можливе через використання програмованих додатків, що можуть впроваджуватись в мережі “SDN”.

Для забезпечення функції централізації управління використовується “SDN”-контролер. На ньому запускаються відповідні мережеві додатки, які виконують функції управління мережею. Поведінка мережі може бути змінена в режимі реального часу, що дає можливість розгортати нові додатки розроблені виробником або написані самостійно під конкретні завдання.

Функція управління виділяються в окремий рівень та передаються окремому компоненту, що зосереджене на оптимізацію мережевих налаштувань та вирішення специфічних завдань, що важко виконати традиційними методами і, зокрема, дають змогу отримати наступні переваги: форматування даних, правила оброблення та технології передачі в маршрутизаторі не обмежені певним типом устаткування, рівнем взаємодії або виробником; як одиницю передачі можна використати багатовимірний вектор, що включає поля з різних рівнів моделі “OSI”; методи автоматизованого виправлення потоків застосовуються при розробці правил пересилання даних та можуть застосовуватися в залежності від нагрузки компонентів; об’єднання контролерів в мережеві домени дає змогу резервувати та оптимізувати канали передачі.

Функції аналітичних розрахунків та прийняття рішень в мережі зосереджені в централізованому мережевому контролері, який відслідковує

загальний стан мережевої інфраструктури і потоків даних, що протікають через неї. Управління мережею переноситься в єдину логічну точку управління, що значно спрощує процес конфігурації та керування. Простішим виглядає і функціонування мережевих пристроїв, тому що на відміну від традиційних підходів не має потреби більше підтримувати та обробляти велику кількість різноманітних протоколів, а достатньо тільки приймати та виконувати інструкції від контролерів. Проведення налаштування мережі відбувається кодуванням програмного контролера мережі, замість того, щоб переписувати сотні рядків кодів в великій кількості мережевих пристроїв. Відслідковування та зміна поведінки мережі відбувається в процесі роботи, а впровадження нових рішень відбувається за набагато коротший час, ніж в традиційній моделі. Проведення централізування мережевих функцій в одній точці перетворює мережі в такі, що можуть конфігуруватися за допомогою засобів програмування. Контролери мережі також мають набори прикладних інтерфейсів, які дають змогу виконувати типові завдання маршрутизації, наприклад, групової передачі, безпека на різних рівнях роботи автономної системи, управління пропусною здатністю, контроль доступу до ресурсів, якість обслуговування користувачів, які впроваджуються під задачі конкретного споживача.

Основною задачею маршрутизатора стає тільки рівень передачі даних. Замість маршрутизатора використовується простіший варіант обладнання, задача якого полягає в аналізі даних, що отримуються на нього та визначення адрес на основі яких, якщо адресат є в таблиці комутації, негайно відбувається передача даних використовуючи комутаційну матрицю. В іншому випадку маршрутизатор через захищений канал відправляє запит до центрального контролера мережі, щоб на основі отриманої інформації, провести необхідні зміни в таблиці комутації, в результаті чого здійснюється оброблення отриманих даних (таким чином устаткування не переналаштовується вручну, а приймає налаштування використовуючи

спеціальне програмне забезпечення). Основною ідеєю створення програмно конфігурованих мереж стає створення однотипного, незалежного від виробника мережевого обладнання, програмно-конфігурованого інтерфейсу між контролером та середовищем транспортування мережі, що було реалізовано на основі протоколу “OpenFlow”. Такий підхід дає змогу користувачам самим визначати і контролювати, на яких умовах і з якою якістю можна взаємодіяти в мережі. В мережах без автоматизації маршрутизації через програмно конфігуровані мережі, адміністратор вручну налаштовує обладнання згідно технічного завдання та прийнятих рішень маршрутизації, і всі зміни здійснюються на апаратному рівні. Протокол “OpenFlow” дає змогу використовувати нові можливості керування мережею, що підвищує її масштабованість та керованість. Функціональність програмно конфігурованих мереж розширюється не тільки розподіленим способом управління, але і правилами пересилки даних, що містяться у таблицях потоків.

Набори інструкцій, що визнаються специфікацією OpenFlow є різноманітними для обробки пакетів даних, серед яких передавання до порту або групи портів чи контролеру (“Output”), зміна полів (“Set-Field, Change-TTL”), робота з тегами “IEEE 802.1Q” та “MPLS (Push-Tag/Pop-Tag)”, групові операції (“Group”) та ін. В запропонованій архітектурі існує специфікація гібридного комутатора, який має змогу підтримувати як “OpenFlow”-операції разом з класичною комутацією чи маршрутизацією. Протокол “OpenFlow” спрощує фахівцям початкові налаштування мережі та передачу її в експлуатацію в автоматичному режимі для підтримки заданого QoS. Все мережеве обладнання об’єднується під управлінням єдиної операційної системи, яка здійснює управління мережею через програмне забезпечення і в режимі реального часу відстежує конфігурацію елементів мережі.

При розгортанні програмно конфігурованих мереж потрібно врахувати можливість виходу з ладу контролера або його дублюючих

елементів. В такому випадку мережа повинна мати альтернативні режими роботи для уникнення створення вузьких місць чи унеможливлення роботи взагалі. При правильному проектуванні мережі та виборі обладнання може відбуватись певне уповільнення передачі даних, проте з врахуванням плану відновлення від критичних ситуацій це дасть час для усунення несправностей.

Контролери можуть бути реалізовані на різноманітному обладнанні, де за допомогою операційної системи забезпечується зв’язок з програмними додатками, що відповідають за визначені функції. Це включає в себе пошук та виявлення активних маршрутизаторів в мережі, знаходження активних портів на пристроях, налагодження зв’язоку за допомогою протоколу OpenFlow. Таблиці потоків заповнюються через опис логіки комутації і маршрутизації пакетів.

Отож, при організації маршрутизації в автономних системах створення віртуалізованих мережевих ресурсів, забезпечення надійної роботи апаратної частини та доступності контролерів є дуже важливою задачею, що потребує правильного проектування та реалізації.

3.3 Висновки до третього розділу

В третьому розділі дипломної роботи на основі проведених досліджень запропоновано модель віртуалізації маршрутизації в автономній системі через резервування мережевих ресурсів з врахуванням потоків інформації та аналізом вимог до роботи. На основі запропонованої моделі визначено два варіанти віртуалізації, що дає змогу вирішувати поставлені завдання з ефективним розподілом ресурсів.

4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Аналіз живучості мереж

Під живучістю системи розуміють її здатність зберігати повну або часткову працездатність в умовах впливу несприятливих факторів (виведення з ладу елементів системи, відмови, критичне збільшення робочого навантаження тощо). Зокрема, живучість, як властивість розподіленої комп'ютерної системи (РКС), характеризує її здатність обирати оптимальний режим функціонування за рахунок власних внутрішніх ресурсів, перебудови структури, зміни функцій та поведінки окремих підсистем у зв'язку зі зміною зовнішніх умов і відповідно до цілі її функціонування.

Під живучою комп'ютерною мережею (далі — ЖКМ) будемо розуміти таку, однією із системних характеристик якої є живучість.

Під фактором впливу на живучість (далі – ФВЖ) будемо розуміти зміну умов роботи ЖКМ, яка призводить до підвищення або зниження її живучості. Під системою моніторингу факторів впливу на живучість (далі – СМФ) будемо розуміти програмно-апаратну систему, яка виконує моніторинг ФВЖ.

Виділимо основні етапи створення системи моніторингу живучості:

1) визначення цілей, стратегії й загальної політики щодо моніторингу живучості;

2) аналіз і розробка вимог;

3) визначення методики проектування – крок, призначенням якого є вибір методів розпізнавання та аналізу ФВЖ і способу їхнього застосування для наступних кроків, яка задовольнятиме вимогам, сформульованим у п. 2;

4) проектування СМФ на основі систематичного застосування обраних на попередньому кроці методів аналізу ФВЖ;

5) реалізація системи та інтеграція її з іншими підсистемами ЖКМ. Даний крок має бути підтриманий підготовкою програм із навчання співробітників, адміністраторів і персоналу служб керування інформаційною безпекою;

6) функціонування СМФ, що охоплює сукупність процедур і дій, таких як: перевірка погодженості засобів системи і їхньої відповідності сформованим вимогам, контроль за коректністю роботи СМФ, перегляд проектних і експлуатаційних рішень за результатами експлуатації, супровід (триваюча розробка) засобів СМФ, відстеження позаштатних ситуацій і реакція на них.

Моніторинг факторів впливу на живучість, є чинником, який дозволяє досліджувати поточний рівень живучості системи та прогнозувати майбутній. Інформація СМФ потребує щоденного аналізу з боку системного адміністратора. В іншому випадку реакція на ФВЖ виявиться спізнілою. Моніторинг передбачає: – збір даних із різних джерел; – визначення кореляцій; – виявлення ознак ФВЖ. Стан живучості системи у будь-який момент часу характеризується параметрами, сукупність яких дає змогу оцінити його функціональну відповідність завданням, що розв’язуються ЖКМ. У той же час оцінка цих параметрів вміщує оцінку відповідних параметрів складових ЖКМ.

Життєвий цикл моніторингу складається з 4-х фаз:

1) ідентифікації ресурсів і проблем;

2) визначення основних можливостей (істотні, несуттєві; проблемні області, способи їхнього усунення й ін.);

3) визначення другорядних можливостей (істотні, несуттєві; проблемні області, способи їхнього усунення й ін.);

4) аналізу живучості (виявлення тенденцій із використання ресурсів, визначення динаміки росту, вироблення політики).

Результатом формування є документ, у якому сформульовано всі типи вимог, у відповідності з обраними стандартами проектування , згруповані наступним чином:

– функціональні;

– інтерфейсні;

– до продуктивності;

– специфічні;

– характеристики якості;

– інші.

Функціональні вимоги:

– збір даних: система моніторигу повинна забезпечувати безперервне отримання даних щодо ФВЖ, як у середині ЖКМ, так і за її межами;

– визначення кореляцій: СМФ повинна забезпечувати автоматичне виявлення залежностей між окремими ФВЖ;

– виявлення ознак ФВЖ: СМФ повинна забезпечувати введення ознак ФВЖ до БД та їхнє автоматичне розпізнавання;

– інформування користувачів: СМФ повинна забезпечувати надсилання повідомлень до визначених користувачів електронною поштою (протокол SMTP) чи шляхом надсилання мережевих повідомлень (для користувачів, які знаходяться в локальній мережі);

– інформування системи керування: СМФ повинна забезпечувати передачу до системи керування повідомлень при виникненні ФВЖ;

– збереження даних: СМФ повинна мати механізми для збереження інформації до БД та наступного її отримання.

Інтерфейсні вимоги:

– вимоги до інтерфейсів користувачів;

– вимоги до апаратних інтерфейсів;

– вимоги до програмних інтерфейсів;

– вимоги до комунікаційних інтерфейсів.

Вимоги до продуктивності:

– кількість і характеристики об’єктів моніторингу;

– максимальна кількість користувачів СМФ;

– максимальна кількість одночасно відкритих файлів.

Специфічні вимоги залежать від особливостей комп’ютерної мережі, у якій здійснюється моніторинг. Їх можна згрупувати наступним чином:

– відповідність стандартам, за якими створюється комп’ютерна мережа;

– особливості апаратного забезпечення ЖКМ.

Основними характеристиками якості СМФ будемо вважати:

– коректність реалізації;

– ефективність;

– гнучкість;

– захищеність;

– здатність до взаємодії;

– переносність;

– достовірність;

– здатність повторного використання;

– здатність до тестування;

– простоту використання.

Додатково доцільно визначити ще ряд вимог:

– вимоги до БД СМФ (граничний обсяг, кількість записів);

– вимоги до адаптації та інсталяції СМФ. Для забезпечення аналізу живучості система моніторингу повинна надавати можливість опису:

– інформаційних процесів ЖКМ;

– користувачів і їхніх функцій, підметів автоматизації в прив’язці до структури ЖКМ;

– інформаційних і фізичних об’єктів мережі;

– сценаріїв виконання інформаційних функцій;

– станів системи;

– матрицю взаємозв’язків між ФВЖ.

Виконання моніторингу живучості й виявлення ФВЖ вимагає наявності в складі СМФ підсистеми формування звітності, необхідної для діагностики мережі й одержання статистичного представлення про її живучість. Звіти формуються на основі записів про виявлені фактори, містять обов’язково часові мітки та характеристики ФВЖ. Звіти мають відображатися в текстовій та графічній формі, і бути пристосованими до легкого експорту в інший формат. До складу звітів, які формуються СМФ, повинні входити:

1) звіт про виявлені ФВЖ – має показувати докладну статистику про розпізнані системою факторів впливу на живучість за заданий проміжок часу, включаючи такі параметри, як тривалість фактору та інші статистичні дані;

2) звіт контролю живучості – має показувати статистику інтегрального показника живучості за заданий період часу;

3) звіт про відновлення живучості – має включати інформацію про заходи, які були ініційовані в системі, з метою подолання негативних ФВЖ і відновлення живучості системи;

4) звіт про поточний стан живучості – має показувати всі активні на даний момент часу фактори;

5) загальний звіт – має показувати загальну тривалість факторів впливу на живучість і загальну кількість повністю чи частково нейтралізованих, виявлених із запізненням ФВЖ. Звіт має бути доступним у графічній і текстовій формі.

Основними ФВЖ, які мають відслідковуватися СМФ, доцільно визначити ті фактори, які призводять до порушення цілісності інформаційного ресурсу ЖКМ:

– порушення цілісності окремих компонентів ЖКМ (пристроїв, обладнання);

– порушення цілісності, у тому числі умисна модифікація інформаційних ресурсів (програмного забезпечення також);

– переривання передачі потоку даних (трафіка);

– виконання ініціації фіктивного з’єднання;

– неправомірна зміна режимів роботи ЖКМ (її окремих компонентів, обладнання, програмних засобів тощо), ініціювання технологічних чи тестувальних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації).

Причинами таких ФВЖ можуть бути:

– зміна умов фізичного середовища (стихійні лиха: землетрус, повінь, пожежа й аварії або інші випадкові події);

– збої та відмови в роботі обладнання та технічних засобів ЖКМ;

– наслідки помилок під час проектування та розробки компонентів ЖКМ (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– впливи природних завад (грозові розряди, іскріння в електромережах, під час електрозварювання та т.п.).

На основі сформованих вище вимог можна запропонувати архітектуру системи моніторингу факторів впливу на живучість. Оскільки ЖКМ представляє собою класичну територіально розподілену комп’ютерну мережу, яка взаємодіє з іншими мережами, наприклад, Internet, і має розвинені засоби адміністрування та зберігання даних, доцільно будувати СМФ, базуючись на доступних засобах моніторингу.

4.2 Безпека живучості мереж

Безпека – це комплексне поняття, що описує обмеження небажаного доступу, збереженість інформації та живучість самої мережі. Актуальність проблеми підтверджується кількістю RFC-документів, опублікованих за останній час.

Існують юридичні аспекти мережевої безпеки, організаційні та програмно-технічні.

Джерелами ненадійності мережі можуть бути:

– стихійні явища, до яких можна віднести відмови обладнання або живлення, а також некомпетентність персоналу, що обслуговує систему;

– несанкціоновані дії операторів ЕОМ.

Основу стабільності мережі складають надійність ЕОМ та мережевого обладнання, а також стійкість каналів зв’язку. Якість мережевого живлення (стабільність напруги та частоти, амплітуда перешкод). Для вирішення даної проблеми використовують спеціальні фільтри, мотор-генератори та UPS.

Так як абсолютна надійність недосяжна, одним із засобів збереження інформації є її дублювання, копіювання та збереження копій в надійному місці.

Багато проблем щодо мережевої безпеки вирішуються під час використання проксі або фаєрволу. Але навіть фаєрвол не може запобігти атакам з боку хакерів, що працюють всередині локальної мережі. Тут до їх послуг величезний арсенал. Це перш за все, використання мережевого інтерфейсу для прийому всіх пакетів, що слідують по сегменту, а також програмні продукти типу tcpdump або Etherfind. Такий режим легко дозволяє перехопити незашифровані паролі, визначати номера портів, або ISN.

Постійний моніторинг широкомовних запитів треба вважати однією з складових частин системи безпеки локальної мережі, тим більше що такий моніторинг не породжує додаткового трафіку.

Визначену користь з точки зору безпеки може принести програми типу wrapper, яка дозволяє відфільтрувати небажані запити та вирішити проблему аутентифікації. Нові можливості в цій сфері надасть нова версія протоколу IPv6. Деякі проблеми можуть бути вирішеними шляхом шифрування вмісту пакетів.

Є правила, яким повинен слідувати будь-який адміністратор. Серед них жорстка вимога до вибору паролів та регулярній зміні є найголовніше. Відомо, що 80% усіх проблем, пов'язаних з нелегальним проникненням в мережу, викликані поганими паролями.

Однією з мір безпеки в локальній мережі може бути кодування усіх пакетів, що посилаються з віддалених терміналів. Для реалізації цього треба модифікувати усе мережеве програмне забезпечення, або забезпечити мережу спеціальними апаратними засобами.

4.3 Висновки до четвертого розділу

В четвертому розділі дипломної роботи розглянуто питання моніторингу живучості комп’ютерних мереж та підвищення живучості за рахунок впровадження контролю безпеки.

5 ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від впровадження маршрутизації в межах автономної системи, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільності впровадження відповідної розробки.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Витрати часу по окремих операціях процесу налагодження та роботи маршрутизації в межах автономної системи відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Витрати праці на створення технічного завдання маршрутизації в межах автономної системи	Інженер	17
2.	Витрати праці на розробку фізичної топології мережі	Інженер	20
3.	Витрати праці на розробку локальної адресації мережі	Інженер	12
4.	Витрати праці на побудову мережі згідно поставленого завдання	Інженер	75
5.	Витрати праці на підготовку документації	Інженер	20
6.	Приблизний час роботи мережі	Інженер	10000
Разом			10144

5.2 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 – 30,00...50,00 грн./год., інженер – 22,41...30,00 грн./год., консультант – 22,41...30,00 грн./год., технік – 22,41...30,00 грн./год., лаборант – 22,41...25,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г, \qquad (5.1)$$

де T_c – тарифна ставка, грн.;

$K_г$ – кількість відпрацьованих годин.

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

$$З_{осн.} = 22{,}41 \cdot 10144 = 227327{,}04 \ грн.$$

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

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод.} = 227327{,}04 \cdot 0{,}15 = 34099{,}06 \ грн.$$

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

$$В_{о.п.} = З_{осн.} + З_{дод.}. \quad (5.3)$$

$$В_{о.п.} = 227327{,}04 + 34099{,}06 = 261426{,}10 \ грн.$$

Крім того, слід визначити відрахування на соціальні заходи в розмірі становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{ОП} \cdot 0{,}235, \quad (5.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$В_{с.з.} = 261426{,}10 \cdot 0{,}235 = 61435{,}13 \ грн.$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 5.2.

Таблиця 5.2 – 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	22,41	10144	227327,04	34099,06	61435,13	322861,23

5.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i, \tag{5.5}$$

Де: q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{Bi}. \tag{5.6}$$

Проведені розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транспортно–заготівельні витрати, грн	Загальна сума витрат на матеріали, грн
1	2	3	4	5	6	7
1. Основні матеріали						
Маршрутизатор	штук	4	35000,00	14000,00	3500,00	143500,00

Продовження таблиці 5.3

Кабель	метри	1500	20,00	30000,00	315,00	30315,00
Комп'ютери	штук	11	15000	165000	2500	167500,00
Інше мережеве обладнання та матеріали	-	-	2000	2000	-	2000
2. Допоміжні витрати						
Використання мережі Internet	години	–	240	240	–	240
Разом:						343555,00

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S \text{ ,} \tag{5.7}$$

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 (0,203 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 0,2436 грн.

Потужність мережевого обладнання – 6 кВт, кількість годин роботи обладнання згідно таблиці 3.1 –10144 годин.

Тоді, $З_е = 6 \cdot 10144 \cdot 0{,}2436 = 14826{,}47$ *грн.*

5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва 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 амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

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

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

$Н_А$ – норма амортизації, %.

Для даного проекту вартість обладнання становить 15000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{15000 \cdot 5\%}{100\%} = 750{,}00 \ грн.$$

Оскільки робота мережі 10144 годин, то амортизаційні відрахування будуть становити:

$$A = \frac{750{,}00 \cdot 10144}{150} = 50720{,}00 \ грн.$$

5.6 Обчислення накладних витрат

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.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6, \tag{5.9}$$

де H_B – накладні витрати.

Отже, накладні витрати:

$H_в = 261426{,}10 \cdot 0{,}2 = 52285{,}22$ *грн.*

5.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	261426,10	33,33
Відрахування на соціальні заходи	61435,13	7,83
Матеріальні витрати	343555,00	43,81
Витрати на електроенергію	14826,47	1,89
Амортизаційні відрахування	50720,00	6,47
Накладні витрати	52285,22	6,67
Собівартість	784247,92	100

Собівартість (C_B) мережі розрахуємо за формулою:

$$C_B = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + A + H_в. \quad (5.10)$$

Отже, собівартість локальної мережі дорівнює:

$$C_B = 261426,10 + 61435,13 + 343555,00 + 14826,47 + 50720,00 + 53285,22 = 784247,92 \text{ грн.}$$

5.8 Розрахунок ціни мережі

Ціну мережі можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ), \quad (5.11)$$

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 розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Вн.і. , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.12)$$

Звідси ціна на проект складе:

$$Ц = 784247{,}92 \cdot (1+0{,}3) \cdot (1+0{,}2) = 1223426{,}75 \; грн.$$

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = \frac{П}{C_В}, \tag{5.13}$$

де $П$ – прибуток;

$C_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_В. \tag{5.14}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 1223426{,}75 - 784247{,}92 = 439178{,}83 \; грн.$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{Св}. \tag{5.15}$$

Тоді, $E_р = \frac{439178{,}83}{784247{,}92} = 0{,}56$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (Тр):

$$T_p = \frac{1}{E_p}, \tag{5.16}$$

Термін окупності дорівнює:

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

5.10 Висновки до п’ятого розділу

В цьому розділі дипломної роботи було розраховано основні техніко–економічні показники від організації маршрутизації в межах автономної системи (таблиця 5.5).

Розраховане значення економічної ефективності становить 0,56, що є прийнятним значенням.

Так само нормальним є термін окупності. Для даної мережі він становить 1,8 років.

Таблиця 5.5 – Техніко–економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	784247,92
2.	Плановий прибуток, грн..	439178,83
3.	Ціна, грн.	1223426,75
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Отже, дані методи маршрутизації в межах автономної системи можуть бути впроваджені та мати подальший розвиток, оскільки вони є економічно вигідним за всіма основними техніко–економічними показниками.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

6.1.1 Особливості стандарту OHSAS 18001 щодо процедур для ідентифікації небезпек та оцінки ризиків, а також особливості методології самого процесу ідентифікації

Стандарт ДСТУ OHSAS 18001:2010 (OHSAS 18001:2007, IDT) регламентує побудову системи якості на підприємстві, яка спрямована на підтримку системи охорони праці на підприємстві, гігієни праці, безпеки співробітників тощо. Він містить мінімальні вимоги до системи охорони праці і промислової безпеки. Підприємство яке впровадило та сертифікувало таку систему демонструє наступні можливості:

– можливість створення кращих та безпечніших умов праці;

– можливість своєчасного виявлення загроз та їх ліквідації;

– зниження вірогідності аварій, нещасних випадків та інцидентів;

– відповідати нормативно-правовим вимогам та підвищувати загальну ефективність персоналу.

Стандарт застосовується до підприємств будь-якого типу, незалежно від розміру, місцезнаходження, характеру та складності виробництва. Він може бути впроваджений самостійно на підприємстві, або інтегрований з будь-якою іншою системою управління, наприклад ISO 9001, ISO 14001 чи ISO 22000.

Орган з сертифікації систем менеджменту проводить сертифікацію систем управління гігієною та безпекою праці, на відповідність вимогам державного стандарту ДСТУ OHSAS 18001:2010 (OHSAS 18001:2007). Завдяки сертифікації вимогам стандарту OHSAS 18001, підприємство отримує наступні переваги:

– позитивний імідж, як з боку партнерів чи споживачів, так і з боку державних наглядових органів;

– інвестиційна привабливість, з причини зниження професійних ризиків;

– підвищення конкурентоспроможності серед конкурентів.

Ідентифікацію небезпек і оцінювання ризиків необхідно виконувати, щоб розпізнати та зрозуміти небезпеки, які можуть виникнути у процесі діяльності підприємства, оцінити ризик, який випливає з конкретної небезпеки, а також запровадити заходи щодо зниження ймовірності виникнення небезпек. Оцінювання ризиків є найбільш ефективним запобіжним заходом, під час якого враховують не тільки ті інциденти, які стались у минулому, але й небезпеки, які ще не викликали негативних наслідків.

Для проведення ідентифікації небезпек і оцінювання ризиків на постійній основі потрібно розробити методику ідентифікації небезпек і оцінювання ризиків, орієнтовану на запобігання інцидентів, яка забезпечує встановлення пріоритетів, документування ризиків і використання необхідних заходів безпеки. При розробленні методики ідентифікації небезпек і оцінювання ризиків враховуються сфера застосування системи управління охороною праці (СУОП), характер можливих небезпек, потреба в докладності отриманих даних за результатами ідентифікації небезпек і оцінювання ризиків, необхідні ресурси, інші чинники, важливі для підприємства. У розробленій методиці має бути обов’язково визначено:

– обов’язки і повноваження посадових осіб, які планують роботи з ідентифікації небезпек і оцінювання ризиків, організовують виконання цих робіт, виконують ці роботи. Ідентифікацію небезпек, оцінювання ризиків і визначення заходів безпеки здійснюють фахівці, які володіють необхідними знаннями про виробничу діяльність, про процедуру ідентифікації небезпек і оцінювання ризиків. Визначається необхідність створення робочих груп у

підрозділах чи на дільницях і можливий склад таких груп: керівник підрозділу/дільниці (начальник відділу, майстер), фахівці (механік, електрик, енергетик, інженер з метрології, досвідчені робітники) тощо;

– процедуру ідентифікації небезпек;

– методологію оцінювання ризиків і встановлення необхідних заходів безпеки;

– форми документів, які потрібно вести під час проведення робіт з ідентифікації небезпек і оцінювання ризиків, а також порядок їх ведення, зберігання тощо;

– строки подання результатів ідентифікації небезпек і оцінювання ризиків керівництву для аналізування й затвердження документів, а також подальшого планування та організації робіт з охорони праці;

– порядок поновлення (внесення змін чи перегляду) документів з ідентифікації небезпек і оцінювання ризиків, умови, за яких їх поновлюють (за результатами атестації робочих місць за умовами праці), та підстави для проведення робіт з ідентифікації небезпек і оцінювання ризиків у вже запровадженій СУОП (зміни в організації діяльності підприємства).

Ідентифікацію небезпек, оцінювання ризиків і визначення заходів безпеки обов’язково здійснюють:

– під час розроблення СУОП;

– щоразу, коли потрібно вносити будь-які зміни до запровадженої СУОП, операцій, процесів, інфраструктури тощо.

Встановлені ризики та визначені засоби безпеки враховують під час розроблення, запровадження та підтримання функціонування СУОП.

За результатами ідентифікації небезпек і оцінювання ризиків, пов’язаних зі змінами, слід визначити:

– появу нових небезпек у зв’язку із запровадженням певних змін та ризиків, пов’язаних з цими небезпеками;

– зміну ризиків, пов’язаних з іншими небезпеками;

– потребу в запроваджені інших заходів безпеки та яких саме.

Необхідність проведення ідентифікації небезпек і оцінювання ризиків також розглядають, якщо наприклад:

– є потреба визначити ефективність і адекватність запроваджених заходів безпеки;

– дані розслідування інцидентів і надзвичайних ситуацій вказують на необхідність проведення повторної ідентифікації небезпек і оцінювання ризиків;

– під час проведення внутрішніх аудитів виявлено невідповідності, прийняття рішення щодо усунення яких можливе за допомогою проведення ідентифікації небезпек і оцінювання ризиків.

У СУОП запроваджують такі етапи виконання робіт з ідентифікації небезпек і оцінювання ризиків:

– планування робіт з ідентифікації небезпек і оцінювання ризиків;

– ідентифікація небезпек;

– оцінювання ризиків і визначення їх прийнятності;

– визначення достатності наявних заходів безпеки;

– запровадження за потреби більш ефективних заходів безпеки;

– моніторинг ризиків у сфері охорони праці та визначених заходів безпеки, аналізування даних моніторингу.

Під час ідентифікації небезпек розглядають діяльність усіх осіб, які мають доступ до робочого місця (зокрема, відвідувачів, підрядників), щоб визначити небезпеки, пов’язані з їхньою діяльністю, та звернути увагу на їхню поведінку.

Людський фактор (психологічна і фізіологічна здатності та їх обмеження, поведінка людини) необхідно враховувати під час оцінювання небезпек і ризиків виробничих процесів і виробничого середовища з точки зору того, чи може цей фактор стати причиною неправильних дій, помилок тощо. Людський фактор треба враховувати кожного разу, коли розглядають

взаємовідносини працівників у колективі, і брати до уваги такі питання, як стрес, втома працівника, погіршення самопочуття, невпевненість під час виконання робіт.

За результатами ідентифікації небезпек має бути щонайменше встановлено:

– небезпека (об’єкт, ситуація чи дія, або їх поєднання);

– місце, де виникає небезпека (підрозділ, дільниця тощо);

– вид робіт, операцій, під час виконання яких виникає небезпека;

– працівники, які наражаються на небезпеку (зокрема їх посада, професія), а також усі сторонні особи, які мають доступ до місця виникнення небезпеки.

Оцінювання ризиків полягає у визначенні величини ризиків, аналізу можливих наслідків і ймовірності їх виникнення, прийнятті рішення стосовно прийнятності чи неприйнятності ризиків.

Методи оцінювання ризиків поділяються на якісні та кількісні. Якісний метод полягає у виявленні та ідентифікації причин і видів ризиків. Кількісний метод – це оцінка частоти ризиків або ймовірності їх наслідків.

Вибір методу проводиться, виходячи з цілей оцінювання ризиків, фахової компетентності, потреби в ресурсах тощо.

У більшості випадків ризик можна оцінити за допомогою методів на основі експертної оцінки фахівців.

За результатами оцінювання ризиків має бути встановлено величину виявленого ризику, зокрема зазначено неприйнятні ризики. Ця інформація використовується під час визначання черговості запровадження заходів безпеки.

За результатами оцінювання ризиків визначають адекватність наявних заходів безпеки, потребу в їх поліпшенні чи запровадженні інших заходів безпеки.

Дані щодо ідентифікованих небезпек, ризиків, пов’язаних з небезпеками, а також вжитих заходів безпеки документують, наприклад у вигляді переліку небезпечних чинників і відповідних заходів безпеки.

6.1.2 Організація робочого місця працівника у сфері ІТ: мікроклімат та вентиляція

Конституція України гарантує кожному право на належні, безпечні і здорові умови праці.

Загальні вимоги до умов праці на підприємствах встановлено законодавством про працю. Відповідно до ч. 1 ст. 6 Закону України “Про охорону праці” від 14.10.92 р. № 2694-XII (далі – Закон про охорону праці) умови праці на робочому місці, безпека технологічних процесів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам законодавства.

Більшість нормативів щодо умов праці офісних працівників встановлено на рівні державних стандартів. Основними з них є:

– Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку ДСН 2.3.6.037-99, затверджені постановою Головного державного санітарного лікаря України від 01.12.99 р. № 37;

– Державні санітарні норми виробничої загальної та локальної вібрації ДСН 3.3.6.039-99, затверджені постановою Головного державного санітарного лікаря України від 01.12.99 р. № 39;

– Державні санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджені постановою Головного державного санітарного лікаря України від 01.12.99 р. № 42;

– Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН

3.3.2.007-98, затверджені постановою Головного державного санітарного лікаря України від 10.12.98 р. № 7;

– Правила охорони праці під час експлуатації електронно-обчислювальних машин, затверджені наказом Держгірпромнагляду від 26.03.2010 р. № 65 (далі — Правила № 65);

– Загальні вимоги стосовно забезпечення роботодавцями охорони праці працівників, затверджені наказом МНС від 25.01.2012 р. № 67.

Відповідно до ч. 1 ст. 13 Закону про охорону праці роботодавець зобов'язаний створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів.

Приміщення для роботи з персональними комп'ютерами мають бути обладнані системами опалення, кондиціонування повітря, або припливно-витяжною вентиляцією. У приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості та рухливості повітря відповідно до норм та правил, а також ДБН В.2.5-67:2013 "Опалення, вентиляція та кондиціонування", затверджених наказом Мінрегіону від 25.01.2013 р. № 24.

Відповідно до санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99 в офісних приміщеннях температура повітря повинна становити 22–25°С, відносна вологість повітря – 40-60%, швидкість руху повітря – не більше 0,1 м/с.

Під час перевищення припустимих значень робочий день співробітників повинен бути скорочений мінімум на 10%.

Для підтримки допустимих значень мікроклімату та концентрації позитивних і негативних іонів необхідно передбачати установки або прилади зволоження та/або штучної іонізації, кондиціювання повітря. В Україні відсутні затверджені на законодавчому рівні гранично допустимі норми вмісту вуглекислого газу в повітрі для житлових, офісних та громадських споруд. Проте, враховуючи його вплив на працівників, а саме суттєве

зниження їх працездатності, роботодавцям варто приділяти цьому питанню увагу та вживати заходи профілактики.

Окрім цього, наслідком сучасного технічного прогресу є зростання з кожним роком енергоспоживання та збільшення навантаження на кабелі, що в свою чергу призводить до збільшення напруги електромагнітних полів, несприятлива дія яких може призвести до погіршення стану здоров'я працівників. Таким чином, роботодавцям варто пам'ятати, що причиною зниження працездатності офісних працівників дуже часто є саме незадовільні параметри мікроклімату.

В розділі "Охорона праці" розглянуто питання особливості стандарту OHSAS 18001 щодо процедур для ідентифікації небезпек та оцінки ризиків, а також особливості методології самого процесу ідентифікації; організації робочого місця працівника у сфері ІТ: мікроклімат та вентиляція.

6.2 Безпека в надзвичайних ситуаціях

6.2.1 Фактори, що впливають на функціональний стан користувачів комп'ютерів

Трудова діяльність користувачів комп'ютерів (ВДТ) відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі – фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників. Вплив хімічних та, особливо, біологічних факторів виробничого середовища на користувачів комп'ютерів – значно менший.

Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп'ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які

забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями.

Професійні якості та виробничий досвід, які визначають внутрішні засоби діяльності, обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи розв'язання виробничих завдань навіть у нестандартних ситуаціях.

Зовнішні засоби діяльності, які в основному визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його елементів, просторового розташування основного і допоміжного устаткування, можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів.

У професійних операторів частіше зустрічаються порушення органів зору, опорно-рухового апарату, центральної нервової, серцево-судинної, імунної та статевої систем, захворювання шкіри. Зафіксована значна кількість скарг операторського персоналу на загальне недомагання, передчасне стомлювання, головний біль, порушення функцій органів зору, які здійснювали несприятливий психофізіологічний вплив на самопочуття та працездатність операторів.

Сучасна професія користувача ВДТ належить до розумової праці, яка характеризується: високою напруженістю зорових функцій; одноманітною позою; великою кількістю стереотипних висококоординованих рухів, що виконуються лише м'язами кистей рук на фоні малої загальної рухової активності; значним нервово-емоційним компонентом, особливо в умовах дефіциту часу; роботою з великими масивами інформації, що викликає активізацію уваги та інших вищихпсихічних функцій. Крім того, при роботі з дисплеями на електронно-променевих трубках виникає вплив на користувача цілої низки факторів фізичної природи – електростатичні поля, радіочастотне та рентгенівське випромінювання тощо.

Діяльність професіоналів можна поділити на три групи:

1. Діяльність, яка пов’язана з виконанням нескладних багаторазово повторюваних операцій, що не вимагають великого розумового напруження. Наприклад, робота операторів комп’ютерного набору, працівників довідкових служб.

2. Діяльність, яка пов’язана із здійсненням логічних операцій, що постійно повторюються. Це робота інженера-економіста, інженера-проектувальника, оператора автоматизованого виробництва.

3. Діяльність, коли в процесі роботи необхідно приймати рішення за відсутності заздалегідь відомого алгоритму. Наприклад, робота інженера-програміста, диспетчерів руху залізничного транспорту, аеропортів тощо.

У користувачів, які інтенсивно використовують комп’ютер в умовах значних розумових напружень досить часто (40-70%) виникають психологічні та поведінкові порушення (нервозність, роздратування, тривога, нерішучість, замкнутість тощо). Серед користувачів ВДТ в США і Європі значного поширення набуло специфічне захворювання, яке отримало назву синдром комп’ютерного стресу (СКС). СКС супроводжується головним болем, запаленням очей, алергією, роздратованістю, млявістю і депресією. Інформаційне перевантаження користувачів ВДТ супроводжується низкою специфічних захворювань, які називають інформаційними. Першим симптомом їх є головний біль. Дослідження, проведені в США, Німеччині, Швейцарії та інших країнах, показали, що робота з обслуговування ВДТ супроводжується підвищеним напруженням зору, інтенсивністю і монотонністю праці, збільшенням статичних навантажень, нервово-психічним напруженням, впливом різного виду випромінювань та ін. Внаслідок цього серед операторів ВДТ, як зазначають фахівці Всесвітньої організації охорони здоров'я, частіше, ніж в інших групах працюючих, трапляються такі професійні захворювання, як передчасна стомлюваність, погіршення зору, м'язові і головні болі, психічні й нервові розлади, хвороби

серцево-судинної системи, онкологічні захворювання та ін. Вважається, що стан організму операторів ВДТ визначається комплексним впливом факторів трудового процесу і середовища, значення яких є неоднаковим. На операторів з малим стажем роботи на ВДТ домінуючий вплив чинять фактори середовища, а на операторів зі стажем понад 5 років – фактори трудового процесу.

Комп'ютерний зоровий синдром (КЗС) – комплекс порушень здоров'я, який може виникати у користувачів персональних комп'ютерів (ПК). Діагноз ставлять, якщо людина, що працює за ПК протягом двох годин, висловлює хоча б дві з десяти скарг: головний біль; сльозотеча; різь; туман; двоїння; свербіж; важкість в очах; фотофобія; миготіння знаків на екрані; нудота.

У користувачів ПК дуже поширені кон'юнктивіти і блефарити, патогенетично пов'язані з КЗС.

Синдром розвивається при умові, що робоче місце організовано неправильно – у користувача незручне крісло, відсутні пюпітри для паперів, підставки для ніг та кистей рук, не встановлена висота і нахил монітора відносно очей, відстань від очей до екрана. За таких умов тіло людини при роботі займає вимушене положення: спина статично напружена, шия витягнута, плечі жорстко фіксовані. Напружені м'язи погіршують кровотік у сонних артеріях, а недостатнє кровозабезпечення головного мозку веде до очманіння, появи головного болю. На фоні шийного остеохондрозу з'являється відчуття випирання очних яблук, туману в очах, мушок та райдужних кіл у полі зору. Розвитку КЗС сприяє поганий мікроклімат приміщення, значна загальна іонізація та мікробне забруднення, а також куріння.

Національною радою з наукових досліджень США для стану зорового дискомфорту був уведений термін "астенопія", який означає "будь-які суб'єктивні зорові симптоми чи емоційний дискомфорт, що є результатом

зорової діяльності”. Симптоми астенопії були класифіковані на “очні” (біль, печія та різь в очах, почервоніння повік та очних яблук, ломота у надбрівній частині тощо) та “зорові” (пелена перед очима, мерехтіння, швидка втома під час зорової роботи та ін.).

У операторів ВДТ “очні” симптоми трапляються частіше, ніж “зорові”, причому частота проявів астенопії вища у жінок, ніж у чоловіків і більше виражена в осіб середнього і старшого віку. Причиною вважається електромагнітне випромінювання від ВДТ.

6.2.2 Оцінка стійості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху

Забезпечення високої стійкості роботи народного господарства держави у НС мирного та військового часу розглядається як одна із головних задач ЦО держави. Стійкість народного господарства держави в цілому та його галузей визначається стійкістю роботи кожного об’єкта.

Під стійкістю роботи(firmness of work) підприємства у надзвичайних умовах мирного та військового часу розуміється його можливість продовжувати випуск установлених видів продукції в об’ємах і номенклатурі передбачених відповідними планами та контрактами, а також пристосованість об’єкта до відновлення функціонування в короткі строки і за рахунок власних фондів у випадках отримання пошкоджень, слабких або середніх зруйнувань. Всі роботи по підвищенню стійкості функціонування об’єкта господраської діяльності (ОГД) повинні проводитись з урахуванням наступних принципових положень: здійснення заходів по підвищенню стійкості роботи об’єкта має бути завчасним; всі заходи по підвищенню стійкості роботи об’єкта повинні проводитись з урахуванням вимог нормативних документів; до здійснюваних заходів по підвищенню стійкості роботи ОГД має застосовуватись комплексний і плановий підхід. Основними напрямками підвищення стійкості роботи ОГД є: забезпечення захисту

робітників та службовців, членів їх сімей; раціональне розташування виробничих фондів ОГД; підготовка ОГД до роботи у надзвичайних умовах; підготовка ОГД до проведення відновлювальних робіт; підготовка системи управління ОГД до роботи у надзвичайних умовах.

Оскільки в сучасних умовах значно зросла імовірність виникнення аварій (катастроф) на небезпечних об’єктах, підвищуються вимоги до стійкості об’єктів. Крім того стійкість роботи об’єктів, які збудовані без врахування вимог ЦО, з часом стає незадовільною. Для підвищення стійкості таких об’єктів періодично проводяться дослідження по оцінці їх стійкості. Дослідження стійкості роботи ОГД ведеться в три етапи: І етап – підготовка до проведення дослідження (наказ начальника, календарний план дослідження, утворення груп (головного механіка, головного енергетика, штабної, головного інженера та ін.) та їх підготовка); ІІ етап – проведення досліджень по оцінці стійкості роботи елементів ОГД і ОГД в цілому (перераховані групи проводять оцінку стійкості роботи відповідних елементів об’єкта і готують звітні матеріали); ІІІ етап – розробка заходів по підвищенню стійкості роботи ОГД (узагальнення результатів дослідження, розробка заходів по підвищенню стійкості роботи ОГД та плану їх реалізації). Організація досліджень по оцінці стійкості роботи ОГД покладається на начальника ЦО. Найбільш ефективним способом забезпечення стійкості роботи ОГД є врахування вимог по їх стійкості ще до початку їх будівництва, тобто на стадії їх проектування. Основним документом, визначаючим стійкість роботи ОГД є «Норми проектування інженерно-технічних заходів ЦО». Вимоги цього документу реалізуються: при розробці нових будинків, споруд підприємств, систем та об’єктів електро-, газо-, водопостачання, зв’язку, транспорту, захисних споруд та ін.; при реконструкції міст, ОГД, комунально-енергетичних мереж та ін., які збудовані без урахування цих вимог.

Світлове випромінювання ядерного вибуху – це потік променистої енергії, який включає ультрафіолетові, інфрачервоні й видимі промені. Джерелом світлового випромінювання є світна сфера, яка складається з повітря і розжарених продуктів вибуху. Зі збільшенням світної сфери (при повітряному вибуху), температура на її поверхні знижується. Коли така куля досягає максимальних розмірів (діаметром понад 200 м), температура на її поверхні дорівнює 8000 – 10000 °С (температура на поверхні Сонця приблизно 6000 °С).

Залежно від потужності ядерного вибуху світлове випромінювання може тривати від кількох секунд до десятків секунд. При ядерному вибуху потужністю 20 кт світлове випромінювання триває 3 с, термоядерному в 1 Мт – 10с, а потужністю 10 Мт – до 23с.

Уражаюча дія світлового випромінювання визначається світловим імпульсом.

Світловий імпульс — це кількість світлової енергії, яка припадає на 1м2 (або на 1см2) освітленої поверхні, розміщеної перпендикулярно поширенню випромінювань протягом всього часу існування світлового потоку ядерного вибуху. Світловий імпульс у системі СІ вимірюється в джоулях на квадратний метр (Дж/м2), несистемна одиниця вимірювання світлового імпульсу кал/см2,1 кал = 4,1868 Дж. Величина світлового імпульсу залежить від потужності та виду ядерного вибуху, відстані освітлювальної поверхні до місця вибуху і атмосферних умов.

Шкідлива дія світлового випромінювання і для органів зору. Від світлового спалаху виникає тимчасове засліплення, причиною якого є руйнування зорового пурпуру сітчастої оболонки. Тривалість засліплення вдень до 5 хв, вночі може бути значно більшою. Опіки рогівки і повік виникають на таких відстанях, як і опіки шкіри. Опіки очного дна виникають, якщо очі були звернені на спалах вибуху. Ураження може бути на великих відстанях від вибуху, під час вибуху потужністю 20 кт, прозорому повітрі

вдень ураження настають на відстані до 60 км, при потужності 1 Мт – до 500км.

Якщо під час спалаху ядерного вибуху очі закриті, ураження не відбувається.

Такі ж ураження очей світлового випромінювання і у тварин.

За тяжкістю опіки у тварин поділяються на чотири ступеня.

Опіки першого ступеня виникають при світловому імпульсі 80— 240 кДж/м2, вони характеризуються почервонінням, невеликою припухлістю, болючістю шкіри, на обпечених ділянках з'являється серозне випотівання, яке швидко засихає і утворюється темно-коричневі кірочки.

Опіки другого ступеня з'являються при світловому імпульсі 240 – 480 кДж/м2, вони характеризуються місцевим підвищенням температури, болючістю уражених місць, пригніченим станом тварини.

Опіки третього ступеня виникають при світловому імпульсі 480 – 800 кДж/м2. При таких опіках з'являється омертвіння шкіри і можливе ураження більш глибоких тканин. Навколо омертвілої ділянки шкіра дуже припухає і болюча, спочатку виділяється серозне випотівання, пізніше, з розвитком інфекції, – гнійний ексудат.

Четвертий ступінь опіків виникає при світловому імпульсі 800 – 1000 кДж/м2і більше. Відкриті ділянки тіла обвуглюються.

Вплив світлового випромінювання на будівлі, споруди, рослини, лісові насадження. Світлове випромінювання залежно від інтенсивності світлового потоку і властивостей матеріалів викликає обвуглювання, оплавлення і спалахування, що веде до пожеж у населених пунктах і лісах, на хлібних масивах, скиртах сіна і соломи.

У результаті дії світлового випромінювання і ударної хвилі можуть виникати окремі, масові, суцільні пожежі та вогняні шторми.

Таким чином, світлове випромінювання – це небезпечний уражаючий фактор ядерного вибуху з великим радіусом дії, який може бути причиною

великих пожеж населених пунктів, лісових масивів і полів, масового ураження людей і тварин.

6.3 Висновки до шостого розділу

В розділі “Безпека в надзвичайних ситуаціях” розглянуто питання факторів, що впливають на функціональний стан користувачів комп’ютерів та оцінку стійкості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху.

7 ЕКОЛОГІЯ

7.1 Використання в Україні альтернативних джерел енергії

За нинішніх темпів використання нафти та газу, цих ресурсів людству вистачить на 50 років. У зв'язку з цим країни ЄС активно стимулюють запровадження альтернативних джерел енергії – до 2020 року їх частка в структурі виробництва електроенергії має скласти до 20%, а у 2030-му – вже 50%. Плани України значно скромніші: відповідно до Енергетичної стратегії на період до 2035 року, частка відновлюваних джерел у генерації електроенергії у 2020 році має складати 7%, а в 2025 – понад 13%.

Встановлена потужність сонячних електростанцій (СЕС) в Україні у 2017 році склала 742 МВт, що на 211 МВт більше, ніж попереднього року. Завдяки великій кількості сонячних днів і помірній температурі повітря, встановлені на території України сонячні станції працюють максимально ефективно. Розвиток альтернативної енергетики стимулює також високий зелений тариф – для промислових СЕС, побудованих у 2017-2019 роках, він становить 15 євроцентів; для СЕС цивільного зразка – 18 євроцентів. Завдяки цьому та відносній доступності СЕС їхній приблизний термін окупності в Україні становить 5-8 років.

Відновлюваними джерелами енергії є сонячна, фотоелектрична та геотермальна енергії, тверда біомаса, біогаз, рідке біопаливо, гідроелектростанції, а також енергії припливів, хвиль океану, вітру тощо. Тож детальніше охарактеризуємо основні альтернативні джерела енергії, вельми перспективні для України.

Серед різних видів альтернативних джерел енергії в Україні біопаливо перебуває на провідних ролях. Сьогодні біомасу як паливо використовують в обсязі лише близько 1 млн т умовного палива, тому значну кількість біомаси, придатної для виробництва енергії, знищують або вивозять на звалища.

Україна належить до країн із високим біоенергетичним потенціалом та темпами зростання біоенергетики. Згідно з офіційними даними, сектор біоенергетики у нашій країні щороку стабільно зростає. Свідченням тому є заміщення біопаливом близько 3 млрд м3 природного газу у 2014 році. Сумарні ресурси основних видів біомаси, придатної для енергетичного використання, за сучасних обсягів господарської діяльності в Україні становлять близько 20 млн т умовного палива на рік.

Загальна кількість встановлених котлів, які працюють на біомасі у муніципальному секторі України (централізоване теплопостачання і бюджетна сфера), зросла з 561 у 2012 р. до 1787 у 2016 р., а встановлена потужність із 285 до 1134 МВт відповідно. Середньорічний темп зростання ринку котлів на біомасі у муніципальному секторі України становить близько 50%.

Біомаса – це не лише рослинна органічна речовина (зернові культури, кукурудза, соняшник, відходи деревини), але й гній, газ звалищ. При цьому установки анаеробної переробки біомаси з отримання біогазу, тобто біогазові, виконують також роль очисних споруд, бо переробляють органічні відходи у нейтральні мінеральні продукти. Якщо установки для використання вітрової чи сонячної енергії є пасивно чистими, то біогазові – активно чистими, оскільки зменшують екологічну небезпеку тих продуктів, які використовують у якості джерела енергії. Наприклад, технологія метанового зброджування гною дає змогу отримувати біогаз і запобігає бактеріальному, хімічному забрудненню ґрунту, води, повітря, до якого призводять процеси, що відбуваються у накопичувачах гною. Водночас виробляють високоякісні добрива, білково-вітамінні кормові добавки, тож ця технологія практично є безвідходною.

Пріоритетами розвитку біоенергетики є створення котелень для спалювання відходів деревини та соломоспалювальних, електростанцій із використанням біогазу звалищ, дооснащення існуючих теплових

електричних станцій для спалювання побутових та промислових органічних відходів.

Перевагою на користь біопалива є можливість використання відходів виробництв та побічної продукції рослинництва. Недоліків використання біопалива фактично – немає.

За висновками науковців, найголовнішим джерелом енергії є Сонце. Приблизно 30% сонячної енергії, досягаючи Землі, відбивається назад у космос, 47% – витрачається на нагрівання земної поверхні, 22% – на кругообіг води у природі, 0,1% – на утворення вітру, хвиль, океанічних течій і лише 0,03% поглинається під час фотосинтезу. Щорічно земна поверхня одержує від Сонця енергію у кількості 31 024 Дж. Якщо порівняти цю величину з оцінками енергії, що міститься у розвіданих запасах енергоємних корисних копалин, то стане зрозуміло, що за один тиждень Земля отримує від Сонця таку кількість енергії, яка більше ніж удвічі перевищує всі відомі запаси енергії на Землі.

Сьогодні для перетворення сонячного випромінювання в електричну енергію існує два способи: використання сонячної енергії як джерело тепла для вироблення електроенергії традиційними способами (наприклад за допомогою турбогенераторів), або ж безпосередньо перетворювати її в електричний струм за допомогою сонячних елементів. Сонячну енергію використовують також після її концентрації за допомогою дзеркал – для плавлення речовин, дистиляції води, нагрівання, опалювання тощо.

Перевагами сонячної енергетики є загальнодоступність і невичерпність джерела енергії; теоретично – повна безпека для навколишнього середовища (проте наразі у виробництві фотоелементів і в них самих використовують шкідливі речовини).

До недоліків сонячної енергетики слід віднести:

– залежність потужності сонячної електростанції від часу доби, пори року і погодних умов;

– потік сонячної енергії на поверхні землі сильно залежить від широти й клімату. У різних місцевостях середня кількість сонячних днів у році може дуже сильно різнитися;

– через відносно невелику величину постійної сонячної енергії для сонячної енергетики потрібне використання великих площ землі під електростанції, але фотоелектричні елементи на великих сонячних електростанціях встановлюють на висоті 1,8 – 2,5 м, що дає змогу використовувати землі під електростанцією для сільськогосподарських потреб, наприклад для випасання худоби;

– відносно висока ціна сонячних фотоелементів;

– попри екологічну чистоту отримуваної енергії, самі фотоелементи містять отруйні речовини, наприклад свинець, кадмій, галій, миш'як тощо, а їхнє виробництво споживає масу інших небезпечних речовин.

Гідроенергетика є технологічно освоєним способом виробництва електроенергії, що має досить гарантований поновлюваний енергоресурс та найменшу собівартість виробництва електроенергії серед традиційних паливних і більшості нетрадиційних технологій її виробництва.

В Україні потужність гідроелектростанцій становить лише 8,8% генеруючих енергоджерел, і може бути підвищена у 2 – 3 рази. Для України реальним є забезпечення розвитку гідроенергетики шляхом спорудження гідроелектростанцій потужністю 20 – 50 МВт та малих гідроелектростанцій на існуючих водоймищах, магістральних каналах, об'єктах водозабезпечення та водовідведення, а також відновлення та реконструкція об'єктів малої гідроенергетики, що виконують функцію із захисту прилеглих територій від повеней.

Переваги гідроелектростанцій: постійно поновлюваний природою запас енергії, простота експлуатації, безпека щодо забруднення навколишнього середовища.

Головним недоліком гідроенергетики є руйнування природного ландшафту та затоплення великих площ родючих земель. Зокрема, на головній водній артерії України – Дніпрі – водосховищами затоплено величезні площі українських чорноземів, які вимірюються тисячами квадратних кілометрів.

Вітрова енергетика – це галузь відновлюваної енергетики, що спеціалізується на використанні кінетичної енергії вітру. Нині силу вітру застосовують для видобутку електроенергії. Хоча ціна 1 кВт год, видобутої з енергії вітру, порівняно невисока, але всі проекти з будівництва нових вітряків зазвичай дуже повільно окуповуються.

Перевагами вітрової енергетика є екологічна чистота. Вона не забруднює атмосферу, не споживає палива і не спричинює теплового забруднення довкілля.

Недоліками вітрових електростанцій є те, що вони створюють шум високої частоти, тому потребують великих земельних площ для свого розміщення, а також створюють незручності мешканцям населеним пунктам, які розташовані поруч. Є ще один вид впливу вітрової енергетики: генератори великих вітродвигунів обертаються зі швидкістю близько 30 об./с і перешкоджають міграції комах.

Геотермальна енергія (природне тепло Землі), акумульована в перших десятьох кілометрах земної кори, за оцінкою вчених, досягає 137 трлн т умовного палива, що вдесятеро перевищує геологічні ресурси всіх видів палива разом узятих. З усіх видів геотермальної енергії найефективнішими є гідрогеотермальні ресурси – термальні води та пароводяні суміші.

Перевагою геотермальної енергії є те, що температура теплоносія значно менша за температуру під час спалювання палива і найкращий спосіб використання геотермальної енергії – комбінований (видобуток електроенергії та обігрів).

До недоліків слід віднести низьку термодинамічну якість, використання тепла неподалік місця його видобування, а також те, що вартість розробки свердловин зростає зі збільшенням глибини.

7.2 Методика дослідження джерел забруднення промислових підприємств

Джерело забруднення атмосфери – це обширне поняття, яке можна широко інтерпретувати, особливо внаслідок діяльності людини, а саме:

– конкретна точка, в якій здійснюється викид шкідливих речовин у повітря (наприклад, димова труба або повітряний вихлоп), у тому значенні, що термін "джерело" застосовується для визначення кількості та типів забруднюючих речовин, для оцінки регіональних технічних проблем, таких як поширення забруднення і висота труби;

– технологічний підхід, тобто врахування технологічного процесу, обладнання (бойлери, печі, коксові батареї, преси, лаконаливні машини, пульверизаційні кабіни, автоматизовані лінії тощо), для яких ця концепція застосовується при встановленні меж викидів, а також оцінці рівня технічних засобів тощо;

– регіональний підхід – ряд джерел у конкретному регіоні, що належать до категорій 1) і 2): контрольовані однією організацією, наприклад, хімічною, металургійною або цементною корпорацією, – ця концепція застосовується для диференціації джерел за величиною, для комплексної оцінки їх впливу на навколишнє середовище тощо.

Оскільки класифікація джерел на технологічні та регіональні блоки є надзвичайно складною, доцільно застосовувати концепцію джерела як технологічного блоку.

На металургійних підприємствах, які є важливим джерелом забруднення атмосфери, проводяться численні операції на стадіях

агломерації, в доменних печах, в електродугових печах, кисневих конверторах, в ливарних, коксових та інших виробничих об'єктах, які роблять свій внесок у забруднення повітря. Цементні виробництва потребують близько 20 технологічних процесів (розмелювання, висушування, подрібнення, нагрівання в печах, охолодження в баштах, транспортування на стрічкових конвеєрах, транспортування готового продукту тощо), що супроводжуються забрудненням повітря, причому кожен з них має особливості і створює власні технічні проблеми. Найбільш складними технологічними блоками є хімічні підприємства. На одному заводі ряд виробничих процесів може спричинити викиди різних забруднюючих речовин, включно з газоподібними (наприклад, при виробництві азотної, сірчаної кислот, віскози та добрив, а також теплової енергії в котельнях).

Численні дослідження вчених-екологів засвідчують, що зі всієї кількості забруднюючих речовин, які викидаються в атмосферне повітря, близько 90 % становлять газоподібні речовини і близько 10 % – тверді та рідкі частинки.

В атмосферу всього потрапляє близько 3 х 10° т газоподібних, рідких і твердих забруднювальних речовин. Зараз на частку людської діяльності припадає близько 10 % від цієї кількості. З інтенсивним розвитком промисловості кількість шкідливих викидів в атмосферу може збільшитися в декілька разів.

В індустріально розвинених країнах, таких як США, Англія, Німеччина, Японія та ін., кількість викидів в атмосферу забруднюючих речовин у цей час становить від 350 до 1000 кг за рік на одну особу. В 2010 році річні викиди шкідливих речовин в атмосферу, за прогнозами вчених, можуть сягнути приблизно 10° т.

Дамо характеристику викидам забруднюючих речовин, які відносять лише до антропогенних джерел, зокрема, на промислових підприємствах.

Викиди шкідливих речовин в атмосферу можна поділити на чотири групи: тверді, рідкі, теплові та парогазоподібні.

Причини утворення твердих речовин (виробничий пил) залежать від типу виробничого процесу та його характеру:

– механічне оброблення різних речовин (буріння, розрівнювання, заповнення, подрібнення, розмелювання, полірування тощо);

– транспортування сипких матеріалів (навантажувально-розвантажувальні процеси, просіювання, змішування тощо).

Одним із значних джерел викидів твердих речовин в атмосферу є металургійна промисловість, зокрема виробництва сирого чавуну (агломерація і доменні печі), сталі (кисневі конвертори та тандем-печі або двополюсні печі), феросплавів, ливарні дільниці та вагранки, коксові установки або генератори.

Основним небезпечним виділенням з доменних печей є колошниковий газ і доменний шлак, в яких є значна кількість пилу. Гранулометричний склад і концентрація та хімічний склад пилу в доменних газах суттєво відрізняються й залежать від фізичних і хімічних властивостей застосованої сировини. Кількість пилу, що утворюється в доменних печах, становить від 20 до 300 кг/т сирого чавуну, або від 2 до 30 % його виробництва. Концентрація пилу змінюється від 10 до 20 мг/м3. Хімічний склад пилу в процесі агломерації: 50 % заліза, по 10 % оксидів кремнію, кальцію та алюмінію, приблизно по 2 % вуглецю, сірки та оксиду магнію. Найбільшим джерелом виділення пилу на металургійних підприємствах є електродугові печі. З джерел літератури відомо, що на 1 т виробленої сталі виділяється 5 – 9 кг пилу.

Виділення твердих і рідких забруднень переважно базується за аналогічними принципами. їх зазвичай об'єднують у групу забруднень у вигляді “частинок”.

Рідкі забруднення (туман, краплі) утворюються: а) при конденсації випарів; б) при розпилюванні або розтіканні рідин; в) у результаті хімічних або фотохімічних реакцій.

Пари можуть конденсуватися внаслідок охолодження в суміші з повітрям або іншим неконденсованим газом. Залежно від точки плавлення конденсованих речовин утворюються рідкі або інколи тверді частинки. Рідина знаходиться в рівновазі з парою при певній температурі й тиску. Якщо парціальний тиск пари в газі перевищує зрівноважуючий парціальний тиск насиченої пари при однаковій температурі, то вважають, що пара перенасичена. При досягненні критичного ступеня перенасичення починається конденсація. Пари речовин в газах конденсуються в основному на дрібнодисперсних пилових частинках унаслідок дії іонів, що знаходяться в атмосфері.

Теплові викиди трапляються під час спалювання, обпалювання, сушіння, плавлення, конденсування, карбонізації, газифікації, дистиляції тощо.

7.3 Висновки до сьомого розділу

В даному розділі розглянуто питання використання в Україні альтернативних джерел енергії та методику дослідження забруднення промислових підприємств.

ВИСНОВКИ

На основі проведеного аналізу маршрутизації в автономній системі запропоновано методи маршрутизації з підвищеними властивостями надійності.

В результаті проведеного дослідження отримано наступні висновки:

– проведено аналіз наукових публікацій, науково-дослідних робіт щодо маршрутизації в автономній системі, що дало змогу організувати стабільну роботу мережі та підвищує стійкість проти мережевих загроз;

– описано вимоги до розроблюваної маршрутизації, що повинна функціонувати в межах автономної системи, а також проаналізовано ризики пов’язані з її порушенням. Здійснено аналіз можливостей застосування статичної маршрутизації для організації обміну даними. Детально визначено ситуації при яких відповідні протоколи, які динамічно визначають маршрути повинні бути застосовані;

– проаналізовано роль протоколів резервування ресурсів для забезпечення постійного та надійного міжмережевого з’єднання. ;

– на основі проведених досліджень запропоновано модель віртуалізації маршрутизації в автономній системі через резервування мережевих ресурсів з врахуванням потоків інформації та аналізом вимог до роботи. На основі запропонованої моделі визначено два варіанти віртуалізації, що дає змогу вирішувати поставлені завдання з ефективним розподілом ресурсів.

В четвертому розділі дипломної роботи розглянуто питання системи моніторингу факторів живучості мережі.

В розділі «Обгрунтування економічної ефективності» було розраховано основні техніко-економічні показники від впровадження маршрутизації в межах автономної системи. Розраховане значення економічної ефективності

становить 0,56, що є прийнятним значенням. Так само нормальним є термін окупності. Для даної мережі він становить 1,8 років.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання особливості стандарту OHSAS 18001 щодо процедур для ідентифікації небезпек та оцінки ризиків, а також особливості методології самого процесу ідентифікації; організації робочого місця працівника у сфері IT: мікроклімат та вентиляція; факторів, що впливають на функціональний стан користувачів комп'ютерів та оцінку стійкості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху.

В розділі «Екологія» розглянуто питання використання в Україні альтернативних джерел енергії та методику дослідження забруднення промислових підприємств.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Клименко О.Ф. та інші “Інформатика та комп’ютерна техніка” Навчальний посібник / О. Клименко – К: КНЕУ, 2002.

2. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

3. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

4. Cisco Systems Руководство по технологиям объединенных сетей / Cisco Systems - 3-е издание. СПб: “Вильямс”, 2002. – 1040 с.

5. Дебра Литтлджон Шиндер Основы компьютерных сетей / Дебра Литтлджон Шиндер - СПб: "Вильямс", 2002. – 656 с.

6. Коротыгин С. Стандарт IEEE 802.11 и его расширения / С. Коротыгин, А. Нежуренко - Сети и телекоммуникации, вып. 6(25), 2002 г.

7. Марк А. Спортак Компьютерные сети. Книга 1. High-Perfomance Networking. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

8. Марк А. Спортак Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

9. Software-Defined Networking: The New Norm for Networks [Електронний ресурс] / ONF. – 2012. // – Режим доступу: https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdnnewnorm.pdf (24.11.2018 р.).

10. Олизарович Е. В. Метод автоматизации построения программно- конфигурируемых сетей / Е. В. Олизарович, А. И. Бражук // Вестник Гродзенского государственного университета им. Я. Купалы. – 2013. – №3(159) – С. 128-134.

11. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

12. Смелянский Р. В. Программно-конфигурируемые сети [Електронний ресурс] / Р. В. Смелянский // Открытые системы. – 2012. – № 9. – Режим доступу: http://www.osp.ru/os/2012/09/13032491 (24.11.2018 р.).

13. OpenFlow Switch Specification Version 1.2 [Електронний ресурс] / ONF. – 2012. // – Режим доступу: https://www.opennetworking.org/images/stories// downloads/ specification/ openflow-spec-vl .2.pdf. (17.01.2019 р.).

14. Nadeau T. SDN: Software Defined Networks / T. Nadeau, K. Gray // O'Reilly. – 2013. – №3. – P. 70-95. 172 10. POX Wiki/POX.2014.URL [Електронний ресурс] // – Режим доступу: https://openflow.stanford.edu/display/ONL/POX+Wiki (10.11.2018 р.).

15. Орлов Є. В. Упровадження адаптивного управління програмно- конфігурованою мережею (SDN) / Є. В. Орлов, І. Е. Похабова // Зв'язок. – 2014. – №2(108). – С. 11-16.

16. Software-Defined Networking (SDN) Definition [Електронний ресурс] / ONF. – 2013. // – Режим доступу: https://www.open-networking.org/sdnresources/sdn-definition (07.03.2019 р.).

17. Framework of Telecom SDN (Software-Defined Networking) // ITU-T Draft Recommendation Y.FNsdn. – February 2013.

18. Egawa T. SDN standardization Landscape from ITU-T Study Group 13 // ITU Workshop on SDN Geneva, Switzerland. – June 2013.

19. McKeown N. OpenFlow Enabling Innovation in Campus Networks / N. McKeown, T. Anderson // SIGCOMM. – 2008. – Vol. 38. – P. 69-74.

20. Стеклов В. К. Проектування телекомунікаційних мереж / В. К. Стеклов, Л. Н. Беркман. ; під ред. В. К. Стеклова – Київ : Техніка, 2002. – 792 с.

21. Стеклов В. К. Сучасні системи управління в телекомунікація / В. К. Стеклов, Б. Я. Костік, Л. Н. Беркман ; під ред. В. К. Стеклова – Київ : Техніка, 2005. – 395 с.

22. Холл Э. Приоритизация трафика в сетях IP / Э. Холл // Сети и системы связи. – 1988. – №11 (33). – С. 34-39

23. Орлов Є. В. Програмно-конфігуровані мережі (SDN): архітектура, міжнародна стандартизація / Є. В. Орлов // Наукові записки УНДІЗ. – 2014. – №4(32) – С. 85-91.

24. Семѐнов Ю. А. Телекоммуникационные технологии [Електронний ресурс] / Ю. А. Семѐнов // – Режим доступу: http://citforum.ck.ua/nets/semenov/4/ /44/ip_441.shtml (15.02.2019 р.).

25. Толубко В. Б. Багатокритеріальна оптимізація параметрів програмно- конфігурованих мереж (SDN) / В. Б. Толубко, Л. Н. Беркман, Л. О. Комарова, Є. В. Орлов // Телекомунікаційні та інформаційні технології. – 2014. – №4. – С. 5- 11.

26. Стеклов В. К. Моделювання пристроїв та систем зв’язку [Навчальний посібник] / В. К. Стеклов, В. В. Мірошніков, І. А. Кожин ; під ред. В. К. Стеклова. – Київ : ДП УНДІЗ, 2000. – 74 с.

27. Чаадаєв В. К. Информационные системы компаний связи / В. К. Чаадаев, И. В. Шеметова, И. В. Шибаева ; под. ред. В. К. Чаадаєва. – Москва : Эко-Трендз, 2004. – 256 с.

28. Толубко В. Б. Багатокритеріальна оптимізація параметрів програмно- конфігурованих мереж (SDN) / В. Б. Толубко, Л. Н. Беркман, Л. О. Комарова, Є. В. Орлов // Телекомунікаційні та інформаційні технології. – 2014. – №4. – С. 5- 11.

29. Xu Xiaofei Carrier SDN: Next-gen carrier Networking [Електронний ресурс] / Xiaofei Xu // Режим доступу: https://www.huawei.com/en/abouthuawei/publications/communicate/hw-259729.htm (27.03.2019 р.).

30. Шестопалов С. В. Інтелектуальна надбудова в NGN / С. В. Шестопалов, Є. В. Орлов // VI Міжнародний науково-технічний симпозіум ―Нові технології в телекомунікаціях‖ ДУІКТ-Карпати’2013, 21-25 січня 2013 р. Збірник тез. – К: ДУІКТ, 2013. – С.110-112.