

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(навчально-науковий інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Здобувача вищої освіти Дворядкіна Дмитра Івановича
(ПІБ)
академічної групи 123М-23-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою «Комп'ютерна інженерія»
(офіційна назва)

на тему «Обґрунтування структури та параметрів комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Кожевніков А.В.			
розділів:				
синтез системи	доц. Бешта Д.О.			
розроблення програмного забезпечення	ас. Панферова Я.В.			
Рецензент	проф. Логвін В.М.			
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ В.В. Гнатушенко
(підпис) (ініціали, прізвище)

« _____ » _____ 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра
(бакалавра, магістра)

здобувача вищої освіти Дворядкіна Д.І. академічної групи 123М-23-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія
за освітньою-професійною програмою «Комп'ютерна інженерія»
(офіційна назва)

на тему «Обґрунтування структури та параметрів комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування»,
затверджену наказом ректора НТУ «Дніпровська політехніка» від 17 жовтня 2024 р. №1388-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів практик, інших науково-технічних джерел сформулювати наукове завдання, конкретизувати предмет та мету досліджень	11.10.2024
Теоретичний	Обґрунтувати теоретичну базу структури та параметрів комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування	25.10.2024
Синтез системи	Розробка комп'ютерної системи ТОВ «Sollar» та моделювання її роботи на основі моделі мережі масового обслуговування	15.11.2024
Розроблення програмного забезпечення	Розробка програмного забезпечення моделі комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування	29.11.2024
Експериментальний розділ	Проведення і обробка результатів експериментів з моделювання комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування	06.12.2024

Завдання видано _____
(підпис керівника)

Дата видачі 06 вересня 2024 р.

Дата подання до екзаменаційної комісії _____

Прийнято до виконання _____
(підпис здобувача вищої освіти)

доц. Кожевніков А.В.
(ініціали, прізвище)

20.12.2024 р.

Дворядкін Д.І.
(ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка: 109 с., 44 рис., 6 табл., 1 дод., 22 джерел.

МЕРЕЖА, ТЕОРІЯ МАСОВОГО ОБСЛУГОВУВАННЯ, МЕРЕЖЕВИЙ ПРИСТРІЙ, ВУЗОЛ

Об'єкт дослідження: комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування.

Мета: Синтез комп'ютерної системи ТОВ «Sollar», визначення вузлів у мережі, які найбільше інформаційно перевантажені, визначення реальних умов експлуатації, параметрів і властивостей технічних мережеских пристроїв, при яких може виникнути значне зниження працездатності комп'ютерної системи ТОВ «Sollar». Розробка рекомендацій щодо модернізації комп'ютерної системи ТОВ «Sollar» з метою підвищення надійності і стійкості роботи в умовах значного інформаційного перевантаження.

Новизна роботи: використання моделі мережі комп'ютерної системи ТОВ «Sollar», розробленої з застосуванням математичного апарату теорії масового обслуговування, з метою виявлення «слабких місць» в мережі при значному вибуховому інформаційному перевантаженні, та у пошуку шляхів для її вдосконалення.

Практичний результат: Розроблена комп'ютерна система ТОВ «Sollar» є відкритою, що дозволяє проводити оперативну технічну та програмну її модернізацію. Виявлення недоліків і шляхів вдосконалення комп'ютерної системи ТОВ «Sollar» досягається за рахунок використання наукового підходу до вирішення поставлених завдань з застосуванням теорії масового обслуговування.

Прикладні наукові результати з розробки комп'ютерної системи ТОВ «Sollar» та моделювання її роботи показали її працездатність на багатьох режимах інформаційного навантаження, що гарантує надійне застосування комп'ютерної системи ТОВ «Sollar».

Результати перевірки роботи моделі комп'ютерної системи ТОВ «Sollar» представлені у вигляді таблиць, графіків, описані у пояснювальній записці, тексти програмного забезпечення моделі наведені і додатках.

ABSTRACT

Explanatory note: 109 pages, 44 figures, 6 tables, 1 addition, 22 sources.

NETWORK, MASS SERVICE THEORY, NETWORK DEVICE, NODE

Object of research: computer system of Sollar LLC based on the model of the mass service network.

Purpose: Synthesis of the computer system of Sollar LLC, identification of nodes in the network that are most informationally overloaded, determination of real operating conditions, parameters and properties of technical network devices, under which there may be a significant decrease in the performance of the computer system of Sollar LLC. Development of recommendations for the modernization of the computer system of Sollar LLC in order to increase the reliability and stability of work in conditions of significant information overload.

Novelty of the work: use of the network model of the computer system of Sollar LLC, developed using the mathematical apparatus of the theory of mass service, in order to identify "weak points" in the network with significant explosive information overload, and in search of ways to improve it.

Practical result: The developed computer system of Sollar LLC is open, which allows for its prompt technical and software modernization. Identification of shortcomings and ways to improve the computer system of Sollar LLC is achieved through the use of a scientific approach to solving the tasks with the application of the theory of mass service.

Applied scientific results on the development of the computer system of Sollar LLC and modeling of its operation showed its operability in many modes of information load, which guarantees the reliable use of the computer system of Sollar LLC.

The results of checking the operation of the model of the computer system of Sollar LLC are presented in the form of tables, graphs, described in the explanatory note, the texts of the model software are given in the appendices.

ЗМІСТ

Перелік умовних позначень, символів, скорочень та термінів	8
Вступ	10
1 Стан питання і завдання дослідження	14
1.1 Загальна інформація про IT-ринок	14
1.2 Галузь застосування комп'ютерної системи	16
1.3 IT - аутсорсинг	19
1.3.1 Загальна інформація	19
1.3.2 Види IT-аутсорсингу	20
1.4 Характеристика і структура об'єкта впровадження	22
1.4.2 Партнерство з ТОВ «Sollar»	27
1.4.3 Організаційна структура управління підприємства	29
1.4.4 Функціональні особливості комп'ютерної системи	30
1.4.5 Критичний аналіз комп'ютерної системи ТОВ «Sollar»	31
1.4 Завдання	33
2 Теоретична частина	34
2.1 Загальна інформація про моделювання КМ	34
2.2 Імітаційні дослідження КМ	36
2.2.1 Передачі інформації окремому користувачу	36
2.2.2 Системи дослідження методом моделювання та отримання результатів	37
2.2.3 Внутрішні вимірювальні інструменти	38
2.2.4 Аналітичні методи оцінювання діяльності	40
2.2.5 Надійність мережі	41
2.3 Імітаційна модель комп'ютерної системи ТОВ «Sollar»	42
2.4 Розрахунок пропускної здатності найбільшого сегмента КМ ТОВ «Sollar»	44
2.4 Висновки за розділом	48
3 Синтез системи	49
3.1 Обстеження об'єкту розробки	49
3.1.1 Програмно-визначені мережі	50

- 3.1.1 Введення50
- 3.1.2 Гібридна SDN архітектура53
- 3.1.3 Стратегія розгортання hSDN54
- 3.2 Острівна модельна пропозиції для КМ ТОВ «Sollar»61
- 3.3 Комплекс технічних засобів комп'ютерної системи64
 - 3.3.1 Технічні вимоги до КС64
 - 3.3.1.1 Вимоги до системи в цілому64
 - 3.3.1.1.1 Структура і функціонування системи64
 - 3.3.1.1.2 Чисельність і кваліфікація персоналу і режим роботи65
 - 3.3.1.1.3 Надійність і безпека65
 - 3.3.1.1.4 Експлуатація, технічне обслуговування, ремонт, збереження66
 - 3.3.1.1.5 Захист інформації66
 - 3.3.1.1.6 Патентна чистота67
 - 3.3.1.1.7 Стандартизація й уніфікація67
 - 3.3.2 Забезпечення67
 - 3.3.2.1 Інформаційне забезпечення67
 - 3.3.2.2 Технічне забезпечення68
 - 3.3.2.3 Організаційне забезпечення69
 - 3.3.2.4 Нормативно-технічна документація69
 - 3.3.3 Апаратні засоби КС ТОВ «Sollar»70
 - 3.3.3.1 Загальні відомості70
 - 3.3.3.2 Маршрутизатор C921-4P71
 - 3.3.3.3 маршрутизатора Cisco 89173
 - 3.3.3.4 Комутатора Catalyst 296074
 - 3.3.3.5 Компоненти КС ТОВ «Sollar»76
 - 3.3.3.5.1 Сервери76
 - 3.3.3.5.2 Мережеве обладнання78
- 3.4 Висновки за розділом78
- 4 Програмне забезпечення79
 - 4.1 Призначення й сфера застосування програми79

4.2	Параметри програми	81
4.2.1	Завдання на розробку	82
4.2.2	Операційне програмне забезпечення для робочого місця	82
4.2.3	Вхідні і вихідні дані	82
4.2.4	Склад програмних засобів	83
4.3	Опис програми	83
4.3.1	Загальні відомості	83
4.3.2	Послідовність розрахунку	84
4.3.3	Функціональне призначення	84
4.3.4	Опис логічної структури	84
4.3.4	Використовувані технічні засоби	85
4.3.5	Цикл роботи програми	85
4.3.6	Вхідні та вихідні дані	85
4.4	Висновок	86
5	Експериментальний розділ	87
5.1	Розробка математичної моделі мережі ТОВ «Sollar»	87
5.2	Розрахунок параметрів моделі мережі	90
5.2.1	Параметри роботи мережі без впливу шкідливого ПЗ	94
5.2.2	Параметри роботи мережі під впливом вірусних програм	98
5.3	Висновки по розділу	104
	Висновки	106
	Перелік посилань	108
	Додаток А	110

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

АРМ	– автоматизоване робоче місце;
ІТ	– інформаційні технології;
ІОД	– інформація обмеженого доступу;

КІСП – комп'ютерна інформаційна система підприємства;

КМ – корпоративна мережа;

КС – комп'ютерна система;

ЛМ – локальна мережа;

ЛОМ – локальна обчислювальна мережа;

ТОВ – товариство з обмеженою відповідальністю;

ПК – персональний комп'ютер;

ЦП – цифровий підпис.

ВСТУП

Комп'ютерні мережі, особливо Інтернет, являють собою складні системи з величезним соціальним впливом. Численні недоліки або навіть відмови реалізації були пов'язані з недостатнім імітаційним та аналітичним моделюванням, що застосовувалося для дослідження продуктивності таких систем. В літературі представлені деякі роботи в цій області на тлі огляду методів, що застосовуються в даний час. Також згадаються проблеми дослідження та оптимізації робастності без будь-яких проблем, пов'язаних з недостатньою продуктивністю системи, хоча наявне обладнання майже завжди буває застарілим [7].

Товариство з обмеженою відповідальністю «Solar» це ІТ сучасна компанія, яка активно розвивається. Послуги інформаційних технологій (ІТ) стали невід'ємною частиною будь-якого бізнес-ландшафту. Швидкий розвиток технологій призвів до фундаментальних змін у тому, як компанії працюють і конкурують. Від підтримки технологічної інфраструктури до посилення заходів безпеки, ІТ-послуги відіграють ключову роль у забезпеченні безперебійного функціонування та розвитку бізнесу.

Основні важливі напрямки ІТ-послуг:

1. Обслуговування технологічної інфраструктури: ІТ-послуги мають важливе значення для підтримки обладнання, програмного забезпечення, мереж та систем в актуальному та добре налаштованому стані. Це технічне обслуговування має вирішальне значення для забезпечення оптимальної продуктивності та надійності.

2. Бізнес-операції: ІТ-послуги забезпечують основу для безперебійних бізнес-операцій. Вони охоплюють обмін електронною поштою, зберігання даних, інструменти для спільної роботи та багато іншого, підвищуючи ефективність і продуктивність у всіх відділах.

3. Безпека даних: В епоху зростання кіберзагроз ІТ-послуги мають вирішальне значення для впровадження надійних заходів безпеки. Вони

захищають конфіденційні дані, захищають від витоків і забезпечують дотримання правил захисту даних.

4. Масштабованість і зростання: У міру того, як бізнес розширюється, змінюються і його ІТ-потреби. ІТ-послуги сприяють безшовному масштабуванню, адаптуючи технологічну інфраструктуру відповідно до зростання, гарантуючи, що системи можуть справлятися зі зростаючими вимогами.

5. Аварійне відновлення: ІТ-послуги включають планування аварійного відновлення, забезпечення регулярного резервного копіювання даних і стратегію швидкого відновлення роботи в разі технологічних збоїв, порушень або збоїв.

6. Інновації та конкурентні переваги: Залишатися в курсі технологічного прогресу життєво важливо для компаній, які прагнуть залишатися конкурентоспроможними. ІТ-послуги дозволяють компаніям впроваджувати нові інструменти та стратегії, які забезпечують чітку перевагу на ринку.

7. Економічна ефективність: Аутсорсинг ІТ-послуг часто може бути економічно вигіднішим, ніж утримання внутрішнього ІТ-відділу. Такий підхід скорочує витрати, пов'язані з пошуком, навчанням та утриманням ІТ-персоналу.

8. Відповідність і регулювання: Підприємства підпадають під галузеві правила. ІТ-послуги допомагають орієнтуватися в цих правилах, гарантуючи, що заходи конфіденційності та безпеки даних відповідають законодавчим вимогам.

Чек-лист для ІТ-потреб компаній:

1. Інвентаризація апаратного та програмного забезпечення: Документує все обладнання та програмне забезпечення, що використовується в організації.

2. Мережева інфраструктура: оцінка архітектури мережі, включаючи маршрутизатори, комутатори та бездротові точки доступу.

3. Заходи безпеки: Оцінює поточні протоколи безпеки, такі як брандмауери, антивірусне програмне забезпечення, шифрування та контроль доступу.

4. Резервне копіювання та відновлення даних: Пропонує стратегії резервного копіювання та відновлення даних, щоб мінімізувати втрату даних під час надзвичайних ситуацій.

5. Хмарні служби: визначає, чи відповідають хмарні рішення потребам організації, включаючи хмарні сховища та програми «програмне забезпечення як послуга» (SaaS).

6. IT-підтримка: Визначає рівень необхідної IT-підтримки, включаючи послуги служби підтримки та усунення несправностей.

7. Відповідність і нормативні вимоги: Враховує галузеві нормативні акти, які впливають на бізнес, і перевіряє, що IT-практики відповідають йому [1].

Об'єкт дослідження. Об'єктом дослідження є програмно-технічна реалізація комп'ютерної системи ТОВ «Sollar».

Предмет і методи дослідження. Предметом дослідження є структура комп'ютерної системи ТОВ «Sollar», інформаційні властивості цієї мережі, а також граничні межі технічних можливостей мережевого апаратного забезпечення. Для виконання завдань дослідження комп'ютерної системи мережі ТОВ «Sollar» використовуються методи теорії масового обслуговування, для чого розроблена математична модель комп'ютерної системи мережі ТОВ «Sollar» - як мережі за теорією масового обслуговування. Проведено доскональне дослідження властивостей комп'ютерної системи ТОВ «Sollar» з різними параметрами інформаційного середовища при застосуванні різних мережевих апаратних засобів.

Мета роботи і завдання дослідження. Удосконалення комп'ютерної системи мережі ТОВ «Sollar» на основі моделі мережі масового обслуговування.

Для удосконалення комп'ютерної системи ТОВ «Sollar» слід визначати закономірності, що мають найбільший вплив на інформаційне перевантаження комп'ютерної системи ТОВ «Sollar». Визначається ефект, який може бути отриманий при використанні виявлених закономірностей, а також обрати шляхи досягнення зниження інформаційного перевантаження комп'ютерної системи ТОВ «Sollar». Визначити основний практичний результат який буде досягнутий

при застосуванні моделі мережі масового обслуговування для зниження інформаційного перевантаження комп'ютерної системи ТОВ «Sollar».

Завдання дослідження: Виявити мережеві вузли мережі, які можуть найбільше постраждати від інформаційного перевантаження комп'ютерної системи ТОВ «Sollar». Визначити необхідні параметри для мережевих технічних пристроїв для реалізації поліпшеної комп'ютерної мережі. Розробити рекомендації щодо модернізації спроектованої комп'ютерної системи ТОВ «Sollar» для підвищення її стійкості до інформаційних перевантажень.

Ідея роботи. Полягає у виявленні найбільш завантажених вузлів комп'ютерної системи ТОВ «Sollar», які в разі інформаційного перевантаження мережі призводять до зниження продуктивності роботи всієї комп'ютерної системи ТОВ «Sollar». Розробка практичних рекомендацій щодо вирішення цієї проблеми.

Вирішення наукового завдання – виявлення недоліків і пошук шляхів вдосконалення комп'ютерної системи ТОВ «Sollar», які ґрунтуються на науковому підході використанням моделей мережі, які ґрунтуються на теорії масового обслуговування.

Новизна роботи – використання моделі мережі комп'ютерної системи ТОВ «Sollar», розробленої з застосуванням математичного апарату теорії масового обслуговування, з метою виявлення «слабких місць» в мережі при значному вибуховому інформаційному перевантаженні, та у пошуку шляхів для її вдосконалення.

Практичні результати - прикладні наукові розробки з моделювання комп'ютерної системи ТОВ «Sollar» показали їх ефективність на різних режимах їх застосування. Результати модулювання і перевірки працездатності комп'ютерної системи ТОВ «Sollar» представлені у вигляді графіків, таблиць, описуються і наводяться в пояснювальній записці і у відповідному додатку.

1 СТАН ПИТАННЯ І ЗАВДАННЯ ДОСЛІДЖЕННЯ

1.1 Загальна інформація про IT-ринок

Комплексний аналіз життєво важливої ролі компаній, що надають IT-послуги, в першу чергу спирається, на результати впровадженні сучасної цифрової економіки, зосереджуючись на їхніх функціях, перевагах та проблемах, з якими вони стикаються.

Літературні джерела пропонують дослідження, які починаються з огляду різних типів компаній, що надають IT-послуги, включаючи консалтингові фірми, аутсорсингові компанії та постачальників хмарних послуг. Кожен тип розглядається з точки зору його специфічного внеску в технологічні інновації та трансформацію бізнесу.

Такі відомі міжнародні компанії, як EPAM, Accenture, Intellias, SoftServe, GlobalLogic, Endava та Globant відзначені за їхню ключову роль у наданні спеціалізованих послуг, які дозволяють бізнесу використовувати передові технології, сприяти цифровій трансформації в різних галузях та розвитку нової розумної економіки.

Вплив IT-сервісних компаній на сучасну економіку відрізняється від традиційних консалтингових фірм («Велика четвірка» та «Велика трійка») та від сучасних сервісних компаній. Традиційні фірми все частіше виходять на цифровий і технологічний простори, часто співпрацюючи з постачальниками IT-послуг, щоб запропонувати комплексні рішення для цифрової трансформації. Приклади конкуренції та співпраці між цими суб'єктами ілюструють динаміку розвитку ринку консалтингу та IT-послуг.

Переваги співпраці з сервісними IT-компаніями гарантують економічну ефективність, доступ до спеціалізованих знань у таких галузях, як штучний інтелект, кібербезпека, хмарні обчислення та аналітика даних, що має вирішальне значення в процесі трансформації бізнесу та переходу до так званої розумної економіки, що приводять до значного зростання бізнесу та інновацій, демонструючи практичні переваги цих партнерства.

Компанії, що надають ІТ-послуги у сприянні цифровій трансформації в різних секторах, мають приклади успішних проектів цифрової трансформації та показують їх позитивні результати. Ці компанії відіграють важливу роль у розробці та впровадженні цифрових стратегій, модернізації ІТ-інфраструктури, прийнятті рішень на основі даних, покращенні клієнтського досвіду та підтримці гнучкої трансформації.

Проблеми, з якими стикаються компанії, що надають ІТ-послуги, включають залучення та утримання талантів, швидкий технологічний прогрес, загрози кібербезпеці та високі очікування клієнтів.

Конкурентний тиск з боку ринків, що розвиваються, і необхідність постійного вдосконалення та диференціації визначають майбутні тенденції розвитку ринку ІТ-послуг у сучасній економіці, яка має значну присутність цифрових технологій.

Впровадження практик agile та DevOps також виділяється як ключова тенденція, що сприяє ефективності та інноваціям у розробці програмного забезпечення (ПЗ) та ІТ-операціях, ще раз підтверджуючи важливість компаній з надання ІТ-послуг у розвитку сучасної економіки, наголошується на їх вирішальній ролі як стратегічних партнерів в інноваційній діяльності.

Майбутній потенціал ІТ-компаній, відзначає їх значний внесок у формування галузей та економік у всьому світі. Прогнозується, що розвиток ландшафту ІТ-послуг продовжуватиме стимулювати прогрес і дозволити компаніям досягати нових висот успіху, підкреслюючи незамінну роль компаній, що надають ІТ-послуги у сприянні сталому економічному розвитку [2].

Агресивне повномасштабне вторгнення росії у 2022 р. призупинило швидкий ріст експорту ІТ-послуг України.

Пік поквартальної динаміки експорту припав на першій чверті російського вторгнення у 4 кварталі 2021 року. Як видно з графіка поквартальної динаміки експорту на рис. 1.1, пік цього показника ІТ-активності припав на переддень російського вторгнення у 4 кварталі 2021 року, коли в Росію було імпортовано 2,1 млрд доларів США. До Росії було імпортовано 2,1 млрд доларів США.

Відтоді середня вартість експорту комп'ютерних послуг поступово знизилася до 1,7 млрд доларів США, а це означає, що рівень щоквартального падіння доходів від експорту ІТ сягнув приблизно -20%.



Рисунок 1.1 - Експорту ІТ-послуг

За перші 18 місяців після війни частка сектору в загальному експорті товарів і послуг України зросла з 8,8% до 13,4%, але ІТ-сектор все ще далекий від того, щоб вважатися рушійною силою збільшення експортного потенціалу, як це було у випадку з довоєнним оптимізмом [22].

1.2 Галузь застосування комп'ютерної системи

Комп'ютерні мережі використовувалися для швидкої передачі даних між багатьма комп'ютерами. Завдяки їм громадяни, уряди та суспільство в цілому можуть досліджувати наявну інформацію та ресурси та мати необмежений доступ до них, взаємодіяти та взаємодіяти з іншими людьми та швидко вести бізнес.

Соціально підключені комп'ютери в комп'ютерній мережі — це групи комп'ютерів, які використовують цю мережу для передачі ресурсів, а також інформації. Основне управління комп'ютерними мережами здійснюється для полегшення зв'язку, творці комп'ютерів діляться апаратним забезпеченням звідусіль, забезпечують віддалений доступ, а також працюють разом.

Комп'ютерні системи – це мережі в умах компаній, освітніх організацій та окремих людей, які розглядають цю технологію як спосіб спілкування та отримання ресурсів.

Комп'ютерна мережа має багато способів використання, зокрема:

Комунікація: через комп'ютерні мережі окремі особи та організації можуть співпрацювати за допомогою каналів зв'язку, які можуть включати електронну пошту, чат і відеоконференції.

Спільне використання ресурсів: ці сумки є благом для користувачів, оскільки вони надають можливість спільно використовувати принтер, сканер і файли, що допоможе покращити робочу діяльність і зменшити витрати.

Віддалений доступ: мережеві технології дозволяють отримати доступ до інформації та підтримку з будь-якої точки земної кулі. Тому користувачі можуть працювати з більшою свободою та комфортом.

Співпраця: Мережі працюють над тим, щоб зробити співпрацю ефективнішою, надаючи можливості для спільної роботи над чимось, обміну ідеями та критики якомога ширше.

Електронна комерція: онлайн-продажі та обробка платежів покращуються завдяки комп'ютерним мережам, які дозволяють підприємствам продавати товари онлайн і здійснювати безпечні платежі.

Освіта: завдяки використанню в освітньому середовищі вони служать основою для дистанційного навчання, доступу до ресурсів вищої освіти та надають можливості для співпраці між студентами та викладачами.

Комп'ютерні мережі мають багато застосувань, зокрема:

- покращена комунікація та спільна робота;
- спільне використання ресурсів може зіграти певну роль у зниженні витрат;
- управління якістю та безпекою даних;
- вищі переваги автоматизації та можливості віддаленого доступу;
- підвищення продуктивності та ефективності;
- недоліки комп'ютерних мереж;

Ось недоліки використання комп'ютерної мережі:

- ризику злому даних та ймовірність витоку даних;
- проблема технічних деталей і оперативного усунення несправностей.

Зростає ймовірність зараження вірусами та шкідливим програмним забезпеченням. Це може призвести до зниження конфіденційності.

Комп'ютерні мережеві технології зараз є невід'ємною частиною нашого повсякденного життя, а технології передачі даних використовуються для забезпечення більш ефективної комунікації з точки зору спільного використання ресурсів, віддаленого доступу, співпраці, електронної комерції, освіти та розваг. Не можна заперечувати, що технологічний прогрес зростає безпрецедентними темпами. В результаті мережі, які з'єднують комп'ютери, зазнають подальших розробок і вдосконалення, створюючи нові і навіть швидші способи взаємодії один з одним і збору даних і документів з будь-якої точки планет [3].

У кваліфікаційній роботі магістра розглядається комп'ютерна система для товариства з обмеженою відповідальністю «Solar», основним видом діяльності якої є надання сучасних ІТ послуг на території держави Україна та за кордоном.

Розроблення ПЗ, на замовлення є пріоритетним направленням функціонування підприємства «Solar». Розробляється ПЗ для сучасних мобільних операційних систем (ОС), таких як: android, Symbian's, iOS, bada та інші. Також підприємство «Solar» займається розробкою, на замовлення ПЗ для персональних комп'ютерів на базі ОС для сімейств Windows та Linux, та розробкою програмного забезпечення для спеціалізованих мікропроцесорів та мікроконтролерів.

ІТ-аутсорсинг представляє собою процес передачі клієнтом поточних функцій обслуговування ІТ-систем для зовнішньої компанії.

Товариство з обмеженою відповідальністю «Solar» займається ІТ-аутсорсингом.

1.3 ІТ - аутсорсинг

1.3.1 Загальна інформація

ІТ-аутсорсинг – це підкатегорія аутсорсингу, яка фокусується виключно на передачі ІТ-функцій сторонньому постачальнику. Але ІТ-аутсорсинг існує в самих різних формах і охоплює широкий спектр ІТ-функцій. Не всі ІТ-аутсорсингові компанії пропонують або спеціалізуються на кожній моделі та охоплюють однакові функції та масштаб проекту.

Різні організації мають різні потреби в ІТ-аутсорсингу.

Велика кількість організацій покладається на постачальників ІТ-аутсорсингу для виконання технічних функцій, тому стратегічно або бізнес-має сенс доручити співпрацю сторонньому спеціалісту. Компанії від великих підприємств до малого та середнього бізнесу часто віддають ІТ-роботу на аутсорсинг з різних причин, зокрема:

Вартість – багато постачальників ІТ-аутсорсингу пропонують спеціалістів, які працюють віддалено з країн з нижчою зарплатою.

Бухгалтерський баланс – договори на ІТ-аутсорсинг враховуються як змінні, а не постійні витрати, на відміну від заробітної плати працівників.

Гнучкість – аутсорсингові ІТ-ресурси можна масштабувати вгору та вниз без найму та звільнення.

Труднощі з підбором персоналу – відсутність внутрішньої експертизи для ефективного підбору персоналу на технічні посади або недостатня кількість кваліфікованих місцевих кандидатів у межах бюджету.

Не тільки компанії користуються ІТ-аутсорсингом. Інші організації, від громадських організацій до місцевих та національних органів влади, спортивні клуби, заходи тощо, можуть мати ІТ-функції, і часто, з тих самих причин, має сенс передати їх на аутсорсинг.

Але потреби місцевої школи або невеликого муніципалітету в аутсорсингу – це не те ж саме, що стартап або мобільна компанія середнього розміру. Компанії корпоративного рівня, такі як банки, компанії споживчих товарів і

виробники, знову будуть мати зовсім інший профіль з більш масштабними проектами і вимогами своїх сторонніх постачальників.

Існують різні типи ІТ-аутсорсингу, і різні типи постачальників ІТ-аутсорсингу покривають різноманітні потреби. Компанія, яка може запропонувати найбільш підходящий сервіс одному типу клієнтів, часто не підійде іншому.

Якщо компанія або організація вимагає, щоб сторонні постачальники були сертифіковані ISO та мали мінімальний рівень плинності кадрів або кількості співробітників, ви, ймовірно, будете обмежені роботою з більшими ІТ-аутсорсинговими компаніями. Можливо, вам доведеться розглянути GDPR або інші правила щодо персональних даних, які означають, що певні ІТ-функції мають бути розташовані в межах ЄС або іншої юрисдикції.

Перш ніж звузити список ІТ-аутсорсингових компаній, з якими можна поговорити про потреби вашої організації, ви повинні спочатку визначити тип ІТ-аутсорсингу, який вам потрібен. Отже, давайте детально розглянемо різні види ІТ-аутсорсингу, які існують на ринку. Це допоможе вам визначити потрібний вам тип як відправну точку для процесу укладання контракту з правильним постачальником.

1.3.2 Види ІТ-аутсорсингу

Спектр доступних послуг ІТ-аутсорсингу можна розбити за типами по-різному. Найбільш очевидними є:

- за ІТ-функцією;
- за моделлю співпраці;
- за моделлю залучення;
- за масштабами;
- за географією;
- ІТ-функції, які можна передати на аутсорсинг.

ІТ-функції, які часто віддають на аутсорсинг, включають:

- довідкова служба та технічна підтримка;

- розробка та обслуговування додатків;
- QA / тестування;
- розробка та обслуговування IoT;
- управління інфраструктурою;
- управління дата-центром;
- кібербезпека;
- розробка штучного інтелекту та машинного навчання;
- IT-консалтинг.



Рис. 1.2 - Основні види аутсорсингу

Більшість IT-аутсорсингових компаній спеціалізуються на одній або декількох, але рідка на всіх IT-функціях. Наприклад, типами IT-аутсорсингу, на яких спеціалізується K&C, є розробка та обслуговування програмних додатків, QA та тестування (автоматизоване та ручне), а також налаштування та управління хмарною інфраструктурою.

Товариство з обмеженою відповідальністю «Solar», яке займається, IT-аутсорсингом пропонує спеціалістів служби підтримки та технічної підтримки, управління дата-центрами або розробку спеціалізованого AI та IoT / вбудованого програмного забезпечення [4].

Сервіс зі спектру доступних послуг ІТ-аутсорсингу підприємством «Solar» надається за договором, а виконавець робіт гарантує замовнику виконання комплексу поставлених завдань. Таким чином, завдяки ІТ-аутсорсингу скорочуються витрати на утримання спеціалістів спеціаліста в штатній компанії замовника, та отримати найвигідніші умови для купівлі програмного забезпечення та офісної техніки, отримати швидкодію у разі виникнення проблем з обладнанням та ПЗ. Представник аутсорсингу надає план розвитку з єдиною точкою входу для виконання необхідних завдань.

До сфери обслуговування комп'ютерної системи організації входять:

- аудит всієї комп'ютерної інфраструктури;
- обслуговування та ремонт комп'ютерів та мереж;
- встановлення та налаштування повного комплексу програмного забезпечення;
- забезпечення безпеки мережі та безпеки зберігання та доступу до даних;
- адміністрування всього корпоративного сервісу;
- консультації та підтримка.

Це все допомагає досягти злагодженої та сталої роботи для комп'ютерної системи замовника послуг і у разі виникнення форс-мажорних завдань їх оперативного вирішення. Фахівці підприємства «Solar» відповідають за повноцінне функціонування локальної комп'ютерної мережі її серверів, електронної пошти, захищають, відновлюють дані, швидко виправляють будь-які критичні помилки та можливі несправності.

1.4 Характеристика і структура об'єкта впровадження

Товариство з Обмеженою Відповідальністю «Solar» (ТОВ «Sollar»), яке знаходиться у інженерно-технічній споруді з 3 поверхів, котра знаходиться у м. Дніпро на вул. Робітнича (рис. 1.3).

Графік роботи ТОВ «Sollar» - понеділок...п'ятниця з десятої години ранку до сьомої години вечора, вихідними дням є субота та неділя. Штат співробітників підприємства становить біля 100 чоловік.

До штату належать:

- директор підприємства;
- замісники директора;
- бухгалтери;
- юристи;
- секретарі;
- менеджери по продажу та консультанти;
- менеджери проектів;
- програмісти;
- системні адміністратори;
- помічники системного адміністратора;
- веб-програмісти;
- охоронці;
- прибиральники та інші.

Додатково підприємство може до роботи залучити 200 і більше програмістів.

Приміщення які знаходяться на підприємстві:

- кабінет директора та кімнати замісників директора;
- зала для засідань;
- кімната бухгалтерів;
- кімната менеджерів з продажу та консультантів;
- приміщення програмістів та менеджерів проектів;
- серверна кімната;
- кімната служби підтримки;
- кімната охорони;
- кімната відпочинку;
- санітарні вузли.

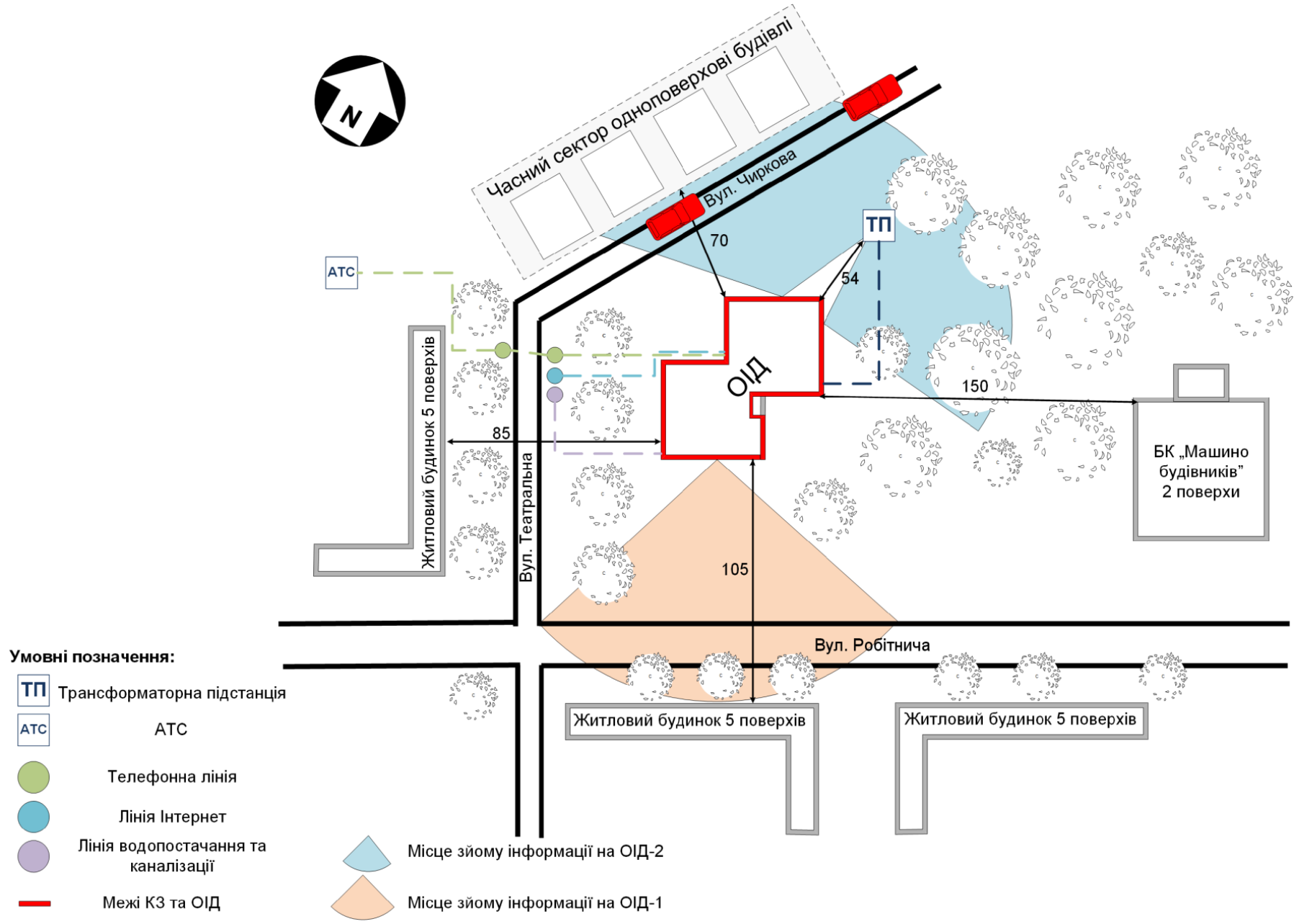


Рисунок 1.3 – Розташування будівлі ТОВ «Solar»

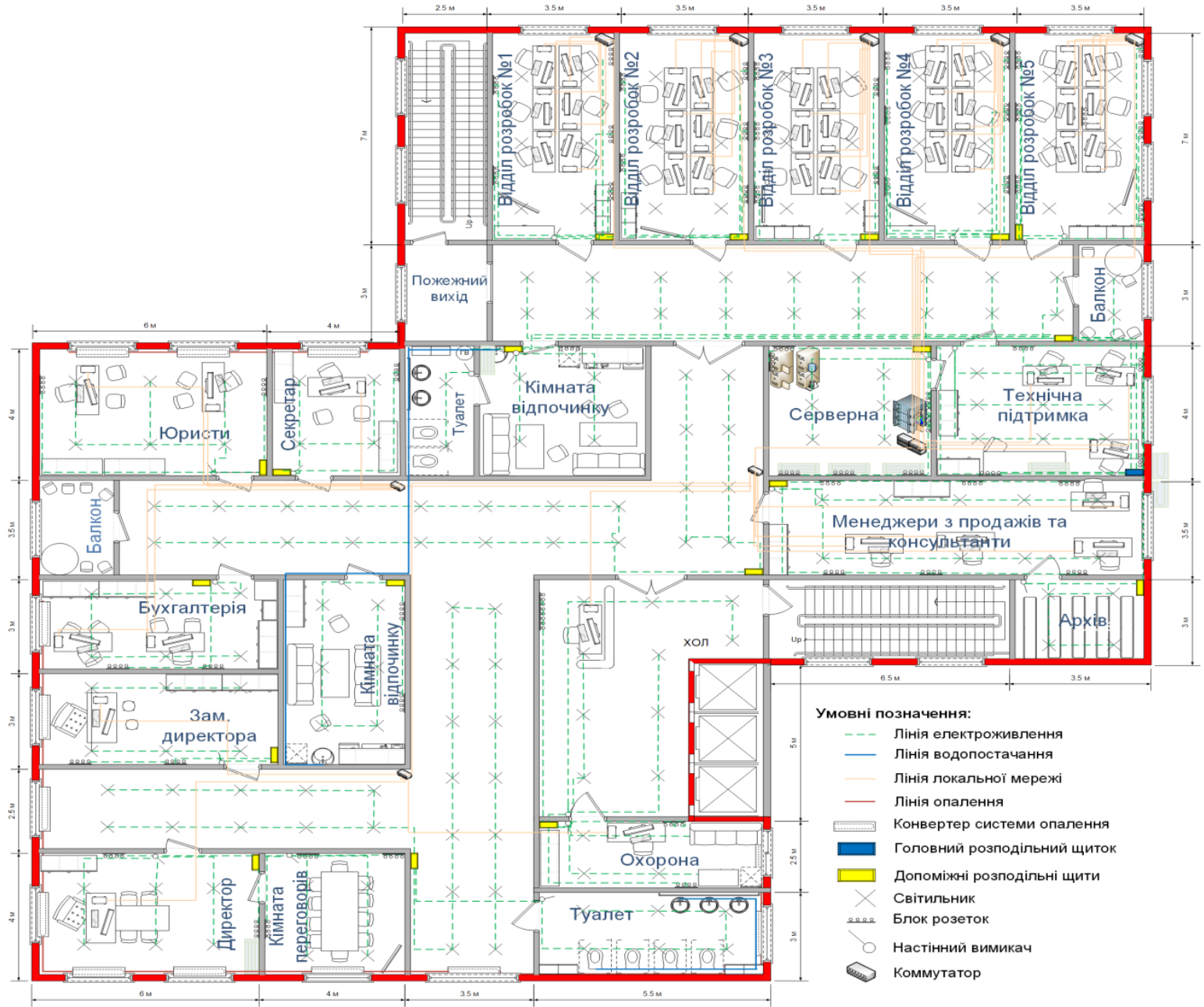


Рисунок 1.4 – План головного офісу

Приміщення, які призначені для обробки, зберігання інформації з обмеженим доступом:

- кімната для переговорів;
- серверна;
- приміщення для програмістів та менеджерів проектів;
- служба підтримки.

Таблиця 1.1 – Визначення прав доступу до службової інформації

Інформація	Правовий режим	Вид носія	Особи, що мають доступ	Де знаходиться інформація
1	2	3	4	5
Організаційно та статутна документація	Відкрита інформація	Паперовий, електронний	Директор. Бухгалтерія. Юристи. Клієнти та партнери по запити.	Кабінет директора. На серверах підприємства
Інформація про підприємство, кількість робітників, систему оплати праці, стан підприємства		Паперовий, електронний	Директор. Бухгалтерія. Юристи. Клієнти та партнери по запити.	На серверах підприємства та бухгалтерії.
Послуги підприємства		Паперовий, електронний	Всі	На серверах підприємства та бухгалтерії.
Ліцензійні згоди		Паперовий, електронний	Всі	На серверах підприємства та у юристів
Результати переговорів	З обмеженим доступом	Паперовий, електронний	Менеджери проектів. Програмісти. Директор. Замісник директора.	На серверах підприємства та в менеджерів проектів.
Договори з клієнтами		Паперовий, електронний	Директор. Замісник директора. Бухгалтера. Юристи.	Бухгалтерія. На сервері підприємства.
Договори з партнерами		Паперовий, електронний	Директор. Замісник директора. Бухгалтера. Юристи.	Бухгалтерія. На сервері підприємства.
Технічне завдання		Паперовий, електронний	Директор. Замісник директора. Програмісти	Менеджерів проектів. На сервері підприємства.

Продовження табл.1.1

1	2	3	4	5
Трудові договори	З обмеженим доступом	Паперовий, електронний	Директор. Замісник директора. Бухгалтера. Юристи.	В бухгалтерії. На сервері підприємства.
Організаційно – розпорядна документація		Паперовий, електронний	Працівники підприємства.	В секретаря. На сервері підприємства.
Інформація про комп'ютерну мережу		Паперовий, електронний	Директор. Системні .адміністратори Помічники системних адміністраторів	Серверна. На серверах підприємства.
База даних клієнтів		Паперовий, електронний	Директор. Бухгалтера. Юристи. Менеджери проектів.	Бухгалтерія. На серверах підприємства.
Бухгалтерська звітність		Паперовий, електронний	Директор. Бухгалтера	Бухгалтерія. На серверах підприємства.
Програмні продукти (власні)		Паперовий, електронний	Директор. Менеджери проектів. Програмісти. Заказник.	На серверах підприємства.
Розроблювані проекти(для замовника)		Паперовий, електронний	Директор. Менеджери проектів. Програмісти. Заказник.	На серверах підприємства.
Вихідний код		Паперовий, електронний	Програмісти. Менеджери проектів. Директор. Замовники.	На серверах підприємства.

1.4.2 Партнерство з ТОВ «Sollar»

ТОВ «Sollar» є постачальником керованих ІТ-послуг, що надає численні переваги замовникам:

1. Експертиза: Постачальники керованих ІТ володіє знаннями та досвідом для ефективного управління складними ІТ-середовищами.

2. Економічна ефективність: Аутсорсинг ІТ-послуг може призвести до економії коштів у порівнянні з утриманням внутрішнього ІТ-відділу.

3. Масштабованість: Керовані ІТ-провайдери можуть пристосуватися до зростання вашого бізнесу та мінливих ІТ-вимог.

4. Безпека: провайдери надають пріоритет безпеці, впроваджуючи передові заходи для захисту від кіберзагроз.

5. Зосередьтеся на основному бізнесі: Аутсорсинг ІТ-завдань дозволяє компаніям - користувачам зосередитися на основній бізнес-діяльності, сприяючи зростанню та інноваціям.

6. Підтримка 24/7: Керовані ІТ-провайдери пропонують цілодобову підтримку для оперативного вирішення проблем і мінімізації часу простою.

7. Передові технології: Партнерство з експертами забезпечує доступ до передових технологій і рішень.

У цифрову епоху ІТ-послуги від ТОВ «Sollar» є основою сучасного бізнесу. ІТ-послуги є невід'ємною частиною успіху компанії, від підтримки технологічної інфраструктури до забезпечення безпеки даних та сприяння зростанню. ТОВ «Sollar» розуміючи ІТ-потреби компаній, використовуючи контрольний список для оцінки та враховуючи переваги партнерства з постачальником керованих ІТ-послуг, можете гарантувати, що компанія - користувач залишатиметься конкурентоспроможною, безпечною та готовою до зростання в технологічному ландшафті, що швидко змінюється.

У ТОВ «Sollar» є непохитна відданість наданню технологічних рішень, які можуть допомогти компаніям – користувачам досягти успіху в бізнесі з використанням керованих ІТ-послуг. Завдяки досвідченій команді ТОВ «Sollar», яка може похвалитися більш ніж багаторічним практичним досвідом у проектуванні, впровадженні та підтримці ІТ-інфраструктур на рівні підприємства, має глибоке розуміння складних потреб бізнесу, починаючи від малих підприємств і закінчуючи глобальними організаціями [1].

1.4.3 Організаційна структура управління підприємства

На рис. 1.5 показана організаційна структура управління підприємством ТОВ «Sollar».

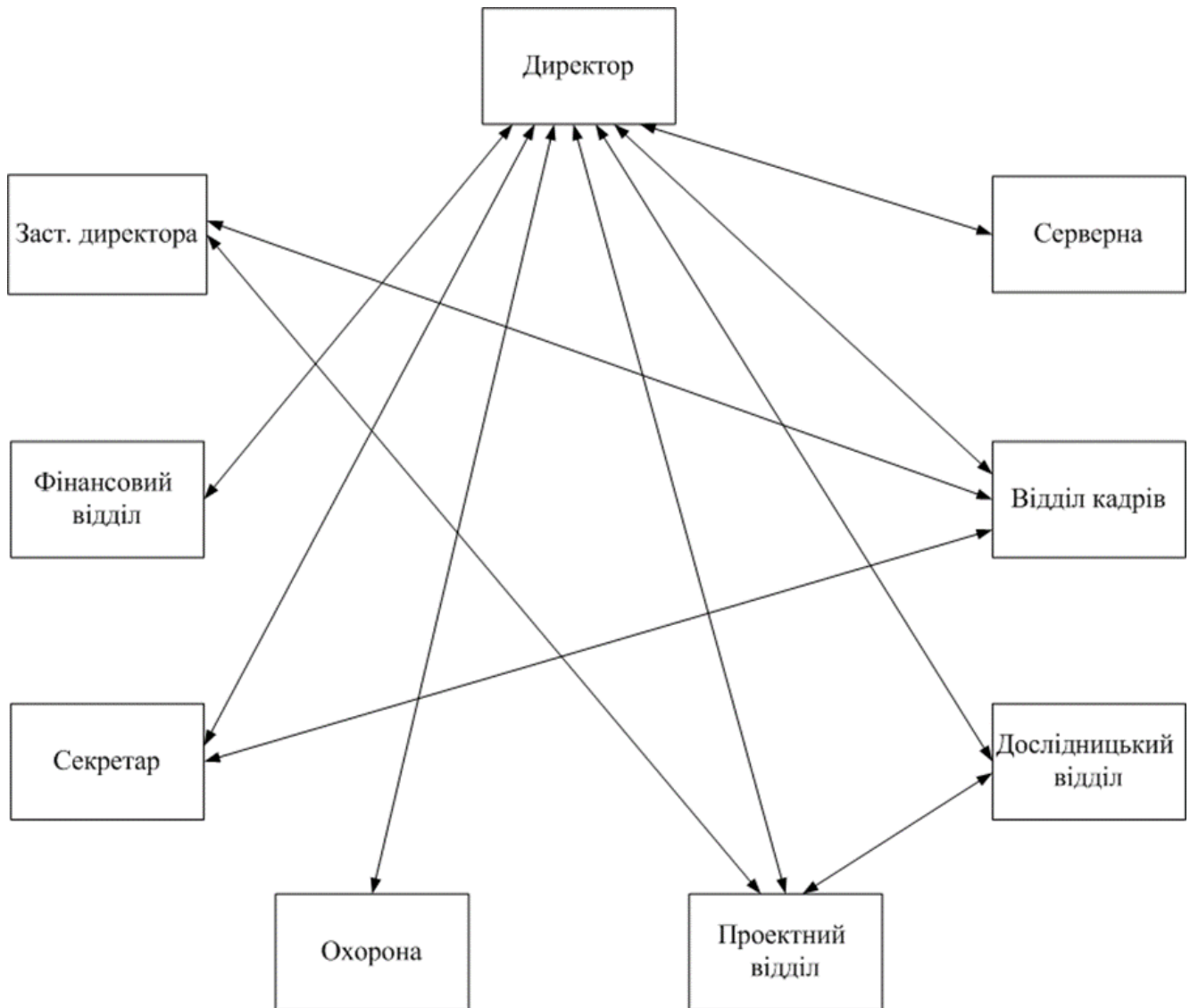


Рисунок 1.5 - Основні інформаційні потоки на підприємстві

За функціональними ознаками структура ТОВ «Sollar» відноситься до лінійно-функціональної з ланками, які реалізують принципи проектного управління.

Так як поле діяльності підприємства досить широке (як за функціональними так і за топологічними ознаками) комп'ютерна система ТОВ «Sollar» повинна забезпечувати роботу віддалених проектних підрозділів та віддалену роботу співробітників.

1.4.4 Функціональні особливості комп'ютерної системи

Основні роботи які виконують співробітники це розробка ПЗ. Відповідно до завдань та виконуваних проектів компанія ТОВ «Sollar» забезпечує розробників необхідними програмними продуктами.

В табл. 1.2 представлені основні програмні продукти, які використовуються в комп'ютерній системі (КС).

Таблиця 1.2 - Найменування ПЗ

Програмне ПЗ		
1	2	3
Назва, версія	Де встановлено	Тип ліцензії
Linux Ubuntu Server 12.04.04 (DNS, IP-tables, cash-server, openSSH, OpenSSL.)	Шлюз + FireWall	GNU GPL (Стандартна загальнодоступна ліцензія обмеженого використання GNU)
Linux Ubuntu Server 12.04.04 (Apache2.1, OpenSSH, Nginx, SQLserver, PHP5.)	Web-server	GNU GPL
Windows Server 2008 SP3 (Active Directory)	Контролер домену	Комерційна
Linux U Server 12.04.04 (FTP, Samba. NAS.)	Файловий сервер	GNU GPL
Linux Ubuntu Server 12.04.04 (Virtualisation (Windows Server 2008 SP3 (Active Directory)), DNS, IP-tables, cash-server, openSSH, FTP, Apache2.1, Nginx, SQLserver, Samba. NAS)	STORAGE (Сервер реплікації комп'ютерної мережі)	GNU GPL
Linux Ubuntu/Debian/Mint/ArchLinux/Slackware/SentOS	ПК 1-30	GNU GPL
Windows 11 Business SP2	ПК 1-30 ПК 31-43	Комерційна
Virtual Machine (Win XP, Win Vista, Win 8)	ПК 1-30	Beta (тестова ОС)
Компілятори GCC, Python, Rubi, Java Machine, Perl.	ПК 1-30	GNU GPL
OpenOffice4.2	ПК 1-43	GNU GPL
LibreOffice3.2	ПК 1-43	GNU GPL
7zip 6	ПК 1-43	FreeWere
Mozilla Firefox 12	ПК 1-43	GNU GPL
VLC 2.5.1	ПК 1-43	GNU GPL

Продовження таблиці 1.2

Прикладне ПЗ		
1	2	3
WinDjView 1.0.3	ПК 1-43	FreeWere
1С:Предприятие 8, Базова версія	ПК 31-32	Комерційна
Захисне ПЗ		
Назва, версія	Де встановлено	Тип ліцензії
Nod 32 4.2 Business	ПК 1-43	Комерційна

1.4.5 Критичний аналіз комп'ютерної системи ТОВ «Sollar»

Комп'ютерна мережа ТОВ «Sollar» призначена для полегшення потоку інформації всередині компанії. Інтернет сьогодні все більш популярний - це гігантська комп'ютерна мережа комп'ютерів, які з'єднані між собою і можуть взаємодіяти. Це стає через те, що розвиток мережевих технологій відбувається дуже швидкими темпами.

Основні проблеми є.

1. Підключення до Інтернету - в певному сенсі підключення до Інтернету може бути небезпечною загрозою, багато атак, які можуть відбуватися як всередині, так і зовні, такі як віруси, трояни та хакери. В кінцевому підсумку важливу роль в даному випадку зіграє безпека комп'ютерів і комп'ютерних мереж. Гарна конфігурація брандмауера та оптимізована для зменшення цих загроз. Конфігурація брандмауера існує 3 типи: екранована система хост-брандмауера (Single-homed bastion), екранована система хост-брандмауера (Dual-homed bastion) і екранований брандмауер підмережі. А також налаштувати брандмауер так, щоб відкривати порти Port right для включення підключення до інтернету, тому що порти для настройки брандмауера який може фільтрувати пакети вхідних даних відповідно до політики або політиками. Це архітектура брандмауера, яка буде використовуватися для оптимізації роботи брандмауера в мережі [5].

2. Інформаційне перевантаження. Проблема інформаційного перевантаження, що існує, стала більш широкою. Як сприйняття, так і фактичні наслідки інформаційного перевантаження загострилися швидким прогресом в інформаційно-

комунікаційних технологіях, хоча не ясно, чи погіршив або поліпшив ситуацію Інтернет. Однією з тем, є парадоксальна ситуація, коли, незважаючи на велику кількість доступної інформації, часто важко отримати корисну, актуальну інформацію, коли вона потрібна. Деякі рішення, запропоновані для зменшення інформаційного перевантаження: зменшення дублювання інформації; прийняття стратегій управління особистою інформацією разом з інтеграцією програмних рішень, таких як технологія Push та інтелектуальні агенти; та надання інформації з доданою вартістю («яку збирають фахівці з програмного забезпечення або інформації»).

Проблема інформаційного перевантаження сьогодні широко визнана. Однак на робочому місці інформація розглядається як ключ до успіху організацій, і багатьом людям доводиться мати справу з величезною кількістю інформації з багатьох джерел у рамках своєї роботи. Люди не можуть ігнорувати інформацію на робочому місці. «Професійне та особисте виживання в сучасному суспільстві явно залежить від здатності сприймати на борт величезні обсяги нової інформації. Проте ця інформація зростає з експоненціальною швидкістю.

Шляхи вирішення проблеми інформаційного перевантаження існують різні, навряд чи можна знайти одну ідеальну відповідь, щоб зменшити або викоринити проблему інформаційного перевантаження. Запропоновані в літературі заходи, які можуть допомогти зменшити проблему інформаційного перевантаження, включають прийняття стратегій управління особистою інформацією; подальше використання технології Push та інтелектуальних агентів; збільшення використання інформації з доданою вартістю (виробленої фахівцями з програмного забезпечення та / або інформації); впровадження управління інформацією та інформаційного менеджменту, заснованого на знаннях. Факти свідчать про зростаюче визнання останньої, що передбачає обмін та використання достовірної, цінної інформації в масштабах всієї компанії.

Завдяки цілісному підходу до обробки інформації інформаційне перевантаження може стати меншим тягарем [6].

1.4 Завдання

При обґрунтуванні структури та параметрів комп'ютерної системи мережі ТОВ «Sollar» треба проаналізувати необхідну продуктивність комп'ютерної мережі в процесі її номінальної експлуатації та визначити її можливості при інформаційному перенавантаженні.

Для більш-менш надійної оцінки показників продуктивності комп'ютерної мережі ТОВ «Sollar» треба спиратися на наступні початкові дані, такі, як - швидкодія використаних мережевих пристроїв, технічні параметри використаного ПЗ, використаних параметрів безпеки для передачі інформації у мережі, інтенсивність потоків даних, обмеження та вимоги на виконання програмного забезпечення користувачів комп'ютерної системи у реальному часі, продуктивність каналів передачі інформації, шкідливі впливи вірусних програм, наявність додаткових каналів для резервної передачі даних та багато інших факторів.

Для виконання поставленого завданням для дослідження поведінки комп'ютерної мережі комп'ютерної системи мережі ТОВ «Sollar» є потреба визначення межі інформаційного навантаження на комп'ютерну мережу, при яких вона буде здатна повноцінно функціонувати та забезпечити обробку запитів з мінімальною затримкою у часі. Це дослідження можна провести на основі моделі мережі масового обслуговування.

Позитивним результатом буде поліпшення роботи комп'ютерної мережі при підвищеному інформаційному навантаженні.

2 ТЕОРЕТИЧНА ЧАСТИНА

В кваліфікаційній роботі магістра на тему «Обґрунтування структури та параметрів комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування» треба визначити режими інформаційного навантаження на мережеві пристроїв. Режим навантаження буде залежати від складності задіяного ПЗ. Для достовірного оцінювання інформаційного навантаження використаємо математичний апарат теорія систем масового обслуговування (СМО). СМО дозволяє ефективно описувати абстрактні процеси - вхід технічного пристрою у вигляді інформаційного потоку, що дозволяє проаналізувати чергу на вході того чи іншого компоненту комп'ютерної мережі (КМ).

2.1 Загальна інформація про моделювання КМ

Сучасні комп'ютерні мережі, враховуючі Інтернет - це складні системами, які потребують дослідження з відповідними методами імітаційного та аналітичного моделювання. Однак на ці проблеми часто звертають увагу реальні розробники та оператори мереж. Типовими є реальні приклади, коли «консультанти» радять замінити симуляційне дослідження більш сучасним комп'ютером.

Є основні методи та інструменти для моделювання дискретних подій, що доступні для дослідження комп'ютерних мереж, деякі з них спеціально виконані для проведення імітаційних досліджень реальних розподілених систем і мереж в реальному часі, що є сучасним, економічним і ефективним способом.

Існують типові зовнішні засоби вимірювання параметрів мережі, а також внутрішній інструмент, який і розроблений для цілей фактичного проектування та експлуатації глобальних мереж і адаптований до потреб реальних мереж типу Інтернет.

Як правило, все одно відчувається недостатність основних відомих в техніці методів аналітичної діяльності, спрямованих на комп'ютерні мережі. Все це

зображується, коротко, дає приблизну аналітичну модель, яка розроблена для конкретних реальних комп'ютерних мереж.

Тому до моделювання надійності комп'ютерної мережі слід застосовувати досвід з реальних проектних робіт, а також враховувати деякі об'єктивні причини для вибору топології розподіленої системи / мережі.

Кількість симуляційних досліджень у світі зростає дуже швидко. Для цікавого класу під назвою моделювання дискретної системи подій доступні численні посилання, браузер вказує приблизно на 150 000 позитивних результатів пошуку.

Доступні мови програмування, орієнтовані на вирішення проблем моделювання, такі як SIMULA, SCL, MILITRAN, SIMSCRIPT, ASPOL, ECSS II, OSSSL, COMSL, VRML, VRBL, CSL Sim, SLAM II, GPSS/H, SDX, Ptolemy, DSDS+, MODSIM, Simple_1, Pasion, WinSAAM, MathCOre, Ps-i. та ін.

Однак переваги цих інструментів компенсуються їх обчислювальною ефективністю, яка зазвичай є низькою для великомасштабних комп'ютерних систем і мереж. Тому пропонуються різні допоміжні засоби моделювання (допомагають в розробці конкретних тренажерів) або тренажери для деяких задалегідь визначених класів об'єктів, що охоплюють такі тренажери та інструменти як: NETSIM (MIT), NIST (Національний інститут стандартів і технологій для мереж банкоматів), INSANE (Каліфорнійський університет, для IP over ATM), NETSIM (Університет Річмонда, для локальних мереж) і менш ефективні, симулятори «загального призначення», такі як: CPSIM (Boycan Tech. Inc.), NEST (Колумбійський університет), REAL (Корнельський університет), NS (Національна лабораторія Лоуренса Берклі), OPNET (MIL 3), SimuNet (комерційний пакет), Prophesy (програмне забезпечення для абстракції), Ipv6 з JAVA (Техаський університет), QoS – Java (Університет Огайо), HYSYS (Hyprotech Ltd.).

Як впливає з наведеного вище огляду додатків для моделювання для оцінки продуктивності мережі, нетривіальні завдання вимагають індивідуального підходу. Спеціалізовані мови програмування високого рівня навряд чи застосовуються. Також

досить недоцільно використовувати спеціалізовані симулятори, оскільки нові мережі, як правило, ними не охоплені.

Відомі деякі конкретні імітаційні дослідження, що проводяться вже протягом більш ніж 30 років [7].

2.2 Імітаційні дослідження КМ

2.2.1 Передачі інформації окремому користувачу

Одна з проблеми імітаційного дослідження була пов'язана з комп'ютерною системою управління / мережею для заводів. Мета дослідження полягала в швидкій передачі технологічної інформації на окремі станції обробки, щоб скоротити міжпартійні затримки (які важливі для виробництва). Крім того, управління виробництвом повинно бути вдосконалено за рахунок автоматичного збору даних і ведення журналів, а також за рахунок аварійного контролю виробництва.

Дуже важливо знати, що жодна заготовка не може бути «втрачена» комп'ютером. Важливо також дізнатися середній час зайнятості процесора, щоб оцінити можливий обсяг повного функціоналу.

Популярні на той час методи теорії масового обслуговування (епоха до Леонарда Клейнрока) зазнали невдачі (досліджувалися відкриті моделі і система була замкнута; вхідні потоки не мали пуассонівського характеру і навіть деякі з них були взаємно залежними; конструкторів цікавили інтервали, в межах яких були сконцентровані невідомі випадкові величини) – не існувало методів теорії масового обслуговування, що відповідають на такі питання) – тоді і, У більшості випадків, навіть зараз. Це і послужило основною причиною розробки специфічного симулятора дискретних подій (рис. 2.1).

Самою основою будь-якого дискретного симулятора подій є генератор випадкових чисел для рівномірного розподілу (2.1). З самого початку автор користувався дуже швидким алгоритмом, розробленим «помилково» вроцлавськими математиками.

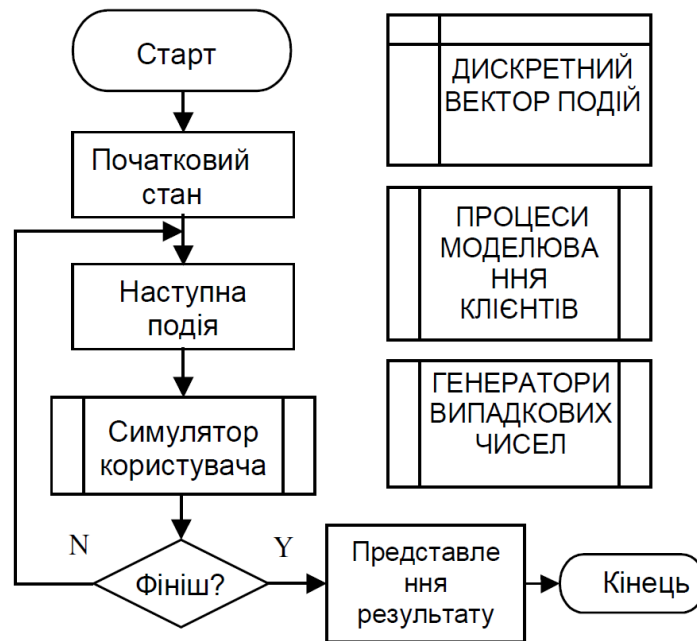


Рисунок 2.1 - Блок-схема дискретного симулятора подій алгоритму Des

$$x := x_0 + 2 \cdot x_1 \pmod{1} \quad (2.1)$$

$$x_0 := x_1 \quad x_1 := x$$

Цифра 2, вставлена оператором, забезпечувала досить низьку кореляцію між послідовними реалізаціями випадкового числа, зберігаючи при цьому високу швидкість (множення вимагало лише одного зсуву). Ця швидкість також була збільшена за рахунок застосування інтервального наближення щільності розподілу для інших розподілів. Іншим рішенням, що підвищило ефективність алгоритму Des, була процедура перегляду таблиці (заснована на так званому принципі «ділення на два», який теоретично є оптимальним) [7].

2.2.2 Системи дослідження методом моделювання та отримання результатів

Система управління та координації стрижневого стану розглядають один з найважливіших результатів - системне детальне знання того, що насправді відбувається в КМ. Вона найчастіше, розробляється на основі функціональних можливостей КМ і, як правило, немає часу розбиратися з детальними проблемами продуктивності. Розуміння проектувальником своїх рішень часто дозволяє, наприклад, досить точно оцінити невідомі інтервали концентрації змінного розподілу.

Такі симуляційні «побічні продукти» були дуже важливими, вони є основою філософії проектування, визначеної при розробці зразкових комп'ютерних систем / мереж. Варто відзначити, що, як правило, наявне в Україні обладнання для КМ на 5...10 років відстає від того, що застосовується в розвинених країнах.

Для конкретного випадку основні дані для моделювання можуть бути такими:

1. обчислювальні потужності використовуються в мінімальному обсязі;
2. жорсткі вимоги в режимі реального часу будуть виконані системою;
3. не знайдено віртуального (змодельованого) сигналу переривання;
4. максимальна довжина черги не загрожує перевантаженістю системи;
5. розроблені апаратні та програмні структури зроблять систему здійсненою.

Отримані результати мають гарантувати, що запропоновані апаратні та програмні рішення можуть виконувати необхідну функцію в режимі реального часу, оптимізувати призначення пріоритетів і попереджати про високі максимальні різниці в часі обслуговування при аналогічних середніх значеннях, що вимагає особливої обережності при інтерпретації середніх значень, можливо, доступних з теорії масового обслуговування.

Описаний вище симулятор Des був адаптований для аналітичного дослідження продуктивності комп'ютерних мереж. В багатьох випадках використовується при налаштуванні та валідації аналітичних наближень [7].

2.2.3 Внутрішні вимірювальні інструменти

Для вимірювання та тестування продуктивності комп'ютерних мереж розробляються спеціальні засоби вимірювання продуктивності. Вони можуть розташовуватися зовні або всередині мережі (зовнішні і внутрішні інструменти відповідно). Внутрішні інструменти важко знайти в довідниках через хворобливу політику конфіденційності великих фірм-розробників мережевого обладнання.

Більшість описів, доступних у відкритому доступі, стосуються зовнішніх. Останній, однак, не дає змоги провести загальні вимірювання мережі, необхідні для перевірки та оптимізації основних мережевих рішень.

Для валідації та оптимізації КМ був розроблений і в даний час адаптований до сучасних мереж, що працюють в рамках набору протоколів TCP/IP система Sitwa (рис. 2.2).

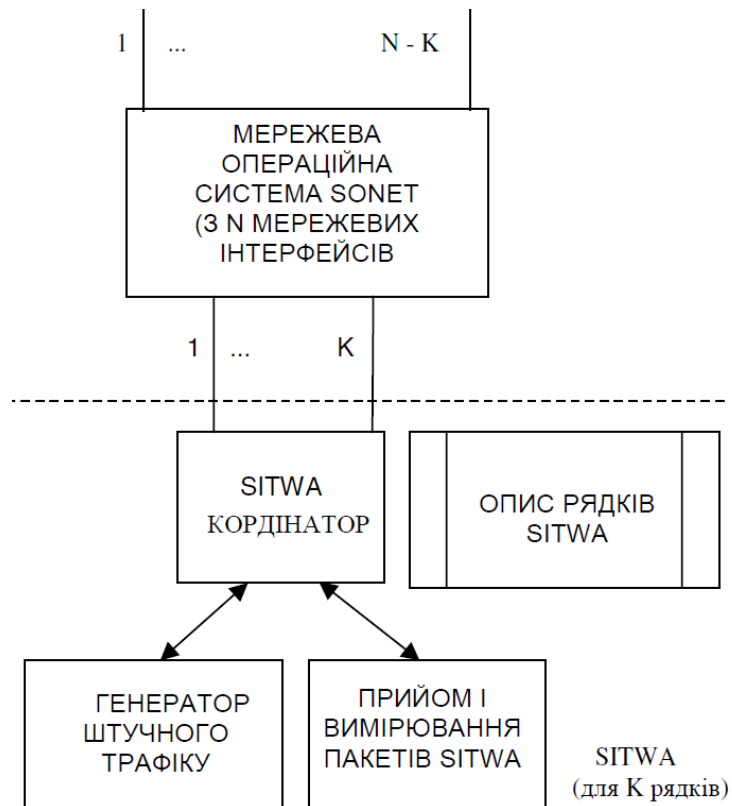


Рисунок 2.2 - Функціональна структурна схеми Sitwa в мережевій операційній системі Sonet

За допомогою Sitwa спрощені припущення, прийняті в Des (перш за все, пропуск пакетів управління потоком і фреймів при моделюванні), що на практиці були підтвержені позитивно. Крім того, тут виконано кілька десятків циклів вимірювання, що дозволяє оцінити продуктивність існуючої та запланованої конфігурації мережі (Sitwa дає можливість вимірювати віртуальну мережу та абонентське обладнання) та перевіряти розроблений наближений (оцінка продуктивності) метод на основі закритого маршруту (Cram). Відкриття Крама, підтвержене вимірюваннями з Sitwa, полягало в тому, що феномен перевантаженості (зниження пропускну здатності при

зменшенні часу мислення) має місце також у мережах з наскрізним підтвердженням без втрати пакетів.

«Побічним продуктом» Sitwa стало краще розуміння явищ, що відбуваються в будь-якій мережі, що призвело до моделювання мереж як суперпозиції закритих маршрутів (з'єднання, дзвінки) і до розробки Cram [7].

2.2.4 Аналітичні методи оцінювання діяльності

Замість досить великих очікувань, реальні проектувальники або оператори комп'ютерних і комунікаційних мереж навряд чи можуть використовувати аналітичні методи для оцінки (не кажучи вже про оптимізацію) продуктивності мереж, що розробляються і / або експлуатуються ними. Метод аналізу середнього значення є мабуть найпопулярнішим методом класичної теорії мережі масового обслуговування. Однак у цьому методі використовується стандартне припущення: задаються ймовірності переходу сутностей з лінії s на наступну лінію s' . Це очевидно невірно для реальних комп'ютерних і комунікаційних мереж.

Фактична мережа комутації пакетів, така як мережа, що працює під набором протоколів ТС/IP, повинна бути проаналізована як мережа Келлі, де час перебування на вузлу залежить від усіх сутностей (пакетів) у мережі. Однак, незважаючи на те, що мережі Kelly були визначені більше двох десятиліть тому, для оцінки класичної черги з продуктивності в цьому випадку у мереж доступні і теоретичні методи, що дозволяють досить близько апроксимувати показники до реальних мереж.

За кілька останніх десяти років було розроблено багато методів оцінки продуктивності систем стохастичного масового обслуговування. Вони також охоплюють цікавий випадок мереж Келлі (також більш загального класу мереж Уиттла). Однак стохастичні методи в основному є теоретичним математичним інструментарієм, який не підходить для реальних проектувальників і операторів мереж, а замкнуті мережі завжди створюють значні проблеми [7].

Це послужило причиною розробки наближеного аналітичного методу Cram (рис. 2.3) на основі закритого маршруту.

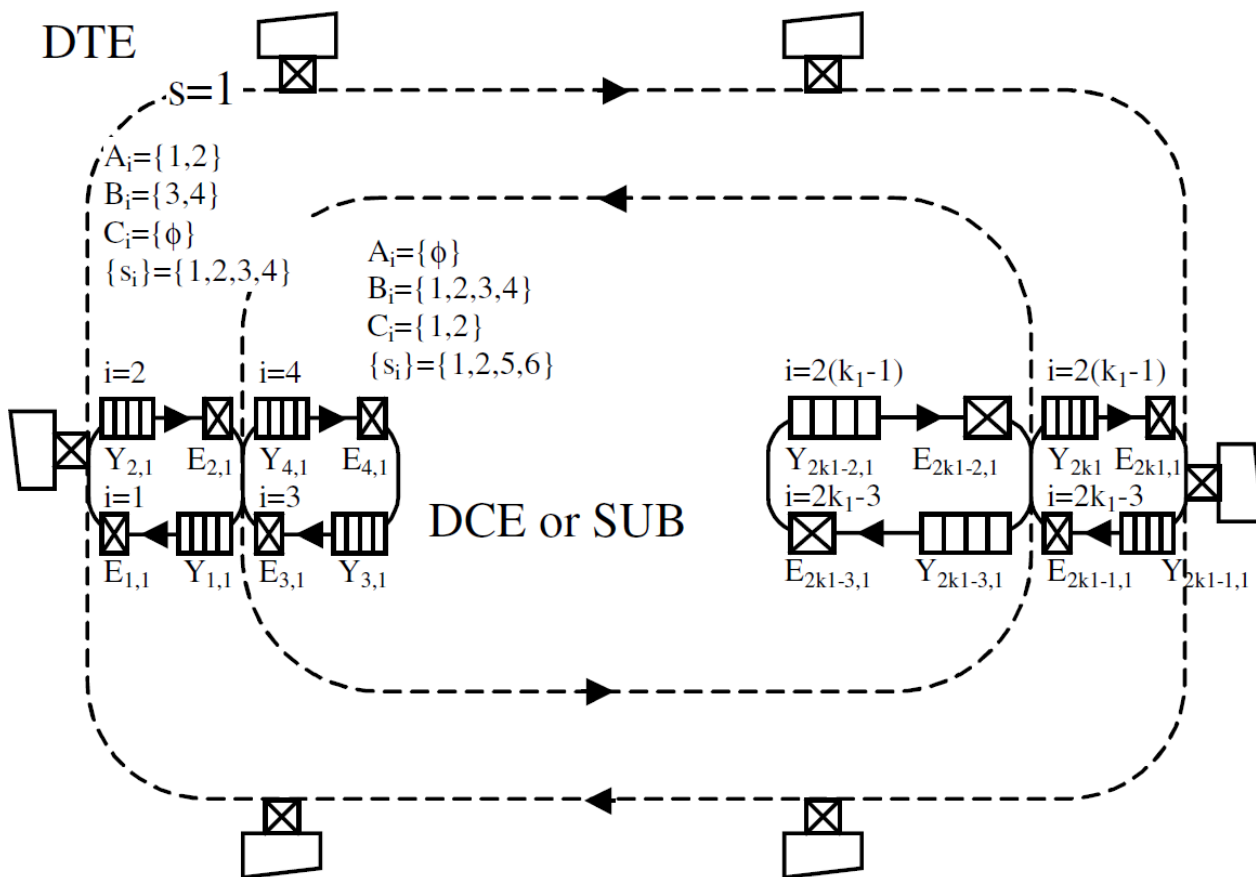


Рисунок 2.3 - Ілюстративна схема мережі на основі замкнутого маршруту

Метод був успішно застосований і валідований (відносна похибка в порівнянні з результатами моделювання і вимірювань, що перевищує 5%, не виявлена) для різних прийнятих і планованих конфігурацій КМ, мереж з зірковою топологією, різних глобальних, локальних і столичних мереж, а також, останнім часом, для мереж комп'ютерно-інтегрованого виробництва і управління (СІММ) [7].

2.2.5 Надійність мережі

У сфері систем автоматичного управління поняття надійності, тобто здатності до збурень, роботи в умовах невизначеності вже в 1982 р Д. Дойл запропонував так звану функцію μ (структурна сингулярна величина), як міру надійності системи. Ця функція була застосована для порівняння топологій розподілених систем управління за деякими обґрунтованими критеріями (рис. 2.4). У зв'язку з тим, що розподілені комп'ютерні системи управління (мережі) можуть розглядатися як обчислення, що складаються тільки з елементів автоматичного управління типу затримки часу,

обчислення, необхідні для оцінки функції μ , досить прості, і цей метод може бути застосований в реальному проектуванні мережі.

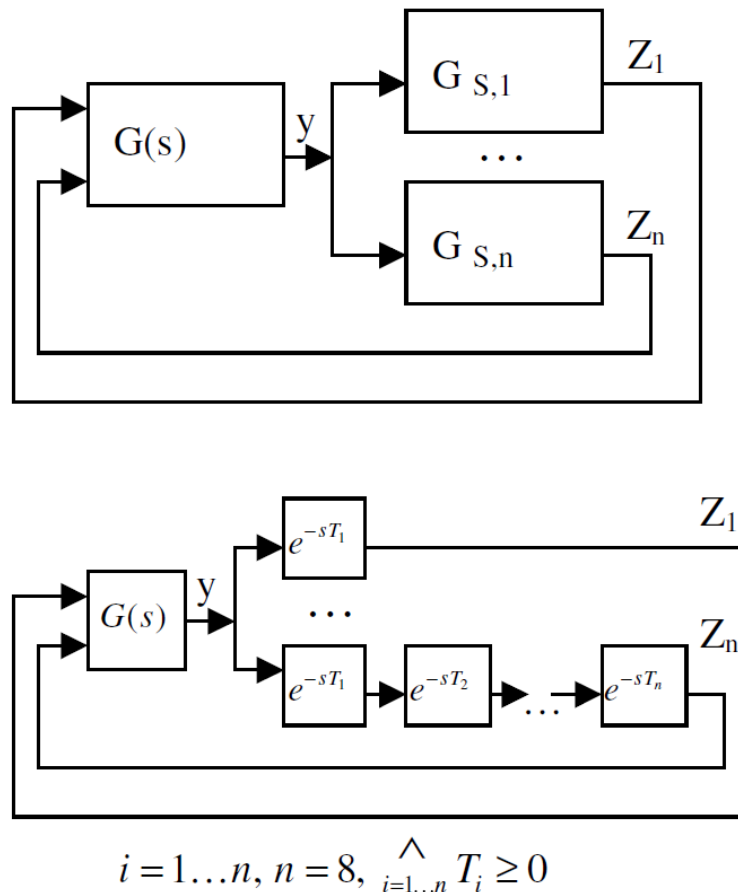


Рисунок 2.4 - Основні схеми для зіркового (верхнього) і спільно-середнього (нижнього) випадків

Цікаво те, що для цього застосування, мережі «застарілої» топології «зірка» набагато надійніші, ніж мережі «спільного-середнього».

2.3 Імітаційна модель комп'ютерної системи ТОВ «Sollar»

У бакалаврській кваліфікаційній роботі була розроблена комп'ютерної системи ТОВ «Sollar» з дворівневою ієрархічною структурою. Верхній рівнем - ядр, та нижнім рівнем – рівнем розподілу (рис. 2.5).

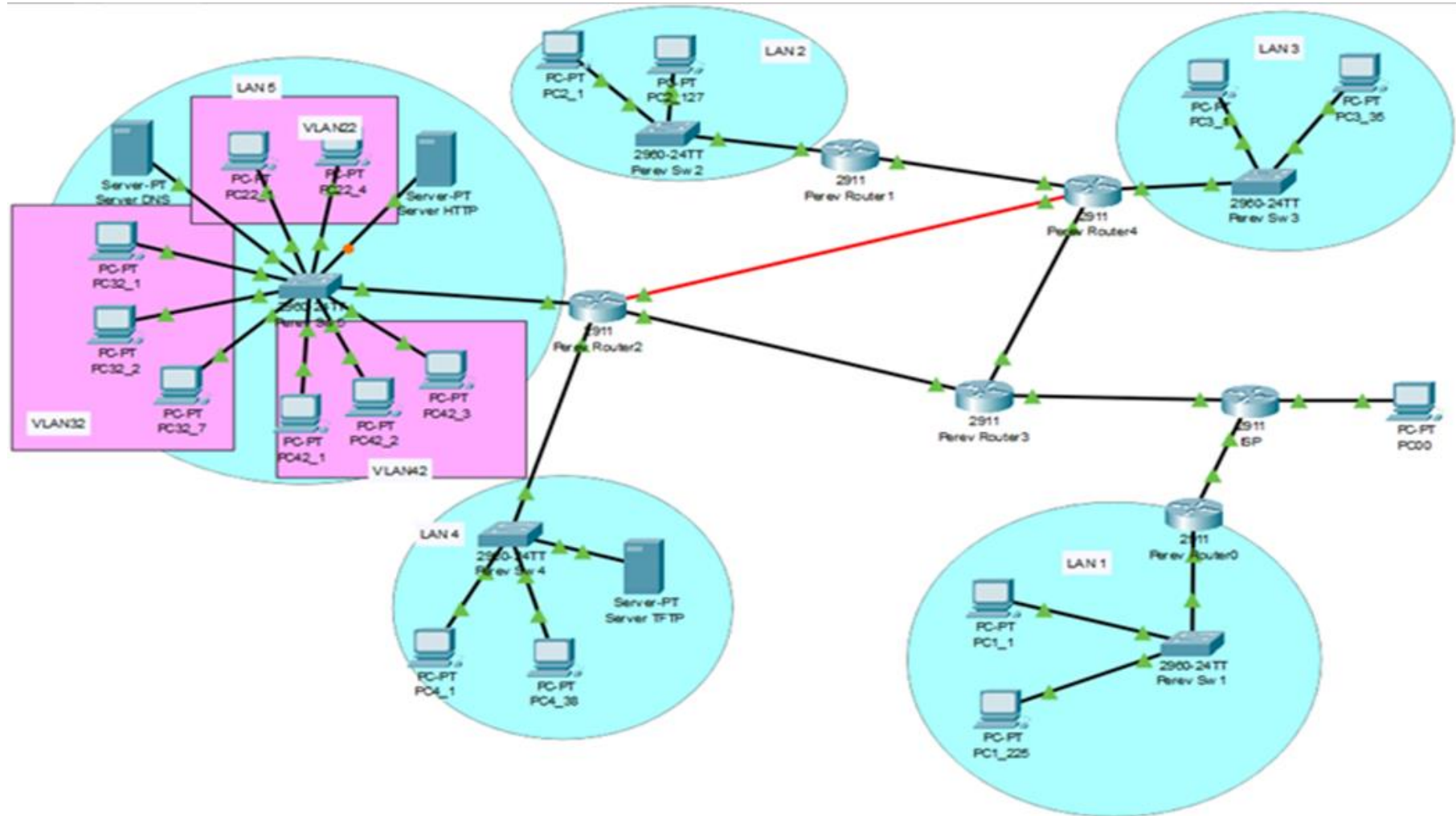


Рисунок 2.5 – Комп'ютерна система ТОВ «Sollar»

Основними показниками для комп'ютерної системи ТОВ «Sollar» є:

1. Структура мережі ТОВ «Sollar» складатися з 5 підмереж LAN1...LAN5;
2. Кількість вузлів: LAN1–62; LAN2–12; LAN3–85; LAN4–42; LAN5–34;
3. Інтенсивність трафіку $\mu = 133$ (кадрів/с);
4. Блок адрес - 10.23.IPn.0/22, для виділення підмереж IPn = 28.
5. Зовнішня адреса HTTP-сервера: 209.165.200.4;
6. Середня довжина вихідного повідомлення в мережі – 650 байт;
7. Затримка передачі пакету в найбільшій мережі – ≤ 6 мс.

8. КМ має можливість функціонувати в наступних режимах: штатний режим та режим системного адміністрування. Штатний режим є основним режимом функціонування КС, він забезпечує виконання повного спектру завдань для КС. Режим системного адміністрування є технологічним режимом та використовуватися для налагодження та супроводу КС.

Для реалізації рівня ядра у КС використовують маршрутизатори, а для реалізації рівня доступу використовують комутатори для робочих груп. На рівні ядра КМ розташовані шість маршрутизаторів. Мережа ТОВ «Sollar» має єдиний простір IP-адресації. Сегменти середовища (IP-підмережі) поділяються маршрутизаторами на шість підмереж. В мережі застосована адресація IP версії 4. Для виходу КМ ТОВ «Sollar» до Internet застосована технологія NAT. Протокол динамічної маршрутизації OSPF забезпечує маршрутизацію для пристроїв мережі.

Корпоративна КМ ТОВ «Sollar» використовує топологію «ієрархічна зірка», яка базується на використанні технології Ethernet. Рівень доступу під'єднано до робочих груп з застосуванням технології Fast Ethernet, а між маршрутизаторами і комутаторами використано технологію GigabitEthernet.

Розроблену у бакалаврській роботі КМ ТОВ «Sollar» з метою перевірки функціонування було змодельовано в PacketTracer.

2.4 Розрахунок пропускної здатності найбільшого сегмента КМ ТОВ «Sollar»

Розрахуємо показники трафіку найбільшого сегменту комп'ютерної мережі ТОВ «Sollar». Режим інформаційного навантаження - максимальний.

Необхідні початкові дані, які необхідні, для здійснення для розрахунку:

- коефіцієнт зайнятості для маршрутизатора;
- завантаження каналу передачі даних для маршрутизатора;
- середня затримка одного пакету;
- середня довжина черги пакетів;
- середній час перебування пакета в черзі;
- максимально можлива пропускна здатність каналу.

Для перевірки пропускної спроможності каналів зв'язку (чи достатньо пропускної спроможності каналів) необхідно розрахувати скільки запитів генерує найбільша локальна мережа КС. Для визначення описаних параметрів локальній мережі КС ТОВ «Sollar» приймаємо як модель мережі масового обслуговування М/М/1, з наступними параметрами:

1. кількість вузлів в найбільшій мережі: 85;
2. середня інтенсивність трафіку: $\mu = 133$ кадрів/с;
3. середня довжина повідомлення: $l = 650$ байт;
4. вимоги до затримки передачі пакету – ≤ 6 мс.

Відповідно до кількості пристроїв в локальній мережі КС ТОВ «Sollar» на рівні розподілу обираємо роутер серії Cisco C921-4P (1 од.), на рівні доступу - комутатор Catalyst 2960 48 10/100 (2 од.).

Вихідний трафік на маршрутизатор має максимальну інтенсивність 100 Мбіт/с.

Для того, щоб комутатор рівня розподілу не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкість їх відправлення.

Послугами локальній мережі КС ТОВ «Sollar» одночасно можуть користуватися 100% абонентів з середньою інтенсивністю трафіку $\mu = 133$ кадрів/с, при середній довжині повідомлення у 650 байт. Розрахуємо пропускну здатність мережі на рівні доступу. Послугами одночасно користуються 100% абонентів.

$$P_{p.d} = \mu * l * n * 8, \text{ Мбіт/с}, \quad (2.1)$$

де n- кількість портів в комутаторі рівня доступу.

$$P_{p.d} = 133 * 650 * 96 * 8 = 66,4 \text{ (Мбіт/с)},$$

Пропускна здатність КМ на рівні розподілу розрахуємо наступним чином - так як до одного роутера рівня розподілу підходять 2 комутатори рівня доступу, а загальна кількість абонентів становить 85, то пропускна здатність мережі на рівні розподілу буде становити:

$$P_{p.p} = \mu * l * N * 8, \text{ Мбіт/с}, \quad (2.2)$$

де N - кількість вузлів в найбільшій мережі.

$$P_{p.p} = 133 * 650 * 85 * 8 = 58,8 \text{ Мбіт/с}.$$

Отримані при розрахунку показники не перевищують задані початкові параметри комп'ютерної мережі для КС ТОВ «Sollar». Отже, інформаційне перевантаження на обраному мережевому обладнанні відсутнє. Якщо комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 100Мбіт/с, то загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{\text{вих}} = 100\,000\,000 / (l * 8), \text{ пакетів/с}, \quad (2.3)$$

де l - середня довжина повідомлення, байт.

$$\mu_{\text{вих}} = 100\,000\,000 / (650 * 8) = 19\,230 \text{ пакетів/с}.$$

Оскільки кожне інформаційне джерело виробляє в середньому 133 пакетів/с, то обмеження для приєднання до комутатора рівня розподілу становитиме:

$$N = \mu_{\text{вих}} / \mu, \text{ джерела}, \quad (2.4)$$

де, $\mu_{\text{вих}}$ - загальне навантаження на комутатор, пакетів/с; μ - середня інтенсивність трафіку, кадрів/с.

$$N = 19\,230 / 133 = 144 \text{ джерела}.$$

Розрахунок показує, що отриманий результат повністю задовольняє вимоги до мережі для КС ТОВ «Sollar» з кількістю абонентів у 85 од.

Розрахуємо інтенсивність вихідного трафіку від всіх користувачів:

$$\lambda = N * \mu, \text{ пакетів/с}, \quad (2.5)$$

де N - обмеження для приєднання до комутатора, джерела; μ - середня інтенсивність трафіку, кадрів/с.

$$\lambda = 85 * 133 = 11\,305 \text{ пакетів/с}.$$

Коефіцієнт затримки на рівні розподілу, який впливає на час прибуття пакету у черзі є по факту показником завантаженості вихідного каналу зв'язку:

$$\rho = \lambda / \mu_{\text{вих}}, \quad (2.6)$$

де λ - інтенсивність вихідного трафіку, пакетів/с; $\mu_{\text{вих}}$ - загальне навантаження на комутатор, пакетів/с

$$\rho = 11\,305 / 19\,230 = 0,58.$$

Коефіцієнт зайнятості для комутатора рівня розподілу становитиме:

$$r = \rho / (1 - \rho), \quad (2.7)$$

де ρ - коефіцієнт затримки на рівні розподілу.

$$r = 0,58 / (1 - 0,58) = 1,4.$$

Тоді середня затримка кадру, яка пов'язана з чергою M/M/1 становитиме:

$$T = 1 / (\mu - \lambda), \text{ с} \quad (2.8)$$

де μ - середня інтенсивність трафіку, кадрів/с; інтенсивність вихідного трафіку від всіх користувачів, пакетів/с

$$T = 1 / (19\,230 - 11\,305) = 126 \text{ мкс.}$$

Середня довжина черги буде визначена наступним чином:

$$L_{\text{чер}} = \rho^2 / (1 - \rho), \quad (2.9)$$

де ρ - коефіцієнт затримки на рівні розподілу

$$L_{\text{чер}} = 0,58^2 / (1 - 0,58) = 0,8.$$

Цей показник буде корисним при реальному налаштуванні черг на обладнанні, так як в мережевому обладнанні можна вказувати максимальний розмір черги пакетів.

В нашому випадку в системі на обслуговуванні менше ніж чим 1 пакет. Це значення є досить умовним і воно свідчить про те, що система працює з великим запасом до максимального інформаційного завантаження.

Середній час перебування пакета в черзі становитиме:

$$T_{\text{оч}} = L_{\text{чер}} / \lambda, \text{ с}, \quad (2.10)$$

де $L_{\text{чер}}$ - довжина черги; λ - інтенсивність вихідного трафіку, пакетів/с.

$$T_{\text{оч}} = 0,8 / 11\,305 = 0,7 \text{ мкс.}$$

Цей розрахований показник є меншим ніж значення з обмеження, яке завдано на рівні ≤ 6 мс, що і задовольняє вимогам.

Пропускную здатність каналу визначимо наступним чином:

$$\lambda = b / l, \text{ біт/с} \quad (2.11)$$

де b - пропускна здатність, біт/с, l - довжина кадру.

Тоді $b = \lambda * l = 11\,305 * 650 * 8 = 54,7$ Мбіт/с.

Отриманий результат повністю задовольняє вимогам до обмеження пропускної здатності вихідного каналу у 100 Мбіт/с.

2.4 Висновки за розділом

Методи імітаційного та аналітичного моделювання навряд чи можуть бути застосовні до 100% реального проектування та функціонування мереж. Основними причинами такого твердження є:

1. Значні припущення, прийняті при описі розслідуваних мереж;
2. Теоретичні моделі, які занадто складні і та важко втілювані до реального проектування мереж;
3. Закрита політика конфіденційності великих КМ.

Основне пояснення на успіх успіхів, буде полягати в тому, що провідний конструктор для проектування КМ буде одночасно залучений до проблем моделювання та аналітичного моделювання, що значно покращить достовірність результатів моделювання. Для цього потрібна бути широка освітня база (з комп'ютерної інженерії, значними знанням у математиці). Це також вимагає багато аналітичної роботи з літературними джерелами на протязі до 35 останніх років, так як, розроблені в минулому і адаптовані в даний час методи імітаційного та аналітичного моделювання можуть бути застосовані для багатьох інших завдань проектування, розробки та експлуатації комп'ютерних мереж та комп'ютерних систем [7].

Розрахунок показників трафіку найбільшого сегменту комп'ютерної мережі ТОВ «Sollar» буде враховано при побудові моделі мережі.

3 СИНТЕЗ СИСТЕМИ

3.1 Обстеження об'єкту розробки

Комп'ютерні системи стають все більш поширеними. У сучасному світі комп'ютерна система – це набагато більше, ніж набір взаємопов'язаних мережевих пристроїв. Комп'ютерні системи - це система взаємопов'язаних комп'ютерів з метою обміну цифровою інформацією. Комп'ютерна система дозволяє аналізувати, систематизувати і поширювати інформацію, необхідну для прибутковості. Розвиток інтрамереж та Інтернету є важливим аспектом комп'ютерних систем. Інтрамережі та інтернети – це приватні бізнес-мережі, які базуються на інтернет-технологіях. В даний час компанії впроваджують інтрамережі шаленими темпами, і лише з однієї причини інтранет дозволяє бізнесу збирати, керувати та поширювати інформацію швидше та простіше, ніж будь-коли раніше. Багато компаній впроваджують інтрамережі просто для того, щоб залишатися конкурентоспроможними; Бізнес, який зволікає, швидше за все, побачить, що його конкуренти випередять їх [9].

Програмно-визначені мережі (SDN) – це еволюційна мережева парадигма, яка була прийнята великими мережевими та хмарними провайдерами, серед яких є технологічні гіганти. Однак прийняття нової та майбутньої парадигми як альтернативи усталеній та зрілій застарілій парадигмі мереж вимагає багато часу, а також значних фінансових ресурсів та технічного досвіду. Отже, багато підприємств не можуть собі цього дозволити. Компромісним рішенням є гібридне мережеве середовище, також відоме як Hybrid SDN (hSDN), в якому використовуються функціональні можливості SDN, а існуючі традиційні мережеві інфраструктури визнаються. Останнім часом hSDN розглядається як життєздатне мережеве рішення для різних підприємств і організацій. Відповідно, обсяг літератури з досліджень hSDN значно покращився [10].

Комп'ютерна система у ТОВ «Sollar» повинна об'єднувати всі мережеві пристрої в єдину комп'ютерну систему, таким чином вона забезпечить необхідні умови для передачі та зберігання даних, гарантуватиме їх цілісність та

конфіденційність. Також комп'ютерна система ТОВ «Sollar» повинна забезпечувати доступність сервісів і швидку обробку даних для хмарних сервісів.

Подальший розвиток комп'ютерної системи ТОВ «Sollar» бачиться у напрямку застосування програмно-визначених мережі у версії гібридного мережевого середовища.

3.1.1 Програмно-визначені мережі

3.1.1 Введення

Комп'ютерні мережі зазвичай будуються з використанням різних пристроїв, таких як комутатори, маршрутизатори, брандмауери та балансувачі навантаження, які обмінюються даними за допомогою різних стандартних протоколів.

Адміністратори мережі відповідають за встановлення відповідних політик і керування всіма мережевими пристроями з метою реагування на широкий спектр мережевих подій. Зазвичай ці складні завдання виконуються вручну за допомогою досить обмеженої кількості доступних інструментів. Отже, управління та конфігурація мережі разом із налаштуванням продуктивності мережі є досить виснажливими та потенційно схильними до помилок завданнями.

«Закостеніння Інтернету» є ще однією серйозною проблемою, з якою стикаються оператори мереж. Інтернет вважається однією з критично важливих інфраструктур у сучасному світі, і він має величезну та дуже складну базу розгортання. Таким чином, надзвичайно складно, а іноді й неможливо, щоб Інтернет оновлювався з точки зору базових протоколів, а також фізичної інфраструктури. Мережева програмованість є запропонованим рішенням для вирішення цих проблем і допомоги в оновленні Інтернету на основі виникаючих додатків і сервісів. Зокрема, програмно-визначені мережі (SDN) є еволюційною мережевою парадигмою, в якій площина управління була відокремлена від площини даних. Це призводить до значного спрощення конфігурації та управління мережевою роботою, а також до підвищеної гнучкості, і спритності (рис. 3.1).

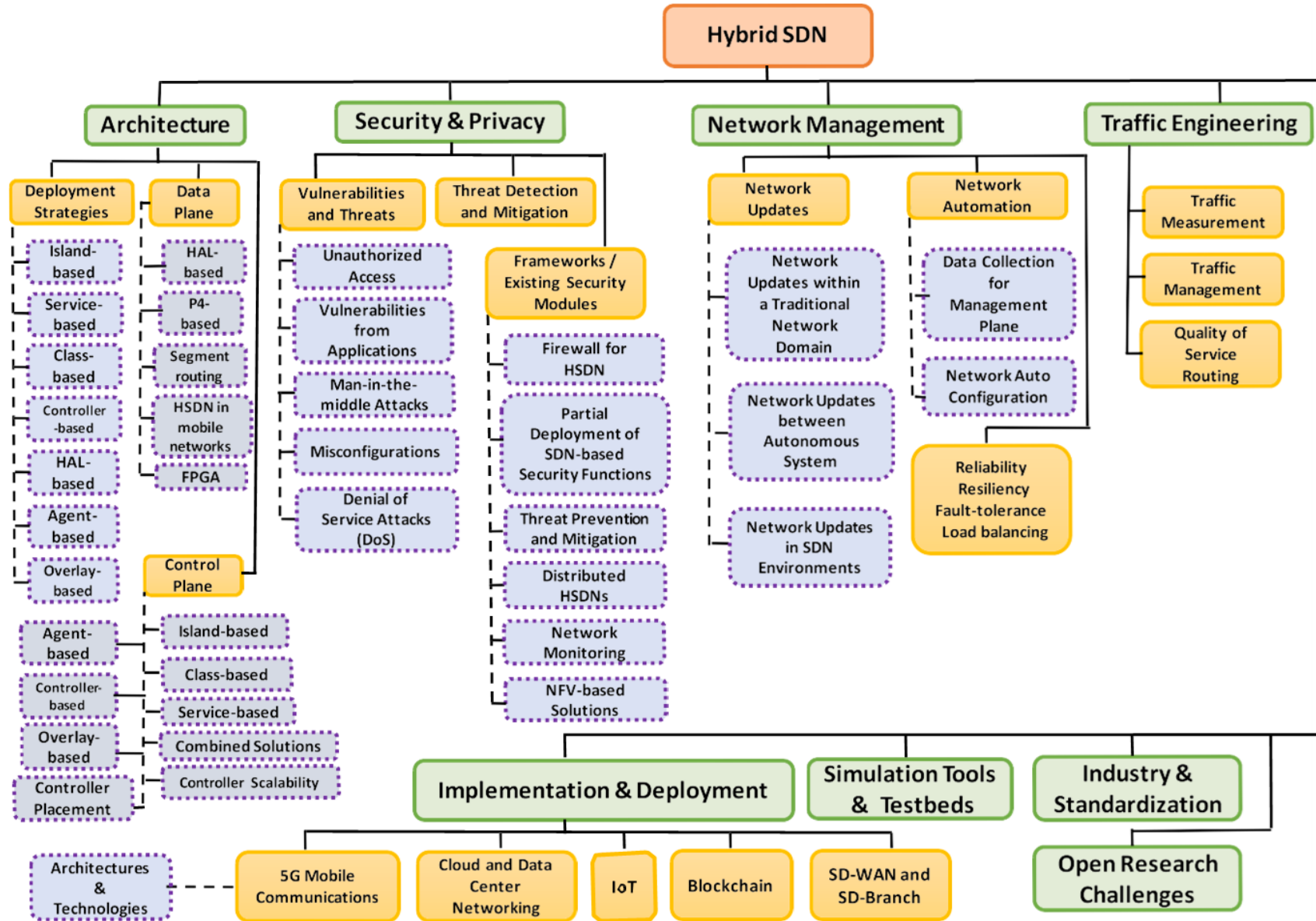


Рисунок 3.1 - Огляд варіантів гібридних програмно-визначених мереж hSDN.

Основна ідея SDN полягає в тому, щоб дозволити логічно-централізованому програмному контролеру (тобто площині управління) піклуватися про мережевий інтелект і прийняття рішень, в той час як площина даних відповідає за завдання переадресації трафіку. Такі завдання можуть бути запрограмовані або за допомогою відкритого стандартного інтерфейсу / протоколу. Наприклад, OpenFlow (OF), або ForCES, або специфічної для предметної області мови (наприклад, Programming Protocol-Independent Packet Processors (P4)). Отже, основні сторони мережевої індустрії створили Open Networking Foundation (ONF) для просування SDN і стандартизації протоколу OF. Це спричинило інтенсивне впровадження SDN майже у всіх сферах мереж, від центрів обробки даних (DC) та хмарних мереж до глобальних мереж (WAN), бездротового зв'язку та нещодавно 5G.

Отже, як промисловість, так і наукові кола витрачають значну кількість часу та грошей, щоб прийняти SDN як переважаючу мережеву парадигму. Відповідно, очікується, що ринок SDN значно зросте і в Україні при середньорічному темпі зростання (CAGR) 26,8% протягом останніх п'яти років.

Незважаючи на те, що SDN є швидкозростаючою мережевою парадигмою, традиційні IP-мережі (також відомі як застарілі мережі) все ще широко використовуються.

На те є вагомі причини. Незважаючи на те, що початкові моделі SDN припускають, що логічно-централізований контролер керує мережею, більші та складніші розгортання SDN вимагають кількох контролерів, які співпрацюють розподілена. Однак масштабованість площини керування, все ще активно досліджуються. Крім того, розподілені SDN-рішення, такі як локальність контролера, розміщення контролера та узгодженість стану мережі, все ще значною мірою покладаються на рішення, що існують у застарілій мережевій області. Безпека SDN – ще одне питання, яке потребує вирішення. Незважаючи на те, що ринок SDN процвітає, а технологічні гіганти, такі як Google, визнали його першими, безпека все ще залишається серйозною проблемою для малих і середніх підприємств. У той час як SDN стає зрілим і широко розгортається, він, безумовно, також стає привабливою мішенню.

Крім того, SDN вводить нові вектори атак, яких не існувало в традиційних мережах.

Складність – ще одна проблема. Незважаючи на те, що SDN є абсолютно конкурентною перевагою для великих технологічних компаній, він може накладати непотрібне навантаження на технічний персонал з точки зору операційних складнощів. Ці складнощі можуть виникнути при впровадженні, розгортанні і навіть адмініструванні мереж. Однак провайдери найвищого рівня отримують вигоду від величезних технічних ресурсів для вирішення цих труднощів, тоді як їхні менші конкуренти просто не можуть.

Строго кажучи, не всі можливі проблеми при прийнятті SDN є технічними. Дійсно, є і бізнесові, і фінансові ризики. Коли існуючі застарілі мережеві інфраструктури працюють безперебійно, організації зазвичай неохоче платять за нове обладнання та перенавчають свій технічний персонал. Також не існує добре вивчених уніфікованих рішень виробничого рівня для підтримки процесу міграції мережі поряд з якістю обслуговування (QoS) і схемами маршрутизації QoS в гібридному середовищі.

3.1.2 Гібридна SDN архітектура

Переваги SDN очевидні: 1 - програмованість мережі, автоматизація мережі, 2 - управління мережею знижує експлуатаційні витрати за рахунок спрощення завдань управління та 3- віртуалізація мережі. Ці аспекти спонукають мережевих операторів і підприємців модернізувати свої мережі за допомогою комутаторів і серверів з підтримкою SDN. Однак впровадження технологій SDN у застарілу мережу вимагає капітальних та операційних інвестицій і може викликати занепокоєння щодо безпеки та надійності. Останні аспекти, розглянуті в цій статті, пов'язані не тільки з самою технологією SDN, але вони також корелюють зі здатністю мережевих архітекторів і адміністраторів визначати стратегію розгортання, яка найкраще підходить для мережевого сценарію, і забезпечувати плавне співіснування між застарілими і SDN пристроями.

Як також обговорювалося в інших роботах, існує безліч стратегій розгортання мереж hSDN. Вибір стратегії залежить від багатьох факторів, таких як

тип мережі (підприємство, оператор зв'язку, дата-центр тощо), тип мережевих послуг, що пропонуються користувачам, необхідна продуктивність, капітальні та операційні бюджети.

3.1.3 Стратегія розгортання hSDN

Запропоновані концепції hSDN, починаючи з класичного плоско-орієнтованого вигляду архітектури SDN, як це зображено на рис. 3.2.



Рисунок 3.2 - Архітектура hSDN.

Знизу вгору площина даних SDN, також відома як площина пересилання даних, побудована з пристроїв з підтримкою SDN (помаранчеві елементи), віртуальних або фізичних, керованих контролером SDN через відкритий незалежний від постачальника інтерфейс South-Bound Interface (SBI). Популярним поширеним SBI є OpenFlow (OF). Площина керування використовує SBI для програмування поведінки пересилання площини даних. Мережа hSDN включає традиційну мережу, в якій трафік перенаправляється на основі рішень розподілених механізмів маршрутизації/комутації, як показано на рис. 3.2 зеленими елементами.

Площина управління SDN складається з централізованого програмного контролера, який переводить вимоги додатків до вузлів площини даних і надає відповідну інформацію аж до додатків SDN. Він підтримує логіку управління мережею і надає прикладному рівню абстрактне уявлення про мережеві ресурси з підтримкою SDN. Площина управління логічна-централізована і зазвичай реалізована як фізично розподілена система для цілей масштабованості і надійності. Набір загальних контролерів представлений на 3.2.

Північний інтерфейс (NBI) контролера SDN дозволяє програмам SDN надсилати команди конфігурації на пристрої SDN і отримувати інформацію про топологію мережі та стан площини даних. На жаль, NBI ще не стандартизований і безліч різних інтерфейси реалізовані в контролерах SDN з відкритим вихідним кодом і комерційних контролерах. Це обмежує переносимість додатків SDN з одного контролера на інший. Деякі приклади таких інтерфейсів показані в блоці NBI на рис. 3.2.

Поступово. Ситуація ускладнюється потенційним ризиком перебоїв у обслуговуванні та порушень Service-Level Agreement (SLA) під час переходу від застарілого до SDN.

Незважаючи на те, що перехід від застарілої мережі до SDN може бути пов'язаний з деякими потенційними проблемами (наприклад, фінансові бар'єри, можливі технічні труднощі та відсутність стандартів для безперешкодної міграції, і це лише деякі з них), SDN все ще має очевидні переваги, які не можна ігнорувати. Таким чином, гібридне розгортання (також відоме як Hybrid SDN (hSDN)) [30,31], де SDN і традиційні мережеві вузли співіснують, може бути компромісним рішенням. Щоб отримати максимальну віддачу від гібридного мережевого робочого рішення, де взаємодіють різноманітне мережеве обладнання, протоколи та парадигми, слід гарантувати безперебійну координацію між логічно-централізованою площиною керування SDN та застарілою розподіленою інформаційною базою маршрутизації (RIB).

Як представлено на рис. 3.3, в мережевій архітектурі hSDN співіснують як застарілі, так і SDN пристрої. У той час як в останньому база формування пересилання (FIB) заповнюється контролером SDN шляхом перекладу

високорівневих політик маршрутизації, виданих додатками SDN, в першому завданні виконується протоколами розподіленої маршрутизації, такими як Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) і Intermediate System to Intermediate System (IS-IS). В обох випадках FIB, також відомий як таблиця пересилання, використовується функцією маршрутизації або мосту для визначення належного вихідного порту пристрою для кожного пакета. Таблиці пересилання реалізуються з використанням адресованої за змістом пам'яті (CAM) або, у випадку комутаторів з підтримкою SDN, з використанням більш складних і дорогих тернарних адресованих за змістом мем-оритів (TCAM). TCAM можуть зберігати три бітові стани (0, 1 і «don») і дуже добре працювати в поєднанні з OpenFlow, де записи в таблиці потоку передбачають біт підстановки, який використовується для інформування перемикача ігнорувати значення вказаного поля заголовка. Оскільки SDN забезпечує набагато тонший контроль трафіку в порівнянні з традиційними переадресаціями L2 і L3, правила пересилання SDN вимагають більше місця в пам'яті (до 773 біт в останніх версіях OF, в порівнянні з 60 бітами при пересиланні запису L2). Це може обмежити простір застосування SDN, коли вдосконалення апаратного забезпечення недоступне або нездійсненне через вартість і енергоспоживання компонентів TCAM.

Питання, пов'язане з пропускнуою здатністю пересилаючих столів SDN, вже було досліджено і вирішено шляхом використання властивостей парадигми SDN. У зв'язку з цим, hSDN можна розглядати не тільки як стратегію перехідного/тестового розгортання в напрямку повного впровадження технологій SDN, але і як можливість максимізувати потенціал технологій SDN, таким чином подолавши обмеження пам'яті за рахунок координованого поєднання SDN і традиційних мереж.

Розглянемо різноманітні стратегії розгортання hSDN, які представлені на рис. 3.4...3.10

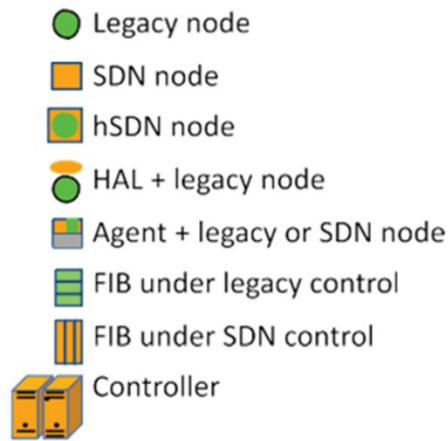


Рисунок 3.3 – Умовні позначки для схем hSDN

На основі острова. - мережа топологічна розділена на області, які ще називають островами, що складаються або зі старих пристроїв, або з вузлів SDN (рис. 3.4). Ця модель розгортання часто використовується для поступового впровадження та тестування технології SDN в обмежених регіонах з обмеженим впливом на існуючі мережеві операції. Прикладом острівної моделі є B4, програмно-визначена глобальна мережа (SD-WAN), реалізована для підключення сайтів Google. Як і в інших варіантах, магістральна мережа управляється за допомогою SDN, де потрібні грубі мережеві політики. Тоді як трафік у DC маршрутизується за допомогою застарілих протоколів і довгих тонких таблиць пересилання.

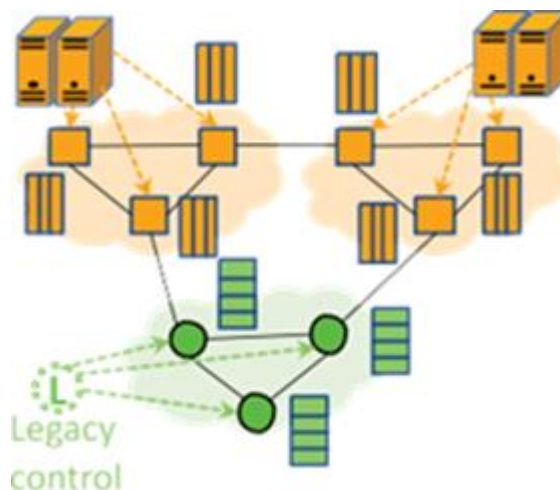


Рисунок 3.4 - Мережа основі острова

На рис. 3.4 показаний приклад моделі острів-база, що складається з трьох островів. На на рис 5.4 помаранчевий колір використовується для представлення елементів SDN вузли, FIB, контролер і мережі, в той час як зелений колір представляє застарілі елементи (вузли, FIB і мережі).

2. На основі сервісу - відповідає вимогам служб, які мають бути виділені в мережі. У той час як розширені послуги зазвичай реалізуються за допомогою технологій SDN (наприклад, балансування навантаження (LB), списки контролю доступу (ACL) тощо), інші зазвичай керуються за допомогою традиційних технологій (віртуальна приватна мережа (VPN), багато-протокольне перемикання міток (MPLS), IPSec, і т.д.). Як зображено на рис. 3.4, стратегія, заснована на обслуговуванні, може використовувати гібридні вузли, де підтримуються як розподілені, так і керуючі площини SDN.

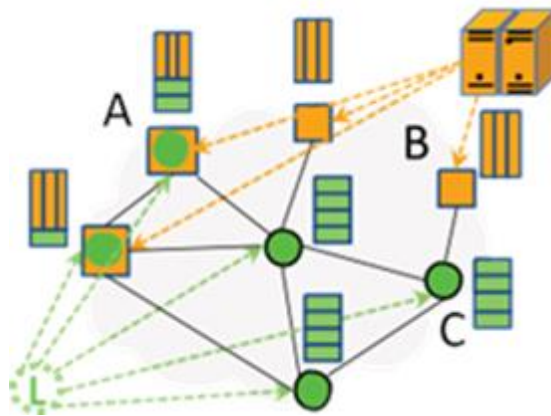


Рисунок 5.5 - Мережа основі сервісу

Цей тип вузлів отримується шляхом додавання можливостей SDN до застарілих маршрутизаторів або комутаторів шляхом виконання програмних агентів, оновлення апаратних компонентів або встановлення програмного перемикача SDN, наприклад, Open Virtual Switch (OvS). У гібридних вузлах таблиці пересилання керуються як застарілою, так і SDN парадигмою і можуть поєднувати TCAM зі стандартною пам'яттю (SRAM/DRAM).

3. На основі класу - модель заснована на поділі мережевого трафіку на різні класи, деякі з них управляються за допомогою SDN, інші - за допомогою традиційних механізмів. Поширеним способом визначення класів є використання тега Virtual LAN (VLAN). Інші варіанти включають поділ трафіку на основі транспортного протоколу (TCP або UDP), протоколу додатків (HTTP, FTP тощо) або сервісу (наприклад, VPN). Як і в сервісній моделі, мережеві пристрої (принаймні їх підмножина) зобов'язані підтримувати як традиційну, так і SDN-мережу (рис. 3.6).

Отже, стратегія класу трафіку може бути прийнята для поступового та

безпечного переходу від традиційних мереж до SDN, оскільки одна з двох парадигм також може служити резервним рішенням.

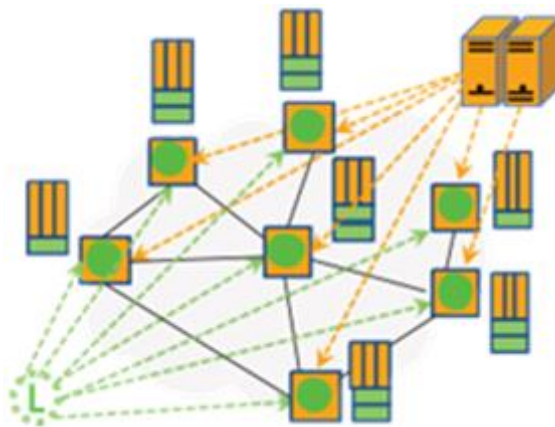


Рисунок 3.6 - Мережа основі класу

4. На основі контролера. Просунуті контролери SDN, такі як ONOS і OpenDaylight, реалізують ряд SBI, деякі з яких дозволяють їм взаємодіяти з застарілими пристроями. Це дуже актуально для розгортання, де централізована площина управління є основною вимогою. У цьому сценарії контролер SDN взаємодіє з площиною керування пристроями для маніпулювання таблицями пересилання або для налаштування параметрів протоколу маршрутизації. Стратегія, заснована на контролері, проілюстрована на рис. 3.7, часто є першим кроком міграції до повноцінного мережевого середовища SDN.

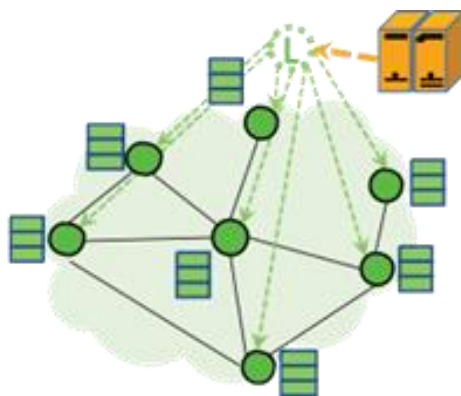


Рисунок 3.7 - Мережа основі контролера

5. На основі HAL. Основна мета HAL полягає в тому, щоб зробити застарілий мережевий пристрій SDN-сумісним за допомогою набору абстракцій. Зокрема, HAL приховує технологію та апаратне забезпечення особливостей мережевого пристрою з метою представлення контролеру відведеного SDN-сумісного пристрою. Цей підхід також може бути використаний для розширення можливостей вузлів з підтримкою SDN, наприклад, підтримка віртуалізації мережі,

сумісність з декількома версіями протоколу OpenFlow. Цей інвазійний підхід вимагає встановлення на пристрій програмних компонентів, специфічних для апаратного забезпечення. HAL бере на себе повний контроль над FIB, як це представлено на рис. 3.8.

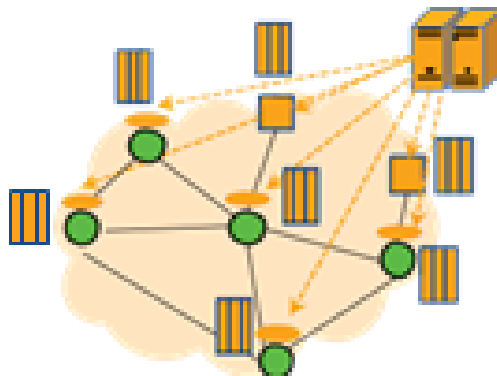


Рисунок 3.8 - Мережа основі HAL

6. На основі агентів. На мережевому пристрої виконується програмний модуль, який називається агентом, для забезпечення контролю трафіку та пересилання через SDN. Також можливе протилежне, хоча і менш поширене, коли на пристроях з підтримкою SDN встановлюється програмний агент для підтримки традиційних протоколів маршрутизації/комутації (рис. 3.9).

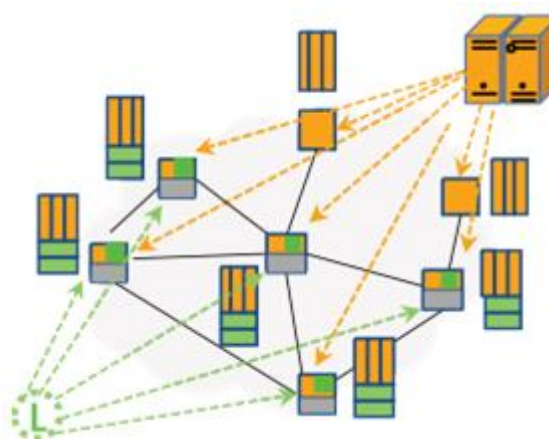


Рисунок 3.9 - Мережа основі агентів

На відміну від HAL, агент дозволяє співіснувати як застарілим, так і SDN керуючим планами, отже, спільними таблицями пересилання пристрою. Це також називається режимом подвійного стека.

7. На основі накладок. Як випливає з назви, ця модель заснована на побудові накладної мережі SDN на вершині змішаної застарілої/SDN мережі (рис. 3.10). Оверлейна мережа складається з віртуальних пристроїв SDN, які відображаються

на SDN-частині фізичної мережі та з'єднані між собою за допомогою віртуальних каналів. Віртуальне посилення може бути відображено на одному або декількох фізичних зв'язках у фізичному субстраті. FIB пристроїв SDN включають правила пересилання трафіку, а також набір записів, які необхідні для побудови віртуального представлення мережі для контролера SDN, наприклад, Big Virtual Switch.

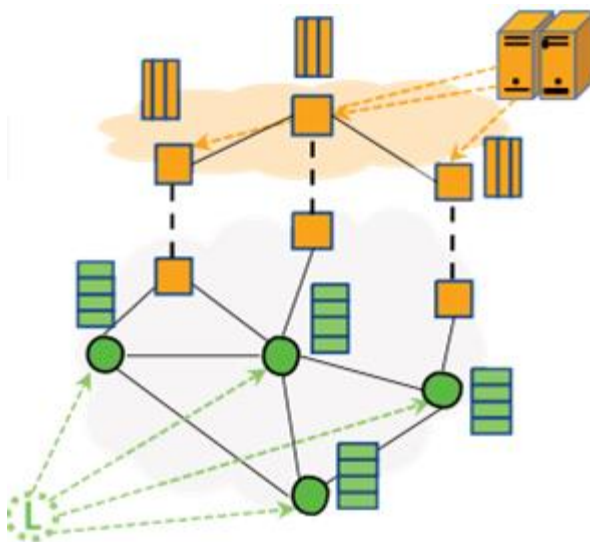


Рисунок 3.10 - Мережа основи HSL

Площина даних виконує обробку трафіку (наприклад, перевірку CRC, чергу QoS, оновлення TTL тощо) та пересилання трафіку на основі визначень керуючої площини. У мережах hSDN площина даних поєднує традиційні пристрої (зазвичай комутатори Ethernet рівня 2 (L2), маршрутизатори рівня 3 (L3) та інші апаратні пристрої) з послугами з підтримкою SDN, на основі прийнятої стратегії розгортання. Частина SDN площини даних складається з простих передавальних апаратів без архітектури або програмного пристрою, або програмного комутатору, або апаратного елементу, включаючи програмовані мережеві карти. P4 дозволяє програмістам визначати різноманітні протоколи та поведінку площини даних, які будуть реалізовані у вузлах, не залежачи від виробників для впровадження нових функцій.

3.2 Острівна модельна пропозиції для КМ ТОВ «Sollar»

У моделі, заснованій на островах, мережа топологічна розбита на області, що складаються лише із застарілих вузлів, тоді як інші області топології мають лише

SDN-вузли. Вони пропонують острівний підхід для розгортання нової служби високошвидкісного з'єднання (в 100 разів швидше, ніж зазвичай) для аутентифікованих користувачів. Ця модель може бути реалізована в ТОВ «Sollar», і представлена на рис. 3.11.

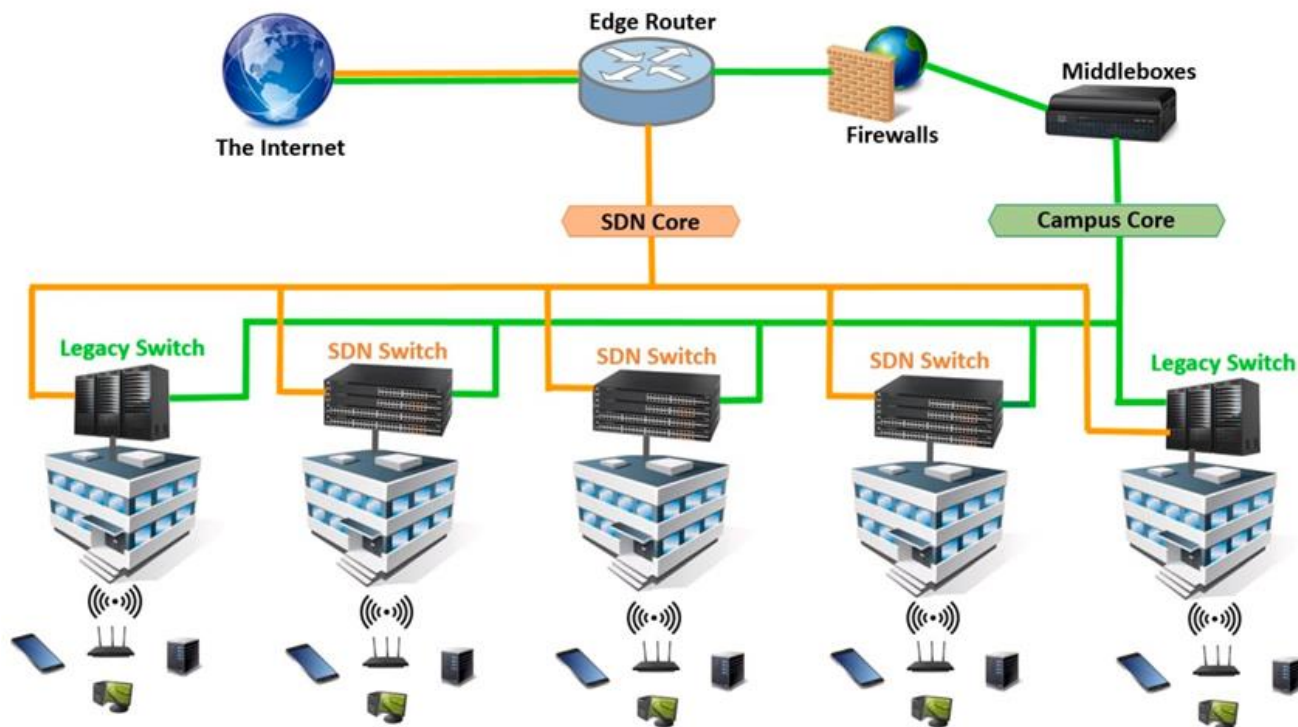


Рисунок 3.11 - Перспективна острівна модель мережі для ТОВ «Sollar»

Частина будівель ТОВ «Sollar» використовує мережі на основі SDN, тоді як інші використовують застарілі моделі пристроїв Cisco.

Щоб спрямувати трафік із застарілих мереж до мережі SDN, слід розробити новий модуль контролера, призначений для зв'язку із застарілими комутаторами за допомогою маршрутизації на основі політик (PBR).

Ключовою ідеєю в цьому підході є інтеграція прикордонних BGP-роутерів, які мають високу ціну і продуктивність, з SDN, які і раніше працюють так само, як і в інтернеті. Маршрутизатори у міждоміній маршрутизації використовують протокол зовнішнього прикордонного шлюзу (eBGP), тоді як вони запускають внутрішній прикордонний шлюз з протоколом (iBGP).

Можна запропонувати архітектуру під назвою «OpenRouteFlow». OpenRouteFlow забезпечує централізований контроль над застарілими вузлами шляхом оновлення програмного забезпечення застарілих вузлів за допомогою агента під назвою «OpenRoute-Flow». Цей агент передає інформацію про

розподілену маршрутизацію контролеру. Крім того, агент OpenRouteFlow отримує, в принципі, інструкції управління, орієнтовані на додаток, від контролера за допомогою повідомлень OF, які потім відображаються в операціях ACL і QoS маршрутизатора.

Також можливий додатковий випадок, коли вузол SDN оновлюється за допомогою застарілого агента. В літературі пропонується застосовувати архітектуру «IGP-as-a-Backup SDN». З одного боку, контролер налаштовує маршрут за допомогою протоколу OF і використовує переваги оптимальної роботи мережі в довгостроковій перспективі. З іншого боку, застарілий агент буде резервні шляхи за допомогою протоколу OSPF. Щоразу, коли відбувається збій мережі, агент Inter Gateway Protocol (IGP) швидко відновлює з'єднання, використовуючи інформацію про локальну маршрутизацію. Таким чином, збої в мережі усуваються швидше, ніж у чистій мережі SDN.

Відомі також рішення де пропонують застосування гібридного перемикача з частковим делегуванням базового мосту та новими механізмами співпраці між контролером та цими перемикачами. Режим обробки потоку за замовчуванням виконується з використанням застарілого протоколу L2. Контролер SDN також може встановлювати правила переадресації на перемикачах.

Нарешті, існує режим «кооперативної» обробки потоку, заснований на тому факті, що контролер знає роботу перемикачів, він може допомогти з деякими конкретними завданнями завдяки своїм глобальним знанням основної роботи, наприклад, для обчислення шляхів відновлення або для допомоги у відновленні таблиць маршрутизації Linux (рис. 3.12).

Площина пересилання вузла OSHI з підтримкою SDN реалізована за допомогою OvS, програмного фреймворку, який реалізує швидкий шлях пересилання в ядрі Linux. Застаріла IP-маршрутизація реалізована за допомогою комбінації IP-мережі ядра Linux і Quagga, який виступає в ролі демона маршрутизації.

Однак, незважаючи на свій великий потенціал, прийняття P4 в гібридні середовища все ще дуже обмежений.

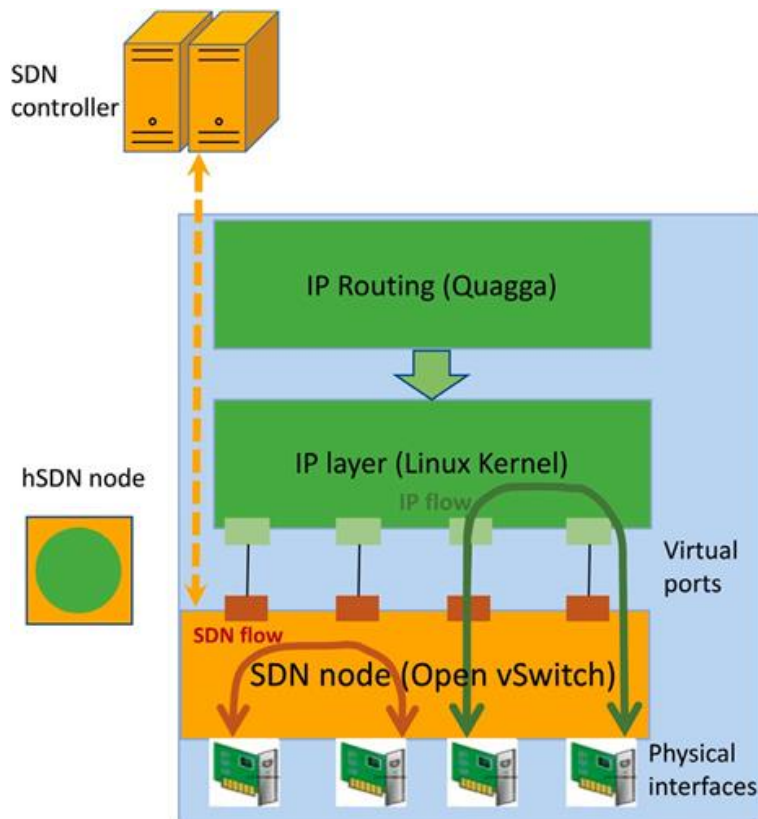


Рисунок 3.12 - Гібридна архітектура вузлів OSHI IP/SDN

3.3 Комплекс технічних засобів комп'ютерної системи

3.3.1 Технічні вимоги до КС

3.3.1.1 Вимоги до системи в цілому

3.3.1.1.1 Структура і функціонування системи

КС ТОВ «Sollar», призначена для підтримки бізнес-операцій підприємства.

Структурно КС ТОВ «Sollar» складається з наступних підсистем:

- підсистема передачі інформації користувача;
- підсистема зберігання даних;
- підсистема доступу до загальних ресурсів;
- підсистеми управління передачею та прийомом інформаційних повідомлень;
- система управління;
- система моніторингу інформаційного трафіку;
- системи безпеки.

Цілями розвитку КС ТОВ «Sollar» є:

- підвищення гнучкості та зручності використання КС за рахунок створення сучасної децентралізованої архітектури;
- зменшення затрат на підключення та на обслуговування;
- зменшення інформаційного навантаження на КС за рахунок апаратних пристроїв, що контролюють передачу повідомлень;
- удосконалення механізмів контролю та моніторингу процесу міжвідомчого інформаційного обміну;
- методологічна підтримка для всіх учасників обміну в електронному вигляді;
- підвищення якості та доступності інформації, що передається.

3.3.1.1.2 Чисельність і кваліфікація персоналу і режим роботи

Персонал, залучений до встановлення, налаштування та експлуатації КС ТОВ «Sollar», повинен мати відповідні сертифікати, ліцензії та дозволи.

Кількість персоналу, залученого до встановлення, налаштування та експлуатації цих систем, визначається відповідно до експлуатаційної документації постачальника, нормативних вимог та вимог до рівня послуг, що надаються з використанням цих систем.

3.3.1.1.3 Надійність і безпека

Всі компоненти КС ТОВ «Sollar» повинні бути надлишковими, що значно підвищить надійність і збереже працездатність КС та цілісність даних у разі часткових відмов ПЗ та апаратних мережевих засобів.

Розробити та доопрацювати в рамках підтримки операції з МРЗ.х. Для підсистеми повинні бути визначені кількісні значення наступних показників надійності.

Загальний режим роботи - 24 години на добу, 7 днів на тиждень - Сумарний допустимий час простою на тиждень, включаючи технічне обслуговування та регламентні роботи при суворому дотриманні регламентних процедур, не повинен перевищувати 30 хвилин.

Детальні вимоги до надійності системи повинні бути визначені на етапі проектування.

Інтерфейс користувача для наступних підсистем буде створено у вигляді веб-інтерфейсу для адміністративної підсистеми, що містить журнал. Остаточний веб-інтерфейс буде адаптований до мінімальної ширини 1280 пікселів. Переходи користувачів між усіма веб-сторінками інтерфейсу здійснюватимуться за допомогою системи навігації, що включає гіперпосилання та інші елементи переходу між сторінками. Остаточний веб-інтерфейс вищезгаданої підсистеми повинен працювати і коректно відображатися в наступних браузерях:

- Microsoft Internet Explorer версії 10 та вище;
- Mozilla Firefox версії 27 та вище;
- Google Chrome версії 28 та вище.

3.3.1.1.4 Експлуатація, технічне обслуговування, ремонт, збереження

На етапі, коли КС ТОВ «Sollar» повністю функціонує, її обслуговуванням повинен займатися системний адміністратор. Ремонт КС повинен здійснюватися спеціалізованим підрядником. Несправні елементи КС повинні бути замінені на нові. Вимоги до методів і засобів зв'язку для обміну інформацією між компонентами КС повинні бути забезпечені відповідно до документації виробника КС та протоколів випробувань, проведених в процесі експлуатації.

3.3.1.1.5 Захист інформації

Доступ до апаратних засобів КС ТОВ «Sollar» повинен бути обмежений технічними та організаційними заходами.

Доступ до елементів повинен бути персоналізованим та обмеженим. Виконані роботи повинні реєструватися. Повинні бути вжиті організаційні та технічні заходи для захисту інформації та запобігання її втраті у разі збою або переривання роботи.

Для забезпечення можливості резервного копіювання та відновлення інформації повинні використовуватися стандартні ПЗ постачальника рішення та / або сторонні засоби з урахуванням вимог до захисту інформації.

У ТОВ «Sollar», де періодично циркулює інформація з обмеженим доступом, слід використовувати спеціалізовані приміщення, комп'ютери, копіювально-

розмножувальну техніку, а також застосовувати апаратні рішення для інформації з обмеженим доступом. Це інформація, що міститься в бухгалтерських книгах, інформація, що описує планові та фактичні показники фінансового планування, інформація про баланс компанії, інформація про стан майна, бюджети, показники продажів, інформація про рух грошових коштів компанії, банківські операції, інформація про фінансові операції, банківські відносини, стан банківських рахунків та операцій компанії, операції з продажу, дані планування та звітності, зобов'язання та інша інформація. Сюди також входить заробітна плата та інші грошові кошти, які є матеріальними активами.

Основними загрозами для діяльності ТОВ «Sollar» є фальсифікація, перешкоджання або знищення цієї інформації, пошкодження або знищення майна чи матеріальних цінностей, нанесення шкоди працівникам, організація нещасних випадків або сприяння виникненню професійних чи інших захворювань.

3.3.1.1.6 Патентна чистота

В комп'ютерній КС ТОВ «Sollar» використовуватися елементи та пристрої, ПЗ ліцензовані та сертифіковані для використання на території України.

3.3.1.1.7 Стандартизація й уніфікація

КС ТОВ «Sollar» повинна бути розроблена в рамках рекомендації зі стандартизації «Інформаційні технології для підтримки життєвого циклу продукції.

Методологія функціонального моделювання». КС повинна відповідати визнаним міжнародним стандартам у галузі розробки інформаційних систем.

3.3.2 Забезпечення

3.3.2.1 Інформаційне забезпечення

ПЗ КС ТОВ «Sollar» надається в електронному форматі Flash-носіях та / або засобами для завантаження через мережі передачі даних. У разі випуску оновлених / модифікованих версій ПЗ, ці оновлені версії ПЗ повинні бути своєчасно встановлені відповідно до чинних правил експлуатації.

Слід використовувати криптографічний шлюз, який призначений для

забезпечення криптографічного захисту під час передачі інформації загальними каналами зв'язку та захисту внутрішнього сегмента VPN від зовнішнього вторгнення.

Криптографічні шлюзи повинні забезпечувати:

- прийом і передачу IP-пакетів за протоколом TCP/IP;
- фільтрацію IP-пакетів відповідно до заданих правил фільтрації;
- ширококомовну трансляцію мережевих адрес відповідно до заданих правил ширококомовної трансляції (NAT);
- криптографічну трансляцію відправлених і отриманих IP-пакетів;
- захист від підробки IP-пакетів, що проходять в VPN;
- приховування внутрішньої структури захищеного сегмента мережі;
- сповіщення в реальному часі про події, що потребують активності та оперативного втручання центру управління мережею криптографічного шлюзу;
- протоколювання подій, пов'язаних з роботою ПЗ криптографічного шлюзу;
- ідентифікація та аутентифікація адміністратора при запуску ПЗ криптографічного шлюзу;
- контроль цілісності ПЗ криптографічного шлюзу;
- робота в режимі «гарячого резерву» (крім криптографічного шлюзу).

3.3.2.2 Технічне забезпечення

Технічне обладнання КС ТОВ «Sollar» повинно бути встановлене в серверній кімнаті з системами контролю доступу та сигналізації. Приміщення повинно мати виділене та гарантоване електропостачання та систему кондиціонування; фізичний доступ персоналу до технічних засобів КС ТОВ «Sollar» повинен бути регламентований та обмежений технічними та організаційними засобами; повинна використовуватися група електроживлення, яка забезпечує всі необхідні джерела живлення для забезпечення функціонування технічних засобів КС ТОВ «Sollar».

Повинна використовуватися група електроживлення, яка забезпечує всі необхідні параметри електроживлення для забезпечення роботи технічних засобів КС ТОВ «Sollar»:

- напруга 220 (-40; +33) В однофазного змінного струму;

- частота 50 Гц, коефіцієнт гармоніки не повинен перевищувати $\pm 5\%$.

Загальна потужність, що подається, повинна відповідати розрахунковому енергоспоживанню; для забезпечення безперервної роботи технічних заходів КС ТОВ «Sollar»: має бути встановлене автономне джерело безперебійного живлення.

3.3.2.3 Організаційне забезпечення

Встановлення, підключення та початкове налаштування технічних засобів КС ТОВ «Sollar» здійснюється персоналом з відповідними навичками та компетенцією.

Слід ретельно переконатися, що КС ТОВ «Sollar» встановлюється фахівцями, які мають відповідні навички та компетенції, підтверджені відповідними сертифікатами. Доступ до підсистеми управління повинен бути обмежений і захищений особистими обліковими даними фахівця.

Усі конфігураційні роботи та зміни параметрів КС ТОВ «Sollar» повинні бути належним чином зареєстровані. Взаємодія з системою моніторингу повинна бути забезпечена під час інсталяції системи.

Доступ до системи моніторингу повинен бути наданий експерту, відповідальному за контроль працездатності системи; він повинен надати план дій щодо реагування на інциденти, проблеми або нещасні випадки, пов'язані з роботою КС ТОВ «Sollar».

3.3.2.4 Нормативно-технічна документація

Звітні документи подаються замовнику українською мовою на паперових носіях та в електронному вигляді (Flash-носій). Супровідні документи (ті, що не визначені як безпосередній результат роботи) подаються тільки в електронному вигляді. Технічна та експлуатаційна документація КС ТОВ «Sollar» розробляється відповідно до вимог комплексу стандартів та керівних документів на автоматизовані системи.

3.3.3 Апаратні засоби КС ТОВ «Sollar»

3.3.3.1 Загальні відомості

В КС ядро мережі забезпечує зв'язок і резервування для всіх компонентів мережі.

Як правило, це високопродуктивний комутатор L2/L3 з мінімальною функціональністю, достатньою для комутації/маршрутизації всього трафіку в мережі. Інші мережеві елементи з більшою функціональністю можуть використовуватися лише на рівні ядра.

Прикладами є прикордонні маршрутизатори та сервісні шлюзи (NAT, BNG, DPI, NGFW). Додаткові функції, що виходять за рамки забезпечення повного зв'язку в межах приватної мережі, виходять за рамки обговорення.

Тенденції ринку мережевого обладнання:

1. Підвищення продуктивності. Мабуть, найбільш очевидною тенденцією є збільшення обсягу інформації, що безпосередньо впливає на вимоги до продуктивності мережі: Стандарт 800GBASE-R буде аносований у 2020 році і незабаром буде розгорнутий у найбільших дата-центрах Стандарт 800GBASE-R буде аносований у 2020 році і незабаром буде розгорнутий у найбільших дата-центрах. Тим часом, комутатори 32x400GE стають все більш доступними, а стандарт 25/100GE поступово витіснить 10/40GE за порівнянними цінами. У той же час, 10GE дешевшає в мережах кампусів, а гігабітні аплінки на рівні доступу стають все менш поширеними. Продуктивність комутаторів доступу до кампусних мереж також покращується, оскільки на ринку з'являється все більше комутаторів 2.5GE. Це збільшує щільність каналів радіо-доступу і вирішує деякі проблеми з буферизацією трафіку.

2. Децентралізація. Розширюється асортимент «голих» комутаторів та комутаторів з «білими коробками». Розробники пропонують нові мережеві операційні системи, які можна встановлювати на різні платформи. Розподілені рішення становлять інтерес для підприємств. Вони привабливі тим, що апаратне забезпечення комутатора можна замінити без необхідності купувати нове обладнання, в будь-який момент змінити постачальника апаратної платформи і підтримувати сумісність з певним програмним забезпеченням. Звичайно, багато

хто віддає перевагу перевіреним закритим рішенням. Але в міру того, як інженери з інтеграції ставатимуть більш компетентними, вони будуть більше довіряти новим підходам.

3. Поширення вільного програмного забезпечення. Стрімке зростання індустрії багато в чому пов'язане з ентузіастами, які вільно поширюють те, що вони розробили. У майбутньому технології розвиватимуться за підтримки користувачів. Лідери індустрії не залишаться осторонь і відкриватимуть свої розробки з відкритим вихідним кодом. Це дозволяє їм створювати спільноти для спільної розробки та продавати професійні послуги, а не саме програмне забезпечення.

Деякі розробки з відкритим кодом включають операційні системи для комутаторів:

- у 2017 році вийшла SONiC від Microsoft, орієнтована переважно на центри обробки даних;
- у 2019 році AT&T запропонує безкоштовну версію DANOS для операторів зв'язку;
- у 2020 році підтримка дешевших комутатори 1/10GE;
- випуск DentOS 1.0, яка забезпечує основну функціональність для мереж кампусів.

Ці ініціативи були підтримані як споживачами, так і виробниками обладнання, що використовують програмне забезпечення з відкритим вихідним кодом як платформу. Такі ініціативи, спрямовані на вільне розповсюдження програмних і апаратних платформ, привернули увагу широкої професійної спільноти.

Великі спільноти об'єдналися під керівництвом таких проектів, як Open Compute Project, Open Networking Foundation та Telecom Infra Project. Ці спільноти об'єднують, обговорюють і знаходять рішення різних галузевих проблем, а також планують їх розвиток і просування.

3.3.3.2 Маршрутизатор C921-4P

Маршрутизатори використовуються як пристрої на межі підприємства, підключаючись до обладнання провайдера через виту пару, коаксіальний кабель,

телефонний кабель (xDSL), оптоволокну, потоки E1/T1, бездротові (3G, 4G, 802/b/g/n) і WAN інтерфейси,

Для резервування і балансування можуть використовуватися кілька WAN портів в залежності від моделі маршрутизатора. LAN інтерфейс маршрутизатора підключається до локальної мережі.

Використовуючи NAT і PAT, кілька пристроїв в мережі КС можуть бути підключені до одного або декількох глобальних статичних або динамічних адрес.



Рисунок 3.13 – Зовнішній вигляд маршрутизатора C921-4P

C921-4P - це високозахищений маршрутизатор Cisco 921 Gigabit Ethernet з вбудованим блоком живлення. Інтегрований захист від загроз захищає вашу мережу від відомих і нових вразливостей та атак в Інтернеті.

Потужний маршрутизатор забезпечує безпечне широкосмугове з'єднання, бездротове з'єднання Metro Ethernet і LTE WAN.

Централізоване управління і можливості віддаленого керування за допомогою веб-інструментів і програмного забезпечення Cisco IOS забезпечують повну видимість і контроль конфігурації мережі на віддалених об'єктах. Маршрутизатори серії 900 забезпечують наскрізну експлуатацію, управління та обслуговування (O&M), моніторинг перевірки відповідності угоди про рівень обслуговування (SLA) і управління конфігурацією, спрощуючи розгортання послуг Ethernet WAN Cisco ISR 900 має чотири-портовий керований інтерфейс, який надає порти LAN для підключення декількох пристроїв.

Таблиця 3.1 - Особливості маршрутизатора Cisco C921-4P [12]

Код товару	C921-4P
Інтерфейси WAN	2 порти Gigabit Ethernet (GE)
Інтерфейси локальної мережі	4-керовані комутатор порту GE
Вбудований порт USB 2.0	Yes
Оперативна пам'ять за замовчуванням і максимальна	За промовчанням 1 GB
За замовчуванням і максимальний обсяг флеш-пам'яті	2 GB; не підлягає оновленню
Розміри (В x Ш x Г)	1.70 x 9.0 x 9.5 in. (4.32 x 22.86 x 24.13 см) (У комплекті гумові ніжки)

3.3.3.3 маршрутизатора Cisco 891

Пристрої безпеки дозволяють захистити доступ до Інтернету, контролювати доступ до зовнішніх ресурсів, переглядати тарифікацію зовнішнього трафіку, призначати та захищати DMZ, здійснювати виявлення / запобігання вторгненням, створювати безпечні тунелі між філіями компанії з розподіленою інфраструктурою, а також надавати безпечний доступ мобільним користувачам. Це дозволяє забезпечити наступне.



Рисунок 3.14 – Зовнішній вигляд маршрутизатора Cisco 891

Таблиця 3.2 - Характеристики маршрутизатора Cisco 891 [12]

Бренд:	Cisco
Тип пристрою:	Маршрутизатор (роутер)
Вхід (WAN порт):	1x 10/100/1000 BASE-T Ethernet, 1x 10/100 BASE-T Ethernet, 1x SFP WAN
Інтерфейс підключення (LAN-порт):	8x 10/100/1000 BASE-T Ethernet
Маршрутизатор	
Брандмауер (Firewall):	є
NAT:	є
Підтримка VPN (віртуальних мереж):	є
DHCP-сервер:	є
Демілітаризована зона (DMZ):	є
Моніторинг та конфігурування	
Веб-інтерфейс:	є
Telnet:	є
Підтримка SNMP:	є
Додатково	
Живлення (PoE/адаптер):	+/+
Можливість встановлення поза приміщенням:	немає
Режим моста:	немає
Інше:	1x USB 2.0; стандартна пам'ять: 512 Мб (максимальна пам'ять: 768 Мб); флеш-пам'ять: 256 Мб
Розміри (мм):	46,2x322,8x248,4
Вага (г):	2500

3.3.3.4 Комутатора Catalyst 2960

Комутатори дозволяють об'єднати мережеві пристрої, такі як ПК, сервери, IP-телефони, принтери та сканери, в єдину мережеву область.

Залежно від призначення комутатора (доступ, агрегація, ядро або серверна ферма), він підтримує роботу на рівнях 2 і 3 ISO/OSI і маршрутизує пакети при поділі мережі на сегменти.



Рисунок 3.15 – Зовнішній вигляд комутатора Catalyst 2960

Таблиця 3.3 - Технічні характеристики комутатора Cisco WS-C2960-24-S [13]

Виробник:	Cisco
Ідентифікатор товару:	WS-C2960-24-S
Опис продукту:	24 порти Ethernet 10/100, програмне забезпечення LAN Lite
Тип продукції:	Комутатор Ethernet
Кількість мережевих (RJ-45) портів:	24
Порт/слот розширення	24 x Fast Ethernet Network
Підтримуваний тип носія:	Кручена пара
Технологія Ethernet:	Швидкий Ethernet
Мережеві технології:	10/100Base-TX
Підтримувані шари:	2
Управління та протоколи	
Керованим:	Yes
Управління:	GUI, Telnet, SNMP, RMON, CiscoView, Device manager, Cisco Network Assistant, Cisco IOS command-line interface (CLI)
Вхідна напруга:	110 V AC; 220 V AC
Фізичні характеристики	1.7"x17.5"x9.3"
Вага (орієнтовна):	8 lb
Комплектація:	<ul style="list-style-type: none"> • Керований комутатор Ethernet Catalyst 2960-24-S • Посібник із початку роботи з перемикачем • Відповідність нормативним вимогам та інформація про безпеку для перемикача Catalyst 2960 • Шнур живлення змінного струму • 4 x гумові ніжки • 2 x 19-дюймові кронштейни для монтажу в стійку (також використовуються для настінного монтажу) • 6 x хрестоподібних гвинтів з плоскою головкою для кріплення кронштейнів до перемикача • 4 x хрестоподібні машинні гвинти для кріплення кронштейнів до стійки • 1 x Кабельна Провідник • 1 x Машинний гвинт Black Phillips для кріплення направляючої кабелю до одного з монтажних кронштейнів • 4 x гвинти з хрестоподібною головкою (для настінних кронштейнів)

3.3.3.5 Компоненти КС ТОВ «Sollar»

3.3.3.5.1 Сервери

Мережевий сервер - це потужний комп'ютер, розроблений для керування мережевими ресурсами та надання послуг іншим комп'ютерам, відомим як клієнти, у мережевих умовах. На відміну від звичайної робочої станції, мережевий сервер призначений для виконання мережевих завдань, таких як зберігання даних, хостинг додатків, обробка електронної пошти тощо.

Від невеликих локальних мереж у бізнес-середовищі до величезних хмарних інфраструктур – мережеві сервери є стрижнем, який забезпечує плавний поворот колеса інформації та послуг. Вони дозволяють централізувати дані та програми, полегшуючи керування, обслуговування та безпеку критично важливих організаційних активів.

Це переважаюча архітектура для сучасних комунікацій, завдяки якій цифрові дані пропонуються серверами клієнтам. Альтернативна модель, відома як реєр-to-реєр або «P2P», покладається на комп'ютери, які підключаються один до одного для обміну даними. На відміну від моделі P2P, архітектура клієнт-сервер спирається на головну серверну машину або набір машин, підключених до мережі, як правило, в центрі обробки даних. Клієнти або звичайні комп'ютери, підключені до Інтернету або локальної мережі, відправляють пакети для запиту даних з сервера. Коли сервер отримує ці запити, він може зробити одну з трьох речей: прийняти пакет, відхилити або «скинути» пакет або тихо завершити з'єднання.

Покладаючись на використання «портів» для керування потоком даних, клієнти та сервери повинні надсилати запити один одному та один від одного на правильні порти. Більшість брандмауерів налаштовані на прийом різного роду запитів. Наприклад, більшість серверів, що використовують протокол передачі гіпертексту (НТТР), приймають запити на отримання даних лише через порт 80 або 443. Відправка пакетів від клієнта на правильно налаштований сервер на інший порт, сервер, як правило, безшумно скидає надіслані пакети.

В табл. 3.4 представлені технічні показники для серверів КС ТОВ «Sollar».

Таблиця 3.4 - Характеристики ПК та серверів

Найменування	Характеристики
ПК 1 – ПК 130	Материнська плата: Asus P8H77-V LE Процесор: Intel core i5 Відео адаптер: Gigabyte readeon HD6570 2048mb HDD: Seagate 1000Gb 64 MB DVD привод: Asus DRV-24x Оперативна пам'ять: Kingston DDR-4 PC-3 8 Gb Блок живлення: AeroCool VP750W Корпус: Metal Master SG2 Монітор: Samsung PN22” Клавіатура: BTC Keyboard120 Мишка: Logitech LTC-19
ПК 131-220	HDD: Seagate 320Gb 64 MB DVD привод: Asus DRV-24x Оперативна пам'ять: Kingston DDR4 PC-3 2 Gb Блок живлення: AeroCool VP500W Корпус: LogicPower SK789-2 Монітор: Samsung E1920 Клавіатура: BTC Keyboard120 Мишка: Logitech LTC-19
Шлюз та Firewall	2 процесора Intel Xeon "Multi Core"; чіпсет Intel i5000V, 2xPCI-E 8x, 2xPCI-X 64bit/133MHz; 8 GB ECC DDR4 667 FBD (4/8 DIMMs); відеокарта ATI Rage Pro 16Mb onboard; блок живлення 750W Fi;
Web- сервер	2 процесора Intel Xeon "Multi Core"; чіпсет Intel i5000V, 2xPCI-E 8x, 2xPCI-X 64bit/133MHz; 16 GB ECC DDR4 667 FBD (4/8 DIMMs); блок живлення 800W Fiber blue;
Контролер домена	Процесор Intel C202, 1xLGA1155, RAM: 8 GB DDR3 1600MHz ECC Unbuffered, 1xHDD Seagate 320Gb SATA 3Gb/s. Intel C202 (RAID levels: 0,1,5,10), Intel graphic mode video
Файловий сервер	Процесор: Intel Xeon E5-2650; 2,0 GHz; Кількість процесорів встановлених/максимально: 2/2; пам'ять: 32 GB; жорсткий диск: 6 x 2000GB; SATA/SAS; мережевий адаптер: 4xGigabit Ethernet
Storage	Процесор - Intel Xeon E5-2650 (6 ядер), 2.0 ГГц Ram: 16 Гб LAN: 1 Гбіт/с / LAN (RJ-45) - 2 шт. HDD: Seagate 1000Gb-SATA Hot Plug. БП - 520 Вт

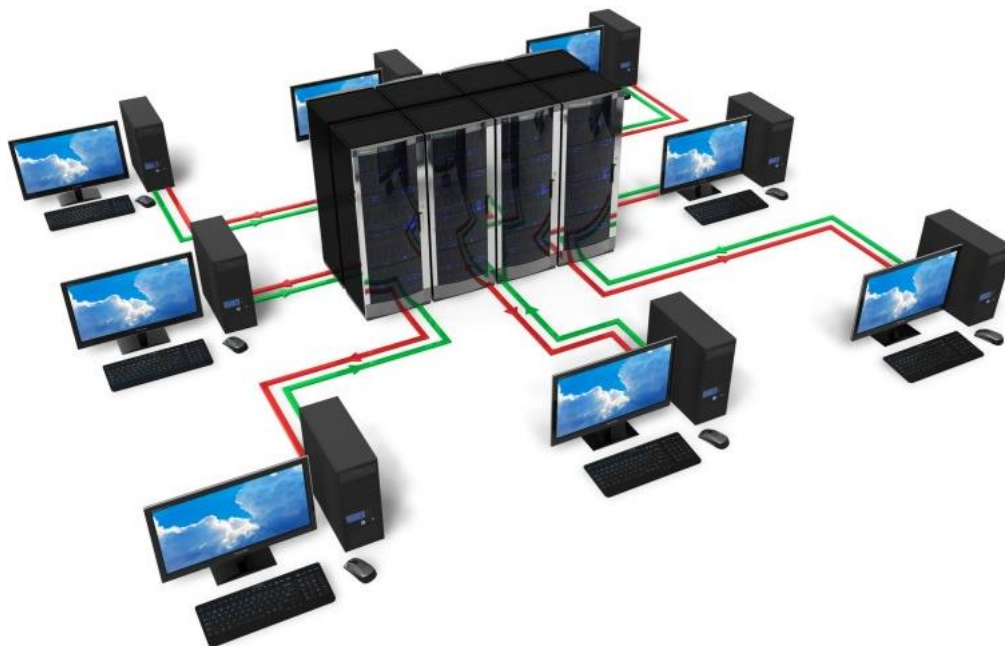


Рисунок 3.16 - Архітектура клієнт-сервер

3.3.3.5.2 Мережеве обладнання

В табл. 3.5 представлені технічні показники для мережевого обладнання КС ТОВ «Sollar».

Таблиця 3.5 - Характеристики мережевого обладнання

Найменування	Характеристика	Кількість, од.
C921-4P - маршрутизатор з високим рівнем безпеки Cisco 921 Gigabit Ethernet з внутрішнім джерелом живлення	Cisco ISR 900 поставляються з 4-портовим керованим інтерфейсом, що надає порти локальної мережі для підключення декількох пристроїв.	5
Комутатор Catalyst WS-C2960+48PST-S від компанії Cisco -	керований комутатор з 48 фіксованими 10/100 Fast Ethernet портами, 2 10/100/1000 Gigabit Ethernet та 2 SFP аплінки, встановлене ПЗ - LAN Lite	8
Кабель UTP кат.5е	Довжина 1305 м; 4 пари; оболонка FR-ПВХ (IEC 332.1); діаметр провідника з ізоляцією не більше ніж 0,001 м; діаметр кабелю не більше ніж 0,005 м	2

3.4 Висновки за розділом

В частині розділу синтез системи розглянуті інженерно-технічні заходи для здійснення синтезу комп'ютерної КМ ТОВ «Sollar».

4 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

4.1 Призначення й сфера застосування програми

Сучасні комп'ютерні системи є більш складними, швидше розвиваються і більш важливими для ведення бізнесу, ніж ті, що були навіть кілька років тому. Результатом є зростаюча потреба в інструментах і методах, які допомагають зрозуміти поведінку цих систем. Таке розуміння необхідне для того, щоб дати розумні відповіді на питання вартості та продуктивності, які виникають протягом усього терміну служби системи.

Дослідження людей, речей або інформації по лінії зв'язку вдало забезпечується за допомогою теорією масового обслуговування.

Затори та їх причини досліджуються при розробці більш практичних та економічно ефективних послуг та інфраструктури в теорії масового обслуговування.

Теорія черги, яка часто застосовується як техніка управління операціями, допомагає з підбором мережевого обладнання, плануванням інформаційних навантажень на мережу.

Теорія масового обслуговування - це специфічний розділ математики, який зосереджений на вивченні черг (черг) в тих випадках, коли спостерігається перевищення попиту на ту чи іншу послугу в порівнянні з наявністю послуги. Це дає можливість розглянути та проаналізувати поведінку систем, які стикаються з перевантаженнями як звичайне явище - комп'ютерні мережі, транспорт тощо.

Спостерігаючи за довжиною черги, часом очікування клієнтів і використанням сервера, моделі черги можуть стати надзвичайно корисними для управління ресурсами та підвищення продуктивності систем.

У корпоративному світі деяке чергування є достатнім для належного управління системою. Мета теорії масового обслуговування полягає в тому, щоб знайти баланс, який був би одночасно ефективним і економічно вигідним.

У хмарних обчисленнях теорія масового обслуговування використовується для аналізу комп'ютерної системи та мережі зв'язку. Простими словами, це

спрощена математична модель для пояснення перевантаження в комп'ютерних мережах.

Теорія масового обслуговування надає глосарій та інструментарій для наближення програмних систем з моделями, міркування про їх поведінку, розуміння даних, які збираються, і кращого вивчення потрібних методів. Ці методи особливо актуальні, коли інфраструктура розподілена, динамічна масштабується і сильно паралельна, що і є властивостями хмарних обчислень.

Є розроблені фреймворк хмарних обчислень для додатків IoT, чутливих до затримок, де активно використовується теорія масового обслуговування для контролю потоку даних по мережах. Запропоновано механізм розподілу завдань для середовища мобільних периферійних обчислень (MEC) [15].

У кваліфікаційній роботі магістра на тему «Обґрунтування структури та параметрів комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування» використаємо математичну модель КС для оцінки її продуктивності різних режимах інформаційного навантаження.

Базова модель теорії масового обслуговування така ж сама, як і в комп'ютерних мережах. Кожна комп'ютерна підмережа представляється у вигляді набору серверів, таких як центральні процесори, пристрої вводу / виводу інформації, кожен з яких має власну чергу на обслуговування інформаційних потоків.

Розроблене ПЗ насамперед призначено для розрахунку безрозмірних параметрів математичної моделі для комп'ютерної мережі ТОВ «Sollar» на основі моделі мережі масового обслуговування (ММО) у вигляді замкненої мережі, яка визначає довжину черги на обслуговування інформаційних пакетів даних.

ПЗ розроблено як базове для спостереження та огляду статистичних методів, які зазвичай використовуються для представлення продуктивності комунікаційних компонентів мереж та інших систем, заснованих на стохастичних процесах.

У кваліфікаційній роботі представлено багато-протокольну комутацію з мітками (MPLS), яка використовується як приклад для оцінки продуктивності сучасних багато-потоківих мереж. Введено деякі базові розподіли для

моделювання розподілу між прибуттями та відправкою інформації для мережевого пристрою.

В роботі представлено метод проектування більш складних процесів з використанням математично розв'язуваних ланцюгів Маркова. На цій основі в розділі розроблено базову модель черги.

Сферою застосування програми є математичне моделювання комп'ютерної мережі ТОВ «Sollar» з використанням цієї математичної мережевої моделі.

4.2 Параметри програми

Теорія масового обслуговування - це розділ математики, який використовується для опису, аналізу та прогнозування довжини черг і часу очікування в системі. Має на увазі розробку моделей процесу прибуття, процесу обслуговування та дисципліни черги моделі. Потім ці моделі кількісно оцінюються, а отримана теорія ймовірності та стохастичні процеси використовуються для розрахунку інших критеріїв ефективності, включаючи середнє число клієнтів, які містить система, середній час, який клієнт проводить в очікуванні в системі, і ймовірність того, що клієнт чекатиме на обслуговування.

Системи черг для мережевих ланцюгів використовуються для формулювання обміну ресурсами та визначення пріоритетів потоків, щоб зменшити можливість перевантаження мережевого обладнання.

Припускається, що проблему масштабованості можна вирішити, додавши до ієрархії управління загальний віртуальний мережевий рівень, і що алгоритми, які дозволяють автономне розділення мережі, можуть бути реалізовані з розумними обчислювальними зусиллями. Використання цього програмного забезпечення призвело до деяких позитивних результатів:

- обчислює середній час очікування початку обслуговування;
- визначає середню довжину черги на обслуговування;
- визначає середню кількість сервісних пристроїв та їх завантаження.

Припускається, що основна проблема миттєвого попиту на зв'язок у випадку зловмисного ПЗ вирішується за допомогою попередньо розрахованої очікуваної

якості обслуговування для попередньо визначеного шляху в межах діапазону та оголошеного наскрізного шляху.

Потім ці моделі кількісно оцінюються, а отримана теорія ймовірності та стохастичні процеси використовуються для розрахунку інших критеріїв ефективності, включаючи середнє число пакетів, які містить мережа, середній час, який пакет проводить в очікуванні в мережі, і ймовірність того, що пакет чекатиме на обслуговування.

4.2.1 Завдання на розробку

Для математичних моделей мереж з використанням закритих черг ПЗ має розраховувати основні безрозмірні властивості комп'ютерних мереж, такі як:

- кількість вузлів у комп'ютерній мережі має бути не менше 16;
- матрицю часових ймовірностей повинна відповідати заданій структурній схемі мережі;
- кількість пакетів в обігу має бути не менше ніж 28;
- кількість конвеєрів обробки запитів на обслуговування має бути не менше 9;
- повинна бути передбачена можливість зміни відносного часу обробки пакетів у вузлу.

4.2.2 Операційне програмне забезпечення для робочого місця

Щоб апаратне забезпечення ПК працювало оптимально, необхідно спочатку встановити всі необхідні драйвери, ПЗ, а саме:

- операційну систему Windows 10 або більш новішої версії;
- Microsoft Office 2016 або новішої версії (MS Access має бути в комплекті);
- математичний пакет Mathcad 15 або більш новішої версії.

4.2.3 Вхідні і вихідні дані

Метод організації вхідних/вихідних даних розробленого програмного забезпечення походить від структурної схеми комп'ютерної мережі, що дозволяє аналізувати пропускну здатність комп'ютерної мережі. Оскільки результати

отримані на основі цієї моделі, вартість аналізу реальної комп'ютерної мережі може бути значно зменшена.

4.2.4 Склад програмних засобів

Технічними та програмними засобами для розробки програмного забезпечення, що дозволяє розраховувати безрозмірні параметри математичної моделі комп'ютерної мережі ТОВ «Sollar», є програмні засоби, розроблені для пакету Mathcad 15.

Для запуску програмного забезпечення для моделювання необхідно використовувати персональний комп'ютер, або notebook з наступною мінімальною конфігурацією:

- процесор Intel Core i5 (2 x 1,7 ГГц);
- жорсткий диск SCSI об'ємом 0,5ТБ;
- 4 ГБ оперативної пам'яті;
- кольоровий монітор діагоналлю 13 дюймів;
- відеокарта з роздільною здатністю екрану не менше 1 920 x 1 080 пікселів і режимом True Colour;
- зовнішні колонки (опціонально);
- мережевий порти швидкістю 100 Мб (опціонально);
- 1 вільний USB-порт (опціонально);
- wi-Fi (опціонально);
- операційна система (ОС) Windows 10.
- Mathcad 15.

4.3 Опис програми

4.3.1 Загальні відомості

ПЗ призначене для розрахунку безрозмірних параметрів математичної моделі комп'ютерної мережі у вигляді мережі із замкненою чергою. ПЗ розрахунку може зберігатися на будь-якому носії інформації.

4.3.2 Послідовність розрахунку

Для початку ПЗ моделі комп'ютерної мережі ТОВ «Sollar» треба встановити значення показників:

- задати кількість циркулюючих інформаційних пакетів в мережі;
- створити матрицю маршрутів PR;
- задати кількість конвеєрів для кожного вузлу: $M_0 \dots M_{11}$;
- середній час обробки інформаційного пакету в одному конвеєрі для кожної мережевого пристрою: $\tau_0 \dots \tau_{11}$;
- створення системи рівнянь в матричному вигляді.

Після цього ПЗ за допомогою методу Гауса отримає наступні показники:

- коефіцієнти передачі $e_0 \dots e_{11}$;
- множину $S(N, K)$, яка означає всі стани мережі;
- можливі стани $\{S_k\}$ для кожного мережевого пристрою, де k - кількість інформаційних пакетів у вузлу;
- ймовірності $P_i(n)$ станів для кожного мережевого пристрою;
- середню кількість інформаційних пакетів даних;
- вхідну інтенсивність;
- середній час перебування пакету у вузлу, обчислені згідно з теоремою Літгла.

4.3.3 Функціональне призначення

Розроблено програмне забезпечення з використанням булевих методів для дослідження математичних моделей ММО.

4.3.4 Опис логічної структури

Логічне програмне забезпечення розділене відповідно на три логічні модулі, які блокують початкові дані за замовчуванням та надають початкові значення для властивостей мережі:

- N - кількість інформаційних пакетів, що доставляються комп'ютерною мережею;
- матриця маршрутів PR;

- кількість трубопроводів для кожного вузла: $M_0 \dots M_{11}$;
- середній час обробки інформаційних пакетів у конвеєрі для кожного з вузлів: $\tau_0 \dots \tau_{11}$;
- коефіцієнти передачі $e_0 \dots e_{11}$;
- пошук множини $S(N, K)$ всіх станів мережі;
- обчислення середньої кількості інформаційних пакетів даних;
- обчислення вхідної потужності;
- використовуючи теорему Літтла обчислити середній час перебування інформаційного пакету у вузлу.

Вивести блоки:

- результати розрахунків у Mathcad у числовому форматі;
- результати розрахунків у Mathcad у графічному форматі.

4.3.4 Використовувані технічні засоби

Програмне забезпечення завантажується для розрахунку відповідно до параметрів комп'ютерної мережі, вказаних користувачем.

4.3.5 Цикл роботи програми

Робочий цикл програми визначається особливостями мови пакету Mathcad 15. Для зберігання великих масивів матриць вихідні дані записуються на жорсткий диск і в міру необхідності замінюються новими даними..

4.3.6 Вхідні та вихідні дані

Вхідними даними для мережевої комп'ютерної моделі ТОВ «Sollar» є наступні показники:

- N_n – кількість інформаційних вузлів мережі;
- τ – час обробки одного інформаційного пакету на вузол;
- P_r - це матриця перехідних ймовірностей;
- m – кількість конвеєрів у вузлах;
- N – кількість інформаційних пакетів циркулюючих в мережі;
- B – матриця ймовірностей черги у вузлах;

Вихідними даними для моделювання комп'ютерної мережі моделі ТОВ «Sollar» є наступне:

- λ – середня інтенсивність запитів на вході до інформаційного вузлу;
- L – середня черга інформаційних пакетів у вузлу;
- t – середній час перебування інформаційного пакету у вузлу;
- e – матриця коефіцієнтів переходів.

4.4 Висновок

У цій частині магістерської роботи розроблено ПЗ для обчислення безрозмірних параметрів математичної моделі для оцінки продуктивності комп'ютерної мережі ТОВ «Sollar».

Модель комп'ютерної мережі представлена у вигляді замкненої ММО і призначена для визначення черговості обслуговування інформаційних пакетів у вузлах мережі. Область застосування програми - математичне моделювання комп'ютерної мережі ТОВ «Sollar», представленою математичною моделлю.

5 ЕКСПЕРИМЕНТАЛЬНИЙ РОЗДІЛ

5.1 Розробка математичної моделі мережі ТОВ «Sollar»

Відповідно до структурної схеми комп'ютерної мережі ТОВ «Sollar» розроблено структуру математичної моделі мережі як замкнуту системи масового обслуговування, що представлена на рис. 5.1.

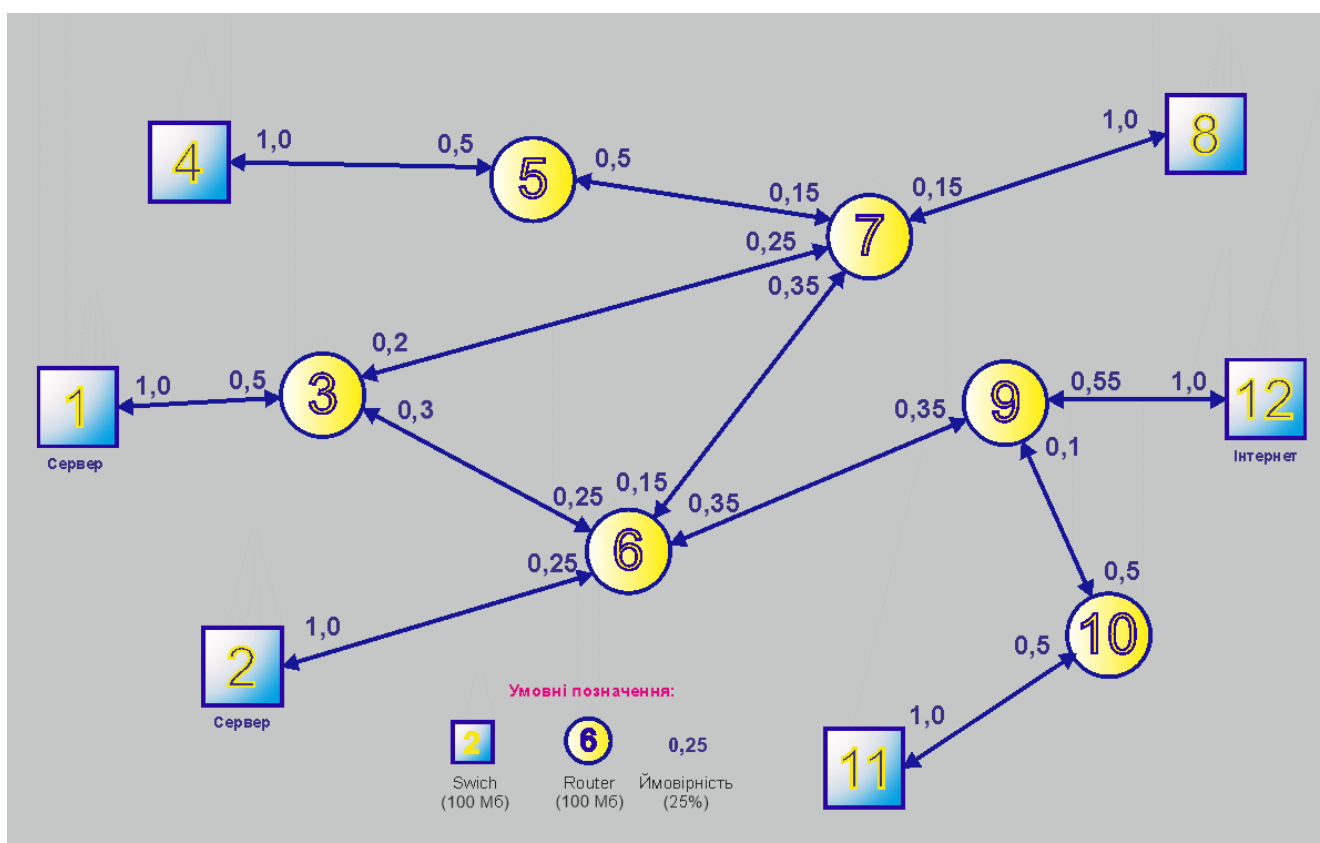


Рисунок 5.1 – Структура математичної моделі комп'ютерної мережі ТОВ «Sollar»

Структура моделі комп'ютерної мережі ТОВ «Sollar» відповідає реальній структурі мережі рівня підприємства комп'ютерної мережі ТОВ «Sollar», яка була розроблена у бакалаврській кваліфікаційній роботі.

Спрощена модель мережі ТОВ «Sollar» відображає ту ж саму архітектуру.

На схемі моделі мережі ТОВ «Sollar» позначено ймовірності для передачі інформаційних пакетів по каналах зв'язку між мережевими пристроями – свічами та роутерами, які були обрані відповідно інформаційної ентропії, можливі об'єми та напрямки інформаційної передачі, та в залежності від швидкості інформаційних каналів відповідно до параметрів існуючих в схемі мережевих пристроїв, джерел яке продукування інформації.

На схемі моделі мережі ТОВ «Sollar» початково присутнє бюджетне мережеве обладнання зі швидкістю передач 100 Мб.

Інформаційний зв'язок між елементами моделі мережі ТОВ «Sollar» – це найбільша можлива ймовірність передачі інформаційних пакетів даних від одного мережевого вузлу до іншого вузлу у мережі. Кожен з вузлів розглядається як елемент теорії СМО. Ймовірність того що вузол в мережі зв'язується сам з собою дорівнює нульовому значенню.

В схемі моделі мережі ТОВ «Sollar» визначено що ймовірність того що інформаційні вузли, що відповідальні за маршрутизацію інформаційних пакетів даних зв'яжуться між собою приблизно однаковим показником ймовірності, та те що найбільший інтенсивний інформаційний зв'язок в мережі ТОВ «Sollar» буде між серверами та інтернетом «вузол №1», «вузол №2» та «вузол №12».

В структурі моделі комп'ютерної мережі ТОВ «Sollar» «вузол №3», «вузол №5», «вузол №6», «вузол №9» та «вузол №10» – є мережевими роутерами, які призначені для обслуговування локальної мережі для кінцевих користувачів цієї мережі.

В структурі моделі комп'ютерної мережі ТОВ «Sollar» «вузол №1», «вузол №2», «вузол №4», «вузол №8» та «вузол №11» – це комутатори, які забезпечують функціонування комп'ютерної мережі ТОВ «Sollar» на рівні доступу для користувачів цієї мережі.

Інформаційні зв'язки між компонентами структури комп'ютерної мережі ТОВ «Sollar» це ймовірність передачі інформаційних пакетів, що є визначальним параметром для аналізу у ПЗ для СМО.

Вірогідність інформаційного зв'язку 100 % відповідає значення 1,0. Сума всіх ймовірностей для одного інформаційного вузлу логічна має дорівнювати значення 1,0. Ще раз акцентуємо, що номінал вірогідності обрано відповідно до конкретних задач, які є комп'ютерної мережі ТОВ «Sollar» і це те завантаження, що очікується для конкретного мережевого вузла, яке воно залежить від специфіки ПЗ кінцевих користувачів цієї мережі.

Ймовірність того, що «вузол №1» зв'яжеться з «вузол №3» становить 1,0.

Ймовірність того, що «вузол №2» зв'яжеться з «вузол №6» становить 1,0.

Ймовірність того, що «вузол №3» зв'яжеться з «вузол №1» становить 0,5.
 Ймовірність того, що «вузол №3» зв'яжеться з «вузол №6» становить 0,3.
 Ймовірність того, що «вузол №3» зв'яжеться з «вузол №7» становить 0,2.
 Ймовірність того, що «вузол №4» зв'яжеться з «вузол №5» становить 1,0.
 Ймовірність того, що «вузол №5» зв'яжеться з «вузол №4» становить 0,5.
 Ймовірність того, що «вузол №5» зв'яжеться з «вузол №7» становить 0,5.
 Ймовірність того, що «вузол №6» зв'яжеться з «вузол №2» становить 0,25.
 Ймовірність того, що «вузол №6» зв'яжеться з «вузол №3» становить 0,25.
 Ймовірність того, що «вузол №6» зв'яжеться з «вузол №7» становить 0,15.
 Ймовірність того, що «вузол №6» зв'яжеться з «вузол №9» становить 0,35.
 Ймовірність того, що «вузол №7» зв'яжеться з «вузол №3» становить 0,25.
 Ймовірність того, що «вузол №7» зв'яжеться з «вузол №5» становить 0,15.
 Ймовірність того, що «вузол №7» зв'яжеться з «вузол №6» становить 0,35.
 Ймовірність того, що «вузол №7» зв'яжеться з «вузол №8» становить 0,15.
 Ймовірність того, що «вузол №8» зв'яжеться з «вузол №7» становить 1,0.
 Ймовірність того, що «вузол №9» зв'яжеться з «вузол №6» становить 0,35.
 Ймовірність того, що «вузол №9» зв'яжеться з «вузол №10» становить 0,1.
 Ймовірність того, що «вузол №9» зв'яжеться з «вузол №12» становить 0,55.
 Ймовірність того, що «вузол №10» зв'яжеться з «вузол №9» становить 0,5.
 Ймовірність того, що «вузол №10» зв'яжеться з «вузол №11» становить 0,5.
 Ймовірність того, що «вузол №11» зв'яжеться з «вузол №10» становить 1,0.

За цим описанням складена маршрутна матриця моделі комп'ютерної мережі ТОВ «Sollar» для ПЗ, яка і показана на рис. 5.2.

Наступним кроком з початковою ініціацією ПЗ моделі комп'ютерної мережі ТОВ «Sollar» є внесення відомостей про швидкодню початково існуючого мережевого обладнання. Ця інформація вноситься в відповідну одномірну матрицю, показана на рис. 5.3. Вона містить умовний час обробки для одного інформаційного повідомлення, яке відає вузлам. Ці дані з часу обробки пропорціональні по співвідношенню з реальним показникам часу до параметрів існуючого мережевого обладнання - згідно цього прийняти, що значення 10 – це абстрактна затримка для мережевого обладнання зі швидкістю передачі 100 Мб, а

значення 1 відповідає абстрактній затримці для мережевого обладнання зі швидкістю передачі 1 000 Мб). Швидкодія для вузлів відповідає схемі структури мережі. Заповнена матриця умовних затримок представлена на рис. 5.4.

$$Pr := \begin{pmatrix} 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0.3 & 0.2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.25 & 0 & 0 & 0 & 0.15 & 0 & 0.35 & 0 & 0 & 0 \\ 0 & 0 & 0.35 & 0 & 0.15 & 0.35 & 0 & 0.15 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.35 & 0 & 0 & 0 & 0.1 & 0 & 0.55 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 \end{pmatrix}$$

Рисунок 5.2 – Маршрутна матриця моделі мережі

$\tau_i :=$

10
10
10
10
10
10
10
10
10
10
10
10

Рисунок 5.3 – Час обробки повідомлення для моделі мережевого обладнання

5.2 Розрахунок параметрів моделі мережі

Сучасні наукові проблеми часто мають міждисциплінарний характер і вимагають інтеграції комп'ютерних моделей з різних дисциплін, кожна з яких має різну функціональну складність, середовища програмування та час обчислень. Емуляція пов'язаного гаусівського процесу (LGP) вирішує цю проблему за допомогою стратегії «розділяй і володаруй», яка інтегрує емулятори гаусівських процесів окремих комп'ютерних моделей у мережу.

Нездатність зрозуміти та передбачити поведінку систем глибокого навчання ускладнює прийняття рішення про те, яку архітектуру та алгоритм використовувати для даної проблеми. У науці та техніці моделювання – це методологія, яка використовується для розуміння складних систем, внутрішні процеси яких непрозорі. Моделювання замінює складну систему більш простим, більш інтерпретованим сурогатом [16].

За допомогою відповідного фрагмента ПЗ для моделювання комп'ютерної мережі ТОВ «Sollar» розрахуємо передаточні коефіцієнти ймовірностей, які визначаються за нормованим показником. Для розрахунку використовуються метод Гауса.

Результат розрахунку коефіцієнтів ймовірності показано на рис. 5.4.

$$e_m := \begin{pmatrix} 1 \\ 0.615 \\ 2 \\ 0.165 \\ 0.33 \\ 2.462 \\ 1.099 \\ 0.165 \\ 2.462 \\ 0.492 \\ 0.246 \\ 1.354 \end{pmatrix}$$

Рисунок 5.4 – Коефіцієнти ймовірностей за нормованим показником

Розрахунок коефіцієнтів, що є пропорційними кількості конвеєрів обробки інформаційних пакетів, що є в кожному з інформаційному вузлу, в моделі мережі СМО задається у матриці, де дані, які необхідні для подальших розрахунків обрано до технічних параметрів інформаційного мережевого обладнання. На початковому стані моделювання у кожному інформаційному мережевому вузлу знаходиться по одному конвеєру для обробки інформаційних пакетів (рис. 5.5).

$$m :=$$

1
1
1
1
1
1
1
1
1
1
1
1
1
1
1

Рисунок 5.5 – Кількість конвеєрів обробки для обробки інформаційних пакетів в мережевих вузлах

Розрахована матриця, що визначає показники вірогідності стану очікування для обробки певної кількості інформаційних пакетів у вузлах моделі.

	0	1	2	3	4
0	1	10	100	$1 \cdot 10^3$	$1 \cdot 10^4$
1	1	6.15	37.822	232.608	$1.431 \cdot 10^3$
2	1	20	400	$8 \cdot 10^3$	$1.6 \cdot 10^5$
3	1	1.65	2.722	4.492	7.412
4	1	3.3	10.89	35.937	118.592
5	1	24.62	606.144	$1.492 \cdot 10^4$	$3.674 \cdot 10^5$
6	1	10.99	120.78	$1.327 \cdot 10^3$	$1.459 \cdot 10^4$
7	1	1.65	2.722	4.492	7.412
8	1	24.62	606.144	$1.492 \cdot 10^4$	$3.674 \cdot 10^5$
9	1	4.92	24.206	119.095	585.95
10	1	2.46	6.052	14.887	36.622
11	1	13.54	183.332	$2.482 \cdot 10^3$	$3.361 \cdot 10^4$

Рисунок 5.6 – Час знаходження вузлу у стані очікування обробки певної кількості інформаційних пакетів

Наступним кроком розрахунку є визначення середніх значень показників інтенсивності вхідного потоку для кожного мережевих вузлів.

Вже понад 40 років Джеффри Бузен є лідером у галузі прогнозування продуктивності комп'ютерних систем та мереж. Його першим великим внеском

став алгоритм, відомий зараз як алгоритм Бузена, який обчислював пропускну здатність і час відгуку будь-якої практичної мережі серверів за кілька секунд. Попередні алгоритми виявилися марними, тому що на одні й ті ж розрахунки знадобилися б місяці або роки.

Прорив Бузена відкрив нову індустрію компаній, що надають послуги з оцінки продуктивності, і заклав наукові основи для проектування систем, що відповідають цілям продуктивності. По дорозі він став стурбований тим фактом, що реальні системи, які він оцінював, серйозно порушували припущення його моделі, і все ж несправні моделі передбачали пропускну здатність з точністю до 5 відсотків від справжнього значення і час відгуку з точністю до 25 відсотків. Він почав ламати голову над цією аномалією і винайшов нову структуру для побудови моделей продуктивності комп'ютера, яку назвав оперативним аналізом.

Операційний аналіз дав ті ж формули, але з припущеннями, які справедливі в більшості систем. Продовжуючи розуміти цю головоломку, він сформулював більш повну теорію випадковості, яку він назвав спостережною стохастикою, і написав книгу «Переосмислення випадковості», в якій виклав свою нову теорію. Ми поговорили з Джеффом Бузеном про його творчість [17].

Розрахунок з визначення середніх значень показників інтенсивності вхідного потоку для кожного мережевих вузлів проведено за алгоритмом Бузена. Результати розрахунку представлені на рис. 5.7.

	0
0	0.017
1	0.01
2	0.034
3	$2.77 \cdot 10^{-3}$
4	$5.54 \cdot 10^{-3}$
$\lambda =$ 5	0.041
6	0.018
7	$2.77 \cdot 10^{-3}$
8	0.041
9	$8.26 \cdot 10^{-3}$
10	$4.13 \cdot 10^{-3}$
11	0.023

Рисунок 5.7 – Інтенсивність вхідного інформаційного потоку пакетів для кожного з вузлів

Підраховані також показники середньої кількості інформаційних пакетів, які будуть очікувати обробку (рис. 5.8)

	0
0	0.274
1	0.156
2	0.678
3	0.038
4	0.079
L = 5	0.923
6	0.308
7	0.038
8	0.923
9	0.122
10	0.058
11	0.514

Рисунок 5.8 – Число пакетів очікування обробки

При цьому результат середнього часу обробки для інформаційних пакетів продемонстровано на рис. 5.9.

	0
0	16.343
1	15.147
2	20.2
3	13.87
4	14.32
t = 5	22.32
6	16.709
7	13.87
8	22.32
9	14.782
10	14.089
11	22.597

Рисунок 5.9 – Середній час обробки інформаційних пакетів

5.2.1 Параметри роботи мережі без впливу шкідливого ПЗ

Для роботи моделі комп'ютерної мережі ТОВ «Sollar» в «звичайному» режимі - без перевантаження, тобто без шкідливої дії вірусного ПЗ маємо наступні початкові параметри:

- кількість інформаційних пакетів у мережі: 5;

- час обробки пакетів: 10 одиниць, що відповідає швидкості мережевого обладнання у 100 Мб;

- кількість конвеєрів для обробки інформації у мережевому обладнанні: 1.

Маємо наступні розрахункові показники - графіки, які показують усереднені параметри для кожного інформаційного мережевого вузлу. Графіки представлені на рис. 5.10...рис. 5.12, де по горизонтальній вісі (X) для всіх графіків – номери вузлів, у діапазоні 0...13 (фактичні номери 1...13, згідно рис. 5.1), а по вертикальній вісі (Y) – відповідно інтенсивність вхідного потоку (умовні одиниці), середній час перебування пакета в черзі (умовні одиниці) та середня кількість пакетів в вузлу на одиницю часу (одиниці).

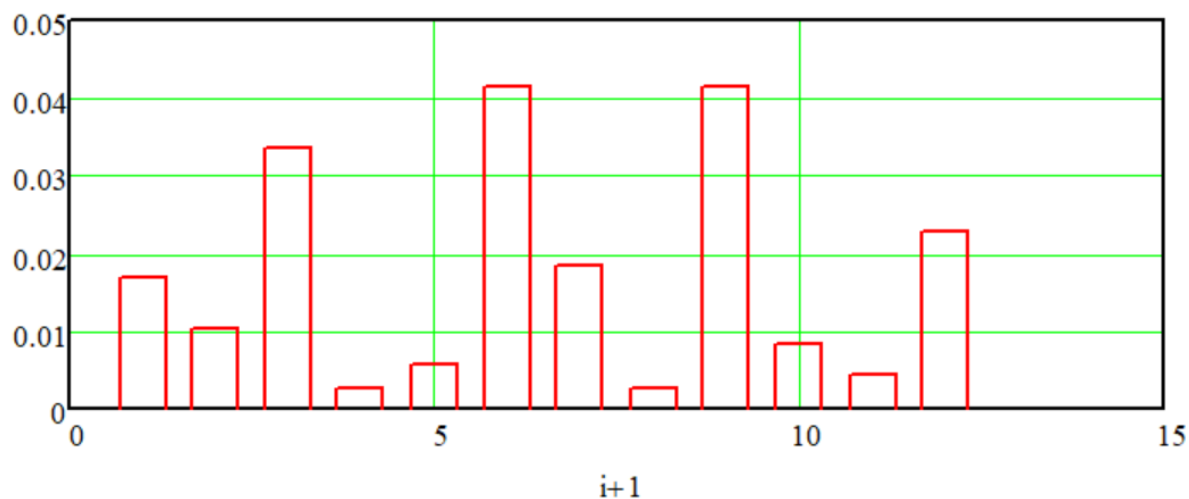


Рисунок 5.10 – Інтенсивність вхідного потоку

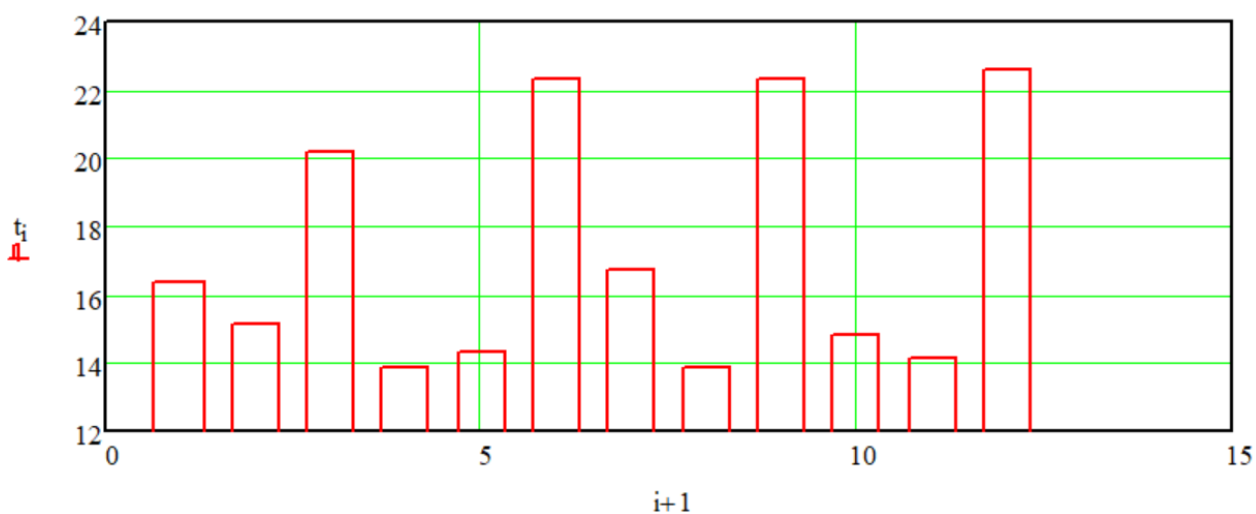


Рисунок 5.11 – Середній час перебування пакета в черзі

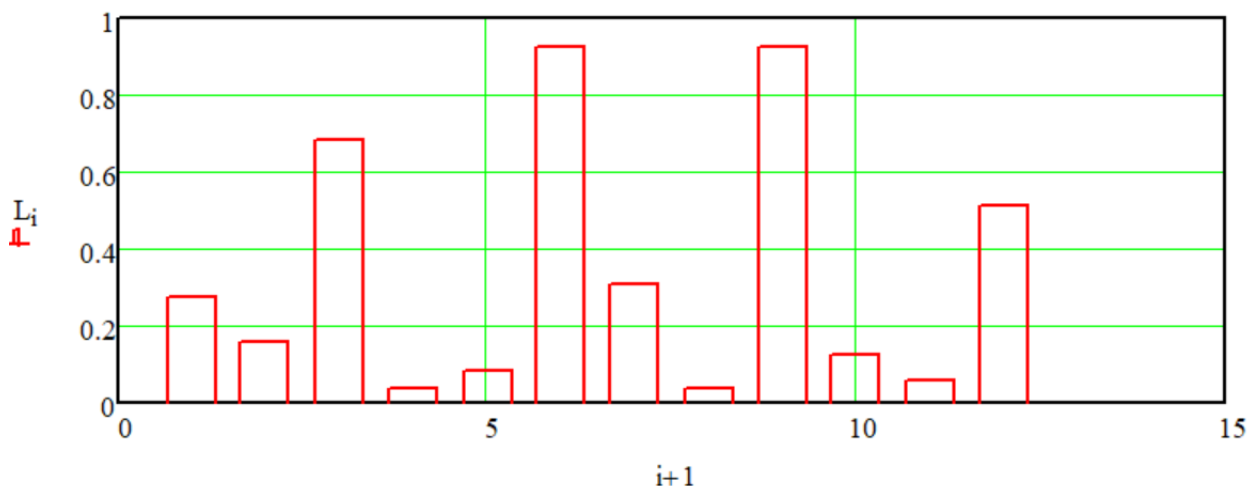


Рисунок 5.12 – Середня кількість пакетів

З візуальної інформації, яка представлена на цих графіках видно, що у всіх інформаційних вузлах моделі комп'ютерної мережі ТОВ «Sollar», які представлені серійним мережевим обладнанням - комутаторами та маршрутизаторами, повідомлення обробляються досить швидко і без значної черги.

Найбільш завантаженим є «вузол №3», «вузол №6», «вузол №9» та «вузол №12».

Висновок. При існуючих початкових параметрах для моделі комп'ютерної мережі ТОВ «Sollar» найбільшою проблемою можуть стати найбільше інформаційно завантажені вузли - «вузол №3», «вузол №6», «вузол №9» та «вузол №12». Показова трьох-мірна візуалізація результату розрахунку моделі показана на рис. 5.13.

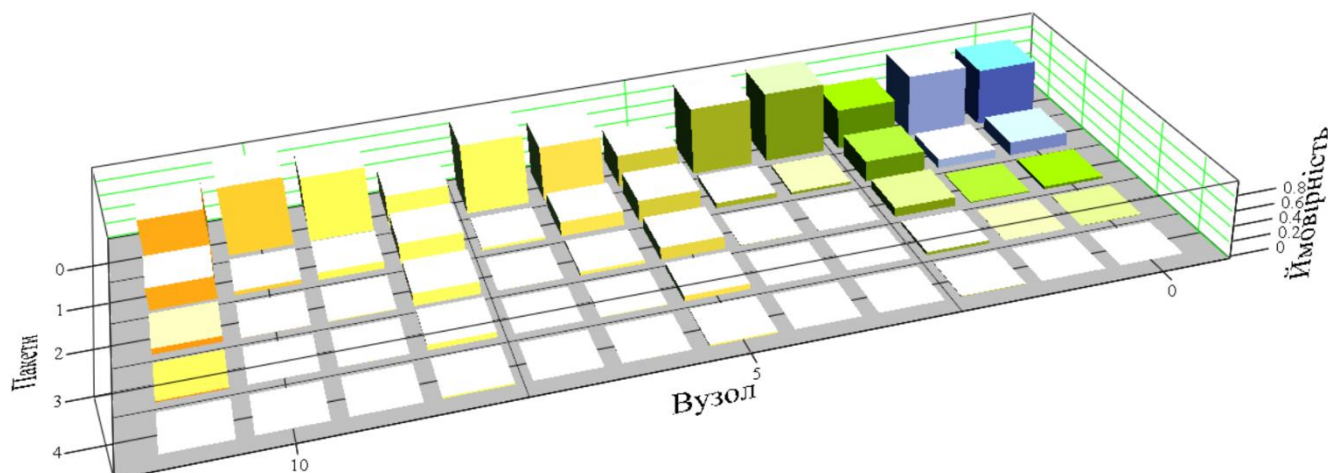


Рисунок 5.13 – Трьох-мірна візуалізація результату розрахунку моделі при довжині повідомлень у 5 інформаційних пакетів

Для вирішення проблеми з перевантаженням найбільш інформаційно завантажених вузлів - «вузол №3», «вузол №6», «вузол №9» та «вузол №12» можна вирішити заміною мережевих вузлів - «вузол №3», «вузол №6», «вузол №9» та «вузол №12» на більш сучасні швидкісні мережеві пристрої зі швидкістю інформаційного каналу у 1 000 МБ.

Після корекції параметрів інформаційного мережевого обладнання для вузлів – «вузол №3», «вузол №6», «вузол №9» та «вузол №12» у мережі більш нема проблемних вузлів. Візуалізація розрахунку скорегованої моделі комп'ютерної мережі ТОВ «Sollar», працюючої у «звичайному» режимі - без перевантаження шкідливою дією вірусного ПЗ, показана на рис. 5.14.

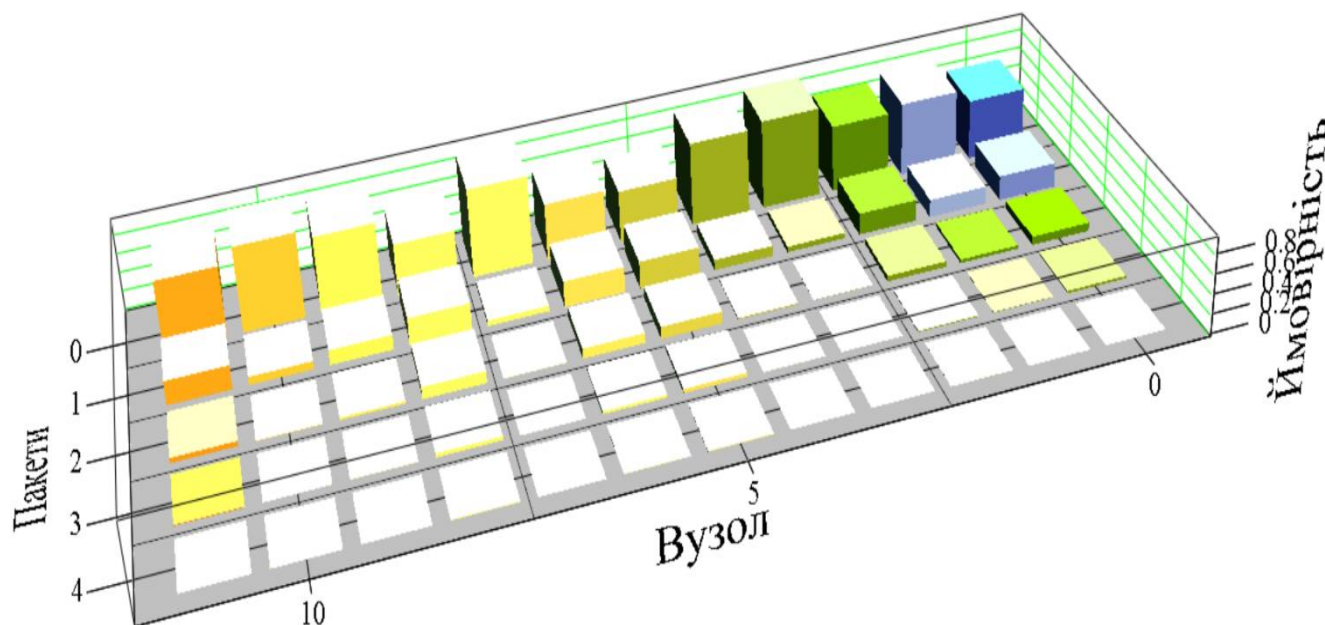


Рисунок 5.14 – Трьох-мірна візуалізація результату розрахунку моделі при довжині повідомлень у 5 інформаційних пакетів, та корекції моделі - «вузол №3», «вузол №6», «вузол №9» та «вузол №12»

Скорегована структурна схема комп'ютерної мережі ТОВ «Sollar» представлена на рис. 5.15.

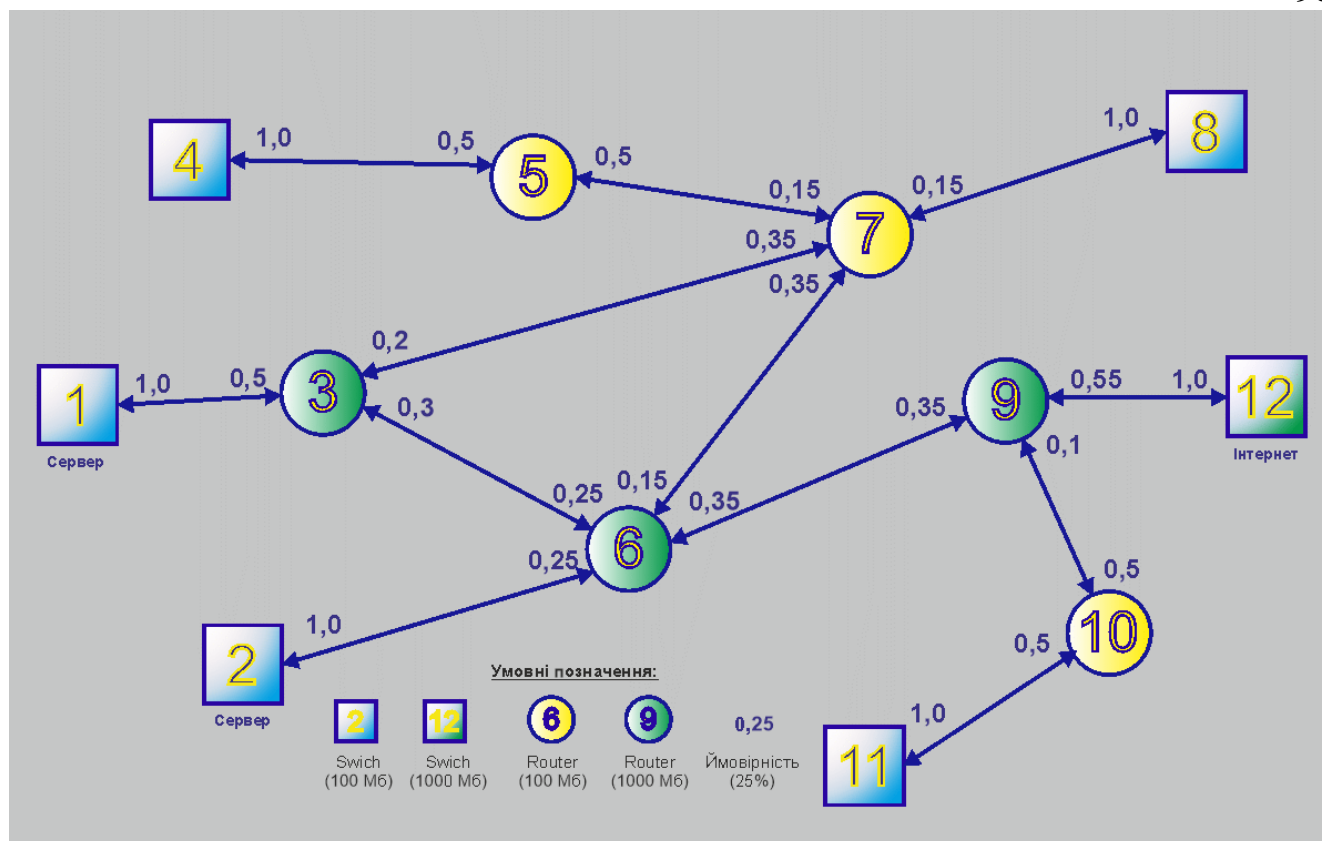


Рисунок 5.15 – Структура скорегованої комп'ютерної мережі працюючої у «звичайному» режимі - без перевантаження шкідливою дією вірусного ПЗ (кількість інформаційних пакетів дорівнює 5)

5.2.2 Параметри роботи мережі під впливом вірусних програм

Мережевий вірус — це тип зловмисного ПЗ, також відомого як зловмисне ПЗ, яке поширюється мережею комп'ютерів, націлившись на окремі машини для виконання несанкціонованих і шкідливих дій. Дії включають крадіжку конфіденційної інформації, пошкодження даних, відмову в обслуговуванні або використання зараженої машини як плацдарму для подальшого проникнення в мережу. Мережеві віруси становлять значну загрозу для приватних осіб, бізнес-операцій і систем національної безпеки в усьому світі.

По суті, мережевий вірус використовує з'єднання мережі для розмноження та поширення. Він використовує мережеві дії, такі як вкладення електронної пошти, спільний доступ до файлів або шкідливі посилання, для входу в комп'ютерну систему. Знайшовши відповідне ПЗ оператора на хост-комп'ютері, він включає свій шкідливий код у носій. Звідти, коли програмне забезпечення носія використовується або відкривається, вірус швидко активується та виконує свої шкідливі функції.

Мережеві віруси мають виняткову здатність до поширення. Основною характеристикою таких вірусів є складні методи, які вони використовують для самовідтворення на різних комп'ютерах. Мережеві віруси, отримавши доступ до мережі, можуть автоматично розмножуватися для зараження комп'ютерів у локальній мережі. Вони можуть поширювати свої можливості на ширший Інтернет і заражати машини по всьому світу.

Існує кілька типів мережевих вірусів, таких як черв'яки, трояни та боти. Хоча всі вони служать одному і тому ж незаконному наміру завдати шкоди та експлуатації, кожен з них діє унікальним чином. Черви можуть самостійно самовідтворюватися без участі людини, швидше поширюючись по мережах. Трояни маскуються під законне програмне забезпечення, щоб обманом змусити користувачів встановити їх, а боти таємно контролюють мережу заражених комп'ютерів для виконання шкідливих завдань.

Боротьба з мережевими вірусами вимагає надійних заходів кібербезпеки в поєднанні з найсучаснішими антивірусними програмами та мережевим обладнанням. Сучасні антивірусні програми розроблені для ефективної боротьби з мережевими вірусами за допомогою різних методів. Сканування таких програм у режимі реального часу захищає комп'ютери, постійно перевіряючи завантажені файли, електронні листи та нові програми на наявність відомих вірусів.

Можливість евристичного аналізу дозволяє антивірусному ПЗ виявляти невідомі мережеві віруси, аналізуючи вразливість програм і порівнюючи їх кодові шаблони з шаблонами задокументованих вірусів.

Антивірусне ПЗ також поміщає в карантин або блокує заражені файли, запобігаючи пошкодженню ними всієї системи. Автоматичні оновлення – це ще одна стандартна функція антивірусу, яка дозволяє програмному забезпеченню постійно оновлювати та вдосконалювати базу даних визначення вірусів. Це дозволяє йому виявляти нещодавно виявлені або оновлені віруси, що дозволяє йому забезпечувати комплексний захист від відомих і нових мережевих вірусів.

Використання інших заходів кібербезпеки, таких як брандмауери, системи виявлення вторгнень (IDS) і більш суворі протоколи безпеки, також допомагає захиститися від мережевих вірусів. Брандмауер ретельно перевіряє вхідний і

вихідний мережевий трафік і блокує трафік з підозрілих або невідомих джерел. IDS відстежує мережі на предмет потенційних порушень або порушень політик і сповіщає адміністраторів про виявлення такої активності.

На додаток до цих технічних реалізацій, культивування належних практик кібербезпеки серед користувачів комп'ютерів та Інтернету може значно мінімізувати загрози мережевих вірусів. Створення складних паролів, регулярне резервне копіювання даних, уникнення підозрілих електронних листів або веб-сайтів, а також оновлення програмного забезпечення та систем може значно знизити сприйнятливість до мережевих вірусів. Мережевий вірус є серйозною загрозою кібербезпеці, яка використовує мережеві можливості комп'ютерів для поширення шкідливих програм, крадіжки даних, завдання шкоди системам і навіть припинення роботи.

Для комплексного захисту потрібні не лише складні антивірусні програми, але й надійні стратегії контролю пошкоджень та надійні методи кібербезпеки серед користувачів. Не можна недооцінювати важливість інформування та навчання користувачів безпечному використанню Інтернету та поведінці в невинній боротьбі з мережевими вірусами [18].

В будь-якому випадку ПЗ шкідливої програми та дії антивірусної програми суттєво збільшує інформаційне навантаження на мережу.

Тепер перевіримо роботу моделі комп'ютерної мережі ТОВ «Sollar» в умовах роботи шкідливого вірусного ПЗ. Припустимо що інформаційне навантаження на мережу зросло в двічі (кількість інформаційних пакетів дорівнює 5).

Для моделі комп'ютерної мережі ТОВ «Sollar» зі скорегованою структурою (рис. 5.18) змодельюємо ситуацію з підвищеного у двічі кількістю інформаційних запитів – 10, замість звичайного режиму роботи кількістю інформаційних запитів, яка дорівнювала 5.

Висновок. При існуючих модернізованих параметрах для моделі комп'ютерної мережі ТОВ «Sollar» при дії шкідливого ПЗ проблемою стали наступні вузли - «вузол №6», «вузол №7» та «вузол №9».

Показова трьох-мірна візуалізація результату розрахунку моделі показана на рис. 5.16.

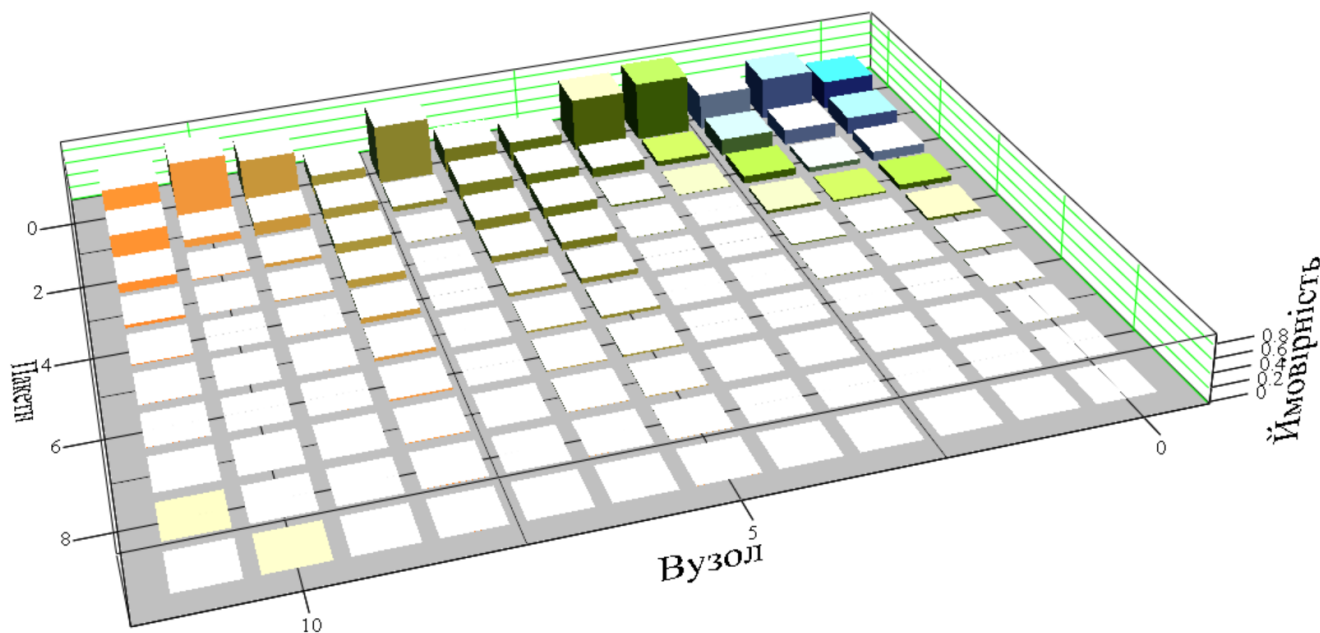


Рисунок 5.16 – Трьох-мірна візуалізація результату розрахунку моделі при довжині повідомлень у 10 інформаційних пакетів, та скорегованої моделі - «вузол №3», «вузол №6», «вузол №9» та «вузол №12»

В результаті моделювання роботи комп'ютерної мережі ТОВ «Sollar» зі збільшеною вдвічі кількістю пакетів було визначено додаткові параметри для інформаційних мережевих вузлів та зміни, які необхідні для конфігурації мережі.

Критерієм налаштування було вирівнювання завантаженості мережевих пристроїв для всієї мережі. Для цього було додаткова застосована заміна обладнання з пропускною здатністю 100 МБ на обладнання з пропускною здатністю 1000 МБ. Для вузлів – «Вузол №3», «Вузол №6» та «Вузол №9» пропонується застосувати маршрутизатор агрегації з пропускною здатністю 1 000 МБ (Cisco Catalyst 8500 модельний ряд [21]), а для вузлу «Вузол №12» - пропонується застосування свіч з пропускною здатністю 1 000 МБ (Cisco Catalyst 1000 модельний ряд [20]).

Служби агрегації в маршрутизаторах і периферійних платформах допомагають забезпечити маршрутизацію периферії мережі. Ці пристрої поєднують канали трафіку на більшій швидкості, щоб задовольнити зростаючу потребу у віддаленому доступі до внутрішніх мереж і зовнішніх мереж.

Великі корпорації використовують пристрої агрегації, щоб допомогти впоратися з вибуховим зростанням мережевого трафіку. Маршрутизатор агрегації

або периферійна платформа може консолідувати потоки трафіку та допомогти підтримувати стабільну продуктивність мережі.

Маршрутизатори агрегації та периферійні платформи допомагають гнучко підвищити операційну ефективність, одночасно знижуючи ризик простою.

Пристрої агрегації можуть дозволити платформі SD-WAN поєднувати кілька WAN-з'єднань, використовуючи різні мережеві транспорти, а також мережеві служби, такі як шифрування. Потім платформа SD-WAN може пересилати ці агреговані з'єднання та послуги через WAN-з'єднання на високій швидкості до зовнішніх мереж, таких як хмара, щоб забезпечити кращий досвід. Якщо маршрутизатор агрегації або периферійна платформа містить площину даних з апаратним прискоренням або спеціальний кремній, продуктивність буде оптимальною.

Новітні маршрутизатори служб агрегації забезпечують мультихмарну архітектуру, надаючи масштабовані хмарні програми для найкращого підключення. Для цього пристрої агрегації надають високопродуктивні платформи SD-WAN і периферійних служб безпечного доступу (SASE), багаті хмарні мережі та можливості безпеки, щоб надати IT-командам необхідну видимість і контроль.

Новітня технологія ASR може забезпечити видимість програм, яка потрібна IT-командам і мережевим командам для забезпечення стабільного, надійного з'єднання та продуктивності додатків у мережах і службах, якими організація може не володіти або безпосередньо не контролювати [19].

Показова трьох-мірна візуалізація результату розрахунку моделі показана на рис. 5.17.

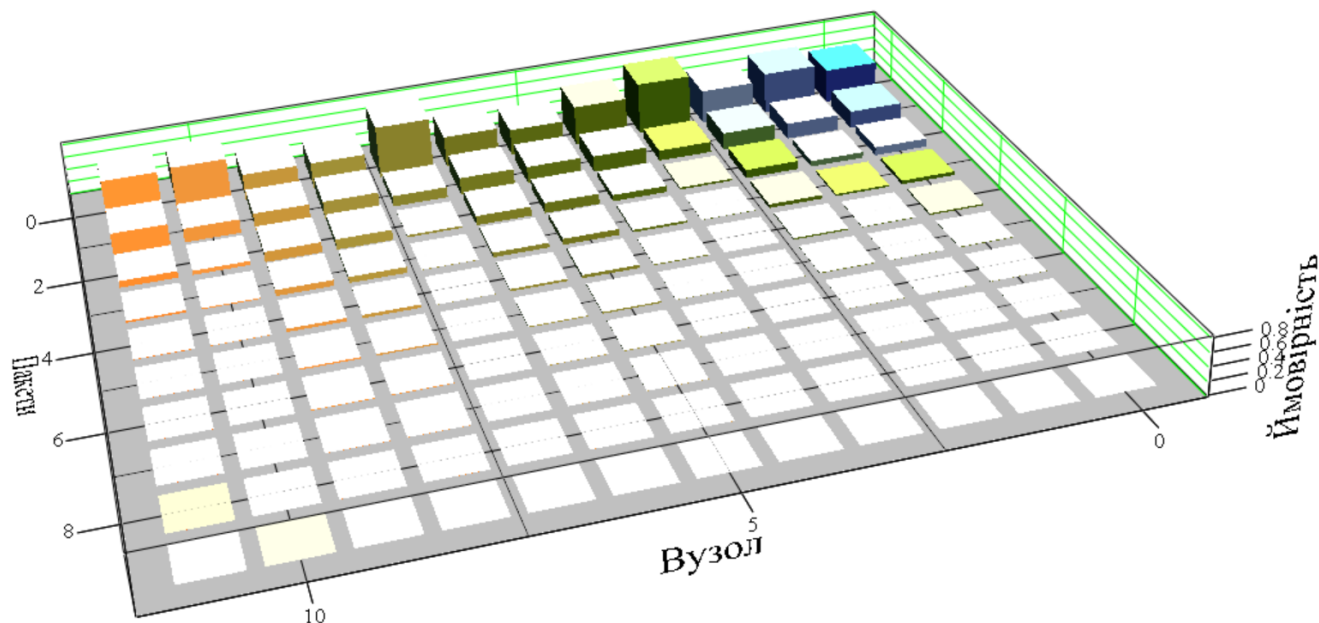


Рисунок 5.17 – Трьох-мірна візуалізація результату розрахунку моделі при довжині повідомлень у 10 інформаційних пакетів та кінцевої моделі комп'ютерної мережі ТОВ «Sollar»

Кінцева конфігурація з пропускної здатності для мережевих пристроїв комп'ютерної мережі ТОВ «Sollar» наступна (рис. 5.18):

«Вузол №1»	100 МБ;
«Вузол №2»	1 000 МБ;
«Вузол №3»	1 000 МБ, агрегація;
«Вузол №4»	100 МБ;
«Вузол №5»	100 МБ;
«Вузол №6»	1 000 МБ, агрегація;
«Вузол №7»	1 000 МБ;
«Вузол №8»	100 МБ;
«Вузол №9»	1 000 МБ, агрегація;
«Вузол №10»	100 МБ;
«Вузол №11»	100 МБ;
«Вузол №12»	1 000 МБ

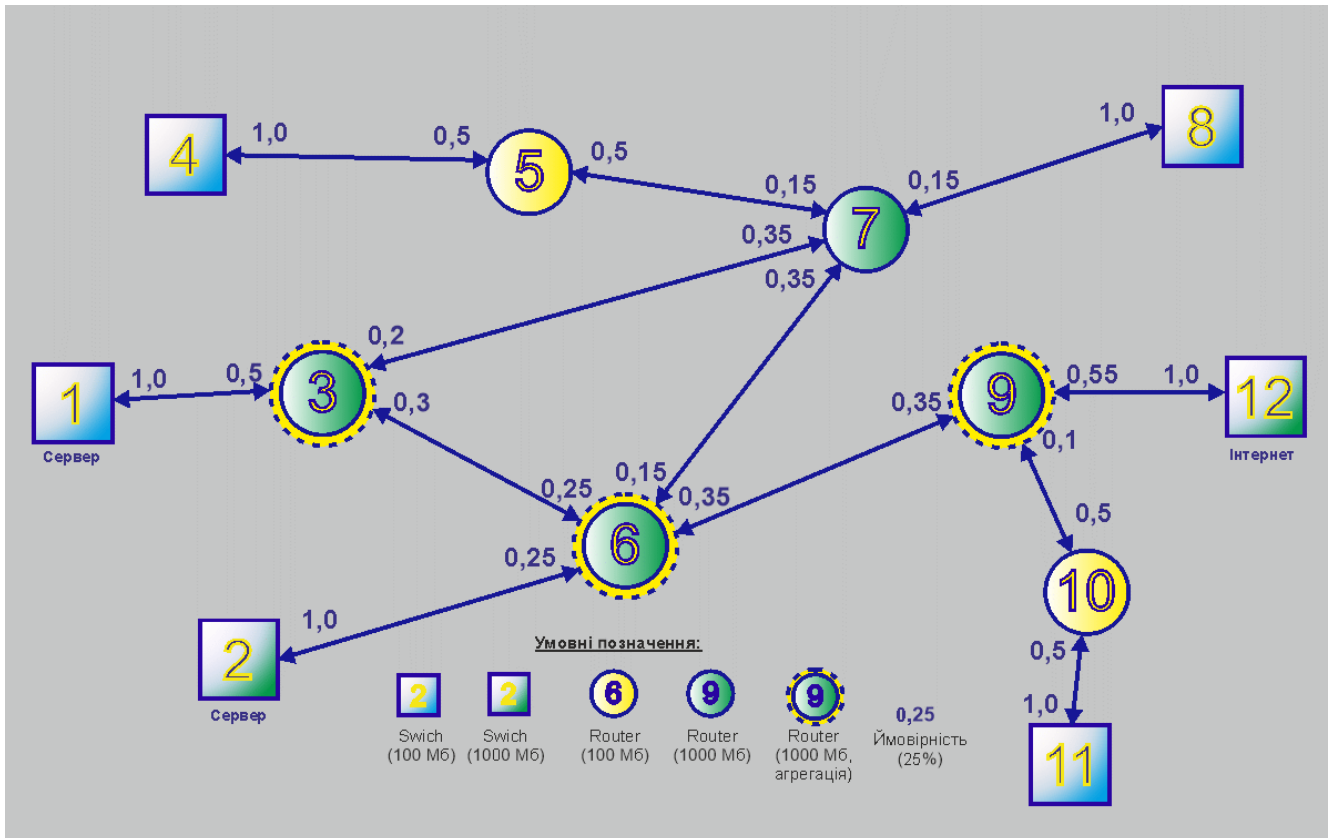


Рисунок 5.18 – Структура поліпшеної математичної моделі комп'ютерної мережі ТОВ «Sollar» для кількості пакетів 10

Результат моделювання мережі комп'ютерної мережі ТОВ «Sollar» по завантаженню вузлів є майже рівномірним, тобто навіть у складних умовах дії вірусного ПЗ з підвищенням інформаційного навантаження на комп'ютерну мережу ТОВ «Sollar» до 200 % вона буде стабільною і зберігати проектну пропускну здатність. Ймовірність черги з двох інформаційних пакетів не перевищує показник 0,2 (20 %)

За результатами порівняння характеристик моделі комп'ютерної мережі ТОВ «Sollar» у всіх розглянутих станах зроблено висновок про те, щонайбільше негативно на характеристиках мережі позначається атака шкідливим ПЗ.

5.3 Висновки по розділу

Розроблена модель комп'ютерної мережі ТОВ «Sollar» дозволяє успішно моделювати поведінку мережі, а саме значення інтенсивності вхідного потоку, час перебування пакетів в мережевих вузлах.

При дії вірусного ПЗ була висока ймовірність виникнення черги у 3...4 пакети для деяких мережевих вузлів комп'ютерній мережі ТОВ «Sollar». Для

підвищення стійкості мережі до перевантаження була здійснена заміна в деяких мережевих вузлах застарілого обладнання з пропускною здатністю 100 МБ на обладнання з пропускною здатністю 1000 МБ. Для вузлів – «Вузол №3», «Вузол №6» та «Вузол №9» пропонується застосувати маршрутизатор агрегації з пропускною здатністю 1 000 МБ (Cisco Catalyst 8500 модельний ряд), а для вузлу «Вузол №12» - пропонується застосування свіч з пропускною здатністю 1 000 МБ (Cisco Catalyst 1000 модельний ряд).

ВИСНОВКИ

Кваліфікаційна робота магістра на тему «Обґрунтування структури та параметрів комп'ютерної системи ТОВ «Sollar» на основі моделі мережі масового обслуговування» є завершеною науковою роботою, в якій вирішена науково-практична задача синтезу програмно-технічної реалізації комп'ютерної системи ТОВ «Sollar».

Новизна роботи полягає в використанні моделі мережі комп'ютерної системи ТОВ «Sollar», розробленої з застосуванням математичного апарату теорії масового обслуговування, з метою виявлення «слабких місць» в мережі при значному вибуховому інформаційному перевантаженні, та у пошуку шляхів для її вдосконалення.

Практичним результатом є розроблена комп'ютерна система ТОВ «Sollar» є відкритою, що дозволяє проводити оперативну технічну та програмну її модернізацію. Виявлення недоліків і шляхів вдосконалення комп'ютерної системи ТОВ «Sollar» досягається за рахунок використання наукового підходу до вирішення поставлених завдань з застосуванням теорії масового обслуговування.

Основними результатами кваліфікаційної роботи є наступне:

1. Відповідно до функціональних особливостей комп'ютерної системи ТОВ «Sollar» показано, що навантаження на комп'ютерну мережу може викликатися дією вірусного програмного забезпечення, яке негативно впливає на роботу комп'ютерної системи ТОВ «Sollar» і з високою ймовірністю може призвести до значних економічних і репутаційних втрат для ТОВ «Sollar».

2. Дослідження поведінки комп'ютерної системи ТОВ «Sollar» було здійснено застосування методів теорії масового обслуговування, так як використання класичних підходів до рішення цього завдання є доволі трудомістким, займає значний проміжок часу та є дуже коштовним.

3. Для математичної моделі комп'ютерної системи ТОВ «Sollar», розглянутої як замкнена СМО для якої визначені параметри налаштувань.

4. Розроблена модель комп'ютерної системи ТОВ «Sollar» дозволяє визначити усереднені показники інтенсивності вхідного потоку, часу перебування пакету в черзі, середню кількість пакетів в черзі до мережевих вузлів.

5. Показники моделі мережі відносяться до класу безрозмірних характеристик.

6. Для підвищення стійкості мережі до перевантаження була здійснена заміна в деяких мережевих вузлах застарілого обладнання з пропускною здатністю 100 МБ на обладнання з пропускною здатністю 1000 МБ. Для вузлів – «Вузол №3», «Вузол №6» та «Вузол №9» пропонується застосувати маршрутизатор агрегації з пропускною здатністю 1 000 МБ, а для вузлу «Вузол №12» - пропонується застосування свіч з пропускною здатністю 1 000 МБ.

Прикладні наукові результати з розробки комп'ютерної системи ТОВ «Sollar» та моделювання її роботи показали її працездатність на багатьох режимах інформаційного навантаження, що гарантує надійне застосування комп'ютерної системи ТОВ «Sollar».

На основі проведених досліджень можна рекомендувати застосування удосконаленої структури комп'ютерної системи ТОВ «Sollar».

ПЕРЕЛІК ПОСИЛАНЬ

1. The Importance of IT Services for Businesses: A Comprehensive Guide. Режим доступу: <https://www.linkedin.com/pulse/importance-services-businesses-comprehensive-guide>
2. Collection of Scientific Papers "Scientific Notes". The crucial role of IT service companies in driving the modern economy. Режим доступу: [https://vz.kneu.ua/archive/2024/35\(2\).18](https://vz.kneu.ua/archive/2024/35(2).18)
3. Utilisations du réseau informatique. Режим доступу: <https://www.geeksforgeeks.org/uses-of-computer-network/>
4. What are the types of IT outsourcing and why do you need to choose your provider based on your specific needs? Режим доступу: https://kruschecompany.com/it-outsourcing-types/#Different_organisations_have_different_IT_outsourcing_needs
5. Computer Networking Company in Business Area. International Research Journal of Management, IT & Social Sciences Available online at <https://sloap.org/journals/index.php/irjmis/> Vol. 2 No. 7, July 2015, pages: 1~4. ISSN: 2395-7492. Режим доступу: <https://sloap.org/journals/index.php/irjmis/article/view/311>
6. The problem of information overload in business organisations: a review of the literature. Angela Edmunds, Anne Morris. PERGAMON. International Journal of Information Management 20 (2000) 17}28. Режим доступу: <http://dea128fc.free.fr/CoursA/A1-Management%20&%20TIC/Articles%20scientifiques/infooverload.pdf>
8. Simulation and Modelling of Computer Networks. Antoni Izworski¹, Slawomir Skowronski¹, and Jozef B., Wroclaw University of Technology, Wyb. Wyspianskiego 27, Wroclaw, Poland.
9. Computer Networking: A Survey. Режим доступу: https://www.researchgate.net/publication/317101504_Computer_Networking_A_Survey
10. Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. Режим доступу: <https://www.sciencedirect.com/science/article/pii/S1389128621001109>

11. Маршрутизатор Cisco C921-4P. Режим доступу: <https://stack-systems.com.ua/marshrutizator-cisco-c921-4p>
12. Маршрутизатор (роутер) Cisco 891F-K9. Режим доступу: <https://hotline.ua/ua/computer-marshrutizatory/cisco-891f-k9/?tab=about>
13. Комутатор Cisco WS-C2960-24-S. Режим доступу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24-s>
15. Fog computing for next-generation Internet of Things: Fundamental, state-of-the-art and research challenges Режим доступу: <https://www.sciencedirect.com/science/article/abs/pii/S1574013723000163>
16. Gaussian Process Surrogate Models for Neural Networks. Michael Y. Li, Erin Grant, Thomas L. Griffiths. Department of Computer Science, Stanford University, Stanford, California, USA, Gatsby Computational Neuroscience Unit, University College London, London, UK, Departments of Psychology and Computer Science, Princeton, NJ, USA. Режим доступу: <https://proceedings.mlr.press/v216/li23c/li23c.pdf>
17. Rethinking Randomness: An interview with Jeff Buzen, Part I. Режим доступу: <https://dl.acm.org/doi/10.1145/2986329>
18. What are Network virus? Режим доступу: <https://cyberpedia.reasonlabs.com/EN/network%20virus.html>
19. What Are Aggregation Services Routers (ASR)? Режим доступу: <https://www.cisco.com/c/en/us/products/routers/what-are-aggregated-services-routers.html>
20. Cisco Catalyst 1000 Series Switches. Режим доступу: <https://www.cisco.com/c/en/us/products/switches/catalyst-1000-series-switches/index.html>
21. Catalyst 8500 Series models. Режим доступу: <https://www.cisco.com/site/us/en/products/networking/sdwan-routers/catalyst-8500-series-platforms/index.html>
22. Розвиток ІТ в Україні: поточна ситуація та перспективи. Режим доступу: <https://blog.youcontrol.market/rozvitok-it-v-ukrayini-potochna-situatsiia-ta-pierspiektivi/>

ДОДАТОК А**Текст програми****Програмно-технічна реалізація модель комп'ютерної системи ТОВ****«Sollar»**

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
ПРОГРАМНО-ТЕХНІЧНА РЕАЛІЗАЦІЯ
КОМП'ЮТЕРНОЇ СИСТЕМИ ТОВ «SOLLAR»

Текст програми

804.02070743.23028-01 12 01

Листів 18

2024

АНОТАЦІЯ

Даний програмний документ містить ПЗ реалізації математичної моделі комп'ютерної системи ТОВ «Sollar».

Тексти програм реалізовані в середовищі Mathcad 15 в середовищі операційної системи Windows 10.

ПЗ реалізує рекурентний метод Бузена для розрахунку параметрів комп'ютерної системи ТОВ «Sollar». як замкнутої СМО.

ЗМІСТ

	стор.
1. Перелік використаних змінних	4
2. Текст програми	6
3. Результати розрахунку	7

1 Перелік використаних змінних, та переклад коментарів

N_n – кількість вузлів мережі.

τ – час обробки одного пакета у вузлу.

P_r – матриця перехідних ймовірностей.

e – матриця перехідних коефіцієнтів.

m – кількість конвеєрів у вузлах.

N – кількість пакетів що циркулюють в мережі.

B – матриця ймовірностей черги у вузлах.

λ – середня інтенсивність запитів на вході у вузол.

L – середня черга пакетів у вузлу.

t – середній час перебування пакета у вузлу.

Average time spent in the node - Середній час перебування у вузлу.

Calculation of function A - Розрахунок функції A.

Calculation of the matrix of constants T - Обчислення матриці констант T.

Calculate the constants for the second and subsequent nodes - Розраховуємо константи для другого і наступних вузлів.

Calculation of the intensity of query processing in network nodes - Розрахунок інтенсивності обробки запитів у вузлах мережі.

Calculation of auxiliary coefficients - Розрахунок допоміжних коефіцієнтів.

Calculation of probabilities of receipt in the last node of applications – j - Розрахунок ймовірностей надходження в останньому вузлу заявок – j.

Determination of transmission coefficients - Визначення коефіцієнтів передачі.

Matrix of transfer coefficients - Матриця передаточних коефіцієнтів.

Number of nodes in the network - Кількість вузлів у мережі.

Transfer matrix - Передаточна матриця.

The number of packets circulating in the network - Кількість пакетів, які циркулюють в мережі.

The number of pipelines in each node - Кількість конвеєрів в кожному вузлу.

The intensity of the input stream - Інтенсивність вхідного потоку.

The average number of packets per node - Середня кількість пакетів в вузлах.

Packet processing time at the node - Час обробки пакета у вузлу.

2 Текст програми

Задаємо кількість вузлів мережі 12 (Nn)

Nn := 11

i := 0..Nn j := 0..Nn

Задаємо час обробки запиту в вузлах мережі (1-1000МБ, 10-100МБ):

$\tau_i :=$

10
10
10
10
10
10
10
10
10
10
10
10
10

$\tau =$

	0
0	10
1	10
2	10
3	10
4	10
5	10
6	10
7	10
8	10
9	10
10	10
11	10

Розрахунок інтенсивності обробки запитів в вузлах мережі

$$\mu_i := \frac{1}{\tau_i}$$

$\mu =$

	0
0	0.1
1	0.1
2	0.1
3	0.1
4	0.1
5	0.1
6	0.1
7	0.1
8	0.1
9	0.1
10	0.1
11	0.1

Задасмо матрицю імовірностей передачі (Pr): (через меню Вставка-Матриця)

$$Pr := \begin{pmatrix} 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0.3 & 0.2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.25 & 0 & 0 & 0 & 0.15 & 0 & 0.35 & 0 & 0 & 0 \\ 0 & 0 & 0.35 & 0 & 0.15 & 0.35 & 0 & 0.15 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.35 & 0 & 0 & 0 & 0.1 & 0 & 0.55 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 \end{pmatrix}$$

Перевірка правильності заповнення передаточної матриці

$$SumPr_i := \sum_{j=0}^{Nn} Pr_{i,j}$$

	0
0	1
1	1
2	1
3	1
4	1
SumPr = 5	1
6	1
7	1
8	1
9	1
10	1
11	1

Розрахунок коефіцієнтів передачі

$$P := Pr^T$$

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0.5	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0.25	0	0	0	0	0	0
2	1	0	0	0	0	0.25	0.35	0	0	0	0	0
3	0	0	0	0	0.5	0	0	0	0	0	0	0
4	0	0	0	1	0	0	0.15	0	0	0	0	0
5	0	1	0.3	0	0	0	0.35	0	0.35	0	0	0
6	0	0	0.2	0	0.5	0.15	0	1	0	0	0	0
7	0	0	0	0	0	0	0.15	0	0	0	0	0
8	0	0	0	0	0	0.35	0	0	0	0.5	0	1
9	0	0	0	0	0	0	0	0	0.1	0	1	0
10	0	0	0	0	0	0	0	0	0	0.5	0	0
11	0	0	0	0	0	0	0	0	0.55	0	0	0

P =

Створюємо діагональну матрицю (D): (через меню Вставка-Матриця)

$$D := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$P1 := P - D$$

	0	1	2	3	4	5	6	7	8	9	10	11
0	-1	0	0.5	0	0	0	0	0	0	0	0	0
1	0	-1	0	0	0	0.25	0	0	0	0	0	0
2	1	0	-1	0	0	0.25	0.35	0	0	0	0	0
3	0	0	0	-1	0.5	0	0	0	0	0	0	0
4	0	0	0	1	-1	0	0.15	0	0	0	0	0
5	0	1	0.3	0	0	-1	0.35	0	0.35	0	0	0

P1 =

6	0	0	0.2	0	0.5	0.15	-1	1	0	0	0	0
7	0	0	0	0	0	0	0.15	-1	0	0	0	0
8	0	0	0	0	0	0.35	0	0	-1	0.5	0	1
9	0	0	0	0	0	0	0	0	0.1	-1	1	0
10	0	0	0	0	0	0	0	0	0	0.5	-1	0
11	0	0	0	0	0	0	0	0	0.55	0	0	-1

$j := 1 .. Nn \quad i := 0 .. Nn$

$$P2_{(j-1),i} := P1_{0,i} + P1_{j,i}$$

P2 =

	0	1	2	3	4	5	6	7	8	9	10	11
0	-1	-1	0.5	0	0	0.25	0	0	0	0	0	0
1	0	0	-0.5	0	0	0.25	0.35	0	0	0	0	0
2	-1	0	0.5	-1	0.5	0	0	0	0	0	0	0
3	-1	0	0.5	1	-1	0	0.15	0	0	0	0	0
4	-1	1	0.8	0	0	-1	0.35	0	0.35	0	0	0
5	-1	0	0.7	0	0.5	0.15	-1	1	0	0	0	0
6	-1	0	0.5	0	0	0	0.15	-1	0	0	0	0
7	-1	0	0.5	0	0	0.35	0	0	-1	0.5	0	1
8	-1	0	0.5	0	0	0	0	0	0.1	-1	1	0
9	-1	0	0.5	0	0	0	0	0	0	0.5	-1	0
10	-1	0	0.5	0	0	0	0	0	0.55	0	0	-1

$j := 0 .. Nn - 1 \quad i := 0 .. Nn - 1 \quad PP2_{j,i} := P2_{j,i+1}$

PP2 =

	0	1	2	3	4	5	6	7	8	9	10	11
0	-1	0.5	0	0	0.25	0	0	0	0	0	0	
1	0	-0.5	0	0	0.25	0.35	0	0	0	0	0	
2	0	0.5	-1	0.5	0	0	0	0	0	0	0	
3	0	0.5	1	-1	0	0.15	0	0	0	0	0	
4	1	0.8	0	0	-1	0.35	0	0.35	0	0	0	
5	0	0.7	0	0.5	0.15	-1	1	0	0	0	0	
6	0	0.5	0	0	0	0.15	-1	0	0	0	0	
7	0	0.5	0	0	0.35	0	0	-1	0.5	0	1	
8	0	0.5	0	0	0	0	0	0.1	-1	1	0	
9	0	0.5	0	0	0	0	0	0	0.5	-1	0	
10	0	0.5	0	0	0	0	0	0.55	0	0	-1	
11												

$$Q_{j,0} := P2_{j,0}$$

$$Q =$$

	0
0	-1
1	0
2	-1
3	-1
4	-1
5	-1
6	-1
7	-1
8	-1
9	-1
10	-1

$$E := \text{Isolve}(PP2, Q)$$

$$E =$$

	0
0	-0.615
1	-2
2	-0.165
3	-0.33
4	-2.462
5	-1.099
6	-0.165
7	-2.462
8	-0.492
9	-0.246
10	-1.354

Створюємо матрицю коефіцієнтів (e): (через меню *Вставка-Матриця* копіюємо значення з E без заку "-", перше значення "1"):

$$e :=$$

1
0.615
2
0.165
0.33
2.462
1.099
0.165
2.462
0.492
0.246
1.354

**Задаємо кількість пакетів які циркулюють в мережі
5 - нормальний режим, 10 - з вірусами (N):**

$i := 0..Nn$

$j := 0..N-1$

$N := 5$

Задаємо кількість конвеєрів в южному вузлі (m_i):

$m_i :=$

1
1
1
1
1
1
1
1
1
1
1
1
1
1
1

	0
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1

Розрахунок значень функції A

$$A_{m_i, j} := \begin{cases} j! & \text{if } m_i \geq N - 1 \\ 1 & \text{if } m_i = 1 \\ j! & \text{if } 1 < m_i < N - 1 \wedge j \leq m_i \\ m_i! \cdot (m_i)^{j-m_i} & \text{if } 1 < m_i < N - 1 \wedge j > m_i \end{cases}$$

A =

	0	1	2	3	4	5
0	1	1	1	1	1	
1	1	1	1	1	1	
2	1	1	1	1	1	
3	1	1	1	1	1	
4	1	1	1	1	1	
5	1	1	1	1	1	
6	1	1	1	1	1	
7	1	1	1	1	1	
8	1	1	1	1	1	
9	1	1	1	1	1	
10	1	1	1	1	1	
11	1	1	1	1	1	
12						

$$X_i := \frac{e_i}{\mu_i}$$

$$X =$$

	0
0	10
1	6.15
2	20
3	1.65
4	3.3
5	24.62
6	10.99
7	1.65
8	24.62
9	4.92
10	2.46
11	13.54

Обчислення матриці констант T

$$T_{i,0} := 1$$

$$T_{i,j} := \frac{(X_i)^j}{A_{i,j}}$$

$$T =$$

	0	1	2	3	4
0	1	10	100	$1 \cdot 10^3$	$1 \cdot 10^4$
1	1	6.15	37.822	232.608	$1.431 \cdot 10^3$
2	1	20	400	$8 \cdot 10^3$	$1.6 \cdot 10^5$
3	1	1.65	2.722	4.492	7.412
4	1	3.3	10.89	35.937	118.592
5	1	24.62	606.144	$1.492 \cdot 10^4$	$3.674 \cdot 10^5$
6	1	10.99	120.78	$1.327 \cdot 10^3$	$1.459 \cdot 10^4$
7	1	1.65	2.722	4.492	7.412
8	1	24.62	606.144	$1.492 \cdot 10^4$	$3.674 \cdot 10^5$
9	1	4.92	24.206	119.095	585.95
10	1	2.46	6.052	14.887	36.622
11	1	13.54	183.332	$2.482 \cdot 10^3$	$3.361 \cdot 10^4$

Розраховуємо константи для другого і наступних вузлів

$$i := 1 \dots N_n \quad k := 0 \dots N - 1$$

$$G_{0,j} := T_{0,j}$$

$$G_{i,k} := \sum_{j=0}^k (T_{i,j} \cdot G_{i-1,k-j})$$

	0	1	2	3	4	5
0	1	10	100	$1 \cdot 10^3$	$1 \cdot 10^4$	
1	1	16.15	199.322	$2.226 \cdot 10^3$	$2.369 \cdot 10^4$	
2	1	36.15	922.322	$2.067 \cdot 10^4$	$4.371 \cdot 10^5$	
3	1	37.8	984.692	$2.23 \cdot 10^4$	$4.739 \cdot 10^5$	
4	1	41.1	$1.12 \cdot 10^3$	$2.599 \cdot 10^4$	$5.597 \cdot 10^5$	
5	1	65.72	$2.738 \cdot 10^3$	$9.341 \cdot 10^4$	$2.86 \cdot 10^6$	
6	1	76.71	$3.581 \cdot 10^3$	$1.328 \cdot 10^5$	$4.319 \cdot 10^6$	
7	1	78.36	$3.711 \cdot 10^3$	$1.389 \cdot 10^5$	$4.548 \cdot 10^6$	
8	1	102.98	$6.246 \cdot 10^3$	$2.927 \cdot 10^5$	$1.175 \cdot 10^7$	
9	1	107.9	$6.777 \cdot 10^3$	$3.26 \cdot 10^5$	$1.336 \cdot 10^7$	
10	1	110.36	$7.048 \cdot 10^3$	$3.434 \cdot 10^5$	$1.42 \cdot 10^7$	
11	1	123.9	$8.726 \cdot 10^3$	$4.615 \cdot 10^5$	$2.045 \cdot 10^7$	
12						

$$B_{Nn,j} := \frac{T_{Nn,j}}{G_{Nn,N-1}} \cdot G_{Nn,N-1-j} \quad B_{Nn,0} := 1 - B_{Nn,1}$$

	0	1	2	3	4	5
0	0	0	0	0	0	
1	0	0	0	0	0	
2	0	0	0	0	0	
3	0	0	0	0	0	
4	0	0	0	0	0	
5	0	0	0	0	0	
6	0	0	0	0	0	
7	0	0	0	0	0	
8	0	0	0	0	0	
9	0	0	0	0	0	
10	0	0	0	0	0	
11	0.694	0.306	0.078	0.015	$1.643 \cdot 10^{-3}$	
12						

Розрахунок допоміжних коефіцієнтів

$$i := 0..Nn-1 \quad j := 1..N-1 \quad Gn_{1,0} := 1$$

	0	1	2	3	4	5
0	0	123.9	$7.487 \cdot 10^3$	$3.742 \cdot 10^5$	$1.584 \cdot 10^7$	
1	1	117.75	$7.964 \cdot 10^3$	$4.078 \cdot 10^5$	$1.761 \cdot 10^7$	
2	1	103.9	$6.248 \cdot 10^3$	$2.87 \cdot 10^5$	$1.122 \cdot 10^7$	
3	1	122.25	$8.522 \cdot 10^3$	$4.471 \cdot 10^5$	$1.969 \cdot 10^7$	
4	1	120.6	$8.317 \cdot 10^3$	$4.327 \cdot 10^5$	$1.893 \cdot 10^7$	
5	1	99.28	$5.676 \cdot 10^3$	$2.467 \cdot 10^5$	$9.089 \cdot 10^6$	
6	1	112.91	$7.364 \cdot 10^3$	$3.656 \cdot 10^5$	$1.538 \cdot 10^7$	
7	1	122.25	$8.522 \cdot 10^3$	$4.471 \cdot 10^5$	$1.969 \cdot 10^7$	
8	1	99.28	$5.676 \cdot 10^3$	$2.467 \cdot 10^5$	$9.089 \cdot 10^6$	
9	1	118.98	$8.116 \cdot 10^3$	$4.186 \cdot 10^5$	$1.818 \cdot 10^7$	
10	1	121.44	$8.421 \cdot 10^3$	$4.4 \cdot 10^5$	$1.932 \cdot 10^7$	
11	1	0	0	0	0	

$$i := 0..Nn-1 \quad j := 0..N-1$$

$$B_{i,j} := \frac{T_{i,j}}{G_{Nn,N-1}} \cdot Gn_{1,N-1-j}$$

B =

	0	1	2	3	4
0	0.774	0.183	0.037	$6.058 \cdot 10^{-3}$	0
1	0.861	0.123	0.015	$1.339 \cdot 10^{-3}$	$6.995 \cdot 10^{-5}$
2	0.549	0.281	0.122	0.041	$7.824 \cdot 10^{-3}$
3	0.963	0.036	$1.134 \cdot 10^{-3}$	$2.685 \cdot 10^{-5}$	$3.624 \cdot 10^{-7}$
4	0.926	0.07	$4.429 \cdot 10^{-3}$	$2.119 \cdot 10^{-4}$	$5.799 \cdot 10^{-6}$
5	0.444	0.297	0.168	0.072	0.018
6	0.752	0.196	0.043	$7.328 \cdot 10^{-3}$	$7.133 \cdot 10^{-4}$
7	0.963	0.036	$1.134 \cdot 10^{-3}$	$2.685 \cdot 10^{-5}$	$3.624 \cdot 10^{-7}$
8	0.444	0.297	0.168	0.072	0.018
9	0.889	0.101	$9.607 \cdot 10^{-3}$	$6.929 \cdot 10^{-4}$	$2.865 \cdot 10^{-5}$
10	0.944	0.053	$2.492 \cdot 10^{-3}$	$8.84 \cdot 10^{-5}$	$1.791 \cdot 10^{-6}$
11	0.694	0.306	0.078	0.015	$1.643 \cdot 10^{-3}$

$i := 0..Nn \quad j := 0..N-1$

$SumB_i := \sum_j B_{i,j}$

SumB =

	0
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1.095

$\lambda_1 := e_1 \cdot \frac{G_{Nn-1, N-2}}{G_{Nn, N-1}}$

$L_{1,1} := \sum_{n=0}^{N-1} \binom{n \cdot B_{1,n}}{n}$

Інтенсивність вхідного потоку

Середнє число пакетів в вузлах

$$\lambda =$$

	0
0	0.017
1	0.01
2	0.034
3	$2.77 \cdot 10^{-3}$
4	$5.54 \cdot 10^{-3}$
5	0.041
6	0.018
7	$2.77 \cdot 10^{-3}$
8	0.041
9	$8.26 \cdot 10^{-3}$
10	$4.13 \cdot 10^{-3}$
11	0.023

$$L =$$

	0
0	0.274
1	0.156
2	0.678
3	0.038
4	0.079
5	0.923
6	0.308
7	0.038
8	0.923
9	0.122
10	0.058
11	0.514

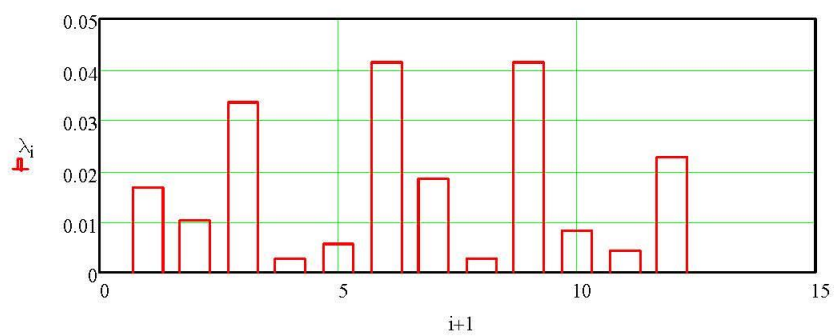
Середній час перебування пакета в вузлі

$$t_i := \frac{L_i}{\lambda_i}$$

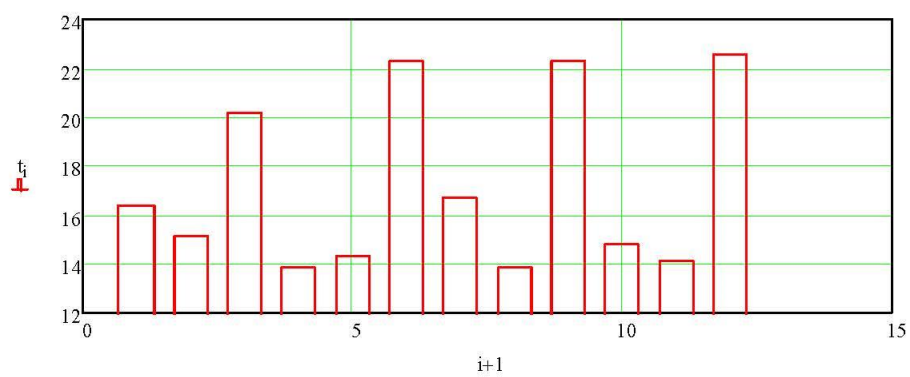
$$t =$$

	0
0	16.343
1	15.147
2	20.2
3	13.87
4	14.32
5	22.32
6	16.709
7	13.87
8	22.32
9	14.782
10	14.089
11	22.597

Інтенсивність вхідного потоку



Середній час перебування пакета



Середня кількість пакетів

