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 Чорненький Д.І.
(ПІБ)
академічної групи 123м-24-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою «Комп'ютерна інженерія»
(офіційна назва)

на тему «Обґрунтування вибору структури та параметрів мережевих пристроїв комп'ютерної системи e-commerce компанії з використанням інструментів внутрішнього контролю та локального інформаційного ресурсу»
(назва за наказом ректора)

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

Дніпро
2025

ЗАТВЕРДЖЕНО:

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

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

« » _____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

Здобувача вищої освіти Чорненький Д.І. **академічної групи** 123м-24-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія
за освітньо-професійною програмою 123 Комп'ютерна інженерія
офіційна назва)

на тему «Обґрунтування вибору структури та параметрів мережевих пристроїв комп'ютерної системи e-commerce компанії з використанням інструментів внутрішнього контролю та локального інформаційного ресурсу»
затверджену наказом ректора НТУ «Дніпровська політехніка» від 13.10.2025 № 1165-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	Проаналізовано особливості функціонування корпоративних мереж e-commerce та сформульовано мету й завдання дослідження	11.10.2025
Теоретичний	Розглянуто теоретичні основи побудови й аналізу комп'ютерних мереж, методи моделювання та показники якості обслуговування	25.10.2025
Синтез системи	Визначено технічні вимоги та обґрунтовано вибір мережевого обладнання і топології.	15.11.2025
Розроблення програмного забезпечення	Реалізовано конфігурацію мережевих сервісів, механізмів безпеки та математичну модель мережі	29.11.2025
Експериментальний розділ	проведено моделювання та аналіз роботи мережі за різних умов навантаження	06.12.2025

Завдання видано _____ доц. Бешта Д.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі 5 вересня 2025

Дата подання до екзаменаційної комісії 10.12.2025 р.

Прийнято до виконання _____
(підпис здобувача) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 112 с., 28 рисунок, 5 табл., 2 додатки, 19 джерел. E-COMMERCE, КОРПОРАТИВНА МЕРЕЖА, VLAN, VPN, МЕРЕЖЕВЕ МОДЕЛЮВАННЯ, ТОПОЛОГІЯ, БЕЗПЕКА, FIREWALL, QoS, БАЗА ДАНИХ.

Об’єкт дослідження – корпоративна мережа e-commerce платформи, що включає серверну інфраструктуру, мережеве обладнання, систему керування доступом, сервіси обробки даних, внутрішні модулі управління та зовнішні інтеграції.

Мета роботи – проєктування, аналіз і перевірка ефективності корпоративної мережі для e-commerce системи, оцінка її продуктивності в умовах реального навантаження та визначення оптимальних параметрів для забезпечення стабільності, безпеки та масштабованості.

У роботі розглянуто принципи побудови корпоративних мереж, проаналізовано структуру підрозділів та їх топологію. Оглянуто сучасні технології передачі та обробки даних у e-commerce, включаючи протоколи маршрутизації, VPN, VLAN та QoS.

Розроблено математичну модель мережі як системи масового обслуговування, проведено оцінку завантаження сегментів та визначено потенційні точки перевантаження. Сформовано вимоги до інфраструктури, серверних ресурсів, резервування, безпеки, політик маршрутизації та сегментації, визначено оптимальну архітектуру для веб-платформи та інтегрованих сервісів.

Практична частина включала моделювання мережі через віртуалізацію та емулятори, тестове навантаження на бази даних, веб-сервіси та API-взаємодію. Проведено аналіз пропускної здатності, часу реакції, затримок, стабільності з’єднань та стійкості до пікових навантажень, що підтвердило відповідність мережі вимогам та визначило шляхи оптимізації.

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

LAN (Local Area Network) – локальна обчислювальна мережа, що охоплює обмежену територію (офіс, будівля).

WAN (Wide Area Network) – глобальна мережа, що забезпечує з’єднання віддалених об’єктів.

VLAN (Virtual Local Area Network) – віртуальна локальна мережа для логічного сегментування трафіку.

DHCP (Dynamic Host Configuration Protocol) – протокол автоматичної видачі IP-адрес і мережевих параметрів.

DNS (Domain Name System) – система доменних імен, що перетворює доменні імена на IP-адреси.

HTTP/HTTPS (HyperText Transfer Protocol / Secure) – протокол та захищений протокол передавання веб-даних.

SSL/TLS (Secure Sockets Layer / Transport Layer Security) – криптографічні протоколи для захищеної передачі даних.

API (Application Programming Interface) – інтерфейс взаємодії між програмними компонентами.

VPN (Virtual Private Network) – віртуальна приватна мережа для захищеного віддаленого доступу.

TCP/IP (Transmission Control Protocol / Internet Protocol) – базовий набір мережевих протоколів Інтернету.

QoS (Quality of Service) – механізми забезпечення якості обслуговування мережевого трафіку.

SLA (Service Level Agreement) – угода про рівень сервісу між постачальником і користувачем.

DBMS (DataBase Management System) – система керування базами даних.

SKU (Stock Keeping Unit) – код товарної позиції у системах e-commerce.
ERP (Enterprise Resource Planning) – система планування ресурсів підприємства.

CRM (Customer Relationship Management) – система управління взаєминами з клієнтами.

DoS/DDoS (Denial of Service / Distributed Denial of Service) – атаки на відмову в обслуговуванні.

SFTP (Secure File Transfer Protocol) – захищений протокол передавання файлів.

Mbps / Gbps – мегабіт та гігабіт за секунду, одиниці вимірювання швидкості передачі даних.

ms (millisecond) – мілісекунда, одиниця вимірювання затримки.
Load Balancing – метод балансування навантаження між серверами або мережевими ресурсами.

СМО (система масового обслуговування) – математична модель для оцінки роботи мережі під навантаженням.

ЗМІСТ

ВСТУП

Сучасні підприємства електронної комерції функціонують у високо динамічному цифровому середовищі, де безперервна доступність онлайн-платформ, надійність корпоративної мережі та швидкість обробки даних є критично важливими чинниками забезпечення конкурентоспроможності. Корпоративна мережева інфраструктура становить основу для роботи веб-сервісів, CRM- та ERP-систем, аналітичних модулів, баз даних, а також інтеграції з платіжними та логістичними сервісами.

Традиційні або недостатньо оптимізовані мережеві рішення не завжди здатні ефективно обробляти інтенсивні та нерівномірні потоки трафіку, що призводить до затримок, перевантажень і збоїв у роботі інформаційних систем. Особливо гостро ці проблеми проявляються під час пікових навантажень, зокрема у періоди сезонних розпродажів, рекламних кампаній або масових маркетингових акцій.

Використання сучасних підходів до проєктування корпоративних мереж електронної комерції дозволяє забезпечити високу продуктивність, масштабованість і відмовостійкість мережевої інфраструктури. Застосування механізмів сегментації, управління якістю обслуговування (QoS), резервування каналів зв’язку, а також засобів моніторингу трафіку сприяє підвищенню стабільності роботи сервісів і якості обслуговування клієнтів.

Актуальність теми зумовлена необхідністю створення ефективних і надійних корпоративних мереж для підприємств електронної комерції, здатних забезпечувати стабільну роботу інформаційних систем за умов високих і змінних навантажень, а також відповідати вимогам інформаційної безпеки та подальшого масштабування.

Метою роботи є обґрунтування структури корпоративної мережі підприємства електронної комерції, визначення її параметрів і принципів функціонування, а також оцінка ефективності роботи мережі за різних режимів навантаження.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати сучасні технології та підходи до побудови корпоративних мереж електронної комерції;

– дослідити вимоги до продуктивності, надійності та безпеки мережевої інфраструктури;

– визначити оптимальну топологію та структуру корпоративної мережі підприємства e-commerce;

– розробити математичну модель корпоративної мережі та потоків даних у ній;

– дослідити вплив навантаження на показники якості обслуговування (QoS);

– виконати імітаційне моделювання роботи мережі та проаналізувати отримані результати;

– обґрунтувати рекомендації щодо оптимізації та масштабування мережевої інфраструктури.

Об’єктом дослідження є процеси передавання та обробки даних у корпоративній мережі підприємства електронної комерції.

Предметом дослідження є структура, параметри та методи проєктування корпоративної мережі, що забезпечують ефективну роботу інформаційних систем підприємства e-commerce.

Наукова новизна роботи полягає в обґрунтуванні моделі корпоративної мережі підприємства електронної комерції з урахуванням змінних навантажень і показників якості обслуговування, а також у розробці рекомендацій щодо підвищення її продуктивності, надійності та масштабованості.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стан питання

Сфера електронної комерції сьогодні є одним із найбільш динамічних сегментів цифрової економіки. Функціонування інтернет-магазинів, маркетплейсів та сервісів онлайн-продажу критично залежить від надійної, масштабованої та захищеної комп'ютерної мережі. Саме мережеве обладнання визначає стабільність роботи веб-ресурсів, час відгуку сервісів, безперервність обміну даними між модулями бізнес-логіки та доступ до внутрішніх інформаційних систем компанії.

У e-commerce підприємствах мережа обробляє такі типи трафіку:

– запити покупців до веб-платформи;

– транзакційні операції;

– дані CRM та ERP;

– інформацію про складські залишки;

– аналітичні дані та бізнес-метрики;

– внутрішні процеси контролю, логування та моніторингу.

Навантаження на мережу постійно зростає через:

– збільшення кількості онлайн-замовлень;

– розширення асортименту;

– інтеграцію різних зовнішніх сервісів (платіжні шлюзи, служби доставки, сторонні маркетплейси);

– зростання вимог до кібербезпеки;

– перехід на мікросервісну архітектуру та хмарні сервіси.

Важливою частиною побудови мережевої інфраструктури e-commerce компанії є впровадження внутрішнього контролю – системи процедур, політик та інструментів, що забезпечують цілісність даних, безпеку операцій і стабільність роботи сервісів. До таких інструментів належать:

– контроль доступу до мережевих ресурсів;

– моніторинг мережевого трафіку;

– журналювання подій;

– перевірка цілісності даних;

– аудит системних конфігурацій.

Разом з тим, дедалі важливішу роль відіграє локальний інформаційний ресурс – внутрішні сервери, репозитарії, кеш-сховища та бази даних, що забезпечують роботу компанії без залежності від зовнішніх факторів та доступ до критичної інформації в режимі 24/7.

Проблематика проєкту полягає у виборі оптимальної структури мережі, що забезпечить:

– високу пропускну здатність;

– підтримку резервування;

– ефективний контроль доступу;

– відповідність вимогам інформаційної безпеки;

– масштабування без зупинки бізнес-процесів;

– інтеграцію з локальними та хмарними інформаційними ресурсами.

1.2 Характеристика галузі та особливості застосування комп’ютерних систем у сфері e-commerce

Галузь електронної комерції є багаторівневою цифровою екосистемою, яка включає веб-сайти, мобільні застосунки, системи управління товарними запасами, платіжні платформи, логістичні модулі та сервіси аналітики. Усі ці компоненти працюють завдяки мережевій інфраструктурі, що повинна гарантувати високу доступність та безперебійну роботу.

Електронна комерція забезпечує значний внесок у світову економіку:

– глобальний e-commerce ринок перевищив 6,3 трильйона доларів;

– понад 2,6 мільярда користувачів здійснюють покупки онлайн;

– частка e-commerce у роздрібній торгівлі щороку зростає на 8-12%;

У межах e-commerce комп’ютерні мережі використовуються для забезпечення:

1. Мережевої доступності веб-платформи: Безперервний доступ до сайту або мобільного застосунку є ключовою вимогою. Будь-яка затримка або помилка під час завантаження сторінок безпосередньо впливає на втрату клієнтів.

2. Захисту транзакцій та персональних даних: Усі платіжні операції повинні відповідати PCI DSS, а передача персональних даних – вимогам GDPR та локальних законодавчих норм.

3. Оптимізації роботи складу та логістики:

Мережеві пристрої забезпечують комунікацію між:

– WMS (warehouse management system);

– ERP;

– інвентаризаційними терміналами;

– автоматизованими сканерами, вагами, стрічковими системами.

4. Інтеграції з маркетплейсами та зовнішніми сервісами

E-commerce компанія повинна мати стабільні API-канали для роботи з:

– Приват24, LiqPay, Stripe або PayPal;

– Новою Поштою, Meest, DHL;

– Google Analytics, BigData сервісами.

5. Функціонування внутрішніх аналітичних систем: Для прогнозування продажів, аналізу поведінки клієнтів та зберігання логів необхідні високопродуктивні мережі із мінімальною затримкою.

Таким чином, особливості застосування комп’ютерних систем у сфері e-commerce визначають високі вимоги до:

– обробки великих обсягів даних;

– стійкості до перевантажень;

– гнучкого масштабування;

– забезпечення кібербезпеки;

– впровадження засобів внутрішнього контролю.

1.3 Характеристика і структура об’єкта впровадження

Об’єктом впровадження є сучасна e-commerce компанія, діяльність якої спрямована на онлайн-продаж продукції, управління цифровим контентом, аналітику та автоматизацію внутрішніх процесів. Компанія функціонує за принципами централізованого управління та має чітко сформовану організаційну структуру, що забезпечує ефективну роботу всіх ключових напрямів.

Керівництво компанією здійснює Chief Executive Officer (CEO), який координує діяльність функціональних підрозділів та визначає стратегічні задачі розвитку. Підпорядкованість побудована таким чином, щоб забезпечити швидкий обмін інформацією, оперативне ухвалення рішень і безперервність бізнес-процесів у сфері електронної комерції.

Структура компанії

Організаційна структура складається з двох основних блоків:

1. Департамент управління персоналом та адміністративної підтримки:

Цей департамент забезпечує кадрове супроводження, організаційну стабільність і адміністративний менеджмент компанії. У його складі працюють фахівці з HR, адміністратори, офіс-менеджери та координатори, що відповідають за ефективну взаємодію персоналу.

До цього департаменту входять два підрозділи:

Комерційний департамент який здійснює управління продажами, розвиток маркетингових стратегій, роботу з клієнтами та просування товарів у цифровому просторі. Команда складається з менеджерів з продажу, маркетологів, спеціалістів з роботи з клієнтами та контент-менеджерів.

Фінансовий департамент який забезпечує фінансовий облік, контроль руху коштів, підготовку аналітичних фінансових звітів та бюджетне планування. Тут працюють бухгалтери, фінансові аналітики та контролери.

2. Науково-дослідний підрозділ:

Відповідає за технічний розвиток компанії, аналіз нових рішень, дослідження технологій та удосконалення інструментів автоматизації бізнес-процесів. Це ключовий елемент у підтримці інфраструктури e-commerce платформи та її масштабуванні.

До його складу входить:

Виробничий відділ який у контексті e-commerce виконує функції технічної підтримки програмного забезпечення, тестування цифрових продуктів, супроводу інформаційних систем, підготовки та обслуговування обладнання. Також забезпечує стабільну роботу серверів, мережевих ресурсів та систем для обробки замовлень.

Організаційна структура компанії представлена у вигляді ієрархічної функціональної схеми, де кожен підрозділ має чітко визначені функції та зони відповідальності.

На рисунку (рисунок 1.1) наведено структурну схему, яка демонструє підпорядкованість та взаємозв’язок департаментів:

Рисунок 1.1 – Схема організаційної структури

– CEO очолює всю організацію.

– адміністративно-кадровий блок забезпечує підтримку комерційних і фінансових процесів.

– дослідницько-технічний блок відповідає за розробки, технологічну підтримку та операційну стабільність цифрової інфраструктури.

Така структура дозволяє компанії ефективно працювати в умовах динамічного ринку електронної комерції, забезпечуючи швидке реагування на зміни, масштабованість технічних рішень і стабільну роботу внутрішніх сервісів.

Усі структурні підрозділи компанії розташовані в одному приміщенні – офісі, що займає третій поверх нежитлової будівлі за адресою: просп. Лесі Українки, 21, м. Дніпро, Дніпропетровська область, 49000. Офіс складається з п'яти кімнат.(рис 1.3).

Топографічна схема розміщення структурних підрозділів показана на рисунок 1.2

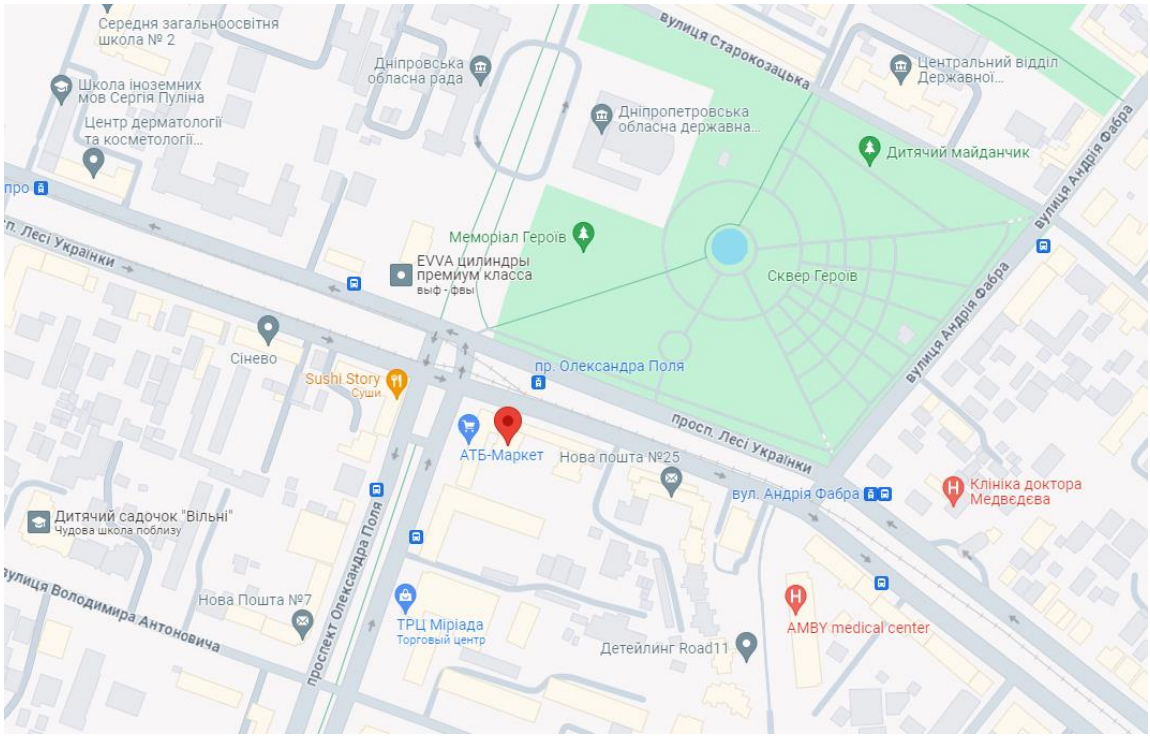


Рисунок 1.2 – Топографічна схема розміщення структурних підрозділів у м. Дніпро

Структурна схема розміщення підрозділів у будівлі включає такі відділи: фінансовий, продажів та маркетингу, адміністративний та кадровий, досліджень та розробок, а також зону досліджень (рисунок 1.3).

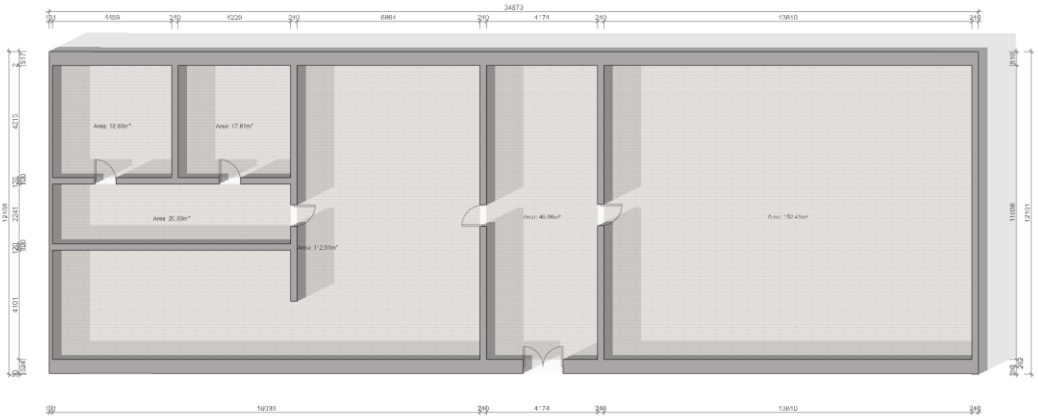


Рисунок 1.3 – Структурна схема розміщення підрозділів у будівлі

1.4 Принципи та технічні способи інформаційного забезпечення об’єкта впровадження

Ефективна робота e-commerce компанії залежить від стабільного функціонування інформаційної інфраструктури, яка забезпечує обробку замовлень, управління даними, комунікацію між підрозділами та взаємодію з клієнтами. Технічне забезпечення базується на сучасних цифрових технологіях, системах автоматизації та інструментах аналітики, що підтримують безперервність бізнес-процесів.

Основні принципи і технічні способи інформаційного забезпечення включають:

1. Автоматизація бізнес-процесів: Системи автоматизації забезпечують оперативну обробку замовлень, управління складськими залишками, формування звітів, контроль логістики та взаємодію з клієнтами. Для цього використовуються CRM-платформи, системи управління контентом (CMS), аналітичні інструменти та модулі автоматичного виставлення рахунків. Автоматизація мінімізує людський фактор і забезпечує швидкий та точний обмін даними між департаментами.

2. Застосування сенсорів, моніторингу та діагностики: Хоча e-commerce не потребує фізичних сенсорів у класичному розумінні, компанія використовує системи цифрового моніторингу:

– контроль навантаження на сервери та веб-платформу;

– моніторинг швидкості обробки транзакцій;

– відстеження стабільності мережевих підключень;

– автоматичне виявлення збоїв та аномалій.

Ці інструменти дозволяють підтримувати безперебійну роботу сайту та внутрішніх сервісів.

3. Системи автоматичного керування та серверної інфраструктури: В основі інформаційної системи компанії працюють сервери, мережеві схеми та хмарні сервіси, які забезпечують:

– обробку великого обсягу даних;

– масштабування при збільшенні навантаження;

– стабільність роботи служб, пов’язаних із продажами, оплатами та комунікацією.

Мікросервісна архітектура або модульні системи керування дозволяють швидко вносити зміни та адаптувати функціонал під потреби бізнесу.

4. Системи віддаленого доступу та управління: Сучасні e-commerce компанії активно використовують хмарні сервіси та віддалений доступ для:

– роботи персоналу з будь-якого місця;

– адміністрування серверів і сервісів;

– дистанційного оновлення платформи;

– керування службами підтримки клієнтів.

Використання VPN, багатофакторної авторизації та корпоративних кабінетів забезпечує безпечний доступ до внутрішніх ресурсів.

5. Безпека та захист даних: Оскільки компанія обробляє персональні дані користувачів, транзакції та конфіденційну бізнес-інформацію, впроваджуються комплексні засоби кіберзахисту:

– шифрування каналів зв’язку;

– автентифікація та контроль доступу;

– системи виявлення вторгнень (IDS/IPS);

– резервне копіювання і відновлення даних;

– захист від DDoS-атак.

Ці заходи гарантують цілісність даних та надійну роботу всіх сервісів.

6. Мережева інфраструктура: Для роботи e-commerce платформи критично важлива стійка та оптимізована мережа, що включає:

– локальні сервери та маршрутизатори;

– хмарні елементи інфраструктури;

– Wi-Fi та кабельні сегменти для офісного персоналу;

– системи розподілу навантаження;

– резервні канали зв’язку.

Стабільна мережа забезпечує високу доступність, швидкість обробки даних та підтримку роботи всіх цифрових сервісів компанії.

1.5 Аналіз існуючих методів обробки та передачі інформації для корпоративної мережі e-commerce

Ефективна корпоративна мережа для e-commerce платформ повинна забезпечувати стабільну обробку замовлень, швидке передавання даних між модулями системи, високий рівень безпеки та готовність до масштабування. Для цього застосовуються сучасні мережеві технології, що дозволяють підтримувати роботу веб-сервісів, систем аналітики, платіжних шлюзів і внутрішніх операцій бізнесу.

У корпоративних e-commerce інфраструктурах поєднуються дротові й бездротові канали.

Ethernet використовується в магістральній частині мережі для підключення серверів, робочих станцій персоналу, робочих зон складу та офісу. Ця технологія гарантує високу пропускну здатність, низьку затримку й стійкість до перешкод.

Wi-Fi забезпечує мобільність співробітників (логісти, менеджери, маркетологи, технічний персонал). Також він використовується для підключення IoT-пристроїв у складських приміщеннях: сканерів штрих-кодів, терміналів збору даних, датчиків контролю середовища.

MPLS (Multiprotocol Label Switching) застосовується у великих e-commerce мережах, де є потреба в гарантованій якості сервісу. Це дозволяє прокладати віртуальні маршрути між дата-центром, офісом і складам, забезпечуючи стабільну передачу трафіку критично важливих систем – CRM, ERP, систем обліку товарів.

Також VPN є необхідністю для e-commerce бізнесів, оскільки: забезпечує захищений доступ співробітників до внутрішніх ресурсів (адмін-панель магазину, база товарів, інструменти розробників). Дозволяє безпечно керувати серверами, навіть якщо вони знаходяться у хмарі або на фізичному майданчику партнера. Шифрує весь трафік, що особливо важливо при роботі з конфіденційними замовленнями, персональними даними клієнтів і платіжними операціями.

Принципи побудови корпоративної мережі для e-commerce:

– масштабованість і гнучкість.

E-commerce бізнес швидко розвивається, а кількість підключених сервісів та вузлів постійно зростає (нові склади, офісні підрозділи, маркетингові інструменти, сервіси доставки). Тому мережа повинна легко масштабуватися – як горизонтально (нові пристрої, сегменти), так і вертикально (збільшення пропускної здатності).

– надійність та стійкість до збоїв.

Корпоративна система повинна працювати безперервно – кожна хвилина простою призводить до реальних фінансових втрат. Для цього впроваджуються:

1) резервні канали зв’язку,

2) дублювання критичних мережевих пристроїв,

3) автоматичне перемикання на альтернативні маршрути,

4) постійний моніторинг завантаження трафіку.

– безпека.

Оскільки e-commerce постійно оперує персональними даними та платіжною інформацією, основними задачами є захист від:

1) зовнішніх атак (DDoS, MITM, перехоплення трафіку),

2) внутрішніх загроз (несанкціонований доступ до баз даних),

3) витоку клієнтської інформації.

Сучасні підходи включають застосування брандмауерів, систем IDS/IPS, сегментацію мережі, багатофакторну автентифікацію, застосування SSL/TLS-шифрування.

1.5.1 Популярні рішення та мережеві продукти на ринку

Для побудови стабільної мережі e-commerce найчастіше використовують обладнання провідних виробників:

– Cisco Systems: Пропонує широкий спектр рішень для офісних, складських і серверних інфраструктур – комутатори, маршрутизатори, брандмауери, Wi-Fi-точки, а також технології побудови VPN і MPLS. Вважається стандартом індустрії для великих e-commerce компаній.

– Juniper Networks: Відомий своїми високопродуктивними маршрутизаторами й захисними системами. Підходить для дата-центрів, у яких розміщуються веб-сервери інтернет-магазину, системи аналітики й бази даних.

– HPE (Hewlett Packard Enterprise): Пропонує економічно ефективне та масштабоване обладнання для комутації, бездротових мереж та побудови серверних комплексів. Часто використовується у середніх і великих e-commerce проєктах.

1.6 Постановка завдання дослідження.

Метою даного дослідження є оцінка продуктивності, стійкості та ефективності корпоративної мережі e-commerce платформи, а також визначення її можливостей щодо підтримки зростаючих навантажень, пов’язаних із роботою веб-сервісів, баз даних, внутрішніх систем управління та зовнішніх інтеграцій. Для цього необхідно виконати комплекс досліджень, спрямованих на моделювання поведінки мережі, аналіз затримок у вузлах та розробку рекомендацій щодо оптимізації інфраструктури.

Першим етапом є аналіз навантаження на мережу. Необхідно відтворити її топологію у віртуальній моделі та перевірити, як різні типи бізнес-трафіку – запити до веб-платформи, операції з базами даних, синхронізація CRM/ERP, робота API та реплікація сервісів – впливають на пропускну здатність і стабільність. Особливо важливо змоделювати пікові сценарії, характерні для e-commerce (акції, сезонні розпродажі), щоб визначити реальні межі навантаження та виявити вузли з потенційними втратами або перевантаженням каналів.

Другим завданням є визначення часу обробки даних на ключових мережевих вузлах. Для цього слід зафіксувати затримки під час проходження трафіку через комутатори, маршрутизатори, сервери зберігання та сервери веб-додатків. Засоби моніторингу (SPAN, Wireshark, Zabbix/Prometheus) дають змогу оцінити, як швидко обробляються внутрішні та зовнішні запити, чи виникають черги, та які сегменти інфраструктури затримують критично важливі операції – наприклад, звернення до бази даних або зовнішніх сервісів оплати й логістики.

На основі отриманих даних формується математична модель мережі як системи масового обслуговування. Це дозволяє прогнозувати її поведінку при різних навантаженнях, оцінювати час очікування, ймовірність виникнення черг, рівень завантаженості окремих вузлів та загальну ефективність архітектури. Модель також дає змогу знайти оптимальні параметри функціонування мережі та визначити межі її масштабованості.

Завершальним етапом є формування рекомендацій щодо покращення продуктивності. На основі результатів моделювання та аналізу затримок будуть визначені необхідні оптимізації конфігурації комутаторів, маршрутизаторів, серверних вузлів, політик маршрутизації, а також підходи до балансування навантаження між сегментами мережі та сервісами.

Таким чином, завдання дослідження полягає у комплексному аналізі роботи корпоративної мережі e-commerce системи, прогнозуванні її поведінки та розробці інженерних рішень, що підвищать стабільність, масштабованість та швидкодію всієї інфраструктури.

1.7 Висновок до першого розділу

У розділі проаналізовано сучасний стан та особливості функціонування корпоративних комп’ютерних мереж у сфері електронної комерції. Показано, що e-commerce є високонавантаженою та динамічною галуззю, у якій мережна інфраструктура відіграє ключову роль у забезпеченні стабільності бізнес-процесів, безпеки даних, швидкодії сервісів і безперервності обслуговування клієнтів. Розглянуто типи трафіку, характерні для e-commerce платформ, та фактори, що зумовлюють постійне зростання навантаження на мережу.

Окрему увагу приділено характеристиці галузі електронної комерції, вимогам до комп’ютерних систем і мереж, а також ролі внутрішнього контролю та локальних інформаційних ресурсів. Описано об’єкт впровадження, його організаційну структуру та просторове розміщення підрозділів, що є важливим для подальшого проєктування й аналізу мережевої інфраструктури.

Також узагальнено принципи та технічні способи інформаційного забезпечення e-commerce компанії, проаналізовано існуючі методи обробки й передачі даних, а також сучасні мережеві технології та популярні рішення, що застосовуються на ринку. На основі проведеного аналізу сформульовано мету та завдання дослідження, спрямовані на оцінку продуктивності, стійкості й

масштабованості корпоративної мережі та розробку рекомендацій щодо її оптимізації.

2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Теоретичне обгрунтування мережевих параметрів

2.1.1 Метод вирішення

Для досягнення поставлених завдань застосовуються такі підходи як:

– моделювання мережі за допомогою програмних комплексів;

– збір та аналіз мережевих параметрів;

– комп'ютерне і статистичне імітаціине моделювання.

2.1.1.1 Моделювання мережі: програмні комплекси моделювання

У процесі дослідження мережевих параметрів одним із ключових методів е моделювання. Це дозволяє створити віртуальне середовище, в якому можна тестувати різні конфігурації, перевіряти продуктивність і аналізувати поведінку системи за різних умов. Для моделювання використовуються спеціалізовані програмні комплекси, кожен із якє має свої особливості.

Cisco Packet Tracer е простим у використанні симулятором, що підходить для створення базових мережевих топологій та їх тестування. Його перевага полягає в наочності та можливості працювати з обмеженим набором пристроїв, які повністю віртуалізовані. Це робить програму чудовим інструментом для початкового етапу проектування мережі. Однак, Packet Tracer не підтримуй роботу з реальними мережевими образами, що обмежує його використання для дослідження складних сценаріїв.

EVE-NG, на відміну від Packet Tracer, е потужною платформою для віртуалізації реальних мережевих образів. Цей комплекс дозволяє створювати мережі з використанням програмного забезпечення пристроїв, таких як Cisco, Juniper, або інші виробників. Завдяки цьому результати моделювання е більш наближеними до реальних умов. Крім того, EVE-NG забезпечує інтеграцію із зовнішніми інструментами для аналізу трафіку, такими як Wireshark.

Недоліком може бути більша складність у використанні та потреба в потужних апаратних ресурсах. Особливістю EVE-NG можливість створення віртуальних мереж, які можуть бути інтегровані з реальними мережами, включно з Інтернетом. Це досягається через використання різних методів з'єднання, таких як підключення до фізичних мережевих інтерфейсів або налаштування віртуальних маршрутизаторів та комутаторів для забезпечення взаємодій з зовнішніми мережами. Завдяки цьому, можна моделювати реальні умови з підключенням до Інтернету, що дає змогу тестувати роботу мережі в умовах реального трафіку та оцінювати її поведінку при інтеграції з існуючими інфраструктурами. Це робить EVE-NG потужним інструментом для створення та тестування гібридних мереж, які поєднують віртуальні та фізичні елементи.

Mininet спеціалізуються на моделюванні програмно-конфігурованих мереж (SDN). Цей інструмент дозволяє швидко розгортати мережеві сценарії з великим числом вузлів та тестувати алгоритми маршрутизації чи керування трафіком.

2.1.1.2 Мережеві пристрої та їх застосування для тестування мережі

Окрім програмного моделювання, для вивчення параметрів мережі важливу роль відіграють апаратні засоби та методи їх використання. Реальні пристрої забезпечують точні дані про поведінку мережі, дозволяють тестувати специфічні конфігурації та отримувати результати в умовах, наближених до реальних.

Одним із ключових механізмів є використання комутаторів, маршрутизаторів і шлюзів, які забезпечують передачу даних між вузлами. Ці пристрої дозволяють організувати тестове середовище, де можна вимірювати затримки, джитгер, втрати пакетів, а також продуктивність у різних умовах навантаження.

Для аналізу мережевого трафіку широко застосовуються механізм дзеркалювання портів (SPAN або RSPAN) [13]. Він дозволяє перехоплювати пакети, які проходять через задані порти мережевих пристроїв, і направляти їх

до системи збору даних. На основі цих даних за допомогою програмного забезпечення, такого як Wireshark, проводиться аналіз параметрів протоколів, зокрема RTP, що використовуються для передачі голосу та відео.

Таким чином, використання апаратного забезпечення дозволяє проводили комплексні дослідження мережевих параметрів, перевіряти роботу мережі в умовах реального навантаження та оптимізувати її функціонування для критичних застосувань, таких як IP-телефонія та системи відеоспостереження.

2.1.1.3 Комп'ютерне і статистичне імітаційне моделювання

Комп'ютерне і статистичне імітаційне моделювання є важливим інструментом для детального вивчення та аналізу складних систем, зокрема комп'ютерних мереж, інформаційних технологій, бізнес-процесів та інших галузей, де велика кількість змінних і взаємодій потребує комплексного підходу. Застосування цього методу дозволяє створювати віртуальні моделі реально систем, що дає змогу детально аналізувати їхню роботу, прогнозувати результати функціонування та знаходити способи підвищення ефективності.

Імітаційне моделювання надає можливість відтворювати і досліджувати різноманітні сценарії, що імітують поведінку системи під дією заданих параметрів і умов. Це дає змогу заздалегідь оцінювати, як система реагуватиме на зміни в умовах експлуатації, виявляти оптимальні шляхи її розвитку, а також виявляти потенційні ризики або недоліки в її конструкції чи управлінні. Такий підхід сприяє глибшому розумінню того, як функціонує система, дозволяє вдосконалювати її, роблячи більш адаптованою до непередбачуваних ситуацій.

Статистичне імітаційне моделювання в свою чергу застосовує статистичні методи для детального аналізу результатів моделювання. Зокрема, теорія ймовірностей, регресійний аналіз, аналіз варіацій і багато інших статистичних методів використовуються для обробки та інтерпретації зібраних даних, що дозволяє отримувати не лише точні, а й обґрунтовані

висновки. Цей процес допомагає виявляти закономірності, оцінювати ймовірність настання події, аналізувати тренди і проводити порівняння з іншими сценаріями.

Завдяки поєднанню комп'ютерного та статистичного підходів, імітаційне моделювання дозволяє здійснювати багатосторонній аналіз, підвищувати ефективність системи, приймати обґрунтовані рішення і значно зменшувати ризики. У середовищах з високою невизначеністю та динамікою, такт як сучасні комп'ютерні мережі, такий підхід е надзвичайно корисним для забезпечення надійності та стійкості роботи системи, оскільки надає можливість здійснювати адаптивне управління в реальному часі.

Задачі, що пов'язані з аналізом замкнутих мереж масового обслуговування, часто вирішуються за допомогою комп'ютерного моделювання. У таких мережах кількість одиниць у системі, тобто кількість пакетів, фіксована, і вони циркулюють між різними вузлами. Завдяки симуляціям можна оцінити ефективність мережі, її параметри та зрозуміти, як поведінка мережі змінюється під різними умовами. Однак ці стимуляційні моделі можуть бути складними у реалізацій та аналізі, тому е необхідність у використанні математичних моделей, які дозволяють спростити цей процес та зробити результати більш загальними та застосовними до широкого кола задач.

Одним із основних математичних інструментів для аналізу замкнутих мереж с алгоритм Бузена, який дозволяє розраховувати характеристику мережі, зокрема очікувану кількість пакетів у кожному з вузлів, час їх перебування в мережі та інші параметри. Алгоритм дає змогу моделювати ситуацію, коли кількість одиниць у системі постійна, і вони циркулюють між різними вузлами з певними ймовірностями. Цей метод дозволяє отримати точні результати, не вдаючись до складних симуляцій, що робить його ідеальним для широкого застосування [14].

У даному прикладі розглядаються замкнена мережа масового обслуговування, що складеться з кількох вузлів, через які передаються пакети

даних. Ця модель дозволяє оцінити характеристики мережі, такі як навантаження, часи затримок, ймовірність втрат пакетів та ефективність обробки трафіку на різних етапах.

Мережа складається з M вузлів, кожен з яких має певну пропускну здатність для обробки пакетів. Кожен вузол обробляєє пакети з певною ймовірністю, і після обробки пакети можуть переміщатися на інші вузли за визначеними ймовірностями. Ці ймовірності переходу між вузлами визначають ефективність маршрутизацій та навантаження на мережу.

Модель замкненої мережі масового обслуговування дозволяє аналізувати потоки трафіку та обчислювати різні параметри мережі, включаючи затримки, навантаження на вузли, ймовірність втрат пакетів та інші важливі характеристики. За допомогою такої моделі можна оптимізувати роботу мережі та забезпечити ефективну передачу даних навіть за високих навантажень.

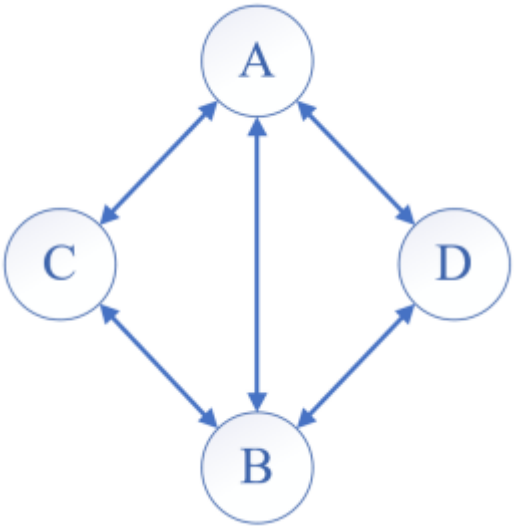


Рисунок 2.1 – Графова модель комп'ютерної мережі

Мережа складається з чотирьох вузлів (A, B, C, D), між якими існують спрямовані зв'язки. Кожен вузол відповідає за обробку пакетів, і зв'язки між ними характеризуються ймовірністю передачі пакетів.

Визначення ймовірностей передачі пакетів.

Задаємо ймовірність передачі пакета між кожним з вузлів. Вона подається у вигляді матриці ймовірностей переходів P, де кожен елемент Pij – це ймовірність того, що пакет, що надійшов у вузол i, буде переданий до вузла j.

$$P = \begin{pmatrix} P_{AA} & P_{AB} & P_{AC} & P_{AD} \\ P_{BA} & P_{BB} & P_{BC} & P_{BD} \\ P_{CA} & P_{CB} & P_{CC} & P_{CD} \\ P_{DA} & P_{DB} & P_{DC} & P_{DD} \end{pmatrix}, \quad (2.1)$$

При цьому, ймовірність того, що вузол зв'язується сам з собою Pii дорівнює 0.

Матриця обробки пакетів.

Кожен вузол має певний час на обробку пакета. Час обробки μi для вузла i визначає, скільки часу потрібно для обробки одного пакета.

Матриця обробки пакетів може бути представлена як:

$$T = \begin{pmatrix} T_A \\ T_B \\ T_C \\ T_D \end{pmatrix}, \quad (2.2)$$

де TA, TB, TC, TD – це час обробки пакета в вузлах A, B, C та D відповідно.

Модель масового обслуговування для кожного вузла.

Кожен вузол мережі можна трактувати як систему масового обслуговування (queueing system), де пакети, що надходять у вузол, обробляються по черзі. Для таких систем розраховуються стандартні параметри, зокрема:

– Інтенсивність потоку пакетів (λi): кількість пакетів, що надходять у вузол i за одиницю часу.

– Час перебування пакета в системі (Wi): середній час, що пакет проводить у вузлі i (включаючи час обробки та час очікування в черзі).

– Кількість пакетів в черзі (Ni): середня кількість пакетів, що знаходяться в обробці або в черзі на обробку у і-му вузлі.

Ці параметри для кожного вузла можна розрахувати, використовуючи теорію масового обслуговування.

Метод Бузена в контексті комп'ютерного та статистичного імітаційного моделювання зазвичай використовується для моделювання складних систем і процесів, де враховуються випадкові зміни і стохастичні явища.

Це метод, який застосовується для оцінки ймовірностей або прогнозування результатів в умовах невизначеності.

Зазначений метод має широкий спектр використання в різних сферах, зокрема для прогнозування поведінки мереж, оцінки ризиків, розробки стратегії управління та оптимізації технічних систем.

2.2 Огляд метрик якості обслуговування в комп’ютерних мережах

Якість функціонування мережі визначається кількома основними параметрами, кожен з яких впливає на ефективність передачі даних та задоволення потреб користувачів. Розуміння цих параметрів дозволяє не лише оцінити поточний стан мережі, але й визначити заходи для покращення її продуктивності.

Швидкість передачі даних (Throughput): Цей параметр характеризує фактичну швидкість передачі даних, з якою стикається користувач під час роботи з мережею.

Пропускна здатність (Bandwidth): Цей параметр характеризує обсяг даних, які можуть передаватися через мережевий канал за одиницю часу, тобто «ширину» або ємність каналу передачі даних. Вимірюється в бітах на секунду (bps) і є ключовим фактором, який визначає, наскільки швидко мережа може обробляти великі обсяги трафіку.

Різниця між пропускною здатністю і швидкістю.

Пропускна здатність визначає ємнісний параметр каналу обґрунтовуючись теоретично, тоді як швидкість задає кількісну

характеристику, яку можна визначити емпірично, тобто вона залежить від поточних умов роботи з’єднання. Наприклад, якщо канал має широку смугу пропускання, але при цьому в конкретний момент часу присутнє високе мережеве навантаження спричинене конкуренцією за канали передачі, недостатньою обчислювальною спроможністю серверів або мережевого обладнання, фактична швидкість з'єднання може бути значно нижчою від заявленого номіналу [19].

Затримка (Delay, Latency): Затримка це параметр що описує час, потрібний для того, щоб пакет даних пройшов від відправника до отримувача. Чим менша затримка, тим менше часу на відгук потребується при роботі в мережі. Термін затримка часто використовується як синонім із латентністю, але між ними є тонка різниця.

Латентність, від лат. latentis – прихований, невидимий, це затримка мережі що стосується загального часу, необхідного для надсилання всього повідомлення, тоді як затримка розповсюдження (Propagation delay) означає час, необхідний для проходження першого біта по каналу між відправником і одержувачем [20].

Затримка розповсюдження описується формулою, d/s, де d – відстань, а s – це швидкість поширення хвилі. Затримка вимірюється в мілісекундах (ms), і її зниження є пріоритетом для додатків реального часу, таких як IP-телефонія або відеозв'язок. На рисунку 2.4 подано діаграму внесків в затримку мережі.

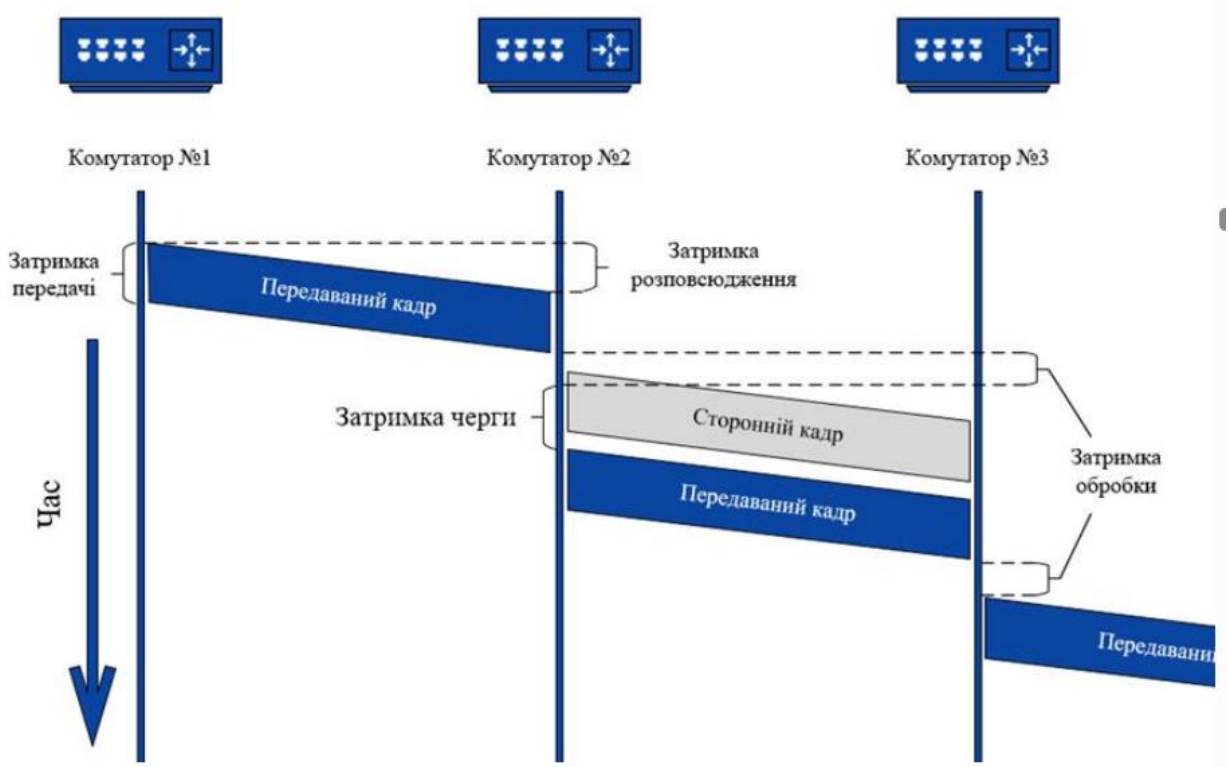


Рисунок 2.2 – Діаграма внесків в затримку мережі

Затримка передачі (Transmission Delay) – визначає, скільки часу потрібно для передачі всіх біт даних через фізичний канал зв'язку. Цей час прямо пропорційний розміру пакету та обернено пропорційний пропускній здатності каналу. Чим більший пакет або менша пропускна здатність каналу, тим довше триватиме передавання.

Затримка розповсюдження, або поширення (Propagation Delay) – це час, який потрібен сигналу, щоб пройти від відправника до отримувача. Він залежить від відстані між пристроями і швидкості поширення сигналу (наприклад, швидкості світла в оптичному волокні або кабелі). Довші відстані або повільніші носії сигналів збільшують час поширення.

Затримка обробки (Processing Delay) – визначає, скільки часу потрібно для обробки пакету в мережевих пристроях, таких як маршрутизатори, комутатори або сервери. Цей час включає перевірку заголовків пакету, маршрутизацію та інші операції. Чим складніші операції обробки, тим більше часу потрібно.

Затримка черги (Queuing Delay) – це час, який пакет очікує в черзі перед тим, як бути переданим через мережу. Цей час залежить від навантаження на мережевий вузол і рівня трафіку. В умовах високого навантаження пакети можуть затримуватися довше, чекаючи своєї черги на передавання. Затримка обробки на кінцевих пристроях (End-Device Processing Delay): Час обробки на кінцевих пристроях визначає, скільки часу потрібно для обробки даних на кінцевих пристроях перед передачею чи після отримання даних. Це залежить від продуктивності кінцевих пристроїв і типу додатка. Наприклад, обробка великих об'ємів даних на повільному пристрої може зайняти більше часу.

Тремтіння, джиттер (Jitter): Цей параметр характеризує коливання тривалості затримки між окремими пакетами [21]. Наприклад, якщо один пакет досягає кінцевого пункту за 30 мс, а наступний – за 40 мс, джиттер у цьому випадку становитиме 10 мс. Джиттер є критичним параметром для мультимедійних сервісів, де постійний потік даних забезпечує високу якість звуку чи зображення.

Для зменшення впливу тремтіння широко використовується буфер джиттеру Принцип роботи буфера джиттеру полягає у тимчасовому зберіганні вхідних пакетів, які надходять із різними затримками, та синхронізації їх перед відтворенням. Це дозволяє уникнути пропусків або спотворень у передачі голосу, відео чи інших потокових даних. Наприклад, у випадку, якщо пакет надходить із запізненням, буфер може компенсувати затримку, подаючи попередньо збережені дані, забезпечуючи таким чином безперервність потоку, як це зображено на рисунку 2.2 [22].

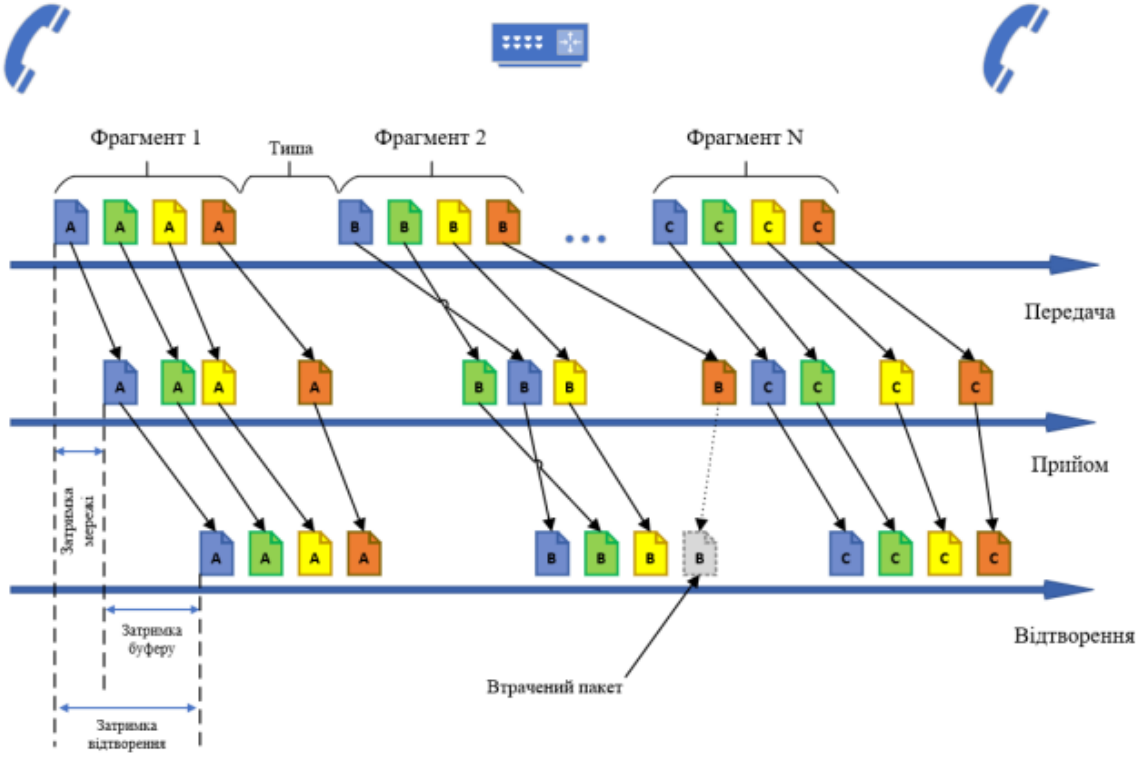


Рисунок 2.3 – Процес передачі та відтворення пакетів у мережі

Визначення оптимального розміру цього буфера є ключовим завданням, адже неправильний вибір може призвести до збільшення затримки зв'язку, як це зображено на рисунку 2.3.

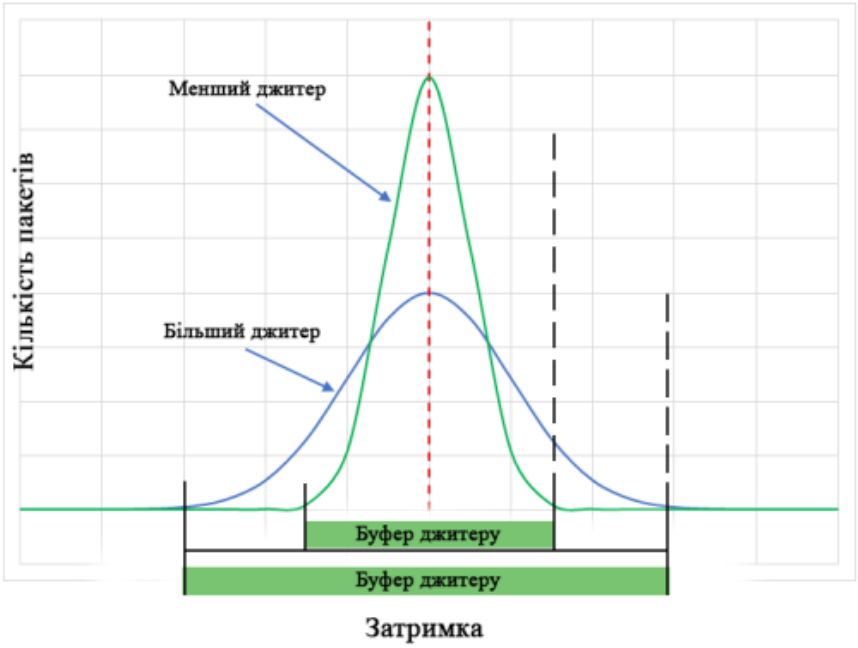


Рисунок 2.4 – Діаграма внесків в затримку мережі

Втрата пакетів (Loss): Під час передачі даних через мережу деякі пакети можуть бути втрачені, не досягши кінцевої точки. Втрата пакетів негативно впливає на якість даних, оскільки знижує цілісність переданої інформації. Оптимізація QoS спрямована на мінімізацію втрат, щоб забезпечити безперебійну передачу даних.

2.3 Мережеві технології для забезпечення якості обслуговування

Забезпечення якості обслуговування (QoS) – це сукупність технологій та методів управління мережевим трафіком, спрямованих на забезпечення надійності, мінімізації затримок та стабільності передачі даних у мережі [23]. QoS відіграє критичну роль у сучасних корпоративних мережах, де працюють різні типи трафіку – від базових веб-запитів до складних сервісів реального часу, таких як IPтелефонія чи відеоконференції. Мережі, що впроваджують QoS, здатні забезпечити необхідні ресурси для кожного типу трафіку, підтримуючи ефективність, стабільність і високу якість обслуговування для користувачів.

Основні технології QoS:

– Класифікація і маркування трафіку. Для ефективного управління трафіком першим кроком є класифікація даних. Класифікація передбачає розподіл пакетів у категорії, залежно від їхньої важливості або типу послуг, що забезпечуються. Для маркування таких пакетів використовується протокол DSCP (Differentiated Services Code Point), що дозволяє ідентифікувати пакети різних типів. Кожен пакет отримує мітку, яка вказує на його пріоритет, що дає можливість мережевим пристроям (маршрутизаторам, комутаторам) коректно обробляти його. Класифікація і маркування є базовими елементами для роботи інших технологій QoS, адже вони дозволяють чітко ідентифікувати критично важливий трафік, як VoIP або відеоконференції.

– Пріорітизація трафіку – це метод, за допомогою якого окремі типи трафіку отримують певний пріоритет в обслуговуванні. Наприклад, пакети з високим пріоритетом (наприклад, голосовий або відеотрафік) можуть

оброблятися першими, навіть якщо мережа завантажена. Це гарантує, що чутливий до затримок 48 трафік не відчуватиме перешкод через низько пріоритетні дані, як електронна пошта чи завантаження файлів. Зокрема, технологія WFQ (Weighted Fair Queueing) забезпечує можливість розподілу пропускної здатності між різними чергами, виділяючи більше ресурсів тим потокам, які мають більший пріоритет.

– Політики керування трафіком (Traffic Policing) – це механізм обмеження трафіку, шляхом відкидання пакетів, які перевищують задану швидкість передачі, як це подано на рисунку 2.4 [24]. Це корисно для забезпечення дотримання певних правил у межах угод про якість обслуговування (SLA). Якщо обсяг даних перевищує встановлений ліміт, надлишкові пакети або відкидаються, або позначаються як «низько пріоритетні». Policing може бути жорстким способом контролю над споживанням пропускної здатності, особливо в корпоративних мережах з обмеженими ресурсами.

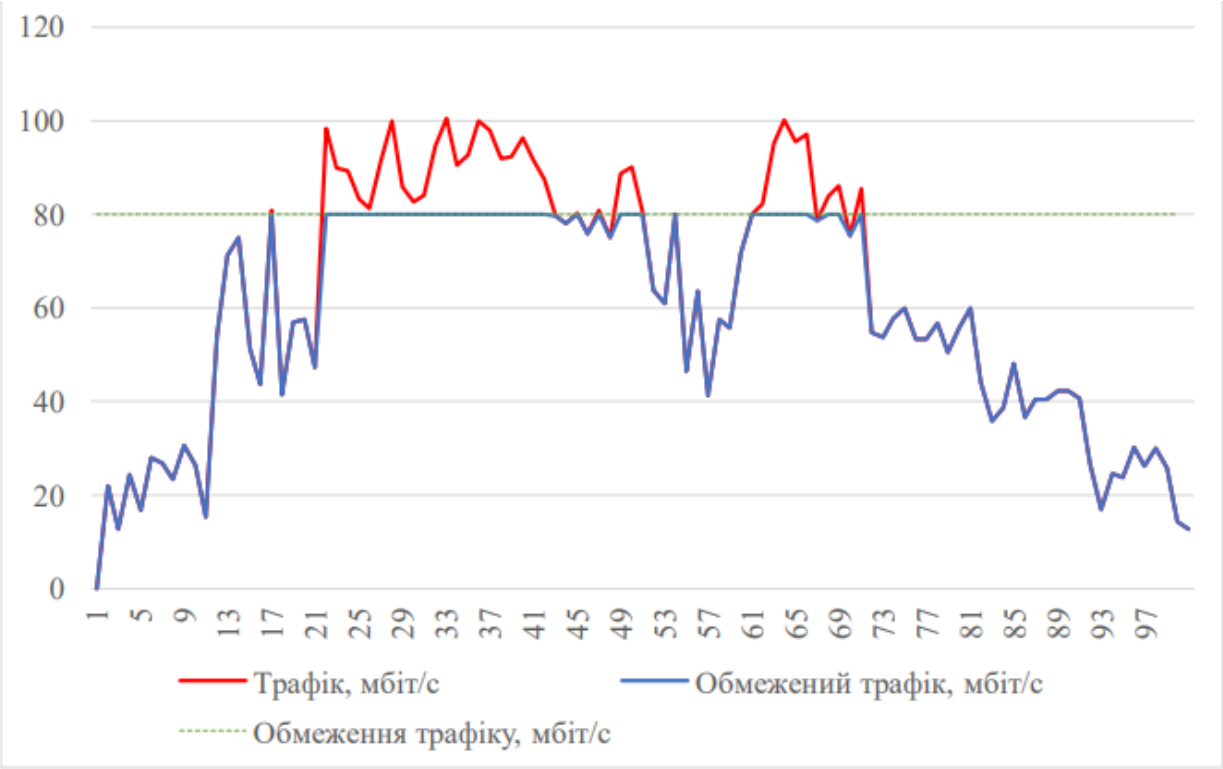


Рисунок 2.5 – Графік впливу політик керування трафіком на передачу інформації

Формування (шейпінг) трафіку (Traffic Shaping). Мережеві пристрої працюють на фізичному рівні, передаючи біти зі швидкістю, визначеною тактовою частотою їх апаратного забезпечення. З технічної точки зору, мережеві інженери можуть контролювати майже все, що стосується налаштування передачі даних, але вони не можуть сповільнити електричний або оптичний сигнал у кабелі довільно, за потребою. Тобто фізично зробити так, щоб сигнали передавалися повільніше, ніж дозволяє тактова частота пристрою неможливо з декількох причин, що пов’язані з принципами фізики сигналів, стандартами передачі даних, і технічними обмеженнями мережевих пристроїв:

– фізична обмеженість лінії зв’язку та інтерфейсів: Мережеві інтерфейси, такі як Ethernet, оптичні канали або серійні порти, розроблені з конкретною частотою передачі даних. Ця частота – це результат не тільки електронної схеми пристрою, а й фізичних характеристик середовища передачі (наприклад, властивостей кабелю або волоконного світловоду). Ці фізичні параметри визначають максимальну частоту сигналу, яка може передаватися без значних втрат якості та цілісності сигналу.

– протоколи та стандарти: Технології зв’язку, як Ethernet, мають чітко визначені стандарти швидкості передачі даних (наприклад, 10 Мбіт/с, 100 Мбіт/с, 1 Гбіт/с тощо). Кожен стандарт має свої технічні параметри, що стосуються частоти тактових імпульсів, кодування сигналів, електромагнітної сумісності тощо. Зміна тактової частоти означала б відступ від цього стандарту, що призвело б до порушення сумісності між пристроями.

– частотна синхронізація між пристроями: Усі мережеві пристрої у зв’язку повинні бути синхронізовані, тобто «узгоджувати» частоту передачі для коректного обміну даними. Змінюючи частоту на одному з пристроїв, виникає порушення синхронізації, що спричинить втрати пакетів, збої у зв’язку, а іноді й повне припинення зв’язку. Коли необхідно обмежити швидкість передачі даних (наприклад, до рівня меншого, ніж підтримує канал), пристрої використовують метод тимчасового призупинення передачі –

«формування» трафіку. Замість того, щоб зменшити швидкість передачі інформації протягом всього проміжку часу, мережевий пристрій чергує періоди активної передачі пакетів з паузами. Таким чином знижується середнє значення швидкості передачі інформації, не обмежуючи загальну пропускну здатність каналу що використовується для передачі даних.

Розглянемо конкретний приклад: припустимо, канал має пропускну здатність 64 кбіт/с. Якщо необхідно обмежити середню швидкість передачі даних між заданими вузлами до 32 кбіт/с, то для досягнення цієї мети мережевий пристрій повинен забезпечити періодичне передавання даних упродовж 50% загального часу, залишаючи інші 50% часу в режимі тиші, як це зображено на рисунку 2.5. Це дозволяє не лише знизити середню пропускну здатність до половини фізичної пропускної здатності каналу, тобто до 32 кбіт/с, але й звільнити ресурс каналу для передачі інших пакетів.\

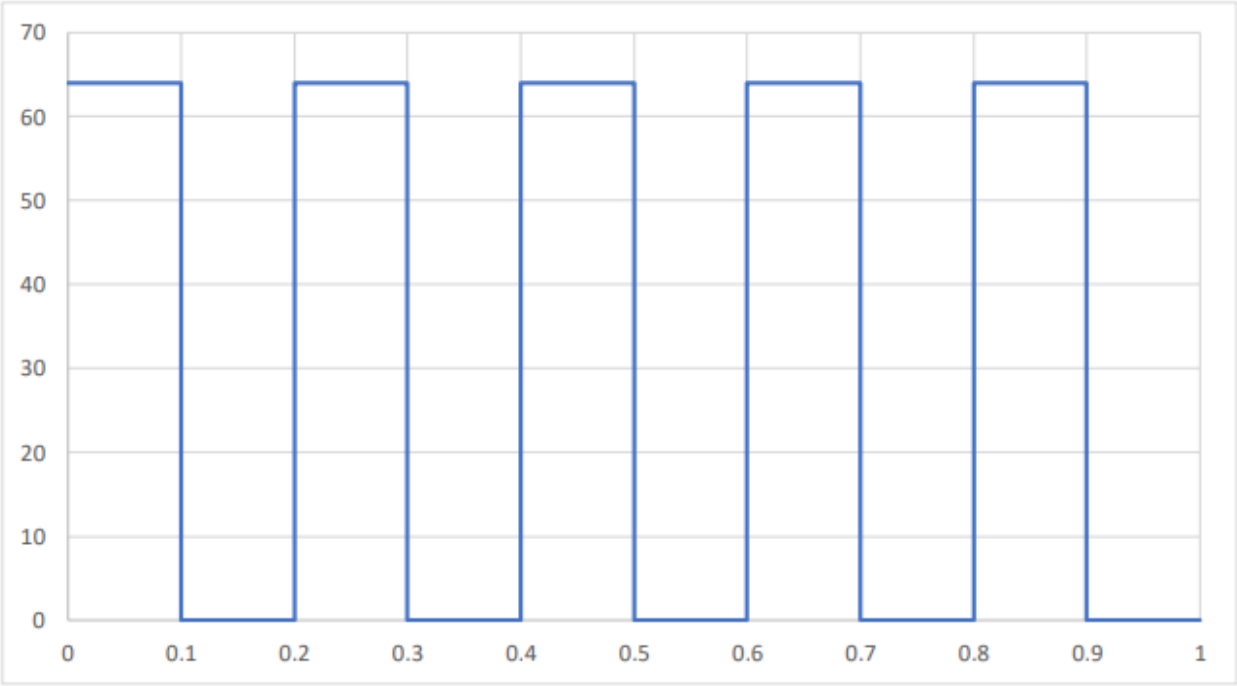


Рисунок 2.6 – Графік імпульсно-періодичної передачі даних з середньою швидкістю 32 кбіт/с

Якщо канал з пропускною здатністю 64 кбіт/с потрібно обмежити до середньої швидкості 28 кбіт/с, мережевий пристрій повинен передавати дані протягом 44% часу та зупиняти передачу на 56% часу. Це досягається шляхом

чергування активних періодів передачі даних і пауз, забезпечуючи таким чином зниження середньої пропускної здатності до бажаного рівня.

$$T_{\text{передачі}} = V/C = \frac{28}{64} = 0{,}4375 \approx 44\%, \tag{2.3}$$

де V – необхідна швидкість передачі інформації, кбіт/с;

C – пропускна здатність каналу, кбіт/с;

28 / 64 = 0.75, тобто передача даних здійснюється 75% від загальної тактової частоти каналу, досягаючи таким чином необхідного середнього показника у 96 кбіт/с, як це подано на рисунку 2.6.

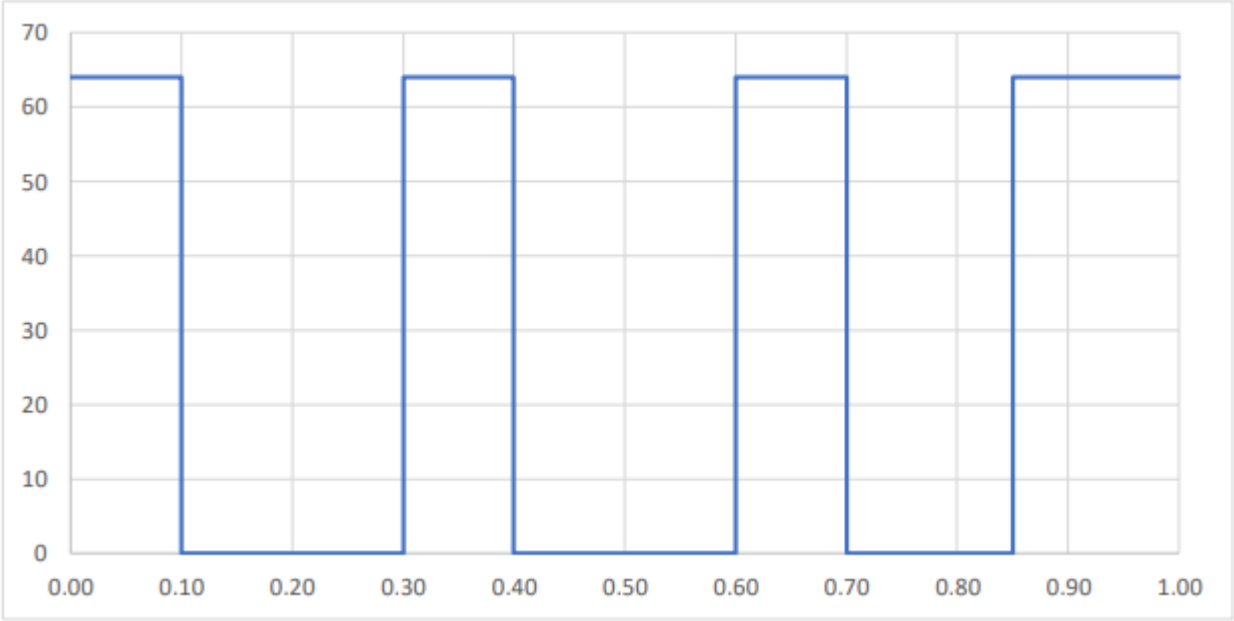


Рисунок 2.7 – Графік імпульсно-періодичної передачі даних з середньою швидкістю 28 кбіт/с

Формування є ключовою технологією в QoS, яка дозволяє обмежувати швидкість передачі певних типів даних у мережі для запобігання перевантаженню каналів. Traffic Shaping згладжує трафік, розподіляючи його протягом часу, як це зображено на рисунку 2.10 [24]. Це дозволяє уникати перевантажень мережевої інфраструктури. Зазвичай застосовується для нестабільного трафіку, наприклад відео або файлових передач, які можуть

перериватиінші, важливі для бізнесу сервіси. Шейпінг реалізується через буферизацію пакетів та обмеження їх виходу на мережевий канал.

Існують дві причини використовувати формування трафіку:

– задля уникнення відкидання трафіка політиками провайдера, можливо сформувати трафік таким чином, щоб не перевищувати ліміт гарантованої смуги пропускання (CIR).

– для запобігання блокування виходів. При переході від більш швидкісного інтерфейсу до менш швидкісного/більш навантаженого інтерфейсу, можуть виникнути втрати у вихідній черзі. В цій ситуації також варто використати формування, щоб гарантувати, що всі дані будуть доставлені

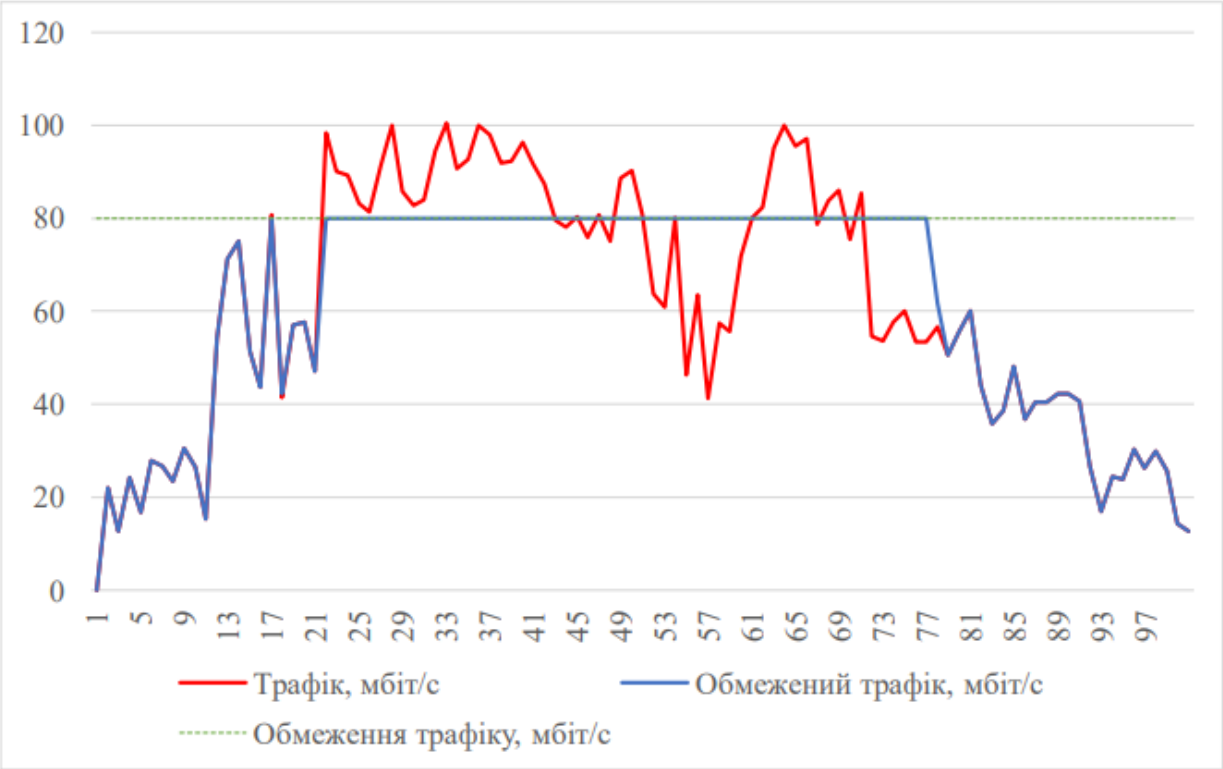


Рисунок 2.8 – Графік впливу формування трафіку на передачу інформації

Управління чергами (Queue Management). Технології управління чергами дозволяють налаштовувати порядок обробки трафіку в разі перевантаження. Один із поширених методів – це зважена випадкова черга раннього виявлення (Weighted Random Early Detection, WRED), яка

автоматично регулює чергу, відкидаючи менше важливі пакети під час завантаження [25]. Це дозволяє уникнути заповнення буферів мережевих пристроїв і сприяє стабільній роботі мережі. Queue Management також включає такі методи, як First-In-First-Out (FIFO) та Priority Queuing, де пакети обробляються в порядку прибуття або відповідно до пріоритетів, що зображено на рисунку 2.8.

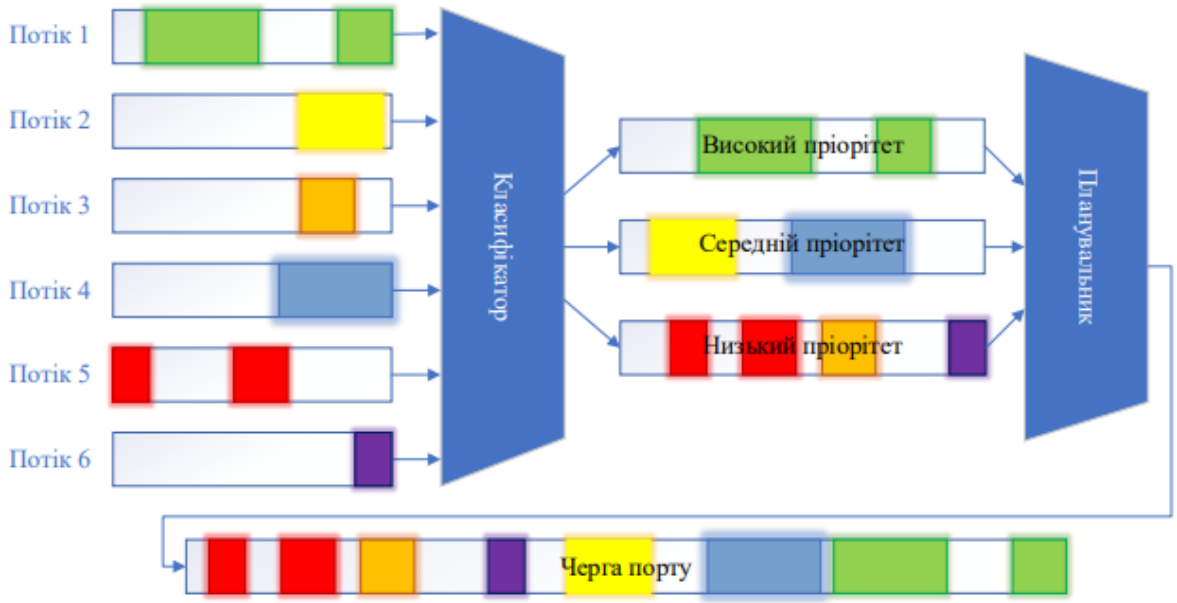


Рисунок 2.9 – Чергування за пріоритетом

Резервування пропускної здатності (Bandwidth Reservation). Цей метод передбачає попереднє виділення певної пропускної здатності для конкретних видів трафіку. У мережах із високою завантаженістю Bandwidth Reservation дозволяє забезпечити мінімальну затримку для критично важливих додатків, таких як IPтелефонія чи відеоконференції. Це особливо корисно у великих мережах, де є потреба в гарантованій пропускній здатності для забезпечення якості обслуговування.

Сучасні мережі поєднують різні методи QoS, залежно від специфіки трафіку та вимог підприємства. У корпоративних мережах, де одночасно обробляється велика кількість даних, ефективне поєднання класифікації, пріоритизації та Класифікатор Планувальник Потік 1 Потік 2 Потік 3 Потік 4 Потік 5 Потік 6 Високий пріорітет Середній пріорітет Низький пріорітет Черга

порту 54 резервування ресурсів дозволяє уникнути затримок і забезпечує високу якість обслуговування. Наприклад, для IP-телефонії може бути виділений окремий сегмент пропускної здатності з високим пріоритетом, щоб уникнути затримок у голосових дзвінках, а для звичайного трафіку можуть бути застосовані методи шейпінгу та технології застосування політик. Це дозволяє адаптувати мережу до специфічних вимог кожного типу трафіку.

Забезпечення QoS у мережах дозволяє підвищити надійність і передбачуваність обслуговування, що особливо важливо для критично важливих додатків і сервісів. Використання QoS допомагає підприємствам досягти високої ефективності використання ресурсів і підтримувати стабільний рівень обслуговування в умовах змінної мережевої активності. Водночас впровадження QoS може вимагати значних витрат на модернізацію обладнання та налаштування, що може ускладнити адаптацію у великих мережах.

QoS є незамінним елементом управління трафіком у сучасних мережах. Його інтеграція та поєднання з іншими технологіями, як-от MPLS та SD-WAN, дозволяють гнучко управляти мережею й оптимізувати її для надання стабільних і надійних послуг користувачам.

2.4 Види програмного забезпечення для e-commerce сервісів

Програмне забезпечення, що використовується у сфері e-commerce, формує основу функціонування онлайн-торгівлі та забезпечує стабільну роботу бізнес-процесів, управління товарами, оплатами, клієнтською взаємодією, аналітикою та захистом інформації. У структурі комп’ютерної системи e-commerce компанії застосовується широкий спектр програмних рішень, які виконують різні функції та інтегруються між собою для досягнення високої продуктивності та безпеки.

Програмне забезпечення e-commerce умовно поділяють на такі основні категорії:

1. Платформи для онлайн-торгівлі (E-commerce Platforms):

Це ядро всієї системи, що забезпечує функціонування інтернет-магазину, обробку замовлень, управління товарами та взаємодію з клієнтами.

До популярних платформ належать: Shopify, WooCommerce, Magento, OpenCart, PrestaShop. Спеціалізовані корпоративні рішення: SAP Commerce Cloud, Microsoft Dynamics 365 Commerce.

Функціональні можливості:

– каталог товарів;
– обробка кошика та оформлення замовлень;
– інтеграція з платіжними сервісами;
– управління користувачами;
– аналітика продажів;
– підтримка декількох складських локацій та валют.

2. Системи управління контентом (CMS)

Забезпечують керування інформаційним наповненням сайту, адаптацію сторінок, роботу блогів, SEO-оптимізацію.

Популярні CMS: WordPress, Joomla, Drupal,

Корпоративні CMS: Bitrix24, Adobe Experience Manager.

CMS часто інтегруються з e-commerce платформами для формування повноцінного інформаційного ресурсу компанії.

3. Платіжні та фінансові сервіси (Payment Gateways)

Забезпечують приймання online-платежів та дотримання стандартів безпеки PCI DSS.

Основні сервіси: LiqPay, WayForPay, Fondy, Stripe, PayPal.

Функції:

– шифрування платіжних даних;
– підтвердження транзакцій через 3D Secure;
– логування та моніторинг фінансових операцій;
– підтримка багатовалютності.

4. Системи управління базами даних (СКБД)

У e-commerce використовуються високопродуктивні СКБД, що забезпечують швидкий доступ до даних та можливість масштабування.

Поширені рішення:

– PostgreSQL, MySQL, MariaDB (реляційні);

– MongoDB, Redis, Cassandra (нереляційні).

Функції СКБД включають:

– зберігання інформації про користувачів, замовлення, транзакції;

– механізми реплікації для забезпечення відмовостійкості;

– індексацію та оптимізацію запитів;

– підтримку аналітичних обчислень.

5. Системи внутрішнього контролю та кібербезпеки

Це важливий компонент e-commerce інфраструктури, який забезпечує захист даних і безпечну роботу мережі.

До програмного забезпечення цієї категорії належать:

1) SIEM-системи (Splunk, Wazuh, IBM QRadar) – аналіз подій безпеки, моніторинг логів, виявлення аномалій.

2) Антивірусні та EDR-рішення (ESET, SentinelOne, CrowdStrike) – захист робочих станцій і серверів.

3) IDS/IPS-системи (Snort, Suricata) – виявлення і блокування підозрілого трафіку.

4) Фаєрволи нового покоління (NGFW) – фільтрація трафіку на рівні додатків, створення політик доступу.

6. Системи логістики та управління складом (WMS)

Для e-commerce логістика є критичною частиною, тому використовуються програми для управління запасами, рухом товарів і доставкою.

Основні функції:

– контроль залишків;

– автоматизація формування заявок;

– інтеграція з поштовими операторами;

– облік повернень і пересортувань.

7. Системи CRM (Customer Relationship Management)

Забезпечують взаємодію з клієнтами та підтримують ключові бізнес-процеси e-commerce.

Поширені системи: Bitrix24, Zoho CRM, Salesforce, HubSpot.

Функції:

– управління лідами та клієнтськими профілями;

– формування статистики по продажах;

– інтеграція з маркетинговими платформами;

– автоматизація e-mail розсилок.

8. Серверні та хмарні сервіси

Для забезпечення масштабованості та високої доступності використовуються:

– AWS, Google Cloud, Microsoft Azure;

– CDN-сервіси (Cloudflare, Akamai);

– Docker-контейнери, Kubernetes;

– системи моніторингу (Grafana, Prometheus).

Хмарні технології дозволяють швидко збільшувати ресурси при рості навантаження.

9. Програмне забезпечення мережевої інфраструктури

Для забезпечення стабільної роботи комп’ютерної мережі використовуються:

– системи керування маршрутизаторами та комутаторами (Cisco IOS, MikroTik RouterOS);

– програмні контролери Wi-Fi (UniFi Network Controller);

– VPN-протоколи (OpenVPN, IPSec);

– інструменти центрального адміністрування та оновлень.

2.5 Топології комп’ютерних мереж і їх застосування в інтернет-торгівлі

Топологія комп’ютерної мережі визначає спосіб фізичного та логічного з’єднання пристроїв між собою, що безпосередньо впливає на продуктивність, масштабованість, відмовостійкість та безпеку e-commerce інфраструктури. Інтернет-торгівля є однією з галузей, де мережеві ресурси зазнають високих навантажень, а простої системи можуть призвести до значних фінансових втрат. Тому правильний вибір топології є критично важливим.

2.5.1 Основні мережеві топології, що використовуються в e-commerce

1) Топологія «Зірка» (Star)

Найпоширеніший варіант для локальних мереж офісів, складів і невеликих дата-центрів.

Переваги:

– простота реалізації та адміністрування;

– ізоляція пошкоджень: вихід з ладу одного вузла не впливає на інші;

– висока керованість повітря між сегментами.

Недоліки:

– точка відмови – центральний комутатор;

– обмежена масштабованість у базовій реалізації.

Застосування в e-commerce: Внутрішні офісні сегменти компанії (бухгалтерія, call-центр, відділ підтримки), робочі місця співробітників, складські термінали, касові POS-системи.

2) Каскадна топологія (Cascaded Star / Hierarchical)

Є розвитком “зірки” з використанням кількох рівнів комутаторів.

Переваги:

– масштабованість – легко додавати нові рівні;

– логічний поділ на зони: DMZ, LAN, VLAN для різних служб.

Недоліки:

– ускладнення схеми керування;

– може виникати перевантаження магістральних ліній.

Застосування: Будівництво корпоративних мереж e-commerce компанії з великою кількістю робочих місць, розмежування трафіку клієнтської частини та внутрішніх сервісів.

3) Кільцева топологія (Ring)

Рідко використовується у чистому вигляді, але принципи зустрічаються у деяких протоколах та промислових рішеннях.

Переваги:

– стабільний і передбачуваний час передачі;

– можливість резервування (Dual Ring).

Недоліки:

– вихід з ладу одного вузла може порушити логічне кільце без резерву.

Застосування: у деяких системах резервування каналів та магістральних лініях між дата-центрами.

4) Шинна топологія (Bus)

Практично не використовується у сучасних e-commerce мережах через обмеження:

Недоліки:

– низька продуктивність;

– високий рівень колізій;

– проблеми з масштабуванням.

Застосування: зустрічається хіба що в дуже старих або бюджетних системах.

5) Топологія «Дерево» (Tree)

Поєднує “зірку” та ієрархічність.

Переваги:

– легке структурне розширення;

– чіткий поділ на магістральний, дистрибутивний та доступовий рівні (стандартна модель корпоративної мережі).

Застосування в e-commerce: організація мережі великого інтернет-магазину з різними поверхами офісів, логістичними зонами, віддаленими складами.

6) Mesh-топологія (Повна або часткова сітка)

Найбільш відмовостійка схема, що забезпечує множинні маршрути.

Переваги:

– висока стійкість до відмов – відмова одного вузла не порушує роботу;

– підвищена пропускна здатність завдяки паралельним каналам.

Недоліки:

– висока вартість реалізації;

– складне адміністрування.

Застосування: мережі між дата-центрами (DC-to-DC). Обробка критично важливих сервісів таких як – оплати, CRM, checkout-сервіси. Хмарні інфраструктури, контейнерні середовища (Kubernetes clusters).

7) Spine-Leaf топологія

Сучасний стандарт для високонавантажених e-commerce платформ.

Особливості:

– кожен Leaf-комутатор підключається до кожного Spine-комутатора;

– забезпечує передбачувану мінімальну затримку та симетричну пропускну здатність.

Переваги:

– ідеальна для масштабування серверних кластерів;

– висока відмовостійкість;

– оптимальна робота з хмарними сервісами, контейнеризацією та мікросервісною архітектурою.

Застосування: У дата-центрах інтернет-магазинів, що обробляють тисячі транзакцій, високі пікові навантаження (Black Friday, сезон розпродажів).

Для e-commerce компанії зазвичай використовується комбінований підхід:

1. Офіс, склад: зірка або дерево.

2. IT-інфраструктура всередині офісів: каскадна зірка з VLAN.

3. Дата-центр та серверні зони: Mesh або Spine-Leaf.

4. Між філіями/складами: VPN-кільце або часткова Mesh через MPLS/SD-WAN.

Такий підхід дозволяє досягти максимального рівня відмовостійкості, швидкодії та гнучкості в масштабуванні.

2.6 Види мережевих пристроїв та їх функціональне призначення

Ефективна мережа e-commerce компанії базується на широкому спектрі мережевих пристроїв, кожен з яких виконує визначені функції: маршрутизацію, комутацію, балансування навантаження, шифрування трафіку, фільтрацію пакетів, контроль доступу, моніторинг і захист від кіберзагроз. У сучасних інтернет-магазинах, які працюють у режимі 24/7, ці пристрої повинні забезпечувати високу продуктивність, відмовостійкість та безпеку даних.

Мережеві пристрої умовно поділяють на кілька груп:

– обладнання доступу (Access Layer),

– обладнання розподілу та маршрутизації (Distribution/Core Layer),

– пристрої безпеки,

– пристрої оптимізації та балансування,

– хмарні та віртуалізовані мережеві компоненти.

2.6.1 Маршрутизатори та балансувальники навантаження

Маршрутизатори виконують ключову роль у побудові мереж e-commerce, оскільки забезпечують маршрутизацію пакетів між внутрішніми сегментами, віддаленими офісами, серверами та Інтернетом. Саме вони визначають оптимальний шлях передачі даних і забезпечують роботу транзакційних сервісів без затримок.

Основні функції маршрутизаторів:

– передавання даних між різними мережами (LAN ↔ WAN);

– підтримка динамічних протоколів маршрутизації (OSPF, BGP, EIGRP, IS-IS);

– створення VPN-тунелів для захисту даних між філіями;

– розмежування трафіку та запобігання перевантаженню каналів;

– забезпечення QoS для пріоритизації важливих сервісів (платіжні дані, API-запити, логістика).

Застосування в e-commerce:

– забезпечення зв’язку між дата-центром та інтернет-провайдером;

– побудова SD-WAN для з’єднання магазинів, складів і центрального офісу;

– маршрутизація запитів до хмарних сервісів (AWS, Azure, GCP);

– доступ до CRM, ERP або внутрішніх мікросервісів.

Для інтернет-торгівлі балансувальники навантаження є критично важливими. Вони розподіляють трафік між серверами, щоб уникнути перевантаження й забезпечити високу доступність сервісів.

Функції Load Balancer:

– розподіл HTTP/HTTPS трафіку між веб-серверами;

– зміна маршруту при відмові сервера (Failover);

– SSL-термінація – обробка зашифрованих з’єднань;

– створення високонавантажених кластерів мікросервісів;

– аналіз стану серверів (Health checking).

Типи балансувальників:

– апартні (F5, Citrix, Cisco) – для великих e-commerce із тисячами запитів у секунду;

– програмні (NGINX, HAProxy, Traefik) – популярні у середніх інтернет-магазинах;

– хмарні (AWS ELB, Cloudflare Load Balancing) – масштабуються автоматично.

Застосування:

1) доставка сторінок каталогу та кошика покупця;

2) обробка API-запитів мобільного додатку;

3) балансування запитів до бази даних та кешів (MySQL cluster, Redis cluster).

2.6.2 Комутатори L2/L3 та їх роль у структурі e-commerce мережі

Комутатори другого рівня (L2 Switches) використовуються для побудови локальних сегментів мережі (Access Layer). Працюють із MAC-адресами й організовують доступ співробітників, камер відеоспостереження, POS-терміналів та складів.

Функції L2 Switch:

– комутація на основі MAC-адрес;

– підтримка VLAN для сегментації трафіку;

– забезпечення безпеки та мінімізація колізій;

– PoE живлення для IoT-обладнання та IP-телефонії.

Використання:

– офісні мережі e-commerce компаній;

– мережа складу (сканери, штрих-термінали, камери);

– мережа торгових точок.

Комутатори третього рівня (L3 Switches) поєднують можливості L2-комутаторів і маршрутизаторів. Це ключовий елемент дата-центрів і серверних кімнат.

Можливості L3 Switch:

– маршрутизація між VLAN;

– підтримка OSPF, BGP – критично важливо для великих магазинів;

– високошвидкісні інтерфейси 10/40/100 GbE;

– функції ACL для фільтрації трафіку.

– Застосування L3 Switch у e-commerce:

– серверна частина інтернет-магазину;

– об’єднання веб- і застосункових серверів;

– побудова Spine-Leaf архітектури;

– оптимізація доступу до бази даних, кешів та сховищ.

Загальна роль комутаторів в e-commerce:

1. Забезпечують швидку доставку даних у внутрішній мережі.

2. Реалізують логічний поділ інфраструктури: DMZ, Backend, Admin, Payment-сегмент.

3. Підтримують SLA та безперервність бізнес-процесів.

4. Визначають масштабованість та продуктивність усіх IT-сервісів.

2.7 Висновок до другого розділу

У теоретичній частині розглянуто наукові та інженерні основи побудови й аналізу корпоративних комп’ютерних мереж, орієнтованих на роботу e-commerce сервісів. У розділі виконано огляд основних метрик якості обслуговування (QoS), таких як пропускна здатність, швидкість передачі,

затримка, джиттер і втрати пакетів, та проаналізовано їхній вплив на роботу сервісів реального часу й транзакційних e-commerce систем. Детально розглянуто сучасні технології QoS, зокрема класифікацію, пріоритизацію, шейпінг, policing, управління чергами та резервування пропускної здатності, які дозволяють забезпечити стабільність і передбачуваність мережевої інфраструктури.

3 СИНТЕЗ СИСТЕМИ

3.1 Цілі впровадження комп’ютерної системи

Метою впровадження комп’ютерної системи є створення на підприємстві єдиної інфраструктури для роботи з даними, керування внутрішніми процесами та забезпечення безпечного доступу до корпоративних ресурсів. Система має гарантувати стабільний обмін інформацією між підрозділами, підтримку службових сервісів, централізоване зберігання та обробку даних, а також створити основу для майбутньої автоматизації та цифрової трансформації підприємства.

Запровадження такої системи спрямоване на підвищення ефективності роботи персоналу, покращення якості взаємодії між структурними підрозділами, спрощення адміністрування IT-інфраструктури й посилення загального рівня кіберзахисту.

3.2 Вибір і обґрунтування принципів побудови системи

Система будується за принципами модульності, доступності, безпеки та масштабованості. Модульність дозволяє легко оновлювати й розширювати систему без втручання в загальну архітектуру – наприклад, додавати нові сервери, робочі станції чи мережеві сегменти. Доступність досягається за рахунок резервування ключових компонентів, що мінімізує простої та гарантує відмовостійкість у разі збоїв.

Безпека закладається у вигляді механізмів контролю доступу, шифрування, аутентифікації користувачів та сегментації мережі, що дозволяє захистити інформаційні потоки і мінімізувати ризики стороннього втручання. Масштабованість забезпечує можливість швидкого збільшення кількості користувачів, робочих станцій або обсягу даних без необхідності повної перебудови системи.

Застосування цих принципів дає змогу створити інфраструктуру, яка відповідає сучасним вимогам підприємства та забезпечує адаптивність до майбутніх змін.

3.3 Формулювання технічних вимог до комп’ютерної системи

3.3.1 Вимоги до структурних характеристик і режимів функціонування

Система повинна забезпечувати авторизований доступ співробітників до внутрішніх ресурсів підприємства, централізовану обробку даних і стабільний обмін інформацією між відділами. Передача даних між територіально роз'єднаними підрозділами має здійснюватися через захищені канали зв’язку (VPN).

Корпоративна мережа повинна охоплювати всі ключові підрозділи підприємства та забезпечувати роботу серверних сервісів, баз даних, внутрішніх платформ та адміністративних систем.

3.3.2 Вимоги до надійності

Інфраструктура повинна працювати з доступністю не менше 99,9% на рік. Ключові компоненти підлягають резервуванню, що дозволяє уникнути простоїв. Дані повинні бути захищені за допомогою RAID-масивів і механізмів регулярного резервного копіювання з можливістю відновлення за останні 24 години.

3.3.3 Вимоги до розвитку системи

Система має підтримувати приріст навантаження та кількості робочих станцій приблизно на 30% без суттєвих змін архітектури. Це включає збільшення обсягу даних, кількості користувачів і додаткових програмних сервісів.

3.3.4 Вимоги до інформаційної безпеки

Для захисту від несанкціонованого доступу впроваджується двофакторна аутентифікація, централізоване управління ролями, політиками безпеки й ACL. Усі критичні елементи системи мають бути ізольовані у відповідних сегментах мережі.

3.3.5 Вимоги до фізичної безпеки

Доступ у приміщення обмежується системою контролю доступу з картками та реєстрацією входів і виходів. Серверні приміщення обладнуються біометричними засобами та сенсорами відкриття дверей. Будівля охороняється за допомогою турнікетів і систем моніторингу переміщення персоналу.

3.3.6 Вимоги до ергономіки

Робочі місця повинні забезпечувати комфортну та безпечну позу оператора. Необхідно дотримуватися санітарних норм щодо площі, освітлення, розміщення обладнання та можливості індивідуального регулювання меблів і пристроїв.

3.3.7 Вимоги до маршрутизаторів (Core/Edge Router)

Маршрутизатори відіграють ключову роль у побудові мережевої інфраструктури головного офісу та віддалених сегментів, забезпечуючи стабільність, високу продуктивність та безпечну передачу даних. Для головного офісу рекомендовано використовувати пристрої з продуктивністю NAT та маршрутизації не нижче 2 Gbps, тоді як у філіалах цей показник може бути зменшений до 300 Mbps. Важливо, щоб маршрутизатори підтримували основні маршрутизуючі протоколи, такі як OSPF, EIGRP або BGP, що дозволяє гнучко інтегруватися з інфраструктурою провайдера та забезпечувати масштабованість мережі.

Резервування шлюзів повинно бути забезпечено технологіями VRRP, HSRP або GLBP. Підтримка IPv6, QoS, ACL, DHCP relay та Policy Based

Routing є обов’язковою умовою, що дозволяє реалізувати сегментацію та пріоритезацію трафіку. На рівні апаратної конфігурації маршрутизатор має мати щонайменше два WAN-порти Gigabit Ethernet і не менше чотирьох LAN-портів, що створює достатню гнучкість при підключенні до різних каналів зв’язку. Для забезпечення захищеної роботи між офісами необхідна підтримка VPN-технологій – IPSec, SSL VPN або DMVPN.

Маршрутизатор повинен підтримувати DPI або мати можливість інтеграції зі SIEM для детального аналізу трафіку. Його продуктивність має становити не менше одного мільйона пакетів на секунду, а таблиця маршрутів повинна утримувати від 12 тисяч записів. Апаратні ресурси, такі як оперативна пам’ять обсягом 512–1024 MB та флеш-пам’ять від 256 MB, дозволяють забезпечувати стабільну роботу. Типовими моделями, що відповідають таким вимогам, є Cisco ISR серій 1100 або 4300, MikroTik CCR2004/CCR2116, а також Juniper SRX320 чи SRX1500.

3.3.8 Вимоги до комутаторів рівнів Access та Distribution

Комутатори доступу та дистрибуції забезпечують надійний зв’язок між офісними робочими станціями, серверним обладнанням, складу, терміналами обробки замовлень і сегментами дата-центру. На рівні доступу комутатор повинен мати 24 або 48 портів зі швидкістю 1 Gbps та щонайменше два uplink-порти формату 10 Gbps SFP+, що дозволяє гарантувати високу пропускну здатність до рівня дистрибуції. Обов’язковою є підтримка технологій VLAN, 802.1Q, різних варіантів STP (RSTP/MSTP), а також засобів безпеки, включно з Port-Security, DHCP Snooping та Dynamic ARP Inspection. Для живлення IoT-пристроїв, камер спостереження та точок доступу бажано використовувати комутатори з підтримкою PoE або PoE+.

На рівні Distribution/Core комутатор повинен забезпечувати значно вищу продуктивність. Пропускна здатність його магістральної шини має бути не меншою за 240 Gbps, а uplink-порти мають підтримувати швидкість від 10 до 40 Gbps. Пристрій повинен підтримувати повноцінні L3-функції: статичну

маршрутизацію, OSPF, VRRP, ECMP, а також механізми агрегації каналів LACP для резервування магістральних ліній. Обсяг буфера комутатора не повинен бути меншим за 16–32 MB для уникнення втрат пакетів під час пікових навантажень. Вимогам відповідають лінійки Cisco Catalyst (2960X, 3560CX, 3850), Aruba 2530/2930F та MikroTik CRS317/CRS326.

3.3.9 Вимоги до міжмережевих екранів (Firewall/UTM)

Міжмережеві екрани є критично важливим елементом інфраструктури електронної комерції, оскільки через мережу проходять персональні дані клієнтів, транзакції, API-виклики та службовий трафік. Продуктивність firewall із увімкненими модулями IPS повинна становити не менше 1 Gbps, а пропускна здатність VPN на базі IPSec – не менше 500 Mbps. Пристрій має підтримувати глибоку перевірку пакетів (DPI) на рівнях L4–L7, функції IDS/IPS, механізми sandboxing або хмарний аналіз файлів, фільтрацію веб-трафіку та застосунків, SSL-inspection, а також модулі протидії ботнетам та спаму.

Важливо, щоб firewall підтримував режими високої доступності (Active/Standby), а доступ адміністраторів був захищений за допомогою двофакторної автентифікації. Інтеграція із SIEM через syslog, API або NetFlow забезпечує централізований контроль і моніторинг безпеки. На апаратному рівні необхідні щонайменше чотириядерний процесор, оптимізований для DPI-навантажень, не менше 8 GB оперативної пам’яті та від 32 до 120 GB флеш- або SSD-накопичувача. Типові рішення: Fortigate 100F, Cisco FirePower 1010/1120, Palo Alto PA-820, Sophos XG210.

3.3.10 Вимоги до точок доступу Wi-Fi

У компанії бездротова мережа використовується в офісних приміщеннях, логістичних зонах, сервісних зонах і на складі, де працюють мобільні термінали. Точки доступу мають підтримувати сучасні стандарти Wi-Fi 5 або Wi-Fi 6 зі швидкістю не менше 1.2 Gbps на кожну точку (для Wi-Fi 6

– до 1.8–2.4 Gbps). Безпека має бути забезпечена за рахунок підтримки WPA3, а мережеве адміністрування – можливістю розділення гостьових та корпоративних VLAN.

Для централізованого керування необхідна підтримка апаратного або хмарного контролера (Cisco, Aruba, TP-Link Omada), а для швидкого роумінгу клієнтів у складських приміщеннях – технологій 802.11r/k/v. Апаратні параметри повинні включати підтримку 2×2 або 4×4 MU-MIMO, живлення PoE 802.3af/at і забезпечення радіусом покриття 30–50 метрів. Прикладами моделей можуть бути Cisco Aironet 1830/2800, Ubiquiti UniFi U6 Lite або U6 LR, а також Aruba AP-505/515.

3.3.11 Вимоги до серверного мережевого обладнання (ToR-комутатори)

У серверних сегментах, де розміщуються служби HTTP, DNS, TFTP, FTP та внутрішні API, використовуються комутатори з підвищеною продуктивністю та надійністю. Вони повинні мати щонайменше чотири uplink-порти зі швидкістю 10 Gbps для підключення до ядра мережі. Обов’язковою є підтримка Jumbo Frames розміром до 9000 байт, збільшені буфери обсягом не менше 32 MB, а також можливість побудови об’єднаних кластерів MLAG або stacking. Надійність роботи забезпечується подвійними блоками живлення, що дозволяє уникнути простоїв у разі відмови одного з них.

3.4 Розробка схеми функціональної структури

Функціональна структура визначає взаємодію підрозділів підприємства та роль комп’ютерної системи в забезпеченні їх роботи. Мета розробки – показати, як інформаційні потоки проходять між відділами, які ресурси вони використовують і які завдання виконують за допомогою корпоративної інфраструктури.

Адміністративний відділ потребує стабільної корпоративної мережі для роботи з документами, внутрішньої координації та управління основними робочими процесами. Юридичний відділ використовує інформаційні системи для доступу до нормативної документації та ведення ділового обліку з підвищеним рівнем захисту даних.

Маркетинговий відділ працює з хмарними платформами, аналітичними інструментами та корпоративними сховищами, що дозволяє проводити дослідження ринку та аналізувати ефективність кампаній. Відділ технічної підтримки забезпечує функціонування комп'ютерної мережі, виконує моніторинг систем, адмініструє сервери та підтримує загальну IT-інфраструктуру.

Логістичні та технічні підрозділи авіаліній працюють із спеціалізованими програмними комплексами, що забезпечують планування, облік та контроль технічного стану обладнання. Відокремлені підрозділи використовують захищені канали для обміну інформацією з головним офісом, що дозволяє підтримувати синхронність операцій незалежно від фізичної віддаленості.

Функціональна структура мережі відображає розподіл ресурсів, маршрути інформаційних потоків і точки взаємодії між підрозділами, формуючи основу для подальшого проєктування системи.

3.5 Обґрунтування вибору елементної бази мережевої інфраструктури

Проєктована мережае-commerce компанії повинна забезпечувати високу доступність, масштабованість та стійкість до навантажень, пов'язаних із обробкою веб-трафіку, онлайн-замовлень, роботою складу та взаємодією із зовнішніми сервісами. Тому вибір обладнання виконувався з урахуванням таких параметрів: продуктивність, надійність, підтримка сучасних протоколів, можливість резервування та централізованого управління.

1. Вибір маршрутизатора (Core/Edge Router)

Для реалізації зв’язку між головним офісом, дата-центром та інтернет-провайдером потрібен маршрутизатор з підтримкою:

– пропускної здатності не менше 5–10 Гбіт/с для NAT і міжмережевої маршрутизації;

– BGP для коректного обміну маршрутами з провайдером;

– OSPF/VRF для побудови внутрішньої багатосегментної мережі;

– апаратного прискорення (ASIC) для високої швидкості обробки пакетів;

– резервування блоків живлення та модульної архітектури.

Такі характеристики найкраще відповідають маршрутизаторам Cisco ASR, Juniper MX, або більш бюджетним варіантам на рівні MikroTik CCR 2216 / CCR2004, що забезпечують до 100 Гбіт/с комутації.

Обґрунтування: Ці маршрутизатори підтримують високошвидкісні інтерфейси (10–25–40 Гбіт/с), апаратне прискорення NAT, сучасні протоколи маршрутизації та дозволяють масштабувати мережу без заміни основного обладнання.

2. Вибір комутаторів доступу (Access Switches)

Робочі місця співробітників, касові термінали, сканери штрих-кодів на складі та Wi-Fi точки потребують надійних L2-комутаторів із такими характеристиками:

– 24/48 портів 1G для підключення офісних пристроїв;

– підтримка PoE/PoE+ для живлення точок доступу та IP-камер;

– uplink 10G для запобігання перевантаженню магістралі;

– підтримка VLAN, STP та QoS.

Підходящі моделі: Cisco Catalyst 2960/9200, HPE Aruba 2530/2540, Ubiquiti UniFi Switch PoE Gen2.

Обґрунтування: Вони забезпечують достатню пропускну здатність для офісних і складських зон, підтримують сегментацію мережі та мають високу надійність.

3. Вибір комутаторів ядра/розподілу (Core/Distribution Switches)

Оскільки топологія включає центральний дата-центр і офісний кластер, між якими проходить критичний трафік, вони потребують потужних L3-комутаторів із такими можливостями:

– 10–40 Гбіт/с uplink інтерфейси;
– апаратна маршрутизація OSPF/BGP;
– VRF для ізоляції мереж;
– стекування або створення відмовостійкого кластеру (MLAG/LACP);
– пропускна здатність від 1,2 до 3 Тбіт/с.

Відповідні моделі: Cisco Catalyst 9500, Aruba 6400, Juniper EX4300/4600.

Обґрунтування: Такі комутатори гарантують низьку затримку всередині мережі та дозволяють створити масштабовану багаторівневу архітектуру.

4. Вибір Wi-Fi інфраструктури

Для офісу та складу обрані точки доступу класу Wi-Fi 6, оскільки ці зони мають високу щільність підключень і потребують стабільного та швидкого бездротового доступу.

Вимоги:

– підтримка MU-MIMO для обслуговування великої кількості одночасних клієнтів;
– централізований контролер для керування політиками доступу;
– роумінг між точками доступу без розриву сесії;
– підтримка WPA3 та сегментації SSID.

Можливі моделі: Ubiquiti UniFi 6 LR, Cisco 9115/9120, Aruba AP-515.

Обґрунтування: Wi-Fi 6 дає суттєве збільшення пропускної здатності, меншу затримку, стабільнішу роботу у високонавантажених зонах (склад, офіс open-space).

5. Вибір системи фільтрації та захисту (Firewall / NGFW)

З огляду на специфіку e-commerce (наявність платіжної інформації, персональних даних, API шлюзів), необхідний NGFW із:

– DPI (Deep Packet Inspection);
– WAF-модулем для захисту веб-сервісів;
– SSL Inspection;
– IPS/IDS;
– підтримкою VPN (IPsec/SSL);
– продуктивністю не менше 5–12 Гбіт/с.

Підходящі моделі: Fortinet FortiGate 100/200 серії, Palo Alto PA-820/PA-1400, Cisco Firepower 2100.

Обґрунтування: NGFW дозволяє захищати мережу від сучасних атак, включно з ботнетами, SQL-ін’єкціями та DDoS низького рівня.

6. Вибір серверного та резервного обладнання

Дата-центр компанії потребує серверів і мережевих адаптерів, що підтримують:

– інтерфейси 10/25 Гбіт/с;
– резервування живлення та мережевих карт;
– інтеграцію з віртуалізацією VMware/Proxmox;
– підтримку iSCSI/NFS для доступу до сховища.

Також передбачені:

– UPS на 1–3 години автономності;
– резервне інтернет-з’єднання;
– система моніторингу (Zabbix, PRTG).

7. Сумісність, масштабованість та стандартизація

Під час вибору елементної бази враховувались:

– підтримка стандартів IEEE 802.1Q, 802.1X, 802.3ad, 802.11ax;

– можливість централізованого керування;

– легка інтеграція з існуючими сервісами компанії (CRM, WMS, ERP);

– можливість збільшення кількості користувачів без заміни ядра мережі;

– наявність офіційної техпідтримки та оновлень ПЗ.

Обрана елементна база повністю відповідає вимогам e-commerce компанії: вона забезпечує високу швидкість, безпеку, резервування, масштабування й централізоване керування. Таке рішення гарантує безперервність роботи ключових сервісів, стабільну роботу складу, швидкий обмін даними між підрозділами та захист конфіденційної інформації.

3.6 Кабельні системи та типи з’єднань для офісу, дата-центру та складу

Коректний вибір кабельної інфраструктури для e-commerce компанії має критичне значення, оскільки від нього залежить пропускна здатність, надійність та масштабованість усієї мережевої системи. У зв’язку з цим кабельні системи проєктуються з урахуванням вимог стандартів TIA/EIA-568, ISO/IEC 11801, а також особливостей експлуатації в офісі, дата-центрі та на складі.

1. Кабельна інфраструктура головного офісу

В офісі зосереджені робочі місця співробітників, точки доступу Wi-Fi, IP-телефонія та адміністративні сервери. Для таких умов використовується структурована кабельна система на основі мідних кабелів категорій Cat 6A і Cat 6.

Обґрунтування вибору:

Cat 6A забезпечує передачу даних до 10 Гбіт/с на відстань до 100 м, що відповідає вимогам сучасних офісних мереж.

Підтримка PoE/PoE+ для точок доступу, IP-камер, VoIP телефонії.

Менша чутливість до перешкод порівняно з Cat 5e, що важливо при щільному розміщенні кабельних трас.

Ключові елементи офісної СКС:

– горизонтальні лінії Cat 6A до робочих місць;

– вертикальні магістралі 10G між поверхами;

– патч-панелі 24/48 портів, маркування відповідно до TIA-606;

– використання кабель-каналів і органайзерів для підтримки порядку та охолодження.

2. Кабельні системи складу та логістичного центру

Складський комплекс має специфічні умови експлуатації: великі відстані, підвищена запиленість, рух техніки, високі стелажі. Це формує окремі вимоги до вибору кабелів та їх прокладання.

Умови та вимоги:

– підключення терміналів збору даних, сканерів штрих-коду, камер відеоспостереження;

– велика площа покриття Wi-Fi;

– підвищені ризики механічних пошкоджень.

– Типи кабелів для складу:

– Захищений мідний кабель Cat 6A S/FTP

– стійкий до механічних пошкоджень та перешкод;

– забезпечує PoE для камер і точок доступу;

– підтримує 10 Гбіт/с.

Одномодове оптоволокно OS2

– для зв’язку між віддаленими зонами складу та головним комутаційним вузлом;

– дозволяє прокладати лінії довжиною 200–800 м без втрати якості.

– Армовані оптоволоконні кабелі

– застосовуються у місцях ризику фізичного пошкодження;

– рекомендовані для зовнішніх каналів між будівлями.

4. Типи з’єднань між офісом, ДЦ та складом

Для взаємозв'язку структурних підрозділів компанії застосовуються:

1. Оптичні канали Backbone

– головний офіс – дата-центр – до 10–40 Гбіт/с;

– дата-центр – склад – 1–10 Гбіт/с;

– підтримка протоколів LACP, MLAG для резервування лінків.

2. WAN-канали від провайдера

– два незалежні провайдери для резервування;

– підтримка BGP для забезпечення безперервності доступу до сайту.

3. VPN-тунелі

– IPsec або SSL-VPN між офісом та складом;

– DDoS-фільтрація на стороні провайдера.

5. Принципи прокладання кабелів

– оптичне волокно розміщується в окремих кабель-лотках, із дотриманням допустимого радіуса згину;

– мідні кабелі – у коробах або кабельних каналах;

– лінії PoE повинні бути розділені від силових кабелів;

– у дата-центрі кабелі прокладаються за схемою Top-of-Rack або End-of-Row;

– маркування обов’язкове згідно зі стандартом TIA-606.

3.7 Висновок до розділу

У розділі 3 виконано синтез комп’ютерної системи e-commerce підприємства та сформовано цілісне бачення її побудови як інтегрованої, масштабованої та безпечної мережевої інфраструктури. Визначено основні

цілі впровадження системи, які полягають у забезпеченні централізованої обробки даних, надійного обміну інформацією між підрозділами, підвищенні ефективності роботи персоналу та створенні основи для подальшої цифрової трансформації бізнесу.

Обґрунтовано принципи побудови системи — модульність, доступність, безпеку та масштабованість — що дозволяють адаптувати інфраструктуру до зростаючих навантажень і змін у діяльності підприємства. Сформульовано комплекс технічних вимог до системи, які охоплюють структурні характеристики, надійність, розвиток, інформаційну й фізичну безпеку, ергономіку робочих місць, а також вимоги до ключових мережевих компонентів: маршрутизаторів, комутаторів, міжмережевих екранів, Wi-Fi інфраструктури та серверного обладнання.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1 Розширена перевірка базового налаштування маршрутизатора

У процесі налаштування доступу, безпеки та підтримки мережевої інфраструктури підприємства електронної комерції одним із першочергових завдань є забезпечення коректної та безпечної конфігурації маршрутизаторів, які слугують центральною ланкою у маршрутизації трафіку між внутрішніми сегментами та зовнішніми каналами зв'язку. Маршрутизатор ecomers_R3 виконує роль ключового елемента у топології, тому перевірка його базових параметрів є обов'язковою частиною первинного аудиту мережі. Така перевірка дозволяє впевнитися, що пристрій працює відповідно до вимог корпоративної політики безпеки, підтримує правильні механізми аутентифікації та шифрування, а також забезпечує стійкість і надійність передавання даних.

Першим кроком під час аудиту є підтвердження наявності правильного системного імені. Наявність заданого hostname є важливою умовою централізованого адміністрування, зручності моніторингу та коректного функціонування SSH, де ім'я пристрою використовується при генерації криптографічних ключів. У конфігурації ecomers_R3 перевіряється наявність команди:

```
hostname ecomers_R3
```

Наступним етапом є перевірка параметрів локального доступу через консольний порт. Консоль є фізичним каналом керування пристроєм, тому наявність пароля і вимкнення анонімного доступу є базовою вимогою безпеки. У конфігурації підтверджується правильність записів:

```
line console 0
 password cisco
 login
```

Далі аналізуються параметри віртуальних термінальних ліній VTY, через які здійснюється віддалений доступ до пристрою. Перевіряється, що базова автентифікація активована, а неконтрольований доступ відключений:

```
line vty 0 15
 password cisco
 login
```

Важливою складовою безпеки маршрутизатора є використання зашифрованого привілейованого паролю. Після аналізу конфігурації підтверджується, що використовується стандартна команда:

enable secret class

Під час перевірки також звертається увага на те, чи включено глобальне шифрування паролів. Це не є сильним криптографічним захистом, проте унеможливлює зчитування відкритих паролів з конфігурації у разі компрометації доступу:

service password-encryption

Наступним кроком є перевірка інформаційного банера Message of the Day (MOTD). Наявність банера є вимогою корпоративної політики, оскільки він попереджає потенційного неавторизованого користувача, що доступ до пристрою дозволений лише уповноваженим особам. Для маршрутизатора ecomers_R3 він встановлений у вигляді:

banner motd # ecomers_R3#

Особлива увага під час аудиту приділяється механізмам безпечного віддаленого керування. В сучасних корпоративних мережах абсолютно недопустимим є використання Telnet, тому перевіряється, що маршрутизатор дозволяє доступ лише через SSH. У конфігурації маршрутизатора повинні бути присутні такі параметри:

```
line vty 0 15
 transport input ssh
 login local
```

Після цього здійснюється аналіз локальної бази користувачів, оскільки саме вона забезпечує контрольований доступ до системи:

username 12321_ecomers_R3 password admincisco

Для коректної роботи SSH маршрутизатор повинен мати вказане доменне ім’я та згенерований криптографічний ключ RSA:

```
ip domain-name ecomers_R3
crypto key generate rsa
1024
```

Ці параметри гарантують, що SSH працює із застосуванням відповідного шифрування, а канал керування захищений від перехоплення.

Завершальний етап перевірки стосується серійних інтерфейсів, які у моделях лабораторної або тестової інфраструктури можуть використовуватися як канали рівня WAN. При наявності DCE-інтерфейсів необхідно перевірити правильність значення тактової частоти, яке задає пристрій, що виступає джерелом синхронізації каналу:

```
int se0/0/0
 clock rate 128000
int se0/0/1
 clock rate 128000
```

Наявність правильного clock rate забезпечує стабільну роботу каналу передачі даних та виключає помилки синхронізації.

Таким чином, комплексна перевірка маршрутизатора ecomers_R3 дозволяє зробити висновок, що його базова конфігурація відповідає вимогам безпеки, стійкості та корпоративним стандартам мережевої інфраструктури e-commerce. Усі ключові елементи – від аутентифікації та шифрування до коректної роботи інтерфейсів – налаштовані відповідно до норм побудови сучасних корпоративних мереж.

4.2 Перевірка налаштування EtherChannel на комутаторах

Першим етапом було виконано діагностичні команди show etherchannel summary та show interfaces port-channel, результати яких засвідчили, що всі інтерфейси, включені до груп channel-group 1 та channel-group 2, перебувають у статусі P (properly bundled) та працюють у складі відповідних логічних каналів. Виявлено, що кожен фізичний порт узгоджено працює в режимі LACP active, що підтверджує правильне формування агрегованих зв’язків.

Подальший аналіз виводу команд show lacp neighbor і show etherchannel port-channel підтвердив, що узгодження між комутаторами відбувається стабільно: ключі агрегації збігаються, ролі Actor/Partner визначені коректно, помилок типу inconsistency не виявлено. Також підтверджено, що логічні канали функціонують у режимі trunk, а список дозволених VLAN відповідає очікуваному (допущено передавання всіх VLAN у межах магістрального з'єднання).

Паралельно була проведена оцінка журналу подій пристроїв. Лог-файли не містили повідомлень про переходи інтерфейсів у стан suspended, втрату синхронізації або err-disabled. Показники якості трафіку (CRC errors, drops, input/output errors) залишаються в межах норми, що свідчить про стабільну роботу агрегованих каналів без втрат продуктивності.

За результатами комплексної перевірки встановлено, що EtherChannel у сегменті функціонує коректно, забезпечує необхідну сумарну пропускну здатність та підтримує підвищену відмовостійкість міжкомутаторних з'єднань. Таким чином, налаштування EtherChannel можна вважати успішно виконаними, а його роботу – повністю відповідною вимогам мережевої інфраструктури компанії електронної комерції.

4.3 Налаштування VLAN

У рамках модернізації мережевої інфраструктури компанії електронної комерції було проведено комплексне налаштування віртуальних локальних мереж (VLAN) на комутаторах . Основною метою цього етапу було забезпечення логічної сегментації мережі, підвищення рівня безпеки, ефективного розподілу мережевого трафіку та створення передумов для централізованого управління. Виконані роботи включали створення VLAN, прив'язку фізичних портів до відповідних VLAN, налаштування транкових портів для міжкомутаторного обміну та підготовку мережі для автоматичного призначення IP-адрес через DHCP.

На першому етапі було створено всі необхідні VLAN у глобальному режимі конфігурації комутатора. Для кожного VLAN визначено унікальний ідентифікатор та логічну назву, що дозволяє швидко ідентифікувати функціональне призначення сегменту та полегшує подальше адміністрування мережі. Команди мали вигляд:

```
configure terminal
vlan 10
 name Users
vlan 20
 name Admin
vlan 30
 name Services
vlan 99
 name Management
vlan 100
 name Core-Native
exit
```

Усі VLAN були активовані та перевірені на наявність конфліктів, відсутність дублювання ідентифікаторів та відповідність плану IP-адресації. Під час перевірки show vlan brief підтверджено, що VLAN 10, 20 та 30 відповідають призначеним групам користувачів і активні на відповідних портах.

Наступним етапом було налаштування фізичних інтерфейсів комутаторів у режимі access. Це дозволило підключати кінцеві пристрої до відповідних VLAN. Наприклад, для робочих станцій користувачів першої групи (VLAN 10) налаштування виглядало так:

```
interface range FastEthernet0/2 - 0/10
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
exit
```

Команди забезпечили не лише прив’язку портів до VLAN, а й швидке підключення кінцевих пристроїв завдяки PortFast, а також захист від потенційних мережевих петель через BPDU Guard. Аналогічні дії були виконані для адміністративного сегменту (VLAN 20) та сервісного сегменту (VLAN 30):

```
interface range FastEthernet0/11 - 15
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
exit

interface range FastEthernet0/16 - 24
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
exit
```

Особливу увагу приділено налаштуванню транкових портів, через які здійснюється передача трафіку між комутаторами і ядром мережі. Конфігурація транкового порту передбачала інкапсуляцію 802.1Q, визначення native VLAN та перелік дозволених VLAN:

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,99,100
 switchport nonegotiate
exit
```

Параметр switchport nonegotiate забезпечив відмову від динамічного обміну DTP-пакетами, що підвищило стабільність роботи транкового каналу та запобігло можливим конфліктам між комутаторами різних виробників. Для резервування каналу був налаштований додатковий транковий інтерфейс GigabitEthernet0/2 із аналогічними параметрами, що забезпечило відмовостійкість та балансування навантаження.

Додатково було проведено налаштування SVI (Switch Virtual Interface) для Management VLAN (VLAN 99), що дозволяє централізовано керувати комутатором через мережу управління:

```
interface vlan 99
 ip address 172.24.129.98 255.255.255.240
 no shutdown
exit
ip default-gateway 172.24.129.97
```

Дане налаштування дозволило комутаторам бути доступними для моніторингу та адміністрування, ізольовано від користувацького трафіку, що підвищує рівень безпеки корпоративної мережі.

Для автоматичного призначення IP-адрес кінцевим пристроям VLAN було інтегровано з DHCP, що дозволяє значно спростити керування мережею і забезпечити централізоване управління адресним простором. На маршрутизаторі було створено DHCP-пули для кожного VLAN:

```
ip dhcp excluded-address 172.24.129.1 172.24.129.5
ip dhcp excluded-address 172.24.129.126 172.24.129.127
ip dhcp pool VLAN10
 network 172.24.129.0 255.255.255.224
 default-router 172.24.129.1
 dns-server 172.24.128.250
ip dhcp pool VLAN20
 network 172.24.129.32 255.255.255.224
 default-router 172.24.129.33
 dns-sever 172.24.128.250
ip dhcp pool VLAN30
 network 172.24.129.64 255.255.255.224
 default-router 172.24.129.65
 dns-server 172.24.128.250
```

Після налаштування було проведено тестування видачі адрес на кінцевих пристроях. Встановлено, що всі хости успішно отримують IP-адресу, маску, шлюз і DNS з відповідного пулу VLAN, що підтверджує коректну інтеграцію DHCP з логічними підмережами.

У підсумку, виконане налаштування VLAN на комутаторах дозволило створити чітко сегментовану мережу з розмежуванням користувацьких, адміністративних та сервісних підмереж, забезпечило стабільну роботу транкових каналів між комутаторами, централізоване управління через Management VLAN, а також автоматичне призначення IP-адрес за допомогою DHCP. Ця конфігурація повністю відповідає вимогам компанії електронної комерції щодо безпеки, масштабованості та надійності мережевої інфраструктури.

4.4 Конфігурація віртуальної приватної мережі (VPN) для віддаленого доступу

У рамках модернізації мережевої інфраструктури компанії електронної комерції було виконано конфігурацію віртуальної приватної мережі (VPN) для забезпечення безпечного доступу віддалених користувачів до корпоративної мережі. Використання VPN дозволяє гарантувати конфіденційність, цілісність і аутентифікацію переданих даних через публічну мережу Інтернет, що є критично важливим для бізнесу, який обробляє персональні дані клієнтів та фінансові транзакції.

Процес налаштування VPN розпочався з активації модуля безпеки на маршрутизаторі, що дозволяє застосовувати криптографічні алгоритми для шифрування трафіку. Було використано команду:

license boot module c2900 technology-package securityk9

Це дозволило включити повний набір функцій безпечного з’єднання, доступних у серії Cisco 2900, включаючи шифрування IPsec, аутентифікацію пірів та управління ключами.

Наступним етапом стало створення списку контролю доступу (ACL) для VPN, який визначає, який трафік основної мережі може проходити через захищений тунель до віддаленої підмережі. Для цього був налаштований розширений ACL:

```
ip access-list extended VPN11
```

```
permit ip 172.24.129.0 0.0.0.127 172.24.128.0 0.0.0.31
permit ip 172.24.129.0 0.0.0.127 172.24.128.32 0.0.0.63
permit ip 172.24.129.0 0.0.0.127 172.24.128.128 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.24.129.128 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.1.128.0 0.0.0.255
```

Ці правила забезпечують, що лише визначений трафік корпоративної мережі може проходити через VPN-тунель, що підвищує рівень безпеки та ізоляції даних.

Далі було налаштовано криптографічну політику ISAKMP, яка визначає параметри шифрування та аутентифікації для встановлення тунелю:

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
```

Використання алгоритму 3DES та хеш-функції MD5 дозволяє забезпечити надійне шифрування даних, а метод pre-shared key гарантує взаємну аутентифікацію пірів.

Для взаємодії з віддаленим VPN-партнером було створено ключ шифрування та прив’язано його до IP-адреси віддаленого маршрутизатора:

crypto isakmp key cisco address 209.165.202.2

Далі був налаштований набір перетворень IPsec, який визначає способи шифрування та аутентифікації трафіку:

crypto ipsec transform-set TS esp-3des esp-md5-hmac

Цей набір забезпечує шифрування даних у тунелі та захист від підробки пакетів.

Створене криптографічне зіставлення (crypto map) пов’язує правила, ACL та трансформації з конкретним інтерфейсом маршрутизатора:

```
crypto map MAP 10 ipsec-isakmp
 set peer 209.165.202.2
 set transform-set TS
 match address VPN11
```

Останнім кроком стало прив’язування криптографічної карти до вихідного інтерфейсу маршрутизатора, який підключений до Інтернету:

```
interface GigabitEthernet0/1
 crypto map MAP
```

Після налаштування VPN було проведено тестування тунелю за допомогою команд show crypto isakmp sa та show crypto ipsec sa, що підтвердило успішне встановлення безпечного з’єднання. Пакети з локальної мережі коректно шифрувалися та передавалися до віддаленої локації, а зворотний трафік успішно доставлявся до корпоративної мережі.

В результаті, налаштування VPN забезпечило безпечний віддалений доступ для працівників компанії, ізольовану передачу даних через публічну мережу та готовність до масштабування, включно з додаванням нових підмереж і віддалених філій. Конфігурація відповідає сучасним вимогам безпеки, стандартам IPsec та корпоративним політикам інформаційної безпеки.

4.5 Налаштування маршрутизаторів на підтримку служби AAA

У корпоративній мережі електронної комерції забезпечення безпечного доступу до мережевих пристроїв та ресурсів є критично важливим завданням. Для цього було виконано налаштування служби AAA (Authentication, Authorization, Accounting) на маршрутизаторах мережі. AAA дозволяє централізовано керувати авторизацією користувачів, а також здійснювати контроль доступу та облік дій у системі. Центральним компонентом цієї системи виступає RADIUS-сервер, що забезпечує єдину точку аутентифікації для всіх користувачів, які підключаються до мережевих пристроїв через консольні або віртуальні інтерфейси.

Процес налаштування було реалізовано на прикладі одного з маршрутизаторів корпоративної мережі. Спершу активовано функціональність AAA за допомогою команди:

```
aaa new-model
```

Це дозволило увімкнути підтримку централізованої аутентифікації та авторизації, включно з використанням зовнішніх серверів та локальної бази користувачів.

Далі було виконано налаштування RADIUS-сервера для забезпечення централізованого управління користувачами. Для цього було вказано IP-адресу сервера, порт підключення та ключ аутентифікації:

radius-server host 172.24.128.251 auth-port 1645 key radius123

Даний крок гарантує, що всі запити на авторизацію користувачів будуть оброблятися централізовано, що підвищує рівень безпеки мережі та дозволяє вести централізований облік дій користувачів.

Наступним етапом було налаштування методів аутентифікації для різних типів доступу. Для доступу через консоль маршрутизатора визначено пріоритет використання RADIUS із резервною локальною базою користувачів:

aaa authentication login console group radius local

line console 0

login authentication console

Таке налаштування дозволяє першочергово перевіряти облікові дані користувачів на RADIUS-сервері, а у разі його недоступності – використовувати локальну базу даних.

Локальна база користувачів була створена для резервного доступу та тестування налаштувань:

aaa authentication login default local

username ecomers_R3 password admin123

Це забезпечує можливість доступу адміністратора до маршрутизатора навіть при тимчасовій відсутності зв’язку з RADIUS-сервером.

Для віддаленого доступу через VTY-порти було налаштовано використання стандартного методу аутентифікації AAA:

line vty 0 15

login authentication default

Це дозволяє забезпечити централізований контроль доступу для всіх віддалених адміністраторів та операторів мережі, гарантуючи, що лише авторизовані користувачі можуть змінювати налаштування маршрутизатора.

4.6 Налаштування firewall та доступу по SSH до серверу

В цьому розділі наведено основні вимоги та реалізація налаштування доступу до серверу для зберігання інформації в системі електронної комерції.

Метою налаштувань є забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів шляхом побудови стійкого шару мережевого захисту на рівні ядра операційної системи (netfilter/iptables) та належної організації доступу по SSH. Розглянуто вимоги, модель загроз, архітектуру правил, практичну реалізацію з командами та методи перевірки, а також рекомендації для експлуатації та відповідності нормативним вимогам безпеки.

4.6.1 Вимоги та обмеження

Функціональні вимоги базуються на фундаментальних потреб безпеки серверного обладнання. В ці вимоги входить:

1. Забезпечити доступ по SSH для адміністратора(ів) сервера.
2. Забезпечити доступ до СУБД (MySQL/PostgreSQL) лише для дозволених клієнтів.
3. Заблокувати ICMP echo-request (пінг) до сервера.
4. Мінімізувати поверхню атаки – заборонити всі непотрібні сервіси та порти (deny-by-default).
5. Забезпечити збереження та відновлюваність правил firewall після перезавантаження.

Нефункціональні вимоги:

1. Сумісність із дистрибутивами Debian/Ubuntu.
2. Автоматична відновлюваність правил після перезапуску сервісів/реінсталяції.

3. Журналювання подій безпеки для подальшого аудиту.

4. Відповідність принципам державних стандартів захисту інформації (практичні вимоги deny-by-default, stateful firewall, захист від сканування та flood-атак).

Аналіз загроз спрямований на виявлення та оцінку потенційних мережевих атак, яким може бути піддана система, та визначення необхідних заходів захисту. Однією з типових загроз є сканування портів, що виконується зовнішніми сканерами для виявлення відкритих сервісів і вразливостей системи. Ще одним ризиком є атака брутфорс на SSH, яка полягає у багаторазових спробах підбору облікових даних для несанкціонованого входу. Серед найбільш небезпечних атак також виділяються SYN- та UDP-флуди, спрямовані на відмову в обслуговуванні, що може призвести до недоступності сервісів. Несанкціонований доступ до баз даних також представляє серйозну загрозу, особливо якщо порти 3306 або 5432 залишаються відкритими, що створює потенційну точку проникнення. Крім того, підміна або підслуховування трафіку вимагає мінімізації відкритих сервісів та використання захищених каналів зв’язку, таких як SSH або HTTPS, щоб забезпечити конфіденційність та цілісність даних.

Архітектура захисту системи будується на комплексному підході, що включає декілька основних принципів. Політика «deny by default» передбачає, що всі ланцюги INPUT і FORWARD за замовчуванням мають ставитися як DROP, тобто будь-який непередбачений трафік блокується автоматично, що мінімізує ризик випадкового доступу. Для коректної роботи сервісів використовується stateful підхід, який враховує стан з’єднання та дозволяє пропускати лише ті пакети, що належать до вже встановлених або пов’язаних з ними з’єднань, забезпечуючи ефективний контроль потоків даних. Додатково впроваджується IP-біллістинг, який дозволяє доступ лише від попередньо відомих та довірених IP-адрес, таких як адміністративні машини, сервери Telegram-бота чи обладнання тепличної системи. Для захисту від атак типу брутфорс та flood передбачене обмеження швидкості нових підключень,

що запобігає перевантаженню системи. Важливою складовою архітектури є документоване збереження та відновлення правил, що здійснюється через файли /etc/iptables/rules.v4 і /etc/iptables/rules.v6 за допомогою пакетів iptables-persistent або netfilter-persistent, що гарантує відновлення захисних налаштувань після перезавантаження системи.

4.7 Налаштування Iptables

Для організації надійного захисту мережі на Debian/Ubuntu спершу потрібно підготувати систему та встановити необхідні пакети для збереження правил iptables, що забезпечить їх автоматичне відновлення після перезавантаження сервера. Виконується оновлення системи та встановлення пакетів iptables, iptables-persistent та netfilter-persistent:

```
sudo apt update
sudo apt install -y iptables iptables-persistent netfilter-persistent
```

Це створює файли /etc/iptables/rules.v4 і /etc/iptables/rules.v6, у яких зберігатимуться правила для IPv4 та IPv6.

Перед застосуванням нових правил необхідно очистити поточні ланцюги та таблиці, щоб уникнути конфліктів зі старими налаштуваннями:

```
sudo iptables -F
sudo iptables -X
sudo iptables -t nat -F
sudo iptables -t mangle -F
```

Далі встановлюються політики за замовчуванням. Усі вхідні та транзитні з’єднання блокуються, а вихідні пакети дозволяються, що реалізує принцип «deny by default»:

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

Для нормальної роботи системи необхідно дозволити локальні процеси та вже встановлені з’єднання. Loopback інтерфейс приймає всі пакети, а

пакети, що належать до станів ESTABLISHED або RELATED, також проходять без обмежень:

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

Щоб контролювати ICMP-повідомлення, блокується запит ping, але дозволяються критичні повідомлення, необхідні для трасування маршрутів та коректної роботи фрагментації пакетів:

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
sudo iptables -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
sudo iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
```

Для захисту SSH від несанкціонованого доступу дозволяються нові підключення на адміністративний порт, а механізм recent обмежує кількість спроб підключення, що ефективно запобігає швидким атакам брутфорс:

```
sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -m recent --name SSH --set
sudo iptables -A INPUT -p tcp --dport 22 -m recent --name SSH --update --seconds 30 --hitcount 6 -j DROP
```

Доступ до бази даних обмежується лише IP Telegram-бота. Це гарантує, що лише легітимний клієнт може підключитися до порту БД

```
sudo iptables -A INPUT -p tcp -s 1.2.3.4 --dport 3306 -m conntrack --ctstate NEW -j ACCEPT
```

Для тепличної системи дозволяється прийом пакетів тільки з її відомого IP на порт API. На рівні сервісу додатково реалізується авторизація через API-ключ або JWT:

```
sudo iptables -A INPUT -p tcp -s 10.20.30.40 --dport 8000 -m conntrack --ctstate NEW -j ACCEPT
```

Для протидії скануванню портів і аномальним TCP-флагам вводяться правила, що блокують пакети з некоректними комбінаціями, які часто використовуються зловмисниками для прихованої розвідки:

```
sudo iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

```
sudo iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
sudo iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
sudo iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
```

З метою захисту від SYN- та UDP-флудів реалізується лімітування нових з'єднань. Всі TCP-пакети без SYN для нових підключень відкидаються, а кількість нових TCP і UDP-з'єднань обмежується через rate limiting:

```
sudo iptables -A INPUT -p tcp ! --syn -m conntrack --ctstate NEW -j DROP
sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 4
-j ACCEPT
sudo iptables -A INPUT -p udp -m limit --limit 5/s --limit-burst 20 -j
ACCEPT
sudo iptables -A INPUT -p udp -j DROP
```

Всі небезпечні та непотрібні сервіси блокуються. Це включає NetBIOS, SMB, RPC, rsh і rlogin, що зазвичай не використовуються на сервері, але представляють підвищену загрозу:

```
sudo iptables -A INPUT -p udp --dport 137:139 -j DROP
sudo iptables -A INPUT -p tcp --dport 137:139 -j DROP
sudo iptables -A INPUT -p tcp --dport 445 -j DROP
sudo iptables -A INPUT -p tcp --dport 512:514 -j DROP
sudo iptables -A INPUT -p udp --dport 512:514 -j DROP
```

Для завершення конфігурації встановлюється останнє правило DROP, яке гарантує відхилення всього неявно дозволеного трафіку:

```
sudo iptables -A INPUT -j DROP
```

Після того як всі правила налаштовані, їх слід зберегти та застосувати для автоматичного відновлення після перезавантаження системи:

```
sudo netfilter-persistent save
sudo netfilter-persistent reload
```

Перевірити збережені правила можна у директорії /etc/iptables:

```
ls -l /etc/iptables
cat /etc/iptables/rules.v4
```

Таким чином, реалізується комплексний захист серверної системи: від обмеження доступу до критичних сервісів і контролю ICMP, до захисту SSH і баз даних, а також протидії мережевим скануванням і flood-атакам. Всі етапи

інтегровані з поясненнями, що дозволяє чітко розуміти призначення кожної групи правил та механізм їхньої дії.

4.7.1 Налаштування та посилення безпеки служби SSH

Для забезпечення безпечного віддаленого доступу до серверної системи було проведено комплексне налаштування служби SSH. Основною метою стало мінімізування ризиків несанкціонованого доступу та зменшення площини атаки завдяки обмеженням на автентифікацію, контрольованим параметрам входу та використанню криптографічно захищених облікових даних.

Було внесено зміни до конфігураційного файлу /etc/ssh/sshd_config, де були встановлені наступні параметри:

1. Port змінено на нестандартний з метою ускладнення автоматичних сканувань та масових атак на порт 22.

2. PermitRootLogin no – заборонено прямий вхід користувача root, що зменшує ризик експлуатації облікового запису з максимальними привілеями.

3. PasswordAuthentication yes – залишено можливість автентифікації паролем, проте паралельно увімкнено PubkeyAuthentication yes для можливості переходу на автентифікацію ключами.

4. PermitEmptyPasswords no – заблоковано використання порожніх паролів.

5. MaxAuthTries 4 – обмежено кількість спроб входу для зниження ефективності brute-force атак.

6. LoginGraceTime 60 – встановлено обмеження часу, протягом якого дозволено вводити облікові дані.

Після внесення змін служба SSH була перезапущена для застосування нової конфігурації.

Усі паролі користувачів системи, які використовуються для доступу через SSH, у Linux не зберігаються у відкритому вигляді. Після виконання налаштувань було підтверджено, що система використовує

механізм криптографічного хешування з сіллю, що відповідає сучасним стандартам безпеки.

Паролі зберігаються у файлі /etc/shadow у вигляді хешів формату: y алгоритм $ сіль $ хеш

У сучасних дистрибутивах Debian/Ubuntu за замовчуванням використовується yescrypt або scram-sha-256 або SHA-512-crypt, які забезпечують:

– індивідуальну сіль для кожного пароля – це унеможливлює використання rainbow-tables;

– повільне обчислення хешу, що робить brute-force в десятки тисяч разів менш ефективним;

– односторонність алгоритму, що гарантує неможливість відновлення оригінального пароля.

Таким чином, навіть у разі гіпотетичного доступу до файлу /etc/shadow зловмисник не має можливості отримати реальні паролі.

Для додаткового захисту була налаштована система автоматичного блокування підозрілої активності – fail2ban, яка аналізує журнал /var/log/auth.log та тимчасово блокує IP-адреси, що перевищують допустиму кількість спроб входу. Це суттєво знижує ризик масового перебору паролів.

У результаті виконаного налаштування служба SSH була посилена відповідно до сучасних рекомендацій безпеки. Доступ до сервера здійснюється з використанням шифрованих каналів, а всі облікові записи захищені хешованими паролями з криптографічною сіллю. Завдяки обмеженням, контролю спроб входу та інтеграції з fail2ban отримано надійний рівень захисту від більшості типових атак на віддалений доступ.

Парадигма deny-by-default, stateful firewall та обмеження доступу по IP відповідають загальним вимогам більшості національних стандартів захисту інформації.

Для повної відповідності до конкретних стандартів (наприклад, ГОСТ Р 57580.* або локальних регламентів) необхідно виконати додатковий аудит, включаючи процедури управління журналами, шифрування каналів передачі та політики доступу на рівні додатку/БД.

Варто документувати всі зміни в політиках доступу, впроваджувати процеси зміни конфігурацій (change control) і періодичні оцінки вразливостей.

Комбінація iptables, збереження правил (iptables-persistent), fail2ban та авторизація на рівні сервісу забезпечує багатошарову систему захисту, що відповідає принципам «least privilege» та «defense in depth».

Парадигма deny-by-default, stateful firewall та обмеження доступу по IP відповідають загальним вимогам більшості національних стандартів захисту інформації.

4.8 Розробка математичної моделі мережі як замкнутої системи масового обслуговування

Відповідно до структурної схеми комп’ютерної мережі та її імітаційної моделі розроблено структуру математичної моделі комп’ютерної мережі як замкнутої системи масового обслуговування (Рисунок 4.1).

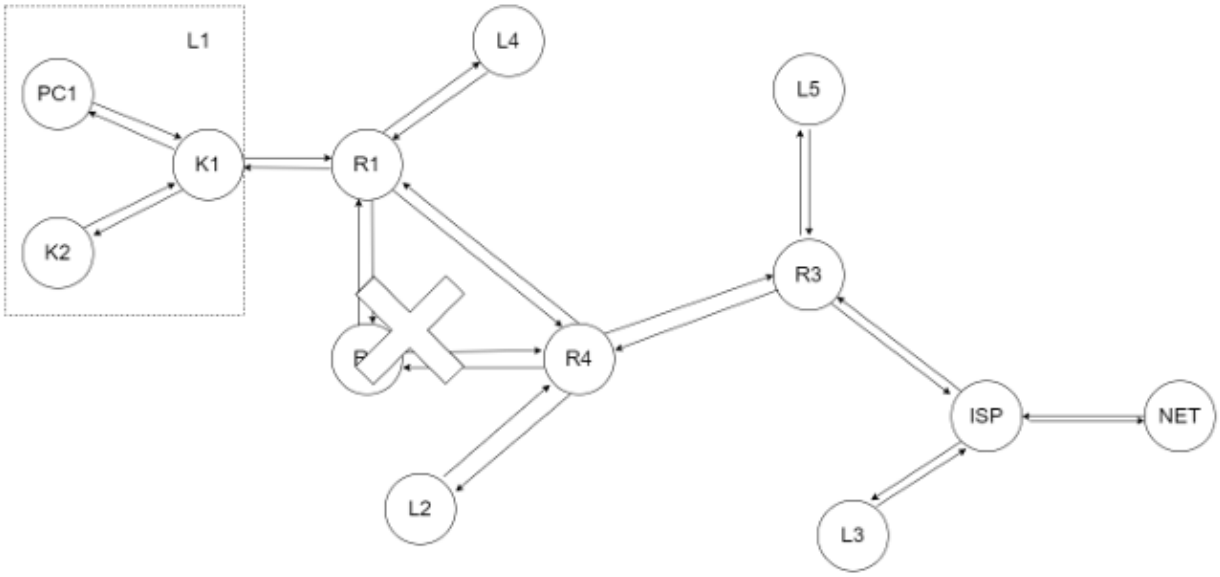


Рисунок 4.1 – Структура математичної моделі комп’ютерної мережі

В структурі моделі комп’ютерної мережі вузли K1, K2, L2, L4, L5, L3 – це комутатори, що обслуговують локальні мережі. Вузли R1, R4, R4, ISP – маршрутизатори. Зв’язки між елементами структури – це вірогідність передачі пакета від одного до другого вузла. Кожен вузол – це система масового обслуговування. Вірогідність того що вузол зв’язується сам з собою дорівнює нулю. Вірогідності зв’язку вузлів між собою описані у маршрутній матриці на рисунку 4.2

$$Pr := \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.25 & 0.25 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.33 & 0 & 0 & 0.33 & 0.34 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.33 & 0.33 & 0 & 0 & 0.34 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0 & 0.33 & 0 & 0.34 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0 & 0.33 & 0 & 0.34 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Рисунок 4.2 – Маршрутна матриця

Матриця стовпчик, що показує час обробки одного повідомлення в відповідному вузлі:

$\tau =$

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

Рисунок 4.3 – Матриця стовпчик

4.9 Розрахунок параметрів мережі по її моделі

Далі методом Гауса розраховується матриця стовпчик з передаточними коефіцієнтами(рисунок 4.4).

Задаємо матрицю m, коефіцієнти якої означають кількість конвеєрів обробки пакетів в кожному із вузлів системи масового обслуговування(рисунок 4.4).

Для розрахунків приймаємо, що в кожному пристрої знаходиться лише один конвеєр обробки пакетів. Матриця B це матриця яка визначає з якою вірогідністю у відповідному вузлі (строчки) буде знаходитися в очікуванні обробки пакетів (номер стовпчика).

$$e := \begin{pmatrix} 1 \\ 1 \\ 4 \\ 6.06 \\ 2.06 \\ 2 \\ 6.24 \\ 6.43 \\ 2.12 \\ 2.19 \\ 6.23 \\ 2.25 \end{pmatrix}$$

m =

	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

Рисунок 4.4 – Виконання методу Гауса та матриця конвеєрів

B =

	0	1	2	3	4
0	0.849	0.128	0.019	$2.927 \cdot 10^{-3}$	$4.414 \cdot 10^{-4}$
1	0.849	0.128	0.019	$2.927 \cdot 10^{-3}$	$4.414 \cdot 10^{-4}$
2	0.395	0.239	0.145	0.088	0.053
3	0.084	0.078	0.072	0.066	0.061
4	0.689	0.215	0.067	0.021	$6.455 \cdot 10^{-3}$
5	0.698	0.211	0.064	0.019	$5.81 \cdot 10^{-3}$
6	0.057	0.054	0.052	0.05	0.047
7	0.028	0.028	0.028	0.028	0.028
8	0.679	0.218	0.07	0.022	$7.145 \cdot 10^{-3}$
9	0.669	0.222	0.073	0.024	$8.011 \cdot 10^{-3}$
10	0.058	0.055	0.053	0.051	0.048
11	0.66	0.34	0.116	0.039	...

Рисунок 4.5 – Матриця B

Відповідно до алгоритму Бузена розраховуються середні значення по кожному із вузлів мережі. (рисунок 4.6-7)

$\lambda =$

	0
0	0.033
1	0.033
2	0.133
3	0.202
4	0.069
5	0.067
6	0.208
7	0.214
8	0.071
9	0.073
10	0.207
11	0.075

Рисунок 4.6 – Інтенсивність вхідного потоку пакетів у кожному вузлі

$L =$

	0
0	0.178
1	0.178
2	1.525
3	9.639
4	0.452
5	0.433
6	13.066
7	19.219
8	0.471
9	0.495
10	12.829
11	0.78

Рисунок 4.7 –Середнє число пакетів що чекають на обробку в кожному вузлі

t =

	0
0	5.353
1	5.353
2	11.457
3	47.81
4	6.596
5	6.511
6	62.941
7	89.847
8	6.684
9	6.79
10	61.897
11	10.421

Рисунок 4.8 – Середній час обробки пакета в вузлі

4.10 Висновок до розділу

У розділі 4 виконано розробку та практичну реалізацію програмно-конфігураційних рішень для забезпечення безпечного, надійного та керованого функціонування корпоративної мережі e-commerce підприємства. Розділ поєднує інженерні налаштування мережевих пристроїв із формальним математичним моделюванням, що дозволяє комплексно оцінити роботу інфраструктури як з практичної, так і з теоретичної точки зору.

Проведено детальну перевірку та аудит базової конфігурації маршрутизаторів, що підтвердило відповідність налаштувань вимогам корпоративної політики безпеки: забезпечено захищений доступ через SSH, коректну автентифікацію користувачів, шифрування паролів, контроль локального та віддаленого доступу, а також стабільну роботу інтерфейсів WAN. Реалізація EtherChannel між комутаторами довела ефективність агрегації каналів для підвищення пропускної здатності та відмовостійкості міжкомутаторних з’єднань.

Налаштування VLAN забезпечило логічну сегментацію мережі з чітким розмежуванням користувацького, адміністративного, сервісного та керуючого трафіку. Інтеграція VLAN із DHCP дозволила автоматизувати керування IP-адресним простором і спростити адміністрування мережі. Реалізація VPN на

базі IPsec гарантувала захищений віддалений доступ до корпоративних ресурсів через публічні канали зв’язку, що є критично важливим для електронної комерції.

Окрему увагу приділено впровадженню служби AAA з використанням RADIUS, що забезпечило централізовану аутентифікацію, авторизацію та облік дій користувачів, підвищивши керованість і контроль доступу до мережевих пристроїв. Розроблено багаторівневу систему захисту серверної інфраструктури на основі iptables, deny-by-default політик, stateful firewall, обмеження доступу по IP, захисту від brute force та flood-атак, а також посилення безпеки служби SSH із використанням сучасних криптографічних механізмів і fail2ban.

Завершальним етапом розділу стала розробка математичної моделі мережі як замкнутої системи масового обслуговування та розрахунок її параметрів за алгоритмом Бузена. Отримані значення інтенсивностей потоків, середніх черг і часу обробки пакетів дозволяють кількісно оцінити навантаження на окремі вузли мережі та визначити потенційні «вузькі місця».

5 ЕКСПЕРЕМЕНТАЛЬНИЙ РОЗДІЛ

5.1 Мета і завдання експерименту

Цей етап досліджень спрямований на вивчення роботи комп'ютерної мережі за різних умов навантаження, включаючи вплив шкідливого програмного забезпечення. Основна мета − оцінити продуктивність мережі, виявити вузли з найбільшою ймовірністю виникнення черг, а також визначити ефективність корекції характеристик проблемних вузлів.

Завдання експерименту:

1. Визначити параметри роботи мережі в «нормальному» режимі без шкідливого ПЗ, включаючи інтенсивність трафіку, час обробки пакетів та кількість пакетів у вузлах.

2. Дослідити вплив вірусних програм на характеристики мережі, зокрема на ймовірність виникнення черг та завантаження вузлів.

3. Оцінити ефективність заходів з корекції вузлів, що найбільше піддаються перевантаженню, шляхом підвищення швидкості обробки пакетів.

4. Методи проведення експерименту включають моделювання мережі за допомогою віртуалізації та мережевих емуляторів, створення тестового навантаження та аналіз середніх і ймовірнісних характеристик роботи вузлів.

Ціль експерименту:

1. Виявити вузли, найбільш уразливі до перевантажень та шкідливих програм.

2. Перевірити ефективність заходів щодо підвищення стійкості мережі.

3. Забезпечити обґрунтовані рекомендації для оптимізації роботи корпоративної мережі та підвищення її надійності.

Таким чином, експеримент охоплює аналіз стану мережі у нормальному режимі, під впливом вірусного ПЗ та після корекції характеристик проблемних вузлів, що дозволяє комплексно оцінити її продуктивність і стійкість до навантажень.

5.2 Параметри роботи мережі без впливу шкідливого програмного забезпечення

Робота комп'ютерної мережі в «нормальному» режимі характеризується наступними параметрами. Кількість пакетів, які циркулюють у мережі дорівнює 5. Час обробки пакетів у всіх вузлах мережі одинаків і складає 5 часових одиниць (для досліджуваної мережі 1 часова одиниця дорівнює 1 мілісекунді). Кількість конвеєрів обробки пакетів у кожному вузлі мережі дорівнює 1. За таких вихідних даних отримано графіки, що показують усереднені характеристики кожного з вузлів.

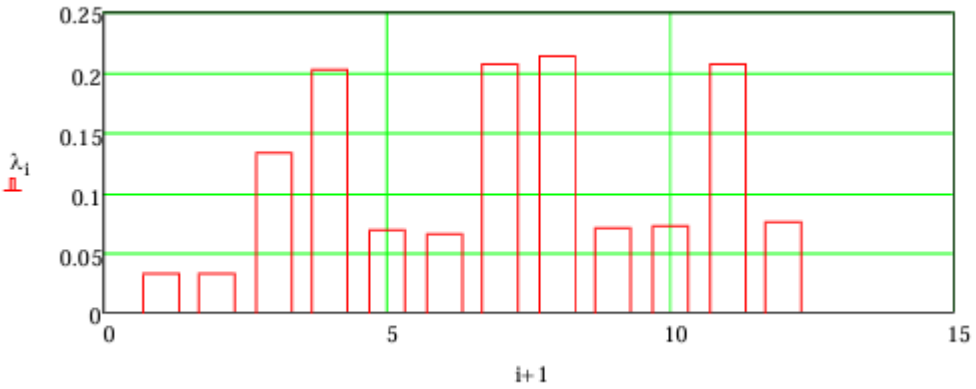


Рисунок 5.1 – Інтенсивність потоку, що входить у вузол

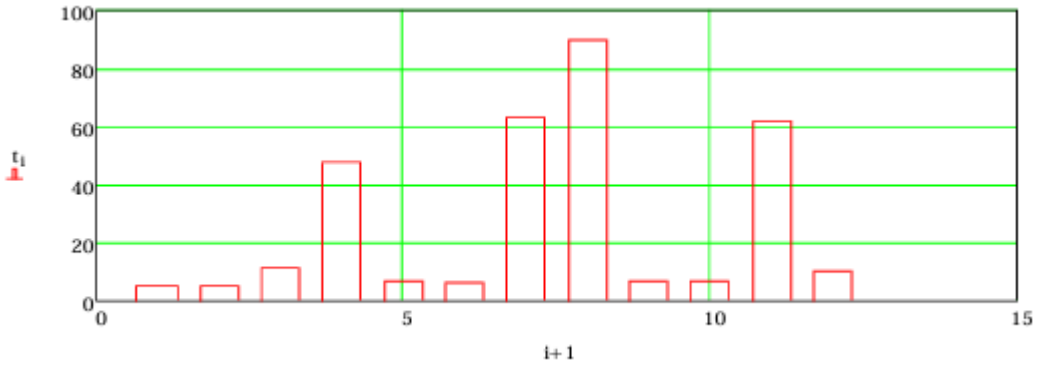


Рисунок 5.2 – Середній час перебування пакета у вузлі

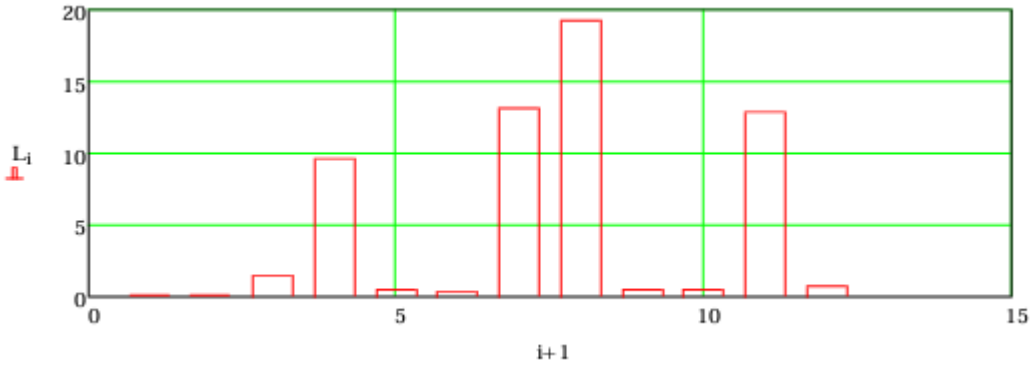


Рисунок 5.3 – Середня кількість пакетів які знаходяться у вузлі

Як бачимо, в цілому у всіх вузлах мережі, які є комутаторами усереднені параметри показують, що усі повідомлення обробляються швидко і без черги. Виключенням є вузли 2,4,5,6,7 які відповідають за маршрутизацію всередині мережі. Рисунок 5.4 показує з якою вірогідністю у вузлах мережі буде черга.

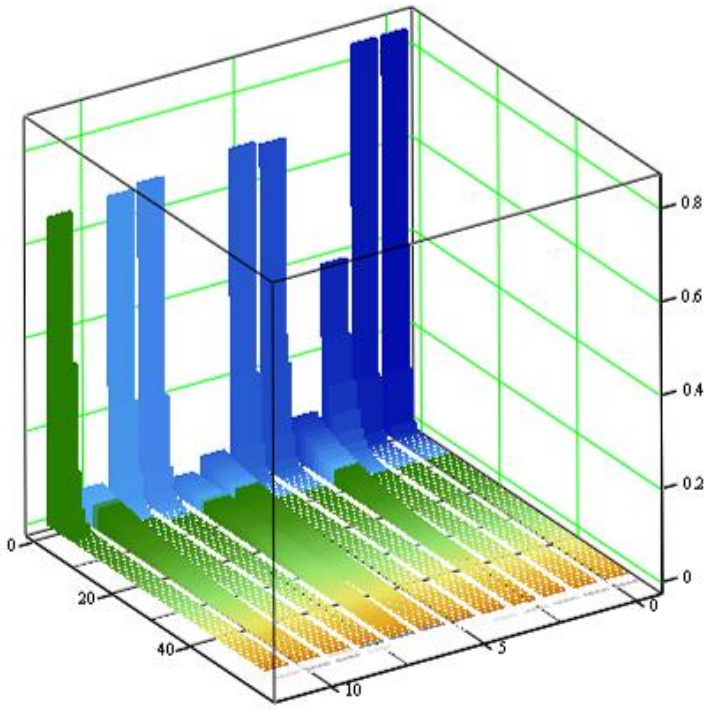


Рисунок 5.4 – Вірогідність черги у вузлах мережі

Можемо зробити попередній висновок про те, що при заданих параметрах маршрутизатори мережі є найбільш проблемним.

5.3 Параметри роботи мережі під впливом вірусних програм

Вірусне ПЗ, як і будь-які інші програми, вимагають певного обсягу ресурсів ЕОМ, на якому вони виконуються, а також можуть генерувати додатковий трафік в мережі. В залежності від виду вірусів, створювана ними навантаження на ЕОМ і мережу може сильно відрізнятися. Так, наприклад, класичні віруси в загальному випадку не створюють навантаження на мережу 35 зовсім. Деякі ж мережеві віруси можуть здійснювати таку кількість мережевих запитів, що обчислювальна мережа може і зовсім перестати функціонувати. Для моделювання подібної ситуації задаємо кількість запитів у мережі збільшуємо чотири рази, N=60.

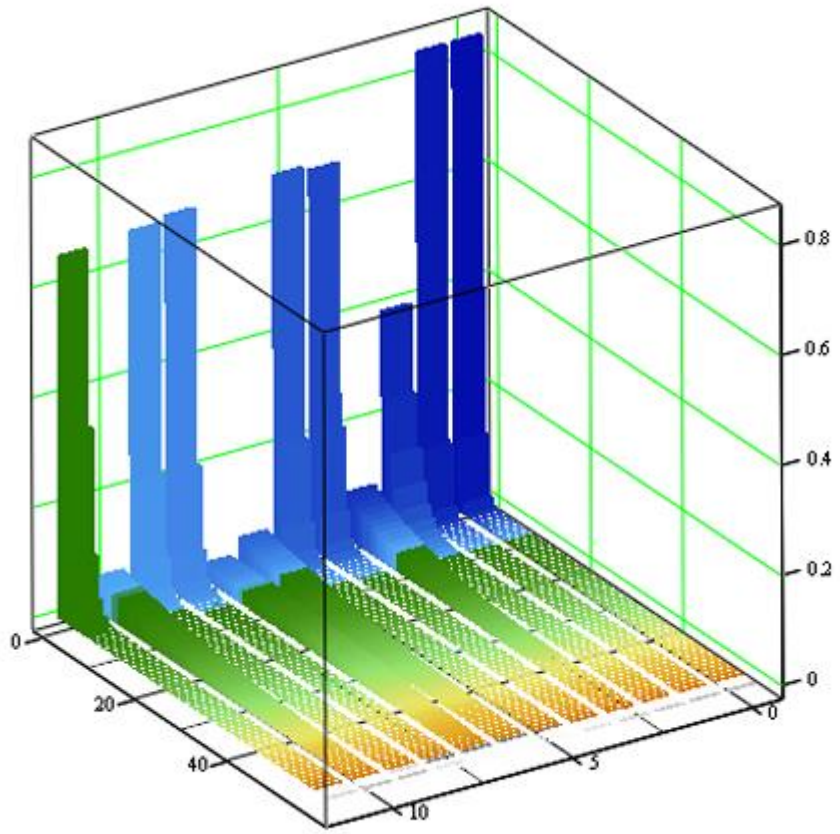


Рисунок 5.5 – Вірогідність черги у вузлах якщо в мережі циркулює 60 пакетів

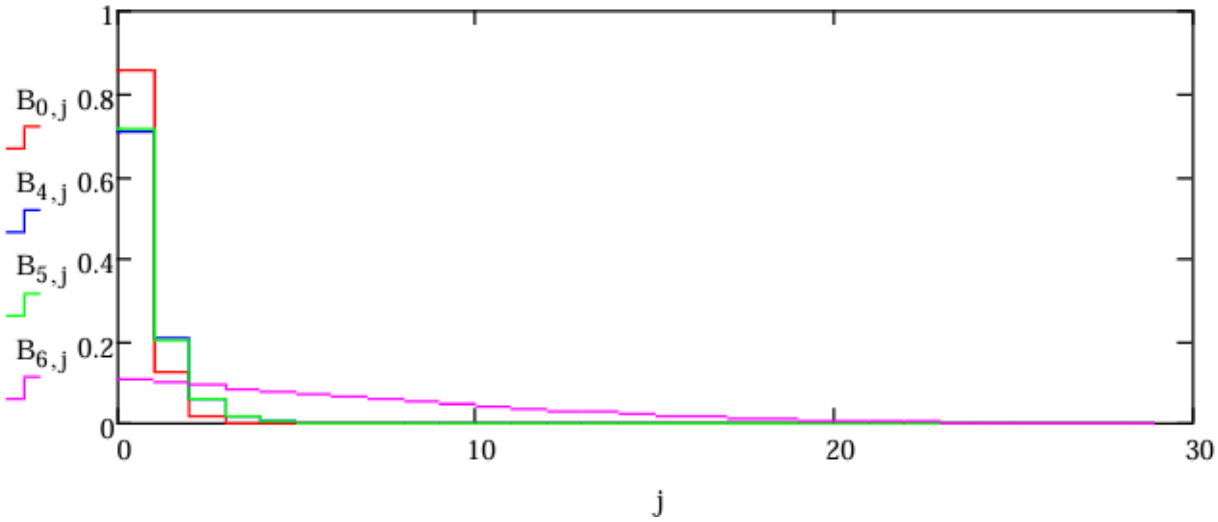


Рисунок 5.6 – Вірогідність черги у вузлах якщо в мережі циркулює 30 пакетів

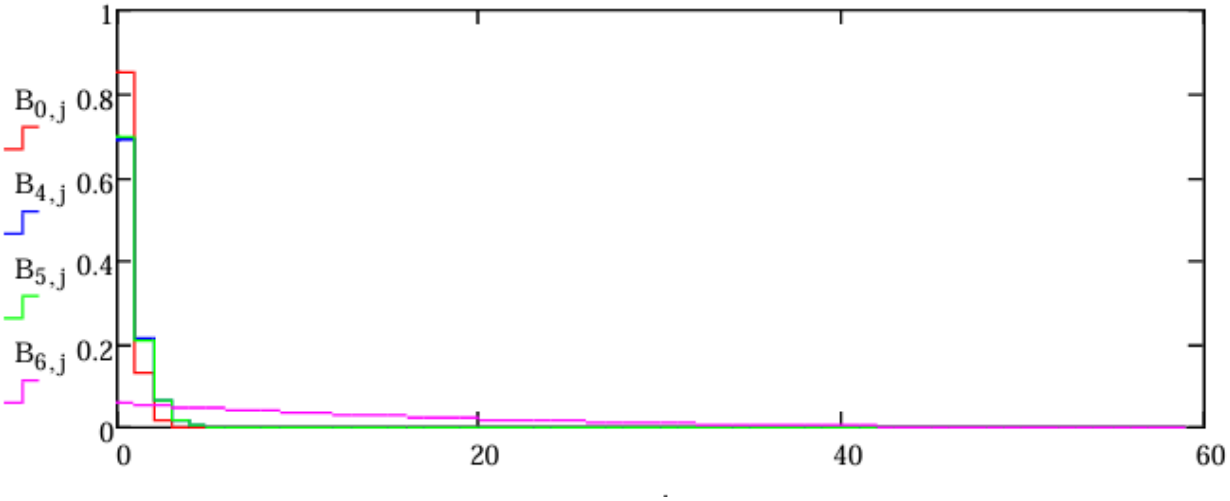


Рисунок 5.7 – Вірогідність черги у вузлах якщо в мережі циркулює 60 пакетів

Результати моделювання показують, що збільшення вдвічі кількості пакетів, що циркулюють в мережі приводить до того, що тільки вузли комутаторів №1,3,8,9,11,13,14,16,18 зростає вірогідність того що в черзі уже будуть знаходитися 2 пакета.

5.4 Робота мережі із скоригованими характеристиками проблемних вузлів

Корекція характеристик вузлів №2,4,5,6,7 проводиться за рахунок підвищення швидкості обробки пакетів.

$\tau =$

	0
0	5
1	3
2	5
3	3
4	2
5	3
6	3
7	5
8	5
9	5
10	5
11	5
12	5
13	5
14	5
15	5
16	5
17	5
18	5

Рисунок 5.8 – Корекція характеристик вузлів

Відповідно до змін розраховані як усереднені так і ймовірнісні характеристики.

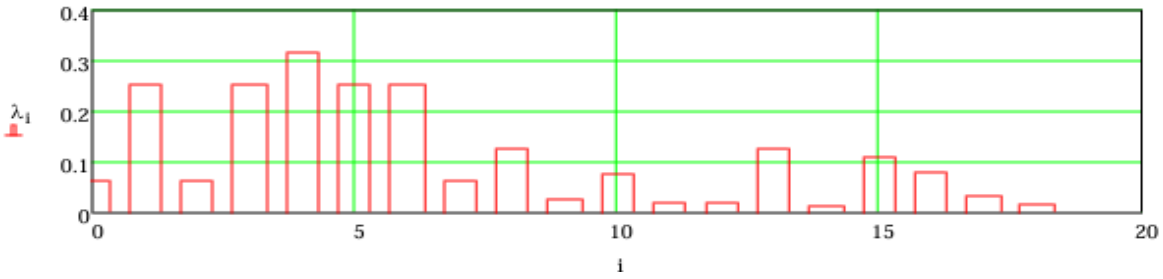


Рисунок 5.9 – Інтенсивність потоку, що входить у вузол

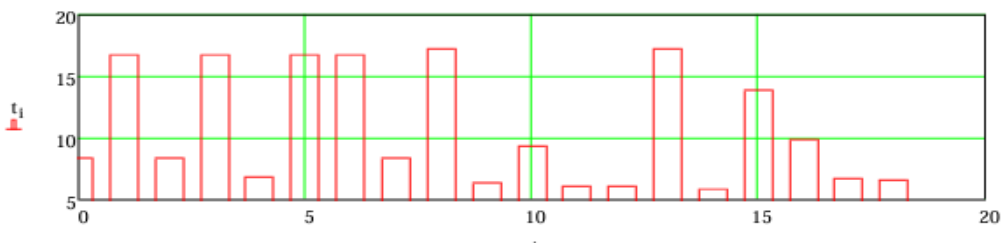


Рисунок 5.10 – Середній час перебування пакета у вузлі

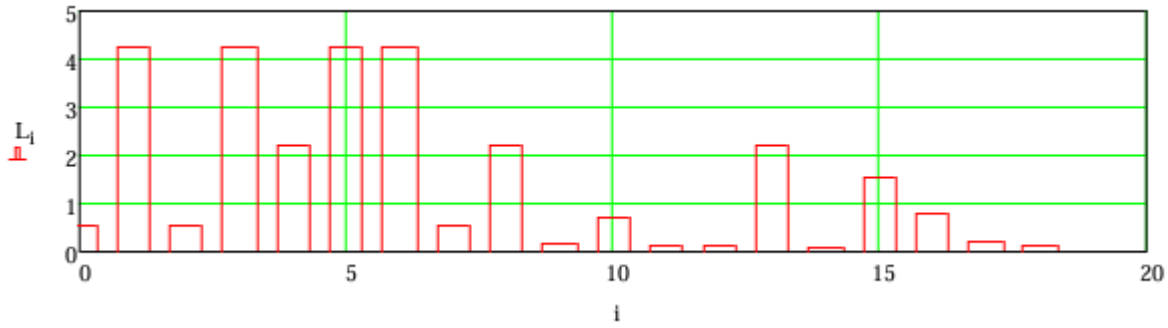


Рисунок 5.11 – Середня кількість пакетів які знаходяться у вузлі

Вірогідність того, що в вузлах мережі може виникнути черга значно знизилася (Рисунок 5.12)

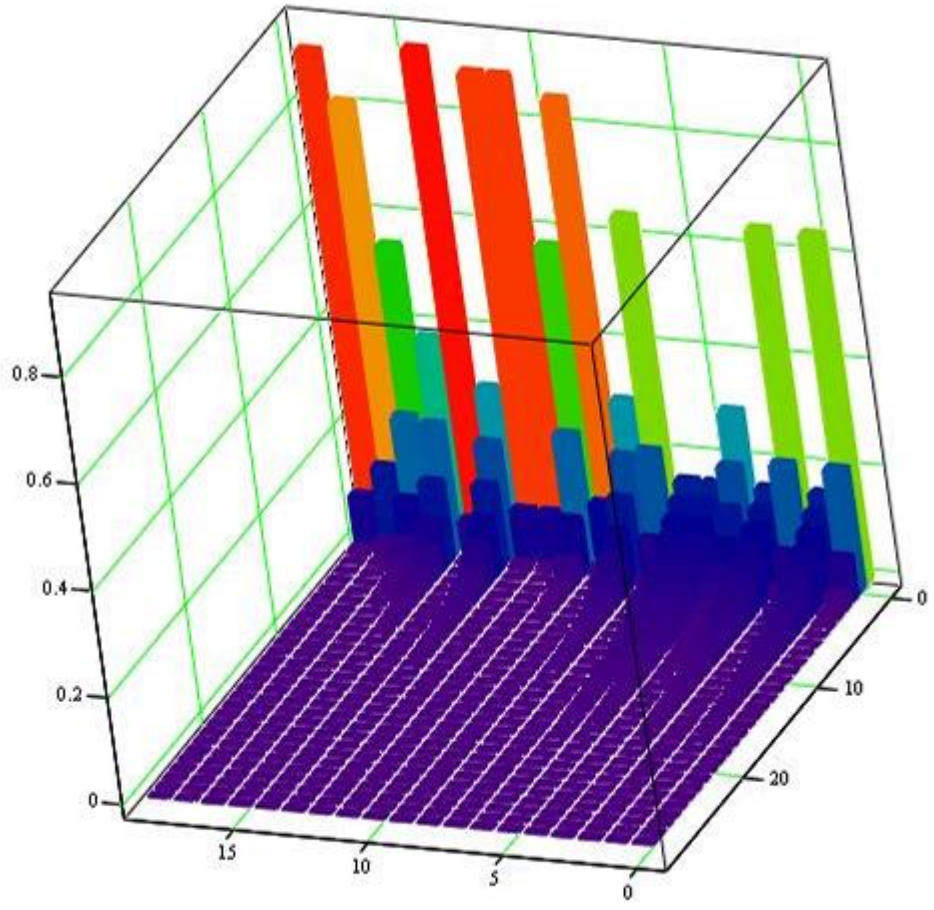


Рисунок 5.12 – Вірогідність черги у вузлах якщо в мережі циркулює 30 пакетів

Якщо в мережі із скоригованими характеристиками буде циркулювати 10 пакетів тоді вірогідність того, що в вузлах не буде черги зменшується для роутерів (Рисунок2.13). Підвищення швидкості обробки пакетів у вузлах, які показали найменшу стійкість до перевантаження дозволили певним чином покращити характеристики мережі.

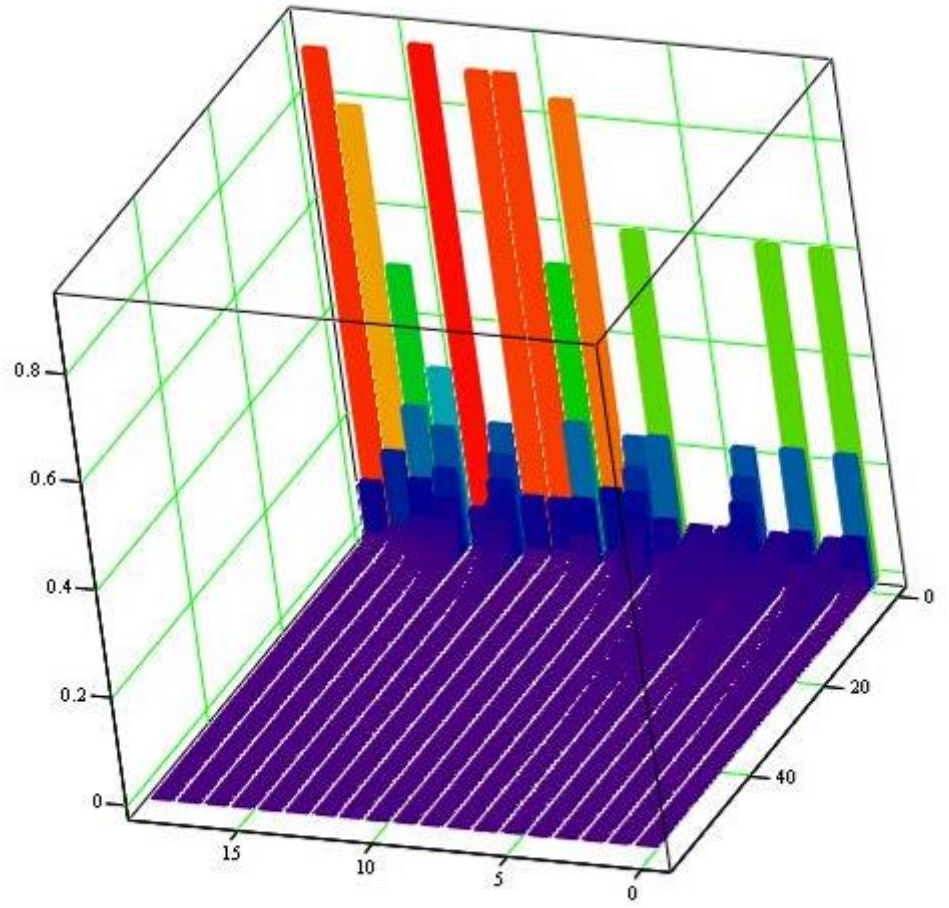


Рисунок 5.13 – Вірогідність черги у вузлах якщо в мережі циркулює 60 пакетів

Згідно з аналізом даних, отриманих в результаті вивчення стану мережі під впливом тільки шкідливих програм, стохастичний характер маршрутної матриці, яка описує мережу, може стати причиною нелінійного зростання основних характеристик в деяких вузлах мережі, незважаючи на те,що завантаження вузлів мережі зростатиме лінійно. Таке явище може призводити до збоїв в роботі комп'ютерної мережі. Аналіз характеристик розглянутої

мережі під впливом тільки АПО показує, що внаслідок запуску антивірусної програми в вузлах мережі з досить 41 високою середньою завантаженістю конвеєрів, основні характеристики можуть погіршитися в рази. За результатами порівняння характеристик обчислювальної мережі у всіх розглянутих станах зроблено висновок про те, щонайбільш негативно на характеристиках мережі позначається атака шкідливими програмами.

5.5 Висновок до експерементального розділу

У експериментальному розділі проведено комплексне дослідження роботи корпоративної комп'ютерної мережі за різних умов функціонування: у нормальному режимі, під впливом шкідливого програмного забезпечення та після корекції характеристик найбільш проблемних вузлів. Метою експерименту було оцінити продуктивність і стійкість мережі, визначити вузли, схильні до перевантажень, а також перевірити ефективність заходів щодо підвищення надійності інфраструктури.

Результати експериментів у штатному режимі показали, що за невеликої кількості пакетів у мережі всі комутаційні вузли працюють стабільно, без формування черг, тоді як маршрутизатори є найбільш уразливими елементами з точки зору виникнення затримок. Моделювання впливу вірусного програмного забезпечення, що супроводжувалося різким зростанням кількості пакетів у мережі, продемонструвало суттєве погіршення характеристик: зросла ймовірність утворення черг, збільшився час перебування пакетів у вузлах та проявилися нелінійні ефекти навантаження, обумовлені стохастичним характером маршрутної матриці.

Після корекції характеристик проблемних вузлів шляхом підвищення швидкості обробки пакетів було зафіксовано значне покращення показників роботи мережі. Ймовірність утворення черг істотно знизилася навіть за підвищених навантажень, а середній час перебування пакетів у вузлах зменшився. Отримані результати підтвердили, що цілеспрямована оптимізація окремих елементів інфраструктури дозволяє ефективно підвищити стійкість

мережі до перевантажень та негативного впливу шкідливого програмного забезпечення.

ВИСНОВОК

Кваліфікаційна робота є завершеною науково-практичною роботою, у межах якої вирішено задачу аналізу, проєктування, реалізації та експериментального дослідження корпоративної комп’ютерної мережі, призначеної для забезпечення стабільної, безпечної та масштабованої роботи e-commerce системи. Робота охоплює повний цикл створення мережевої інфраструктури — від аналізу предметної області та теоретичного обґрунтування до практичної реалізації, математичного моделювання та експериментальної перевірки отриманих рішень.

У процесі виконання роботи було проведено комплексний аналіз стану питання функціонування корпоративних мереж у сфері електронної комерції. Розглянуто організаційну структуру об’єкта впровадження, особливості топологічного розміщення підрозділів, типи трафіку та вимоги до інформаційної інфраструктури, що забезпечує роботу веб-платформи, платіжних сервісів, внутрішніх інформаційних систем і зовнішніх інтеграцій. Визначено ключові фактори, які впливають на продуктивність, надійність і безпеку e-commerce мереж.

На основі теоретичних досліджень проаналізовано методи обробки та передачі інформації, сучасні мережеві технології, показники якості обслуговування (QoS), а також принципи побудови корпоративних мереж. Обґрунтовано доцільність використання моделей масового обслуговування для аналізу мережевого трафіку та прогнозування поведінки мережі за різних рівнів навантаження. Розглянуто підходи до забезпечення пріоритизації трафіку, відмовостійкості та керованості мережевої інфраструктури.

У роботі виконано синтез комп’ютерної системи e-commerce підприємства, сформульовано цілі впровадження та визначено технічні вимоги до мережевої інфраструктури, зокрема щодо надійності, масштабованості, інформаційної та фізичної безпеки. Розроблено функціональну структуру мережі, обґрунтовано вибір топології, елементної

бази мережевого обладнання, кабельних систем і типів з’єднань для офісу, дата-центру та складу. Запропоновані рішення відповідають сучасним стандартам і забезпечують можливість подальшого розвитку системи.

У практичній частині реалізовано налаштування ключових мережевих сервісів і механізмів безпеки, зокрема маршрутизації, VLAN, EtherChannel, VPN, служби AAA, міжмережевого екрану та захищеного доступу по SSH. Побудовано багаторівневу систему захисту серверної інфраструктури з використанням iptables, deny-by-default політик, stateful firewall, обмеження доступу по IP та захисту від мережевих атак. Це забезпечило відповідність мережі вимогам інформаційної безпеки та корпоративним політикам доступу.

Окремим етапом виконано розробку математичної моделі корпоративної мережі як замкнутої системи масового обслуговування та проведено розрахунок її параметрів за алгоритмом Бузена. На основі цієї моделі здійснено експериментальне дослідження роботи мережі в нормальному режимі, під впливом шкідливого програмного забезпечення та після корекції характеристик проблемних вузлів. Отримані результати дозволили виявити найбільш уразливі елементи інфраструктури, оцінити нелінійний характер зростання навантажень і підтвердити ефективність оптимізаційних заходів.

Таким чином, у кваліфікаційній роботі досягнуто поставленої мети та виконано всі визначені завдання. Запропонована корпоративна мережа e-commerce системи забезпечує високу продуктивність, стійкість до перевантажень, належний рівень інформаційної безпеки та готовність до масштабування. Отримані теоретичні, практичні й експериментальні результати можуть бути використані для подальшого вдосконалення мережевої інфраструктури, оптимізації параметрів обладнання та підвищення ефективності функціонування e-commerce платформи в умовах зростаючих вимог до швидкодії та надійності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основи побудови корпоративних мереж. Навчальний матеріал Cisco Networking Academy [Електронний ресурс] – Режим доступу: https://www.netacad.com/ (дата звернення 10.12.2025р.)

2. Архітектура мережевих рішень Cisco – Documentation [Електронний ресурс] – Режим доступу: https://www.cisco.com/ (дата звернення 10.12.2025р.)

3. Juniper Networks – Networking Concepts Overview [Електронний ресурс] – Режим доступу: https://www.juniper.net/ (дата звернення 10.12.2025р.)

4. Hewlett Packard Enterprise – Network Solutions Library [Електронний ресурс] – Режим доступу: https://www.hpe.com/ (дата звернення 10.12.2025р.)

5. Основи електронної комерції. Навчальний посібник / Міщенко А. С., Юрченко Т. В. – КНЕУ, 2021. – 184 с. [Електронний ресурс] – Режим доступу: https://kneu.edu.ua (дата звернення 10.12.2025р.)

6. Моделювання комп’ютерних мереж. Практикум / Олійник В. М., Шульга Д. А. – КПІ ім. І. Сікорського, 2020. – 112 с. [Електронний ресурс] – Режим доступу: https://kpi.ua (дата звернення 10.12.2025р.)

7. Системи масового обслуговування: теорія та застосування / Гнатюк С. О., Колесник В. П. – ЛНУ ім. І. Франка, 2019. – 96 с. [Електронний ресурс] – Режим доступу: https://lnu.edu.ua (дата звернення 10.12.2025р.)

8. Principles of E-commerce Networking. IBM Developer Library [Електронний ресурс] – Режим доступу: https://developer.ibm.com/ (дата звернення 10.12.2025р.)

9. Cloudflare Documentation – Network Performance and Security [Електронний ресурс] – Режим доступу: https://developers.cloudflare.com/ (дата звернення 10.12.2025р.)

10. NIST Special Publication 800-53 – Security and Privacy Controls [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/ (дата звернення 10.12.2025р.)

11. Моніторинг мережевої інфраструктури. Навчальний матеріал Zabbix [Електронний ресурс] – Режим доступу: https://www.zabbix.com/ (дата звернення 10.12.2025р.)

12. Протоколи динамічної маршрутизації. Навчальна лекція. – ХНУРЕ, 2022. – 24 с. [Електронний ресурс] – Режим доступу: https://nure.ua (дата звернення 10.12.2025р.)

13. Правила побудови VLAN та сегментування мереж. Cisco Learning Hub [Електронний ресурс] – Режим доступу: https://learningnetwork.cisco.com/ (дата звернення 10.12.2025р.)

14. VPN Technologies Overview. Fortinet Documentation [Електронний ресурс] – Режим доступу: https://www.fortinet.com/ (дата звернення 10.12.2025р.)

15. Amazon Web Services – E-commerce Architecture Best Practices [Електронний ресурс] – Режим доступу: https://aws.amazon.com/architecture/ (дата звернення 10.12.2025р.)

16. Google Cloud Network Design Guide [Електронний ресурс] – Режим доступу: https://cloud.google.com/architecture (дата звернення 10.12.2025р.)

17. Бойко М. М. Комп’ютерні мережі та телекомунікації. Практикум. – НАУ, 2020. – 134 с. [Електронний ресурс] – Режим доступу: https://nau.edu.ua (дата звернення 10.12.2025р.)

18. Основи кібербезпеки корпоративних мереж. Навчальний курс / Сіренко І. В. – ХПІ, 2021. – 78 с. [Електронний ресурс] – Режим доступу: https://khpi.edu.ua (дата звернення 10.12.2025р.)

19. RFC 793 – Transmission Control Protocol (TCP). Internet Engineering Task Force [Електронний ресурс] – Режим доступу: https://www.rfc-editor.org/ (дата звернення 10.12.2025р.)

ДОДАТОК А

Дапм налаштування елементів КМ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24004-01 12 01

Листів 9

2025

АНОТАЦІЯ

Дана програма містить в собі команди для налаштування маршрутизаторів та комутаторів корпоративної мережі. Команди призначені для налаштування IP-адрес, базового налаштування пристроїв, налаштування DHCP, NAT, VPN, AAA, OSPF, VLAN, статичних маршрутів, EtherChannel та безпеки портів.

ЗМІСТ

1. ecomers_R1

```
 ecomers_R1#show run
Current configuration : 2251 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname  ecomers_R1
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.128.33 172.24.128.35
ip dhcp excluded-address 172.24.128.127
ip dhcp excluded-address 172.24.128.128
ip dhcp pool LAN-2
network 172.24.128.0 255.255.255.128
default-router 172.24.128.33
dns-server 172.24.128.250
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 123191_ ecomers_R1 password 7 082048430017061E010803
username  ecomers12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX1524W772-
ip domain-name  ecomers_R1
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.24.128.33 255.255.255.128
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 172.1.128.17 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/3/0
ip address 172.1.128.6 255.255.255.252
!
interface Serial0/3/1
ip address 172.1.128.9 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
```

```
no passive-interface GigabitEthernet0/2
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
auto-cost reference-bandwidth 1000
network 172.24.128.0 0.0.0.127 area 0
network 172.1.128.16 0.0.0.3 area 0
network 172.1.128.4 0.0.0.3 area 0
network 172.1.128.8 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
banner motd ^C ecomers_R1^C
radius server host
address ipv4 172.24.128.251 auth-port 1645
key radius123
radius server 172.24.128.251
address ipv4 172.24.128.251 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end
```

2. ecomers_R3

```
 ecomers_R3#show run
Current configuration : 2937 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname  ecomers_R3
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 123191_ ecomers_R3 password 7 082048430017061E010803
username  ecomers12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX152413GN-
ip domain-name  ecomers_R3
spanning-tree mode pvst
```

```
interface GigabitEthernet0/0
ip address 172.1.128.2 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/2/0
ip address 209.165.202.1 255.255.255.252
ip nat outside
!
interface Serial0/2/1
no ip address
clock rate 128000
!
interface Serial0/3/0
ip address 172.1.128.14 255.255.255.252
ip nat inside
!
interface Serial0/3/1
ip address 172.1.128.5 255.255.255.252
ip nat inside
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface Serial0/2/0
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
auto-cost reference-bandwidth 1000
network 172.1.128.0 0.0.0.3 area 0
network 172.1.128.12 0.0.0.3 area 0
network 172.1.128.4 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT11 pool Internet
ip nat inside source static 172.24.128.251 209.165.200.4
ip nat inside source static 172.24.128.250 209.165.200.3
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
!
ip access-list extended NAT11
deny ip 172.24.128.0 0.0.0.31 172.24.129.0 0.0.0.127
deny ip 172.24.128.0 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.24.128.128 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.24.129.128 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.1.128.0 0.0.0.255 172.24.129.0 0.0.0.127
permit ip 172.24.128.0 0.0.0.31 any
permit ip 172.24.128.0 0.0.0.127 any
permit ip 172.24.128.128 0.0.0.127 any
permit ip 172.24.129.128 0.0.0.127 any
permit ip 172.1.128.0 0.0.0.255 any
!
banner motd ^C ecomers_R3^C
!
radius server host
address ipv4 172.24.128.251 auth-port 1645
key radius123
radius server 172.24.128.251
address ipv4 172.24.128.251 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end
```

3. ecomers_R0

```
Current configuration : 3192 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname  ecomers_R0
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.129.1 172.24.129.5
ip dhcp excluded-address 172.24.129.126
ip dhcp excluded-address 172.24.129.127
```

```
ip dhcp excluded-address 172.24.129.1 172.24.129.10
ip dhcp excluded-address 172.24.129.5
!
ip dhcp pool LAN4-VLAN10
network 172.24.129.0 255.255.255.224
default-router 172.24.129.1
dns-server 172.24.128.250
ip dhcp pool LAN4-VLAN20
network 172.24.129.32 255.255.255.224
default-router 172.24.129.33
dns-server 172.24.128.250
ip dhcp pool LAN4-VLAN30
network 172.24.129.64 255.255.255.224
default-router 172.24.129.65
dns-server 172.24.128.250
!
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
ip cef
no ipv6 cef
!
!
!
username 123191_ ecomers_R0 password 7 082048430017061E010803
username  ecomers12321ck1 password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524MF8K-
license boot module c2900 technology-package securityk9
ip domain-name  ecomers_R0
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 64.100.13.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.24.129.1 255.255.255.224
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 172.24.129.33 255.255.255.224
!
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.24.129.65 255.255.255.224
```

```
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.24.129.97 255.255.255.240
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface GigabitEthernet0/1.10
no passive-interface GigabitEthernet0/1.20
no passive-interface GigabitEthernet0/1.30
no passive-interface GigabitEthernet0/1.99
auto-cost reference-bandwidth 1000
network 172.24.129.0 0.0.0.127 area 0
network 64.100.13.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended VPN1
permit ip 172.24.129.0 0.0.0.127 172.24.128.0 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.24.128.0 0.0.0.31
permit ip 172.24.129.0 0.0.0.127 172.24.128.128 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.24.129.128 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.1.128.0 0.0.0.255
!
banner motd ^C ecomers_R0^C
!
radius server host
address ipv4 172.24.128.251 auth-port 1645
key radius123
radius server 172.24.128.251
address ipv4 172.24.128.251 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
```

```
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end
```

4.switch12

```
Current configuration : 1828 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
!
```

```
interface FastEthernet0/11
switchport access vlan 20
!
interface FastEthernet0/12
switchport access vlan 20
!
interface FastEthernet0/13
switchport access vlan 20
!
interface FastEthernet0/14
switchport access vlan 20
!
interface FastEthernet0/15
switchport access vlan 20
!
interface FastEthernet0/16
switchport access vlan 20
!
interface FastEthernet0/17
switchport access vlan 30
!
interface FastEthernet0/18
switchport access vlan 30
!
interface FastEthernet0/19
switchport access vlan 30
!
interface FastEthernet0/20
switchport access vlan 30
!
interface FastEthernet0/21
switchport access vlan 30
!
interface FastEthernet0/22
switchport access vlan 30
!
interface FastEthernet0/23
switchport access vlan 30
!
interface FastEthernet0/24
switchport access vlan 30
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
line con 0
!
line vty 0 4
login
line vty 5 15
login
```

5.switch0

```
Current configuration : 1420 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
description Link to Other Switch
switchport mode trunk
!
interface Port-channel2
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/4
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
```

```
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
end
```

ДОДАТОК Б

Опис програми для моделювання компютерних мереж як мемо

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ МОДЕЛЮВАННЯ КРИТИЧНИХ СТАНІВ ВУЗЛІВ

Текст програми

804.02070743.24004-01 12 01

Листів 9

2025

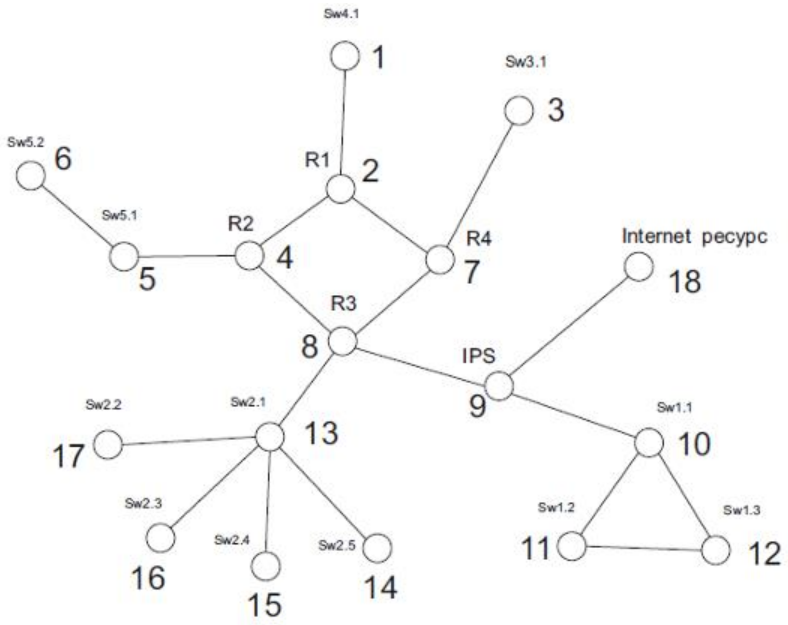
АНОТАЦІЯ

Програма призначена для моделювання та аналізу роботи корпоративної комп’ютерної мережі за різних умов навантаження, включаючи вплив шкідливого програмного забезпечення. Основна функція програми – визначення параметрів мережі, таких як інтенсивність трафіку, час обробки пакетів у вузлах, середня кількість пакетів у черзі та ймовірність виникнення затримок.

За допомогою програми здійснюється оцінка роботи вузлів мережі у «нормальному» режимі та під впливом вірусних програм, що дозволяє виявляти найбільш критичні точки перевантаження. Крім того, програма забезпечує моделювання корекції характеристик проблемних вузлів для підвищення пропускної здатності та зменшення часу обробки пакетів.

ЗМІСТ

1. Текст програми



Кількість вузлів мережі

Nn := 17

i := 0.. Nn

j := 0.. Nn

Час обробки запиту в вузлах мережі

$\tau_i :=$

3
3
3
3
3
3
3
3
3
3
3
3
3
3
3
3
3
3

$\tau =$

	0
0	3
1	3
2	3
3	3
4	3
5	3
6	3
7	3
8	3
9	3
10	3
11	3
12	3
13	3
14	3
15	3
16	3
17	3
18	

Розрахунок інтенсивності обробки запитів в вузлах мережі

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

$\mu =$

	0
0	0.333
1	0.333
2	0.333
3	0.333
4	0.333
5	0.333
6	0.333
7	0.333
8	0.333
9	0.333
10	0.333
11	0.333
12	0.333
13	0.333
14	0.333
15	0.333
16	0.333
17	0.333
18	
19	

Матриця імовірностей передачі

$$Pr := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.3 & 0 & 0 & 0.35 & 0 & 0 & 0.35 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.3 & 0 & 0 & 0.4 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.4 & 0.2 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.2 & 0 & 0 & 0.2 & 0 & 0.4 & 0 & 0 & 0 & 0.2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0.3 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0 & 0.4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 & 0.2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Перевірка правильності заповнення передаточної матриці

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

$SumPr =$

	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
12	1
13	1
14	1
15	1
16	1
17	1

Визначення коефіцієнтів передачі

$$P := Pr^{T}$$

P =

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	0	0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0.3	0	0	0.4	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0.2	0	0	0	0	0	0	0	0	0	0	0
3	0	0.35	0	0	0.5	0	0	0.2	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0.4	0	1	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0.35	1	0	0	0	0	0.2	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0.3	0	0	0.4	0	0.4	0	0	0	0.2	0	0	0	0	0
8	0	0	0	0	0	0	0	0.4	0	0.4	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0.3	0	0.6	0.6	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0.3	0	0.4	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0.3	0.4	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0.2	0	0	0	0	0	1	1	1	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0.3	0	0	0	0	0	0	0	0	0
18																		

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

$$P1 := P - D$$

P1 =

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	-1	0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	-1	0	0.3	0	0	0.4	0	0	0	0	0	0	0	0	0	0	0
2	0	0	-1	0	0	0	0.2	0	0	0	0	0	0	0	0	0	0	0
3	0	0.35	0	-1	0.5	0	0	0.2	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0.4	-1	1	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0.5	-1	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0.35	1	0	0	0	-1	0.2	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0.3	0	0	0.4	-1	0.4	0	0	0	0.2	0	0	0	0	0
8	0	0	0	0	0	0	0	0.4	-1	0.4	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0.3	-1	0.6	0.6	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0.3	-1	0.4	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0.3	0.4	-1	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0.2	0	0	0	0	-1	1	1	1	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0.2	-1	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	-1	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	0	-1	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	-1	0
17	0	0	0	0	0	0	0	0	0.3	0	0	0	0	0	0	0	0	-1

$j := 1 .. Nn$

$i := 0 .. Nn$

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

P2 =

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	0	-0.7	0	0.3	0	0	0.4	0	0	0	0	0	0	0	0	0	0	0
1	-1	0.3	-1	0	0	0	0.2	0	0	0	0	0	0	0	0	0	0	0
2	-1	0.65	0	-1	0.5	0	0	0.2	0	0	0	0	0	0	0	0	0	0
3	-1	0.3	0	0.4	-1	1	0	0	0	0	0	0	0	0	0	0	0	0
4	-1	0.3	0	0	0.5	-1	0	0	0	0	0	0	0	0	0	0	0	0
5	-1	0.65	1	0	0	0	-1	0.2	0	0	0	0	0	0	0	0	0	0
6	-1	0.3	0	0.3	0	0	0.4	-1	0.4	0	0	0	0.2	0	0	0	0	0
7	-1	0.3	0	0	0	0	0	0.4	-1	0.4	0	0	0	0	0	0	0	1
8	-1	0.3	0	0	0	0	0	0	0.3	-1	0.6	0.6	0	0	0	0	0	0
9	-1	0.3	0	0	0	0	0	0	0	0.3	-1	0.4	0	0	0	0	0	0
10	-1	0.3	0	0	0	0	0	0	0	0.3	0.4	-1	0	0	0	0	0	0
11	-1	0.3	0	0	0	0	0	0.2	0	0	0	0	-1	1	1	1	1	0
12	-1	0.3	0	0	0	0	0	0	0	0	0	0	0.2	-1	0	0	0	0
13	-1	0.3	0	0	0	0	0	0	0	0	0	0	0.2	0	-1	0	0	0
14	-1	0.3	0	0	0	0	0	0	0	0	0	0	0.2	0	0	-1	0	0
15	-1	0.3	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	-1	0
16	-1	0.3	0	0	0	0	0	0	0.3	0	0	0	0	0	0	0	0	-1
17																		

$j := 0 .. Nn - 1$

$i := 0 .. Nn - 1$

$PP2_{j,i} := P2_{j,i+1}$

PP2 =

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	-0.7	0	0.3	0	0	0.4	0	0	0	0	0	0	0	0	0	0	0	
1	0.3	-1	0	0	0	0.2	0	0	0	0	0	0	0	0	0	0	0	
2	0.65	0	-1	0.5	0	0	0.2	0	0	0	0	0	0	0	0	0	0	
3	0.3	0	0.4	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	
4	0.3	0	0	0.5	-1	0	0	0	0	0	0	0	0	0	0	0	0	
5	0.65	1	0	0	0	-1	0.2	0	0	0	0	0	0	0	0	0	0	
6	0.3	0	0.3	0	0	0.4	-1	0.4	0	0	0	0.2	0	0	0	0	0	
7	0.3	0	0	0	0	0	0.4	-1	0.4	0	0	0	0	0	0	0	1	
8	0.3	0	0	0	0	0	0	0.3	-1	0.6	0.6	0	0	0	0	0	0	
9	0.3	0	0	0	0	0	0	0	0.3	-1	0.4	0	0	0	0	0	0	
10	0.3	0	0	0	0	0	0	0	0.3	0.4	-1	0	0	0	0	0	0	
11	0.3	0	0	0	0	0	0.2	0	0	0	0	-1	1	1	1	1	0	
12	0.3	0	0	0	0	0	0	0	0	0	0	0.2	-1	0	0	0	0	
13	0.3	0	0	0	0	0	0	0	0	0	0	0.2	0	-1	0	0	0	
14	0.3	0	0	0	0	0	0	0	0	0	0	0.2	0	0	-1	0	0	
15	0.3	0	0	0	0	0	0	0	0	0	0	0.2	0	0	0	-1	0	
16	0.3	0	0	0	0	0	0	0.3	0	0	0	0	0	0	0	0	-1	

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

Q =

	0
0	0
1	-1
2	-1
3	-1
4	-1
5	-1
6	-1
7	-1
8	-1
9	-1
10	-1
11	-1
12	-1
13	-1
14	-1
15	-1
16	-1
17	

E := lsolve (PP2, Q)

E =

	0
0	-3.333
1	-0.583
2	-3.889
3	-3.111
4	-1.556
5	-2.917
6	-5.833
7	-5.833
8	-4.375
9	-2.188
10	-2.188
11	-5.833
12	-1.167
13	-1.167
14	-1.167
15	-1.167
16	-1.75

Формуємо матрицю коефіцієнтів e

$$e := \begin{pmatrix} 1 \\ 3.333 \\ 0.583 \\ 3.889 \\ 3.111 \\ 1.556 \\ 2.917 \\ 5.833 \\ 5.833 \\ 8.75 \\ 4.375 \\ 4.375 \\ 5.833 \\ 1.167 \\ 1.167 \\ 1.167 \\ 1.167 \\ 1.75 \end{pmatrix}$$

Кількість пакетів які циркулюють в мережі

$N := 5$

$i := 0..Nn$

$j := 0..N - 1$

Кількість конвеєрів в кожному вузлі

$m_i :=$

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

$m =$

	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
12	1
13	1
14	1
15	1
16	1
17	1
18	
19	

Розрахунок значень функції A

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

$A =$

	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	...	

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

X =

	0
0	3
1	9.999
2	1.749
3	11.667
4	9.333
5	4.668
6	8.751
7	17.499
8	17.499
9	26.25
10	13.125
11	...

Обчислення матриці констант T

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

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

T =

	0	1	2	3	4	5
0	1	3	9	27	81	
1	1	9.999	99.98	999.7	$9.996 \cdot 10^3$	
2	1	1.749	3.059	5.35	9.357	
3	1	11.667	136.119	$1.588 \cdot 10^3$	$1.853 \cdot 10^4$	
4	1	9.333	87.105	812.95	$7.587 \cdot 10^3$	
5	1	4.668	21.79	101.717	474.814	
6	1	8.751	76.58	670.152	$5.864 \cdot 10^3$	
7	1	17.499	306.215	$5.358 \cdot 10^3$	$9.377 \cdot 10^4$	
8	1	17.499	306.215	$5.358 \cdot 10^3$	$9.377 \cdot 10^4$	
9	1	26.25	689.063	$1.809 \cdot 10^4$	$4.748 \cdot 10^5$	
10	1	13.125	172.266	$2.261 \cdot 10^3$	$2.968 \cdot 10^4$	
11	1	13.125	172.266	$2.261 \cdot 10^3$	...	

Розраховуємо константи для другого і наступних вузлів

$i := 1..Nn$

$k := 0..N-1$

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

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

$G =$

	0	1	2	3	4	5
0	1	3	9	27	81	
1	1	12.999	138.977	$1.417 \cdot 10^3$	$1.425 \cdot 10^4$	
2	1	14.748	164.771	$1.705 \cdot 10^3$	$1.723 \cdot 10^4$	
3	1	26.415	472.955	$7.223 \cdot 10^3$	$1.015 \cdot 10^5$	
4	1	35.748	806.591	$1.475 \cdot 10^4$	$2.392 \cdot 10^5$	
5	1	40.416	995.253	$1.94 \cdot 10^4$	$3.297 \cdot 10^5$	
6	1	49.167	$1.426 \cdot 10^3$	$3.187 \cdot 10^4$	$6.086 \cdot 10^5$	
7	1	66.666	$2.592 \cdot 10^3$	$7.723 \cdot 10^4$	$1.96 \cdot 10^6$	
8	1	84.165	$4.065 \cdot 10^3$	$1.484 \cdot 10^5$	$4.556 \cdot 10^6$	
9	1	110.415	$6.963 \cdot 10^3$	$3.311 \cdot 10^5$	$1.325 \cdot 10^7$	
10	1	123.54	$8.585 \cdot 10^3$	$4.438 \cdot 10^5$	$1.907 \cdot 10^7$	
11	1	136.665	$1.038 \cdot 10^4$	$5.8 \cdot 10^5$	$2.669 \cdot 10^7$	
12	1	154.164	$1.308 \cdot 10^4$	$8.089 \cdot 10^5$	$4.084 \cdot 10^7$	
13	1	157.665	$1.363 \cdot 10^4$	$8.566 \cdot 10^5$	$4.384 \cdot 10^7$	
14	1	161.166	$1.419 \cdot 10^4$	$9.063 \cdot 10^5$	$4.701 \cdot 10^7$	
15	1	164.667	$1.477 \cdot 10^4$	$9.58 \cdot 10^5$	$5.037 \cdot 10^7$	
16	1	168.168	$1.536 \cdot 10^4$	$1.012 \cdot 10^6$	...	

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

$$B_{Nn,0} := 1 - B_{Nn,1}$$

B =

	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	0	0	0	0	
12	0	0	0	0	0	
13	0	0	0	0	0	
14	0	0	0	0	0	
15	0	0	0	0	0	
16	0	0	0	0	...	

Розрахунок допоміжних коефіцієнтів

$i := 0..Nn - 1$

$j := 1..N - 1$

$Gn_{i,0} := 1$

$$Gn_{i,j} := G_{Nn,j} - \sum_{k=1}^{j} \left(T_{i,k} \cdot Gn_{i,j-k}\right)$$

$Gn =$

	0	1	2	3	4	5
0	1	170.418	$1.575 \cdot 10^4$	$1.048 \cdot 10^6$	$5.638 \cdot 10^7$	
1	1	163.419	$1.453 \cdot 10^4$	$9.345 \cdot 10^5$	$4.87 \cdot 10^7$	
2	1	171.669	$1.596 \cdot 10^4$	$1.069 \cdot 10^6$	$5.775 \cdot 10^7$	
3	1	161.751	$1.424 \cdot 10^4$	$9.073 \cdot 10^5$	$4.687 \cdot 10^7$	
4	1	164.085	$1.465 \cdot 10^4$	$9.453 \cdot 10^5$	$4.943 \cdot 10^7$	
5	1	168.75	$1.546 \cdot 10^4$	$1.021 \cdot 10^6$	$5.455 \cdot 10^7$	
6	1	164.667	$1.475 \cdot 10^4$	$9.548 \cdot 10^5$	$5.007 \cdot 10^7$	
7	1	155.919	$1.323 \cdot 10^4$	$8.125 \cdot 10^5$	$4.047 \cdot 10^7$	
8	1	155.919	$1.323 \cdot 10^4$	$8.125 \cdot 10^5$	$4.047 \cdot 10^7$	
9	1	147.168	$1.172 \cdot 10^4$	$6.701 \cdot 10^5$	$3.087 \cdot 10^7$	
10	1	160.293	$1.399 \cdot 10^4$	$8.836 \cdot 10^5$	$4.527 \cdot 10^7$	
11	1	160.293	$1.399 \cdot 10^4$	$8.836 \cdot 10^5$	...	

$i := 0 .. Nn - 1$

$j := 0 .. N - 1$

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

$B_{11,j} := B_{10,j}$

$B =$

	0	1	2	3	4
0	0.945	0.053	$2.375 \cdot 10^{-3}$	$7.711 \cdot 10^{-5}$	$1.357 \cdot 10^{-6}$
1	0.816	0.157	0.024	$2.738 \cdot 10^{-3}$	$1.675 \cdot 10^{-4}$
2	0.968	0.031	$8.185 \cdot 10^{-4}$	$1.539 \cdot 10^{-5}$	$1.568 \cdot 10^{-7}$
3	0.785	0.177	0.032	$4.305 \cdot 10^{-3}$	$3.105 \cdot 10^{-4}$
4	0.828	0.148	0.021	$2.236 \cdot 10^{-3}$	$1.272 \cdot 10^{-4}$
5	0.914	0.08	$5.645 \cdot 10^{-3}$	$2.877 \cdot 10^{-4}$	$7.957 \cdot 10^{-6}$
6	0.839	0.14	0.019	$1.849 \cdot 10^{-3}$	$9.828 \cdot 10^{-5}$
7	0.678	0.238	0.068	0.014	$1.571 \cdot 10^{-3}$
8	0.678	0.238	0.068	0.014	$1.571 \cdot 10^{-3}$
9	0.517	0.295	0.135	0.045	$7.957 \cdot 10^{-3}$
10	0.759	0.194	0.04	$6.074 \cdot 10^{-3}$	$4.973 \cdot 10^{-4}$
11	0.759	0.194	0.04	$6.074 \cdot 10^{-3}$	$4.973 \cdot 10^{-4}$
12	0.678	0.238	0.068	0.014	$1.571 \cdot 10^{-3}$
13	0.936	0.061	$3.217 \cdot 10^{-3}$	$1.222 \cdot 10^{-4}$	$2.518 \cdot 10^{-6}$
14	0.936	0.061	$3.217 \cdot 10^{-3}$	$1.222 \cdot 10^{-4}$	$2.518 \cdot 10^{-6}$
15	0.936	0.061	$3.217 \cdot 10^{-3}$	$1.222 \cdot 10^{-4}$	$2.518 \cdot 10^{-6}$
16	0.936	0.061	$3.217 \cdot 10^{-3}$	$1.222 \cdot 10^{-4}$	...

$i := 0 .. Nn$

$j := 0 .. N - 1$

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

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
12	1
13	1
14	1
15	1
16	1
17	1.008

$$\lambda_i := e_i \cdot \frac{C_{Nn-1,N-2}}{C_{Nn,N-1}}$$

$$L_i := \sum_{n=0}^{N-1} \left(n \cdot B_{i,n}\right)$$

Результати розрахунку

Інтенсивність вхідного потоку

Середнє число пакетів в вузлах

$\lambda =$

	0
0	0.017
1	0.057
2	$9.885 \cdot 10^{-3}$
3	0.066
4	0.053
5	0.026
6	0.049
7	0.099
8	0.099
9	0.148
10	0.074
11	0.074
12	0.099
13	0.02
14	0.02
15	0.02
16	0.02
17	0.03

$L =$

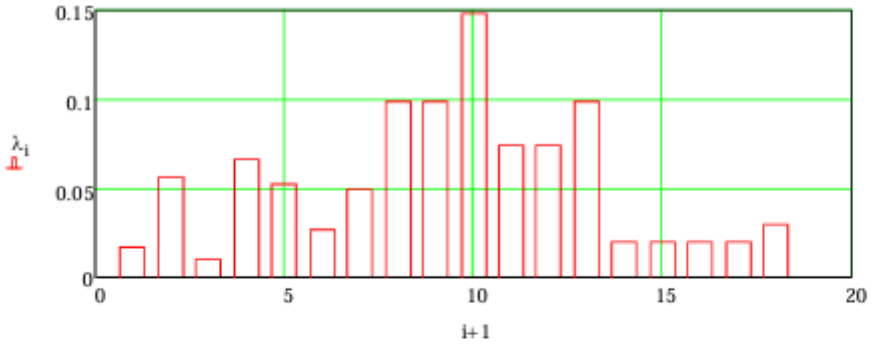
	0
0	0.058
1	0.214
2	0.033
3	0.257
4	0.198
5	0.092
6	0.184
7	0.422
8	0.422
9	0.731
10	0.295
11	0.295
12	0.422
13	0.068
14	0.068
15	0.068
16	0.068
17	0.113
18	
19	

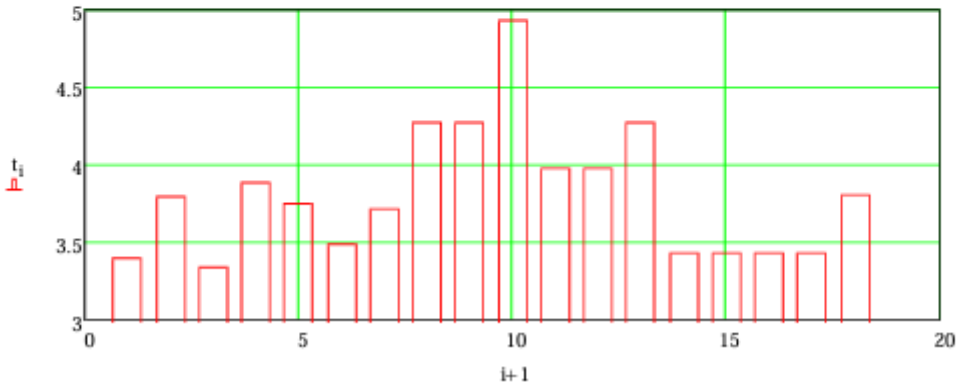
Середній час перебування пакета в вузлі

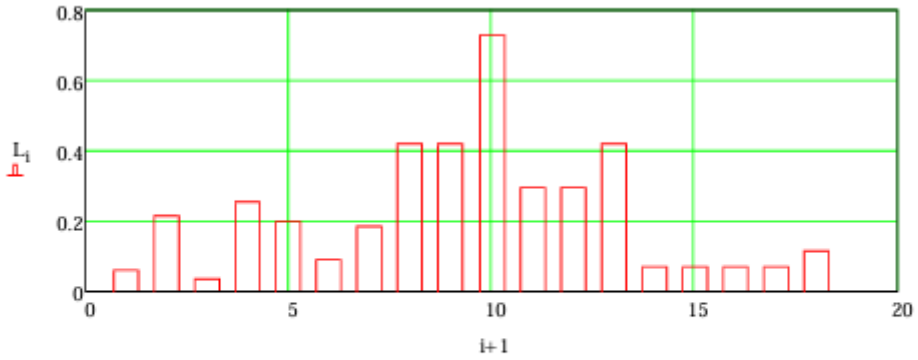
$$t_i := \frac{L_i}{\lambda_i}$$

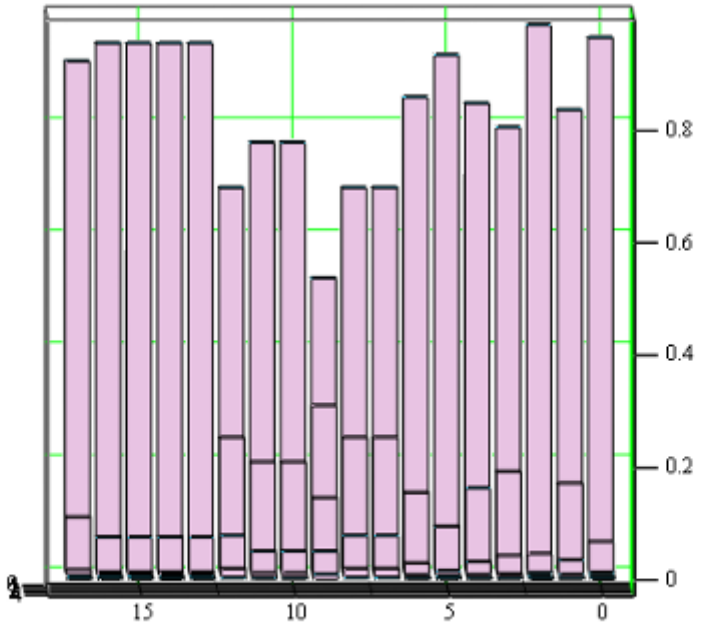
t =

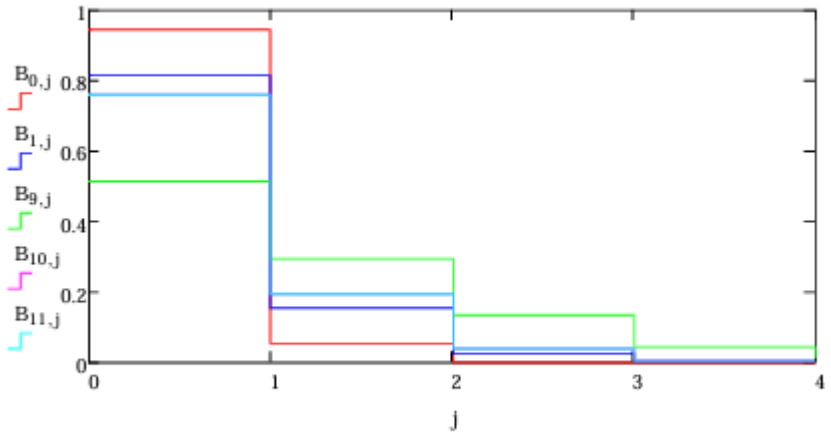
	0
0	3.403
1	3.79
2	3.339
3	3.891
4	3.751
5	3.49
6	3.717
7	4.271
8	4.271
9	4.927
10	3.982
11	3.982
12	4.271
13	3.429
14	3.429
15	...






0.8
0.6
0.4
0.2
0
L_i
0
5
10
15
20
i+1


0.8
0.6
0.4
0.2
0
15
10
5
0


1
0.8
0.6
0.4
0.2
0
$B_{0,j}$
$B_{1,j}$
$B_{9,j}$
$B_{10,j}$
$B_{11,j}$
0
1
2
3
4
j