ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти бакалавр

на тему: **«Моделювання та аналіз продуктивності корпоративної VPN-мережі на основі теорії масового обслуговування з програмною реалізацією на Python»**

Виконав: здобувач вищої освіти
за освітньою програмою
Інформаційні управляючі системи
спеціальності 126 Інформаційні
системи та технології
ступеня вищої освіти бакалавр
групи 126ІСТ_бз_2022
Гайдабура Олександр Борисович
Керівник: Поночовний Юрій
Леонідович
Рецензент: Муравльов Володимир
Вячеславович

Полтава – 2026 року

ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій
Кафедра інформаційних систем та технологій

Освітня програма Інформаційні управляючі системи
Спеціальність 126 Інформаційні системи та технології
Рівень вищої освіти перший (бакалаврський)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Юрій УТКІН
«10» квітня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Гайдабурі Олександру Борисовичу

1. Тема роботи:
«Моделювання та аналіз продуктивності корпоративної VPN-мережі на основі теорії масового обслуговування з програмною реалізацією на Python»,
керівник роботи д.т.н., професор, професор кафедри інформаційних систем та технологій Поночовний Юрій Леонідович.
Затверджено наказом закладу вищої освіти від «19» березня 2026 року № 282-ст

2. Строк подання здобувачем вищої освіти роботи 26 травня 2026 року

3. Вихідні дані до роботи: стандарти проєктування мережевої інфраструктури та розробки програмного забезпечення, технічна документація виробників обладнання https://www.cisco.com/, https://www.dlink.com/, документація бібліотек та інструментів https://simpy.readthedocs.io/, https://scipy.org/, https://matplotlib.org/, https://www.python.org/, середовища розробки Visual Studio Code, інтерпретатор Python 3.10+.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

Розділ 1. Теоретичні основи побудови корпоративних VPN-мереж
Розділ 2. Проектування корпоративної VPN-мережі
Розділ 3. Програмна реалізація Python моделі та аналіз продуктивності мережі

5. Перелік графічного матеріалу: схеми, рисунки, графіки, діаграми за темою та об’єктом дослідження.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання отримав
Розрахунок економічної ефективності результатів дослідження	Шкурупій О. В., д. е. н., професор, професор кафедри економіки та публічного управління	24.03.2026 р.	09.04.2026 р.

7. Дата видачі завдання «10» квітня 2025 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	Вибір і затвердження теми роботи	01.04.2025 р.	
2	Складання і затвердження розгорнутого плану та завдання на кваліфікаційну роботу	02.04.2025 р. – 10.04.2025 р.	
3	Опрацювання джерел інформації	03.06.2025 р. – 15.06.2025 р.	
4	Збір, вивчення і обробка інформації, необхідної для виконання роботи	16.06.2025 р. – 04.07.2025 р.	
5	Виконання теоретико-методологічного розділу роботи	08.09.2025 р. – 15.11.2025 р.	
6	Виконання дослідницько-аналітичного розділу роботи	16.11.2025 р. – 30.01.2026 р.	
7	Виконання проєктно-рекомендаційного розділу роботи	01.02.2026 р. – 21.03.2026 р.	
8	Розрахунок економічної ефективності результатів дослідження	24.03.2026 р. – 09.04.2026 р.	
9	Оформлення тексту роботи	10.04.2026 р. – 25.05.2026 р.	
10	Попередній захист роботи на кафедрі	26.05.2026 р.	
11	Доопрацювання роботи з урахуванням зауважень і пропозицій	27.05.2026 р. - 28.05.2026 р.	
12	Нормоконтроль	29.05.2026 р.	
13	Захист кваліфікаційної роботи	03.06.2026 р.	

Здобувач вищої освіти **Олександр ГАЙДАБУРА**

Керівник роботи **Юрій ПОНОЧОВНИЙ**

ЗМІСТ

ВСТУП

Актуальність. У сучасному корпоративному середовищі надійна та захищена передача даних між географічно розподіленими підрозділами є одним із ключових чинників ефективної діяльності організацій. Зростання кількості віддалених працівників, розширення філіальних мереж та перехід до хмарних сервісів суттєво підвищують вимоги до мережевої інфраструктури підприємств. За даними аналітичних досліджень [1, 4], глобальний ринок VPN-рішень для корпоративного сектору щорічно зростає на 15-20 %, що свідчить про стабільний попит на технології захищеної передачі даних. В Україні, в умовах активної цифровізації бізнесу та переходу підприємств на дистанційні форми роботи, питання організації корпоративних мереж набуває особливої практичної значущості.

Технологія віртуальних приватних мереж (VPN) є одним із найбільш поширених і економічно обґрунтованих рішень для побудови захищених каналів зв'язку між офісами компанії. Вона дозволяє організувати захищений тунель поверх публічної мережі Інтернет без необхідності оренди виділених фізичних каналів, що суттєво знижує витрати на телекомунікаційну інфраструктуру [2, 9]. Водночас проектування VPN-мережі вимагає коректного розрахунку навантаження та оцінки характеристик якості обслуговування, оскільки недостатня пропускна здатність або неправильно обране обладнання призводять до деградації сервісів – насамперед IP-телефонії та відеоконференцій.

Для кількісної оцінки продуктивності мережі широко застосовується теорія масового обслуговування (ТМО), що дозволяє аналітично розрахувати затримку пакетів, довжину черги та ймовірність втрат без проведення дорогих натурних експериментів [12, 13]. Поєднання аналітичних моделей ТМО з імітаційним моделюванням засобами мови Python утворює потужний та доступний інструментарій для дослідження мережевої продуктивності, придатний як для наукових досліджень, так і для практичного проектування корпоративних мереж [18, 20].

Метою кваліфікаційної роботи є моделювання та аналіз продуктивності корпоративної VPN-мережі на основі теорії масового обслуговування з програмною реалізацією на Python, а також техніко-економічне обґрунтування ефективності розробленого рішення.

Відповідно до мети роботи необхідно вирішити наступні *завдання:*

1. Провести аналіз архітектури та протоколів сучасних VPN-мереж, методів криптографічного захисту, математичного апарату теорії масового обслуговування та існуючих програмних засобів моделювання мережевої продуктивності;

2. Спроектувати корпоративну VPN-мережу: визначити вимоги до інфраструктури, обґрунтувати вибір топології, протоколів та обладнання, виконати розрахунок навантаження і налаштування мережевих вузлів;

3. Розробити програмний модуль моделювання на Python, виконати аналіз характеристик якості обслуговування на основі моделей M/M/1 та M/M/1/K, а також провести техніко-економічне обґрунтування ефективності розробленої системи.

Об'єкт дослідження – процеси передачі та обслуговування мережевого трафіку в корпоративній VPN-мережі з захищеними тунелями на основі протоколів IPsec та DMVPN.

Предмет дослідження – моделювання та аналіз продуктивності корпоративної VPN-мережі засобами теорії масового обслуговування з програмною реалізацією на Python.

Методи досліджень – робота базується на методах теорії масового обслуговування (аналітичні моделі M/M/1 та M/M/1/K), імітаційного моделювання з дискретними подіями (бібліотека SimPy), аналізу чутливості, мережевого проектування (розрахунок навантаження, вибір обладнання та протоколів), а також техніко-економічного аналізу (NPV, ROI, дисконтований термін окупності).

Інформаційна база – наукові статті та монографії з теорії масового обслуговування і телекомунікаційних мереж, технічна документація виробників

мережевого обладнання (Cisco Systems, D-Link), стандарти інформаційної безпеки (ДСТУ ISO/IEC 27001:2023), рекомендації ITU-T щодо якості сервісів IP-телефонії, документація бібліотек Python (SimPy, NumPy, SciPy, Matplotlib), а також інтернет-ресурси з мережевих технологій та VPN-рішень.

Практична значущість – розроблений програмний комплекс моделювання дозволяє кількісно оцінити продуктивність корпоративної VPN-мережі до її фізичного розгортання, визначити оптимальну пропускну здатність каналу та перевірити відповідність QoS-вимогам для різних сценаріїв навантаження. Запропонована методика проектування мережі на базі DMVPN/IPsec із верифікацією засобами ТМО може бути застосована для інших організацій з розподіленою структурою, а модульна архітектура програмного комплексу спрощує його адаптацію до нових вхідних умов без зміни програмного коду.

Результати роботи апробовані в рамках наукової конференції здобувачів вищої освіти за результатами науково-дослідної роботи у 2025-2026 рр.

Структура кваліфікаційної роботи логічно пов’язана з задачами досліджень і містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел. Загальний обсяг текстової частини кваліфікаційної роботи складає 53 сторінки формату А4. Вона містить 13 рисунків і 14 таблиць.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ VPN-МЕРЕЖ

1.1 Архітектура та протоколи сучасних VPN-мереж

Корпоративні мережі передачі даних є критичною інфраструктурою сучасного підприємства. Зі зростанням кількості віддалених працівників, розподілених офісів та хмарних сервісів питання безпечного та ефективного з'єднання мережевих вузлів набуває першочергового значення. Технологія віртуальних приватних мереж (VPN, від англ. Virtual Private Network) є одним із найбільш поширених рішень для організації захищених каналів зв'язку поверх публічних мереж, зокрема мережі Інтернет [1]. VPN-мережа являє собою логічну мережу, що створюється поверх фізичної інфраструктури загального користування. На рисунку 1.1 наведено узагальнену схему архітектури корпоративної VPN-мережі.

Рисунок 1.1 – Архітектура корпоративної VPN-мережі

Ключова ідея технології полягає в побудові так званого «тунелю» – зашифрованого каналу між двома або більше вузлами, по якому передаються інкапсульовані пакети даних. Завдяки цьому зловмисник, перехопивши трафік у публічному середовищі, не може ні прочитати його вміст, ні однозначно

встановити кінцеві точки з'єднання [2]. Архітектуру VPN-мережі визначають три основні компоненти: тунельний протокол, механізм шифрування та система автентифікації. Залежно від комбінації цих складових формуються різні рішення, кожне з яких має власну область застосування (табл. 1.1).

Таблиця 1.1 – Порівняльна характеристика основних VPN-протоколів

Протокол	Рівень OSI	Шифрування	Швидкість	Типове застосування
IPsec (тунельний)	3 (мережевий)	AES-256, 3DES	Висока	Міжмережеве з'єднання
L2TP/IPsec	2+3	AES-256	Середня	Віддалений доступ
OpenVPN	4 (транспортний)	AES-256-GCM	Середня	Крос-платформні рішення
WireGuard	3 (мережевий)	ChaCha20	Дуже висока	Сучасні корпоративні мережі

Серед протоколів тунелювання найбільш поширеними у корпоративному середовищі є IPsec, OpenVPN, WireGuard та L2TP/IPsec. Протокол IPsec (IP Security) працює на мережевому рівні моделі OSI і забезпечує автентифікацію та шифрування кожного IP-пакета. Він підтримує два режими роботи: транспортний, у якому шифрується лише корисне навантаження пакета, та тунельний, у якому шифрується весь пакет разом із заголовком. Для корпоративних рішень, де необхідно приховати топологію внутрішньої мережі, використовується переважно тунельний режим [3].

Протокол L2TP (Layer 2 Tunneling Protocol) сам по собі не забезпечує шифрування і тому практично завжди застосовується у зв'язці з IPsec. Така комбінація дозволяє передавати кадри канального рівня через тунель із повноцінним криптографічним захистом. OpenVPN є програмним рішенням із відкритим кодом, що базується на бібліотеці OpenSSL і підтримує протоколи TLS/SSL. Завдяки гнучкості налаштування та підтримці широкого спектра платформ OpenVPN залишається популярним вибором для організацій, що потребують кросплатформних рішень [4].

Відносно новим, але технологічно прогресивним рішенням є протокол WireGuard, розроблений у 2016 році та включений до ядра Linux починаючи з

версії 5.6. Порівняно з IPsec і OpenVPN він має суттєво меншу кодову базу (близько 4000 рядків коду проти десятків тисяч у конкурентів), що спрощує аудит безпеки та знижує імовірність вразливостей. Продуктивність WireGuard за результатами незалежних досліджень у середньому на 20-50% вища, ніж у OpenVPN [5].

Вибір протоколу безпосередньо впливає на показники продуктивності мережі: затримку (latency), пропускну здатність (throughput) та джиттер. Наприклад, накладні витрати на інкапсуляцію та шифрування пакета можна охарактеризувати через коефіцієнт корисного навантаження:

$$\eta = \frac{L_{payload}}{L_{payload} + L_{header} + L_{crypto}}, \tag{1.1}$$

де $L_{payload}$ – розмір корисних даних,

L_{header} – розмір заголовків тунельного протоколу,

L_{crypto} – додатковий обсяг, що вноситься механізмом шифрування та автентифікації [6].

Окремої уваги заслуговує архітектура DMVPN (Dynamic Multipoint VPN), розроблена компанією Cisco. Вона поєднує технології mGRE (Multipoint Generic Routing Encapsulation) та NHRP (Next Hop Resolution Protocol), що дозволяє динамічно встановлювати тунелі між вузлами-клієнтами без необхідності заздалегідь конфігурувати кожен з'єднувальний маршрут. Один центральний маршрутизатор (hub) виступає сервером NHRP і зберігає актуальні зовнішні IP-адреси всіх клієнтських вузлів (spoke). Така схема є масштабованою та добре підходить для корпоративних мереж із великою кількістю філій [7].

Таким чином, сучасний ринок пропонує широкий спектр архітектурних рішень і протоколів для побудови корпоративних VPN-мереж. Вибір конкретного підходу визначається вимогами до безпеки, продуктивності, масштабованості та бюджету проекту. Для коректного проектування та подальшого моделювання системи необхідно також розглянути математичний апарат оцінки навантаження на мережу.

1.2 Огляд методів забезпечення безпеки та шифрування в корпоративних мережах

Забезпечення інформаційної безпеки в корпоративних мережах є комплексним завданням, що охоплює захист даних як у стані зберігання, так і під час передачі. У контексті VPN-технологій ключову роль відіграють криптографічні механізми, протоколи автентифікації та системи контролю доступу. Нормативною основою для побудови таких систем в Україні слугує стандарт ДСТУ ISO/IEC 27001:2023, який визначає вимоги до систем керування інформаційною безпекою [8].

Криптографічний захист у VPN реалізується на двох рівнях. Перший – шифрування каналу передачі даних, що унеможливлює перехоплення та читання трафіку третіми особами. Другий – автентифікація вузлів, яка гарантує, що до мережі підключаються лише авторизовані учасники. Поєднання цих двох механізмів забезпечує конфіденційність, цілісність та доступність інформації – три фундаментальні властивості, що складають модель CIA (Confidentiality, Integrity, Availability) [9].

Сучасні VPN-рішення використовують симетричні та асиметричні алгоритми шифрування у комбінації. Асиметрична криптографія (зокрема RSA або ECDH – Elliptic-Curve Diffie-Hellman) застосовується на етапі встановлення з'єднання для безпечного обміну сеансовими ключами. Після узгодження ключів подальша передача даних здійснюється із застосуванням значно швидших симетричних алгоритмів – AES-256-GCM або ChaCha20-Poly1305. Такий гібридний підхід оптимально поєднує криптографічну стійкість з продуктивністю [10].

Центральне місце в архітектурі захисту VPN займає протокол IPsec, який включає три ключові компоненти. Протокол AH (Authentication Header) забезпечує цілісність та автентифікацію пакета, але не шифрує корисне

навантаження. Протокол ESP (Encapsulating Security Payload) реалізує як автентифікацію, так і шифрування. Протокол IKE (Internet Key Exchange), на сьогодні у версії IKEv2, відповідає за автоматичне узгодження параметрів захищеної асоціації SA (Security Association) між двома вузлами. На рис. 1.2 наведено структуру взаємодії компонентів IPsec.

Рисунок 1.2 – Структура протоколів IPsec

Процес встановлення захищеного з'єднання IKEv2 відбувається у два етапи. На першому (IKE_SA_INIT) вузли домовляються про криптографічні алгоритми та виконують обмін ключами за протоколом Діффі-Геллмана. На другому (IKE_AUTH) виконується взаємна автентифікація сторін та формуються дочірні SA для захисту трафіку ESP. Завдяки механізму MOBIKE протокол IKEv2 підтримує зміну IP-адреси без розривання сесії, що є важливим для мобільних користувачів [9].

Окремої уваги заслуговує роль брандмауерів (firewall) у загальній архітектурі безпеки. Міжмережевий екран контролює весь вхідний та вихідний трафік на основі наперед визначених правил і є першою лінією захисту периметра мережі. У сучасних рішеннях застосовуються міжмережеві екрани наступного покоління (NGFW – Next-Generation Firewall), що поєднують

традиційну фільтрацію пакетів із глибокою інспекцією трафіку (DPI), аналізом на рівні застосунків та системами виявлення вторгнень (IDS/IPS) [11].

Таблиця 1.2 – Порівняння алгоритмів шифрування у VPN

Алгоритм	Тип	Довжина ключа, біт	Відносна швидкість	Рівень стійкості
AES-128-GCM	Симетричний	128	Дуже висока	Достатній
AES-256-GCM	Симетричний	256	Висока	Рекомендований
ChaCha20-Poly1305	Симетричний	256	Висока	Рекомендований
RSA-2048	Асиметричний	2048	Низька	Достатній
ECDH P-256	Асиметричний	256	Середня	Рекомендований

Важливим аспектом безпеки є також управління сертифікатами та інфраструктура відкритих ключів PKI (Public Key Infrastructure). У корпоративному середовищі автентифікація вузлів VPN зазвичай виконується за допомогою цифрових сертифікатів X.509, виданих внутрішнім або довіреним зовнішнім центром сертифікації (CA). Такий підхід є значно надійнішим порівняно з автентифікацією на основі спільного секрету (pre-shared key), оскільки компрометація одного сертифіката не ставить під загрозу безпеку всієї мережі [8].

Ефективність криптографічного захисту також залежить від правильного налаштування параметрів алгоритмів. Зокрема, критично важливим є вибір достатньої довжини криптографічного ключа. Відповідно до рекомендацій NIST, мінімально допустима стійкість симетричного ключа у сучасних системах має відповідати еквіваленту не менше 128 біт. Стійкість алгоритму RSA з довжиною ключа n біт приблизно відповідає стійкості симетричного ключа довжиною s біт, що визначається за наближеною формулою:

$$s \approx \frac{1.923 \cdot (\ln n)^{1/3} \cdot (\ln \ln n)^{2/3} - 4.69}{\ln 2}, \tag{1.2}$$

де n – довжина ключа RSA у бітах,

s – еквівалентна стійкість у бітах симетричного шифру [10].

Таким чином, сучасна система захисту корпоративної VPN-мережі є багаторівневою і включає шифрування трафіку, взаємну автентифікацію вузлів, управління ключами та міжмережеве екранування. Розуміння принципів роботи цих механізмів є необхідною умовою як для коректного проектування мережі, так і для побудови адекватної моделі її продуктивності, що розглядається у наступних підрозділах.

1.3 Теорія масового обслуговування як інструмент аналізу мережевого трафіку

Проектування корпоративної VPN-мережі вимагає не лише вибору відповідних протоколів та обладнання, а й кількісної оцінки її продуктивності. Одним із найбільш обґрунтованих математичних інструментів для вирішення цього завдання є теорія масового обслуговування (ТМО), що вивчає системи, у яких заявки (пакети даних) надходять у деякий обслуговуючий пристрій (маршрутизатор, комутатор, VPN-шлюз) і очікують на обробку у черзі [12]. Застосування ТМО дозволяє аналітично оцінити такі ключові показники якості обслуговування, як середній час затримки пакета, довжина черги та ймовірність втрати даних – без проведення дорогих натурних експериментів.

Базовою моделлю у ТМО є система Кендалла, яка позначається у вигляді $A/B/c/K$, де A – закон розподілу інтервалів між надходженнями заявок, B – закон розподілу часу обслуговування, c – кількість обслуговуючих пристроїв, K – місткість черги. Для моделювання мережевого трафіку найчастіше використовується модель M/M/1, у якій потік пакетів є пуасонівським (показниковий розподіл між надходженнями), час обслуговування підпорядковується показниковому закону, а черга необмежена [13]. Незважаючи на певні спрощення, ця модель дає достатньо

точні результати для аналізу завантаженості мережевих вузлів за умов відносно рівномірного трафіку.

Ключовим параметром моделі M/M/1 є інтенсивність навантаження ρ, що визначає ступінь використання обслуговуючого пристрою:

$$\rho = \frac{\lambda}{\mu} \tag{1.3}$$

де λ – інтенсивність надходження пакетів (пакетів/с),

μ – інтенсивність обслуговування (пакетів/с).

Система є стійкою лише за умови $\rho < 1$, тобто коли пристрій встигає обробляти пакети швидше, ніж вони надходять [12]. При наближенні ρ до одиниці довжина черги та затримка різко зростають, що на практиці відповідає перевантаженню каналу або маршрутизатора.

Для практичного аналізу VPN-мережі особливий інтерес становить середній час перебування пакета в системі W (сума часу очікування в черзі та часу обслуговування), що визначається за формулою Літтла. Графічну залежність середньої довжини черги від інтенсивності навантаження для моделі M/M/1 наведено на рисунку 1.3.

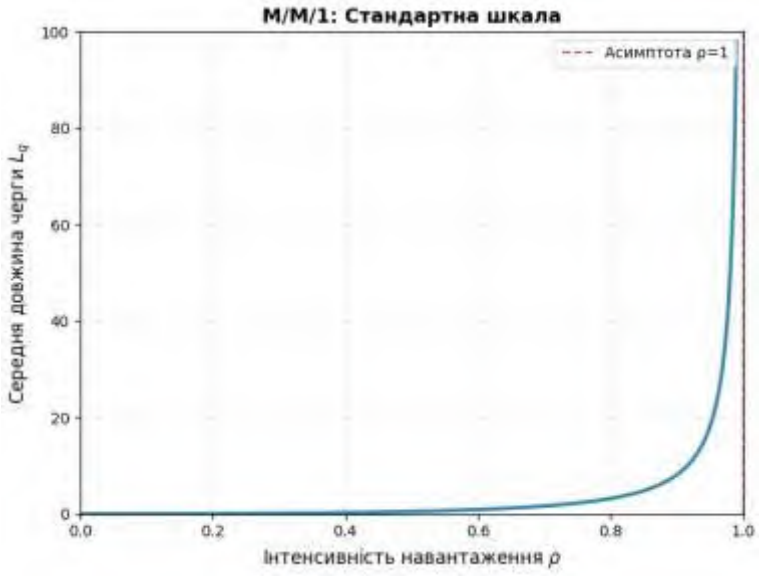

Рисунок 1.3 – Залежність середньої довжини черги від інтенсивності навантаження для моделі M/M/1

Модель M/M/1 є найпростішим, але не єдиним інструментом ТМО для аналізу мереж. У реальних корпоративних VPN-мережах трафік, як правило, є неоднорідним: відеоконференції, передача файлів, робота з корпоративними базами даних та IP-телефонія генерують потоки з різними характеристиками інтенсивності та розміру пакетів. Для таких сценаріїв застосовуються більш складні моделі: M/G/1 (з довільним розподілом часу обслуговування), M/D/1 (з детермінованим часом обслуговування, що відповідає потокам з фіксованим розміром пакетів) та моделі з пріоритетним обслуговуванням [14].

Важливим розширенням базової моделі є система M/M/1/K з обмеженою місткістю черги K. Вона краще відображає реальну поведінку мережевих буферів, оскільки маршрутизатори мають скінченний обсяг пам'яті. У цій моделі пакети, що надходять до повного буфера, відкидаються, що призводить до ненульової ймовірності втрати P_{loss}. Таблиця 1.3 ілюструє вплив місткості черги на ймовірність втрати пакетів за різних значень навантаження.

Таблиця 1.3 – Ймовірність втрати пакетів у системі M/M/1/K залежно від навантаження та місткості черги

Місткість черги K	ρ = 0.5	ρ = 0.7	ρ = 0.85	ρ = 0.95
5	0.016	0.050	0.098	0.167
10	0.001	0.007	0.028	0.087
20	< 0.001	< 0.001	0.003	0.024
50	< 0.001	< 0.001	< 0.001	0.001

Аналіз даних таблиці 1.3 показує, що навіть при відносно помірному навантаженні $\rho = 0.85$ і малій місткості буфера $K = 5$ ймовірність втрати пакетів досягає майже 10%, що є неприйнятним для більшості корпоративних застосунків. Збільшення місткості черги до 20 знижує цей показник до менш ніж 0.3%. Це безпосередньо впливає на вимоги до апаратного забезпечення мережевих вузлів.

Для VPN-мереж ТМО дозволяє також враховувати накладні витрати шифрування. Кожен пакет, що проходить через VPN-шлюз, потребує додаткового часу на криптографічну обробку, що збільшує ефективний час

обслуговування $1/\mu$ і, відповідно, знижує пропускну здатність вузла. Середнє значення часу обслуговування пакета з урахуванням шифрування визначається як:

$$\frac{1}{\mu_{eff}} = \frac{L_{pkt}}{C} + t_{crypto}, \tag{1.4}$$

де L_{pkt} – середній розмір пакета у бітах,

C – пропускна здатність каналу у бітах за секунду,

t_{crypto} – середній час криптографічної обробки одного пакета на VPN-шлюзі [15].

Саме цей параметр є одним із ключових при порівнянні продуктивності різних VPN-протоколів у межах однієї апаратної платформи.

Застосування ТМО у поєднанні з програмним моделюванням на Python дозволяє будувати аналітичні та імітаційні моделі VPN-мереж, варіювати параметри навантаження та досліджувати поведінку системи в умовах пікового трафіку. Такий підхід є значно економічнішим порівняно з розгортанням фізичного стенду та забезпечує відтворюваність результатів. Огляд конкретних програмних засобів, що реалізують методи ТМО для аналізу мереж, наведено у наступному підрозділі.

1.4 Аналіз існуючих програмних засобів моделювання мережевої продуктивності

Практичне застосування теорії масового обслуговування для аналізу корпоративних VPN-мереж нерозривно пов'язане з використанням програмних інструментів моделювання. Сучасний ринок пропонує широкий спектр таких засобів – від спеціалізованих комерційних пакетів до бібліотек із відкритим кодом. Вибір інструменту визначається вимогами до точності моделі,

доступністю, можливістю інтеграції з іншими системами та рівнем кваліфікації дослідника [16].

Серед спеціалізованих мережевих симуляторів найбільш поширеними є NS-3 (Network Simulator 3) та GNS3. NS-3 є симулятором з дискретними подіями, що розробляється з відкритим кодом і широко застосовується в академічних дослідженнях. Він підтримує моделювання протоколів канального, мережевого та транспортного рівнів, включаючи реалістичні моделі трафіку та черг. GNS3, натомість, орієнтований на емуляцію реального мережевого обладнання – він дозволяє запускати образи операційних систем Cisco IOS, Juniper та інших виробників у віртуальному середовищі, що робить його незамінним для тестування конфігурацій перед розгортанням у продуктивному середовищі [17]. Проте обидва інструменти мають суттєвий недолік з точки зору аналітичного моделювання: вони не надають вбудованих засобів для розрахунку характеристик ТМО та потребують значних обчислювальних ресурсів.

Альтернативою є використання мов програмування загального призначення з відповідними бібліотеками. Особливе місце серед них займає Python, що завдяки екосистемі наукових бібліотек став де-факто стандартом для інженерних та наукових розрахунків. Для задач моделювання мереж на основі ТМО найбільш актуальними є бібліотеки SimPy, NumPy, SciPy та Matplotlib [18]. SimPy реалізує імітаційне моделювання з дискретними подіями безпосередньо у середовищі Python, дозволяючи описувати процеси надходження та обслуговування заявок у природному для мови об'єктно-орієнтованому стилі. NumPy та SciPy забезпечують ефективні чисельні розрахунки аналітичних характеристик моделей ТМО, а Matplotlib використовується для візуалізації результатів.

Окремої уваги заслуговує середовище MATLAB із пакетом розширення Communications Toolbox. Воно надає потужні засоби для аналітичного та імітаційного моделювання телекомунікаційних систем, включаючи вбудовані функції для розрахунку характеристик систем масового обслуговування. Однак висока вартість ліцензії робить MATLAB малодоступним для більшості

організацій, що є суттєвим обмеженням у порівнянні з безкоштовними альтернативами [19]. На рисунку 1.4 наведено порівняльну схему програмних засобів моделювання мережевої продуктивності за ключовими критеріями.

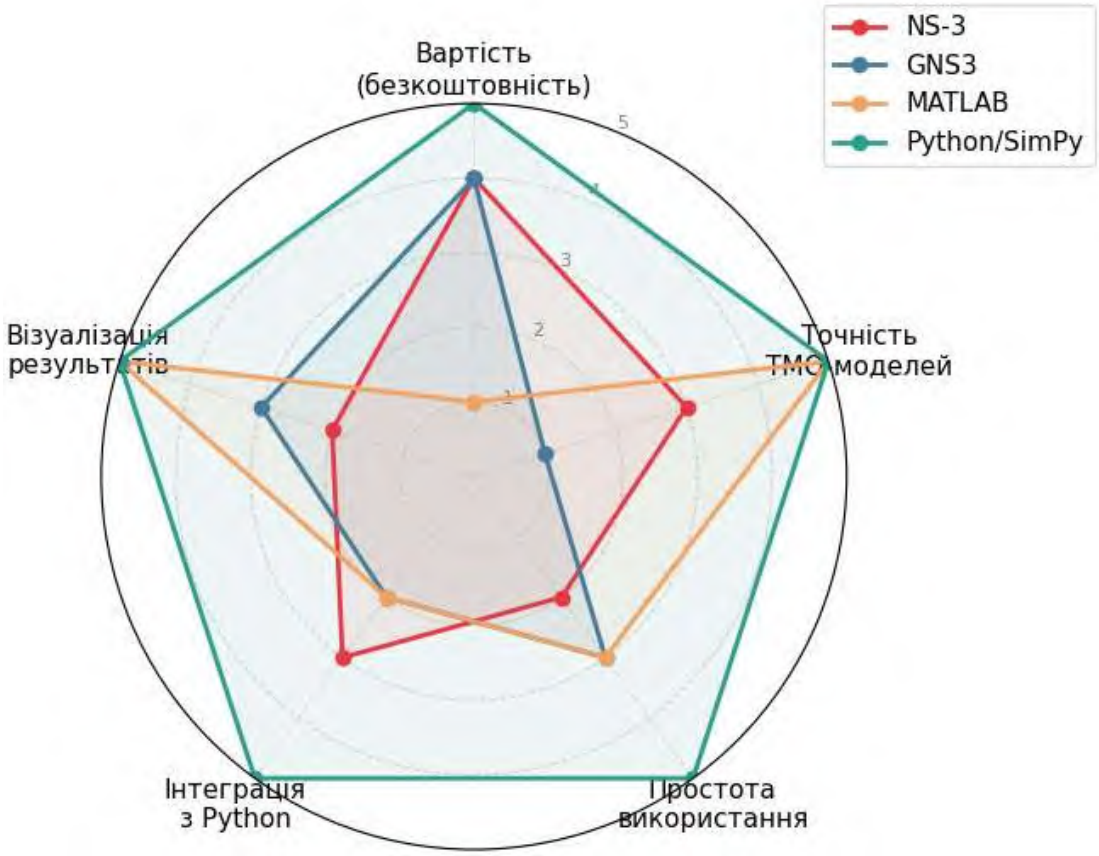

Рисунок 1.4 – Порівняння програмних засобів моделювання мережевої продуктивності

Таблиця 1.4 – Порівняльна характеристика програмних засобів моделювання мереж

Засіб	Тип	Ліцензія	Підтримка ТМО	Складність освоєння	Візуалізація
NS-3	Симулятор подій	Відкрита	Часткова	Висока	Обмежена
GNS3	Емулятор обладнання	Відкрита	Відсутня	Середня	Вбудована
MATLAB	Аналітичне середовище	Комерційна	Повна	Середня	Розвинена
Python + SimPy	Мова + бібліотека	Відкрита	Повна	Низька	Розвинена
Python + SciPy	Мова + бібліотека	Відкрита	Повна	Низька	Розвинена

З огляду на дані таблиці 1.4, комбінація Python із бібліотеками SimPy та SciPy є оптимальним вибором для реалізації моделі продуктивності корпоративної VPN-мережі. Ця комбінація є безкоштовною, добре задокументованою, підтримує як аналітичне, так і імітаційне моделювання систем масового обслуговування та дозволяє реалізовувати повний цикл дослідження – від введення параметрів до інтерпретації та візуалізації результатів.

Продуктивність програмної реалізації моделі безпосередньо залежить від кількості модельованих подій. Середній час виконання імітації T_{sim} для моделі M/M/1 у середовищі SimPy зростає лінійно з кількістю оброблених пакетів N:

$$T_{sim} = \alpha \cdot N + \beta, \tag{1.5}$$

де α – час обробки однієї події симулятором (залежить від апаратного забезпечення),

β – постійна складова, пов'язана з ініціалізацією моделі [18].

Для типових досліджень, де N становить від 10^5 до 10^6 пакетів, час виконання на сучасному персональному комп'ютері не перевищує кількох хвилин, що робить такий підхід цілком практичним.

Важливим аспектом є також відтворюваність результатів імітаційного моделювання. Оскільки процеси надходження та обслуговування у моделях ТМО є стохастичними, для отримання статистично значущих оцінок необхідно виконувати багаторазові незалежні запуски та усереднювати результати. У бібліотеці SimPy це реалізується через фіксацію початкового стану генератора псевдовипадкових чисел, що гарантує можливість точного відтворення будь-якого експерименту [18]. Можливість верифікації та повторення розрахунків є важливою вимогою до наукових досліджень і суттєвою перевагою програмного підходу над натурним експериментом [20].

Таким чином, було розглянуто теоретичні основи побудови корпоративних VPN-мереж: проаналізовано архітектуру та сучасні протоколи

тунелювання (IPsec, L2TP, WireGuard, DMVPN), досліджено методи криптографічного захисту та автентифікації, що відповідають вимогам стандарту ДСТУ ISO/IEC 27001:2023, викладено математичний апарат теорії масового обслуговування стосовно аналізу мережевого трафіку, а також виконано порівняльний огляд програмних засобів моделювання. Встановлено, що комбінація аналітичних моделей ТМО (зокрема M/M/1 та M/M/1/K) із програмною реалізацією на Python із використанням бібліотек SimPy та SciPy є методологічно обґрунтованим і практично доцільним підходом для дослідження продуктивності корпоративної VPN-мережі.

РОЗДІЛ 2
ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ VPN-МЕРЕЖІ

2.1 Характеристика об'єкта проектування та вимоги до мережевої інфраструктури

Об'єктом проектування у цій роботі є корпоративна VPN-мережа інтернет-провайдера середнього масштабу, що має два географічно розподілені офіси та надає послуги доступу до мережі Інтернет, IP-телефонії та передачі даних юридичним особам. Подібна структура є типовою для регіональних телекомунікаційних компаній, що активно розвиваються та потребують надійного захищеного з'єднання між своїми підрозділами для забезпечення централізованого управління мережею, біллінговою системою та технічною підтримкою клієнтів [21].

Головний офіс розташований у центральному вузлі мережі та виконує роль hub-маршрутизатора у топології DMVPN. Тут зосереджені основні серверні потужності, включаючи сервер біллінгової системи, поштовий сервер та сервер управління мережею. Другий офіс є віддаленим підрозділом, де розміщені комерційний відділ та частина технічного персоналу. Загальна кількість співробітників, що використовують корпоративну мережу, становить 29 осіб, розподілених між двома локаціями згідно зі штатним розписом, наведеним у таблиці 2.1.

Таблиця 2.1 – Розподіл персоналу за підрозділами та локаціями

Посада	Кількість, осіб	Локація
Технічний директор	1	Головний офіс
IT-інженер	2	Головний офіс
VoIP-інженер	1	Головний офіс
Радіоінженер	1	Головний офіс
Начальник лінійного відділу	1	Головний офіс
Монтажники	15	Головний офіс
Комерційний директор	1	Віддалений офіс
Менеджери з продажу	7	Віддалений офіс
Бухгалтери	4	Віддалений офіс

Аналіз діяльності компанії дозволяє сформулювати конкретні функціональні вимоги до мережевої інфраструктури. По-перше, необхідне постійне захищене з'єднання між двома офісами для забезпечення доступу до централізованої біллінгової системи LanBilling, яка зберігається на сервері в головному офісі. По-друге, мережа повинна підтримувати відеоконференції між підрозділами, корпоративну IP-телефонію та захищений доступ технічного персоналу до мережевого обладнання через протокол SSH. По-третє, адміністратори повинні мати можливість підключатися до корпоративної мережі дистанційно, з будь-якого місця, де є доступ до Інтернету [22].

З точки зору нефункціональних вимог першочерговими є надійність і безпека. Доступність VPN-каналу між офісами має становити не менше 99,5% робочого часу. Затримка передачі пакетів у тунелі не повинна перевищувати 50 мс для забезпечення прийнятної якості IP-телефонії відповідно до рекомендацій ITU-T G.114 [23]. Вимоги до пропускної здатності каналу між офісами формуються виходячи із сукупного навантаження, що генерується всіма категоріями користувачів одночасно. Логічну схему організації мережі наведено на рисунку 2.1.

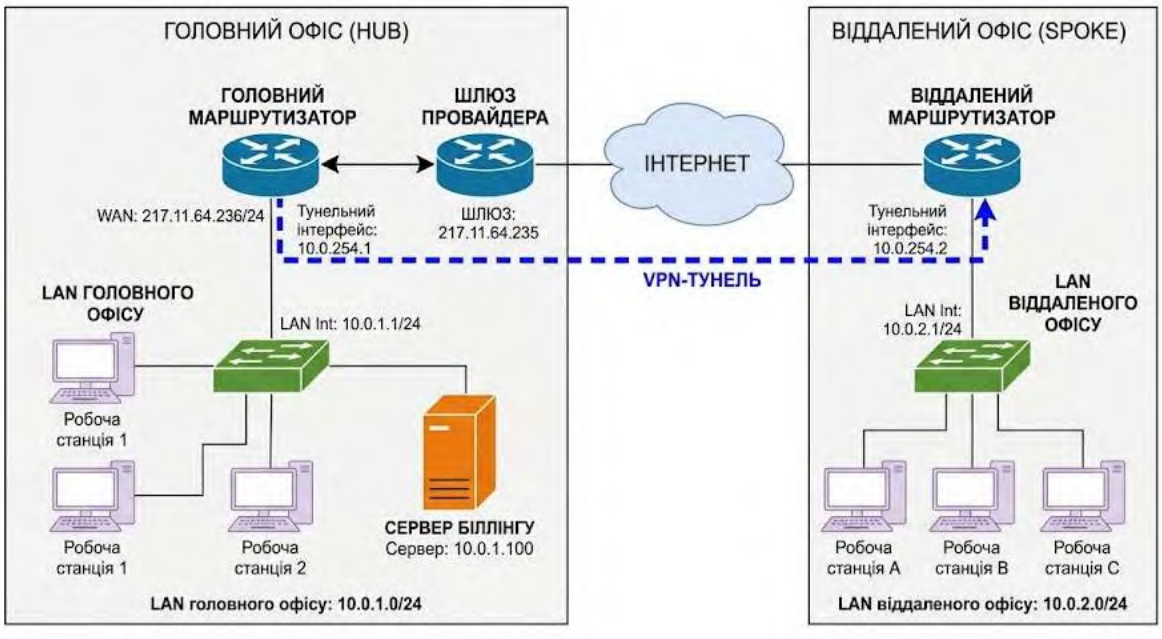

Рисунок 2.1 – Логічна схема організації корпоративної мережі

Мережева інфраструктура кожного офісу організована за дворівневою ієрархічною моделлю. На рівні доступу розташовані некерований або керований комутатор другого рівня OSI та робочі станції користувачів. На рівні ядра знаходиться маршрутизатор, що забезпечує підключення до Інтернету через провайдера вищого рівня та формує кінцеву точку VPN-тунелю.

Адресний простір мережі розділено на зовнішній та внутрішній сегменти. Зовнішні IP-адреси виділяються провайдером вищого рівня та використовуються як кінцеві точки VPN-тунелю. Внутрішні адреси належать до діапазону 10.0.0.0/8 та розподіляються між підмережами офісів і тунельним інтерфейсом згідно із затвердженою схемою адресації, що наведена у таблиці 2.2.

Таблиця 2.2 – Схема IP-адресації мережі

Сегмент мережі	Адреса підмережі	Призначення
Зовнішній інтерфейс (головний офіс)	217.11.64.236/24	WAN-інтерфейс hub-маршрутизатора
Шлюз провайдера	217.11.64.235	Маршрутизатор провайдера
Тунельна підмережа DMVPN	10.0.254.0/24	Адреси тунельних інтерфейсів
LAN головного офісу	10.0.1.0/24	Внутрішня мережа головного офісу
LAN віддаленого офісу	10.0.2.0/24	Внутрішня мережа віддаленого офісу
Резервний діапазон	10.0.3.0-10.0.253.255	Резерв для розширення

Окремою вимогою є масштабованість рішення. Компанія планує відкриття ще одного регіонального відділення протягом наступних двох років, тому архітектура мережі повинна передбачати можливість підключення нових вузлів без кардинальної зміни конфігурації існуючої інфраструктури. Технологія DMVPN на основі протоколу NHRP задовольняє цю вимогу, оскільки додавання нового spoke-вузла потребує лише локальної конфігурації на новому маршрутизаторі без втручання в налаштування hub-вузла [24].

Коефіцієнт готовності A каналу зв'язку, що характеризує частку часу, протягом якого система є працездатною, визначається через середній час між відмовами $MTBF$ та середній час відновлення $MTTR$:

$$A = \frac{MTBF}{MTBF + MTTR}. \quad (2.1)$$

Для досягнення цільового значення $A \geq 0{,}995$ при типовому для корпоративного обладнання значенні $MTTR = 4$ год необхідно забезпечити $MTBF \geq 796$ год, що відповідає приблизно 33 діб безперервної роботи [23]. Це є досяжним показником для обладнання корпоративного класу за умови дотримання рекомендацій виробника щодо обслуговування.

2.2 Вибір топології мережі, протоколів та обладнання

Вибір топології є одним із ключових рішень при проектуванні корпоративної VPN-мережі, оскільки він визначає масштабованість, відмовостійкість та складність подальшого адміністрування. Для мережі з одним центральним вузлом та кількома віддаленими підрозділами найбільш обґрунтованою є топологія «зірка» із застосуванням технології DMVPN (Dynamic Multipoint VPN). Ця технологія дозволяє динамічно встановлювати тунелі між spoke-вузлами через протокол NHRP, не навантажуючи центральний hub надлишковим транзитним трафіком [25]. Водночас додавання нових вузлів не потребує зміни конфігурації вже розгорнутої інфраструктури, що є принциповою перевагою порівняно зі статичними топологіями типу «точка-точка».

Як тунельний протокол обрано mGRE (Multipoint Generic Routing Encapsulation) у поєднанні з IPsec у транспортному режимі. Протокол mGRE забезпечує мультиточкову інкапсуляцію пакетів в єдиному тунельному інтерфейсі, що суттєво спрощує конфігурацію порівняно зі створенням окремого GRE-тунелю для кожної пари вузлів. IPsec у транспортному режимі при цьому шифрує корисне навантаження GRE-пакета, забезпечуючи конфіденційність та цілісність трафіку [26]. Для автоматичного узгодження параметрів захищеної

асоціації використовується протокол IKEv2 з автентифікацією на основі попередньо розподіленого ключа (pre-shared key). Як алгоритм шифрування обрано AES-256-GCM, а для забезпечення цілісності – HMAC-SHA-256.

Для динамічної маршрутизації між підмережами офісів через VPN-тунель застосовується протокол OSPF (Open Shortest Path First). Він автоматично розповсюджує інформацію про маршрути між вузлами та забезпечує швидку збіжність у разі зміни топології. На тунельних інтерфейсах налаштовується тип мережі OSPF «broadcast», що дозволяє hub-маршрутизатору виступати в ролі призначеного маршрутизатора (DR) і мінімізувати кількість обміну пакетами стану витка [25].

Вибір активного обладнання проводився виходячи з вимог до пропускної здатності, підтримуваних протоколів та співвідношення ціни та якості. Для ролі маршрутизаторів обрано серію Cisco 2900, а саме модель Cisco 2901. Ця модель підтримує апаратне прискорення криптографічних операцій, протоколи DMVPN, IPsec, OSPF та забезпечує пропускну здатність з увімкненим шифруванням понад 26 Мбіт/с, що перекриває розраховані потреби мережі [27]. На рисунку 2.2 наведено зовнішній вигляд обраного маршрутизатора.

Рисунок 2.2 – Маршрутизатор Cisco 2901

На рівні доступу для кожного офісу обрано керований комутатор другого рівня D-Link DES-3200-28. Ця модель підтримує налаштування VLAN стандарту IEEE 802.1Q, що дозволяє логічно розділити трафік різних підрозділів в межах одного фізичного обладнання, а також функції контролю широкомовного

шторму та Port Security для захисту від несанкціонованих підключень [28]. Технічні характеристики обраного активного обладнання зведено у таблиці 2.3.

Таблиця 2.3 – Технічні характеристики обраного активного обладнання

Параметр	Cisco 2901	D-Link DES-3200-28
Тип пристрою	Маршрутизатор ISR	Керований комутатор L2
Кількість портів	2 × GE, слоти HWIC	24 × 100 Мбіт/с, 4 × GE/SFP
Пропускна здатність	26+ Мбіт/с (з IPsec)	12,8 Гбіт/с
Підтримувані протоколи	DMVPN, IPsec, OSPF, NHRP	VLAN 802.1Q, STP, LACP
Операційна система	Cisco IOS 15.x	DES-3200 firmware
Апаратне шифрування	Так (AES, 3DES)	Не застосовується

Як фізичне середовище передачі даних у межах офісних приміщень обрано кабель витої пари категорії FTP CAT5e. Ця категорія забезпечує швидкість передачі до 1000 Мбіт/с при використанні всіх чотирьох пар і підтримує смугу пропускання 100 МГц, чого цілком достатньо для організації гігабітної мережі доступу. Наявність загального екрана з фольги у кабелі FTP забезпечує захист від електромагнітних наводок, що є важливим у серверних приміщеннях з великою щільністю кабельних трас [29]. Максимальна довжина сегмента кабелю відповідно до стандарту IEEE 802.3 становить 100 м, що перекриває потреби будь-якого з розглянутих офісів.

Загальна вартість активного мережевого обладнання для обох офісів розраховується як сума вартості маршрутизаторів, комутаторів, SFP-модулів та кабельної продукції з урахуванням коефіцієнта непередбачених витрат k_{res}:

$$C_{total} = \left(\sum_{i=1}^{n} C_i \cdot q_i \right) \cdot (1 + k_{res}), \tag{2.2}$$

де C_i – ціна одиниці обладнання i-го найменування,

q_i – кількість одиниць,

n – загальна кількість найменувань,

$k_{res} = 0{,}10$ – коефіцієнт резерву на непередбачені витрати [30].

Таким чином, для побудови корпоративної VPN-мережі обрано архітектуру DMVPN на базі маршрутизаторів Cisco 2901 із протоколами mGRE, IPsec (AES-256-GCM) та динамічною маршрутизацією OSPF. На рівні доступу застосовуються керовані комутатори D-Link DES-3200-28 із підтримкою VLAN. Кабельна інфраструктура побудована на основі FTP CAT5e. Така конфігурація забезпечує необхідний рівень безпеки, продуктивності та масштабованості мережі відповідно до сформульованих у попередньому підрозділі вимог.

2.3 Розрахунок навантаження та пропускної здатності каналів зв'язку

Коректне визначення необхідної пропускної здатності каналу між офісами є критично важливим кроком проектування, оскільки недостатній канал призводить до деградації якості сервісів, а надмірний – до невиправданих фінансових витрат. Розрахунок виконується методом підсумовування пікових навантажень, що генеруються окремими категоріями користувачів та застосунків, з подальшим застосуванням коефіцієнта одночасності [31].

Першим кроком є визначення питомого навантаження для кожного типу сервісу. На основі вимірювань реального трафіку у подібних корпоративних середовищах встановлено такі орієнтовні значення: відеоконференція у форматі HD – близько 2048 кбіт/с на учасника, робота з корпоративною поштою – 460 кбіт/с, звернення до баз даних (MeDoc, біллінгова система) – 128 кбіт/с, завантаження вебсторінок та хмарних ресурсів – 252 кбіт/с, SSH-сесія віддаленого адміністрування – 72 кбіт/с, підключення через віддалений робочий стіл RDP – 260 кбіт/с [31]. Ці значення відповідають середньому навантаженню протягом робочого дня і є основою для подальших розрахунків.

На основі зазначених питомих значень розраховується сумарне навантаження для кожної категорії персоналу. Менеджери комерційного відділу (7 осіб) інтенсивно використовують поштовий сервер, відеозв'язок та хмарні бази даних. Технічний персонал (4 особи у віддаленому офісі: бухгалтери та

комерційний директор) активно звертається до біллінгової системи та хмарних сервісів. Навантаження, що генерується підрозділами віддаленого офісу, є визначальним для розміру міжофісного VPN-каналу, оскільки весь цей трафік проходить через тунель до головного офісу.

Таблиця 2.4 – Розрахункове навантаження від підрозділів віддаленого офісу

Категорія	Кількість, осіб	Сервіси	Навантаження на 1 особу, кбіт/с	Сумарно, кбіт/с
Менеджери	7	Пошта, відео, БД, веб	2888	20216
Бухгалтери	4	MeDoc, пошта, відео, веб	2888	11552
Комерційний директор	1	Пошта, відео, веб, RDP	3020	3020
Разом	12	–	–	34788

Сумарне розрахункове навантаження від усіх користувачів віддаленого офісу становить близько 34,8 Мбіт/с. Однак враховувати цю цифру як мінімально необхідну пропускну здатність каналу некоректно, оскільки не всі користувачі одночасно виконують найбільш навантажені операції. Для врахування цього факту застосовується коефіцієнт одночасності k_{sim}, що для корпоративних мереж з кількістю користувачів до 50 осіб зазвичай приймається у діапазоні 0,6-0,75 [32]. Необхідна пропускна здатність каналу C_{req} з урахуванням коефіцієнта одночасності та запасу на накладні витрати VPN-шифрування k_{vpn} визначається за формулою:

$$C_{req} = \sum_{j=1}^{m} (n_j \cdot a_j) \cdot k_{sim} \cdot k_{vpn} \tag{2.3}$$

де n_j – кількість користувачів j-ї категорії,

a_j – питоме навантаження одного користувача j-ї категорії (кбіт/с),

m – кількість категорій,

$k_{sim} = 0{,}65$ – коефіцієнт одночасності,

$k_{vpn} = 1{,}15$ – коефіцієнт накладних витрат на інкапсуляцію та шифрування IPsec [31].

Підставляючи числові значення: $C_{req} = 34788 \cdot 0{,}65 \cdot 1{,}15 \approx 26{,}0$ Мбіт/с. Отже, мінімально необхідна пропускна здатність каналу між офісами становить близько 26 Мбіт/с. З урахуванням рекомендації закладати 30-40% резерву на майбутнє зростання навантаження, до провайдера вищого рівня слід замовити канал із пропускною здатністю не менше 35-40 Мбіт/с. Для практичної реалізації обрано канал 52 Мбіт/с, що є найближчим стандартним тарифним планом і забезпечує достатній запас продуктивності. На рисунку 2.3 наведено структуру розподілу навантаження між категоріями користувачів у піковий робочий час.

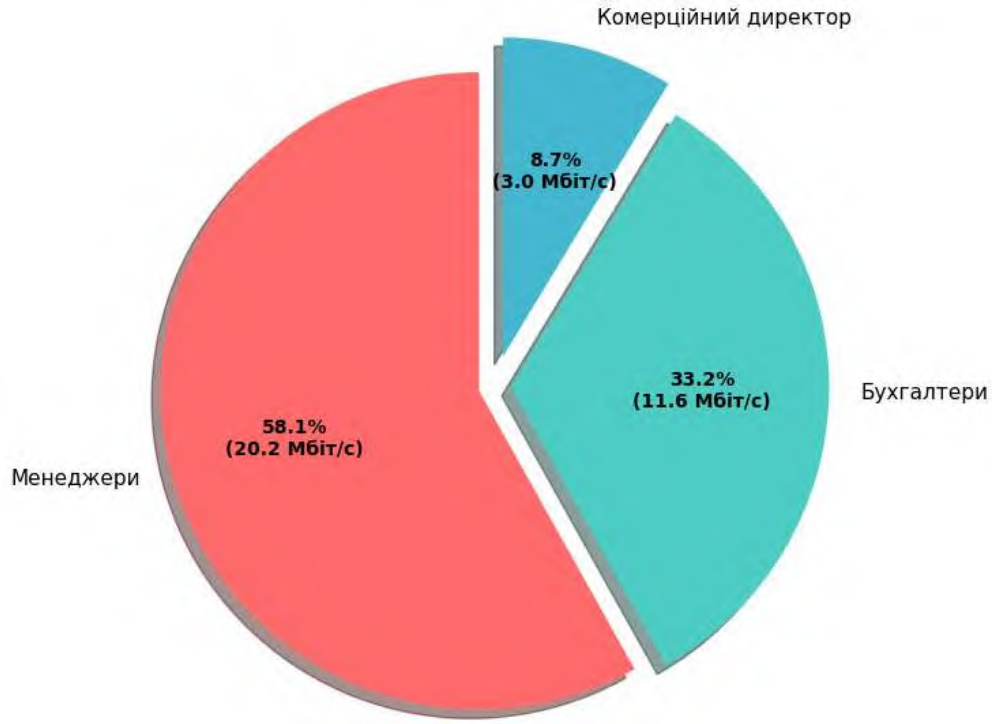

Рисунок 2.3 – Розподіл мережевого навантаження між категоріями користувачів віддаленого офісу

Для перевірки адекватності розрахунку також виконано аналіз завантаженості каналу за методом теорії масового обслуговування з використанням моделі M/M/1. При пропускній здатності каналу $C = 52$ Мбіт/с та інтенсивності трафіку, що відповідає розрахунковому значенню 26 Мбіт/с,

інтенсивність навантаження $\rho = 26/52 = 0{,}5$. Це є комфортним робочим режимом для системи масового обслуговування, при якому середня довжина черги пакетів залишається мінімальною, а затримка не перевищує допустимих значень для VoIP та відеоконференцій.

Додатково слід враховувати, що у перспективі відкриття третього офісу загальне навантаження на канал головного офісу зросте пропорційно. Завдяки обраній архітектурі DMVPN новий офіс формуватиме окремий тунель до hub-маршрутизатора, а трафік між spoke-вузлами може маршрутизуватися безпосередньо, оминаючи hub. Це дозволяє уникнути «вузького місця» у точці концентрації трафіку та забезпечує лінійне масштабування пропускної здатності мережі [32].

2.4 Налаштування VPN-тунелів та конфігурація мережевого обладнання

Після визначення архітектури мережі, вибору обладнання та розрахунку необхідної пропускної здатності переходять до практичного етапу – конфігурації мережевих пристроїв. Налаштування виконується поетапно: спочатку конфігурується hub-маршрутизатор головного офісу, потім – spoke-маршрутизатор віддаленого офісу. Усі команди вводяться через термінальний інтерфейс у режимі конфігурації операційної системи Cisco IOS [27].

Першим кроком на hub-маршрутизаторі є створення тунельного інтерфейсу Tunnel0 та його прив'язка до фізичного WAN-порту. Тунельному інтерфейсу присвоюється IP-адреса з підмережі DMVPN (10.0.254.1/24). Далі активується протокол NHRP у режимі динамічного запам'ятовування адрес клієнтських вузлів із зазначенням ідентифікатора мережі network-id. Режим тунелювання встановлюється як mGRE (tunnel mode gre multipoint), що дозволяє одному інтерфейсу обслуговувати одночасно кілька spoke-вузлів. Для захисту трафіку на тунельному інтерфейсі застосовується профіль IPsec, попередньо

сконфігурований із параметрами шифрування AES та хешування SHA-HMAC [25].

Конфігурація криптографічного захисту на hub-маршрутизаторі включає такі кроки: створення політики ISAKMP з автентифікацією на основі pre-shared key, визначення спільного ключа для всіх spoke-вузлів (із зазначенням адреси 0.0.0.0 для прийняття підключень від будь-якого вузла), створення transform-set із алгоритмами esp-aes та esp-sha-hmac у транспортному режимі, та формування профілю IPsec, який прив'язується до тунельного інтерфейсу командою tunnel protection. Таблицю основних команд конфігурації hub-маршрутизатора наведено у таблиці 2.5.

Таблиця 2.5 – Основні команди конфігурації hub-маршрутизатора (alm-R1)

Команда IOS	Призначення
interface Tunnel0	Створення тунельного інтерфейсу
ip address 10.0.254.1 255.255.255.0	Призначення адреси тунельного інтерфейсу
ip nhrp map multicast dynamic	Динамічне запам'ятовування адрес spoke
ip nhrp network-id 1	Ідентифікатор DMVPN-домену
tunnel source fa0/1	Прив'язка до фізичного WAN-інтерфейсу
tunnel mode gre multipoint	Увімкнення режиму mGRE
tunnel protection ipsec profile DAN-VPN	Захист тунелю профілем IPsec
crypto isakmp policy 1	Створення політики IKE фази 1
crypto ipsec transform-set DAN2711-NET esp-aes esp-sha-hmac	Визначення алгоритмів шифрування
router ospf 1	Увімкнення динамічної маршрутизації OSPF

Конфігурація spoke-маршрутизатора віддаленого офісу (ast-R2) принципово відрізняється від hub тим, що вузол повинен явно вказати адресу NHS-сервера (hub) для реєстрації у DMVPN-домені. На тунельному інтерфейсі spoke-вузла задається статичне відображення між тунельною адресою hub (10.0.254.1) та його зовнішньою IP-адресою, а також адреса NHS командою ip nhrp nhs. Параметр ip ospf priority 0 на тунельному інтерфейсі spoke-вузла запобігає його участі у виборах призначеного маршрутизатора OSPF, залишаючи цю роль за hub [25]. Принципову схему встановлення DMVPN-тунелю між вузлами наведено на рисунку 2.4.

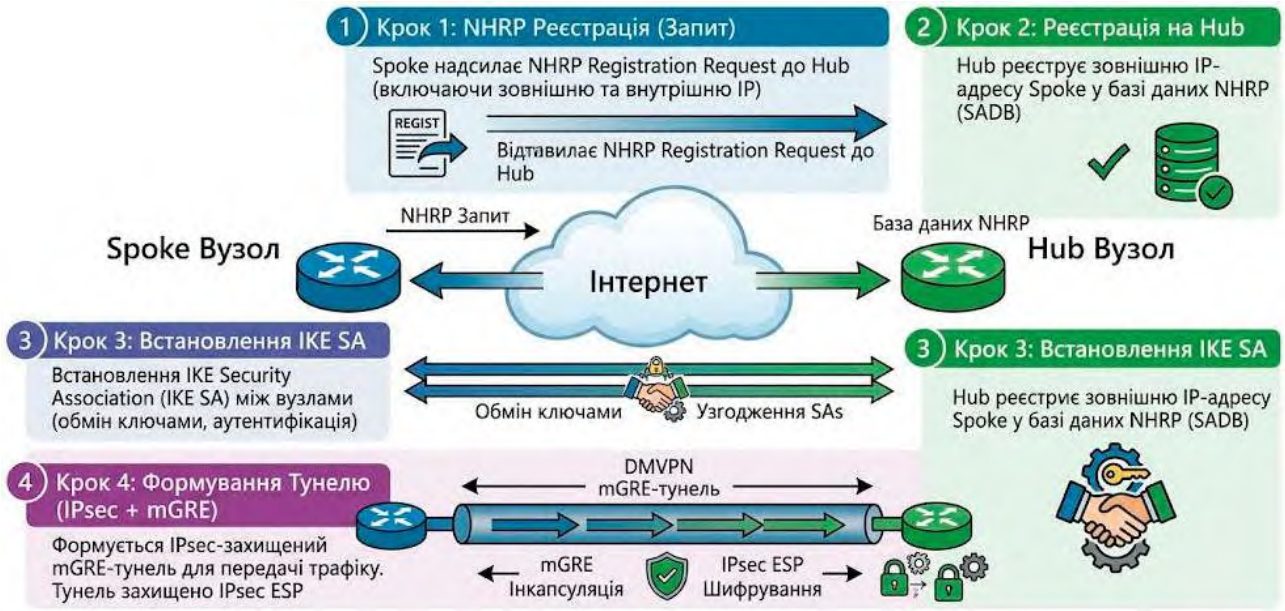

Рисунок 2.4 – Схема встановлення DMVPN-тунелю між hub та spoke вузлами

Після завершення налаштування тунельних інтерфейсів виконується конфігурація протоколу OSPF на обох маршрутизаторах. Оголошується підмережа 10.0.0.0/8 в зоні 0 (backbone area), що охоплює як тунельні адреси, так і адреси локальних підмереж офісів. Завдяки цьому маршрутизатори автоматично обмінюються інформацією про досяжні підмережі та формують таблиці маршрутизації без ручного втручання адміністратора [26].

На рівні доступу комутатори D-Link DES-3200-28 налаштовуються із розподілом портів на VLAN-групи відповідно до організаційної структури: VLAN 10 для технічного відділу, VLAN 20 для адміністративного персоналу, VLAN 30 для серверного сегменту. Між VLAN-групами маршрутизація здійснюється на рівні маршрутизатора за схемою «router-on-a-stick» через субінтерфейси фізичного LAN-порту [28]. Це забезпечує ізоляцію трафіку між підрозділами та підвищує загальну безпеку мережі.

Для верифікації правильності налаштування використовуються стандартні діагностичні команди Cisco IOS. Команда show dmvpn відображає стан NHRP-реєстрацій та тип встановлених тунелів, show crypto ipsec sa – статистику шифрованих з'єднань, show ip ospf neighbor – стан сусідства OSPF між вузлами. Успішне налаштування підтверджується наявністю spoke-вузла у стані NHRP

«UP» та активним OSPF-сусідством між hub та spoke [27]. Додатково перевіряється наскрізна досяжність між підмережами офісів командою ping та вимірюється затримка каналу для підтвердження відповідності встановленим вимогам.

Було виконано повний цикл проектування корпоративної VPN-мережі: сформульовано вимоги до інфраструктури та визначено склад користувачів, обґрунтовано вибір топології DMVPN та протоколів mGRE/IPsec/OSPF, розраховано необхідну пропускну здатність міжофісного каналу (не менше 26 Мбіт/с з урахуванням коефіцієнта одночасності та накладних витрат шифрування), обрано активне мережеве обладнання класу Cisco 2901 та D-Link DES-3200-28, а також детально описано конфігурацію всіх мережевих вузлів. Розроблена мережа відповідає вимогам безпеки згідно з ДСТУ ISO/IEC 27001:2023, забезпечує необхідний рівень доступності та є готовою до аналітичного моделювання продуктивності методами теорії масового обслуговування, що виконується у наступному розділі.

РОЗДІЛ 3
ПРОГРАМНА РЕАЛІЗАЦІЯ PYTHON МОДЕЛІ ТА АНАЛІЗ ПРОДУКТИВНОСТІ МЕРЕЖІ

3.1 Розробка програмного модуля моделювання мережі на Python

Для дослідження продуктивності корпоративної VPN-мережі розроблено програмний комплекс мовою Python, що реалізує як аналітичну, так і імітаційну моделі системи масового обслуговування. Вибір Python як інструментарію обумовлений розвиненою екосистемою наукових бібліотек, відкритою ліцензією та широкою підтримкою у дослідницькій спільноті [18]. Комплекс складається з трьох модулів: файлу конфігурації config.json, основного модуля vpn_model.py із реалізацією моделей та скрипту run_analysis.py, що керує запуском розрахунків, збереженням результатів і побудовою графіків.

Архітектура комплексу побудована за принципом розділення відповідальності. Усі вхідні параметри зосереджені в єдиному конфігураційному файлі формату JSON, що дозволяє змінювати сценарії моделювання без редагування програмного коду. Файл config.json містить чотири групи параметрів: налаштування імітаційної моделі (кількість прогонів, час моделювання, час прогріву), характеристики мережевого каналу (пропускна здатність, середній розмір пакета, накладні витрати шифрування), опис трафіку (перелік категорій користувачів із чисельністю та питомим навантаженням, коефіцієнти одночасності та VPN-накладних витрат) та порогові значення QoS. Така структура відповідає сучасним практикам розробки програмного забезпечення і спрощує повторне використання моделі для інших вхідних умов [20].

Модуль vpn_model.py реалізує три незалежні компоненти. Перший – аналітична модель M/M/1, що обчислює класичні характеристики системи масового обслуговування з необмеженою чергою: середню кількість пакетів у системі L, середню довжину черги L_q, середній час перебування пакета у системі

W та середній час очікування у черзі W_q. Другий компонент – аналітична модель M/M/1/K з обмеженою місткістю черги K, яка додатково розраховує ймовірність відмови P_{loss} та ефективну інтенсивність обслуговування з урахуванням відкинутих пакетів. Третій компонент – імітаційна модель на базі бібліотеки SimPy, що моделює дискретні події надходження та обслуговування пакетів у реальному масштабі часового вікна [18]. Вхідні параметри для всіх компонентів обчислюються автоматично на основі даних конфігурації через функції calc_arrival_rate() та calc_service_rate(). Структуру програмного комплексу та взаємодію його складових наведено на рисунку 3.1.

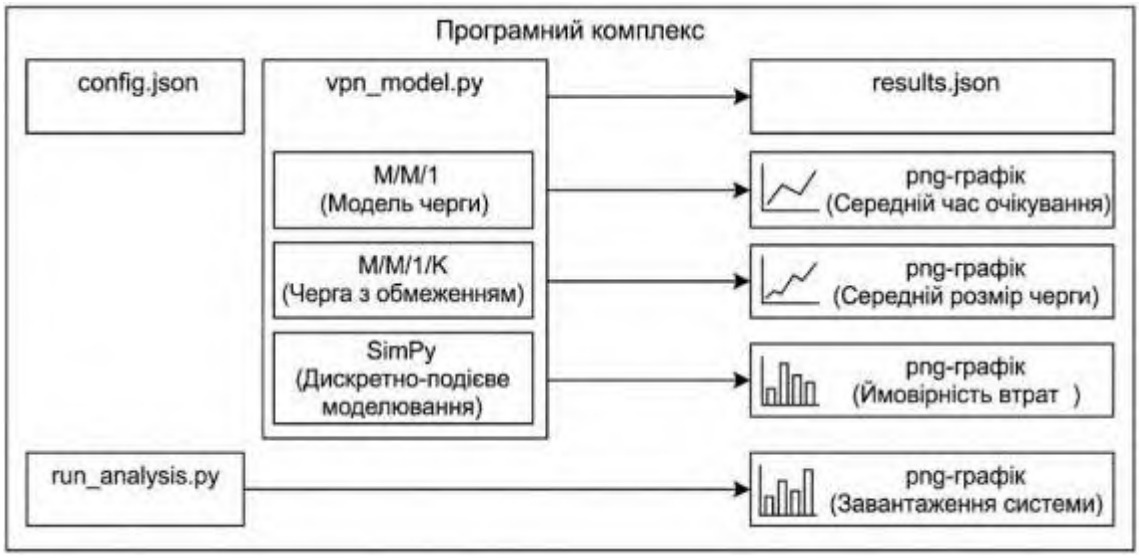

Рисунок 3.1 – Структура програмного комплексу моделювання VPN-мережі

Інтенсивність надходження пакетів λ розраховується шляхом підсумовування питомих навантажень усіх категорій користувачів з подальшим застосуванням коефіцієнта одночасності $k_{sim} = 0{,}65$ та коефіцієнта накладних витрат VPN-шифрування $k_{vpn} = 1{,}15$. Для каналу пропускною здатністю 52 Мбіт/с та середнього розміру пакета 1500 байт із накладними витратами шифрування 15 мкс на пакет розраховані значення складають $\lambda = 2167{,}0$ пакетів/с та $\mu = 4068{,}9$ пакетів/с. Отже, інтенсивність навантаження $\rho = 0{,}533$, що відповідає стабільному режиму роботи системи зі значним запасом до насичення.

Для підвищення достовірності результатів імітаційна модель виконує п'ять незалежних прогонів із різними початковими станами генератора псевдовипадкових чисел та усереднює отримані значення. Кожен прогін охоплює 3600 секунд модельного часу з часом прогріву 300 секунд, протягом якого статистика не збирається – це дозволяє виключити вплив нестаціонарного перехідного процесу на результати [18]. Підсумкові результати зберігаються у файл results.json з деталізацією по кожному прогону та усередненими показниками, що забезпечує їх придатність для подальшого аналізу.

Коректність програмної реалізації підтверджується перехресною перевіркою результатів аналітичної та імітаційної моделей. Як видно з табл. 3.1, відхилення між аналітично розрахованими та імітаційно отриманими значеннями ключових характеристик не перевищує 0,03%, що свідчить про відсутність алгоритмічних помилок у реалізації симулятора. Додатковою перевіркою є виконання закону Літтла – рівності $L = \lambda \cdot W$, яка виконується з точністю до шостого знаку після коми.

Таблиця 3.1 – Порівняння результатів аналітичної та імітаційної моделей

Показник	Аналітична M/M/1	Імітаційна (SimPy, сер.)	Відхилення,%
Середній час у системі W, мс	0,5258	0,5259	0,02
Середній час очікування Wq, мс	0,2800	0,2801	0,02
Середня довжина черги Lq, пакетів	0,6068	0,6070	0,03
Кількість відкинутих пакетів	–	0	–

Відтворюваність результатів між незалежними прогонами є ще одним показником якості моделі. Коефіцієнт варіації середньої затримки між п'ятьма прогонами становить лише 0,186%, що підтверджує статистичну стабільність імітаційної моделі. Жоден із прогонів не зафіксував відкинутих пакетів, що є очікуваним результатом для системи з $\rho \approx 0{,}53$ та місткістю буфера $K = 50$.

Важливою практичною перевагою розробленого комплексу є його гнучкість. Зміна будь-якого параметра у config.json – наприклад, збільшення кількості користувачів, зменшення пропускної здатності каналу або введення

нових категорій трафіку – автоматично перераховує всі характеристики моделі без необхідності модифікації коду. Це дозволяє використовувати комплекс як інструмент підтримки прийняття рішень при плануванні розширення мережі або оцінці наслідків зміни навантаження [20].

Розроблений програмний комплекс повністю задовольняє потреби дослідження: він коректно реалізує моделі M/M/1 та M/M/1/K, забезпечує статистично достовірні імітаційні результати, зберігає вихідні дані у структурованому форматі для подальшого аналізу та автоматично генерує графіки залежностей.

3.2 Моделювання черг та аналіз затримок на основі теорії масового обслуговування

Центральним результатом моделювання є кількісна оцінка характеристик якості обслуговування пакетів у VPN-шлюзі за реальних умов навантаження спроектованої мережі. Відповідно до розрахованих вхідних параметрів, інтенсивність навантаження системи становить $\rho = 0{,}533$, тобто маршрутизатор використовує трохи більше половини своєї обчислювальної та пропускної спроможності. Це є комфортним робочим режимом, який забезпечує стабільну роботу без накопичення черг навіть у пікові години [12].

Ключовий показник якості сервісу – середній час перебування пакета у системі $W = 0{,}526$ мс. Це значення включає як час очікування в черзі ($W_q = 0{,}280$ мс), так і час безпосереднього обслуговування (шифрування та передачі по каналу). Для порівняння: рекомендація ITU-T G.114 встановлює максимально допустиму односторонню затримку для IP-телефонії на рівні 150 мс, а практичний поріг комфортної роботи – 50 мс [23]. Отримане значення 0,526 мс є у 95 разів меншим за цей поріг, що означає повну відсутність проблем із якістю голосового зв'язку та відеоконференцій у спроектованій мережі.

Важливою характеристикою є не лише середня затримка, а й її розподіл. За результатами імітаційної моделі, 95-й перцентиль затримки становить $W_{p95} = 1{,}575$ мс – тобто лише 5% пакетів затримуються більш ніж на 1,575 мс. Стандартне відхилення затримки дорівнює 0,526 мс, що свідчить про відносно рівномірний розподіл без значних сплесків. Такі характеристики джиттера є прийнятними для всіх типів корпоративного трафіку, включаючи потокове відео та VoIP [23].

Середня довжина черги $L_q = 0{,}607$ пакетів означає, що у будь-який момент часу у буфері маршрутизатора в середньому очікує менше одного пакета. Це підтверджує відсутність систематичного перевантаження вузла за поточних умов навантаження. Зведені результати аналітичної моделі M/M/1 для робочої точки наведено у таблиці 3.2.

Таблиця 3.2 – Характеристики якості обслуговування VPN-шлюзу за робочих умов навантаження

Показник	Позначення	Значення	Одиниця
Інтенсивність навантаження	ρ	0,5326	–
Середня кількість пакетів у системі	L	1,1394	пакетів
Середня довжина черги	L_q	0,6068	пакетів
Середній час у системі	W	0,526	мс
Середній час очікування в черзі	W_q	0,280	мс
Ймовірність втрати пакета (K=20)	P_{loss}	$1{,}58\times10^{-6}$	–
95-й перцентиль затримки (імітація)	W_{p95}	1,575	мс

Для розуміння поведінки системи за різних умов навантаження виконано аналіз чутливості – розрахунок характеристик у діапазоні ρ від 0,10 до 0,95. Залежність середньої затримки від інтенсивності навантаження наведено на рисунку 3.2. Графік демонструє нелінійне зростання затримки при наближенні ρ до одиниці, що є класичною поведінкою системи M/M/1 [12]. Робоча точка спроектованої мережі ($\rho = 0{,}533$) знаходиться у пологій частині кривої, де затримка ще практично не залежить від незначних коливань навантаження.

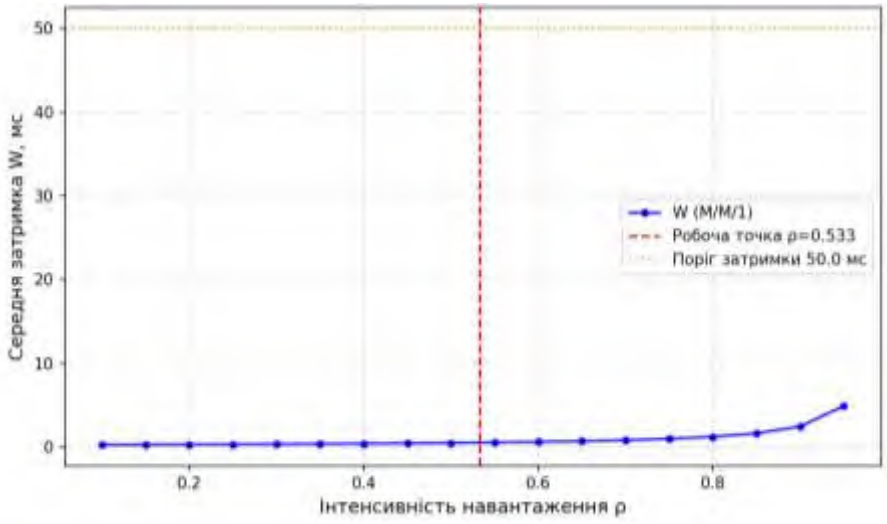

Рисунок 3.2 – Залежність середньої затримки пакета від інтенсивності навантаження

Аналогічну нелінійну поведінку демонструє залежність середньої довжини черги від навантаження, наведена на рисунку 3.3. При $\rho = 0{,}7$ довжина черги сягає вже 1,63 пакета, при $\rho = 0{,}85$ – 4,82 пакета, а при $\rho = 0{,}95$ – 18,05 пакета, що впритул наближається до межі буфера. Ці дані наочно ілюструють важливість підтримання запасу пропускної здатності та підтверджують доцільність обраного каналу 52 Мбіт/с замість мінімально розрахованих 26 Мбіт/с.

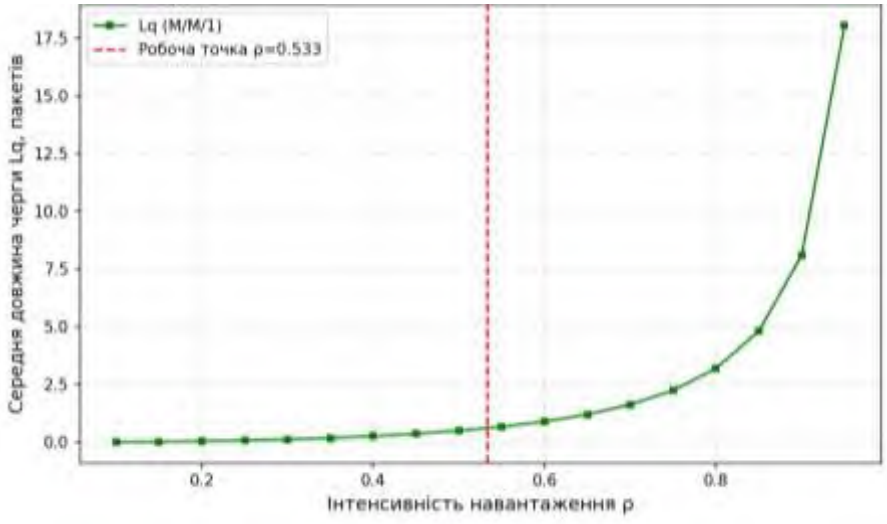

Рисунок 3.3 – Залежність середньої довжини черги від інтенсивності навантаження

Аналіз моделі M/M/1/K з обмеженою місткістю буфера $K = 20$ показує, що ймовірність втрати пакета при поточному навантаженні становить $P_{loss} = 1{,}58 \times 10^{-6}$, тобто втрачається менш ніж два пакети на мільйон. Це значення на чотири порядки менше від допустимого порогу 0,01 (1%), що відповідає найвищому класу якості обслуговування для корпоративних мереж [9]. На рисунку 3.4 наведено залежність ймовірності втрати від навантаження для моделі M/M/1/K.

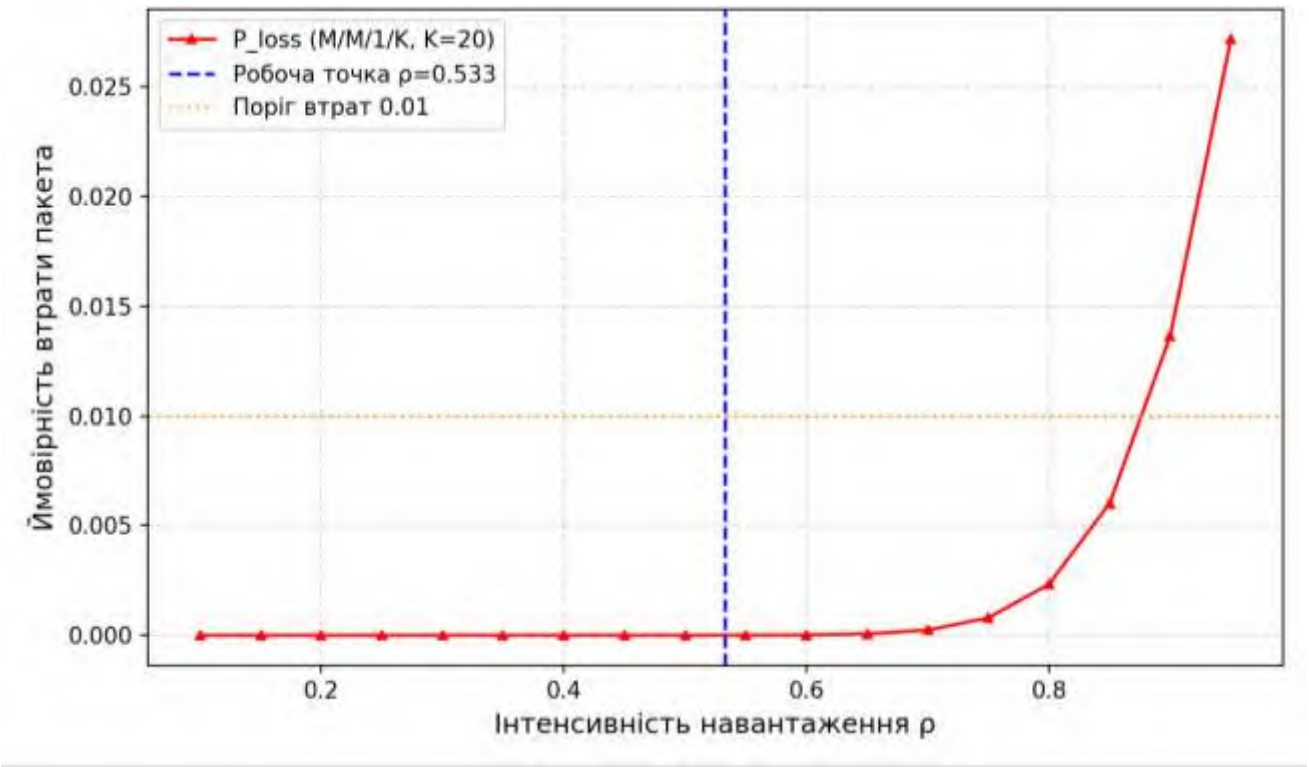

Рисунок 3.4 – Залежність ймовірності втрати пакета від інтенсивності навантаження (M/M/1/K, K=20)

Окремий практичний інтерес становить питання: при якому навантаженні мережа починає порушувати QoS-вимоги? За результатами аналізу чутливості, наведеними у таблиці 3.3, поріг допустимої ймовірності втрат $P_{loss} \leq 0{,}01$ порушується при $\rho \geq 0{,}90$, що відповідає навантаженню близько 46,7 Мбіт/с на канал 52 Мбіт/с. Поріг затримки 50 мс для M/M/1 не досягається навіть при $\rho = 0{,}95$ (затримка 4,92 мс), що свідчить про те, що обране обладнання та канал мають значний запас навіть у надзвичайних ситуаціях.

Таблиця 3.3 – Характеристики системи при критичних значеннях навантаження

ρ	Навантаження, Мбіт/с	W, мс	Lq, пакетів	P_loss (K=20)	QoS
0,50	26,0	0,492	0,500	$< 10^{-6}$	✓
0,53	27,6	0,526	0,607	$1{,}58\times10^{-6}$	✓
0,70	36,4	0,819	1,633	$2{,}4\times10^{-4}$	✓
0,85	44,2	1,639	4,817	$6{,}0\times10^{-3}$	✓
0,90	46,8	2,458	8,100	$1{,}37\times10^{-2}$	✗
0,95	49,4	4,915	18,050	$2{,}72\times10^{-2}$	✗

Таким чином, результати моделювання підтверджують, що спроектована VPN-мережа з каналом 52 Мбіт/с та обладнанням Cisco 2901 повністю забезпечує необхідний рівень якості обслуговування при поточному навантаженні ($\rho = 0{,}533$) з запасом до критичного рівня завантаженості у $\Delta\rho \approx 0{,}37$, що відповідає додатковим 19 Мбіт/с трафіку. Цього запасу достатньо для підключення нового офісу або суттєвого зростання кількості користувачів без необхідності модернізації каналу зв'язку.

3.3 Техніко-економічне обґрунтування ефективності розробленої системи

Економічна оцінка проєкту розгортання корпоративної VPN-мережі з програмним модулем моделювання виконується методом порівняння витрат на впровадження та експлуатацію з отриманими вигодами. Відповідно до методичних рекомендацій щодо оцінки ІТ-проєктів, загальна сума витрат включає прямі витрати на впровадження, непрямі витрати та щорічні витрати на утримання [8]. Як критерії економічної ефективності використовуються показники NPV, ROI та термін окупності.

Прямі витрати на впровадження проєкту охоплюють вартість мережевого обладнання, організацію робочих місць та витрати на оплату праці. Перелік і

вартість основного обладнання для побудови VPN-мережі наведено у таблиці 3.4.

Таблиця 3.4 – Капітальні витрати на придбання та впровадження обладнання

Найменування	Кількість	Ціна, грн	Сума, грн
Маршрутизатор Cisco 2901	2 шт.	36000	72000
Комутатор D-Link DES-3200-28	2 шт.	5740	11480
Модуль SFP TX	2 шт.	3850	7700
Модуль SFP RJ45	2 шт.	3900	7800
Кабель FTP CAT5e, м	1000 м	5	5000
Витрати на монтаж (8% від вартості обладнання)	–	–	8318
Витрати на транспортування (5% від вартості обладнання)	–	–	5199
Непередбачені витрати (10%)	–	–	11750
Разом			129247

Витрати на розробку програмного модуля моделювання визначаються через трудомісткість робіт. Розробку виконує один IT-інженер. Загальна трудомісткість складає 120 людино-годин, що включає аналіз вимог (16 год), проєктування архітектури моделі (24 год), написання та налаштування коду (48 год), тестування та верифікацію результатів (20 год) та документування (12 год). При годинній ставці IT-інженера 250 грн/год витрати на розробку ПЗ складуть:

$$В_{ПЗ} = T \cdot S = 120 \cdot 250 = 30000 \text{ (грн)} \quad (3.1)$$

де T – трудомісткість у людино-годинах,

S – годинна ставка спеціаліста.

З урахуванням єдиного соціального внеску (22%) витрати на оплату праці складуть 36600 грн. Таким чином, загальні прямі витрати на впровадження проєкту $ВП = 129247 + 36600 = 165847$ грн.

Щорічні витрати на утримання системи включають витрати на технічне обслуговування обладнання (5% від вартості обладнання на рік) та оплату послуг інтернет-каналу 52 Мбіт/с. Орієнтовна вартість корпоративного каналу такої пропускної здатності в Україні станом на 2025 рік складає близько 4500 грн на

місяць, або 54000 грн на рік [31]. Щорічні витрати на технічне обслуговування обладнання: $0{,}05 \times 104180 = 5209$ грн. Отже, загальні щорічні витрати на утримання $В_{УТР} = 54000 + 5209 = 59209$ грн.

Економічний ефект від впровадження VPN-мережі досягається насамперед за рахунок відмови від оренди виділеного фізичного каналу зв'язку між офісами, що у разі традиційного підходу обходилося б значно дорожче. За ринковими цінами оренда виділеного MPLS-каналу між двома офісами аналогічної пропускної здатності коштує орієнтовно 18000 грн на місяць, або 216000 грн на рік. Різниця між вартістю виділеного каналу та обраним рішенням на базі VPN формує пряму річну економію $Е = 216000 - 59209 = 156791$ грн.

Розрахунок чистої теперішньої вартості (NPV) виконується за п'ятирічний горизонт планування при ставці дисконтування $i = 20\,\%$ (відповідає середній обліковій ставці НБУ та ризику проєкту):

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+i)^t} - INV_0, \tag{3.2}$$

де CF_t – чистий грошовий потік у році t (дорівнює річній економії 156791 грн),

$INV_0 = 165847$ грн – початкові інвестиції,

$n = 5$ років.

Результати розрахунку дисконтованих грошових потоків наведено у таблиці 3.5.

Таблиця 3.5 – Розрахунок дисконтованих грошових потоків проєкту

Рік	Грошовий потік CF, грн	Коефіцієнт дисконтування $1/(1+i)^t$	Дисконтований CF, грн	Накопичений NPV, грн
0	−165847	1,000	−165847	−165847
1	156791	0,833	130611	−35236
2	156791	0,694	108813	73577
3	156791	0,579	90762	164339
4	156791	0,482	75533	239872
5	156791	0,402	63010	302882

За п'ять років NPV проєкту складає 302882 грн, що є суттєво більшим за нуль – проєкт є економічно привабливим. Показник рентабельності інвестицій розраховується за формулою:

$$ROI = \frac{AP}{(INV_1 + INV_2)/2} \times 100\%, \quad (3.3)$$

де AP – середньорічний чистий прибуток (економія) 156791 грн,

$INV_1 = 165847$ грн – початкові інвестиції,

$INV_2 = 0$ – залишкова вартість наприкінці горизонту.

$$ROI = 156791/(165847/2) \times 100 = 189\,\%.$$

Таке значення ROI значно перевищує мінімально прийнятний рівень рентабельності (20-25%), що підтверджує високу економічну ефективність проєкту [8].

Дисконтований термін окупності (DPP) визначається з таблиці 3.5 як момент, коли накопичений NPV змінює знак із від'ємного на додатній. Це відбувається між першим та другим роками. Точний термін окупності становить приблизно 1 рік і 4 місяці, що є відмінним показником для проєктів у галузі телекомунікаційної інфраструктури. На рисунку 3.5 наведено графік зміни накопиченого NPV проєкту протягом горизонту планування.

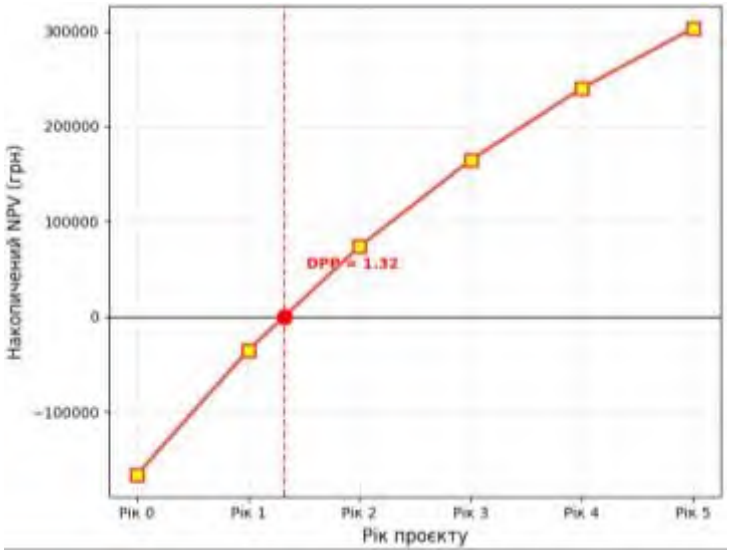

Рисунок 3.5 – Динаміка накопиченого NPV проєкту впровадження корпоративної VPN-мережі

Таким чином, було розроблено програмний комплекс мовою Python для моделювання продуктивності корпоративної VPN-мережі на основі аналітичних моделей M/M/1 та M/M/1/K і імітаційної моделі SimPy; виконано аналіз характеристик якості обслуговування, що підтвердив повну відповідність спроектованої мережі вимогам QoS: середня затримка пакета становить 0,526 мс (у 95 разів менше допустимого порогу), ймовірність втрати пакетів – $1{,}58 \times 10^{-6}$ при допустимих 0,01, а запас пропускної здатності каналу становить близько 19 Мбіт/с, достатній для розширення мережі; техніко-економічне обґрунтування підтвердило високу ефективність проєкту: NPV за п'ять років складає понад 302 тис. грн, ROI – 189%, дисконтований термін окупності – близько 1 року і 4 місяців.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнута її початкова мета та вирішені всі поставлені завдання. Проведено аналіз наукової, технічної та нормативної літератури з теми побудови корпоративних VPN-мереж, методів криптографічного захисту та програмних засобів моделювання мережевої продуктивності.

Розглянуто архітектуру та протоколи сучасних VPN-мереж, включаючи IPsec, L2TP/IPsec, OpenVPN, WireGuard та DMVPN. Проаналізовано їх функціональні можливості, переваги та недоліки, що дозволило обґрунтувати вибір технології DMVPN на базі протоколів mGRE та IPsec як оптимального рішення для корпоративної мережі з розподіленою структурою. Досліджено методи криптографічного захисту – алгоритми AES-256-GCM та ChaCha20-Poly1305, протоколи автентифікації IKEv2 та інфраструктуру відкритих ключів PKI – і підтверджено їх відповідність вимогам стандарту ДСТУ ISO/IEC 27001:2023. Виконано порівняльний огляд програмних засобів моделювання мережевої продуктивності (NS-3, GNS3, MATLAB, Python/SimPy), за результатами якого обрано комбінацію Python із бібліотеками SimPy та SciPy як оптимальний інструментарій для реалізації моделі.

Спроектовано корпоративну VPN-мережу інтернет-провайдера з двома географічно розподіленими офісами та загальною кількістю 29 співробітників. Визначено функціональні та нефункціональні вимоги до інфраструктури, обґрунтовано вибір топології «зірка» з динамічною маршрутизацією OSPF, обрано активне мережеве обладнання класу Cisco 2901 та D-Link DES-3200-28. Виконано розрахунок необхідної пропускної здатності міжофісного каналу: з урахуванням коефіцієнта одночасності 0,65 та накладних витрат VPN-шифрування 1,15 мінімально необхідне значення склало 26 Мбіт/с, для практичної реалізації обрано канал 52 Мбіт/с. Детально описано конфігурацію маршрутизаторів в операційній системі Cisco IOS, включаючи налаштування DMVPN, IPsec та OSPF.

Розроблено програмний комплекс мовою Python, що реалізує аналітичні моделі M/M/1 та M/M/1/K і імітаційну модель на базі SimPy. Верифікація моделі підтвердила її коректність: відхилення між аналітичними та імітаційними результатами не перевищує 0,03%, закон Літтла виконується з точністю до шостого знаку, коефіцієнт варіації між п'ятьма незалежними прогонами становить лише 0,186%. За результатами моделювання встановлено, що при інтенсивності навантаження ρ=0,533 середня затримка пакета складає 0,526 мс, що у 95 разів менше допустимого порогу 50 мс для IP-телефонії; ймовірність втрати пакетів дорівнює $1{,}58 \cdot 10^{-6}$ при допустимих 0,01; середня довжина черги становить 0,607 пакетів. Усі QoS-вимоги виконуються з великим запасом, а аналіз чутливості показав, що критичний рівень навантаження, при якому порушуються вимоги до втрат пакетів, відповідає $\rho \approx 0{,}9$, тобто запас становить близько 19 Мбіт/с додаткового трафіку.

Техніко-економічне обґрунтування підтвердило високу економічну ефективність проєкту. Загальні капітальні витрати на впровадження склали 165847 грн, річна економія порівняно з орендою виділеного каналу – 156791 грн. Чиста теперішня вартість за п'ятирічний горизонт планування при ставці дисконтування 20% становить 302882 грн, рентабельність інвестицій ROI – 189%, дисконтований термін окупності – близько 1 року і 4 місяців, що є відмінними показниками для проєктів телекомунікаційної інфраструктури.

Таким чином, поставлені завдання вирішені у повному обсязі. Напрямками подальших досліджень є розширення моделі для врахування неоднорідного трафіку з пріоритетним обслуговуванням (моделі M/G/1 та системи з кількома класами заявок), дослідження впливу пакетних втрат та джиттера на якість VoIP-сервісів засобами імітаційного моделювання, а також інтеграція розробленого програмного комплексу з системами моніторингу мережі реального часу для автоматичного прогнозування перевантажень та підтримки рішень щодо масштабування інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a virtual private network (VPN). URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html (дата звернення: 05.05.2026).

2. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство*. 2023. № 56. URL: https://doi.org/10.32782/2524-0072/2023-56-118 (дата звернення: 05.04.2026).

3. Чепурна І. С. Метод організації захищеного сегмента приватних SDN-мереж на основі протоколу Bittorrent. *Вісник Херсонського національного технічного університету*. 2025. Т. 2, № 3(94). С. 515–525. URL: https://doi.org/10.35546/kntu2078-4481.2025.3.2.66 (дата звернення: 05.05.2026).

4. OpenVPN. URL: https://openvpn.net/community-resources/openvpn-protocol/ (дата звернення: 05.05.2026).

5. Мілєвський О. А., Міночкін Д. А. Порівняння протоколів шифрування у корпоративній мережі. *Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій»*, (*ПТ-2022*), 11-15 квітня 2022 р., м. Київ, 2022, С. 167–170. URL: https://conferenc-journal.its.kpi.ua/article/view/328513 (дата звернення: 05.05.2026).

6. Knyazev V., Lazurenko B., Serkov A. Methods and tools for assessing the level of noise immunity of wireless communication channels. *Innovative Technologies and Scientific Solutions for Industries*. 2022. No. 1 (19). P. 92–98. URL: https://doi.org/10.30837/itssi.2022.19.092 (дата звернення: 05.05.2026).

7. WireGuard: Next Generation Secure Kernel Network Tunnel. URL: https://archive.fosdem.org/2017/schedule/event/wireguard/ (дата звернення: 05.05.2026).

8. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Київ: УкрНДНЦ, 2023. 45 с. URL:

https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398 (дата звернення: 05.05.2026).

9. IKEv2/IPsec: Secure VPN protocols explained. URL: https://nordvpn.com/uk/blog/ikev2ipsec/ (дата звернення: 05.05.2026).

10. Types of AES-256 Encryption: Complete Guide to Modes, Uses & Pitfalls. URL: https://terrazone.io/aes-256-encryption-types/ (дата звернення: 05.05.2026).

11. Міжмережевий екран нового покоління NGFW що це і навіщо він потрібен. URL: https://westelecom.ua/blog/mezsetevoj-ekran-novogo-pokolenia-ngfw-cto-eto-i-zacem-on-nuzen (дата звернення: 05.05.2026).

12. Giambene G. Queuing Theory and Telecommunications. Cham : Springer International Publishing, 2021. 413 P. URL: https://doi.org/10.1007/978-3-030-75973-5 (дата звернення: 05.05.2026).

13. Wang Y. Research on the Queuing Theory based on M/M/1 Queuing Model. *Highlights in Science, Engineering and Technology*. 2023. Vol. 61. P. 80–87. URL: https://doi.org/10.54097/hset.v61i.10276 (дата звернення: 05.05.2026).

14. Vishvakarma T. A Review of Modern Computer Networks. *International Journal for Research in Applied Science and Engineering Technology*. 2022. Vol. 10, no. 9. P. 368–376. URL: https://doi.org/10.22214/ijraset.2022.46637 (дата звернення: 05.05.2026).

15. Performance assessment of the impact of the encryption layer on a highly available campus network / N. Morsli et al. *Procedia Computer Science*. 2024. Vol. 238. P. 572–577. URL: https://doi.org/10.1016/j.procs.2024.06.062 (дата звернення: 05.05.2026).

16. GNS3. Version 2.2.57. Your Virtual Network in a Suitcase. URL: https://www.gns3.com/software (дата звернення: 05.05.2026).

17. Getting Started with GNS3. URL: https://docs.gns3.com/docs/ (дата звернення: 05.05.2026).

18. SimPy. Discrete event simulation for Python. URL: https://simpy.readthedocs.io/en/latest/ (дата звернення: 05.05.2026).

19. MATLAB Communications Toolbox. URL: https://www.mathworks.com/products/communications.html (дата звернення: 05.05.2026).

21. Scipy. Fundamental algorithms for scientific computing in Python. URL: https://scipy.org/about/ (дата звернення: 05.05.2026).

22. Хто такий провайдер і звідки він бере інтернет: простими словами про роботу провайдера. URL: https://ipnet.ua/blog/khto-takyi-provaider-i-zvidky-vin-bere-internet-prostymy-slovamy-pro-robotu-provaidera (дата звернення: 05.05.2026).

23. Що таке білінг, та як працює білінгова система. URL: https://whitepay.com/uk/news/what-is-billing-and-how-does-the-billing-system-work (дата звернення: 05.05.2026).

24. ITU-T G.114: One-way transmission time . URL: https://www.itu.int/rec/T-REC-G.114/en (дата звернення: 05.05.2026).

25. Cisco DMVPN - Concepts & Configuration. URL: https://learningnetwork.cisco.com/s/article/dmvpn-concepts-amp-configuration (дата звернення: 05.05.2026).

25. Dynamic Multipoint VPN Configuration Guide, Cisco IOS XE Everest 16.6. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16-6/sec-conn-dmvpn-xe-16-6-book/sec-conn-dmvpn-mtt.html (дата звернення: 05.05.2026).

26. What is GRE tunneling? How GRE protocol works. URL: https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/ (дата звернення: 05.05.2026).

27. Cisco 2900 Integrated Services Router. URL: https://www.cisco.com/c/en/us/support/routers/2900-series-integrated-services-routers-isr/series.html (дата звернення: 05.05.2026).

28. Комутатор мережевий D-Link DES-3200-28. URL: https://brain.com.ua/ukr/Komutator_merejheviy_D-Link_DES-3200-28-p43758.html (дата звернення: 05.05.2026).

29. Structured Cabling Standards Explained. URL: https://www.telco-data.com/blog/structured-cabling-standards/ (дата звернення: 05.05.2026).

30. МВ 42.1-37641918-794:2024 Методичні вказівки зі складання кошторису видатків на утримання служби замовника та визначення розміру коштів на її утримання під час виконання робіт з відновлення та розвитку

інфраструктури. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=114086 (дата звернення: 05.05.2026).

31. How to Calculate Network Load and Needs for Business. URL: https://versatech.com.ph/calculate-network-load/ (дата звернення: 05.05.2026).

32. Kovalenko A., Kuchuk H., Tkachov V. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. *Системи управління, навігації та зв'язку. Збірник наукових праць*. 2021. Т. 1, № 63. С. 90–95. URL: https://doi.org/10.26906/sunz.2021.1.090 (дата звернення: 05.05.2026).