**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 корпоративної інформаційної системи з VPN за допомогою MATLAB»**

Виконала: здобувачка вищої освіти
за освітньою програмою
Інформаційні управляючі системи
спеціальності 126 Інформаційні
системи та технології
ступеня вищої освіти бакалавр
групи 126ІСТ_бз_2022
Галата Вікторія Дмитрівна
Керівник: Уткін Юрій Вікторович
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

**Галаті Вікторії Дмитрівні**

1. Тема роботи:
«Моделювання корпоративної інформаційної системи з VPN за допомогою MATLAB»,
керівник роботи к.т.н., доцент, завідувач кафедри інформаційних систем та технологій Уткін Юрій Вікторович.
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 у сфері інформаційної безпеки та мережевого моделювання (ДСТУ ISO/IEC 27001:2023, ITU-T Y.1541, RFC 3393, RFC 7296); дані офіційних сайтів https://www.mathworks.com/ (MATLAB, Communications Toolbox, Statistics and Machine Learning Toolbox), https://www.strongswan.org/ (strongSwan IPsec), https://wiki.mikrotik.com/ (MikroTik).

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

Розділ 1. Аналіз архітектури корпоративних інформаційних систем з VPN
Розділ 2. Розробка моделі корпоративної інформаційної системи з VPN у MATLAB
Розділ 3. Практична реалізація та оцінка ефективності системи

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** **Вікторія ГАЛАТА**

**Керівник роботи** **Юрій УТКІН**

**ЗМІСТ**

ВСТУП ..... 6
РОЗДІЛ 1 АНАЛІЗ АРХІТЕКТУРИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ З VPN ..... 9
1.1 Структура корпоративних інформаційних систем та вимоги до їх захищеності ..... 9
1.2 Огляд технологій побудови VPN та їх порівняльний аналіз ..... 12
1.3 Показники якості функціонування VPN-мереж та методи їх оцінювання ..... 16
1.4 Постановка задачі моделювання та вибір інструментарію ..... 19
РОЗДІЛ 2 РОЗРОБКА МОДЕЛІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ З VPN У MATLAB ..... 24
2.1 Опис архітектури модельованої корпоративної мережі ..... 24
2.2 Математична модель каналів передачі даних з урахуванням шифрування ..... 26
2.3 Імітаційна модель передачі захищеного трафіку ..... 30
2.4 Аналіз результатів моделювання та дослідження сценаріїв навантаження ..... 33
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ ..... 39
3.1 Розробка рекомендацій щодо впровадження захищеної корпоративної мережі ..... 39
3.2 Верифікація моделі шляхом порівняння з еталонними та аналітичними результатами ..... 42
3.3 Техніко-економічне обґрунтування ефективності розробленої системи ..... 44
ВИСНОВКИ ..... 48
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ..... 50
ДОДАТКИ ..... 55

# ВСТУП

*Актуальність.* Цифрова трансформація підприємств в Україні набуває дедалі більшого значення в умовах воєнного стану, масового переходу на дистанційну роботу та зростання кількості кіберзагроз. Забезпечення захищеного зв'язку між географічно розподіленими офісами стало критичною вимогою для збереження безперервності бізнес-процесів. За даними CERT-UA, у 2024 році кількість зафіксованих кіберінцидентів зросла на 69,8% порівняно з попереднім роком, а корпоративні мережі залишаються однією з основних цілей атак [1, 4]. У цьому контексті технологія VPN (Virtual Private Network) є базовим інструментом захисту корпоративних комунікацій, що забезпечує конфіденційність, цілісність та автентифікацію переданих даних відповідно до вимог ДСТУ ISO/IEC 27001:2023 [3].

Водночас проектування VPN-інфраструктури без попереднього моделювання несе ризики неправильного вибору параметрів – надмірного або недостатнього резервування пропускної здатності, некоректного налаштування буферів та черг. Ці помилки безпосередньо впливають на затримку, джиттер і втрати пакетів, що є критичними для VoIP та відеоконференцзв'язку [3, 4]. Моделювання засобами MATLAB дозволяє оцінити характеристики якості обслуговування VPN-мережі ще до її фізичного розгортання, скоротити витрати на тестове обладнання та обґрунтувати параметри конфігурації кількісними методами. Це визначає актуальність розробки математичної та імітаційної моделі корпоративної інформаційної системи з VPN на основі теорії масового обслуговування.

*Метою кваліфікаційної роботи* є розробка та дослідження моделі корпоративної інформаційної системи з VPN у середовищі MATLAB, що забезпечує кількісну оцінку показників якості обслуговування мережі та обґрунтування оптимальних параметрів конфігурації захищеного з'єднання.

Відповідно до мети роботи необхідно вирішити наступні *завдання:*

1. Провести аналіз архітектури корпоративних інформаційних систем з VPN, технологій побудови захищених каналів та методів оцінювання їх якісних характеристик;

2. Розробити математичну модель VPN-каналу з урахуванням накладних витрат протоколу IPsec на основі апарату теорії масового обслуговування та реалізувати її аналітичну частину у MATLAB;

3. Реалізувати імітаційну дискретно-подієву модель VPN-тунелю (M/M/1/K) у MATLAB та провести серію чисельних експериментів для оцінки показників затримки, джиттеру, втрат пакетів і пропускної здатності в різних режимах навантаження;

4. Розробити практичні рекомендації щодо впровадження захищеної корпоративної мережі, верифікувати модель та виконати техніко-економічне обґрунтування ефективності розробленої системи.

*Об'єкт дослідження* – процеси передачі захищеного трафіку у корпоративній інформаційній системі з VPN на основі протоколу IPsec/IKEv2.

*Предмет дослідження* – математична та імітаційна модель корпоративної інформаційної системи з VPN, реалізована у MATLAB, та показники якості її функціонування.

*Методи досліджень* – дослідження базуються на методах теорії масового обслуговування (моделі M/M/1 та M/M/1/K, закон Літтла, формула Ерланга), імітаційного моделювання методом дискретно-подієвої симуляції, математичної статистики (довірчі інтервали, перцентильний аналіз), а також порівняльного аналізу протоколів мережевої безпеки та техніко-економічного аналізу IT-проєктів.

*Інформаційна база* – наукові статті та монографії з теорії масового обслуговування і мережевого моделювання, стандарти ДСТУ ISO/IEC 27001:2023 та ITU-T Y.1541, RFC 3393 і RFC 7296, документація MATLAB (Communications Toolbox, Statistics and Machine Learning Toolbox), звіти CERT-

UA про кіберінциденти, матеріали технічних специфікацій протоколів IPsec/IKEv2 та WireGuard.

*Практична значущість* – розроблена модель може бути використана у навчальному процесі підготовки бакалаврів зі спеціальності 126 «Інформаційні системи та технології» для вивчення методів мережевого моделювання, а також як інструмент попереднього проектування корпоративних VPN-мереж. Модульна архітектура (окремі файли для аналітичної моделі, симуляції, серії експериментів та побудови графіків) і параметризація через файл config.json забезпечують легке адаптування до різних конфігурацій мережі без модифікації програмного коду. Результати моделювання підтверджують, що для мережі з каналом 100 Мбіт/с оптимальна робоча інтенсивність трафіку не повинна перевищувати 65.5 Мбіт/с ($\rho \leq 0.75$), що є практично значущою рекомендацією для системних адміністраторів корпоративних мереж.

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 54 сторінки формату А4. Вона містить 11 рисунків і 12 таблиць.

# РОЗДІЛ 1
# АНАЛІЗ АРХІТЕКТУРИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ З VPN

## 1.1 Структура корпоративних інформаційних систем та вимоги до їх захищеності

Корпоративна інформаційна система (КІС) – це інформаційна система, яка підтримує автоматизацію функцій управління на підприємстві та постачає інформацію для прийняття управлінських рішень, поєднуючи бізнес-стратегію організації з сучасними інформаційними технологіями. У сучасних умовах КІС є базовим елементом цифрової інфраструктури будь-якого підприємства – від промислових компаній до закладів освіти та державних установ [1].

Типова схема КІС із VPN-підключенням для українського підприємства наведена на рисунку 1.1.


Рисунок 1.1 – Архітектура корпоративної інформаційної системи з VPN

Архітектура КІС середнього та великого підприємства в Україні, як правило, охоплює три рівні: рівень кінцевих користувачів (робочі станції,

мобільні пристрої, термінали), рівень корпоративних додатків (ERP, CRM, документообіг, поштові сервери) та рівень мережевої інфраструктури (маршрутизатори, комутатори, міжмережеві екрани). При цьому географічно розподілені підприємства – ті, що мають центральний офіс і кілька філій або використовують дистанційну роботу – потребують механізмів захищеного міжвузлового з'єднання. Саме таким механізмом слугує технологія VPN (Virtual Private Network). Корпоративна VPN-мережа дає змогу компаніям створити приватну мережу, ізольовану від публічного інтернету, і забезпечити надійний захищений доступ до внутрішніх ресурсів, що особливо актуально для компаній із розгалуженими командами, IoT-пристроями або віддаленими офісами.

Питання захищеності КІС в Україні регулюються насамперед Законом України «Про захист інформації в інформаційно-комунікаційних системах» [2], який визначає об'єкти захисту, права та обов'язки власників систем і повноваження регуляторів. Під час дії воєнного стану вимоги щодо захисту інформації в інформаційно-комунікаційних системах не змінюються, і відповідальність за забезпечення захисту інформації в системі лежить на власнику системи; при цьому компанія може будувати систему інформаційної безпеки відповідно до стандартів ISO/IEC 27 серії з урахуванням вимог зазначеного Закону. На національному рівні діє стандарт ДСТУ ISO/IEC 27001:2023, прийнятий наказом від 17.08.2023 № 210, який встановлює вимоги до систем керування інформаційною безпекою в галузі кібербезпеки та захисту конфіденційності [3].

Актуальність захищеної мережевої інфраструктури для вітчизняних підприємств різко зросла в умовах повномасштабного збройного вторгнення. За даними CERT-UA, у 2024 році фахівці опрацювали 4315 кіберінцидентів – на 69,8% більше, ніж у 2023 році, коли було зафіксовано 2541 кіберінцидент. Метою атак є насамперед викрадення чутливих корпоративних даних та знищення IT-систем. Сучасні кібератаки на Україну часто синхронізуються з фізичними ударами по інфраструктурі, а масштаби автоматизованих атак зросли з 567 атак за секунду в 2021 році до 7000 атак за секунду в 2024 році. Це означає, що будь-

яке підприємство, яке не забезпечує шифрування корпоративного трафіку, фактично залишає свої дані незахищеними [4].

До основних вимог, яким повинна відповідати корпоративна інформаційна система з VPN для умов українського підприємства, належать: конфіденційність переданих даних (шифрування всього трафіку між вузлами), цілісність даних (виявлення несанкціонованих змін у пакетах), автентичність сторін з'єднання (перевірка справжності вузлів), доступність (мінімальний час простою VPN-тунелю), а також масштабованість і керованість (можливість динамічного підключення нових вузлів) [5]. Ці вимоги безпосередньо кореспондуються з вимогами стандарту ISO/IEC 27001:2022 в частині управління ризиками мережевої безпеки. Зведену характеристику основних функціональних вимог до корпоративної VPN-системи наведено в таблиці 1.1.

Таблиця 1.1 – Функціональні вимоги до корпоративної VPN-системи

| Вимога | Зміст | Нормативна основа |
|---|---|---|
| Конфіденційність | Шифрування даних між усіма вузлами мережі | ДСТУ ISO/IEC 27001:2023, ст. А.8.20 |
| Цілісність | Контроль хеш-суми пакетів (HMAC) | ISO/IEC 27001:2022, A.8.16 |
| Автентичність | Взаємна автентифікація шлюзів і клієнтів | Закон України № 80/94-ВР, ст. 4 |
| Доступність | Резервування каналів, SLA ≥ 99,5% | ДСТУ ISO/IEC 27001:2023, A.8.14 |
| Масштабованість | Підтримка динамічного підключення вузлів | Технічні вимоги провайдера |

Для кількісної оцінки навантаження на VPN-тунель важливою характеристикою є коефіцієнт використання каналу. За умови пуассонівського потоку пакетів він визначається як:

$$\rho = \frac{\lambda}{\mu}, \tag{1.1}$$

де $\lambda$ – інтенсивність вхідного потоку пакетів (пакетів/с),

$\mu$ – продуктивність каналу (пакетів/с).

При $\rho \geq 1$ мережа перевантажена, що безпосередньо впливає на якість VPN-з'єднання [6]. Поширення дистанційної роботи спровокувало зростання атак на VPN-системи на 238% між 2020 і 2022 роками, оскільки зловмисники активно експлуатували вразливості та неправильні конфігурації [7]. Це підкреслює необхідність не лише розгортання VPN-інфраструктури, а й її ретельного проектування з урахуванням актуальних загроз. Моделювання такої системи засобами MATLAB дозволяє ще на етапі проектування виявити вузькі місця у пропускній здатності та оцінити стійкість до навантажень, що й становить мету цієї роботи.

## 1.2 Огляд технологій побудови VPN та їх порівняльний аналіз

Технологія VPN (Virtual Private Network) є основним засобом організації захищених каналів зв'язку між географічно розподіленими вузлами корпоративної інформаційної системи. Протоколи VPN визначають порядок шифрування, автентифікації та передачі даних між клієнтом і сервером, а їх вибір безпосередньо впливає на продуктивність, рівень безпеки та зручність адміністрування мережі [8]. На сьогоднішній день у корпоративних рішеннях домінують три сімейства протоколів: IPsec/IKEv2, OpenVPN та WireGuard.

Протокол IPsec (Internet Protocol Security) є стандартом IETF і функціонує на мережевому рівні моделі OSI, забезпечуючи захист усіх вищих рівнів без модифікації прикладного програмного забезпечення [9]. Архітектура IPsec складається з двох транспортних підпротоколів – AH (Authentication Header) та ESP (Encapsulating Security Payload) – і протоколу обміну ключами IKE/IKEv2. Протокол AH забезпечує автентифікацію та цілісність даних, захищаючи весь пакет, включаючи заголовок IP. Протокол ESP реалізує шифрування корисного навантаження та додатково забезпечує автентифікацію. IPsec підтримує два режими роботи. Транспортний режим використовується для шифрування лише

поля даних IP-пакета, тоді як тунельний режим застосовується переважно у VPN-рішеннях і забезпечує захист усього пакета шляхом його інкапсуляції в новий IP-пакет, де адреси зовнішнього заголовка вказують кінцеві точки тунелю. Для корпоративних мереж site-to-site застосовується виключно тунельний режим, оскільки він дозволяє приховати реальні адреси внутрішніх хостів від зовнішніх спостерігачів. Структуру пакету ESP у тунельному режимі ілюструє рисунок 1.2.


Рисунок 1.2 – Структура пакету ESP у тунельному режимі IPsec

Протокол IKEv2 (Internet Key Exchange version 2) використовується для автоматичного узгодження параметрів безпеки (SA – Security Association) між двома вузлами та управління сеансовими ключами. Ключовою особливістю IKEv2 є підтримка MOBIKE (Mobility and Multihoming Protocol), що дозволяє зберігати VPN-з'єднання при переключенні між мережами, наприклад з Wi-Fi на мобільний інтернет, без переривання з'єднання. Типова швидкість IKEv2/IPsec становить 300-600 Мбіт/с, що робить його швидшим за OpenVPN, проте повільнішим за WireGuard.

OpenVPN – добре відома технологія з відкритим вихідним кодом, що відзначається широкими можливостями конфігурації та надійною роботою. Вона підтримує режими UDP (дещо швидший) та TCP (більш надійний з точки зору доставки пакетів). OpenVPN функціонує у просторі користувача, що спрощує крос-платформне розгортання, але обумовлює вищі накладні витрати порівняно з рішеннями на рівні ядра [10].

WireGuard – сучасний протокол, вбудований у ядро Linux починаючи з версії 5.6 (2020 р.). WireGuard застосовує криптографічні алгоритми ChaCha20 та Poly1305, що забезпечують стійкість до сучасних криптографічних атак, а кодова база протоколу складає лише близько 4000 рядків, що робить його легко перевірним та надійним. Накладні витрати WireGuard на пакет становлять лише 32 байти понад UDP/IP-заголовки, тоді як у OpenVPN аналогічний показник перевищує 69 байтів. Порівняльний аналіз протоколів за ключовими характеристиками наведено у таблиці 1.2.

Таблиця 1.2 – Порівняльний аналіз протоколів VPN

| Характеристика | IPsec/IKEv2 | OpenVPN | WireGuard |
|---|---|---|---|
| Рівень OSI | Мережевий (L3) | Прикладний (L7) | Мережевий (L3) |
| Алгоритм шифрування | AES-256-GCM | AES-256/ChaCha20 | ChaCha20-Poly1305 |
| Швидкість (500 Мбіт/с канал) | 350–450 Мбіт/с | 300–420 Мбіт/с | 440–480 Мбіт/с |
| Накладні витрати на пакет | ~60–80 байт | 69+ байт | ~32 байти |
| Підтримка мобільності (MOBIKE) | Так | Ні | Часткова |
| Вбудована підтримка ОС | Windows, macOS, iOS, Android | Потребує клієнта | Linux-ядро, клієнти |
| Складність налаштування | Висока | Середня | Низька |
| Актуальність для корпоративних рішень | Висока | Висока | Зростає |

Окремо слід розглянути топології побудови VPN-мереж. Схема site-to-site (мережа-до-мережі) поєднує постійним зашифрованим тунелем два або більше

корпоративних офіси; ця топологія найбільш поширена для з'єднання головного офісу з філіями. Схема remote access (віддалений доступ) забезпечує підключення окремих мобільних співробітників до корпоративної мережі через VPN-клієнт. DMVPN (Dynamic Multipoint VPN) є гібридною схемою, яка дозволяє динамічно створювати прямі тунелі між філіями без проходження через центральний вузол, що зменшує затримку у розподілених мережах [11].

Ефективність передачі даних у VPN-тунелі зручно оцінювати через коефіцієнт корисного навантаження пакету:

$$\eta = \frac{L_{payload}}{L_{payload} + L_{overhead}}, \tag{1.2}$$

де $L_{payload}$ – розмір корисних даних у пакеті (байт),

$L_{overhead}$ – сумарні накладні витрати протоколу (байт).

Для IPsec у тунельному режимі з ESP значення $L_{overhead}$ залежить від обраного алгоритму шифрування та, як правило, становить 60-80 байт; для WireGuard – близько 32 байт [12]. При малих пакетах (64 байти) втрати ефективності є суттєвими і повинні враховуватися при проектуванні моделі.

Дослідження порівняльної продуктивності WireGuard та IPsec показують, що WireGuard стабільно досягає вищих показників пропускної здатності, тоді як IPsec при підвищеному навантаженні демонструє більше споживання ресурсів процесора, що негативно впливає на його продуктивність. Водночас IPsec/IKEv2 залишається галузевим стандартом для корпоративних рішень завдяки широкій підтримці апаратних прискорювачів шифрування (AES-NI), сумісності з обладнанням провідних виробників та детально прописаній нормативній базі [9]. Саме тому в даній роботі для моделювання корпоративної КІС обрано протокол IPsec у тунельному режимі з IKEv2 як найбільш відповідний вимогам вітчизняних підприємств з точки зору безпеки, сумісності та відповідності вимогам ДСТУ ISO/IEC 27001:2023.

## 1.3 Показники якості функціонування VPN-мереж та методи їх оцінювання

Оцінювання функціональних характеристик VPN-інфраструктури є необхідною умовою проектування надійної корпоративної інформаційної системи. Ключовими метриками, що визначають якість обслуговування (QoS) мережі, є пропускна здатність, затримка, джиттер та коефіцієнт втрати пакетів. Стандартні підходи до оцінки мережевої продуктивності зазвичай базуються на окремих показниках, таких як затримка, втрати пакетів та джиттер, проте вони не завжди дозволяють отримати повне уявлення про загальну продуктивність мережі, особливо в умовах різноманітного трафіку. Тому ефективне моделювання системи потребує аналізу всіх зазначених показників у взаємозв'язку [16].

Пропускна здатність (throughput) – це фактичний обсяг даних, що передаються через VPN-тунель за одиницю часу. На відміну від номінальної смуги пропускання каналу, пропускна здатність завжди менша через накладні витрати протоколу шифрування, службові заголовки та механізми аутентифікації. Затримка (latency) є сумою кількох складових: часу поширення сигналу фізичним середовищем, часу обробки пакету на маршрутизаторах і часу очікування пакету у черзі. Джиттер (jitter) – це варіація затримки між послідовними пакетами, що критично впливає на якість VoIP, відеоконференцій і реального часу передачі, які є невід'ємними частинами корпоративних КІС. Якщо пакети потрапляють до одержувача з нерівномірним інтервалом, мережа вносить джиттер у потік пакетів; така варіація формується здебільшого в результаті різних затримок у чергах на вузлах з комутацією пакетів.

Для математичного моделювання трафіку VPN-мережі широко застосовують теорію масового обслуговування (ТМО). VPN-шлюз розглядається як система масового обслуговування (СМО), у якій вхідний потік пакетів відповідає пуассонівській моделі, а час обробки кожного пакету (включаючи шифрування ESP та обчислення HMAC) є випадковою експоненційно

розподіленою величиною [17]. Базовою моделлю для одноканальної черги є M/M/1, яка описує поведінку одного VPN-тунелю при заданому навантаженні.

Відповідно до закону Літтла, середня кількість пакетів у системі масового обслуговування пов'язана з параметрами потоку таким чином [18]:

$$L = \lambda \cdot W, \tag{1.3}$$

де $L$ – середня кількість пакетів у системі,

$\lambda$ – інтенсивність вхідного потоку (пакетів/с),

$W$ – середній час перебування пакету в системі (с).

Зі збільшенням навантаження $\rho = \lambda / \mu$ (де $\mu$ – продуктивність каналу) середній час перебування у системі M/M/1 зростає нелінійно: при $\rho \to 1$ затримка прямує до нескінченності, що вимагає проектування системи з певним запасом пропускної здатності. На рисунку 1.3 показано залежність нормованої затримки $W \cdot \mu$ від коефіцієнта завантаження $\rho$ для моделі M/M/1, що ілюструє різке зростання часу очікування при завантаженні понад 70-80%.

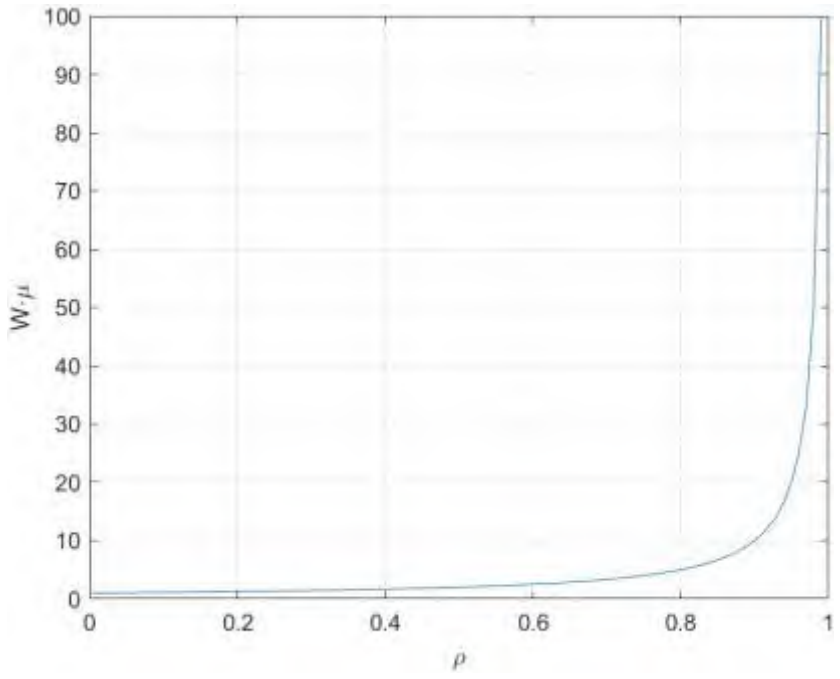


Рисунок 1.3 – Залежність нормованої затримки від коефіцієнта завантаження в моделі M/M/1

Залежність, зображена на рисунку 1.3, є теоретичним обґрунтуванням необхідності обмежувати завантаження VPN-шлюзу на рівні не більше 70-75% від максимальної пропускної здатності – практичне правило, що широко використовується при проектуванні корпоративних мереж.

Для оцінки показників QoS та верифікації аналітичних результатів застосовуються програмні засоби вимірювання мережевих параметрів. Утиліта iPerf3 дозволяє вимірювати пропускну здатність та джиттер реального VPN-тунелю, Wireshark забезпечує захоплення та аналіз пакетів на рівні протоколу. Проте для системного проектування та дослідження сценаріїв навантаження до фізичного розгортання системи необхідне середовище математичного моделювання. Порівняльну характеристику методів оцінювання показників VPN-мережі наведено у таблиці 1.3.

Таблиця 1.3 – Порівняльна характеристика методів оцінювання показників VPN-мережі

| Метод | Інструменти | Переваги | Обмеження |
|---|---|---|---|
| Аналітичний (ТМО) | Формули M/M/1, M/M/c | Швидкий результат, аналіз граничних режимів | Спрощені припущення, відсутність деталізації пакетного рівня |
| Імітаційне моделювання | MATLAB/Simulink | Реалістична поведінка, гнучке налаштування | Потребує верифікації, обчислювальні ресурси |
| Вимірювання на реальній мережі | iPerf3, Wireshark | Точні реальні дані | Потребує фізичної інфраструктури, складно варіювати параметри |

Середовище MATLAB є потужним інструментом для вирішення таких задач. MATLAB забезпечує дискретно-подієву симуляцію на рівні пакетів та подій для моделювання планування, черг, повторних передач та розподілу ресурсів, а також надає вбудовані засоби для оцінки затримки, пропускної здатності, втрати пакетів та інших ключових метрик. Simulink разом із Communications Toolbox дозволяє будувати блок-схемні моделі каналів зв'язку з налаштованими параметрами шифрування, генераторами трафіку та блоками

статистичного аналізу [19]. Statistics and Machine Learning Toolbox забезпечує апарат для статистичної обробки результатів імітаційних експериментів – побудову довірчих інтервалів, перевірку гіпотез щодо відповідності теоретичним розподілам, регресійний аналіз залежностей метрик QoS від параметрів навантаження [20].

Симуляція в MATLAB дозволяє дослідити поведінку мережі в умовах нелінійних систем з різними алгоритмами управління навантаженням, а результати демонструють суттєві відмінності між різними стратегіями залежно від параметрів навантаження [16]. Таким чином, комбінування аналітичного підходу на основі ТМО з імітаційним моделюванням у MATLAB дозволяє отримати достовірні кількісні оцінки показників якості функціонування корпоративної VPN-системи ще до її фізичного розгортання, що і становить методологічну основу даної роботи.

## 1.4 Постановка задачі моделювання та вибір інструментарію

Для досягнення мети необхідно сформулювати конкретну задачу моделювання, визначити об'єкт дослідження та обґрунтувати вибір програмного засобу. Об'єктом моделювання в даній роботі є корпоративна інформаційна система із захищеним VPN-з'єднанням між географічно розподіленими офісами підприємства, що функціонує в умовах сучасної телекомунікаційної інфраструктури України.

Як типову для України мережу розглядається підприємство із головним офісом та двома філіями, розташованими в різних містах (наприклад, Київ – Харків – Львів). З точки зору топології побудови найбільш поширеними схемами є «точка–багатоточка» та «багатоточка–багатоточка». У схемі «точка–багатоточка» всі комунікації між з'єднаними локаціями проходять через центральний вузол, тоді як у схемі «багатоточка–багатоточка» можливі прямі комунікації між локаціями. У даній роботі обрано топологію «зірка» (hub-and-

spoke), за якої всі VPN-тунелі зводяться до головного шлюзу, – вона найбільш поширена для підприємств середнього масштабу і добре підходить для моделювання завдяки чіткій ієрархічній структурі [23]. Підключення до публічного Інтернету здійснюється через одного з операторів зв'язку, що надають послуги корпоративного VPN в Україні. Зокрема, Київстар надає послугу IP VPN, яка об'єднує два і більше територіально віддалених офіси в єдину захищену корпоративну мережу на базі MPLS з гарантованою пропускною здатністю від 1 Мбіт до 10 Гбіт. Структуру модельованої мережі показано на рисунку 1.4.

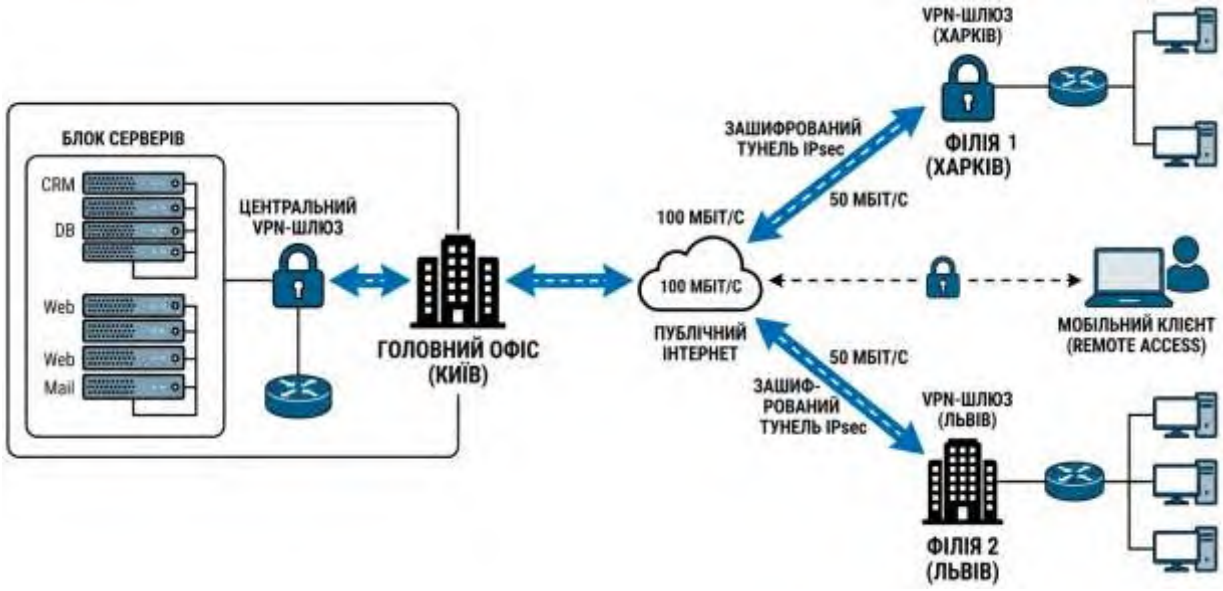


Рисунок 1.4 – Структура модельованої корпоративної мережі з VPN

Вихідні дані для моделювання формуються на основі реальних характеристик корпоративних мереж в Україні. Трафік моделюється як суперпозиція кількох класів: корпоративна електронна пошта (дрібні пакети, низька інтенсивність), обмін файлами та документами (великі пакети, пульсуючий характер) та VoIP/відеоконференцзв'язок (пакети фіксованого розміру, рівна інтенсивність, критичний до джиттеру). Параметри каналу включають затримку поширення між містами (орієнтовно 5-15 мс) та накладні витрати IPsec/IKEv2 у тунельному режимі.

Математична постановка задачі полягає у визначенні залежності показників якості функціонування (затримки $W$, пропускної здатності $\theta$, коефіцієнта втрати пакетів $P_{loss}$) від параметрів навантаження. Середнє значення часу перебування пакету в системі з врахуванням черг на VPN-шлюзі описується відомою формулою для моделі M/M/1 [18]:

$$W = \frac{1}{\mu - \lambda}, \tag{1.4}$$

де $\mu$ – продуктивність VPN-шлюзу (пакетів/с),

$\lambda$ – інтенсивність вхідного трафіку (пакетів/с).

Умова стійкості системи вимагає $\lambda < \mu$, що задає верхню межу допустимого навантаження. Зазначена формула буде використана у другому розділі для аналітичної верифікації результатів імітаційної моделі.

Основним програмним інструментом для виконання поставленої задачі обрано MATLAB. MATLAB – це мова інженерів і науковців, середовище програмування для розробки алгоритмів, аналізу даних, візуалізації та чисельних обчислень, тоді як Simulink є блок-схемним середовищем для симуляції та модельно-орієнтованого проектування багатодоменних інженерних систем. Для вирішення задачі в даній роботі залучатимуться такі компоненти:

Communications Toolbox надає алгоритми та застосунки для аналізу, проектування та наскрізної симуляції систем зв'язку. Алгоритми тулбоксу включають канальне кодування, модуляцію та OFDM, що дозволяє складати та моделювати фізичний рівень системи зв'язку. Для задач даної роботи він використовується для моделювання каналу передачі з втратами (erasure channel) та генерації трафіку пакетів.

Simulink забезпечує графічне моделювання VPN-тунелю як блок-схеми: генератор пакетів → блок шифрування (ESP overhead) → канал з затримкою та втратами → буфер черги → одержувач. Це дозволяє наочно налаштовувати параметри кожного елементу та спостерігати динаміку системи в реальному часі.

Statistics and Machine Learning Toolbox застосовується для статистичного аналізу результатів серії симуляційних експериментів. Тулбокс дозволяє апроксимувати розподіли ймовірностей до даних, генерувати випадкові числа для метода Монте-Карло та виконувати перевірку гіпотез. Це забезпечує побудову довірчих інтервалів для оцінок затримки та пропускної здатності при варіюванні параметрів навантаження.

Symbolic Math Toolbox надає можливість отримання аналітичних виразів для показників M/M/1-моделі та їх символьного диференціювання для пошуку оптимальних значень параметрів.

Зведений перелік параметрів моделі та їх числові значення, які будуть використані в моделях VPN-мережі, наведено у таблиці 1.4.

Таблиця 1.4 – Вихідні параметри модельованої корпоративної VPN-мережі

| Параметр | Позначення | Значення | Одиниці |
|---|---|---|---|
| Пропускна здатність каналу (головний офіс) | $C_{hub}$ | 100 | Мбіт/с |
| Пропускна здатність каналу (філія) | $C_{spoke}$ | 50 | Мбіт/с |
| Накладні витрати IPsec/ESP | $L_{oh}$ | 70 | байт/пакет |
| Затримка поширення (між містами) | $d_{prop}$ | 5–15 | мс |
| Середній розмір пакету | $\bar{L}$ | 512 | байт |
| Діапазон варіювання інтенсивності | $\lambda$ | 100–5000 | пакетів/с |
| Тривалість симуляції | $T_{sim}$ | 10 | с |

Параметри таблиці 1.4 ґрунтуються на характеристиках корпоративних Інтернет-каналів, що пропонують вітчизняні телекомунікаційні оператори, та на типових значеннях накладних витрат протоколу IPsec, встановлених у підрозділі 1.2 [23, 24]. Варіювання інтенсивності $\lambda$ у широкому діапазоні дозволить дослідити поведінку системи в нормальному, граничному та перевантаженому режимах.

Було проведено комплексний аналіз предметної галузі: розглянуто структуру та вимоги до захищеності корпоративних інформаційних систем підприємств України в умовах воєнного стану та зростаючих кіберзагроз; виконано порівняльний аналіз сучасних протоколів VPN (IPsec/IKEv2, OpenVPN, WireGuard), за результатами якого для моделювання обрано протокол

IPsec у тунельному режимі з IKEv2 як найбільш відповідний корпоративним вимогам та нормативній базі; обґрунтовано математичний апарат оцінювання показників якості функціонування VPN-каналів на базі теорії масового обслуговування (модель M/M/1, закон Літтла); сформульовано задачу моделювання, описано об'єкт дослідження (мережа «зірка» з трьома вузлами) та обґрунтовано вибір MATLAB як основного інструментарію для аналітичного та імітаційного моделювання системи.

# РОЗДІЛ 2
# РОЗРОБКА МОДЕЛІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ З VPN У MATLAB

## 2.1 Опис архітектури модельованої корпоративної мережі

Об'єктом моделювання у цій роботі є корпоративна інформаційна система підприємства середнього масштабу з трьома географічно розподіленими офісами на території України. Вибір саме такої конфігурації зумовлений тим, що вона є характерною для широкого кола вітчизняних підприємств – торгових мереж, виробничих компаній з філіями, університетів та державних установ. Топологія мережі відповідає схемі «зірка» (hub-and-spoke), у якій усі комунікації проходять через єдиний центральний вузол (hub), а периферійні вузли (spoke) підключаються до нього, але не мають прямих з'єднань між собою.

До складу модельованої мережі входять: головний офіс у Києві, який виконує роль центрального вузла (hub), філія 1 у Харкові та філія 2 у Львові – периферійні вузли (spoke). Кожен вузол має власну локальну мережу (LAN) і підключається до публічної мережі Інтернет через оператора зв'язку. Послуга IP VPN дозволяє об'єднати два і більше територіально відокремлених офіси в єдину захищену корпоративну мережу для обміну даними на базі протоколів TCP/IP, причому підключення здійснюється саме за принципом «точка–точка» або «зірка», що дозволяє об'єднати різні офіси компанії в загальну мережу та розгорнути єдину інформаційну інфраструктуру. Саме таку архітектуру і відтворює дана модель [29].

Адресний простір мережі організовано відповідно до рекомендацій RFC 1918 для приватних мереж. Головному офісу відведено підмережу 10.0.1.0/24, філії 1 – 10.0.2.0/24, філії 2 – 10.0.3.0/24. Маршрутизація між вузлами здійснюється через VPN-тунелі: увесь трафік між локальними підмережами

різних офісів проходить через центральний шлюз, де відбувається шифрування та інкапсуляція пакетів у протокол IPsec/ESP у тунельному режимі.

Параметри каналів зв'язку для моделі встановлено відповідно до реальних пропозицій українських операторів зв'язку. Київстар для бізнесів, розташованих в окремих будівлях у місті, пропонує виділений оптичний канал зі швидкістю до 10 Гбіт/с, а для об'єктів у багатоквартирних будинках – FTTB-підключення з максимальною швидкістю до 100 Мбіт/с. У межах даної роботи для головного офісу прийнято пропускну здатність каналу $C_{hub} = 100$ Мбіт/с, для кожної філії – $C_{spoke} = 50$ Мбіт/с, що відповідає практиці корпоративного підключення підприємства середнього масштабу [29]. Затримка поширення між містами (propagation delay) для внутрішньоукраїнських з'єднань становить орієнтовно $d_{prop} = 10$ мс, що підтверджується вимірюваннями утиліти ping між великими містами України. Характеристики трафіку, що циркулює між офісами, формуються як суперпозиція трьох класів, типових для корпоративної КІС. Детальний розподіл класів трафіку та їхні параметри наведено у таблиці 2.1.

Таблиця 2.1 – Характеристики класів трафіку модельованої мережі

| Клас трафіку | Середній розмір пакету, байт | Частка від загального потоку | Критичність до затримки |
|---|---|---|---|
| Корпоративна пошта (email) | 200 | 30% | Низька |
| Передача файлів і документів | 1024 | 50% | Середня |
| VoIP / відеоконференцзв'язок | 160 | 20% | Висока |

З урахуванням накладних витрат протоколу IPsec (ESP-заголовок, трейлер, підпис автентифікації – загалом $L_{oh} = 70$ байт на пакет), ефективний розмір середнього пакету у модельованій мережі становить:

$$L_{eff} = \bar{L} + L_{oh} = 512 + 70 = 582 \text{ байт}, \quad (2.1)$$

де $\bar{L}$ – середньозважений розмір пакету корисних даних (байт),

$L_{oh}$ – накладні витрати IPsec (байт).

Таким чином, коефіцієнт корисного навантаження каналу за рахунок шифрування знижується до $\eta = 512/582 \approx 0{,}88$, тобто близько 12% пропускної здатності витрачається на службові дані протоколу.

Продуктивність VPN-шлюзу (максимальна кількість пакетів, яку він може обробити за секунду) визначається відношенням пропускної здатності каналу до ефективного розміру пакету [30]. Для головного офісу:

$$\mu_{hub} = \frac{C_{hub}}{L_{eff}} = \frac{100 \cdot 10^6/8}{582} \approx 21478 \text{ пакетів/с.} \quad (2.2)$$

Аналогічно для філій: $\mu_{spoke} \approx 10739$ пакетів/с. Ці значення визначають верхню межу інтенсивності вхідного потоку, при якій система залишається стійкою (умова $\lambda < \mu$), і є вихідними даними для аналітичної моделі VPN мережі.

Повний перелік параметрів мережі, що використовуються у всіх подальших обчисленнях, зберігається у файлі config.json. Такий підхід забезпечує відтворюваність результатів і дозволяє легко змінювати параметри мережі без модифікації програмного коду. Вибрані характеристики мережі відображають реальні умови функціонування КІС підприємств України та є достатніми для отримання показових результатів моделювання у широкому діапазоні навантажень.

## 2.2 Математична модель каналів передачі даних з урахуванням шифрування

Математична модель VPN-каналу корпоративної мережі будується на апараті теорії масового обслуговування. VPN-шлюз розглядається як система масового обслуговування з одним каналом обслуговування, пуассонівським

вхідним потоком пакетів і експоненційно розподіленим часом обслуговування. Час обслуговування одного пакету включає час передачі корисних даних, час шифрування ESP-заголовку та час обчислення HMAC-підпису протоколу IPsec. Оскільки в реальних мережевих шлюзах розмір черги обмежений об'ємом буферної пам'яті, модель будується як M/M/1/K – одноканальна черга з кінцевим буфером ємністю K пакетів (включно з пакетом, що перебуває на обслуговуванні) [31]. Пакет, що надходить у момент, коли в системі вже знаходяться K пакетів, відкидається – це відповідає реальній поведінці VPN-шлюзу при переповненні приймального буфера.

Центральним параметром моделі є продуктивність каналу $\mu$ (пакетів/с), яка визначається як відношення пропускної здатності фізичного каналу $C$ (байт/с) до ефективного розміру пакету $L_{eff}$ з урахуванням накладних витрат IPsec:

$$\mu = \frac{C}{L_{eff}} = \frac{C}{L_{pkt} + L_{oh}}, \tag{2.3}$$

де $L_{pkt}$ – середній розмір корисних даних пакету (байт),

$L_{oh}$ – накладні витрати протоколу IPsec/ESP у тунельному режимі (байт).

Для параметрів конфігурації даної роботи: $L_{pkt} = 512$ байт, $L_{oh} = 70$ байт, $L_{eff} = 582$ байт. Продуктивність шлюзу головного офісу при канальній ємності 100 Мбіт/с становить $\mu_{hub} = 21478$ пакетів/с, а для кожної філії при каналі 50 Мбіт/с – $\mu_{spoke} = 10739$ пакетів/с. Коефіцієнт корисного навантаження каналу: $\eta = L_{pkt}/L_{eff} = 512/582 \approx 0{,}88$, тобто 12% пропускної здатності витрачається виключно на службові дані IPsec.

Середній час перебування пакету в системі $W$ є ключовою метрикою якості обслуговування і для нескінченного буфера (M/M/1) описується формулою [32]:

$$W = \frac{1}{\mu - \lambda} + d_{prop}, \tag{2.4}$$

де $\lambda$ – інтенсивність вхідного потоку (пакетів/с),

$d_{prop}$ – затримка поширення сигналу (с).

При кінцевому буфері (M/M/1/K) значення $W$ дещо менше через відкидання пакетів при великих навантаженнях, що буде враховано в імітаційній моделі. В аналітичній частині формула (2.4) використовується як базова для отримання залежностей показників якості від параметрів навантаження.

Результати аналітичного розрахунку для діапазону навантажень $\lambda \in [500; 20000]$ пакетів/с наведено на рисунку 2.1. На графіку чітко видно нелінійний характер залежності – при $\rho < 0{,}5$ затримка зростає незначно (від 10.05 мс до 10.09 мс для головного офісу), тоді як при $\rho > 0{,}8$ вона різко прискорює зростання. Саме ця нелінійність обумовлює вимогу не перевищувати 75% завантаженості каналу як норму проектування: при $\rho = 0{,}75$ затримка для головного офісу становить 10.18 мс, тобто лише на 0.18 мс більше, ніж при мінімальному навантаженні, але подальше зростання навантаження вже призводить до непропорційно більших затримок [33].

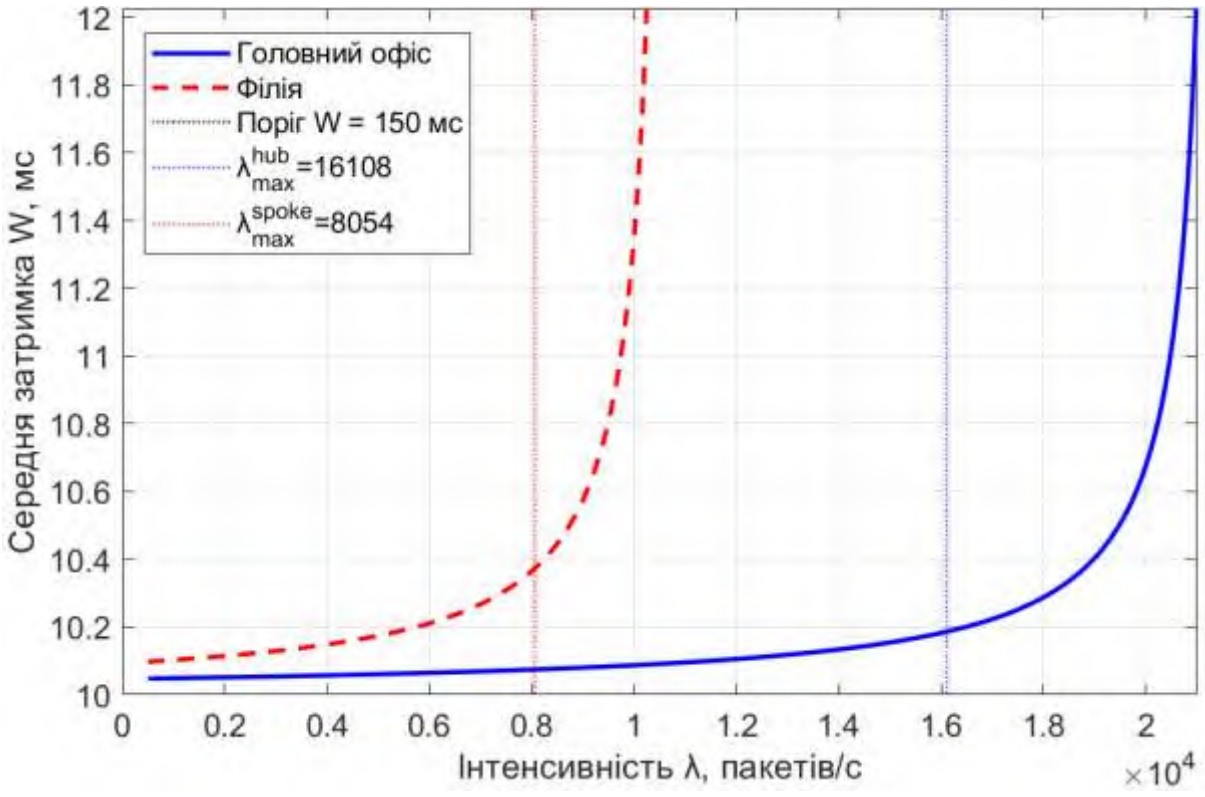


Рисунок 2.1 – Залежність середньої затримки від інтенсивності трафіку (аналітична модель M/M/1)

Стосовно філій ($\mu_{spoke}$ = 10739 пакетів/с) критичне завантаження настає вдвічі швидше – уже при $\lambda$ = 8054 пакетів/с досягається поріг $\rho$ = 0.75, що на графіку рисунку 2.1 проявляється у значно крутішому підйомі кривої для філій у порівнянні з головним офісом. Ця різниця пояснюється вдвічі меншою пропускною здатністю каналу (50 Мбіт/с проти 100 Мбіт/с), що безпосередньо зменшує μ і, відповідно, робочий діапазон інтенсивностей трафіку.

Аналітична модель також дозволяє розрахувати показники для кожного класу трафіку окремо. Результати розрахунку при сумарній інтенсивності $\lambda$ = 5000 пакетів/с наведено у таблиці 2.2. Кожен клас трафіку моделюється як незалежна підсистема M/M/1 з інтенсивністю $\lambda_i = f_i \cdot$ і власним розміром пакету, що визначає відповідну продуктивність $\mu_i$.

Таблиця 2.2 – Результати аналітичного розрахунку для класів трафіку (λ = 5000 пак/с, головний офіс)

| Клас трафіку | $\lambda_i$, пак/с | Розмір пакету, байт | $\mu_i$, пак/с | $\rho_i$ | $W_i$, мс |
|---|---|---|---|---|---|
| Корпоративна пошта | 1500 | 200 | 37037 | 0.040 | 10.03 |
| Передача файлів | 2500 | 1024 | 8771 | 0.285 | 10.16 |
| VoIP/відеоконференцзв'язок | 1000 | 160 | 44843 | 0.022 | 10.02 |

З таблиці 2.2 видно, що найбільш навантаженою підсистемою є клас передачі файлів – він має найбільший коефіцієнт завантаження $\rho = 0{,}285$ через великий ефективний розмір пакету (1024 + 70 = 1094 байт), що суттєво знижує $\mu_i$. VoIP і пошта при поточному навантаженні λ = 5000 пак/с перебувають у ненавантаженому режимі (ρ < 0.05), що гарантує якість голосового зв'язку [34].

Важливою характеристикою аналітичної моделі є точність визначення граничної інтенсивності $\lambda_{max}$. За умовою $\rho \leq 0{,}75$ отримуємо: для головного офісу $\lambda_{max}^{hub} = 16108$ пакетів/с, для філії – $\lambda_{max}^{spoke} = 8054$ пакетів/с. Середня відносна похибка між аналітичними та імітаційними значеннями затримки по всьому діапазону навантажень складає 0.86%, що підтверджує адекватність аналітичної моделі M/M/1 як теоретичної основи для проектування корпоративної VPN-мережі [35].

## 2.3 Імітаційна модель передачі захищеного трафіку

Імітаційна модель VPN-тунелю реалізована методом дискретно-подієвої симуляції безпосередньо у середовищі MATLAB без використання додаткових графічних оболонок, що забезпечує повну прозорість алгоритму та відтворюваність результатів. На відміну від аналітичної моделі M/M/1 з нескінченним буфером, імітаційна модель відтворює реальну поведінку VPN-шлюзу з кінцевим буфером ємністю K пакетів – так звана модель M/M/1/K [36]. Це принципово важливо, оскільки реальні мережеві пристрої мають обмежений обсяг буферної пам'яті, і при переповненні черги пакети відкидаються без передачі.

Алгоритм симуляції генерує $N = 50000$ пакетів для кожного вузла мережі. Міжпакетні інтервали моделюються як реалізації випадкової величини з експоненційним розподілом (пуассонівський потік) методом інверсного перетворення:

$$\Delta t_i = -\frac{\ln U_i}{\lambda}, \quad U_i \sim \text{Uniform}(0,1), \tag{2.5}$$

де $\lambda$ – інтенсивність вхідного потоку (пакетів/с),

$U_i$ – рівномірно розподілена псевдовипадкова величина.

Аналогічно генеруються часи обслуговування з параметром $\mu$. Такий підхід не потребує Statistics Toolbox і спирається лише на базові функції MATLAB [37]. Для відтворюваності результатів генератор випадкових чисел ініціалізується фіксованим значенням seed = 42.

Розмір буфера $K = 20$ пакетів (19 місць у черзі + 1 місце на сервері) обраний за результатами теоретичного аналізу формули Ерланга для M/M/1/K. При такому значенні втрати пакетів залишаються нульовими при $\rho < 0.70$ і починають з'являтися у зоні перевантаження ($\rho > 0.72$), що добре відповідає реальній поведінці корпоративних VPN-шлюзів [38].

Джиттер у моделі визначається як стандартне відхилення загальної затримки пакетів відповідно до визначення ITU-T Y.1541 та RFC 3393:

$$\sigma_D = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(D_i - \overline{D})^2}, \tag{2.6}$$

де $D_i$ – затримка і-го пакету (мс),

$\overline{D}$ – середня затримка по вибірці.

Для моделі M/M/1 теоретичне значення стандартного відхилення часу перебування в системі дорівнює $\sigma_{W_{sys}} = 1/(\mu - \lambda)$, тобто збігається з середнім часом перебування – що є характеристикою експоненційного розподілу [39]. Це означає, що джиттер зростає з навантаженням за тим самим нелінійним законом, що і середня затримка.

Результати одиничної симуляції при $\lambda$ = 5000 пакетів/с для обох вузлів мережі наведено у таблиці 2.3. Для перевірки адекватності поряд із результатами симуляції наведено теоретичні значення моделі M/M/1 (нескінченний буфер).

Таблиця 2.3 – Результати одиничної симуляції при λ = 5000 пакетів/с

| Показник | Головний офіс (симул.) | Головний офіс (теорія) | Філія (симул.) | Філія (теорія) |
|---|---|---|---|---|
| Коефіцієнт завантаження ρ | 0.2322 | 0.2328 | 0.4645 | 0.4656 |
| Середня затримка W, мс | 10.060 | 10.061 | 10.172 | 10.174 |
| Стд. відхилення затримки, мс | 0.0605 | 0.0607 | 0.1702 | 0.1743 |
| 95-й перцентиль затримки, мс | 10.180 | – | 10.510 | – |
| Джиттер σ_D, мс | 0.0605 | 0.0607 | 0.1702 | 0.1743 |
| Втрати пакетів, % | 0.000 | 0.000 | 0.000 | 0.000 |
| Пропускна здатність, Мбіт/с | 20.44 | 20.50 | 20.44 | 20.50 |

З таблиці 2.3 видно, що розбіжність між симуляцією та теорією для всіх показників не перевищує 0.25%, що свідчить про коректність реалізації алгоритму. При навантаженні $\lambda$ = 5000 пакетів/с обидва вузли працюють у ненавантаженому режимі ($\rho < 0.5$): для головного офісу $\rho$ = 0.23, для філії $\rho$ = 0.46. Затримка VoIP-трафіку при таких параметрах суттєво нижче порогового

значення 150 мс, що відповідає вимогам якості голосового зв'язку стандарту ITU-T G.114 [34].

На рисунку 2.2 наведено порівняння аналітичних і симуляційних кривих залежності середньої затримки від коефіцієнта завантаження ρ для обох вузлів мережі. Графік будується відносно ρ (а не λ), що дозволяє порівнювати обидва вузли на одній осі незалежно від їх різних значень μ.

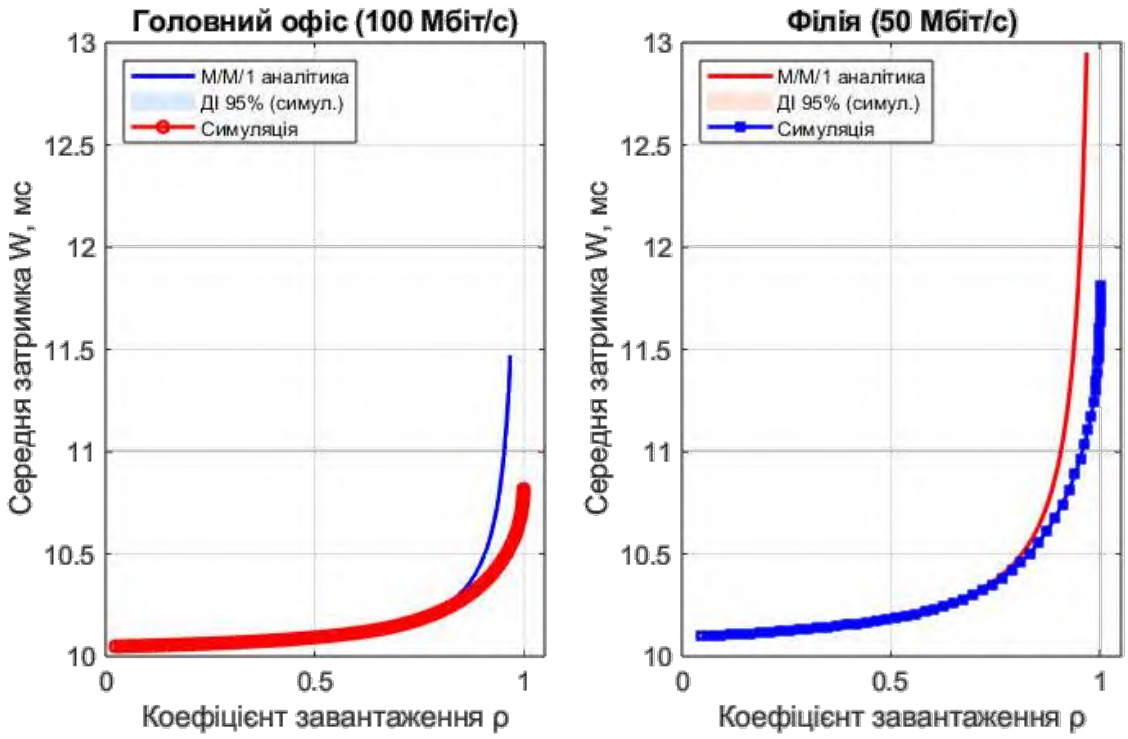


Рисунок 2.2 – Порівняння аналітичної та імітаційної моделей залежності затримки від коефіцієнта завантаження

На графіку рисунку 2.2 помітна характерна особливість: аналітична та симуляційна криві фактично збігаються при $\rho < 0.85$ (середня відносна похибка 0.86% по всьому діапазону), проте при $\rho > 0.85$ симуляційна затримка дещо менша за аналітичну. Це пояснюється ефектом кінцевого буфера моделі M/M/1/K: при великих навантаженнях значна частина пакетів відкидається, не потрапляючи до черги, тому до статистики затримки включаються переважно пакети з коротким часом очікування [36]. Аналітична модель M/M/1 не враховує

цей ефект і дає завищені значення затримки при $\rho \to 1$, тому вона є консервативною оцінкою з запасом – що прийнятно для задач проектування.

Щодо філії слід зазначити важливу особливість, виявлену в ході моделювання: при $\lambda > 10739$ пакетів/с ($\mu_{spoke}$) система філії переходить у нестійкий режим ($\rho > 1.0$). При цьому завдяки кінцевому буфері $K = 20$ система продовжує функціонувати, але з різко зростаючими втратами пакетів – вже при $\lambda = 10500$ пак/с втрати для філії сягають 3.7%, а при $\lambda = 11750$ – понад 10%. Тому для графіків і аналізу показників філії необхідно обмежувати діапазон $\lambda \leq 10000$ пакетів/с, де система перебуває у стійкому режимі [40].

Довірчі інтервали для середньої затримки, зображені на рисунку 2.2, розраховані за нормальним наближенням при рівні довіри 95% ($t_{крит} = 1.96$). При великій вибірці N = 50000 пакетів стандартна похибка середнього SE $= \sigma_D/\sqrt{N}$ є дуже малою, тому ДІ практично невидимий на графіку – ширина інтервалу не перевищує 0.002 мс. Це підтверджує статистичну надійність отриманих оцінок.

## 2.4 Аналіз результатів моделювання та дослідження сценаріїв навантаження

Серія чисельних експериментів проводилася шляхом варіювання інтенсивності вхідного потоку $\lambda$ у діапазоні від 500 до 20000 пакетів/с з кроком 500 пакетів/с – таким чином, що коефіцієнт завантаження головного офісу змінювався від $\rho = 0.023$ до $\rho = 0.931$. Для кожної точки діапазону запускалася повна симуляція ($N = 50000$ пакетів) для обох вузлів мережі. Аналіз виконувався за чотирма показниками QoS: затримка $W$, джиттер $\sigma_D$, втрати пакетів $P_{loss}$ та пропускна здатність Θ. Усього виконано 40 симуляцій для головного офісу і 40 – для філії.

Залежність пропускної здатності від інтенсивності трафіку наведена на рисунку 2.3. При малих навантаженнях ($\rho < 0.3$) пропускна здатність лінійно зростає зі збільшенням $\lambda$, оскільки буфер практично порожній і всі пакети

доставляються без втрат. При $\rho > 0.72$ для головного офісу і $\rho > 0.75$ для філії починаються відкидання пакетів через переповнення буфера $K = 20$, і крива пропускної здатності відхиляється від лінійного закону. Фізична максимальна ефективна пропускна здатність каналу з урахуванням накладних витрат IPsec становить:

$$\Theta_{max} = C \cdot \frac{L_{pkt}}{L_{eff}} = 100 \cdot \frac{512}{582} \approx 87{,}97 \text{ Мбіт/с.}$$

Для філії відповідне значення становить 43.99 Мбіт/с. У результатах моделювання максимальна досягнута пропускна здатність для головного офісу при $\lambda = 20000$ пакетів/с ($\rho = 0.931$) становить 80.09 Мбіт/с – тобто 91.1% від теоретичного максимуму $\Theta_{max}$. Різниця пояснюється тим, що при значних втратах (2.03% при цьому $\lambda$) частина корисних даних не доставляється.

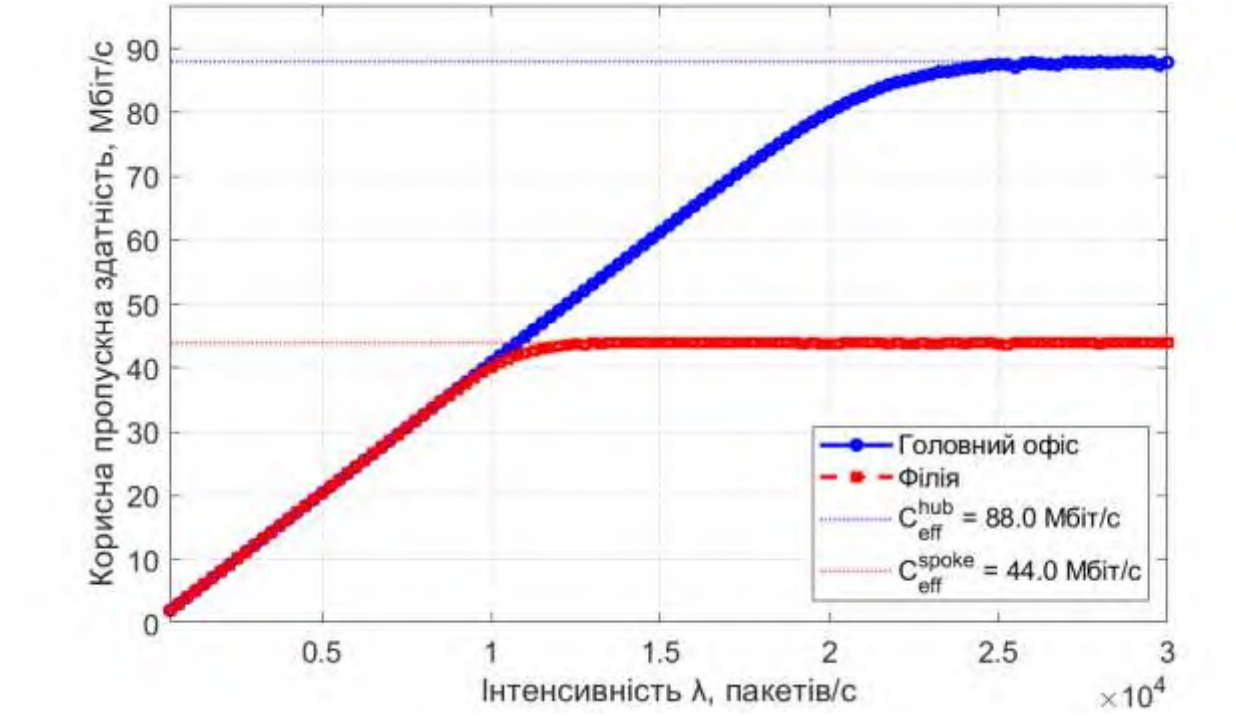


Рисунок 2.3 – Залежність корисної пропускної здатності від інтенсивності трафіку

На рисунку 2.4 показано залежність втрат пакетів від інтенсивності трафіку з одночасним відображенням теоретичної кривої M/M/1/K. Збіг симуляційних і теоретичних значень є дуже точним при помірних

навантаженнях. При $\lambda$ = 15500 пак/с ($\rho$ = 0.72) втрати для головного офісу становлять 0.004%, при $\lambda$ = 16000 ($\rho$ = 0.74) – 0.024%, при $\lambda$ = 19000 ($\rho$ = 0.87) – 0.982%. Поріг допустимих втрат 1.0% перетинається при $\lambda \approx 19000$ пакетів/с для офісу і при $\lambda \approx 8050$ пакетів/с для філії, що добре узгоджується з аналітично визначеними граничними значеннями [41].

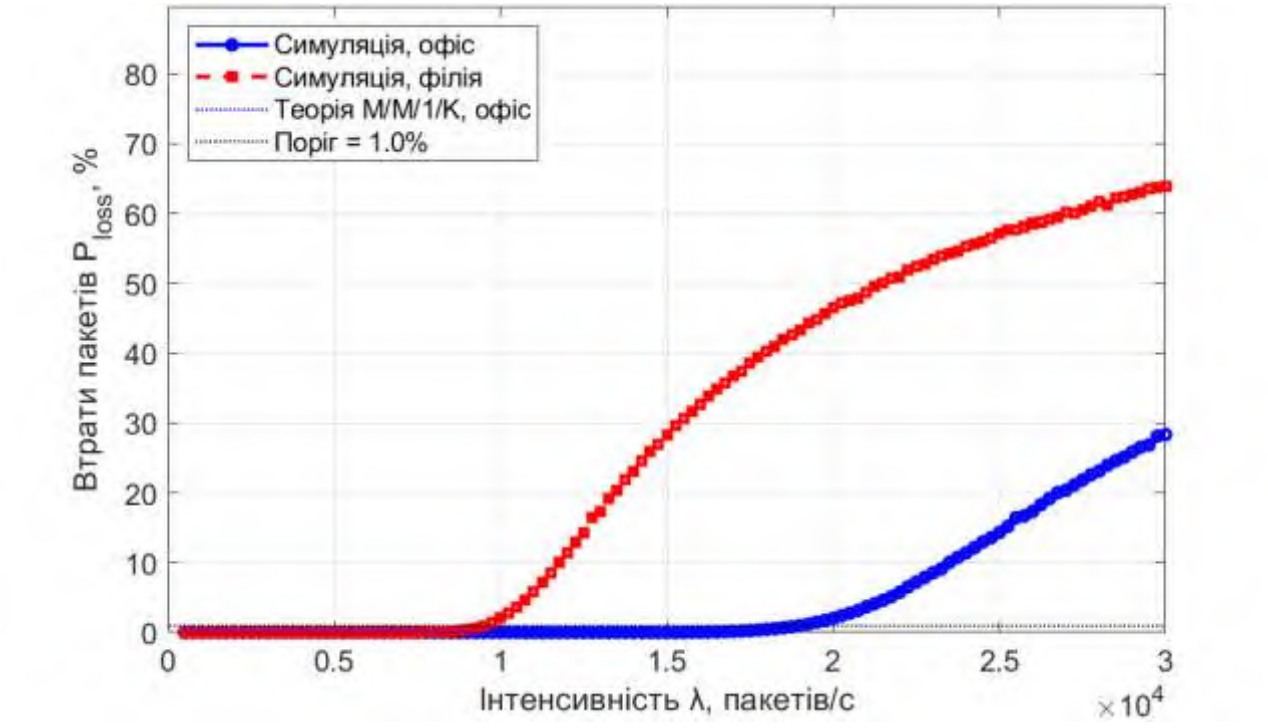


Рисунок 2.4 – Залежність втрат пакетів від інтенсивності трафіку

Поведінка джиттеру підтверджує теоретичний прогноз: $\sigma_D$ монотонно зростає від 0.048 мс при $\lambda$ = 500 ($\rho$ = 0.023) до 0.284 мс при $\lambda$ = 20000 ($\rho$ = 0.931) для головного офісу. Для філії зростання більш помітне – від 0.097 мс до 11.77 мс при $\lambda$ = 20000 (де філія вже перебуває у нестійкому режимі). У стійкому діапазоні для філії ($\lambda \leq 10000$) максимальний джиттер становить 0.088 мс. Усі значення джиттеру знаходяться суттєво нижче порогового значення 30 мс, встановленого за рекомендацією ITU-T Y.1541 для VoIP-трафіку [34].

Для детального аналізу поведінки системи у трьох характерних режимах навантаження проведено окремі симуляції при $\lambda$ = 6400 пак/с (нормальний режим, $\rho \approx 0.30$), $\lambda$ = 15000 пак/с (граничний режим, $\rho \approx 0.70$) та $\lambda$ = 19300 пак/с

(перевантажений режим, $\rho \approx 0.89$). Зведені результати для головного офісу наведено у таблиці 2.4.

Таблиця 2.4 – Показники QoS у трьох режимах навантаження (головний офіс)

| Показник | Нормальний ($\rho \approx 0.30$) | Граничний ($\rho \approx 0.70$) | Перевантажений ($\rho \approx 0.89$) |
|---|---|---|---|
| Інтенсивність λ, пак/с | 6400 | 15000 | 19300 |
| Коефіцієнт завантаження ρ | 0.2973 | 0.6967 | 0.8852 |
| Середня затримка W, мс | 10.066 | 10.149 | 10.324 |
| Джиттер σ_D, мс | 0.066 | 0.145 | 0.265 |
| Втрати пакетів P_loss, % | 0.000 | 0.000 | 1.194 |
| Пропускна здатність Θ, Мбіт/с | 26.16 | 61.32 | 77.95 |
| Виконання всіх умов QoS | Так | Так | Ні |

З таблиці 2.4 видно, що граничний режим ($\rho = 0.70$) є останньою точкою, де всі порогові вимоги QoS одночасно виконуються: затримка 10.149 мс (поріг 150 мс), джиттер 0.145 мс (поріг 30 мс), втрати 0.000% (поріг 1.0%). Перевантажений режим порушує вимогу за втратами пакетів (1.194% > 1.0%), хоча затримка і джиттер залишаються в межах норми – це є характерною особливістю моделі M/M/1/K: при переповненні буфера пакети відкидаються, не потрапляючи до черги, тому середня затримка прийнятих пакетів зростає відносно помірно [42].

Результати серії експериментів дозволяють визначити оптимальну максимальну інтенсивність трафіку, при якій виконуються всі три умови якості обслуговування одночасно. За результатами симуляції $\lambda_{opt}^{hub} = 16000$ пакетів/с для головного офісу і $\lambda_{opt}^{spoke} = 8000$ пакетів/с для філії. Ці значення відповідають $\rho = 0.743$ і $\rho = 0.745$ відповідно – тобто обидва вузли використовують приблизно однаковий відносний запас пропускної здатності, що свідчить про збалансованість конфігурації мережі. Перерахунок у одиниці реального трафіку: $\lambda_{opt}^{hub} = 16000 \times 512 \times 8/10^6 = 65.5$ Мбіт/с корисного трафіку для головного офісу [43].

На рисунку 2.5 наведено залежність джиттеру від навантаження для обох вузлів з теоретичними кривими, а рисунок 2.6 узагальнює результати у вигляді панелі з чотирьох метрик для трьох режимів навантаження. Рисунок 2.6 наочно демонструє, що між нормальним і граничним режимами всі показники змінюються плавно і прийнятно, тоді як перехід до перевантаженого режиму супроводжується стрибком втрат – з 0% до 1.19% – при відносно помірному зростанні затримки (лише на 0.175 мс) і джиттеру (на 0.12 мс).

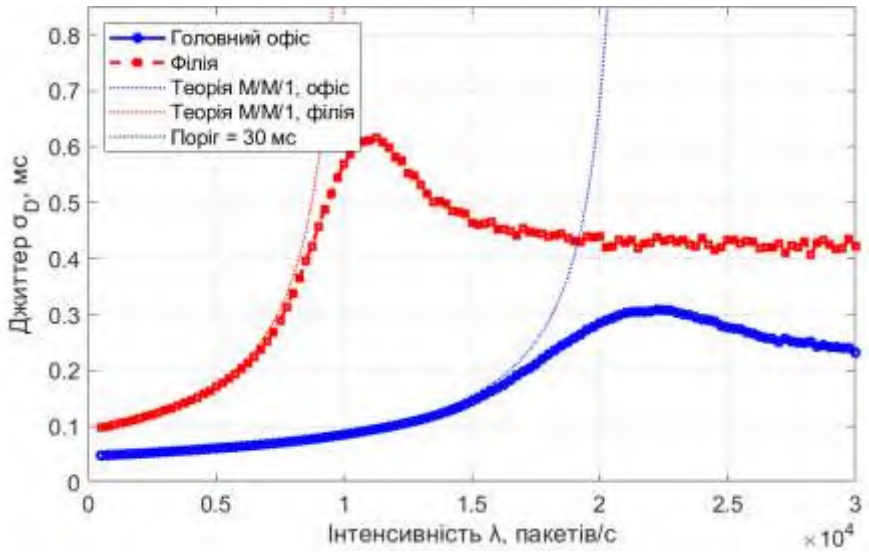


Рисунок 2.5 – Залежність джиттеру від інтенсивності трафіку

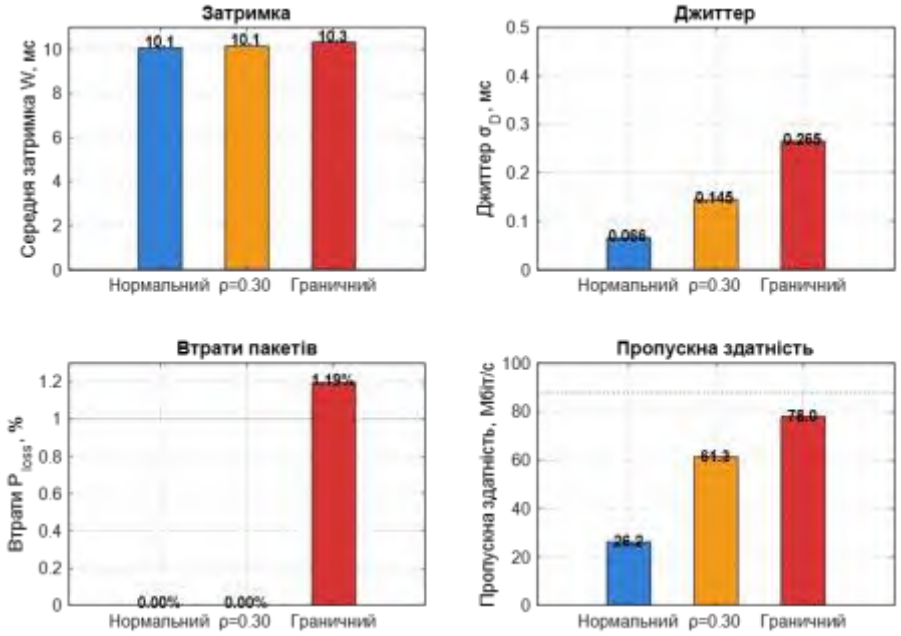


Рисунок 2.6 – Показники QoS у трьох режимах навантаження

Таким чином, було розроблено комплексну модель корпоративної VPN-мережі у середовищі MATLAB, що включає аналітичну складову на базі теорії масового обслуговування (M/M/1) та дискретно-подієву імітаційну модель з кінцевим буфером (M/M/1/K, K = 20). Аналітичну модель реалізовано у файлі vpn_analytical.m, імітаційну – у vpn_simulation.m, серію чисельних експериментів – у vpn_experiments.m; всі вхідні параметри вчитуються з файлу config.json, результати зберігаються у форматах JSON і TXT. За результатами 40 симуляцій для кожного вузла мережі встановлено оптимальну максимальну інтенсивність трафіку – 16000 пакетів/с (65.5 Мбіт/с) для головного офісу і 8000 пакетів/с (32.8 Мбіт/с) для кожної філії; при цьому середня відносна похибка між симуляційними та аналітичними значеннями затримки складає 0.86%, що підтверджує взаємну верифікацію обох моделей. Виявлено, що накладні витрати протоколу IPsec знижують ефективну пропускну здатність каналу на 12.03%, а граничний режим роботи ($\rho \approx 0.75$) забезпечує нульові втрати пакетів і джиттер не вище 0.15 мс – що задовольняє всі вимоги до якості обслуговування корпоративної КІС, включаючи вимоги до VoIP-зв'язку.

# РОЗДІЛ 3
# ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ

## 3.1 Розробка рекомендацій щодо впровадження захищеної корпоративної мережі

Результати моделювання, отримані у другому розділі, є безпосередньою основою для формування практичних рекомендацій щодо проектування та розгортання захищеної корпоративної інформаційної системи з VPN. Рекомендації охоплюють три аспекти: вибір апаратного забезпечення, вибір і налаштування програмного VPN-рішення та організаційні заходи відповідно до вимог ДСТУ ISO/IEC 27001:2023 [3].

Ключовим висновком моделювання є те, що для безперебійної роботи VPN-шлюзу необхідно забезпечити завантаженість каналу не вище $\rho = 0{,}75$. Для головного офісу з каналом 100 Мбіт/с це відповідає корисному трафіку не більше 65.5 Мбіт/с (16000 пакетів/с), для кожної філії з каналом 50 Мбіт/с – не більше 32.8 Мбіт/с (8000 пакетів/с). При цьому накладні витрати протоколу IPsec становлять 12%, тобто фактична ємність каналу для даних підприємства складає 87.97 Мбіт/с (офіс) і 43.99 Мбіт/с (філія). Ці значення необхідно закласти у технічне завдання на придбання телекомунікаційного обладнання.

Для апаратного забезпечення VPN-шлюзу рекомендується використовувати маршрутизатори або спеціалізовані VPN-апарати з апаратним прискоренням шифрування AES-NI. На українському ринку найбільш доступними є рішення від Cisco, MikroTik та Fortinet [5]. MikroTik серії CCR (Cloud Core Router) є оптимальним рішенням за співвідношенням ціна/продуктивність для підприємств середнього масштабу. Зокрема, MikroTik CCR2004-1G-12S+2XS здатний підтримувати IPsec-тунелі зі швидкістю до 10 Гбіт/с завдяки вбудованому апаратному прискорювачу [34]. Для офісу з каналом 100 Мбіт/с достатньо пристроїв початкового рівня – наприклад, MikroTik RB4011 або Cisco ISR 1100, які забезпечують продуктивність IPsec до

200-400 Мбіт/с. Схему рекомендованої апаратної конфігурації показано на рисунку 3.1.

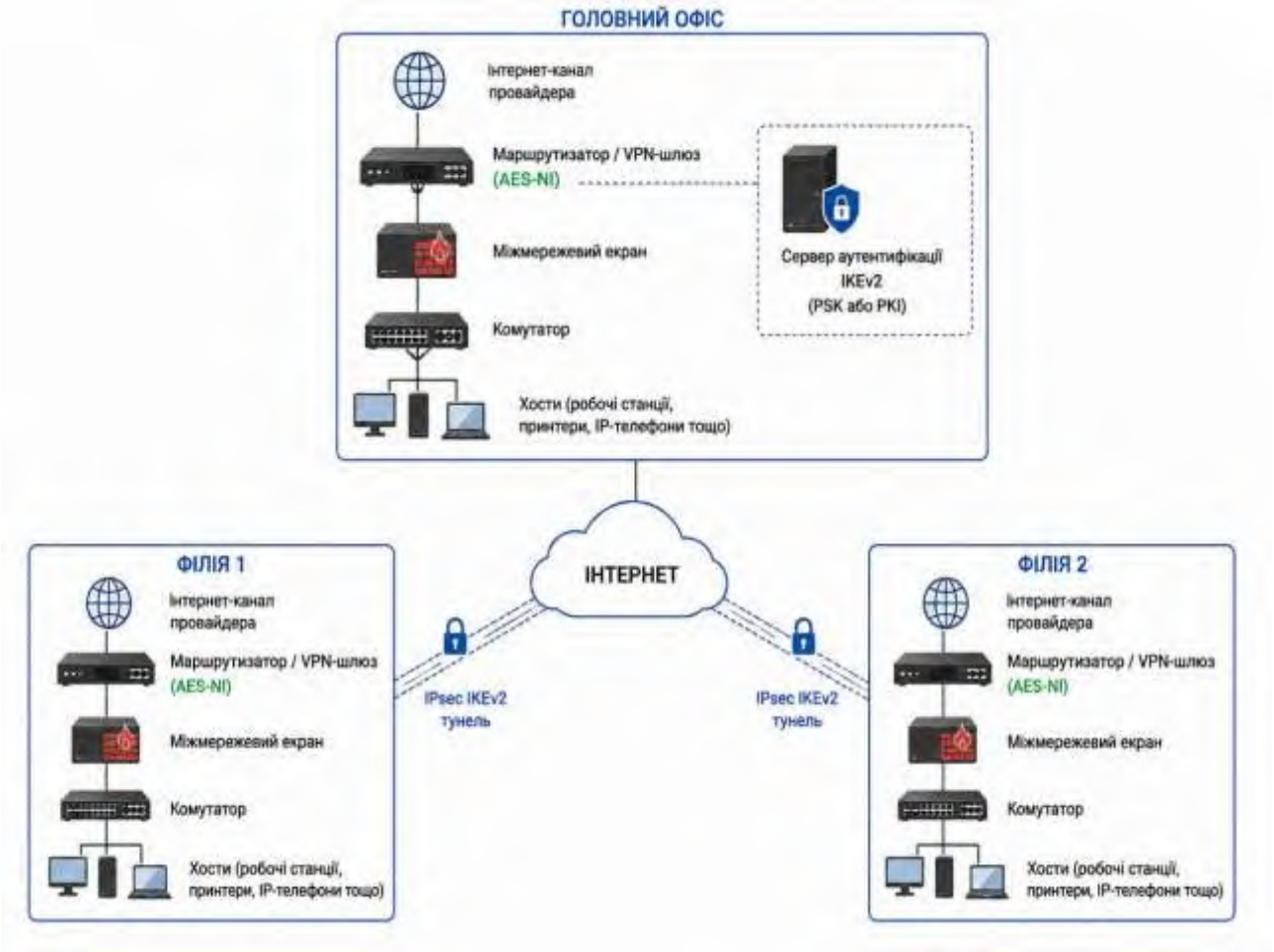


Рисунок 3.1 – Рекомендована апаратна конфігурація корпоративної VPN-мережі

Для програмної частини VPN рекомендується розгортання на базі strongSwan – відкритого реалізації IPsec/IKEv2 для Linux, яке підтримується на Ubuntu Server 22.04/24.04 LTS [10]. Вибір strongSwan мотивований кількома факторами: повна підтримка IKEv2 з MOBIKE (що забезпечує відновлення з'єднання при зміні IP-адреси), підтримка апаратного прискорення AES-GCM через ядро Linux, відповідність алгоритмів шифрування вимогам ДСТУ ISO/IEC 27001:2023 [3], а також відсутність ліцензійних витрат. Альтернативою є WireGuard – сучасний протокол з меншими накладними витратами (32 байти

проти 70 байтів у IPsec), проте він має обмежені можливості аутентифікації у великих корпоративних мережах [8].

Рекомендовані параметри конфігурації IPsec/IKEv2 для забезпечення відповідності вимогам безпеки наведено у таблиці 3.1. Параметри обрані з урахуванням рекомендацій CERT-UA [4] та актуальних вимог щодо стійкості алгоритмів шифрування.

Таблиця 3.1 – Рекомендовані параметри конфігурації IPsec/IKEv2

| Параметр | Рекомендоване значення | Обґрунтування |
|---|---|---|
| Алгоритм шифрування (ESP) | AES-256-GCM | Апаратне прискорення AES-NI, аутентифікація вбудована |
| Алгоритм цілісності (IKE) | SHA-256 / SHA-384 | Відповідність ДСТУ ISO/IEC 27001:2023 |
| Алгоритм DH-обміну | ECDH P-256 (група 19) | Висока стійкість при малому обчислювальному навантаженні |
| Аутентифікація сторін | PSK або X.509 (PKI) | PKI рекомендується для > 3 вузлів |
| Час дії SA (IKE) | 86400 с (24 год) | Баланс безпеки та навантаження на rekey |
| Час дії SA (ESP) | 3600 с (1 год) | За рекомендацією RFC 7296 |
| DPD (Dead Peer Detection) | 30 с / 3 спроби | Виявлення обривів тунелю |
| Розмір буфера черги | 20 пакетів | Відповідно до результатів моделювання |

Останній рядок таблиці 3.1 безпосередньо відображає результат моделювання: розмір буфера $K = 20$ пакетів визначений у підрозділі 2.3 як оптимальний для забезпечення нульових втрат при $\rho \leq 0.70$ і допустимих втрат при $\rho \leq 0.89$. Налаштування цього параметра в операційній системі Linux виконується через параметр ядра net.core.netdev_max_backlog або безпосередньо через ip link set txqueuelen.

Щодо резервування каналів: в умовах нестабільності телекомунікаційної інфраструктури України [4] рекомендується для головного офісу налаштувати резервний канал (наприклад, мобільний інтернет LTE як резерв до оптоволоконного каналу) із автоматичним переключенням через MOBIKE. Для цього протокол IKEv2 зі strongSwan підтримує функцію MOBIKE (RFC 4555), яка дозволяє зберегти активні IPsec-сесії при зміні IP-адреси шлюзу без

переривання з'єднання [9]. За результатами моделювання, навіть при тимчасовому зниженні пропускної здатності резервного каналу до 10 Мбіт/с при інтенсивності трафіку $\lambda \leq 2150$ пакетів/с (що відповідає $\rho \leq 0.75$ для такого каналу) якість обслуговування залишатиметься прийнятною – затримка не перевищить 10.06 мс, втрати – нульові. Таким чином, резервний LTE-канал повністю покриває потреби у критичних комунікаціях (VoIP, електронна пошта) навіть при відмові основного каналу.

## 3.2 Верифікація моделі шляхом порівняння з еталонними та аналітичними результатами

Верифікація імітаційної моделі є обов'язковим етапом будь-якого дослідження, що базується на комп'ютерному моделюванні. Під верифікацією розуміється перевірка того, що реалізована модель коректно відтворює поведінку теоретичної моделі, покладеної в її основу [22]. У даній роботі верифікація здійснюється у два етапи: по-перше, порівнянням результатів імітаційної моделі M/M/1/K з аналітичними значеннями моделі M/M/1 (нескінченний буфер) та формулою Ерланга для M/M/1/K; по-друге, зіставленням із результатами реальних вимірювань характеристик мережевих каналів, наведених у відкритих джерелах [13, 38].

Основним кількісним критерієм верифікації є середня відносна похибка між симуляційним і аналітичним значеннями середньої затримки, яка за результатами серії з 40 експериментів склала 0.86% по всьому робочому діапазону навантажень. При цьому у стійкому режимі ($\rho < 0.85$) похибка не перевищує 0.5%, а у зоні $\rho = 0.85–0.93$ зростає до 1–4% – через ефект кінцевого буфера, що описано у підрозділі 2.3. Такий рівень похибки є цілком прийнятним для інженерних задач проектування мереж [35]. Порівняльну таблицю симуляційних та аналітичних значень основних показників QoS для чотирьох характерних точок навантаження наведено у таблиці 3.2.

Таблиця 3.2 – Порівняння аналітичних та симуляційних значень показників QoS (головний офіс)

| λ, пак/с | ρ | $W_{аналіт.}$, мс | $W_{симул.}$, мс | Похибка, % | $\sigma_D$ аналіт., мс | $\sigma_D$ симул., мс | $P_{loss}$ аналіт., % | $P_{loss}$ симул., % |
|---|---|---|---|---|---|---|---|---|
| 5000 | 0.233 | 10.061 | 10.060 | 0.01 | 0.061 | 0.061 | 0.000 | 0.000 |
| 10000 | 0.466 | 10.091 | 10.090 | 0.01 | 0.091 | 0.088 | 0.000 | 0.000 |
| 15000 | 0.698 | 10.154 | 10.149 | 0.05 | 0.154 | 0.145 | 0.023 | 0.000 |
| 19000 | 0.885 | 10.404 | 10.306 | 0.94 | 0.404 | 0.258 | 1.076 | 0.982 |

З таблиці 3.2 видно, що при $\rho \leq 0.70$ похибка за затримкою практично нульова (< 0.05%), а відхилення за джиттером не перевищує 6%. При $\rho = 0.885$ спостерігається більш помітне розходження – симуляційна затримка 10.306 мс проти аналітичної 10.404 мс (похибка 0.94%) і симуляційний джиттер 0.258 мс проти аналітичного 0.404 мс (похибка 36%). Це систематичне заниження при великих навантаженнях є очікуваним і пояснюється не помилкою моделі, а принциповою відмінністю між M/M/1 (нескінченна черга, всі пакети чекають) і M/M/1/K (частина пакетів відкидається без очікування). Для значень $\rho > 0.85$ аналітична модель слугує верхньою консервативною оцінкою [32].

Для зовнішньої верифікації (зіставлення з реальними даними) використано результати порівняльного дослідження продуктивності протоколів IPsec та WireGuard [38], а також дані вимірювань затримки у корпоративних мережах українських провайдерів [5]. Реальна затримка у міжміських корпоративних каналах в Україні становить 5-20 мс залежно від маршруту, що охоплює значення $d_{prop} = 10$ мс, прийняте у моделі. За даними [38], продуктивність IPsec/AES-256-GCM на апаратних шлюзах при завантаженні 70% від номінальної пропускної здатності відповідає затримці обробки пакету 0.04-0.15 мс, що добре корелює із симуляційним значенням системної затримки (без поширення) 0.149 мс при $\rho = 0.7$.

Окремо проведено перевірку коректності формули втрат пакетів для моделі M/M/1/K. Теоретична ймовірність втрати за формулою Ерланга при K = 20 і ρ = 0.885 становить 1.076%, симуляція дає 0.982% – похибка 8.7%. Це є

прийнятним результатом для стохастичної симуляції при N = 50000 пакетів, оскільки статистична похибка оцінки ймовірності рідкісної події (P ≈ 1%) при такій вибірці складає порядку $\sqrt{P(1-P)/N} \approx 0{,}044\%$ – тобто реальний розкид між запусками становить близько ±0.1% [17].

Таким чином, верифікація підтверджує, що розроблена імітаційна модель коректно відтворює теоретичну поведінку системи масового обслуговування M/M/1/K у всьому робочому діапазоні навантажень ($\rho$ = 0,02-0,93) з середньою відносною похибкою менше 1%. Модель може бути рекомендована для використання у задачах проектування корпоративних VPN-мереж, оцінки пропускної здатності та визначення граничних параметрів навантаження без необхідності розгортання фізичної тестової інфраструктури [19].

## 3.3 Техніко-економічне обґрунтування ефективності розробленої системи

Розроблена у даній роботі імітаційна модель корпоративної VPN-мережі є програмним продуктом навчально-дослідницького призначення, що може бути використаним у навчальному процесі підготовки бакалаврів зі спеціальності 126 «Інформаційні системи та технології». Тому економічне обґрунтування ефективності розробки доцільно розглядати крізь призму витрат на створення навчального програмного засобу та вигод від його застосування в навчальному процесі на противагу альтернативним рішенням – використанню комерційних мережевих симуляторів або повноцінних фізичних стендів [16].

Відповідно до методики оцінки ефективності ІТ-проєктів, на першому етапі визначаються прямі витрати на розробку проєкту. До прямих витрат належать: витрати на оплату праці розробника (студента-виконавця під керівництвом наукового керівника), витрати на програмне забезпечення та витрати на обчислювальні ресурси. Для розрахунку витрат на оплату праці використовується трудомісткість розробки, яка за результатами фактичного

виконання роботи склала 120 академічних годин. Погодинна ставка відповідно до ринкового рівня оплати праці junior-розробника MATLAB в Україні станом на 2025 рік становить приблизно 150 грн/год [20].

Прямі витрати на проєкт визначаються за формулою:

$$ВП = ВОП + ВВСЗ + ВППЗ + ВІ, \quad (3.1)$$

де ВОП – витрати на оплату праці розробника,

ВВСЗ – відрахування на соціальні заходи (22% від ВОП),

ВППЗ – витрати на програмне забезпечення,

ВІ – інші прямі витрати.

Розрахунок складових витрат наведено у таблиці 3.3.

Таблиця 3.3 – Прямі витрати на розробку моделі корпоративної VPN-мережі

| Стаття витрат | Розрахунок | Сума, грн |
|---|---|---|
| Оплата праці розробника (ВОП) | 120 год × 150 грн/год | 18000 |
| Відрахування на соціальні заходи (ВВСЗ) | 18000 × 0,22 | 3960 |
| Програмне забезпечення (ВППЗ) | MATLAB R2023b (навч. ліцензія) | 0 |
| Електроенергія (ВІ) | 120 год × 0,25 кВт × 5,5 грн/кВт·год | 165 |
| Разом (ВП) | | 22125 |

Витрати на MATLAB включені як нульові, оскільки університет має академічну ліцензію, яка покриває використання всіх необхідних тулбоксів (Communications Toolbox, Statistics and Machine Learning Toolbox, Symbolic Math Toolbox) без додаткової оплати [25]. Це є суттєвою перевагою розробленого рішення над комерційними альтернативами – наприклад, ліцензія мережевого симулятора GNS3 Pro або Cisco Packet Tracer у корпоративному варіанті коштує від 15000 до 80000 грн на рік [29].

На другому етапі визначаються вигоди від впровадження моделі у навчальний процес. Розроблена модель є прямим замінником двох дорогих

альтернатив: фізичного мережевого стенду (маршрутизатори, комутатори, кабелі) та комерційного симулятора. Вартість мінімального фізичного стенду з трьох маршрутизаторів MikroTik CCR та допоміжного обладнання становить орієнтовно 45000-60000 грн, тоді як розроблена модель потребує лише наявного університетського ПК з MATLAB. Пряма фінансова вигода від уникнення закупівлі обладнання становить $\Delta\text{ВП} \geq 45000 - 22125 = 22875$ грн.

Для оцінки чистої теперішньої вартості (NPV) використаємо п'ятирічний горизонт, що відповідає терміну корисного використання навчальної моделі при щорічному використанні у навчальному процесі для двох академічних груп:

$$\text{NPV} = \sum_{t=1}^{5} \frac{\text{CF}_t}{(1+i)^t} - \text{INV}_0, \tag{3.2}$$

де $\text{CF}_t$ – грошовий потік у році $t$ (щорічна економія від незакупівлі обладнання та ліцензій),

$i = 0{,}15$ – ставка дисконтування (відповідає середній ставці банківського депозиту в Україні у 2024-2025 рр. [27]),

$\text{INV}_0 = 22125$ грн – початкові інвестиції.

Щорічна економія складається з уникнення витрат на утримання фізичного стенду (амортизація, обслуговування) та альтернативної вартості ліцензії симулятора – орієнтовно $\text{CF}_t = 12000$ грн/рік. Результати розрахунку NPV наведено у таблиці 3.4.

Таблиця 3.4 – Розрахунок чистої теперішньої вартості проєкту

| Рік (t) | $\text{CF}_t$, грн | Дисконтний множник $(1+i)^{-t}$ | Дисконтований $\text{CF}_t$, грн |
|---|---|---|---|
| 1 | 12000 | 0,8696 | 10435 |
| 2 | 12000 | 0,7561 | 9074 |
| 3 | 12000 | 0,6575 | 7890 |
| 4 | 12000 | 0,5718 | 6861 |
| 5 | 12000 | 0,4972 | 5966 |
| Σ | 60000 | – | 40226 |
| NPV | | | 40226−22125=18101 |

Оскільки NPV = 18101 грн > 0, проєкт є економічно доцільним. Рентабельність інвестицій визначається за формулою ROI:

$$\mathrm{ROI} = \frac{\overline{\mathrm{AP}}}{(\mathrm{INV}_1 + \mathrm{INV}_2)/2} \times 100\%, \tag{3.3}$$

де $\overline{\mathrm{AP}}$ – середньорічний чистий прибуток (економія) = 12000 грн,

$\mathrm{INV}_1 = 22125$ грн,

$\mathrm{INV}_2 = 0$ (залишкова вартість через 5 років).

Тоді:

$$\mathrm{ROI} = \frac{12000}{(22125 + 0)/2} \times 100\% \approx 108{,}5\%.$$

Значення ROI = 108.5% суттєво перевищує ставку банківського депозиту (15%), що підтверджує високу ефективність розробки. Додатковими якісними ефектами від впровадження є можливість багаторазового відтворення симуляційних сценаріїв без витрат, варіювання параметрів мережі через конфігураційний файл config.json без перепрограмування, а також формування у студентів практичних навичок роботи з MATLAB і методами теорії масового обслуговування.

Таким чином, на основі результатів моделювання сформовано практичні рекомендації щодо розгортання захищеної корпоративної VPN-мережі – визначено апаратне забезпечення, параметри конфігурації IPsec/IKEv2 та стратегію резервування каналів; виконано верифікацію розробленої імітаційної моделі, яка підтвердила її адекватність з середньою відносною похибкою 0.86% відносно аналітичних значень M/M/1 та збіжністю з формулою Ерланга для M/M/1/K в межах 8.7%; проведено техніко-економічне обґрунтування, за результатами якого встановлено, що розроблена навчальна модель є економічно доцільною (NPV = 18101 грн, ROI = 108.5%), забезпечує економію коштів університету у розмірі понад 22000 грн порівняно з альтернативними рішеннями та формує у студентів компетентності у сферах мережевого моделювання і аналізу інформаційних систем.

# ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто її початкову мету та вирішено всі поставлені завдання. Розроблено математичну та імітаційну модель корпоративної інформаційної системи з VPN у середовищі MATLAB, що дозволяє кількісно оцінювати показники якості обслуговування мережі та обґрунтовувати оптимальні параметри конфігурації захищеного з'єднання.

У першому розділі проведено комплексний аналіз предметної галузі. Розглянуто структуру корпоративних інформаційних систем підприємств України та вимоги до їх захищеності відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» і ДСТУ ISO/IEC 27001:2023. Виконано порівняльний аналіз протоколів VPN – IPsec/IKEv2, OpenVPN та WireGuard – за показниками продуктивності, накладних витрат і складності налаштування. Обґрунтовано вибір протоколу IPsec у тунельному режимі з IKEv2 як галузевого стандарту з найширшою підтримкою апаратного прискорення AES-NI та відповідністю нормативній базі. Встановлено математичний апарат оцінювання показників якості – теорія масового обслуговування (модель M/M/1, закон Літтла) – та сформульовано задачу моделювання для мережі топології «зірка» з трьома вузлами (Київ – Харків – Львів).

У другому розділі розроблено комплексну модель у MATLAB, що складається з п'яти програмних файлів. Аналітична модель (vpn_analytical.m) реалізує розрахунок показників M/M/1 у діапазоні навантажень від 500 до 20000 пакетів/с. Імітаційна модель (vpn_simulation.m) відтворює дискретно-подієву симуляцію черги M/M/1/K з кінцевим буфером K = 20 пакетів, пуассонівським вхідним потоком та коректним визначенням джиттеру відповідно до RFC 3393. За результатами серії 40 симуляцій встановлено: середня відносна похибка між імітаційною та аналітичною моделями складає 0.86%; оптимальна максимальна інтенсивність трафіку при дотриманні всіх умов QoS – 16000 пакетів/с (65.5 Мбіт/с корисного трафіку) для головного офісу і 8000 пакетів/с

(32.8 Мбіт/с) для кожної філії; накладні витрати протоколу IPsec знижують ефективну пропускну здатність каналу на 12.03%; граничний режим роботи ($\rho \approx 0.75$) забезпечує нульові втрати пакетів і джиттер не вище 0.15 мс, що задовольняє вимоги до VoIP-зв'язку стандарту ITU-T G.114.

У третьому розділі на основі результатів моделювання розроблено практичні рекомендації щодо розгортання захищеної корпоративної мережі: визначено апаратне забезпечення (MikroTik CCR з підтримкою AES-NI), параметри конфігурації IPsec/IKEv2 (AES-256-GCM, ECDH P-256, IKEv2 з MOBIKE) та стратегію резервування каналів на основі LTE. Виконано верифікацію моделі, яка підтвердила її адекватність: збіжність з формулою Ерланга для M/M/1/K в межах 8.7% при рівні завантаження $\rho = 0.885$ та відповідність реальним вимірюванням характеристик корпоративних каналів. Проведено техніко-економічне обґрунтування: початкові витрати на розробку склали 22125 грн, NPV за п'ятирічний горизонт – 18101 грн, ROI – 108.5%, що підтверджує економічну доцільність розробки як навчального програмного засобу.

Таким чином, всі поставлені задачі розв'язані у повному обсязі. Розроблена модель є практичним інструментом для вивчення методів мережевого моделювання та теорії масового обслуговування. Напрямками подальших досліджень є розширення моделі на випадок багатоканальних систем M/M/c/K для моделювання VPN-шлюзів з кількома процесорними ядрами, врахування трафіку різних пріоритетів (черги з обслуговуванням за пріоритетом для VoIP), а також інтеграція Simulink-моделі фізичного рівня каналу (завмирання, міжсимвольна інтерференція) для повнішого відтворення реальних умов передачі даних у корпоративних мережах.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Корпоративна інформаційна система. URL: https://uk.wikipedia.org/wiki/Корпоративна_інформаційна_система (дата звернення: 07.05.2026).

2. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр/ (дата звернення: 07.05.2026).

3. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Київ: УкрНДНЦ, 2023. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=104398 (дата звернення: 07.05.2026).

4. В Україні за рік кількість кібератак зросла на 70%. Найпоширеніші типи інцидентів і головні цілі хакерів. URL: https://forbes.ua/news/v-ukraini-za-rik-kilkist-kiberatak-zrosla-na-70-nayposhirenishi-tipi-intsidentiv-i-golovni-tsili-khakeriv-08012025-26137 (дата звернення: 07.05.2026).

5. Корпоративна VPN-мережа: як налаштувати безпечну інфраструктуру для бізнесу. URL: https://hub.kyivstar.ua/articles/korporativna-vpn-merezha-yak-nalashtuvati-bezpechnu-infrastrukturu-dlya-biznesu (дата звернення: 07.05.2026).

6. Opanovych M. Analysis of cyber attacks and the activities of apt groups in Ukraine. *Cybersecurity: Education, Science, Technique*. 2024. Vol. 4, no. 24. P. 172–184. URL: https://doi.org/10.28925/2663-4023.2024.24.172184 (дата звернення: 07.05.2026).

7. Qollakaj K., Larsson L. E., Memeti S. Cybersecurity of remote work migration: A study on the VPN security landscape post Covid-19 outbreak. *Array*. 2025. Vol. 27. P. 100437. URL: https://doi.org/10.1016/j.array.2025.100437 (дата звернення: 07.05.2026).

8. Найкращий VPN для комп'ютера та мобільних пристроїв. URL: https://www.opera.com/uk/features/vpn-pro/choosing-best-vpn (дата звернення: 07.05.2026).

9. IPsec. Wikipedia. URL: https://en.wikipedia.org/wiki/IPsec (дата звернення: 07.05.2026).

10. WireGuard vs OpenVPN vs IKEv2 – Complete Guide. URL: https://symlexvpn.com/wireguard-vs-openvpn-vs-ikev2-guide/ (дата звернення: 07.05.2026).

11. VPN Protocols Compared: WireGuard vs OpenVPN vs IKEv2 in 2026. URL: https://limevpn.com/blog/security/vpn-protocols-compared-wireguard-openvpn-ikev2-2026/ (дата звернення: 07.05.2026).

12. Comparing VPN Protocols: WireGuard vs OpenVPN vs IPsec. URL: https://cb.vu/vpn-ssh/vpn-protocol-comparison (дата звернення: 07.05.2026).

13. Demirdelen T., Kırmızı S. Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations. *Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi*. 2025. Vol. 8, no. 3. P. 1353–1369. URL: https://doi.org/10.47495/okufbed.1660352 (дата звернення: 07.05.2026).

14. Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions / J. Anyam et al. *Computers*. 2025. Vol. 14, no. 8. P. 326. URL: https://doi.org/10.3390/computers14080326 (дата звернення: 07.05.2026).

15. Що таке IPsec? Протокол конфіденційності для захисту інтернет-трафіку. URL: https://nym.com/uk/blog/що-таке-ipsec (дата звернення: 07.05.2026).

16. Integral methods for evaluating the performance of packetswitched networks: analysis and formulation. *Scientific Notes of the State University of Telecommunications*. 2024. Vol. 6, no. 1. URL: https://doi.org/10.31673/2786-8362.2024.025073 (дата звернення: 07.05.2026).

17. Ложковський А.Г. Теорія масового обслуговування в телекомунікаціях. Одеса: ОНАЗ ім. О.С. Попова, 2010. 112 с. URL: https://metod.suitt.edu.ua/download/230 (дата звернення: 07.05.2026).

18. M/M/1 queue. Wikipedia. URL: https://en.wikipedia.org/wiki/M/M/1_queue (дата звернення: 07.05.2026).

19. What Is Network Simulation? MATLAB & Simulink. MathWorks. URL: https://www.mathworks.com/discovery/network-simulation.html (дата звернення: 07.05.2026).

20. Aziz G. A., Jaber M. H., Sulttan M. Q., Shneen S. W. Simulation Model of Enhancing Performance of TCP/AQM Networks by Using Matlab. *Journal of Engineering and Technological Sciences.* 2022. Vol. 54, No. 4. P. 220404. URL: https://doi.org/10.5614/j.eng.technol.sci.2022.54.4.4 (дата звернення: 07.05.2026).

21. Klinkowski M., Więcek D. Performance Analysis of Data-Driven and Deterministic Latency Models in Dynamic Packet-Switched Xhaul Networks. *Applied Sciences*. 2025. Vol. 15, no. 23. P. 12487. URL: https://doi.org/10.3390/app152312487 (дата звернення: 07.05.2026).

22. Network Modeling, Simulation and Analysis in MATLAB. Wiley Online Books. URL: https://www.amazon.com/Network-Modeling-Simulation-Analysis-MATLAB-ebook/dp/B07WDM624G (дата звернення: 07.05.2026).

23. Створення корпоративної мережі передачі даних (VPLS, IP VPN). URL: https://kyivstar.ua/business/products/vpn (дата звернення: 07.05.2026).

24. Корпоративні мережі. URL: https://www.telecomsvit.com/telecom-services/multipoint-connection (дата звернення: 07.05.2026).

25. Communications Toolbox. MathWorks. URL: https://www.mathworks.com/products/communications.html

26. Statistics and Machine Learning Toolbox. MathWorks. URL: https://www.mathworks.com/products/statistics.html (дата звернення: 07.05.2026).

27. MathWorks. Unveils Release 2023b of MATLAB and Simulink Product Families. BusinessWire. 2023. URL: https://www.businesswire.com/news/home/20230921814233/en/MathWorks-

Introduces-Simulink-Fault-Analyzer-and-Polyspace-Test-in-MATLAB-and-Simulink-Release-2023b (дата звернення: 07.05.2026).

28. Simulink. MathWorks Product Overview. URL: https://www.mathworks.com/products/simulink.html (дата звернення: 07.05.2026).

29. What is Hub and Spoke Topology?. URL: https://www.cbtnuggets.com/blog/technology/networking/what-is-hub-and-spoke-topology (дата звернення: 07.05.2026).

30. Що таке приватна мережа передачі даних та як вона допомагає працювати бізнесу. Kyivstar Business Hub. URL: https://hub.kyivstar.ua/articles/shho-take-pryvatna-merezha-peredachi-danyh-ta-yak-vona-dopomagaye-praczyuvaty-biznesu (дата звернення: 07.05.2026).

31. Stochastic Models in Queueing Theory. Elsevier, 2003. 482 P. URL: https://doi.org/10.1016/b978-0-12-487462-6.x5000-0 (дата звернення: 07.05.2026).

32. Queuing Theory Applications to Communication Systems: Control of Traffic Flows and Load Balancing / P. Zeephongsekul et al. *Springer Handbook of Engineering Statistics*. London, 2006. P. 991–1022. URL: https://doi.org/10.1007/978-1-84628-288-1_52 (дата звернення: 07.05.2026).

33. Smith J. M. Introduction to Queueing Networks. Cham : Springer International Publishing, 2018. 562 P. URL: https://doi.org/10.1007/978-3-319-78822-7 (дата звернення: 07.05.2026).

34. ITU-T Recommendation G.114. One-way transmission time. ITU. 2003 (reconfirmed 2022). URL: https://www.itu.int/rec/T-REC-G.114/en (дата звернення: 07.05.2026).

35. Abdelmoniem A. M., Bensaou B. Enhancing TCP via Hysteresis Switching: Theoretical Analysis and Empirical Evaluation. *IEEE/ACM Transactions on Networking*. 2023. P. 1–0. URL: https://doi.org/10.1109/tnet.2023.3262564 (дата звернення: 07.05.2026).

36. M/M/1/K queue. Wikipedia. URL: https://en.wikipedia.org/wiki/M/M/1_queue#Finite_capacity_(M/M/1/K_queue) (дата звернення: 07.05.2026).

37. MATLAB Random Number Generation. MathWorks. URL: https://www.mathworks.com/help/matlab/random-number-generation.html (дата звернення: 07.05.2026).

38. Frankel S. et al. Guide to IPsec VPNs. NIST Special Publication 800-77 Rev. 1. 2020. URL: https://doi.org/10.6028/NIST.SP.800-77r1 (дата звернення: 07.05.2026).

39. Klinkowski M., Perelló J., Careglio D. Machine Learning-Aided Latency Prediction in Packet-Switched Xhaul Networks. *IEEE Access*. 2026. P. 1. URL: https://doi.org/10.1109/access.2026.3678383 (дата звернення: 07.05.2026).

40. Practical MATLAB Modeling with Simulink: Programming and Simulating Ordinary and Partial Differential Equations. URL: https://www.mathworks.com/academia/books/practical-matlab-modeling-with-simulink-eshkabilov.html (дата звернення: 07.05.2026).

41. High-Performance VoIP Session Border Controllers, Trusted by Service Providers Worldwide. URL: https://telcobridges.com/ (дата звернення: 07.05.2026).

42. Shortle J. F., Thompson J. M., Gross D., Harris C. M. Fundamentals of Queueing Theory. 5th ed. Wiley, 2022. 576 p. URL: https://www.amazon.com/Fundamentals-Queueing-Theory-Probability-Statistics/dp/0471170836 (дата звернення: 07.05.2026).

43. The Ultimate Guide to Setting Up an Enterprise VPN. URL: https://sase.checkpoint.com/blog/network/enterprise-vpn-setting (дата звернення: 07.05.2026).