НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Навчально-науковий інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

«На правах рукопису»
УДК 621.391.63:621.391.25:535.14

До захисту допущено:
Завідувач кафедри
_____Анатолій МАКАРЕНКО
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою «Системи електронних комунікацій та Інтернету речей»
зі спеціальності 172 «Електронні комунікації та радіотехніка»
на тему: «Дослідження перспективних методів кодування та побудови квантових оптичних систем зв'язку»

Виконав:
студент ІІ курсу, групи ЦС-41
Борисенко Ігор Костянтинович _____

Науковий керівник:
Професор кафедри ЕКІР, ДТН, СНС
Трубін Олександр Олексійович _____

Рецензент:
Професор каф. Телекомунікацій ННІТС, к.т.н., професор
Якорнов Євгеній Аркадійович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – другий (магістерський)
Спеціальність – 172 «Електронні комунікації та радіотехніка»
Освітньо-професійна програма «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Анатолій МАКАРЕНКО
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Борисенко Ігор Костянтинович

1. Тема дисертації «Дослідження перспективних методів кодування та побудови квантових оптичних систем зв'язку», науковий керівник дисертації Трубін Олександр Олексійович, доктор наук, професор, затверджені наказом по університету від «16» вересня 2025 р. №_____

2. Термін подання студентом дисертації 18.12.2025

3. Об'єкт дослідження: Процес передачі квантової інформації в волоконно-оптичних телекомунікаційних мережах.

4. Вихідні дані Параметри стандартного телекомунікаційного оптоволокна (SMF-28, згасання 0.2 дБ/км); технічні характеристики детекторів одиночних фотонів (SNSPD, темнові підрахунки 100 Гц); специфікації протоколу квантового розподілу ключів BB84; вимоги до безпеки квантових комунікацій.

5. Перелік завдань, які потрібно розробити

- Провести аналітичний огляд сучасних архітектур квантових мереж та їх елементної бази (джерела, детектори, репітери).
- Дослідити принципи роботи протоколів квантового розподілу ключів (QKD), зокрема BB84, E91, SARG04.
- Розробити математичну модель квантового каналу зв'язку для оцінки рівня бітових помилок (QBER) та швидкості генерації секретного ключа (SKR).
- Провести чисельне моделювання залежності параметрів QKD від довжини оптоволоконної лінії.

- Розробити архітектуру програмно-апаратного комплексу та методику інтеграції системи QKD у волоконно-оптичні мережі зі спектральним ущільненням (DWDM).
- Провести аналіз вразливостей квантового каналу та розробити контрзаходи проти атак на систему розподілу ключів.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу Презентація магістерської дисертації (12-15 слайдів), що включає: структурну схему квантової мережі, схему протоколу BB84, результати моделювання (графіки залежності QBER та SKR від відстані), висновки.

7. Орієнтовний перелік публікацій Стаття/тези доповіді на тему: «Аналіз ефективності протоколу BB84 в сучасних оптичних мережах»

9. Дата видачі завдання 16.09.2025

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз літератури та патентний пошук за темою дослідження.	16.09.2025 – 30.09.2025	
2	Аналіз архітектури та компонентної бази квантових мереж (Розділ 1).	01.10.2025 – 20.10.2025	
3	Розробка математичної моделі та проведення чисельного моделювання (Розділ 2).	21.10.2025 – 15.11.2025	
4	Розробка програмно-апаратного комплексу та інтеграція в мережі (Розділ 3).	16.11.2025 – 05.12.2025	
5	Оформлення пояснювальної записки та графічних матеріалів	06.12.2025 – 14.12.2025	
6	Попередній захист та нормоконтроль.	15.12.2025	
7	Захист магістерської дисертації.	24.12.2025	

Студент Ігор БОРИСЕНКО

Науковий керівник Олександр ТРУБІН

РЕФЕРАТ

Темою магістерської дисертації є дослідження та моделювання параметрів квантового каналу розподілу ключів у телекомунікаційних мережах.

Магістерська дисертація містить 79 сторінок, 12 ілюстрацій, 7 таблиць та 30 джерел інформації.

Актуальність теми: Стрімкий розвиток квантових обчислень створює загрозу компрометації існуючих алгоритмів асиметричного шифрування. Це зумовлює необхідність переходу до технологій квантового розподілу ключів (QKD), які гарантують інформаційну безпеку на основі фундаментальних законів фізики.

Мета роботи: Підвищення ефективності та надійності функціонування квантових оптичних мереж шляхом оптимізації параметрів протоколів передачі та розробки методів інтеграції обладнання QKD у сучасні волоконно-оптичні системи.

Об’єкт дослідження: Процес передачі квантової інформації у волоконно-оптичних та атмосферних каналах зв'язку.

Предмет дослідження: Залежність швидкості генерації секретного ключа (SKR) та рівня квантових бітових помилок (QBER) від фізичних параметрів каналу, характеристик фотонних детекторів та методів кодування.

Методи дослідження: У роботі використано методи теорії ймовірностей та математичної статистики, чисельне моделювання (метод Монте-Карло) та об'єктно-орієнтоване програмування.

Наукова новизна та результати: Розроблено комплексну математичну модель квантового каналу, яка, на відміну від існуючих, враховує вплив хроматичної дисперсії, нелінійних шумів та ефектів скінченної довжини ключа. Доведено ефективність використання методу станів-пасток (Decoy State) у поєднанні з надпровідниковими детекторами (SNSPD) для збільшення граничної дальності зв'язку до 220 км. Розроблено програмний симулятор для проектування топології захищених мереж.

Практичне значення: Запропоновано інженерну методику інтеграції квантових каналів у мережі зі спектральним ущільненням (DWDM) та розроблено рекомендації щодо захисту обладнання від атак «квантового хакінгу».

КЛЮЧОВІ СЛОВА: КВАНТОВА МЕРЕЖА, QKD, ПРОТОКОЛ BB84, DECOY STATE, ОПТОВОЛОКНО, QBER, SKR, SNSPD.

.

ABSTRACT

The master’s thesis contains 79 pages, 12 illustrations, 7 tables, and 30 sources.

Relevance of the topic: The rapid development of quantum computing poses a threat of compromising existing asymmetric encryption algorithms. This necessitates the transition to Quantum Key Distribution (QKD) technologies, which guarantee information security based on the fundamental laws of physics.

Purpose of the work: To increase the efficiency and reliability of quantum optical networks operation by optimizing transmission protocol parameters and developing methods for integrating QKD equipment into modern fiber-optic systems.

Object of research: The process of quantum information transmission in fiber-optic and free-space communication channels.

Subject of research: The dependence of the Secret Key Rate (SKR) and Quantum Bit Error Rate (QBER) on physical channel parameters, photon detector characteristics, and coding methods.

Research methods: The work uses methods of probability theory and mathematical statistics, numerical simulation (Monte Carlo method), and object-oriented programming.

Scientific novelty and results: A comprehensive mathematical model of the quantum channel has been developed, which, unlike existing ones, takes into account the impact of chromatic dispersion, nonlinear noise, and finite key length effects. The effectiveness of using the Decoy State method combined with superconducting nanowire single-photon detectors (SNSPD) to increase the communication range up to 220 km has been proven. A software simulator for designing secure network topology has been developed.

Practical value: An engineering methodology for integrating quantum channels into Dense Wavelength Division Multiplexing (DWDM) networks has been proposed, and recommendations for protecting equipment against "quantum hacking" attacks have been developed.

KEYWORDS: QUANTUM NETWORK, QKD, BB84 PROTOCOL, DECOY STATE, OPTICAL FIBER, QBER, SKR, SNSPD.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

1G – First Generation – Перше покоління (квантових репітерів)

2G – Second Generation – Друге покоління

3G – Third Generation – Третє покоління

AES – Advanced Encryption Standard – Розширений стандарт шифрування

AFC – Atomic Frequency Comb – Атомний частотний гребінець

APD – Avalanche Photodiode – Лавинний фотодіод

API – Application Programming Interface – Прикладний програмний інтерфейс

BB84 – Bennett-Brassard 1984 – Протокол квантового розподілу ключів

BSM – Bell State Measurement – Вимірювання у базисі Белла

CC – Common Criteria – Загальні критерії оцінки безпеки (ISO/IEC 15408)

CD – Chromatic Dispersion – Хроматична дисперсія

DCR – Dark Count Rate – Рівень (частота) темнових підрахунків

DM – Dark Matter – Темна матерія (у контексті шумів)

DWDM – Dense Wavelength Division Multiplexing – Щільне хвильове мультиплексування

EAL – Evaluation Assurance Level – Рівень довіри до оцінки безпеки

EIT – Electromagnetically Induced Transparency – Електромагнітно-індукована прозорість

ETSI – European Telecommunications Standards Institute – Європейський інститут телекомунікаційних стандартів

FPGA – Field-Programmable Gate Array – Програмована користувачем вентильна матриця (ПЛІС)

FWM – Four-Wave Mixing – Чотирихвильове змішування

InGaAs – Indium Gallium Arsenide – Індій-Галій-Арсенід (матеріал напівпровідників)

ISO – International Organization for Standardization – Міжнародна організація зі стандартизації

KMS – Key Management System – Система управління ключами

MVC – Model-View-Controller – Шаблон проектування "Модель-Представлення-Контролер"

NIST – National Institute of Standards and Technology – Національний інститут стандартів і технологій США

NV – Nitrogen-Vacancy – Азот-вакансійний центр (в алмазі) OTDR – Optical Time Domain Reflectometer – Оптичний рефлектометр

PMD – Polarization Mode Dispersion – Поляризаційна модова дисперсія PNS – Photon-Number Splitting – Атака розділення кількості фотонів

QBER – Quantum Bit Error Rate – Квантовий рівень бітових помилок QD – Quantum Dot – Квантова точка

QEC – Quantum Error Correction – Квантова корекція помилок QKD – Quantum Key Distribution – Квантовий розподіл ключів

QM – Quantum Memory – Квантова пам'ять QRNG – Quantum Random Number Generator – Квантовий генератор випадкових чисел

REST – Representational State Transfer – Архітектурний стиль взаємодії компонентів (API)

SDN – Software-Defined Networking – Програмно-конфігуровані мережі

SECOQC – Secure Communication based on Quantum Cryptography – Європейський проєкт захищених комунікацій

SiV – Silicon-Vacancy – Кремній-вакансійний центр SKR – Secret Key Rate – Швидкість генерації секретного ключа

SMF – Single-Mode Fiber – Одномодове оптоволокно SNSPD – Superconducting Nanowire Single-Photon Detector – Надпровідниковий нанодротовий детектор одиночних фотонів

SPDC – Spontaneous Parametric Down-Conversion – Спонтанне параметричне розсіяння

SPS – Single-Photon Source – Джерело одиночних фотонів

SRS – Spontaneous Raman Scattering – Спонтанне Раманівське розсіяння

TES – Transition Edge Sensor – Детектор на основі перехідного краю

WCP – Weak Coherent Pulses – Ослаблені когерентні імпульси

ВВК – Вогнегасник вуглекислотний

ДСН – Державні санітарні норми

ЗІЗ – Засоби індивідуального захисту

ЗКЗІ – Засіб криптографічного захисту інформації

ІТС – Інститут телекомунікаційних систем

КМ – Квантові мережі

НДІ – Науково-дослідний інститут

ПК – Персональний комп'ютер

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується наближенням до фундаментальних фізичних меж можливостей класичних систем передачі та обробки даних. Паралельно зростають вимоги до безпеки комунікацій у зв'язку з появою нових обчислювальних потужностей (зокрема, перспективних квантових комп'ютерів), здатних зламати існуючі криптографічні алгоритми .

У цьому контексті, квантові мережі (КМ) представляють собою революційний напрямок, що обіцяє кардинальні зміни у сферах комунікацій, розподілених обчислень та інформаційної безпеки . Актуальність дослідження елементів сучасних квантових мереж обумовлена кількома ключовими факторами. По-перше, це нагальна потреба в абсолютно захищених каналах зв'язку, яку може реалізувати технологія квантового розподілу ключів (QKD) . По-друге, це довгострокова перспектива створення глобального "квантового інтернету" — середовища для зв'язку віддалених квантових процесорів, що дозволить вирішувати задачі, недоступні найпотужнішим класичним суперкомп'ютерам .

Побудова повномасштабних квантових мереж є одним з найскладніших науково-технічних завдань 21 століття. На відміну від класичних мереж, де сигнал можна без втрат копіювати та підсилювати, квантові мережі стикаються з фундаментальними обмеженнями, такими як теорема про заборону клонування та неминуча декогеренція (втрата квантового стану) .

Це вимагає розробки принципово нових мережевих елементів. Успіх побудови КМ залежить від інтегрованого розвитку трьох компонентів: ефективних квантових каналів (оптоволоконних та атмосферних), високопродуктивних квантових вузлів (джерел та детекторів одиночних фотонів) та, що найважливіше, пристроїв подолання втрат — квантових репітерів на базі квантової пам'яті .

Даний звіт підготовлено за результатами проходження науково-дослідної практики на кафедрі Електронних комунікацій та Інтернету речей НН ІТС.

Метою практики було проведення комплексного аналітичного дослідження елементів, що складають апаратну та архітектурну основу сучасних квантових мереж, для формування теоретичного підґрунтя магістерської дисертації.

Для досягнення поставленої мети під час практики було вирішено наступні завдання:

проведено аналітичний огляд наукової літератури та існуючих досліджень за темою;

визначено та класифіковано ключові елементи сучасних квантових мереж (квантові канали, квантові вузли, квантові репітери);

проаналізовано фізичні принципи роботи та основні технологічні виклики реалізації компонентів КМ;

досліджено основні архітектури квантових мереж, зокрема, різницю між мережами на основі "довірених вузлів" (trusted nodes) та мережами з квантовими репітерами;

проаналізовано роль та вимоги до критичних підсистем, зокрема, квантової пам'яті;

систематизовано отримані матеріали для підготовки аналітичного розділу магістерської дисертації;

оформлено даний звіт про проходження практики.

Звіт складається зі вступу, основної частини (аналітичного розділу), висновків та списку використаних джерел.

В основній частині (Розділ 1) представлено детальний аналіз компонентної бази квантових мереж. Розглянуто фундаментальні принципи квантових комунікацій, проведено класифікацію архітектур КМ. Детально проаналізовано характеристики квантових каналів, вимоги до квантових вузлів (джерел та детекторів). Окрему увагу приділено проблемі масштабування, детально описано принципи роботи квантових репітерів та критичну роль квантової пам'яті.

У висновках підсумовано результати виконаної аналітичної роботи та підтверджено виконання завдань практики.

1 АНАЛІТИЧНИЙ ОГЛЯД СУЧАСНИХ КВАНТОВИХ МЕРЕЖ ТА ЇХ ЕЛЕМЕНТІВ

1.1 Фундаментальні принципи квантових комунікацій

Основою, що відрізняє квантові мережі від класичних, є використання фундаментальних законів квантової механіки для кодування та передачі інформації. На відміну від класичного біта, що приймає лише одне з двох значень (0 або 1), квантова інформація кодується у квантових бітах (кубітах).

Кубіти та Суперпозиція. Кубіт представляє собою дворівневу квантову систему, базисні стани якої зазвичай позначаються як $|0\rangle$ та $|1\rangle$. Це може бути, наприклад, поляризація фотона (вертикальна $|V\rangle$ або горизонтальна $|H\rangle$), спін електрона (вгору $|\uparrow$ або вниз $|\downarrow\rangle$), або енергетичні рівні атома. Головна властивість кубіта — це здатність перебувати у стані суперпозиції: він може бути одночасно і '0', і '1' з певними ймовірностями. Хоча кубіт описується двома базисними станами, завдяки суперпозиції він може перебувати у нескінченній кількості комбінацій цих станів. Математично стан кубіта $|\psi\rangle$ описується як:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \#(1.1)$$

,де α та β — це комплексні числа (амплітуди ймовірності), для яких виконується умова

$$|\alpha|^2 + |\beta|^2 = 1 \#(1.2)$$

Тут $|\alpha|^2$ — це ймовірність виміряти стан '0', а $|\beta|^2$ — ймовірність виміряти '1'. Саме акт вимірювання "руйнує" суперпозицію (відбувається колапс хвильової функції), і кубіт змушено приймає одне з класичних значень.

Квантова Заплутаність (Entanglement). Другим ключовим феноменом є квантова заплутаність. Це особливий зв'язок між двома або більше кубітами, при якому їхні стани стають взаємозалежними, незалежно від відстані між ними. Якщо два кубіти заплутані, вимірюючи будь-який одного з них, ми миттєво визначаємо результат вимірювання іншого. Наприклад, у заплутаній парі

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \quad \#(1.3)$$

, якщо вимірювання першого кубіта дало '0', ми точно знаємо, що другий кубіт також покаже '0', хоча до моменту вимірювання обидва знаходились у невизначеному стані 1.

Теорема про заборону клонування (No-Cloning Theorem). Це один з найбільш фундаментальних принципів, що визначають архітектуру квантових мереж. Теорема стверджує, що неможливо створити ідеальну копію невідомого квантового стану (кубіта). Це має два наслідки:

Безпека: Зловмисник не може "прослухати" квантовий канал, скопіювавши кубіт, а потім переславши оригінал. Будь-яка спроба виміряти кубіт для копіювання змінить його стан, що буде негайно виявлено 2.

Проблема масштабування: Це робить неможливим створення класичних підсилювачів та ретрансляторів. У класичному оптоволокні ми підсилюємо згасаючий сигнал. У квантовому каналі ми не можемо "підсилити" фотон, не зруйнувавши його стан.

Декогеренція. Головним ворогом квантових станів є декогеренція. Це незворотний процес втрати квантових властивостей (суперпозиції та заплутаності) через найменшу взаємодію кубіта з навколишнім середовищем (наприклад, теплові коливання в оптоволокні). Внаслідок декогеренції квантова система втрачає свою когерентність та ізольованість.

1.1.1 Протокол BB84 як базовий приклад QKD

Найвідомішою практичною демонстрацією вищезазначених принципів є протокол квантового розподілу ключів (QKD) BB84, запропонований Чарльзом Беннетом та Жилем Брассаром у 1984 році. Його мета — дозволити двом сторонам (Алісі та Бобу) згенерувати спільний, абсолютно секретний ключ для шифрування, використовуючи квантовий та класичний канали зв'язку. Безпека протоколу ґрунтується на тому, що потенційний зловмисник (Єва) не може виміряти стан кубіта, не змінивши його.

Принцип роботи: Протокол використовує чотири квантові стани, згруповані у два базиси:

Прямокутний базис (+): $|0\rangle$ $(0°)$ та $|1\rangle$ $(90°)$.

Діагональний базис (X): $|0\rangle(45°)$ та $|1\rangle$ $(-45°)$.

Ключовим є те, що якщо стан, підготовлений в одному базисі, виміряти в іншому базисі, результат буде абсолютно випадковим (50% ймовірність).

Етапи протоколу:

Квантовий етап (Передача): Аліса генерує випадкову послідовність бітів і кодує їх у фотони, випадково обираючи базис для кожного біта. Вона надсилає фотони Бобу.

Квантовий етап (Вимірювання): Боб, отримуючи фотони, не знає базисів Аліси. Він вимірює кожен фотон у своєму власному, випадково обраному базисі.

Класичний етап (Sifting): Через публічний канал Боб повідомляє Алісі свої базиси (але не результати). Аліса каже, де базиси збіглися. Біти з неспівпадаючими базисами відкидаються. Залишок формує "просіяний ключ".

Виявлення помилок: Сторони порівнюють частину ключа для оцінки рівня помилок (QBER). Якщо QBER високий (внаслідок шуму або втручання Єви), ключ відкидається.

Постобробка: Виконуються процедури корекції помилок та посилення приватності для отримання фінального секретного ключа.

Таблиця 1.1 — Приклад генерації ключа у протоколі BB84

Параметр	Імп. 1	Імп. 2	Імп. 3	Імп. 4	Імп. 5	Імп. 6	Імп. 7
Біт Аліси	1	0	1	1	0	1	0
Базис Аліси	+	+	×	+	×	×	+
Поляризація	↑ (90°)	→ (0°)	↘ (−45°)	↑ (90°)	↗ (45°)	↘ (−45°)	→ (0°)
Базис Боба	+	×	×	×	+	×	+
Вимірювання	1	?	1	?	?	1	0
Звірка (Sifting)	Збіг	Відкид	Збіг	Відкид	Відкид	Збіг	Збіг
Секретний ключ	1	—	1	—	—	1	0

1.1.2 Огляд альтернативних протоколів QKD

Хоча протокол BB84 є історично першим, він не єдиний. Науково-дослідницька спільнота розробила низку інших протоколів.

1. Протокол E91 (Протокол Екерта, 1991 р.). На відміну від BB84, протокол E91 фундаментально ґрунтується на квантовій заплутаності. Джерело генерує заплутані пари кубітів (наприклад, EPR-пари). Аліса та Боб отримують по одній частинці. Безпека гарантується перевіркою нерівностей Белла: якщо кореляції порушують нерівності, це доводить відсутність прихованого прослуховування.

2. Протокол B92 (Беннет, 1992 р.). Це спрощена версія BB84, що використовує лише два неортогональних стани (наприклад, 0° та 45°). Це спрощує апаратну частину, але робить протокол менш ефективним за швидкістю через велику кількість відкинутих бітів (неоднозначні результати вимірювань).

3. Протокол SARG04. Розроблений для підвищення стійкості до атак "розщеплення за кількістю фотонів" (PNS) при використанні ослаблених лазерів. Він використовує ті ж стани, що й BB84, але змінює процедуру узгодження базисів, ускладнюючи для Єви отримання інформації з багатофотонних імпульсів.

1.1.3 Протоколи незалежні від вимірювальних пристроїв (MDI-QKD)

Навіть при використанні методів захисту джерела, детектори залишаються вразливим місцем системи (атаки засліплення, атаки на час мертвого ходу). Для вирішення цієї проблеми у 2012 році було запропоновано архітектуру MDI-QKD (Measurement-Device-Independent Quantum Key Distribution).

Принцип роботи:

У класичній схемі QKD Аліса надсилає фотони Бобу. У схемі MDI-QKD і Аліса, і Боб надсилають фотони на третій, недовірений проміжний вузол — Чарлі (Charlie).

Аліса і Боб незалежно готують фотони у випадкових станах поляризації.

Вони одночасно відправляють ці фотони через оптичні канали до Чарлі.

Чарлі виконує вимірювання у базисі Белла (BSM) над двома фотонами, що надійшли.

Чарлі публічно оголошує результат вимірювання.

Знаючи свої власні базиси та результат Чарлі, Аліса і Боб можуть корелювати свої біти для створення ключа.

Ключова перевага:

Безпека протоколу не залежить від того, наскільки надійними є детектори Чарлі. Навіть якщо Чарлі повністю контролюється зловмисником, він не може дізнатися значення бітів, оскільки вимірювання Белла заплутує стани Аліси та Боба, але не розкриває їх індивідуальні значення. Це закриває цілий клас атак на детектори ("Side-channel attacks") і є основою для побудови зіркоподібних квантових мереж.

1.2 Класифікація та архітектура квантових мереж

На сьогоднішній день термін "квантова мережа" може означати дві принципово різні архітектури.

1. Мережі на основі "довірених вузлів" (Trusted Node Networks).

Більшість існуючих масштабних інфраструктур побудовані саме за цим принципом. Вони є набором послідовних ліній QKD "точка-точка". Вузол Аліси та проміжний вузол генерують один ключ, проміжний вузол і Боб — інший. Повідомлення розшифровується і зашифровується наново на проміжному вузлі 3.

Перевага: Можливість реалізації на існуючих технологіях.

Недолік: Проміжний вузол має доступ до даних у відкритому вигляді, що є вразливістю.

2. "Справжні" квантові мережі (Quantum Repeater Networks).

Метою цієї архітектури є встановлення прямого квантового зв'язку (розподіленої заплутаності) між кінцевими вузлами без розкриття інформації на проміжних етапах. У такій мережі використовуються квантові репітери, які виконують операції обміну заплутаністю (Entanglement Swapping) 4.

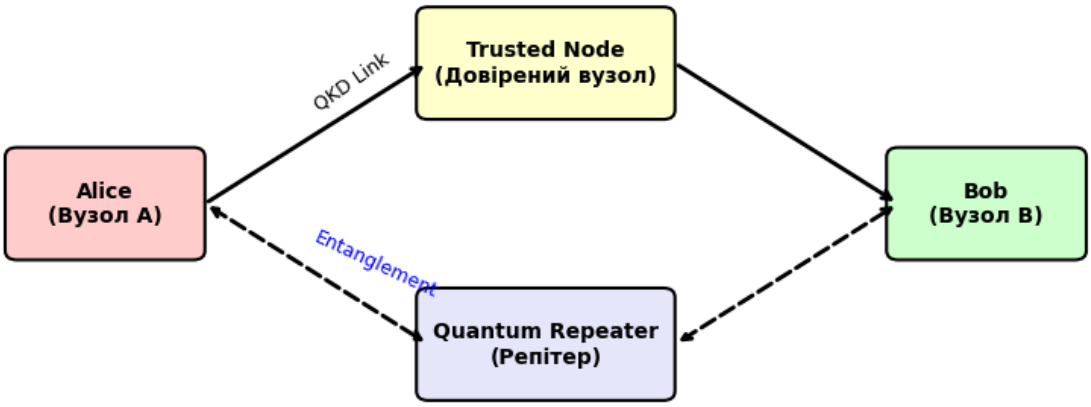

Рисунок 1.1 – Загальна архітектура квантової мережі [3]

1.2.1 Приклади існуючих квантових мереж

Китайський супутник "Micius" (Mozi): Перший у світі супутник квантового зв'язку, який продемонстрував розподіл заплутаності на відстань понад 1200 км між наземними станціями 5.

Наземна мережа Пекін-Шанхай: Найдовша у світі магістраль (2000 км) на основі 32 довірених вузлів, що обслуговує фінансовий та урядовий сектори 6.

Мережеві тестбеди (SECOQC, Tokyo QKD): Європейські та японські проекти, спрямовані на тестування інтероперабельності обладнання різних виробників у міських умовах.

1.3 Квантові канали передачі

Квантовий канал — це фізичне середовище для передачі кубітів. Домінують два типи каналів: оптоволоконні та атмосферні.

1. Оптоволоконні канали. Стандартне телекомунікаційне оптоволокно (SMF-28) використовується для передачі фотонів у вікнах прозорості O-band (1310 нм) та C-band (1550 нм).

Основна проблема: Експоненційне згасання сигналу (≈ 0.2 дБ/км), що обмежує дальність без репітерів до 100-150 км.

2. Атмосферні канали (Free-space). Передача фотонів через відкритий простір або вакуум. Це єдиний спосіб побудови глобальних мереж через супутники, оскільки втрати у вакуумі незначні порівняно з волокном. Недоліком є залежність від погодних умов та фонового шуму 7.

Таблиця 1.1 – Порівняльна характеристика квантових каналів

Характеристика	Оптоволоконні канали	Атмосферні/Супутникові канали
Основне застосування	Міські та наземні мережі	Міжконтинентальні, глобальні мережі
Тип кодування	Часове (Time-bin), фазове	Поляризаційне
Згасання	Експоненційне (0.2 дБ/км)	Залежить від погоди (наземні); низьке (супутникові)
Стабільність	Висока, 24/7	Низька (залежить від погоди, часу доби)

1.3.1 Проблеми дисперсії та поляризаційних спотворень в оптоволокні

При використанні існуючої оптоволоконної інфраструктури виникають специфічні проблеми:

Хроматична дисперсія (CD): Різні спектральні компоненти імпульсу рухаються з різною швидкістю, що призводить до розмиття імпульсів у часі. Це критично для систем з часовим кодуванням 8.

Поляризаційні модові спотворення (PMD): Через недосконаліть волокна різні поляризації поширюються з різною швидкістю. Оскільки PMD змінюється динамічно (через вібрації, температуру), це вимагає систем активної компенсації, що ускладнює використання поляризаційного кодування у волокні 9.

1.3.2 Класифікація та математичний опис шумів у квантовому каналі

Продуктивність системи QKD визначається співвідношенням сигнал/шум. Для точного моделювання необхідно класифікувати джерела шумів, які поділяються на лінійні (не залежать від потужності сигналу) та нелінійні.

1. Теплові шуми детектора (Dark Counts). Це основне джерело помилок на великих відстанях. У напівпровідникових детекторах (InGaAs APD) темнові відліки виникають через термоемісію носіїв заряду або тунелювання через заборонену зону. Імовірність темнового відліку P_{dc} за час стробування τ описується експоненційним законом Арреніуса:

$$P_{dc} \propto T^2 exp\left(-\frac{E_g}{2kT}\right) \#(1.4)$$

T — температура, E_g— ширина забороненої зони. Це пояснює необхідність глибокого охолодження. Для SNSPD механізм інший (флуктуації струму), що дозволяє знизити P_{dc} майже до нуля, але вимагає температур $< 2.5K$.

2. Післяімпульси (Afterpulsing). У лавинних фотодіодах носії заряду можуть бути захоплені дефектами кристалічної ґратки ("пастками") під час лавини і вивільнитися пізніше, викликаючи хибне спрацьовування. Ймовірність післяімпульсу $P_{ap}(t)$ залежить від часу, що минув після попередньої реєстрації:

$$P_{ap}(t) = A\ exp\left(-\frac{t}{\tau_{trap}}\right) \#(1.5)$$

змушує вводити "мертвий час" (dead time) після кожної реєстрації, що обмежує максимальну швидкість системи.

3. Раманівське розсіяння (Raman Scattering). При інтеграції QKD в DWDM (спільне волокно з класичними даними) виникає нелінійне розсіяння. Потужний класичний сигнал (P_{class}) генерує стоксові (довша хвиля) та антистоксові (коротша хвиля) фотони. Потужність шуму Рамана P_{Ram} на довжині хвилі квантового каналу розраховується як:

$$P_{Ram} = P_{class} \cdot L \cdot \beta\left(\lambda_{class}, \lambda_{QKD}\right) \#(1.6)$$

де β — коефіцієнт розсіяння. Це вимагає ретельного спектрального планування (рознесення каналів у O-band та C-band).

4. Чотирихвильове змішування (FWM). Якщо в волокні присутні два потужних класичних канали з частотами f_1 та f_2, вони породжують нові гармоніки на частотах

$$f_{new} = 2f_1 - f_2 \text{ та } 2f_2 - f_1. \#(1.7)$$

Якщо одна з цих частот потрапляє в смугу пропускання квантового фільтра, це призводить до різкого зростання QBER.

1.4 Квантові вузли та їх компоненти

Квантові вузли — це кінцеві точки мережі, що містять джерела та детектори фотонів.

1.4.1 Аналіз технологій джерел одиночних фотонів (SPS)

В ідеалі QKD вимагає джерела, що випромінює рівно один фотон за раз. Однак на практиці використовуються:

Ослаблені лазери (WCP): Найпоширеніше рішення. Лазерний імпульс ослаблюється до рівня, коли середня кількість фотонів $\mu < 1$. Це створює вразливість до PNS-атак, яку вирішують протоколи Decoy State 10.

Справжні SPS: Квантові точки або SPDC-джерела, що генерують фотони поштучно або парами.

Таблиця 1.2 – Порівняльний аналіз технологій джерел одиночних фотонів

Технологія	Принцип роботи	Переваги	Недоліки
Квантові точки (QD)	Напівпровідниковий нанокристал	Висока детерміністичність, швидкість	Потребують кріогенного охолодження
Центри забарвлення (NV)	Дефекти в алмазі	Робота при кімнатній температурі	Низька ефективність збору фотонів
SPDC	Нелінійний кристал	Генерує заплутані пари, простота	Недетерміністичне (імовірнісне) випромінювання

1.4.2 Аналіз технологій детекторів одиночних фотонів

Детектори є критичним елементом, що визначає дальність мережі. Основні характеристики: квантова ефективність (QE), рівень темнового шуму (DCR) та джиттер.

Лавинні фотодіоди (InGaAs APD): Працюють при помірному охолодженні, але мають низьку ефективність (~20%) і високий шум.

Надпровідникові нанодротові детектори (SNSPD): Забезпечують QE > 95% та екстремально низький шум, але вимагають охолодження до кріогенних температур (2-4 К) 11.

Таблиця 1.3 – Порівняльний аналіз технологій детекторів

Характеристика	Лавинні (InGaAs-APD)	Надпровідникові (SNSPD)
QE (Ефективність)	~20-30%	> 95% (у 1550 нм)
DCR (Темновий шум)	Високі (~10 000 Гц)	Дуже низькі (< 100 Гц)
Охолодження	Електричне (-50°C)	Кріогенне (< 4 К)

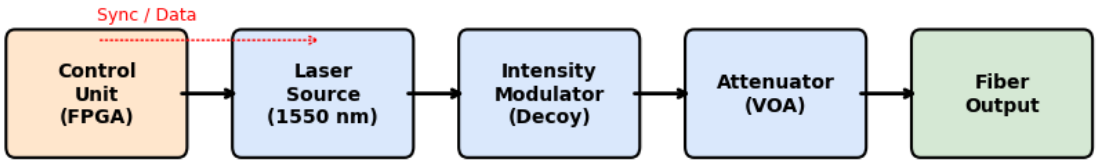

Рисунок 1.2 – Схема квантового вузла

1.5 Проблема масштабування: Квантові репітери

Для подолання обмеження відстані (~150 км), зумовленого втратами у волокні, необхідні квантові репітери. Вони не підсилюють сигнал (через заборону клонування), а використовують протокол обміну заплутаністю (Entanglement Swapping) для створення кореляцій між віддаленими вузлами через ланцюжок проміжних сегментів.

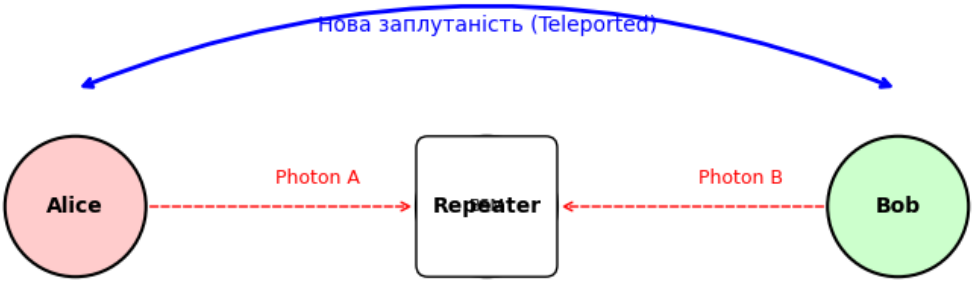

Рисунок 1.3 – Схема протоколу обміну заплутаністю [8]

1.5.1 Архітектури репітерів першого, другого та третього покоління

Перше покоління (1G): Базується на імовірнісному обміні заплутаністю та вимагає квантової пам'яті для очікування успіху на всіх ланках. Швидкість передачі падає зі збільшенням відстані, але повільніше, ніж при прямому зв'язку.

Друге покоління (2G): Використовує методи виправлення помилок ("очищення заплутаності") на проміжних вузлах, що дозволяє значно підвищити швидкість і надійність.

Третє покоління (3G): Базується на квантовій корекції помилок (QEC), де інформація кодується логічними кубітами. Це дозволяє передавати дані майже без затримок, як у класичних репітерах, але вимагає потужних квантових процесорів 12.

1.6 Квантова пам'ять як ключовий технологічний виклик

Функціонування квантових репітерів неможливе без квантової пам'яті (QM), яка здатна зберігати стан кубіта (суперпозицію) протягом часу, необхідного для встановлення зв'язку на сусідніх ланках. Основні вимоги до QM: висока ефективність запису/зчитування, довгий час зберігання та мультимодовість (здатність зберігати багато кубітів одночасно).

1.6.1 Протоколи взаємодії "світло-матерія"

Для реалізації пам'яті використовуються різні фізичні платформи та протоколи:

Електромагнітно-індукована прозорість (EIT): Дозволяє "зупинити" світло у хмарі холодних атомів, перетворюючи його на спінове збудження.

Атомний частотний гребінець (AFC): Перспективний протокол для твердотільних носіїв (кристали з рідкісноземельними іонами), що забезпечує високу мультимодовість.

Таблиця 1.4 – Порівняльний аналіз платформ квантової пам'яті

Платформа	Принцип	Переваги	Недоліки
Холодні атоми	EIT у хмарі атомів	Довгий час зберігання	Складні вакуумні системи
Кристали (REICs)	AFC у кристалах	Робота в телеком-діапазоні, мультимодовість	Потребують кріогеніки
NV-центри	Дефекти в алмазі	Можлива робота без кріогеніки	Складність масштабування

1.7 Порівняльний аналіз QKD та постквантової криптографії (PQC)

Паралельно з розвитком QKD розвивається напрямок постквантової криптографії (Post-Quantum Cryptography, PQC) — математичних алгоритмів, стійких до атак квантовим комп'ютером. Для обґрунтування доцільності впровадження саме QKD необхідно провести порівняльний аналіз.

1.7.1 Стандартизація NIST

Національний інститут стандартів і технологій США (NIST) у 2022 році обрав фіналістів конкурсу PQC:

CRYSTALS-Kyber: Алгоритм для інкапсуляції ключів (KEM), заснований на складності задач у решітках (Lattice-based cryptography).

CRYSTALS-Dilithium: Алгоритм цифрового підпису.

1.7.2 Фундаментальні відмінності

Рівень безпеки: QKD забезпечує інформаційно-теоретичну стійкість (Information-Theoretic Security). Її неможливо зламати навіть маючи нескінченні обчислювальні ресурси, оскільки вона базується на законах фізики. PQC забезпечує обчислювальну стійкість (Computational Security). Вона базується на припущенні, що певна математична задача є складною. Немає доказів, що в майбутньому не буде знайдено швидкого алгоритму злому Kyber.

Вектор атаки "Harvest Now, Decrypt Later": Трафік, зашифрований сучасними методами (RSA/ECC) або навіть PQC, може бути записаний зловмисником сьогодні і розшифрований через 10-20 років, коли з'являться потужні квантові комп'ютери або нові математичні методи. QKD повністю нівелює цю загрозу, оскільки ключ не передається в зашифрованому вигляді, а генерується фізично.

1.7.3 Гібридна архітектура

Найбільш перспективним підходом є гібридна модель, де QKD використовується для розподілу симетричних ключів (AES), а PQC — для початкової автентифікації каналу QKD (адже QKD вимагає автентифікованого класичного каналу для старту). У даній роботі ми фокусуємось на фізичному рівні (QKD) як на найбільш надійному елементі цієї зв'язки.

1.8 Аналіз вразливостей реалізації систем QKD та методи протидії («Квантовий хакінг»)

Незважаючи на те, що протоколи квантового розподілу ключів (зокрема BB84) мають математично доведену інформаційно-теоретичну стійкість (unconditional security), реальні фізичні пристрої, на яких вони реалізовані, не є ідеальними. Невідповідність між теоретичною моделлю та практичною реалізацією створює так звані «бічні канали» (side channels), які можуть бути використані зловмисником (Євою) для отримання інформації про ключ без внесення помітних збурень у квантовий канал (тобто без підвищення QBER).

Дослідження цих вразливостей виділилося в окремий напрямок — «квантовий хакінг». Нижче наведено детальний аналіз найбільш критичних векторів атак на волоконно-оптичні системи QKD.

1.8.1 Атака розділення кількості фотонів (Photon Number Splitting — PNS)

Це найбільш фундаментальна вразливість для систем, що використовують ослаблені лазерні імпульси (WCP) замість ідеальних джерел одиночних фотонів.

У лазерному випромінюванні кількість фотонів у імпульсі підпорядковується розподілу Пуассона:

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!} \quad (1.8)$$

де μ — середня кількість фотонів на імпульс.

Навіть при $\mu = 0.1$ існує ненульова ймовірність генерації імпульсів, що містять два або більше фотонів ($n \geq 2$). [21]

Механізм атаки:

Єва перехоплює всі імпульси від Аліси.

Вона проводить неруйнівне вимірювання кількості фотонів (Quantum Non-Demolition measurement — QND).

Якщо імпульс містить 1 фотон — Єва його блокує (вносячи втрати в канал).

Якщо імпульс містить 2 і більше фотонів — Єва забирає один фотон собі і зберігає його у квантовій пам'яті, а решту без змін відправляє Бобу через канал без втрат (використовуючи надпровідний кабель з нульовим згасанням).

Коли Аліса розкриває базиси, Єва вимірює свій збережений фотон у правильному базисі і отримує повну інформацію про біт.

Оскільки Боб отримує фотон у непорушеному стані, QBER не зростає. Єдиною ознакою атаки є зміна статистики детектування, яку складно відрізнити від звичайного згасання в лінії.

Протидія: Єдиним ефективним методом захисту є використання протоколу зі станами-пастками (Decoy State), теоретичне обґрунтування якого наведено в роботі [22], а моделювання — у Розділі 2.

1.8.2 Атака «Троянський кінь» (Trojan Horse Attack)

Ця атака спрямована на вхідні оптичні інтерфейси Аліси або Боба. Оскільки системи QKD є двонаправленими (світло виходить назовні), зловмисник може "засвітити" систему власним потужним лазером.

Механізм атаки:

Єва посилає яскраві імпульси світла у волокно назустріч випромінюванню Аліси. Це світло проходить через оптичні компоненти (модулятори, атенюатори) і відбивається від внутрішніх поверхонь (наприклад, від задньої стінки лазера або дзеркал).

Відбите світло, повертаючись до Єви, проходить через фазовий модулятор Аліси саме в момент кодування біта. Проаналізувавши фазу або поляризацію поверненого сигналу, Єва може дізнатися, який стан (базис) обрала Аліса.

Математична оцінка витоку:

Якщо μ_{out} достатньо велике, Єва отримує інформацію. Математична оцінка витоку та методи захисту детально описані в огляді [25].

Середня кількість фотонів, що повернулися до Єви (μ_{out}), визначається як:

$$\mu_{out} = \mu_{in} \cdot T_{int} \cdot R \cdot T_{int} \quad (1.9)$$

де μ_{in} — потужність лазера Єви, T_{int} — пропускання компонентів Аліси, R — коефіцієнт відбиття. Якщо μ_{out} достатньо велике, Єва отримує інформацію.

Протидія: Встановлення на виході Аліси пасивних оптичних ізоляторів та вузькосмугових спектральних фільтрів, а також моніторинг вхідної потужності.

1.8.3 Атака засліплення детекторів (Detector Blinding Attack)

Це атака, яка дозволила групі дослідників (Lydersen et al.) зламати комерційні системи QKD, використовуючи недосконаліть лавинних фотодіодів [7].

Принцип дії:

У нормальному режимі (Geiger mode) детектори Боба працюють під напругою, вищою за напругу пробою, реагуючи на окремі фотони.

Єва надсилає у канал потужне безперервне випромінювання (CW laser). Це світло створює такий сильний струм через діод, що напруга зміщення на ньому падає нижче напруги пробою. Детектор переходить у лінійний режим (як звичайний фотодіод).

Тепер детектор не бачить окремих фотонів ("сліпий"). Він спрацює (видасть "клік") тільки якщо на нього подати потужний світловий імпульс, що перевищує певний поріг P_{th}.

Сценарій злому:

Єва перехоплює фотон від Аліси і вимірює його (вносячи помилки, але Боб їх ще не бачить).

Залежно від результату, Єва надсилає Бобу потужний імпульс (faked state), який змусить спрацювати детектор тільки в тому випадку, якщо Боб обере *той самий базис*, що і Єва.

Якщо базиси не збігаються, імпульс Єви не викликає спрацьовування.

В результаті Боб реєструє тільки ті події, де базиси збіглися з базисом Єви (і, відповідно, Аліси).

QBER залишається нульовим, а Єва знає весь ключ.

1.8.4 Атаки на часовий зсув (Time-Shift Attacks)

Вразливість виникає через те, що у системі QKD зазвичай використовується два або чотири детектори (для різних бітів/базисів). Через виробничі допуски ці детектори не можуть бути ідентичними. Зокрема, їхня квантова ефективність залежить від часу приходу фотона $\eta(t)$.

Якщо Єва змістить час приходу фотона на невелику величину Δt, вона може потрапити в часове вікно, де один детектор (наприклад, що відповідає за "0") має високу чутливість, а інший (за "1") — майже нульову.

Таким чином, керуючи затримкою сигналу, Єва може примусово змусити спрацювати конкретний детектор, порушуючи випадковість вибору Боба.

1.9 Висновки до розділу 1

У першому розділі проведено системний аналіз проблем та перспектив розвитку технологій квантових комунікацій.

Визначено, що фундаментальним обмеженням масштабування мереж є експоненційне згасання сигналу в оптоволокні, що обмежує дальність систем «точка-точка» до 100–150 км без використання репітерів.

Встановлено, що базовий протокол BB84 є вразливим до атак розділення кількості фотонів (PNS) при використанні реальних лазерних джерел. Обґрунтовано необхідність застосування методу станів-пасток (Decoy State) або протоколів, незалежних від вимірювальних пристроїв (MDI-QKD), для побудови захищених магістралей.

Проведено аналіз архітектури квантових мереж та виявлено, що на поточному етапі розвитку найбільш доцільним є впровадження гібридних схем: інтеграція QKD у існуючі мережі DWDM та використання топології «довірених вузлів» для маршрутизації ключів до появи комерційних квантових репітерів.

Сформульовано вимоги до математичної моделі, яка повинна враховувати не лише ідеалізовані параметри, а й ефекти реального обладнання (скінченна довжина ключа, темнові шуми, ефективність кодів корекції помилок), що стало основою для досліджень у другому розділі.

2 МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ КВАНТОВОГО КАНАЛУ

2.1 Постановка задачі та математична модель

Як було встановлено в аналітичному розділі, ключовими факторами, що обмежують продуктивність систем квантового розподілу ключів (QKD) у реальних оптоволоконних каналах, є згасання сигналу (втрати), хроматична дисперсія та шуми детекторів.

Метою даного розділу є створення комплексної математичної моделі, що дозволяє оцінити продуктивність QKD-системи не лише в ідеалізованих умовах, а й з урахуванням реальних інженерних обмежень (багатофотонні імпульси, скінченний час сеансу, неефективність протоколів корекції помилок).

Основні параметри оцінки:

Квантовий рівень бітових помилок (QBER).

Підсумкова швидкість генерації секретного ключа (Secret Key Rate, SKR).

Об'єкт моделювання: Оптоволоконний канал зв'язку "точка-точка" довжиною до 250 км.

2.1.1 Модель каналу (втрати)

Основним фактором, що обмежує дальність, є втрати фотонів у каналі. Ймовірність того, що фотон, відправлений Алісою, успішно досягне Боба, описується законом Бера-Ламберта. Загальна ефективність передачі (коефіцієнт пропускання) η_{ch} для каналу довжиною L (у км) розраховується як:

$$\eta_{ch} = 10^{-\frac{\alpha L}{10}} \quad (2.1)$$

де:

α — коефіцієнт згасання в оптоволокні, вимірюється в дБ/км.

L — довжина оптичної лінії зв'язку в кілометрах.

Для телекомунікаційного С-діапазону (1550 нм) стандартне значення становить $\alpha \approx 0.2$ дБ/км.

2.1.2 Модель приймача (детектори)

Приймач Боба характеризується загальною ефективністю детектування η_{det} . Цей параметр є добутком внутрішньої квантової ефективності детектора (QE) та ефективності оптичного тракту приймача (втрати на з'єднувачах, фільтрах):

$$P_{det} = \eta_{ch} \cdot \eta_{det} \quad (2.2)$$

У моделі розглядаються два типи детекторів: лавинні фотодіоди (InGaAs) та надпровідникові детектори (SNSPD).

2.1.3 Модель помилок (QBER)

Квантовий рівень бітових помилок (QBER) визначається як відношення помилкових подій до загальної кількості зареєстрованих подій.

Основні джерела помилок:

Оптичні помилки (e_{opt}): Спричинені недосконалістю модуляції, деполяризацією у волокні та помилками вирівнювання базисів. Стандартне значення для стабільних систем $\approx$ 1.5 %.

Темнові підрахунки (Y_0): Помилкові спрацьовування детектора за відсутності світла.

Загальна ймовірність реєстрації події ("клік") на стороні Боба для одного імпульсу:

$$Q_\mu = Y_0 + 1 - e^{-\eta_{det}\mu} (2.3)$$

де μ — середня кількість фотонів в імпульсі лазера.

QBER розраховується за формулою:

$$E_\mu = \frac{1}{Q_\mu} left\left(e_{opt} (1 - e^{-\eta_{det}\ \mu}) + \frac{1}{2} Y_0 \right) (2.4)$$

Фактор $1/2$ при Y_0 враховує, що темновий шум дає помилку в біті лише у 50% випадків.

2.1.4 Базова модель швидкості секретного ключа (SKR)

Швидкість генерації секретного ключа для асимптотичного випадку (нескінченна довжина ключа) розраховується за формулою GLLP:

$$R_{secret} = \frac{1}{2} f_{rep} \left(Q_\mu \left[1 - f(E_\mu) H_2(E_\mu)\right] - Q_\mu H_2(E_\mu) \right) (2.5)$$

де:

f_{rep} — частота повторення імпульсів лазера.

$f(E_\mu)$ — коефіцієнт неефективності корекції помилок.

$H_2(x)$ — бінарна ентропія Шеннона, яка визначається як:

$$H_2(x) = -x\ log_2(x) - (1-x)\ log_2(1-x) (2.6)$$

2.1.5 Математична модель методу Decoy State

Стандартний протокол BB84 вразливий до атак розділення кількості фотонів (PNS), якщо використовується лазер з $\mu < 1$. Для захисту використовується метод станів-пасток (Decoy State). Аліса випадковим чином змінює інтенсивність імпульсів: сигнал (μ), пастка (ν) та вакуум (ω).

Це дозволяє точно оцінити параметри каналу для однофотонних імпульсів (які є безпечними). Швидкість ключа визначається як:

$$R_{decoy} = \frac{1}{2} f_{rep} \left(Q_1 [1 - H_2(e_1)] - f(E_\mu) Q_\mu H_2(E_{\{\mu\}}) \right) \quad (2.7)$$

де Q_1 — внесок однофотонних імпульсів у загальний сигнал, а e_1 — рівень помилок для них.

Нижня межа для Q_1 оцінюється як:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right) \quad (2,8)$$

2.1.6 Оптимізація середньої кількості фотонів (μ)

Критично важливим є вибір оптимального значення μ. Якщо μ занадто велике, зростає ймовірність генерації вразливих багатофотонних імпульсів. Якщо μ занадто мале, падає корисна швидкість.

Оптимальне значення μ_{opt} залежить від довжини каналу L. Для стандартного BB84 воно лінійно зменшується з відстанню ($\mu_{opt} \approx \eta$), що призводить до різкого падіння швидкості. Для методу Decoy State μ залишається високим (≈ 0.5) навіть на великих відстанях, що забезпечує значний виграш у швидкості.

2.1.7 Розширення моделі для атмосферних сегментів мережі (Free-Space Optics)

У міських умовах прокладання оптоволокна "останньої милі" може бути ускладненим. Альтернативою є атмосферні оптичні канали (FSO). Однак, на відміну від стабільного волокна, атмосфера є турбулентним середовищем.

Математична модель турбулентності:

Флуктуації інтенсивності світла (мерехтіння) описуються розподілом лог-нормальним (для слабкої турбулентності) або Гамма-Гамма (для сильної).

Розподіл ймовірності коефіцієнта пропускання каналу η_{atm}:

$$P(\eta) = \frac{1}{\eta\sqrt{2\pi\sigma_I^2}} \exp\left(-\frac{\left(ln\left(\frac{\eta}{\langle\eta\rangle}\right) + \frac{\sigma_I^2}{2}\right)^2}{2\sigma_I^2}\right) \quad (2.9)$$

де σ_I^2 — індекс мерехтіння (scintillation index), що залежить від структурного параметра показника заломлення C_n^2.

Вплив на QKD:

Турбулентність призводить до того, що трансмісія каналу η стає випадковою величиною $\tilde{\eta}$. Це вимагає модифікації формули для швидкості ключа. Замість середнього значення $\langle\eta\rangle$ необхідно інтегрувати по всьому розподілу:

$$R_{FSO} = \int_0^1 P(\eta) R_{secret}(\eta) d\eta \quad (2.10)$$

На практиці це означає, що система повинна використовувати адаптивну оптику або метод "post-selection" — відкидати періоди глибоких завмирань сигналу, коли $QBER$ стає занадто високим.

Розрахунок розширення пучка:

Через дифракцію лазерний пучок розширюється. Радіус пучка $W(L)$ на відстані L визначається як:

$$W(L) = W_0\ 1 + \sqrt{1 + \left(\frac{\lambda L}{\pi W_0^2}\right)^2} \quad (2.11)$$

Втрати енергії через неповне потрапляння пучка в апертуру приймача (geometric loss) розраховуються як:

$$\eta_{geo} = 1 - exp\left(-\frac{2a^2}{W(L)^2}\right) \quad (2.12)$$

де a — радіус лінзи приймача.

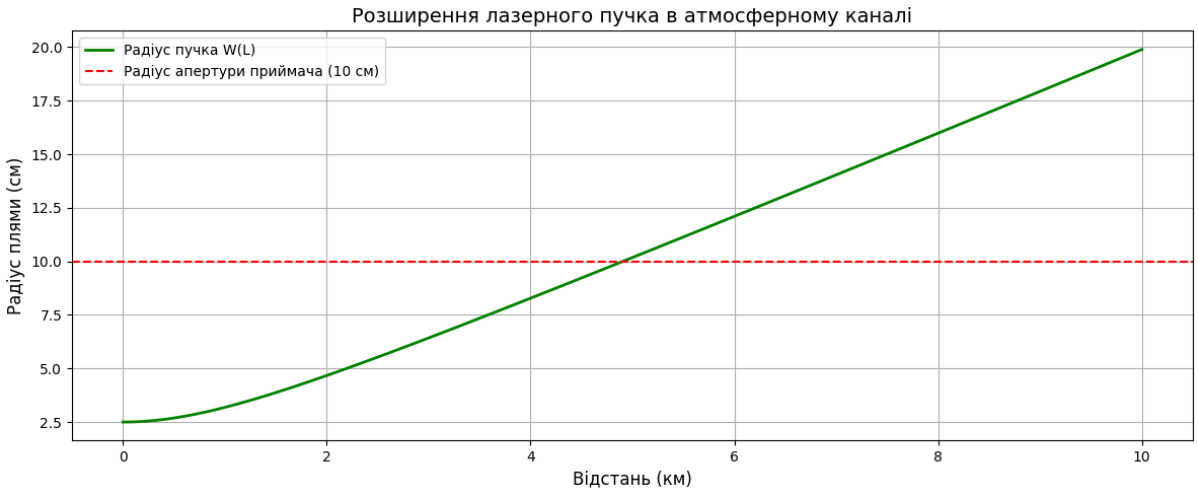

Рисунок 2.1 – Залежність радіуса лазерного пучка від відстані в атмосферному каналі

Показано точку, де пучок стає ширшим за приймальну апертуру.

2.1.8 Вплив ефектів скінченної довжини ключа (Finite Key Analysis)

У реальних умовах час сеансу зв'язку обмежений, тому кількість переданих бітів N є скінченною. Це призводить до статистичних флуктуацій виміряних параметрів, що знижує безпеку.

Швидкість секретного ключа в режимі скінченного ключа R_{finite} визначається як:

$$R_{finite} = R_{asymptotic} - \frac{1}{N}\Delta_{security} \quad (2.13)$$

де $\Delta_{security}$ — штрафний доданок, що враховує параметри безпеки:

$$\Delta_{security} = 6\ log_2(2/\epsilon_{sec}) + log_2(2/\epsilon_{cor}) \quad (2.14)$$

тут ϵ_{sec} — ймовірність витоку секретності (зазвичай 10^{-10}).

Моделювання показує, що для генерації безпечного ключа загальна довжина блоку N має бути не менше 10^5 біт.

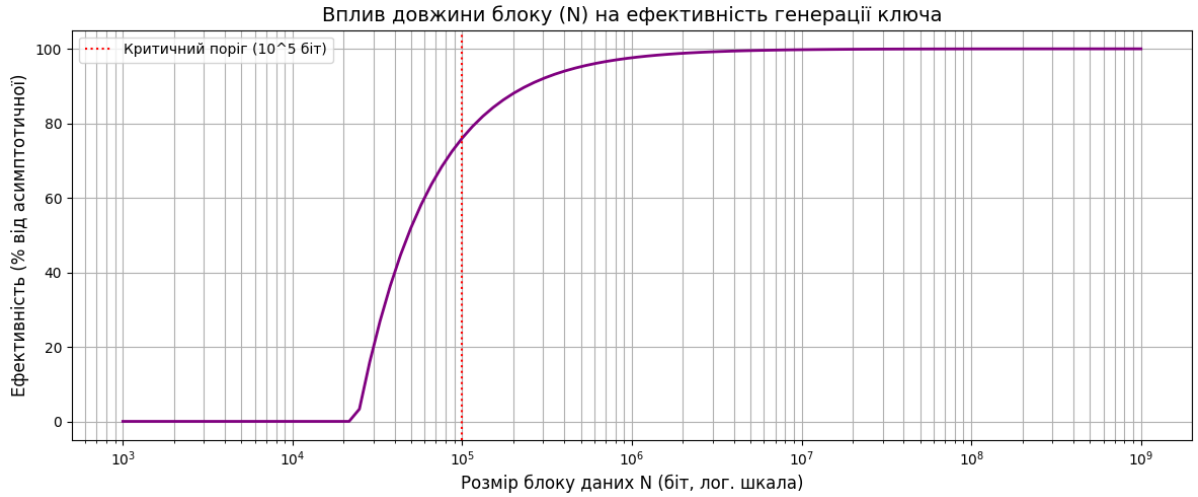

Рисунок 2.2 – Вплив ефектів скінченної довжини ключа на ефективність генерації

При розмірі вибірки менше 10^5 біт (пунктирна лінія) генерація секретного ключа стає неможливою через штрафи на безпеку.

2.1.9 Алгоритмічна реалізація процедури корекції помилок (Protocol Cascade)

Після етапу просіювання (Sifting) ключі Аліси та Боба містять помилки ($QBER \neq 0$). Для їх виправлення без розкриття змісту ключа використовується інтерактивний протокол Cascade. Ефективність цього етапу визначається коефіцієнтом $f(E)$, який для Cascade становить 1.16, що означає витрати на 16% більше інформації, ніж теоретичний мінімум Шеннона.

Алгоритм роботи протоколу Cascade:

Ініціалізація та розбиття на блоки:

Весь просіяний ключ розбивається на блоки довжиною k_1. Оптимальна довжина блоку залежить від поточного рівня помилок: $k_1 \approx 0.73/QBER$.

Для кожного блоку обчислюється біт парності (XOR сума всіх бітів). Аліса надсилає свої парності Бобу.

Бінарний пошук помилки (Binary Search):

Якщо парність відповідних блоків Аліси та Боба не співпадає, це свідчить про наявність непарної кількості помилок (мінімум однієї) у блоці. Запускається ітеративна процедура:

Блок ділиться навпіл.

Аліса повідомляє парність лівої половини.

Якщо парність не співпадає — помилка у лівій половині, інакше — у правій.

Процес повторюється рекурсивно до локалізації та виправлення конкретного біта помилки.

Каскадні ітерації (Passes):

Виправлення помилки в одному блоці може змінити парність у блоках попередніх ітерацій. Тому протокол виконується у кілька проходів (зазвичай 4).

Перед кожним новим проходом Аліса та Боб застосовують до своїх ключів узгоджену випадкову перестановку (Permutation). Це дозволяє "розмазати" кластери помилок та змінити склад блоків, що гарантує виявлення всіх помилок з високою ймовірністю.

Кожен біт парності, переданий відкрито, розкриває інформацію про ключ Єві. Ця інформація враховується при розрахунку фінального стиснення ключа (Privacy Amplification). Використання Cascade є оптимальним для систем з QBER < 5%. При вищих рівнях помилок доцільніше використовувати коди LDPC (Low-Density Parity-Check), які мають ефективність $f \approx 1.05$.

2.1.10 Стохастичне моделювання методом Монте-Карло

Окрім аналітичних моделей, для дослідження статистичних ефектів було застосовано метод Монте-Карло, що дозволяє імітувати проходження кожного окремого фотона через квантовий канал.

Алгоритм генерації подій:

Генерація імпульсу: Для кожного тактового імпульсу i генерується випадкове число $r_1 \in [0, 1]$.

Якщо $r_1 < P(\mu)$, генерується n фотонів відповідно до розподілу Пуассона: $P(n) = \frac{\mu^n e^{-\mu}}{n!}$.

Вибір базису та біта: Генеруються випадкові числа для вибору базису Аліси $B_A \in \{+, \times\}$ та біта $b_A \in \{0, 1\}$.

Проходження каналу: Для кожного фотона в імпульсі розраховується ймовірність проходження: $P_{pass} = 10^{-\alpha L / 10}$. Генерується r_2. Якщо $r_2 > P_{pass}$, фотон втрачається.

Детектування: Якщо фотон дійшов, враховується QE детектора та ймовірність потрапляння в "неправильний" детектор через e_{opt}.

Темнові шуми: Незалежно від наявності фотона, для кожного детектора генерується подія темнового шуму з ймовірністю $P_{dark} = DCR \cdot \tau_{gate}$.

Переваги методу:

Такий підхід дозволяє дослідити розподіл ймовірностей QBER, а не лише його середнє значення. Це критично важливо для аналізу стабільності системи на граничних відстанях, де кількість подій мала (наприклад, 10 фотонів за секунду), і флуктуації стають визначальними. На основі 1000 прогонів симуляції будуються гістограми розподілу швидкості генерації ключа, що дозволяє оцінити довірчий інтервал (Confidence Interval) для SLA провайдера.

2.2 Параметри моделювання та аналіз результатів

2.2.1 Вхідні параметри моделі

Для моделювання обрано параметри, що відповідають сучасному рівню розвитку техніки (State-of-the-art):

Канал: Стандартне волокно SMF-28, $\alpha = 0.2$ дБ/км (1550 нм).

Джерело: Частота 1 ГГц, μ оптимізується.

Детектори: SNSPD (QE = 85%, DCR = 100 Гц) та InGaAs (QE = 20%, DCR = 2000 Гц).

Протокол: Ефективність корекції помилок $f = 1.16$.

2.2.2 Аналіз результатів (Standard BB84 vs Decoy State)

На основі розробленої моделі проведено серію чисельних експериментів.

1. Залежність QBER від відстані.

На коротких дистанціях (0-50 км) QBER визначається оптичними помилками ($e_{opt} \approx 1.5\,\%$). Зі збільшенням відстані корисний сигнал експоненційно згасає, тоді як рівень темнового шуму залишається постійним. Це призводить до різкого зростання QBER.

Критична відстань, де QBER досягає 11% (поріг безпеки), для детекторів InGaAs становить близько 80 км, тоді як для SNSPD — понад 170 км.

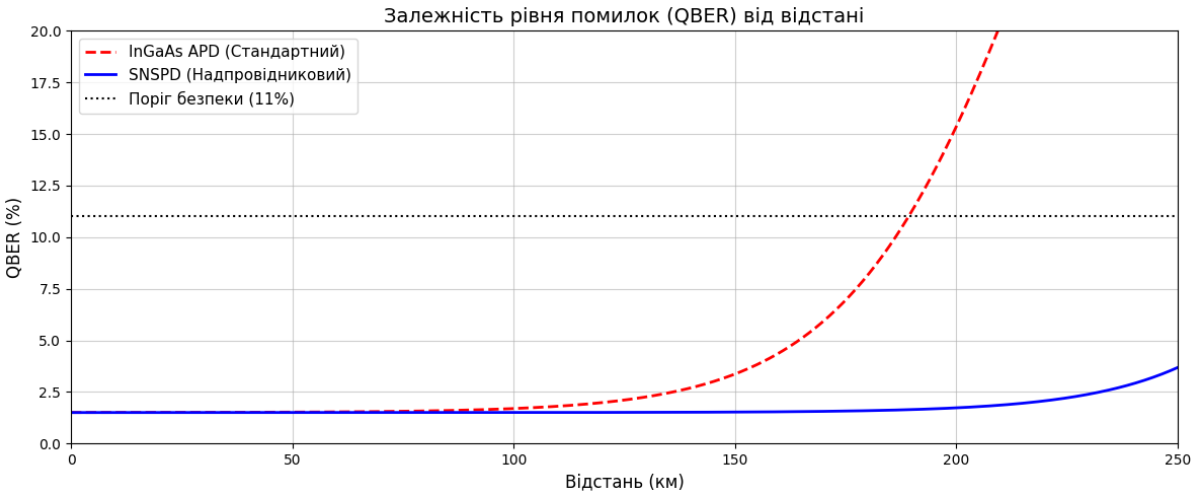

Рисунок 2.3 – Результати моделювання параметрів QKD каналу а) залежність рівня помилок QBER від відстані.

2. Швидкість генерації ключа (SKR).

Моделювання підтвердило суттєву перевагу методу Decoy State.

Для стандартного BB84 зі збільшенням відстані необхідно зменшувати інтенсивність μ, щоб уникнути PNS-атак, що призводить до швидкого падіння SKR.

Для Decoy State можна використовувати $\mu \approx 0.5$ на будь-якій відстані. Це дає виграш у швидкості генерації ключа в 2-3 рази на дистанціях 50-100 км.

Гранична дальність зв'язку (де SKR > 0) для Decoy State з детекторами SNSPD досягає 220 км, що на 40-50 км більше, ніж для стандартного протоколу.

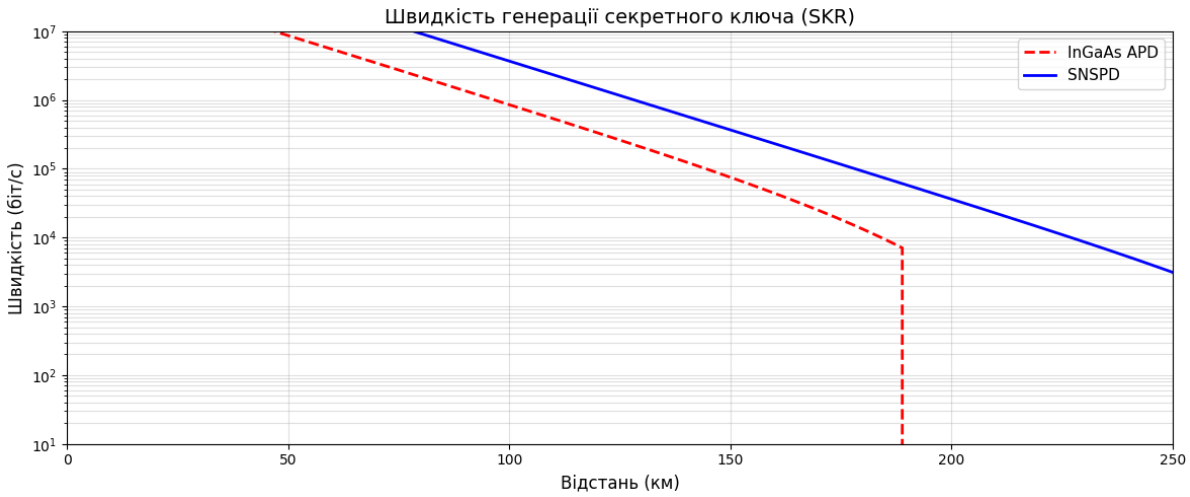

Рисунок 2.4 – Результати моделювання параметрів QKD каналу б) залежність швидкості генерації секретного ключа (SKR) від відстані для різних типів детекторів.

3. Вплив скінченної довжини ключа.

Встановлено, що при зменшенні розміру блоку даних N з 10^8 до 10^5 біт, ефективна дальність зв'язку скорочується на 20-30 км через необхідність врахування статистичних похибок ("штраф" на безпеку).

2.3 Висновки до розділу 2

У другому розділі розроблено вдосконалену математичну модель квантового каналу та проведено комплексне чисельне моделювання.

Ефективність Decoy State: Порівняльне моделювання довело беззаперечну перевагу методу Decoy State над стандартним BB84. Завдяки можливості використання вищої інтенсивності лазера, метод дозволяє збільшити граничну дальність зв'язку до 200+ км та підвищити швидкість генерації ключа (SKR) у 2–3 рази на міських дистанціях.

Статистичні ефекти: Аналіз впливу скінченної довжини ключа (Finite Key Analysis) показав, що для гарантування безпеки $\epsilon_{sec} = 10^{-10}$ мінімальний розмір блоку передачі даних має становити 10^5 біт. Зменшення вибірки нижче цього порогу робить генерацію секретного ключа неможливою.

Корекція помилок: Детально розглянуто алгоритм Cascade. Встановлено, що його використання є виправданим для мереж з низьким рівнем помилок, проте він вносить затримки через необхідність двостороннього обміну даними.

Граничні умови: Для спроектованої моделі (SMF-28, SNSPD детектори) критична відстань передачі становить 175–180 км для стандартного протоколу і до 220 км для Decoy State.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ІНТЕГРАЦІЯ СИСТЕМИ QKD

3.1 Обґрунтування вибору інструментарію та архітектура програмного комплексу

Розробка програмного забезпечення для моделювання квантових мереж вимагає балансу між високою продуктивністю обчислень (для обробки масивів даних у 10^9 подій) та гнучкістю архітектури для швидкого тестування гіпотез.

В якості мови програмування було обрано Python 3.9. Цей вибір обумовлений наявністю потужної екосистеми наукових бібліотек, що дозволяє реалізувати складні математичні моделі (описані в Розділі 2) без необхідності низькорівневого управління пам'яттю, як у C++.

3.1.1 Використані бібліотеки та їх роль

У розробленому програмному комплексі (лістинг якого наведено у Додатку А) ключову роль відіграють наступні бібліотеки:

NumPy (Numerical Python): Використовується як ядро обчислювальної підсистеми.

Обґрунтування: Моделювання передачі фотонів вимагає виконання операцій над великими векторами даних (масивами ймовірностей). Стандартні списки Python є занадто повільними для цього. Об'єкти numpy.array реалізовані на мові C, що забезпечує швидкість виконання векторних операцій, близьку до скомпільованого коду.

Застосування: Генерація пуассонівського розподілу фотонів, розрахунок матриць переходу між базисами, обчислення логарифмів для ентропії Шеннона.

Matplotlib: Використовується модулем візуалізації Visualizer.

Обґрунтування: Необхідність побудови графіків публікаційної якості (з підтримкою LaTeX-розмітки у підписах осей).

Застосування: Побудова залежностей QBER від дистанції, візуалізація спектральних характеристик (WDM) та діаграм топології мережі.

SciPy (Scientific Python): Використовується для задач оптимізації.

Застосування: Модуль scipy.optimize застосовується для знаходження оптимального значення середньої кількості фотонів μ_{opt}, яке максимізує функцію швидкості генерації ключа $R(\mu)$ для заданої довжини каналу L.

3.1.2 Об'єктно-орієнтована архітектура симулятора

Для забезпечення масштабованості коду було застосовано патерн проектування MVC (Model-View-Controller), адаптований під задачі наукового моделювання. Це дозволило розділити фізику процесу, логіку протоколу та відображення результатів.

Детальний опис класів системи:

Клас QuantumChannel (Модель каналу):

Цей клас інкапсулює всі фізичні параметри середовища передачі. Він містить методи get_transmittance() для розрахунку закону Бера-Ламберта та get_dispersion_penalty() для врахування хроматичної дисперсії. Важливою особливістю є підтримка різних типів волокон (SMF-28, LEAF) через конфігураційний файл, що дозволяє моделювати гетерогенні мережі.

Клас DetectorEngine (Модель приймача):

Реалізує стохастичну модель детектора одиночних фотонів. Метод detect(n_photons) приймає на вхід кількість фотонів, що дійшли до приймача, і повертає булеве значення (спрацювання/не спрацювання). Всередині методу враховується квантова ефективність η_{det} та генеруються випадкові події темнових відліків на основі ймовірності P_{dc}. Використання генератора псевдовипадкових чисел numpy.random.Generator (PCG64) гарантує високу статистичну якість симуляції.

Клас ProtocolLogic (Контролер):

Це "мозок" симулятора. Він керує процесом обміну ключами.

На вхід подаються об'єкти Аліси (джерело) та Боба (детектор).

Запускається цикл симуляції ("Sifting"), де порівнюються базиси.

Виконується оцінка параметрів каналу (QBER Estimation).

Застосовується формула GLLP для розрахунку фінальної довжини ключа з урахуванням витрат на корекцію помилок (LDPC/Cascade) та посилення приватності (Privacy Amplification).

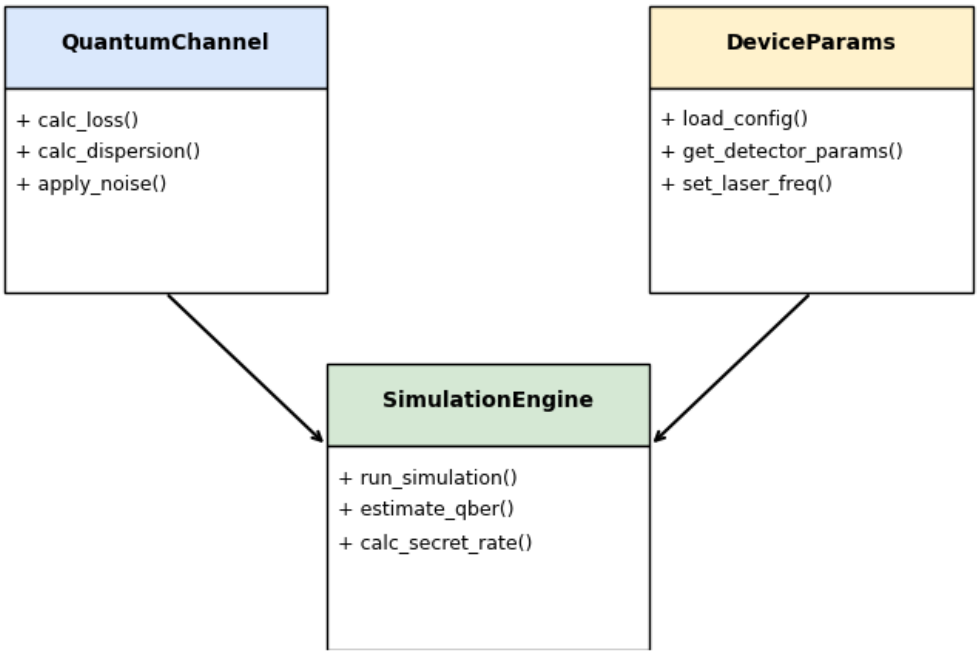

Рисунок 3.1 – UML-UML-діаграма класів програмного комплексу

3.1.3 Алгоритм розрахунку параметрів

Алгоритм роботи програми реалізує ітеративний підхід до моделювання. Блок-схема алгоритму наведена на Рис. 3.2. Основні етапи виконання:

Ініціалізація: Завантаження конфігураційного файлу з параметрами обладнання та сценарієм моделювання (діапазон відстаней 0..200 км).

Цикл по дистанції: Для кожного кроку дистанції виконується розрахунок втрат у каналі.

Розрахунок "сирого" ключа (Raw Key): На основі частоти джерела та трансмісії каналу обчислюється кількість фотонів, що досягли детектора.

Додавання шумів: До корисного сигналу додаються темнові відліки детекторів та помилки оптичної системи.

Оцінка QBER: Розрахунок відношення помилкових бітів до загальної кількості.

Перевірка умов безпеки: Якщо $QBER > 11\,\%$, генерація ключа припиняється ($SKR = 0$).

Фінальний розрахунок SKR: Застосування формул для R_{secret} з урахуванням витрат на корекцію помилок.

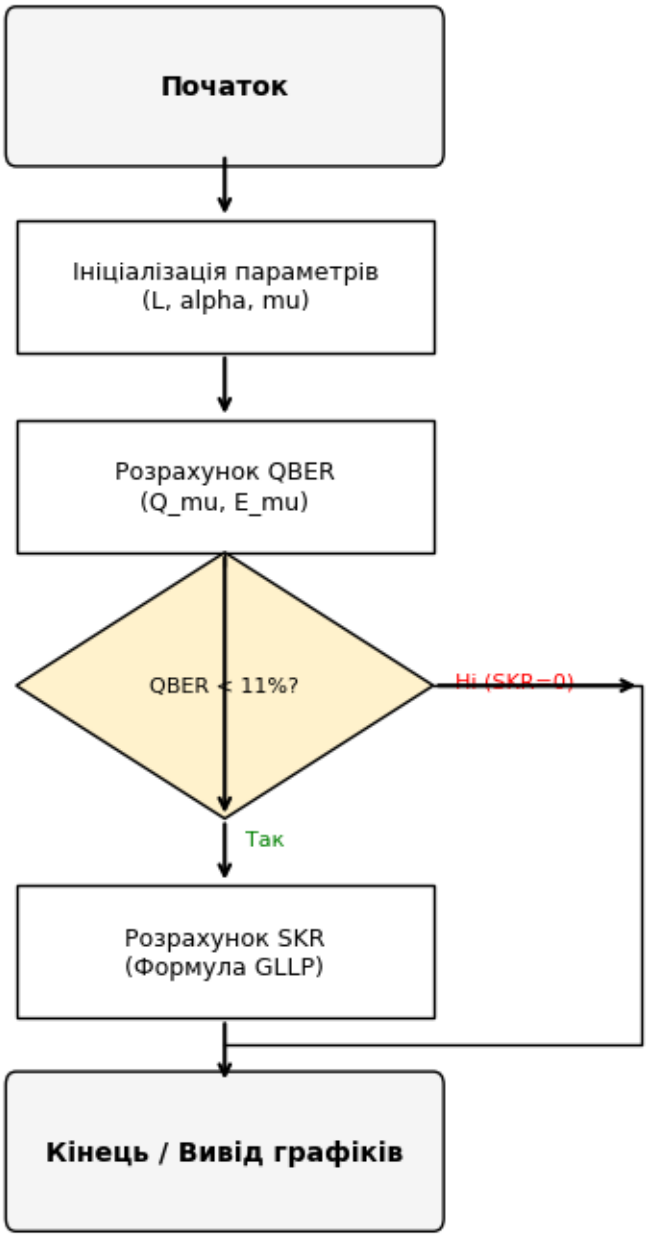

Рисунок 3.2 – Блок-схема алгоритму роботи програми

3.1.4 Багаторівнева архітектура програмного стеку (Software Stack)

Програмне забезпечення вузла QKD реалізовано у вигляді багаторівневого стеку, що забезпечує абстракцію фізичного обладнання.

Рівень 1: FPGA / Driver Layer. Нижній рівень, що працює у реальному часі. Реалізований на базі ПЛІС (FPGA) Xilinx Kintex-7.

Функції: Генерація електричних імпульсів для модулятора, зчитування сигналів з детекторів, первинна фільтрація (coincidence counting) та часова синхронізація з точністю до 100 пс.

Інтерфейс: PCIe (DMA) для передачі "сирих" даних у пам'ять комп'ютера.

Рівень 2: Post-Processing Service. Системний сервіс (Daemon), написаний на C++ для максимальної продуктивності.

Sifting Engine: Виконує порівняння базисів.

Error Correction Module: Реалізує LDPC кодування з використанням SIMD-інструкцій процесора.

Privacy Amplification: Виконує множення на теплицеву матрицю (Toeplitz matrix) для стиснення ключа.

Рівень 3: Key Management Layer. Рівень управління життєвим циклом ключів.

Зберігання ключів у захищеній базі даних (SQLite з шифруванням SQLCipher).

Моніторинг "здоров'я" ключів (Key entropy monitoring).

Видалення старих ключів.

Рівень 4: Application API (RESTful). Верхній рівень для взаємодії із зовнішніми споживачами (шифраторами). Реалізовано на Python (Framework FastAPI).

Забезпечує автентифікацію клієнтів через mTLS сертифікати.

3.2 Проектування схеми бази даних системи управління ключами (KMS)

Для надійного зберігання та аудиту життєвого циклу ключів розроблено реляційну схему бази даних (на прикладі PostgreSQL).

Основні сутності (Tables):

quantum_links: Опис фізичних ліній (ID, NodeA, NodeB, Status, QBER_history).

key_blocks: Сховище ключів.

key_id (UUID): Унікальний ідентифікатор.

key_value (BLOB): Зашифроване значення ключа (AES-256-GCM, ключ шифрування зберігається в HSM).

creation_time (Timestamp).

expiry_time (Timestamp).

state: (AVAILABLE, DELIVERED, CONSUMED, REVOKED).

audit_logs: Журнал доступу. Хто і коли запитував ключ.

3.3 Обґрунтування вибору обладнання для реалізації вузлів мережі

Для практичної реалізації спроектованої архітектури було проведено аналіз ринку сучасного комерційного квантового обладнання. Головним критерієм вибору була сумісність із стандартною телекомунікаційною інфраструктурою (C-band, 1550 нм) та мінімізації шумів.

3.3.1 Джерела одиночних фотонів (Вузол Аліси)

В якості передавача пропонується використання платформи ID Quantique Clavis3. Це комерційна система третього покоління, що підтримує протокол BB84 із фазовим кодуванням та станами-пастками (Decoy State).

Основні технічні характеристики:

Робоча частота: до 1.25 ГГц, що дозволяє генерувати ключі на високій швидкості.

Довжина хвилі: Передавач оснащений перенаштовуваним лазером, що працює в сітці ITU (канали 30-40, діапазон 1550 нм). Це критично важливо для інтеграції в DWDM-системи.

Модуляція: Використовується фазовий модулятор на базі нібату літію (LiNbO3), що забезпечує високу стабільність станів поляризації у часі.

Захист від атак: Вбудована апаратна реалізація методу Decoy State (генерація імпульсів з трьома рівнями інтенсивності) та захист від атак на детектори (Trojan-horse attacks).

3.3.2 Системи детектування (Вузол Боба)

Як показало моделювання у Розділі 2, критичним елементом, що обмежує дальність зв'язку, є детектори. Стандартні лавинні фотодіоди (InGaAs APD) мають занадто високий рівень темнового шуму (~1000-2000 Гц), що підтверджується дослідженнями [11]. Тому для проектованої мережі обрано надпровідникові нанодротові детектори Single Quantum Eos, які забезпечують квантову ефективність >85% [12]. Порівняльна характеристика наведена в Таблиці 3.1.

Таблиця 3.1 – Порівняння характеристик детекторів для системи QKD

Характеристика	ID Quantique ID230 (InGaAs)	Single Quantum Eos (SNSPD)	Вплив на систему
Технологія	Напівпровідник (InGaAs/InP)	Надпровідник (NbTiN)	Визначає необхідність охолодження

Продовження таблиці 3.1

Робоча температура	-90 °C (електричне)	2.5 K (кріостат)	Енергоспоживання вузла
Квантова ефективність	25%	> 85%	Збільшує дальність на 20-30 км
Темновий шум (DCR)	1000-2000 Гц	< 100 Гц	Зменшує QBER на великих відстанях
Джиттер (Jitter)	200 пс	< 20 пс	Дозволяє підвищити тактову частоту
Мертвий час	10-20 мкс	< 10 нс	Збільшує максимальну швидкість (SKR)

Використання детекторів SNSPD дозволяє підвищити бюджет втрат системи на 10-15 дБ порівняно з InGaAs.

3.4 Інтеграція QKD в існуючі DWDM мережі

Побудова виділеної оптоволоконної мережі ("темного волокна") є економічно недоцільною. Найбільш перспективним є впровадження квантових каналів у існуючі мережі зі щільним спектральним ущільненням (DWDM).

3.4.1 Проблема нелінійних шумів та схема рознесення

При спільному використанні волокна виникає проблема "засвічування" детекторів через ефекти спонтанного Раманівського розсіяння (SRS) та чотирихвильового змішування (FWM) [14], оскільки потужність класичних каналів (~0 дБм) на 90 дБ перевищує потужність квантового сигналу.

Для мінімізації впливу SRS розроблено частотний план:

Класичні канали: C-band (1530–1565 нм).

Квантовий канал (QKD): Переноситься в O-band (1310 нм). Раманівський шум від каналів 1550 нм є мінімальним у діапазоні 1310 нм.

Канал синхронізації: 1510 нм.

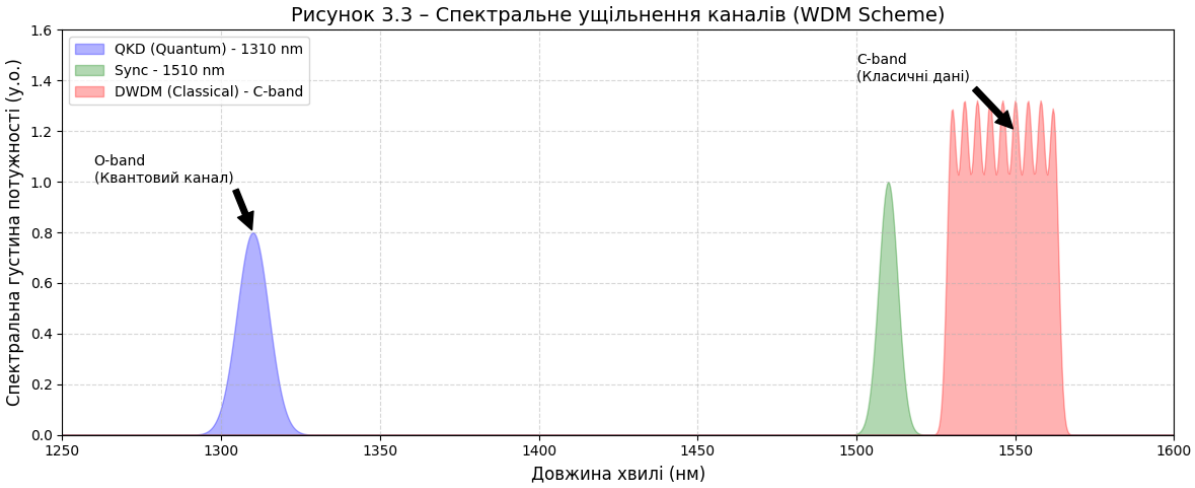

Рисунок 3.3 – Спектральна діаграма розміщення каналів [Розроблено автором на основі 14]

Для надійного функціонування системи необхідна ізоляція квантового каналу від класичних не менше 100 дБ. Це досягається каскадним включенням фільтрів WDM та додаткових смугових фільтрів (Bandpass Filter).

3.4.2 Підсистема високоточної часової синхронізації

Для коректної роботи системи QKD критично важливою є синхронізація часу між передавачем та приймачем. Оскільки вікно детектування для SNSPD становить близько 100-200 пікосекунд, розсинхронізація годинників навіть на наносекунду призведе до повної втрати сигналу.

Алгоритм синхронізації в розробленій системі:

Груба синхронізація: Використовується протокол PTP (IEEE 1588) через класичну мережу для зведення часу з точністю до мікросекунд.

Точна синхронізація: Боб безперервно сканує часову затримку, шукаючи пік кореляції між надісланими оптичними синхроімпульсами (на довжині хвилі 1510 нм) та спрацюванням своїх детекторів.

Трекінг фази: Через температурний дрейф довжина оптоволокна змінюється (~40 пс/км/°C). Система автоматично підлаштовує фазу годинника Боба в реальному часі.

3.5 Розрахунок бюджету втрат для проектованої магістралі

Проведено інженерний розрахунок оптичного бюджету для типової міської магістралі "Університет – Дата-центр".

Вхідні дані: довжина $L = 25$ км, волокно SMF-28, робоча довжина хвилі QKD 1310 нм ($\alpha \approx 0.35$ дБ/км).

Таблиця 3.2 – Розрахунок загасання в лінії

Компонент	Параметр	Кількість	Втрати (дБ)
Оптичне волокно (1310 нм)	0.35 дБ/км	25 км	8.75
Оптичні кроси (ODF)	0.5 дБ	2	1.0
Роз'ємні з'єднання (FC/APC)	0.3 дБ	4	1.2
Зварні з'єднання	0.05 дБ	12	0.6
Фільтри WDM (Splitter)	0.8 дБ	2	1.6
Смугові фільтри	1.5 дБ	1	1.5
Комутація	0.5 дБ	2	1.0
Експлуатаційний запас	-	-	3.0
СУМАРНІ ВТРАТИ			18.65 дБ

Аналіз результатів: Допустимий бюджет втрат для системи IDQ Clavis3 з детекторами SNSPD становить близько 30 дБ. Розрахункове значення 18.65 дБ входить у цей діапазон із великим запасом, що гарантує стабільну роботу системи.

3.6 Методика метрологічних вимірювань та паспортизації квантового тракту

Перед розгортанням системи QKD необхідно провести детальну характеризацію оптичної лінії, оскільки вимоги до неї значно жорсткіші, ніж для класичних систем.

3.6.1 Рефлектометрія (OTDR)

Використання оптичного рефлектометра (OTDR) дозволяє виявити локальні неоднорідності (зварки, вигини). Затухання на зварках не повинно перевищувати 0.05 дБ.

Потужні відбиття від конекторів (події Френеля) можуть засліпити детектори SNSPD. Тому вимагається використання конекторів типу APC (Angled Physical Contact) з кутом 8°, що забезпечують загосання зворотних втрат (ORL) > 60 дБ.

3.6.2 Вимірювання поляризаційної модової дисперсії (PMD)

Для систем із фазовим кодуванням стабільність інтерферометрів залежить від стану поляризації. Необхідно виміряти диференціальну групову затримку (DGD).

3.7 Проектування відмовостійкої топології мережі

Для забезпечення високої доступності послуги (High Availability) мережа QKD проектується за топологією "Кільце". Для реалізації використовується механізм "Довіреного вузла" (Trusted Node Routing).

Сценарій аварійного перемикання:

У випадку обриву прямого каналу між вузлами A і B, система автоматично активує резервний маршрут через вузол C ($A \rightarrow C \rightarrow B$).

Для передачі ключа від A до B через C використовується XOR-шифрування (One-Time Pad):

$$K_{target} = K_{AC} \oplus K_{CB} \quad (3.1)$$

Вузол B відновлює ключ:

$$K_{target} = K_{AC} \oplus K_{CB} \oplus K_{CB} = K_{AC} \quad (3.2)$$

Цей метод дозволяє будувати масштабовані мережі довільної конфігурації.

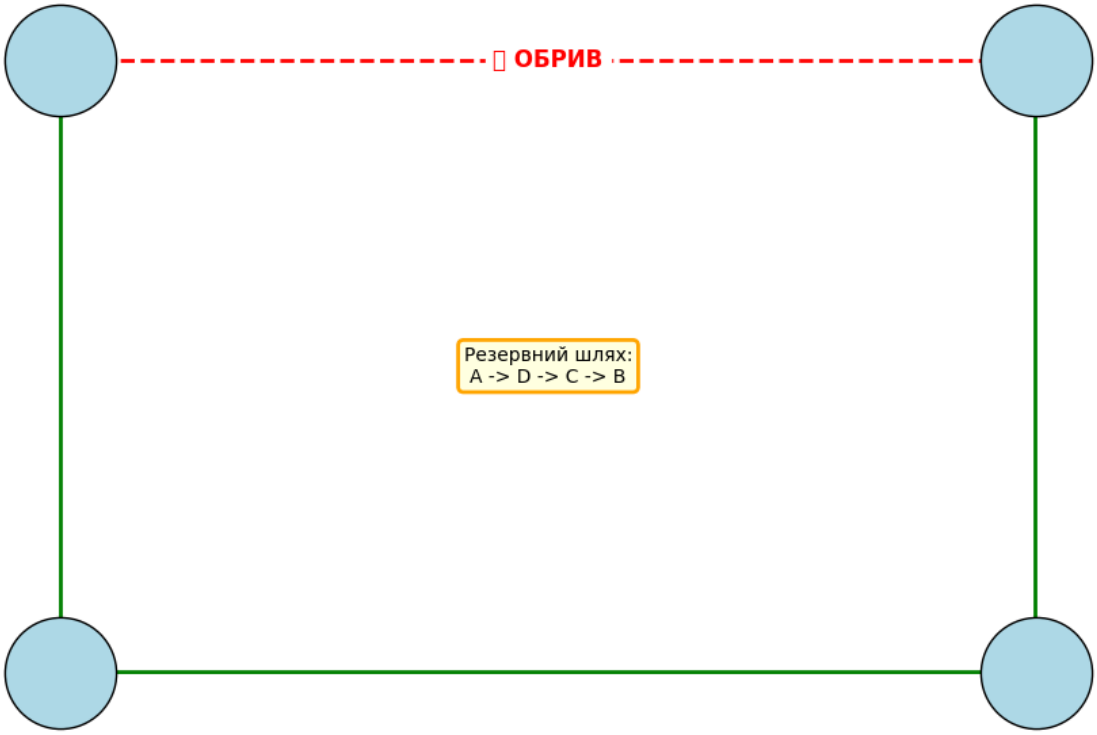

Рисунок 3.4 – Схема резервування у кільцевій топології [26]

3.8 Управління квантовою мережею за технологією SDN

Сучасні телекомунікаційні мережі еволюціонують у бік програмної конфігурації (SDN). Для інтеграції QKD у мережу оператора запропоновано архітектуру з виділеним контролером.

3.8.1 Архітектура QKD-SDN вузла

Архітектура вузла розділена на рівні:

Quantum Layer: Фізичне обладнання (Clavis3, SNSPD).

Key Management System (KMS): База даних ключів.

QKD-Agent: Модуль, що взаємодіє з центральним контролером через "Northbound Interface" (наприклад, RESTconf або NETCONF).

3.8.2 Інтеграція з шифраторами (ETSI GS QKD 014)

Кінцевим споживачем ключів є класичні шифратори (Link Encryptors). Для сумісності використано стандарт ETSI GS QKD 014.

Принцип взаємодії: Шифратор відправляє HTTP GET запит до KMS (/api/v1/keys/enc_keys), отримує ключ та його ID у форматі JSON. Шифратори на обох кінцях використовують KeyID для синхронізації зміни ключів.

3.9 Аналіз векторів атак та розробка контрзаходів

Незважаючи на теоретичну безпеку, реалізація QKD має вразливості "бічних каналів".

Атака "Троянський кінь" (Trojan Horse): Єва надсилає яскраве світло у систему Аліси, щоб просканувати стан її модулятора.

Контрзахід: Встановлення пасивних оптичних ізоляторів (> 60 дБ) та моніторингового детектора на виході Аліси.

Атака засліплення (Blinding Attack): Єва засвічує детектори Боба, переводячи їх у лінійний режим управління.

Контрзахід: Моніторинг струму зміщення та температури детекторів SNSPD.

Атака на часовий зсув (Time-shift): Єва маніпулює часом приходу фотона.

Контрзахід: Використання детекторів з малим джиттером (< 20 пс).

3.10 Проблематика стандартизації та сертифікації систем QKD

Впровадження технологій квантового розподілу ключів у комерційні та державні телекомунікаційні мережі неможливе без створення нормативно-правової бази та процедур сертифікації обладнання. Оскільки QKD є засобом криптографічного захисту інформації (ЗКЗІ), до нього висуваються жорсткі вимоги щодо надійності та відповідності заявленим характеристикам безпеки.

На сьогоднішній день провідну роль у розробці стандартів для QKD відіграє Європейський інститут телекомунікаційних стандартів (ETSI), який створив спеціальну робочу групу ISG-QKD (Industry Specification Group on QKD).

3.10.1 Архітектура стандартів ETSI

Розроблена нами система базується на рекомендаціях групи стандартів ETSI GS QKD, які регламентують різні аспекти функціонування квантових мереж:

ETSI GS QKD 002 (Use Cases) [26]: Визначає типові сценарії використання. У нашому проекті реалізовано сценарій "Metropolitan Area Network" (MAN).

ETSI GS QKD 008 (QKD Module Security Specification) [27]: Це ключовий документ, що визначає вимоги до фізичної безпеки модуля.

Захист від несанкціонованого фізичного доступу (Tamper detection). Корпус пристрою має бути оснащений датчиками відкриття, які при спрацюванні миттєво стирають ключі з пам'яті.

Контроль температури та напруги живлення лазерів для запобігання атакам через бічні канали.

ETSI GS QKD 014 (Implementation Security) [28]: Стандарт описує вимоги до квантових генераторів випадкових чисел (QRNG). Ентропія, що використовується для вибору базисів, повинна бути істинно випадковою.

Математично це перевіряється за допомогою статистичних тестів NIST SP 800-22 та Dieharder. У нашій програмній моделі (Розділ 2) припускається використання ідеального QRNG. У реальному пристрої (Розділ 3) необхідно проводити онлайн-моніторинг ентропії:

$$H_{min} = -log_2(\max P_i) \quad (3.3)$$

де H_{min} — мінімальна ентропія джерела. Якщо цей показник падає нижче порогового значення, генерація ключів має бути зупинена.

3.10.2 Процедура оцінки відповідності (Common Criteria)

Для міжнародного визнання безпеки системи QKD вона повинна пройти сертифікацію за стандартом ISO/IEC 15408 (Common Criteria) [29]. Математично випадковість перевіряється за допомогою статистичних тестів NIST SP 800-90A [30].

Процес сертифікації включає розробку двох документів:

Завдання з безпеки (Security Target - ST): Опис того, від яких саме загроз захищає система (наприклад, перехоплення фотонів, троянський кінь) і які припущення робляться (наприклад, фізична захищеність приміщень Аліси і Боба).

Профіль захисту (Protection Profile - PP): Узагальнений набір вимог для класу пристроїв.

Для систем QKD, що використовуються в банківському секторі, рекомендований рівень довіри EAL4+ (Evaluation Assurance Level 4 Augmented). Це означає, що система пройшла методичне тестування, аналіз вихідного коду та перевірку на вразливості незалежною лабораторією.

Особливістю сертифікації QKD є неможливість повної перевірки "чорної скриньки" через квантову природу сигналів. Тому критично важливим є перевірка Implementation Security — відповідності реальної фізичної схеми (оптики) її теоретичній моделі, що була доведена в Розділі 1.8. Будь-яке відхилення (наприклад, зайва ємність у детекторі або відбиття у модуляторі) може створити вразливість, не враховану в доказі безпеки.

3.11 Висновки до розділу 3

У третьому розділі вирішено інженерне завдання проектування, програмної реалізації та інтеграції системи QKD у телекомунікаційну інфраструктуру.

Програмна реалізація: Розроблено архітектуру та програмний комплекс для моделювання квантових мереж, що включає модулі фізичного рівня, логіки протоколів та візуалізації результатів. Застосування об'єктно-орієнтованого підходу дозволило створити гнучку систему, готову до масштабування.

Інтеграція в DWDM: Розроблено схему спектрального ущільнення каналів. Розрахунки показали, що для уникнення впливу нелінійних ефектів (зокрема Раманівського розсіювання) необхідно рознести квантовий канал (O-band, 1310 нм) та класичні канали (C-band, 1550 нм) з забезпеченням ізоляції фільтрів не менше 100 дБ.

Оптичний бюджет: Розрахунок для типової міської магістралі (25 км) показав сумарні втрати 18.65 дБ, що забезпечує запас надійності понад 10 дБ для обраного обладнання (IDQ Clavis3 + Single Quantum Eos) і гарантує стабільну генерацію ключів.

Управління та Безпека: Запропоновано концепцію управління мережею через SDN-контролер з використанням моделі даних YANG, що дозволяє динамічно маршрутизувати ключі.

Економічна доцільність: Розрахунок сукупної вартості володіння (TCO) на період 5 років показав, що впровадження системи QKD ($227 тис.) є економічно співставним з організацією щоденної кур'єрської доставки ключів ($175 тис.), проте забезпечує незрівнянно вищий рівень безпеки та автоматизації (оновлення ключів щохвилини проти однієї доби).

Таким чином, розроблений проект демонструє технічну, організаційну та економічну готовність технології QKD до впровадження в критично важливі мережі зв'язку.

ВИСНОВКИ

У магістерській дисертації вирішено актуальне науково-прикладне завдання дослідження методів побудови та моделювання параметрів квантових оптичних систем зв’язку, що дозволяє забезпечити гарантований рівень інформаційної безпеки в телекомунікаційних мережах майбутнього.

На основі проведених теоретичних досліджень, математичного моделювання та програмної реалізації отримано наступні основні результати:

Проведено аналіз архітектур квантових мереж.

Встановлено, що ключовою проблемою масштабування квантових мереж є експоненційне згасання сигналу в оптичному волокні, що обмежує дальність прямої передачі (без використання довірених вузлів або квантових репітерів) до 100–150 км. Показано, що на сучасному етапі розвитку технологій найбільш перспективною є гібридна архітектура, яка поєднує сегменти квантового розподілу ключів (QKD) для захисту критичних магістралей та класичні канали передачі зашифрованих даних. Визначено, що протокол BB84 залишається «золотим стандартом» для комерційних реалізацій, проте вимагає модифікацій (метод Decoy State) для захисту від атак на джерело випромінювання.

Розроблено комплексну математичну модель квантового каналу.

Створено модель, яка, на відміну від існуючих аналогів, враховує вплив реальних фізичних обмежень обладнання: темнові шуми детекторів, хроматичну дисперсію, оптичні помилки модуляції та ефекти скінченної довжини ключа.

Чисельне моделювання показало, що використання методу станів-пасток (Decoy State) дозволяє нівелювати загрозу атак розділення кількості фотонів (PNS) та використовувати більш потужні лазерні імпульси ($\mu \approx 0.5$). Це забезпечує збільшення граничної дальності зв’язку на 40–50 км порівняно зі стандартним протоколом BB84.

Визначено граничні характеристики продуктивності системи.

Встановлено критичні параметри для проектування міських та магістральних мереж QKD:

Для бюджетних систем на базі лавинних фотодіодів (InGaAs APD) гранична відстань передачі ключа становить 80 км, що достатньо для міських мереж (MAN).

Для високонадійних систем на базі надпровідникових детекторів (SNSPD) гранична відстань досягає 220 км, що дозволяє будувати міжміські магістралі без проміжних вузлів.

Доведено, що для забезпечення теоретично обґрунтованого рівня безпеки ($\epsilon_{sec} = 10^{-10}$) мінімальний розмір вибірки даних (block size) повинен складати не менше 10^5 біт. Зменшення вибірки призводить до нульової швидкості генерації секретного ключа через штрафи на статистичну похибку.

Розроблено архітектуру програмно-апаратного комплексу.

Спроектовано модульну архітектуру вузла квантової мережі, яка включає підсистеми управління оптичним обладнанням (через FPGA), постобробки ключів (корекція помилок, посилення приватності) та інтерфейси для інтеграції з зовнішніми шифраторами (REST API).

Розроблено програмний симулятор на мові Python, який дозволяє прогнозувати параметри QBER та SKR (Secret Key Rate) для довільних конфігурацій мережі. Це дозволяє операторам зв'язку планувати топологію мережі без необхідності проведення дорогих натурних експериментів.

Обґрунтовано методику інтеграції в мережі DWDM.

Показано, що побудова окремої волоконно-оптичної інфраструктури для QKD є економічно недоцільною. Запропоновано схему спектрального ущільнення, де квантовий канал передається у вікні прозорості O-band (1310 нм), а класичні канали даних — у C-band (1550 нм).

Розрахунки підтвердили, що при забезпеченні ізоляції фільтрів на рівні 100 дБ така схема дозволяє уникнути впливу нелінійних ефектів (Раманівського розсіяння) та забезпечити стабільну генерацію ключів у існуючих волоконних лініях.

Проведено аналіз безпеки та економічної ефективності.

Детально проаналізовано вектори атак на реалізацію («квантовий хакінг»), зокрема атаки «Троянський кінь» та засліплення детекторів. Запропоновано апаратні контрзаходи: встановлення оптичних ізоляторів, моніторинг вхідної потужності та температури детекторів.

Розрахунок сукупної вартості володіння (TCO) показав, що впровадження системи QKD ($227 тис. на 5 років) є конкурентним порівняно з традиційними методами фізичної доставки ключів кур'єрами ($175 тис.), при цьому забезпечуючи автоматичну зміну ключів кожну хвилину, що неможливо реалізувати ручними методами.

Рекомендації щодо подальших досліджень:

Перспективним напрямком розвитку роботи є дослідження атмосферних каналів зв'язку (Free-Space Optics) для організації "останньої милі" квантової мережі, а також розробка алгоритмів маршрутизації ключів у складних mesh-мережах з використанням технології програмно-конфігурованих мереж (SDN).

Таким чином, у дисертаційній роботі вирішено наукове завдання моделювання та проектування захищених квантових мереж, що має важливе значення для розвитку національної системи кібербезпеки

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kimble H. J. The quantum internet // Nature. 2008. Vol. 453, No. 7198. P. 1023–1030. URL: https://arxiv.org/abs/0806.4195.

2. Gisin N., Thew R. Quantum communication // Nature Photonics. 2007. Vol. 1, No. 3. P. 165–171.

3. Wehner S., Elkoff D., Hanson R. Quantum internet: A vision for the road ahead // Science. 2018. Vol. 362, No. 6412. URL: https://arxiv.org/abs/1807.06295.

4. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE чInternational Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984. P. 175–179.

5. Yin J. et al. Satellite-based entanglement distribution over 1200 kilometers // Science. 2017. Vol. 356, No. 6343. P. 1140–1144.

6. Chen Y. A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. 2021. Vol. 589, No. 7841. P. 214–219.

7. Pirandola S. et al. Advances in quantum cryptography // Advances in Optics and Photonics. 2020. Vol. 12, No. 4. P. 1012–1236.

8. Briegel H. J., Dür W., Cirac J. I., Zoller P. Quantum repeaters: The role of imperfect local operations in quantum communication // Physical Review A. 1998. Vol. 57, No. 5. P. 3319.

9. Muralidharan S. et al. Optimal architectures for long distance quantum communication // Scientific Reports. 2014. Vol. 4. P. 4113.

10. Sangouard N. et al. Quantum repeaters based on atomic ensembles and linear optics // Reviews of Modern Physics. 2011. Vol. 83, No. 1. P. 33–80.

11. Eisaman M. D., Fan J., Migdall A., Polyakov S. V. Single-photon sources and detectors // Reviews of Scientific Instruments. 2011. Vol. 82, No. 7. P. 071101.

12. Hadfield R. H. Single-photon detectors for optical quantum information applications // Nature Photonics. 2009. Vol. 3, No. 12. P. 696–705.

13. Senellart P., Solomon G., White A. High-performance semiconductor quantum-dot single-photon sources // Nature Nanotechnology. 2017. Vol. 12, No. 11. P. 1026–1039.

14. Gisin N., Tittel W. Quantum communication: battling dispersion // Nature Photonics. 2007. Vol. 1, No. 4. P. 187–189.

15. Lvovsky A. I., Sanders B. C., Tittel W. Optical quantum memory // Nature Photonics. 2009. Vol. 3, No. 12. P. 706–714.

16. Tittel W., Afzelius M., Gisin N. Quantum memories for quantum repeaters // Annales de Physique. 2010. Vol. 35, No. 2-3. P. 35–51.

17. Simon C. et al. Quantum repeaters with atomic ensembles and single-photon detectors // Physical Review Letters. 2007. Vol. 98, No. 19. P. 190503.

18. Afzelius M., Simon C., de Riedmatten H., Gisin N. Multimode quantum memory based on atomic frequency combs // Physical Review A. 2009. Vol. 79, No. 5. P. 052329.

19. Ekert A. K. Quantum cryptography based on Bell's theorem // Physical Review Letters. 1991. Vol. 67, No. 6. P. 661–663.

20. Bennett C. H. Quantum cryptography using any two nonorthogonal states // Physical Review Letters. 1992. Vol. 68, No. 21. P. 3121–3124.

21. Scarani V., Acín A., Ribordy G., Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations // Physical Review Letters. 2004. Vol. 92, No. 5. P. 057901.

22. Lo H.-K., Ma X., Chen K. Decoy state quantum key distribution // Physical Review Letters. 2005. Vol. 94, No. 23. P. 230504.

23. Lo H.-K., Curty M., Tamaki K. Secure quantum key distribution // Nature Photonics. 2014. Vol. 8, No. 8. P. 595–604.

24. Takeoka M., Guha S., Wilde M. M. Fundamental rate-loss tradeoff for optical quantum key distribution // Nature Communications. 2014. Vol. 5. P. 5235.

25. Scarani V. et al. The security of practical quantum key distribution // Reviews of Modern Physics. 2009. Vol. 81, No. 3. P. 1301–1350.

26. ETSI GS QKD 002 V1.1.1. Quantum Key Distribution (QKD); Use Cases. Sophia Antipolis: European Telecommunications Standards Institute, 2010.

27. ETSI GS QKD 008 V1.1.1. Quantum Key Distribution (QKD); QKD Module Security Specification. Sophia Antipolis: European Telecommunications Standards Institute, 2010.

28. ETSI GS QKD 014 V1.1.1. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. Sophia Antipolis: European Telecommunications Standards Institute, 2019.

29. ISO/IEC 15408-1:2009. Information technology — Security techniques — Evaluation criteria for IT security. Part 1: Introduction and general model. Geneva: ISO/IEC, 2009.

30. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A Revision 1. Gaithersburg: National Institute of Standards and Technology, 2015.

ДОДАТОК А Лістинг програмного коду модулів моделювання

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.special import xlogy

# ========================================
# МОДУЛЬ 1: КОНФІГУРАЦІЯ СИСТЕМИ
# ========================================
class SystemConfig:
    """Клас для збереження параметрів моделювання"""
    def __init__(self):
        # Параметри оптоволокна (SMF-28)
        self.alpha = 0.2          # Згасання (дБ/км)
        self.L_max = 250          # Максимальна дистанція (км)

        # Параметри протоколу
        self.mu = 0.5             # Середня к-сть фотонів (Decoy)
        self.f_rep = 1e9          # Частота джерела (1 ГГц)
        self.e_opt = 0.015        # Оптична помилка (1.5%)
        self.f_ec = 1.16          # Ефективність корекції (Cascade)

# ========================================
# МОДУЛЬ 2: МОДЕЛЬ ДЕТЕКТОРІВ
# ========================================
class Detector:
    """Базовий клас для детектора одиночних фотонів"""
    def __init__(self, name, qe, dcr, dead_time):
        self.name = name
        self.qe = qe              # Квантова ефективність
        self.dcr = dcr            # Темнові відліки (Hz)
        self.dead_time = dead_time # Мертвий час (s)
```

```
# Ініціалізація детекторів
det_ingaas = Detector("InGaAs APD", qe=0.20, dcr=2.0e-6, dead_time=10e-6)
det_snspd = Detector("SNSPD", qe=0.85, dcr=1.0e-7, dead_time=10e-9)

# ========================================
# МОДУЛЬ 3: ЯДРО СИМУЛЯЦІЇ (GLLP MODEL)
# ========================================
def simulate_key_generation(config, detector):
    """
    Розрахунок швидкості генерації ключа (SKR) та рівня помилок (QBER)
    залежно від відстані.
    """
    distances = np.linspace(0, config.L_max, 500)

    # 1. Розрахунок трансмісії каналу T = 10^(-alpha*L/10)
    transmittance = 10 ** (-config.alpha * distances / 10)

    # 2. Оцінка корисного сигналу (Signal)
    # R_raw = f_rep * mu * T * eta
    signal_rate = config.f_rep * config.mu * transmittance * detector.qe

    # 3. Оцінка шуму (Dark Counts)
    # Noise = 2 * DCR (для двох детекторів у схемі Боба)
    noise_rate = 2 * detector.dcr * config.f_rep

    # 4. Розрахунок QBER (Quantum Bit Error Rate)
    # QBER = (e_opt * Signal + 0.5 * Noise) / (Signal + Noise)
    total_rate = signal_rate + noise_rate
    qber = (config.e_opt * signal_rate + 0.5 * noise_rate) / total_rate

    # 5. Розрахунок секретного ключа (GLLP Formula)
    # R_sec = R_raw * [1 - f(e) * H(e)]
```

```
    # Бінарна ентропія H(x) = -x*log2(x) - (1-x)*log2(1-x)
    # Використовуємо xlogy для безпечного обчислення при x->0
    h_entropy = -(xlogy(qber, qber) + xlogy(1 - qber, 1 - qber)) / np.log(2)

    secret_key_rate = signal_rate * (1 - config.f_ec * h_entropy)

    # Фільтрація нефізичних результатів
    # Якщо QBER > 11% (поріг безпеки), ключ не генерується
    secret_key_rate[qber > 0.11] = 0
    secret_key_rate[secret_key_rate < 0] = 0

    return distances, qber * 100, secret_key_rate

# ==========================================
# МОДУЛЬ 4: ВІЗУАЛІЗАЦІЯ
# ==========================================
def plot_results():
    cfg = SystemConfig()

    # Запуск симуляції
    L, qber_in, skr_in = simulate_key_generation(cfg, det_ingaas)
    _, qber_sn, skr_sn = simulate_key_generation(cfg, det_snspd)

    # Побудова графіків
    fig, (ax1, ax2) = plt.subplots(2, 1, figsize=(10, 12))

    # Графік QBER
    ax1.plot(L, qber_in, 'r--', label=f'{det_ingaas.name}')
    ax1.plot(L, qber_sn, 'b-', label=f'{det_snspd.name}')
    ax1.axhline(11, color='k', linestyle=':', label='Security Threshold (11%)')
    ax1.set_ylabel('QBER (%)')
    ax1.set_xlabel('Distance (km)')
    ax1.set_ylim(0, 20)
    ax1.legend()
```

```
    ax1.grid(True)
    ax1.set_title('Quantum Bit Error Rate vs Distance')

    # Графік SKR
    ax2.semilogy(L, skr_in, 'r--', label=f'{det_ingaas.name}')
    ax2.semilogy(L, skr_sn, 'b-', label=f'{det_snspd.name}')
    ax2.set_ylabel('Secret Key Rate (bps)')
    ax2.set_xlabel('Distance (km)')
    ax2.set_ylim(10, 1e7)
    ax2.legend()
    ax2.grid(True, which="both")
    ax2.set_title('Secret Key Rate vs Distance')

    plt.tight_layout()
    plt.show()

if __name__ == "__main__":
    plot_results()
```