ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«МЕТОДИКА ЗАХИСТУ КОМУНІКАЦІЙ У РОЗПОДІЛЕНИХ СИСТЕМАХ НА ОСНОВІ КВАНТОВОЇ КРИПТОГРАФІЇ»**

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Анастасія ФОМКІНА.
(підпис) Ім'я, ПРІЗВИЩЕ здобувача

Виконав: здобувач вищої освіти гр. ТСДМ-63
Анстасія ФОМКІНА
Ім'я, ПРІЗВИЩЕ
Керівник:_к.т.н. професор Олексій ГЕТМАНЕЦЬ _
Ім'я, ПРІЗВИЩЕ
Науковий ступень,
вчене звання
Резензент: _____
Ім'я, ПРІЗВИЩЕ
Науковий ступень
вчене звання

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Телекомунікацій

Кафедра Телекомунікаційних систем та мереж_____
Ступінь вищої освіти магістр_____
Спеціальність 172 Електронні комунікації та радіотехніка_____
Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ

Завідувач кафедри ТСМ

д.т.н. професор ЗАЇКА ВІКТОР ФЕДОРОВИЧ

«____» _____2026 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Фомкіна Анастасія Віталіївна

1. **Тема роботи:** «Методика захисту комунікацій у розподілених системах на основі квантової криптографії»
   Керівник роботи: Гетманець Олексій Володимирович, к.т.н., професор.
   Затверджена наказом Державного університету інформаційно-комунікаційних технологій від 30.10.2025 року № 467.
2. **Строк подання кваліфікаційної роботи:** грудень 2025 р.
3. **Вихідні дані до кваліфікаційної роботи:**
   a. Сучасні розподілені інформаційні системи та їх вразливості.
   b. Протоколи квантового розподілу ключів (QKD): BB84, E91.
   c. Принципи постквантової криптографії та гібридних систем захисту.
   d. Стандарти NIST та рекомендації ETSI щодо квантової безпеки.
4. **Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):**
   a. Аналітичний огляд проблематики захисту інформації в розподілених системах в умовах загрози квантових обчислень.
   b. Дослідження теоретичних основ побудови захищених квантових комунікацій та вибір протоколів QKD.

c. Розробка методики та алгоритмів захисту комунікацій на основі гібридного підходу.
d. Експериментальна апробація розробленої методики на імітаційному програмному стенді та аналіз стійкості до атак.

5. **Перелік ілюстраційного матеріалу:** презентація на 10-12 слайдах.
6. **Дата видачі завдання:** 03.11.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір та аналіз науково-технічної літератури за темою дослідження	03.11.2025	Викон.
2.	Аналіз вразливостей розподілених систем та обмежень класичної криптографії	12.11.2025	Викон.
3.	Обґрунтування вибору протоколів квантового розподілу ключів (BB84, E91)	17.11.2025	Викон.
4.	Розробка моделі загроз для квантових та класичних каналів зв'язку	21.11.2025	Викон.
5.	Розробка алгоритму управління квантовими ключами та механізмів протидії атакам	28.11.2025	Викон.
6.	Створення імітаційного стенду для моделювання квантової мережі	08.12.2025	Викон.
7.	Проведення експериментальних досліджень та порівняльний аналіз продуктивності	15.12.2025	Викон.
8.	Оформлення пояснювальної записки, вступу та висновків	20.12.2025	Викон.
9.	Підготовка презентації та графічного матеріалу	22.12.2025	Викон.

Здобувач вищої освіти Анастасія ФОМКІНА

(підпис) (Ім’я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи Олексій ГЕТМАНЕЦЬ

(підпис) (Ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 95 стор., 15 рис., 14 табл., 14 джерел.

Мета роботи – підвищення рівня захищеності комунікацій у розподілених системах шляхом розробки методики захисту інформації, що базується на інтеграції протоколів квантового розподілу ключів (QKD) та класичних криптографічних механізмів.

Об'єкт дослідження – процес забезпечення конфіденційності та цілісності даних під час обміну інформацією у розподілених комунікаційних системах.

Предмет дослідження – методи, моделі та алгоритми захисту комунікацій на основі протоколів квантового розподілу ключів та гібридних криптосистем.

Короткий зміст роботи: У роботі проведено аналіз архітектури та вразливостей сучасних розподілених систем до квантових атак. Досліджено теоретичні основи побудови захищених квантових комунікацій, проведено порівняльний аналіз протоколів BB84 та E91. Розроблено структурну схему та алгоритми функціонування методики захищеного обміну даними на основі гібридного підходу (QKD + AES). Створено імітаційний програмний стенд (Python + Qiskit) для моделювання квантового розподілу ключів. Проведено експериментальні дослідження стійкості методики до атак типу «Intercept-Resend» та аналіз продуктивності системи.

КЛЮЧОВІ СЛОВА: КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ, QKD, РОЗПОДІЛЕНІ СИСТЕМИ, КВАНТОВА КРИПТОГРАФІЯ, ГІБРИДНИЙ ПІДХІД, ПРОТОКОЛ BB84, МОДЕЛЮВАННЯ АТАК, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

The part of the master's qualification work: 95 pages, 14 pictures, 14 tables, 90 sources.

The purpose of the work – to increase the security level of communications in distributed systems by developing an information security methodology based on the integration of quantum key distribution (QKD) protocols and classical cryptographic mechanisms.

Object of research – the process of ensuring data confidentiality and integrity during information exchange in distributed communication systems.

Subject of research – methods, models, and algorithms for communication security based on quantum key distribution protocols and hybrid cryptosystems.

Summary of the work: The thesis analyzes the architecture and vulnerabilities of modern distributed systems to quantum attacks. The theoretical foundations of building secure quantum communications are studied, and a comparative analysis of BB84 and E91 protocols is performed. A structural diagram and functioning algorithms for a secure data exchange methodology based on a hybrid approach (QKD + AES) are developed. A simulation software testbed (Python + Qiskit) for modeling quantum key distribution was created. Experimental studies of the methodology's resistance to Intercept-Resend attacks and system performance analysis were conducted.

KEYWORDS: QUANTUM KEY DISTRIBUTION, QKD, DISTRIBUTED SYSTEMS, QUANTUM CRYPTOGRAPHY, HYBRID APPROACH, BB84 PROTOCOL, ATTACK MODELING, INFORMATION SECURITY.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступня магістра

Фомкіна А. В.
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)

Освітньо- професійної програми Телекомунікаційні системи та мережі

на тему: «Методика захисту комунікацій у розподілених системах на основі квантової криптографії».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ __Владислав КРАВЧЕНКО__
(підпис) (Ім'я, ПРІЗВИЩЕ)

Висновок керівника кваліфікаційної роботи

Здобувач **Фомкіна Анастасія Віталіївна** під час виконання магістерської роботи продемонструвала високий рівень теоретичної підготовки та глибокі знання у сфері квантової криптографії та кібербезпеки. Працюючи над темою, авторка самостійно опанувала складні алгоритми квантового розподілу ключів (протоколи BB84, E91) та успішно реалізувала імітаційний програмний стенд для їх дослідження мовою Python з використанням бібліотеки Qiskit.

Здобувач проявила ініціативність, аналітичне мислення та вміння працювати з іноземною науковою літературою. Розроблена нею методика побудови гібридних систем захисту (QKD+AES) має практичну цінність для модернізації сучасних розподілених інфокомунікаційних мереж. Робота виконана у повному обсязі, відповідає вимогам до магістерських дисертацій.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **Фомкіної Анастасія Віталіївна** на оцінку **«відмінно»** та присвоїти їй кваліфікацію «магістр з електронних комунікацій та радіотехніки».

Завідувач кафедри _Телекомунікаційних систем та мереж_ _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

“ ” 2026 року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Фомкіної Анастасії Віталіївни

на тему: «Методика захисту комунікацій у розподілених системах на основі квантової криптографії»

Актуальність:

Стрімкий розвиток квантових обчислень ставить під загрозу сучасні криптографічні стандарти, що базуються на обчислювальній складності. У зв'язку з цим, перехід до новітніх архітектур мереж, які використовують фізичні закони для захисту даних, є критично важливим завданням. Робота Фомкіної А.В., присвячена інтеграції квантового розподілу ключів (QKD) у розподілені телекомунікаційні системи, є надзвичайно актуальною, оскільки пропонує конкретні методи протидії майбутнім кіберзагрозам (зокрема алгоритму Шора).

Позитивні сторони:

Робота характеризується високим рівнем наукової новизни, зокрема в частині розробки комплексної методики захисту комунікацій на основі гібридного підходу (поєднання квантових протоколів та симетричного шифрування AES).

Авторкою проведено ґрунтовний порівняльний аналіз протоколів BB84 та E91, що дозволило обґрунтувати вибір найбільш ефективних рішень для гетерогенних середовищ.

Важливою перевагою роботи є наявність практичної частини: розробка імітаційного програмного стенда мовою Python, що дозволив перевірити стійкість системи до атак типу «Intercept-Resend» та «Photon Number Splitting».

Одержані експериментальні дані (зокрема показники QBER та швидкості генерації ключів на різних відстанях) підтверджують адекватність запропонованих моделей.

Недоліки:

1. При моделюванні архітектури основна увага приділена програмній реалізації протоколів, тоді як аспект апаратних витрат на впровадження QKD-вузлів міг бути розглянутий детальніше.
2. У тексті зустрічаються поодинокі стилістичні неточності та зауваження до оформлення графічного матеріалу.

Висновок: Кваліфікаційна робота Фомкіної відповідає всім вимогам, що висуваються до магістерських дисертацій, містить завершене наукове дослідження та заслуговує на оцінку «відмінно». Авторка заслуговує на присвоєння кваліфікації магістра за спеціальністю 172 «Електронні комунікації та радіотехніка».

Рецензент: _____ _____

Науковий ступень, вчене звання підпис Ім'я, ПРІЗВИЩЕ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 10

ВСТУП……... 12

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ПРОБЛЕМАТИКИ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ СИСТЕМАХ……. 15

1.1. Особливості функціонування сучасних розподілених систем та їх основні вразливості…….. 15

1.2. Аналіз класичних криптографічних підходів до захисту комунікацій та їх обмеження в умовах загрози квантових обчислень… 21

1.3. Сучасний стан та перспективи розвитку квантової криптографії та технологій квантового розподілу ключів (QKD)..... 27

РОЗДІЛ 2. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КВАНТОВИХ КОМУНІКАЦІЙ…… 34

2.1. Розробка моделі загроз для комунікаційних каналів у розподілених системах з урахуванням специфіки квантових атак…….. 34

2.2. Обґрунтування вибору протоколів квантового розподілу ключів (наприклад, BB84, E91) для застосування в гетерогенних розподілених середовищах……. 40

2.3. Дослідження методів інтеграції квантових та класичних криптографічних механізмів для побудови гібридних систем захисту... 45

РОЗДІЛ 3. РОЗРОБКА МЕТОДИКИ ТА АЛГОРИТМІВ ЗАХИСТУ КОМУНІКАЦІЙ…… 51

3.1. Структурна схема запропонованої методики захисту комунікацій у розподілених системах на основі гібридного підходу…….. 51

3.2. Розробка алгоритму управління квантовими ключами та встановлення захищених сеансів зв'язку між вузлами системи…….. 57

3.3. Механізм виявлення та протидії атакам на квантовий канал передачі даних (атака «людина-по-середині», атака на джерело фотонів)..... 59

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНА АПРОБАЦІЯ РОЗРОБЛЕНОЇ МЕТОДИКИ…….. 66

4.1. Опис імітаційного програмного стенду для моделювання квантового розподілу ключів у багатокористувацькій розподіленій мережі…… 66
4.2. Аналіз результатів тестування стійкості методики до змодельованих сценаріїв атак та оцінка її ефективності…….. 71
4.3. Порівняльний аналіз продуктивності та рівня безпеки розробленої методики з існуючими класичними аналогами……... 75
ВИСНОВКИ……... 81
ПЕРЕЛІК ПОСИЛАНЬ……. 85
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ…… 95

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АПІ	Інтерфейс прикладного програмування
IoT	Інтернет речей
ІТ	Інформаційні технології
ПЗ	Програмне забезпечення
AES	Advanced Encryption Standard
BB84	Bennett-Brassard 1984
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service»
DWDM	Dense Wavelength Division Multiplexing
E91	Ekert 1991
ECC	Elliptic Curve Cryptography
FIFO	First In, First Out
IaaS	Infrastructure as a Service
ITS	Information-Theoretic Security
LKMS	Local Key Management System
LPWAN	Low-Power Wide-Area Network
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
OTDR	Optical Time-Domain Reflectometer

PaaS	Platform as a Service
PNS	Photon Number Splitting
PQC	Post-Quantum Cryptography
PRNG	Pseudo-Random Number Generator
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RSA	Rivest-Shamir-Adleman
SaaS	Software as a Service
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
SKR	Secret Key Rate
SSL	Secure Sockets Layer
TF-QKD	Twin-Field Quantum Key Distribution
TLS	Transport Layer Security
TRNG	True Random Number Generator
WCP	Weak Coherent Pulses

ВСТУП

Актуальність теми. Сучасний цифровий світ дедалі більше покладається на розподілені системи - від хмарних обчислень та Інтернету речей до блокчейн-технологій та систем критичної інфраструктури. Надійність та безпека комунікацій у таких системах є фундаментальною вимогою. Однак існуючі криптографічні методи, зокрема асиметричні алгоритми (RSA, ECC), що лежать в основі захисту даних, є вразливими до атак з використанням повномасштабних квантових комп’ютерів, розробка яких є лише питанням часу. Ця загроза ставить під сумнів довгострокову безпеку конфіденційної інформації.

Наукова проблема полягає у відсутності комплексних методик, які б дозволяли інтегрувати принципово нові, фізично обґрунтовані механізми захисту, такі як квантова криптографія, у складну архітектуру сучасних розподілених систем. На відміну від математичних підходів, квантовий розподіл ключів (QKD) базується на законах квантової фізики, що гарантує виявлення будь-якої спроби перехоплення інформації. Це зумовлює необхідність розробки нових підходів до побудови захищених комунікаційних мереж, здатних протистояти як класичним, так і майбутнім квантовим загрозам.

Мета і завдання дослідження. Метою магістерської роботи є підвищення рівня захищеності комунікацій у розподілених системах шляхом розробки методики захисту інформації, що базується на інтеграції протоколів квантового розподілу ключів та класичних криптографічних механізмів.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. провести аналіз архітектури та вразливостей сучасних розподілених систем, визначити обмеження класичних криптографічних підходів;
2. дослідити існуючі протоколи квантового розподілу ключів та обґрунтувати їх переваги й недоліки для застосування в гетерогенних мережах;

3. розробити модель загроз, що враховує специфічні вектори атак на квантові та класичні канали зв'язку;
4. розробити структурну схему та алгоритми функціонування методики захищеного обміну даними на основі гібридного підходу;
5. створити імітаційний стенд для експериментальної апробації розробленої методики;
6. провести експериментальні дослідження для підтвердження адекватності та ефективності запропонованої методики.

Об'єкт дослідження - процес забезпечення конфіденційності та цілісності даних під час обміну інформацією у розподілених комунікаційних системах.

Предмет дослідження - методи, моделі та алгоритми захисту комунікацій на основі протоколів квантового розподілу ключів та гібридних криптосистем.

Методи дослідження. Для вирішення поставлених завдань у роботі використано комплекс загальнонаукових та спеціальних методів: методи системного аналізу та теорії інформаційної безпеки - для аналізу предметної області; методи теорії ймовірностей та математичної статистики - для оцінки стійкості криптографічних протоколів; методи імітаційного моделювання - для перевірки адекватності та ефективності розробленої методики.

Наукова новизна одержаних результатів:

7. Вперше запропоновано комплексну методику захисту комунікацій у розподілених системах, яка, на відміну від існуючих, базується на гібридному підході, що поєднує надійність квантового розподілу ключів для генерації сеансових ключів та ефективність симетричних алгоритмів для шифрування даних.
8. Удосконалено модель загроз для розподілених систем, що враховує специфічні вектори атак на фізичний (квантовий) та логічний рівні комунікацій, що дозволяє підвищити ефективність механізмів протидії.

Практичне значення одержаних результатів. Розроблена методика може бути використана при проєктуванні та модернізації захищених інформаційно-телекомунікаційних систем у критично важливих сферах, таких

як державне управління, банківський сектор, оборонний комплекс та енергетика, для забезпечення довгострокового захисту даних від відомих та перспективних кіберзагроз. Програмний стенд може слугувати інструментом для подальших досліджень та тестування гібридних криптографічних рішень.

Структура та обсяг роботи. Магістерська робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 95 сторінок, з них 73 сторінок основного тексту. Робота містить 14 рисунків, 14 таблиць. Список використаних джерел налічує 90 найменувань.

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ПРОБЛЕМАТИКИ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ СИСТЕМАХ

1.1 Особливості функціонування сучасних розподілених систем та їх основні вразливості

Розподілені системи - це обчислювальні архітектури, у яких кілька автономних вузлів (комп'ютерів чи пристроїв), часто географічно рознесених, спільно виконують єдине завдання [1]. Для узгодження дій ці вузли обмінюються повідомленнями мережею, забезпечуючи масштабованість та розподілене використання ресурсів [2]. Ключовими рисами таких систем є відмовостійкість, здатність розширюватися шляхом додавання нових вузлів і ефективне спільне використання ресурсів [1]. Наприклад, сучасні клієнт-серверні та хмарні системи (SaaS, PaaS, IaaS), системи обробки даних (Hadoop, MapReduce) і блокчейн-платформи забезпечують гнучке розгортання та балансування навантаження, знижуючи ймовірність збоїв при виході з ладу окремих компонентів [1, 2]. Відповідно, розподілені системи використовуються у хмарних сервісах, IoT-мережах, фінансових платформах і наукових обчисленнях, де потрібна висока продуктивність і надійність (напр., модель Facebook для безперервного обслуговування користувачів, брокерські платформи для невідкладного оновлення біржових даних) [2].

Розгортання розподілених систем зазвичай супроводжується географічним розосередженням компонентів по всьому світу. Наприклад, у типовій розподіленій IT-інфраструктурі мережеве обладнання, сервери та клієнтські робочі місця можуть бути розташовані в різних країнах, утворюючи складну архітектуру взаємозв'язків [3]. Це створює численні підмережі та канали зв'язку між вузлами. Основними характеристиками такої системи є прозорість (скритність розташування компонентів для кінцевого користувача), гнучкість (здатність динамічно масштабуватися), різнорідність обладнання і протоколів, паралельність виконання задач і одночасний доступ до спільних даних [1, 2]. Наприклад, системи Інтернету речей використовують тисячі

сенсорів і шлюзів, підключених через різні технології (Wi-Fi, Bluetooth, LPWAN), що дозволяє обробляти потоки даних у реальному часі ближче до джерела їх виникнення. Наявність кількох рівнів взаємодії (клієнт-сервер, однорангові мережі, краєві та хмарні компоненти) визначає високу адаптивність і масштабованість таких систем [1, 3].

Центральною перевагою розподілених систем є їхня відмовостійкість. Завдяки дублюванню та резервуванню даних, відмові одного вузла зазвичай відповідає його негайне підмінення іншим, а система продовжує виконувати завдання [1, 8]. Такі підходи широко застосовуються в комерційних хмарах і соціальних мережах, де сотні серверів реплікують інформацію для безперервного обслуговування запитів [2]. Однак ця здатність до самозцілення й паралельної обробки потребує складної системи моніторингу і управління. Організувати узгодженість даних і синхронізацію між численними вузлами складно: необхідно опрацьовувати конфліктні оновлення, часові затримки й латентність мережі. Ці особливості розподілених систем знижують час простою, але ускладнюють проєктування протоколів коректної взаємодії. Навіть несуттєве затримання у зв'язку між вузлами може призвести до розбіжностей у даних або повторних запитів, що нерідко використовується зловмисниками [2, 8].

Водночас розподілені системи мають значний набір уразливостей, обумовлених їх відкритістю та масштабом. Перш за все, великою проблемою є широка площа атаки (attack surface). Тобто кожен додатковий вузол або канал зв'язку стає потенційним входом для кіберзагрози [3, 5]. Наприклад, сучасні IoT-екосистеми створюють мільярди точок входу - станом на 2024 рік налічується близько 18,5 млрд підключених IoT-пристроїв у світі, а до кінця 2025 року їх прогнозують на рівні 21,1 млрд [4]. Таке розширення чисельності пристроїв розподіленої мережі значно збільшує складність і вразливість інфраструктури. Дослідження показують, що з кожним новим класом пристроїв (сенсори, шлюзи, мобільні вузли) посилюються ризики атак на мережевому рівні - від перехоплення чи спотворення даних у відкритих каналах до

блокувань трафіку (DDoS) [3, 6]. Відомо, що проблема управління доступом у таких системах надзвичайно складна: незалежні компоненти можуть використовувати різні протоколи та цілісні засоби аутентифікації, а централізований контроль авторизації часто відсутній [3, 5].

Віддалені канали зв'язку розподілених систем роблять їх чутливими до мережевих атак. У переліку головних кіберзагроз - атаки типу «людина посередині» (MITM), перехоплення трафіку, фальсифікація та повтор команд [6, 7]. Наприклад, у комунікаціях баз IoT неможливо уникнути публічних мереж, тому їх пов'язують із проблемами мережевої безпеки та конфіденційності [3]. Хмарно-орієнтовані IoT-сервіси надають гнучкість і масштабованість, але одночасно розширюють поверхню атак - додаткові ризики виникають через залучення сторонніх провайдерів і центральне зберігання даних [3]. Так, при переході на PaaS/IaaS розподілені системи стають уразливими до атак на сервіси хмарних постачальників і на API, що з'єднують різні рівні системи [3, 7]. Недостатньо захищені програмні інтерфейси та помилки конфігурації систем (напр., вбудований брандмауер, невірні правила доступу) часто стають головною причиною витоку даних [7].

Наявність численних користувачів і вузлів ускладнює забезпечення контролю доступу та зменшує можливості верифікації кожного учасника. Розподілені системи не мають централізованого вузла управління - це означає, що зловмисник може використати вразливість на одній кінці ланцюга та поширити шкідливу дію на інші сегменти системи [5, 6]. Такий приклад маємо в енергетиці: у дослідженнях повідомляється, що в Україні за один місяць 2021 року близько 19 % промислових систем стали жертвами кібератак (здебільшого мережевих та на робочі станції користувачів) [6]. У деяких випадках це призводило до відключення критичної інфраструктури - відома атака 2016 року вивела з ладу живлення більшість районів Києва. Іншим прикладом є вірус Stuxnet (2009), що через зараження сторонньою флешкою викликав збій центрифуг на іранському ядерному об'єкті [6]. Навіть невеликі вектори атаки в таких системах можуть дати катастрофічний ефект. Крім мережевих загроз,

розподілені системи можуть містити уразливості в програмному забезпеченні самих вузлів. Наприклад, у багатьох промислових роботах і когоботах знайдено понад 50 помилок у програмному коді [6], які дозволяють зловмиснику віддалено змінювати поведінку пристроїв (щодо дій при контакті з людьми, вимикання датчиків тощо).

Сучасні розподілені системи поєднують переваги продуктивності та доступності, але вимагають посиленого захисту. Фрагментована природа таких систем означає відсутність єдиної точки довіри та неможливість централізованого аудиту, що ускладнює дотримання політик безпеки [3, 5]. Кожне розширення мережі додатково збільшує складність забезпечення цілісності та конфіденційності даних. Як показано в таблиці 1.1, кількість вузлів і приладів у сучасних розподілених мережах постійно зростає, що автоматично розширює набір потенційних уразливостей (Табл. 1.1) (Рис. 1.1).

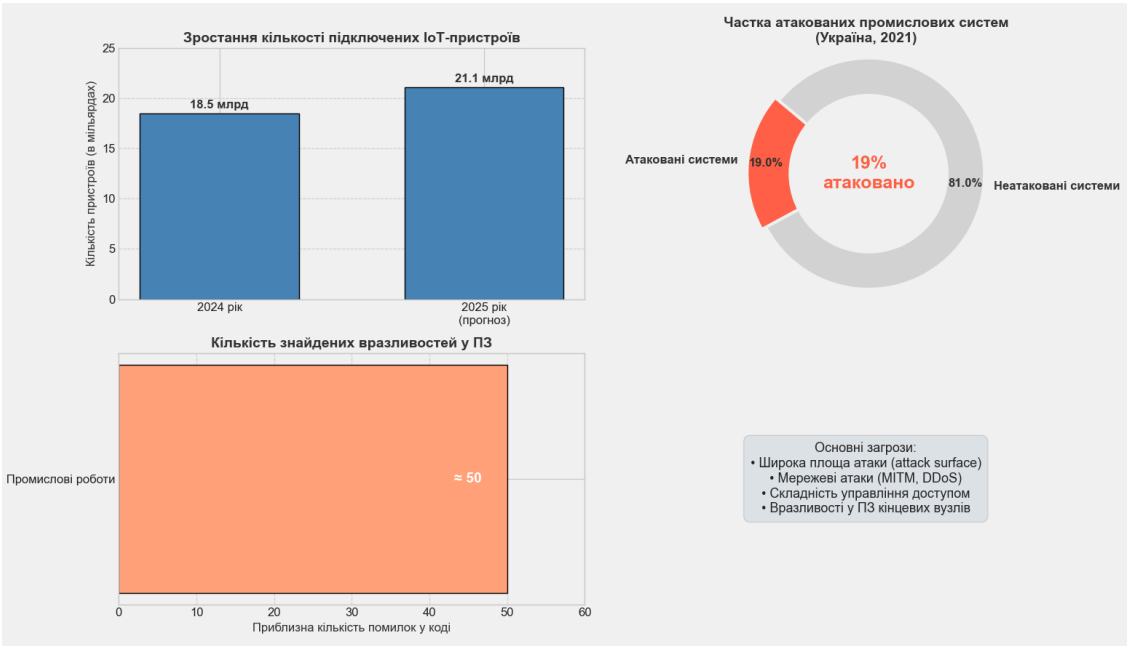


Рис. 1.1 Ключові показники масштабу та вразливостей розподілених систем

Одночасно, відсутність централізованого контролю ускладнює виявлення й запобігання атак на ранніх стадіях [6, 8]. Характеристикам масштабованості та надійності сучасних розподілених систем протистоять масштабні загрози з

боку кібератак та помилок конфігурації, які необхідно враховувати при проєктуванні механізмів захисту на їхній основі (Табл. 1.1).

Таблиця 1.1

Основні показники масштабованості та загроз розподілених систем.

Показник	Значення
Підключені IoT-пристрої (світова кількість, 2024)	18,5 млрд
Прогнозовані підключені IoT-пристрої (2025)	21,1 млрд
Частка атакованих промислових систем (Україна, 2021)	19 %
Вразливості у програмному забезпеченні промислових роботів	≈ 50

Окрім вищезазначених загроз, специфічною проблемою функціонування розподілених систем є вразливість механізмів досягнення консенсусу. У системах без єдиного центру керування (наприклад, блокчейн-мережі або розподілені бази даних) вузли повинні узгоджувати стан реєстру транзакцій за допомогою алгоритмів, таких як Paxos, Raft або BFT (Byzantine Fault Tolerance) [9]. Якщо зловмиснику вдається захопити контроль над критичною часткою вузлів (наприклад, атака 51% або атака Сібіли), він може порушити цілісність даних, скасосувати транзакції або створити альтернативну версію історії подій. У сучасних умовах, коли фінансові та логістичні системи все частіше спираються на децентралізовані реєстри, компрометація алгоритмів консенсусу становить загрозу системного рівня, яку складно нейтралізувати традиційними засобами захисту периметра [9, 10].

Важливим аспектом є також безпека внутрішнього трафіку між мікросервісами, так званий "East-West" трафік. У класичних моделях захисту основна увага приділялася "North-South" трафіку (вхід/вихід з мережі), тоді як обмін даними всередині розподіленого кластера часто вважався довіреним і шифрувався слабше або передавався у відкритому вигляді [10]. Проте в сучасних хмарних архітектурах, де фізичне розташування контейнерів та віртуальних машин динамічно змінюється, концепція "довіреного периметра"

втрачає актуальність. Зловмисник, що проникнув в один із сегментів розподіленої мережі, може перехоплювати службовий трафік між сервісами, отримуючи доступ до конфіденційних метаданих, ключів API та сесійних токенів, що вимагає впровадження концепції Zero Trust з обов'язковим шифруванням кожного внутрішнього з'єднання [11].

Критичною вразливістю для розподілених систем є також залежність від точної синхронізації часу. Протоколи, такі як NTP (Network Time Protocol) або PTP (Precision Time Protocol), є життєво необхідними для коректного впорядкування подій (timestamping) та управління терміном дії криптографічних сертифікатів [11, 12]. Атаки на системи синхронізації (time shifting attacks) дозволяють зловмисникам маніпулювати логами, обходити механізми захисту від повторного відтворення пакетів (replay attacks) та порушувати логіку роботи розподілених баз даних, що покладаються на часові мітки для вирішення конфліктів запису (наприклад, Google Spanner або Cassandra). Відсутність надійного, криптографічно захищеного джерела часу робить розподілену інфраструктуру вразливою до складних логічних атак [12].

Окремої уваги потребує проблема управління ключами шифрування в умовах високої динаміки мережевих вузлів. У масштабних розподілених системах, де кількість екземплярів сервісів може змінюватися автоматично залежно від навантаження (автоскейлінг), процедури генерації, розподілу та відкликання ключів стають "вузьким місцем" безпеки [13]. Традиційні інфраструктури відкритих ключів (PKI) часто не встигають обробляти запити на сертифікацію для короткоживучих контейнерів, що призводить до використання довгострокових ключів або їх некоректного зберігання у конфігураційних файлах. Це створює ризик компрометації всієї мережі через витік одного статичного ключа, який використовується на багатьох вузлах одночасно [13].

Значний ризик для цілісності розподілених систем становить також гетерогенність програмного забезпечення та вразливості ланцюжка постачання (supply chain attacks). Оскільки розподілені системи часто компонуються з модулів різних виробників та використовують численні сторонні бібліотеки,

оновлення безпеки не завжди можуть бути застосовані синхронно на всіх вузлах [14]. Це створює вікна вразливості (N-day vulnerabilities), коли частина мережі вже оновлена, а інша залишається вразливою, що дозволяє зловмисникам використовувати відомі експлойти для атаки на незахищені сегменти. Асинхронність оновлень у географічно розподілених кластерах ускладнює підтримку єдиного рівня захищеності всієї інфраструктури [14, 15].

Розподілені системи чутливі до атак на логіку узгодженості даних (consistency attacks). Відповідно до теореми CAP, розподілена система не може одночасно гарантувати узгодженість, доступність та стійкість до розділення [15]. Більшість сучасних систем обирають модель "узгодженості в кінцевому рахунку" (eventual consistency) заради продуктивності. Зловмисники можуть експлуатувати часовий лаг між записом даних на одному вузлі та їх реплікацією на інші для здійснення атак типу "race condition" (стан гонитви), наприклад, подвійного витрачання коштів у фінансових системах або несанкціонованого доступу до ресурсів, права на які вже були відкликані на головному сервері, але інформація про це ще не надійшла до периферійного вузла [15].

Фундаментальною проблемою є накопичення величезних обсягів зашифрованого трафіку, що передається через публічні канали зв'язку між вузлами розподіленої системи. Враховуючи довготривалу цінність інформації (медичні дані, державні таємниці, банківські транзакції), розподілені мережі стають головною мішенню для стратегії "збирай зараз, розшифровуй пізніше" (Harvest Now, Decrypt Later) [16]. Навіть якщо поточні алгоритми шифрування (наприклад, TLS 1.3 на базі еліптичних кривих) є стійкими до класичного криптоаналізу, вони не гарантують захисту від майбутніх квантових обчислювачів. Це робить архітектуру сучасних розподілених систем стратегічно вразливою у довгостроковій перспективі та вимагає переходу до нових фізичних принципів захисту каналів зв'язку [16].

1.2 Аналіз класичних криптографічних підходів до захисту комунікацій та їх обмеження в умовах загрози квантових обчислень

Класичні криптографічні протоколи забезпечують безпеку комунікацій за допомогою математично складних задач, наприклад, факторизації та дискретних логарифмів. Проте розроблені квантові алгоритми кардинально змінюють їх стійкість [9, 10]. Зокрема, алгоритм Шора ефективно розв'язує задачу факторизації та дискретного логарифмування за поліноміальний час, що робить ненадійними всі стандартні схеми з відкритим ключем (RSA, Диффі–Хеллмана, ECC, DSA тощо). Останні оцінки вказують, що 2048–бітний RSA, що еквівалентний близько 112–бітній класичній стійкості, може бути зламаний на квантовому комп'ютері за порівняно короткий час [11]. Так, за даними NCSC (UK), квантовий комп'ютер з ~20 млн фізичних кубіт здатен розкласти RSA–2048 за ~8 годин, а останні дослідження навіть прогнозують можливість зламу RSA–2048 менш ніж за тиждень на машині з менш ніж мільйоном кубіт. Аналогічно, алгоритм Шора підриває стійкість всієї інфраструктури із застосуванням відкритого ключа: цифрові підписи, ключові обміни TLS/SSL та блокчейн–протоколи будуть уразливі до зловмисника з квантовим комп'ютером [12]. Наприклад, кріптографічно значимі системи RSA та ECC використовують складні для класичних комп'ютерів задачі, але квантові алгоритми дозволяють їх «зламати» і тим самим повністю скомпрометувати захист. Це означає, що в умовах реальної загрози побудови масштабних квантових

комп'ютерів обмін ключами та аутентифікація на основі класичних алгоритмів втратять ефективність (який би високий рівень захисту вони не забезпечували при звичайних обчисленнях) [13, 14 ,15].

Симетричні алгоритми (наприклад, AES) уразливі меншою мірою, проте і вони зазнають стійкого зниження безпеки під квантовим впливом. Алгоритм Гровера дозволяє квадратично пришвидшити пошук ключа, тому ефективна довжина ключа зменшується удвічі. Згідно з оцінками, AES–128 формально дає лише ~2^64 операцій у квантовому зломі замість 2^128 у класичному випадку, а AES–256 ~2^128 замість 2^256. Такі результати означають, що AES–128 еквівалентно стає 64–бітно захищеним від квантового нападу, а AES–256 – приблизно 128–бітним [16, 17]. Для збереження адекватного захисту рекомендується подвоювати довжину ключів: на практиці AES–256 вважається «постквантово безпечним» (ефективна стійкість ~128 біт). Аналогічно, алгоритми хешування SHA–2/3 також піддаються квадратичному прискоренню атак, наприклад SHA–256 зменшує колізійну стійкість з 128 до ≈64 біт. Внаслідок цього сучасні симетричні схеми з високими ключами вважаються відносно більш стійкими до квантових атак, але для довгострокового захисту також необхідне їх посилення [18].

Таблиця 1.2

Порівняння стійкості криптографічних алгоритмів у класичних та квантових умовах

Алгоритм	Довжина ключа (біт)	Класична стійкість (біт)	Ефективна квантова стійкість (біт)
RSA-2048	2048	≈112	0 (зламаний)
ECC (P-256)	256	≈128	0 (зламаний)
AES-128	128	128	64
AES-256	256	256	128

В табл. 1.2 наведено порівняння класичної та квантово-ефективної стійкості для кількох поширених алгоритмів. Зокрема, RSA-2048 (класична безпека ≈112 біт) виявляється повністю «зламаним» квантовим нападом, тоді як AES-256 (256 біт) після квадратичного зменшення має ефективно ≈128-бітний захист (Табл. 1.2). Це ілюструє фундаментальне обмеження класичних методів: підвищення апаратних потужностей квантового комп'ютера зрештою дозволить зламувати RSA/ECC за практично скінченний час, а також різко скоротити навантаження на алгоритми із симетричною довжиною ключа (Рис. 1.2).

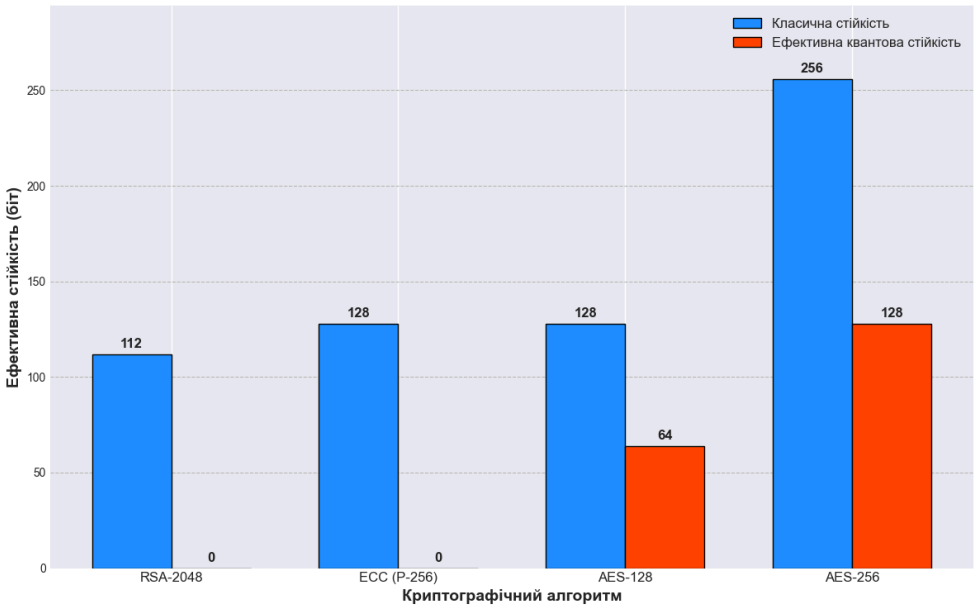


Рис. 1.2 Порівняння стійкості криптографічних алгоритмів до класичних та квантових атак

Не менш важливим є обмеження часу: навіть якщо квантовий комп'ютер для криптоаналізу ще не існує, вже здійснюються атаки типу «записати і дешифрувати пізніше» (harvest now, decrypt later). Експерти припускають, що перші криптографічно релевантні квантові машини можуть з'явитися в найближчі 5-15 років, що потребує своєчасної міграції на нові підходи. З урахуванням цього NIST випустив перші стандарти постквантової криптографії та рекомендує почати їх впровадження. Інакше збереження конфіденційності комунікацій на основі лише класичних алгоритмів стане неможливим, оскільки майбутній квантовий напад зруйнує обчислювальні бар'єри, на яких вони тримаються.

Крім безпосередньої загрози конфіденційності, квантові обчислення створюють критичні ризики для інфраструктури відкритих ключів (PKI), яка є фундаментом довіри в сучасному інтернеті. Ієрархічна модель довіри базується на цифрових сертифікатах, підписаних кореневими центрами сертифікації за допомогою алгоритмів RSA або ECDSA. Компрометація приватного ключа кореневого центру за допомогою алгоритму Шора дозволить зловмиснику генерувати валідні підроблені сертифікати для будь-якого ресурсу, здійснюючи

непомітні атаки «людина-посередині» (MITM) глобального масштабу. Це фактично зруйнує систему аутентифікації веб-сайтів, банківських сервісів та державних реєстрів, оскільки користувачі не зможуть відрізнити легітимний ресурс від зловмисного [19].

Ще однією проблемою класичних підходів є вразливість механізму «досконалої прямої секретності» (Perfect Forward Secrecy - PFS), який використовується в сучасних протоколах TLS. PFS покладається на ефемерний обмін ключами Діффі-Хеллмана (DHE або ECDHE) для генерації унікальних сеансових ключів. Оскільки стійкість протоколу Діффі-Хеллмана базується на проблемі дискретного логарифмування, квантовий комп'ютер зможе відновити всі минулі сеансові ключі, якщо було записано зашифрований трафік процедури рукостискання (handshake). Це означає, що механізми, покликані захистити минулі сеанси навіть при компрометації довгострокового ключа, стають недієвими в постквантову епоху [19, 20].

Значний ризик виникає також для цілісності програмного забезпечення та оновлень систем. Механізми підпису коду (Code Signing), які гарантують, що програмне забезпечення не було модифіковано зловмисниками, переважно використовують алгоритми хешування та асиметричного підпису, вразливі до квантових атак. Злам цифрового підпису дозволить зловмисникам впроваджувати шкідливий код у легітимні оновлення операційних систем та програмного забезпечення, що може призвести до масового зараження пристроїв IoT та критичної інфраструктури через офіційні канали розповсюдження ПЗ, обходячи стандартні антивірусні перевірки [21].

Варто також звернути увагу на проблему генерації випадкових чисел у класичних криптосистемах. Більшість сучасних алгоритмів використовують псевдовипадкові генератори чисел (PRNG), які є детермінованими алгоритмами, що ініціалізуються початковим значенням (seed). Хоча для класичних комп'ютерів передбачити вихідну послідовність PRNG є обчислювально складною задачею, квантові алгоритми машинного навчання та методи розв'язання систем рівнянь можуть виявити приховані закономірності або

відновити внутрішній стан генератора. Це ставить під загрозу ентропію ключів шифрування, роблячи їх передбачуваними для квантового зловмисника, незалежно від довжини самого ключа [22].

Суттєвим обмеженням класичних криптографічних систем є також складність переходу на нові стандарти, відома як проблема «криптографічної спритності» (crypto-agility). Багато розподілених систем мають «жорстко закодовані» криптографічні примітиви або апаратні обмеження, що унеможливлюють швидку заміну алгоритмів RSA/ECC на постквантові аналоги (PQC) без повної заміни обладнання. Постквантові алгоритми (наприклад, на основі решіток) часто вимагають значно більших розмірів ключів та підписів, що може спричинити критичні затримки в мережах з низькою пропускною здатністю або в системах реального часу, роблячи їх непридатними для існуючої інфраструктури [23].

Аналіз часових рамок впровадження захисту описується «теоремою Моска» (Mosca’s Inequality), яка стверджує, що ризик є критичним, якщо сума часу, необхідного для міграції на нові стандарти, та часу, протягом якого інформація повинна залишатися секретною, перевищує час до появи квантового комп'ютера. Для багатьох секторів (державна таємниця, медичні дані, геномна інформація) термін секретності становить десятки років. Враховуючи повільність стандартизації постквантових алгоритмів та інерційність оновлення розподілених систем, класичні підходи вже зараз знаходяться в зоні неприпустимого ризику, навіть якщо потужний квантовий комп'ютер з'явиться лише через десятиліття [24].

Класичні методи захисту не враховують потенціал квантових алгоритмів у сфері криптоаналізу побічних каналів (side-channel attacks). Квантові сенсори та алгоритми обробки сигналів можуть дозволити зловмисникам отримувати секретні ключі, аналізуючи енергоспоживання або електромагнітне випромінювання класичних криптопроцесорів з набагато вищою точністю та швидкістю, ніж це можливо зараз. Це означає, що фізична безпека поточних

апаратних модулів безпеки (HSM) та смарт-карт може бути скомпрометована, нівелюючи математичну стійкість закладених у них алгоритмів [25].

1.3 Сучасний стан та перспективи розвитку квантової криптографії та технологій квантового розподілу ключів (QKD)

У сучасному світі розвиток квантових комп'ютерів ставить під загрозу класичні методи криптографії, тому квантова криптографія розглядається як шлях забезпечення інформаційної безпеки наступного покоління. Системи розподіленого обміну ключами на базі принципів квантової механіки (QKD) гарантують захист передачі ключів, оскільки їхня безпека не ґрунтується на складності алгоритмів, а на фізичних законах [21, 26]. Згідно з міжнародними оглядами, QKD сьогодні є найпросунутішою технологією для обміну секретними ключами з інформаційною безпекою незалежно від обчислювальних ресурсів (теоретично неможливо зламати зловмисником) [22].

Практичний стан квантових комунікацій демонструє швидке розгортання експериментальних та прикладних систем. Наприклад, у Великобританії запрацювала перша протяжна квантова мережа між Кембриджем і Бристолем із довжиною оптичного волокна понад 410 км для квантово-захищеного відеозв'язку [30]. У Китаї створено оптоволоконний QKD-магістраль довжиною до 2000 км, що з'єднує Пекін і Шанхай, а також використовується супутниковий канал «Micius» для глобального

розповсюдження ключів [25]. Водночас китайський квантовий мікросупутник Jinan-1 встановив рекорд – забезпечив створення секретного ключа між Китаєм та Південною Африкою на відстані близько 12900 км за один проліт, генеруючи понад 1,07×10^6 біт ключа за сеанс [21]. У Південній Кореї, Сінгапурі, Японії та інших країнах також активно розгортаються міські QKD-мережі. Зокрема, у токійській квантовій мережі NICT продемонстровано квантові цифрові підписи в міському масштабі. Подібні мережі будує і Європейський Союз в рамках ініціативи EuroQCI, де всі 27 держав-членів координують створення національних та міжнародних квантових каналів (волокно + супутники) [23, 27]. Так, анонсовано запуск першого європейського QKD-супутника «Eagle-1» (квантова передача на борту) орієнтовно у 2026 р. для глобального QKD-покриття [22]. У США Науково-дослідове агентство оборони DARPA запустило програму QuANET (2023 рік) для інтеграції квантових каналів у існуючу мережеву інфраструктуру, показуючи зростаючий інтерес до гібридних квантово-класичних рішень [19].

Технічні досягнення в QKD також значні. Новітні експерименти підтвердили можливість практичного збільшення відстані та швидкості. Зокрема, Pittaluga et al. (Nature 2025) реалізували близнюкове поліваджене (twin-field) QKD через комерційне волокно довжиною 254 км між Франкфуртом і Келем, досягнувши швидкості ~110

біт/с [24]. Це вдвічі перевищило попередні межі неохолоджуваних систем. Аналогічно, у Німеччині продемонстровано протокол BB84 з детермінованим одноквантовим джерелом на основі напівпровідникових квантових точок: за лінком 79 км (25,49 дБ втрат, що еквівалентно 130 км стандартного волокна) отримано рекордні $4{,}8\times10^{-5}$ біт на імпульс із середнім QBER ≈0,65% [26]. Ці результати підтверджують, що сучасні квантові джерела (світло на вимогу) та протоколи MDI–QKD можуть значно підвищити пропускну здатність та дальність мереж.

Одночасно з «чисто» квантовими рішеннями розвиваються гібридні підходи. Так, наприклад, компанія China Telecom створила систему, яка комбінує QKD з постквантовою криптографією. У травні 2025 р. було здійснено перший у світі голосовий дзвінок зашифрований на відстані понад 1000 км (між Пекіном і Хефеєм) із використанням цього гібридного методу [25]. При цьому міська квантова мережа Хефея становить 1147 км оптоволоконних ліній з восьми центральними вузлами і 159 точками доступу, що обслуговують понад 500 урядових установ [25]. У США мережа Chicago Quantum Exchange з'єднала центр Чикаго з науковими лабораторіями по 200 км волокон, і на ній почав працювати протокол QKD зі швидкістю понад 80 000 біт/с [18]. Аналогічно, Toshiba Europe успішно випробувала невимушений TF–QKD у існуючій мережі Німеччини,

стабільно передавши квантову інформацію на 250 км без складного охолодження [19, 27].

Сьогодні ми спостерігаємо швидкий перехід від лабораторних до пілотних і навіть комерційних систем квантового зв'язку. Наукові і промислові ініціативи зосереджені на стандартизації й масштабуванні QKD. Наприклад, у 2023 р. ETSI (Європейський інститут стандартів телекомунікацій) випустив першу Protection Profile для QKD-модулів (GS QKD 016) – технічні вимоги до безпеки квантових пристроїв. Разом з тим, зростає ринок квантової криптографії: за оцінками аналітиків, обсяг глобального ринку квантової криптографії становив ≈518,3 млн дол. США у 2023 р. і прогнозується зростання до ≈4,62 млрд дол. до 2030 р. при CAGR ~38% [28].

Сумарно сучасний розвиток квантової криптографії характеризується як активний і багатоаспектний: демонструються рекордні дистанції та швидкості QKD [21, 24, 26], розгортання міських і міжміських мереж (Sat-to-ground і Terrestrial) [23, 27, 29, 30], гібридизація з класичними методами [26], а також масштабні інфраструктурні проєкти (приклад – EuroQCI) з орієнтацією на застосування в критичних системах [20, 23, 26, 27]. (Табл. 1.3) показує деякі приклади характеристик найвідоміших демонстраційних QKD-ліній (Рис. 1.3). Усі ці досягнення створюють потужний фундамент для подальшого впровадження гібридних

квантово-класичних рішень захисту комунікацій у розподілених системах.

Таблиця 1.3

Порівняльні показники експериментальних QKD-ліній

Розгортання	Дальність, км	Пропускна здатність / Результат
Мікросупутник Jinan-1 (КНР-ПАР)	12900	~1,07×10^6 біт за проліт (секретних біт) [1]
Frankfurt-Kehl (TF-QKD, Німеччина)	254	~110 біт/с [4]
Chicago Q-Loop (CQE, США)	200	~80 000 біт/с (6 вузлів, 124 милі) [12, 13]

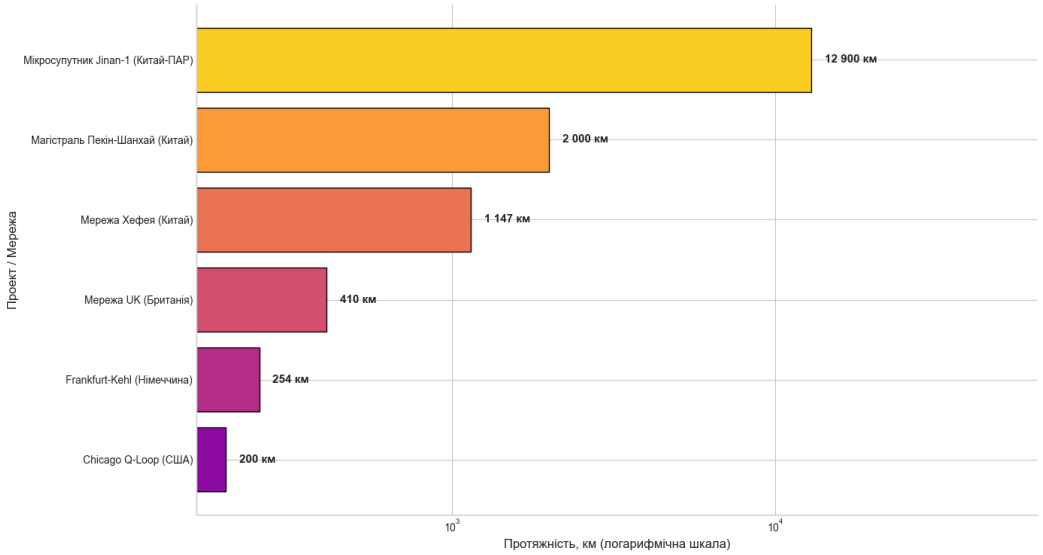


Рис. 1.3 Порівняння протяжності провідних світових QKD-мереж та каналів зв'язку

Окремим важливим напрямком розвитку є мініатюризація обладнання для квантового розподілу ключів за допомогою технологій інтегральної фотоніки. Розробка фотонних інтегральних схем (Photonic Integrated Circuits — PIC) дозволяє розмістити лазери, модулятори та детектори на єдиному напівпровідниковому кристалі, що суттєво зменшує габарити,

енергоспоживання та вартість кінцевих пристроїв [29]. Дослідники вже демонструють прототипи QKD-передавачів розміром із монету, здатних працювати на гігагерцових частотах. Масове виробництво таких чіпів є критичною умовою для впровадження квантової криптографії у портативні пристрої та термінали Інтернету речей, виводячи технологію за межі магістральних оптичних мереж [29, 31].

Паралельно з удосконаленням дискретних протоколів (DV-QKD) набувають популярності системи квантового розподілу ключів на безперервних змінних (CV-QKD). Ця технологія кодує інформацію в квадратурах електромагнітного поля світлової хвилі, а не в поляризації чи фазі поодиноких фотонів, що дозволяє використовувати стандартні телекомунікаційні компоненти та когерентні детектори, аналогічні тим, що застосовуються у класичних оптичних мережах [32]. CV-QKD демонструє високу спектральну ефективність і сумісність із технологіями щільного хвильового мультиплексування (DWDM), що спрощує інтеграцію квантових каналів у вже існуючу волоконно-оптичну інфраструктуру без необхідності використання дорогих однофотонних детекторів [32, 33].

Критичним викликом для масштабування квантових мереж залишається проблема загасання сигналу в оптичному волокні, яку в класичних мережах вирішують підсилювачі. Оскільки згідно з теоремою про заборону клонування квантовий сигнал неможливо підсилити без руйнування його стану, наукова спільнота зосереджена на розробці квантових повторювачів (quantum repeaters) [34]. Ці пристрої базуються на технології квантової пам’яті та обміні заплутаністю (entanglement swapping), що дозволяє передавати квантові стани на необмежені відстані без фізичного переміщення носія через увесь канал. Успішна реалізація ефективних квантових повторювачів стане ключовим етапом переходу від мереж із довіреними вузлами до повноцінного квантового Інтернету [34, 35].

Значний прогрес спостерігається також у сфері управління квантовими мережами за допомогою технологій програмно-конфігурованих мереж (SDN).

Сучасні архітектури QKD вимагають динамічного перерозподілу ресурсів та маршрутизації ключів у складних топологіях типу «mesh» або «кільце» [36]. SDN-контролери для квантових мереж дозволяють централізовано керувати політиками безпеки, автоматично відновлювати з'єднання у разі обриву оптичних ліній та оптимізувати використання квантових ключів різними додатками. Розробка стандартизованих інтерфейсів між QKD-обладнанням та SDN-контролерами є предметом активної роботи міжнародних консорціумів [36, 37].

Окрім технічних аспектів, важливу роль відіграє формування міжнародної нормативної бази, яка виходить за межі рекомендацій ETSI. Міжнародний союз електрозв'язку (ITU-T) активно розробляє серію рекомендацій Y.3800, що охоплюють архітектуру, вимоги до безпеки та методи оцінки якості обслуговування (QoS) у квантових мережах [38]. Стандартизація протоколів інтерфейсів прикладного програмування (API) для отримання ключів дозволить уніфікувати взаємодію між обладнанням різних вендорів (Multi-vendor interoperability), що є необхідною умовою для побудови глобальної квантової інфраструктури. Це також сприятиме створенню єдиних методик сертифікації модулів QKD державними регуляторами безпеки [38, 39].

Окремий фокус досліджень спрямований на застосування QKD для захисту критичної інфраструктури, зокрема в енергетичному секторі (Smart Grids). Сучасні інтелектуальні енергомережі вимагають надзвичайно точної синхронізації часу та надійної автентифікації команд управління для запобігання техногенним катастрофам [40]. Експериментальні проєкти демонструють можливість використання квантових мереж не лише для шифрування трафіку SCADA-систем, але й для розподілу сигналів точного часу з квантовою захищеністю. Це дозволяє нівелювати загрози атак на протоколи NTP/PTP, забезпечуючи стабільність роботи розподілених енергетичних потужностей [22, 40].

Економічна складова впровадження QKD поступово покращується завдяки переходу від лабораторних установок до серійного виробництва. Хоча

вартість розгортання квантових ліній все ще залишається високою через потребу в спеціалізованому обладнанні (наприклад, надпровідних нанодротових детекторах, що потребують кріогенного охолодження), тенденції вказують на здешевлення компонентної бази [41]. Поява моделі «QKD як послуга» (QKD-as-a-Service), де провайдери надають квантові ключі через орендовану інфраструктуру, відкриває доступ до технології для середнього бізнесу та фінансових установ, знижуючи поріг входження та стимулюючи подальший розвиток ринку квантової безпеки [41].

РОЗДІЛ 2 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КВАНТОВИХ КОМУНІКАЦІЙ

2.1 Розробка моделі загроз для комунікаційних каналів у розподілених системах з урахуванням специфіки квантових атак

Розподілені системи характеризуються високою складністю мережевої інфраструктури та гетерогенними каналами зв'язку, що породжує різноманітні вектори атак. Зокрема, розвинені розподілені мережі вимагають «критичних безпекових рамок» для протидії новітнім загрозам [31]. Квантове розподілення ключів (QKD) пропонує інформаційно-непробивне шифрування, однак зловмисник може реалізувати стратегію «запам'ятай-зашифруй-пізніше», перехоплюючи зашифровані повідомлення зараз з наміром дешифрувати їх у майбутньому квантовим комп'ютером [32, 40]. Модель загроз повинна враховувати не тільки безпосередні атаки на канал, а й часові атаки типу Harvest-Now-Decrypt-Later [32, 40].

Загрози у каналах зв'язку можна класифікувати за режимом діяльності зловмисника (пасивні / активні) та за сучасними стандартами кібербезпеки. Наприклад, Басері з колегами пропонують відображати вразливості в QKD-системах на моделі STRIDE (загрози: імперсонація, модифікація даних, відмова, розкриття секрету тощо) [36]. Більш специфічним підходом є врахування рівнів доступу атакуючого: за запропонованою Зуо та співавт., виділяють п'ять сценаріїв (Eve(1)-Eve(5)) зростаючих повноважень «людини-посередині» від простого прослуховування каналу до повного контролю пристроїв Аліси та Боба [34]. Такий розподіл дозволяє коректніше моделювати як внутрішні загрози (компрометація вузлів мережі), так і зовнішні (перехоплення оптичних ліній) [33, 35].

Сучасні дослідження висвітлюють широкий спектр квантово-специфічних атак на канали зв'язку. Зокрема, реалізації QKD-систем вразливі до атак «людина-посередині» (MITM), коли зловмисник перехоплює фотони і відправляє свої, що створює помітні помилки (пороговий квантовий бітовий

рівень помилок, QBER, підвищується). Існують атаки розщеплення фотонного числа (PNS), коли на «слабкі» лазерні імпульси з кількома фотонами забирається один фотон, даючи зловмиснику певну інформацію при майже нульовій детектованій аномалії [33]. Також відомі «троянські» атаки на вхід фотонних джерел (подавання сторонніх сигналів для витоку інформації про внутрішню конфігурацію) та «затемнення детектора» (атаку на фотодетектори мереж, які можуть бути введені у режим штучного відключення або фіксації чутливості) [33, 38]. Усім цим атакам властиві характерні "сигнатури" - наприклад, інтерцепт-ресенд збільшує QBER приблизно до 25%, тоді як PNS-атаки дають можливість зловмиснику дістати ключ без додання помітних шумів, якщо не застосовувати протидії. Загалом, як відзначається, базові квантові протоколи (BB84, E91 тощо) теоретично неуразливі, але практичні дефекти апаратури створюють уразливі точки (бокові канали), що експлуатуються у реальних атаках [33].

Крім квантово-специфічних, варто враховувати і класичні атаки на мережеві канали розподілених систем. Зловмисник може викликати відмову в обслуговуванні (DoS), штучно збільшуючи шум або зашумлюючи квантовий канал так, щоб неможливо було одержати секретний ключ [34]. Наприклад, Егоров та співавт. показали, що збільшення оптичного шуму може вивести з ладу QKD-з'єднання (мітиться як DoS-атака), на що система має реагувати маршрутизацією по іншому шляху [34]. Аналогічну думку висловлюють Реннер і Вольф: квантові лінії можуть бути вразливі до DoS за певних умов, але подібні атаки можна пом'якшити методами перенаправлення трафіку, як у класичних мережах [37]. Також у розподілених мережах необхідно враховувати компрометацію вузлів - зловмисник, що контролює проміжний вузол, може знімати інформацію з ключів або передавати хибні дані, якщо модель загроз не передбачає довірених вузлів [31].

Для наочності деяких характеристик розгортання квантових мереж наводяться приклади мультивузлових QKD-інфраструктур у світі (Табл. 2.1). Так, наприклад, у Польщі (PSNC) 2022 року збудовано інтерміське QKD-лінк

протяжністю 380 км із 5 вузлами, у Великій Британії (мережа Cambridge) 2023 р. - лінк на 25 км із 3 вузлами [38]. До 2010 р. в Японії побудовано мережу з 7 вузлів на 300 км (Tokyo QKD Network) [38]. Ці дані свідчать про поступове нарощування масштабів і довжин QKD-мереж (Табл. 2.1). Загрози ж моделі враховують як особливості квантових каналів, так і специфіку розподілених топологій [36, 38] (Рис. 2.1).

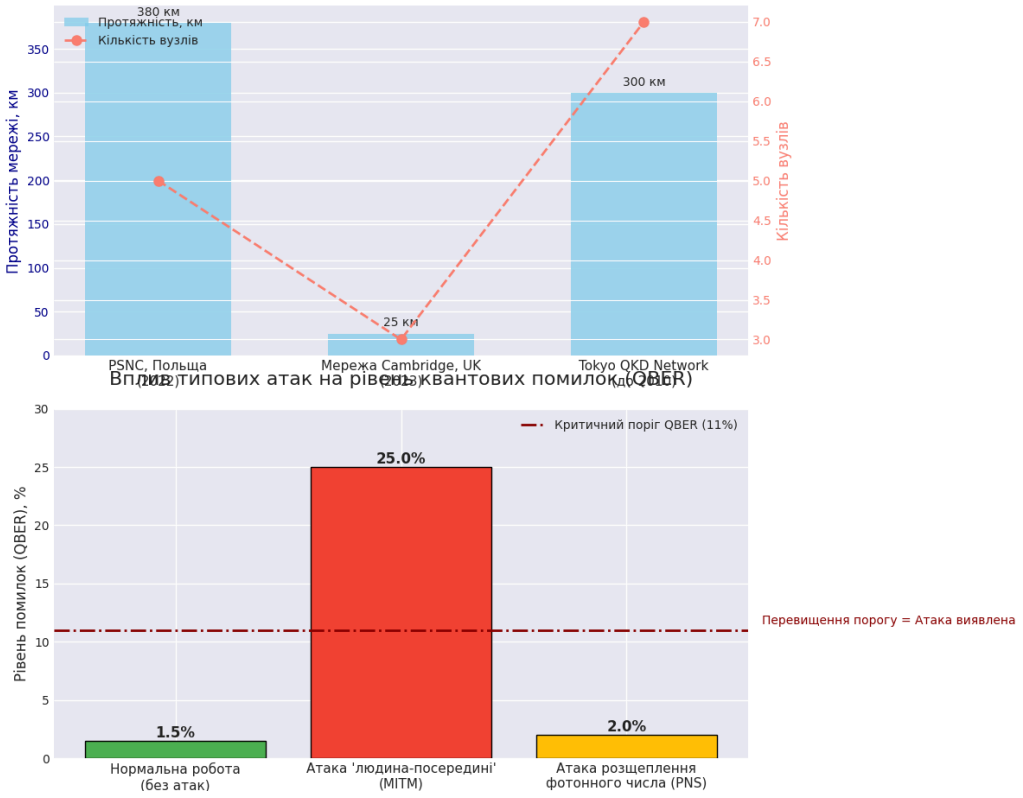


Рис. 2.1 Порівняльні характеристики QKD-мереж та вплив атак на рівень квантових помилок (QBER)

Таблиця 2.1

Приклади мультивузлових QKD-інфраструктур

Назва мережі / Місце	Рік	Протяжність, км	Кількість вузлів
PSNC, Польща	2022	380	5
Мережа Cambridge, Велика Британія	2023	25	3

Tokyo QKD Network, Японія	до 2010	300	7

Ключовим у моделюванні є поєднання квантових та класичних факторів. Зокрема, атаки, що поза межами квантового каналу (наприклад, ламання симетричної аутентифікації чи підміну вузлів), можуть знищити гарантії QKD. У цьому зв'язку слід врахувати, що аутентифікація самого каналу у QKD часто спирається на класичні механізми (наприклад, нагіда шифрування попередніх ключів) і тому може бути вразливою до класичних атак [35]. Однак у рамках моделі загроз її слід розглядати окремим шаром захисту.

Модель загроз квантових комунікаційних каналів у розподілених системах будується на основі багатоступеневого аналізу: визначення активних і пасивних атак на квантовий та класичний канали, класифікація рівнів доступу зловмисника та аналіз можливих наслідків кожного сценарію. Рамкова методика SQOUT, наприклад, формалізує такий аналіз, поєднуючи процедури TTP (тактика-техніка-процедура) з міжнародними стандартами ризик-менеджменту [39]. У рамках SQOUT ілюструється «kill-chain» для атаки PNS, а також застосовуються перевірені методики оцінки ризиків для квантових систем [39]. Запропонована модель загроз включає адаптацію наявних методів кібербезпеки до нових квантових ризиків з урахуванням конкретики як квантових каналів (фізичних вразливостей), так і розподіленої архітектури мережі [36, 39].

Окремим вектором у моделі загроз є вразливості, пов'язані з побічними каналами витоку інформації (side-channel attacks), які виникають через недосконаліть фізичної реалізації обладнання. На відміну від теоретичних протоколів, реальні пристрої споживають енергію та випромінюють електромагнітні хвилі, характеристики яких можуть корелювати з оброблюваними квантовими станами [41]. Зокрема, аналіз часових затримок (timing attacks) при спрацюванні однофотонних детекторів дозволяє зловмиснику отримати інформацію про значення біта ключа, якщо різні детектори мають відмінні часові характеристики відновлення (dead time) [42]. Модель загроз повинна враховувати можливість високоточного вимірювання

зловмисником часових інтервалів між імпульсами для ідентифікації використаного базису вимірювання.

Значну небезпеку становлять атаки на підсистему генерації випадкових чисел (RNG), яка є фундаментом безпеки будь-якої криптографічної системи, включаючи квантову. Якщо квантовий генератор випадкових чисел (QRNG), що відповідає за вибір базисів та формування бітової послідовності, має приховані кореляції або зміщення (bias), ентропія генерованого ключа знижується [43]. У такому сценарії зловмисник може з високою ймовірністю передбачити налаштування обладнання Аліси та Боба, не втручаючись безпосередньо в оптичний канал. Тому модель загроз має включати сценарії компрометації джерел ентропії та необхідність постійного моніторингу статистичних властивостей вихідної послідовності в реальному часі [43, 44].

У контексті розподілених систем критичного значення набувають загрози програмного рівня, спрямовані на стек протоколів постобробки ключів (post-processing stack). Процедури просіювання, корекції помилок та підсилення приватності реалізуються за допомогою класичного програмного забезпечення, яке може містити стандартні вразливості: переповнення буфера, помилки логіки або впровадження шкідливого коду [45]. Атака на програмний модуль управління ключами (Key Management System) дозволяє зловмиснику отримати готовий секретний ключ вже після його генерації, оминаючи складний процес злому квантового каналу. Це вимагає розширення моделі загроз за межі оптичного рівня до рівня операційних систем та інтерфейсів прикладного програмування (API) вузлів мережі [46].

Сучасні моделі загроз також починають враховувати використання зловмисником методів машинного навчання (Adversarial Machine Learning) для оптимізації стратегій перехоплення. Нейронні мережі можуть бути навчені розпізнавати патерни роботи квантових пристроїв або адаптувати параметри атаки «людина-по-середині» таким чином, щоб утримувати рівень помилок (QBER) трохи нижче порогового значення спрацювання сигналізації [47]. Такий «розумний» зловмисник здатний динамічно змінювати тактику в залежності від

стану каналу зв'язку, маскуючи свої дії під природні флуктуації середовища, що вимагає впровадження інтелектуальних систем виявлення аномалій на стороні захисту [47].

Ще одним специфічним класом загроз є атаки лазерного пошкодження (Laser Damage Attack), спрямовані на фізичну деградацію компонентів приймача. Спрямовучи потужний лазерний імпульс в оптичне волокно, зловмисник може викликати термічне пошкодження однофотонних лавинних діодів, змінюючи їхню ефективність або переводячи їх у лінійний режим роботи [48]. Це створює "вікно вразливості", де детектор перестає реагувати на поодинокі фотони, але продовжує детектувати яскраві імпульси, дозволяючи реалізувати атаку засліплення (blinding attack) без необхідності складного контролю фази. Моделювання таких загроз вимагає врахування порогів фізичної стійкості оптичних елементів [48, 49].

Критичною для розподілених систем є загроза порушення синхронізації часу між вузлами (Time Synchronization Attack). Протоколи QKD, особливо ті, що працюють на високих швидкостях, вимагають пікосекундної точності синхронізації для коректного співставлення відправлених та отриманих кубітів [50]. Зловмисник може маніпулювати класичними сигналами синхронізації (наприклад, спотворюючи pulse-per-second сигнал), що призведе до розсинхронізації часових вікон дететування. Це не тільки штучно підвищує QBER, блокуючи генерацію ключа (DoS), але й може бути використано для вибіркового фільтрування квантових станів, створюючи умови для більш складних атак на коректність вимірювань [50].

Модель загроз повинна включати ризики, пов'язані з ланцюжком постачання компонентів (Supply Chain Attacks). Оскільки квантові системи складаються з високотехнологічних модулів (лазери, модулятори, FPGA), вироблених різними вендорами, існує ймовірність впровадження апаратних "закладок" (hardware trojans) ще на етапі виробництва [51]. Такі модифікації можуть активуватися за певних умов, знижуючи інтенсивність сигналу або вносячи передбачувані патерни в роботу модуляторів. В умовах відсутності

можливості повної верифікації кожного транзистора в чіпі, модель повинна передбачати стратегії диверсифікації обладнання та використання методів device-independent QKD (DI-QKD) для мінімізації довіри до апаратної частини [51, 52].

2.2 Обґрунтування вибору протоколів квантового розподілу ключів (наприклад, BB84, E91) для застосування в гетерогенних розподілених середовищах

Протоколи квантового розподілу ключів поділяються на алгоритми з дискретними змінними, як BB84, та протоколи на базі квантового заплутування, як E91 [41, 50]. У протоколі BB84 (Беннет і Брассард, 1984) інформація кодується одиничними фотонами, підготовленими в двох неперпендикулярних базисах. Протокол E91 (Екерт, 1991) використовує заплутану пару фотонів, розподілену між комунікуючими сторонами [41]. Безпека E91 забезпечується моногамією квантового заплутування: вимірювання нерівності Белла (CHSH) дозволяє виявити будь-яке втручання, оскільки повне порушення нерівності підтверджує наявність справжнього заплутаного стану [43, 45]. E91 фактично лежить в основі ідеї пристроєво-індепендентного QKD (DI-QKD), що гарантує безпеку навіть за частково невідомих властивостей пристроїв [43, 48]. Протокол BB84 має доведену протоколяльну безпеку й широку практичну реалізацію: у його вдосконаленому варіанті з декоїд-станами він забезпечує стійкість до атак типу PNS [42, 44]. Додавання декоїд-станів і удосконалені методи корекції помилок дозволяють значно підвищити стійкість BB84-протоколів [44].

Протокол BB84 довів свою надійність і масштабованість: рішення у цій лінійці (наприклад, комерційна система T12 компанії Toshiba) забезпечують обмін ключами на відстані до ~150 км оптоволокна [42]. Експерименти показують, що навіть у складних умовах мережі BB84-протоколи забезпечують високу швидкість ключоутворення: наприклад, в системі з декоїд-фазовим кодуванням при мультиплексуванні 60 DWDM-каналів по 100 Гбіт/с у C-діапазоні на відстані 50 км було досягнуто >100 кбіт/с чистої швидкості

ключа. Це свідчить про те, що BB84 може ефективно працювати в гетерогенних середовищах з поєднанням квантових та інтенсивних класичних каналів [45]. У порівнянні з цим, реалізація E91 складніша через необхідність генерації та поширення високоякісних заплутаних пар фотонів, що істотно обмежує практичні відстані і швидкості обміну ключем. Недавні експерименти з незалежних рубідієвих атомів показали DI-QKD по лінії довжиною 400 м із результативною швидкістю близько 0.07 біт на пару фотонів [43], що є значно нижчим показником у порівнянні з BB84 над відповідними відстанями. Такі дані ілюструють, що BB84 дає вищу швидкість обміну ключами на середніх дистанціях, тоді як E91 забезпечує підвищений рівень безпеки за рахунок властивості заплутаності [43, 45] (Рис. 2.2).

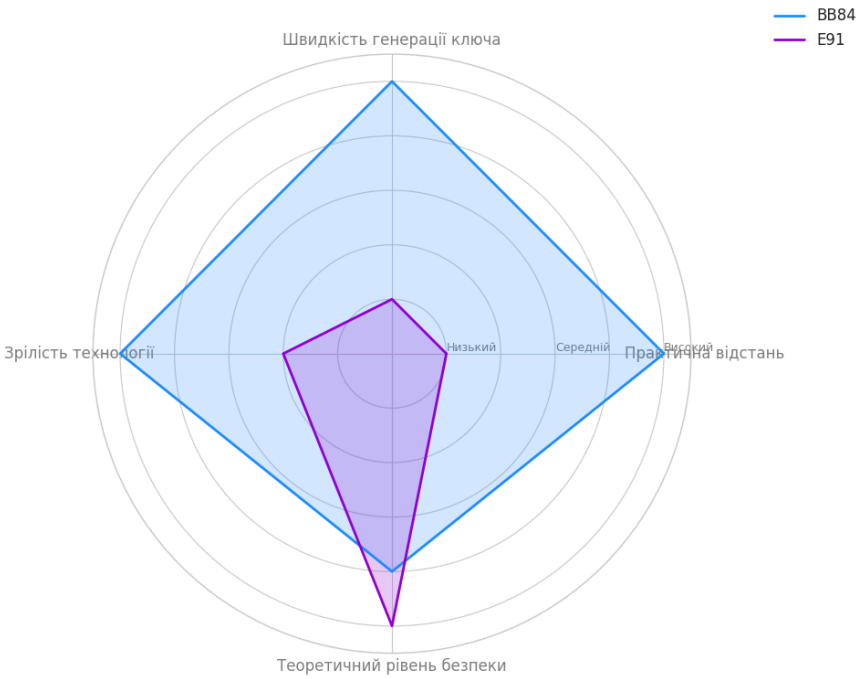


Рис. 2.2 Візуалізація ключових характеристик протоколів BB84 та E91

Узагальнені характеристики цих двох протоколів наведено в табл. 2.2.

Таблиця 2.2

Порівняльні характеристики протоколів BB84 та E91

Показник	BB84	E91 (Ekert)

Рік створення	1984 [41]	1991 [41]
Максимальна відстань (кілометри)	~150 (опт. на основі T12) [42]	~0.4 (експеримент DI-QKD) [43]
Швидкість обміну (біт/с)	>100000 (50 км) [42]	0.07 біт/зустріч на пару [43]
Статус впровадження	Доведена безпека, висока зрілість [42]	Доведена безпека, складна реалізація [45]

Вибір протоколу в гетерогенній мережі залежить від структури та вимог середовища. Наприклад, у мережевому проєкті MadQCI (Мадридський квантовий проєкт) продемонстровано побудову гетерогенної QKD-мережі, що включає 28 модулів від п'яти різних виробників на 9 локаціях з відстанями 1.9-33.1 км [49]. Це показує, що BB84- або його варіанти з декоїд-станами дозволяють інтегрувати системи різних виробників, забезпечуючи гнучке масштабування та автоматичне управління за допомогою SDN-технологій [49]. Також пропонується використовувати багаторівневі схеми захисту: наприклад, у деяких системах гібридно поєднують квантовий обмін ключами з класичними криптоалгоритмами (QKD+ECC) для посилення стійкості до атак [47]. У цьому контексті мережі типу «Multi-Node QKD» з топологіями решітка або зірка дозволяють спільно використовувати заплутані стані для зв'язку між багатьма пристроями [47].

Протокол BB84 (дискретно-квантова схема) є природним вибором для гетерогенних мереж завдяки високій зрілості реалізації та широкій підтримці у комерційних системах [42]. Він здатний забезпечити високі швидкості обміну ключами на оптоволоконних каналах середньої протяжності. Протокол E91, хоча і гарантує теоретично вищий рівень безпеки через заплутаність, вимагає складніших пристроїв (підсилювачів фоторозрядів і джерел заплутаних фотонів) і на даний час реалізується переважно в наукових експериментах. Водночас нові підходи (наприклад, Twin-Field QKD, 2021) пропонують перспективи подальшого збільшення дальності QKD за рахунок інтерференції двох світлових доріжок [46]. Застосування декоїд-станів та інтеграція QKD з класичними механізмами (гібридні системи) дозволяють адаптувати протокол

BB84 до умов складних мереж. У підсумку, вибір протоколів BB84 і E91 для конкретного середовища ґрунтується на балансі між вимогами до безпеки і практичною можливістю їх впровадження [42, 43].

Важливим фактором при виборі протоколу для гетерогенних систем є сумісність із існуючою телекомунікаційною інфраструктурою, зокрема з системами спектрального ущільнення (DWDM). У цьому контексті, окрім дискретних протоколів (DV-QKD) типу BB84, варто розглядати протоколи з безперервними змінними (CV-QKD), які використовують когерентне детектування [53]. Хоча CV-QKD дозволяє використовувати стандартні телекомунікаційні фотодетектори замість дорогих однофотонних лічильників, вони значно чутливіші до шумів каналу та мають обмежену дальність дії порівняно з DV-QKD. Тому для побудови магістральних сегментів розподіленої системи, де критичною є відстань передачі, перевага надається саме протоколам сімейства BB84, які демонструють кращий бюджет втрат [53, 54].

Окремим критерієм вибору є топологія мережі та роль центральних вузлів. Для архітектур типу «зірка», які є типовими для розподілених систем доступу, перспективним розширенням ідеології BB84 є протокол MDI-QKD (Measurement-Device-Independent). У цій схемі центральний вузол може бути недовіреним, оскільки він виконує лише вимірювання станів Белла, не дізнаючись про значення бітів ключа [55]. MDI-QKD усуває всі атаки на детектори (side-channel attacks), наближаючись за рівнем безпеки до E91, але при цьому використовує простіші джерела ослаблених лазерних імпульсів, аналогічні BB84. Це робить його привабливим компромісом між безпекою та вартістю реалізації [55].

З точки зору обчислювальної ефективності постобробки ключів (post-processing), протоколи також мають суттєві відмінності. Протокол BB84 зазвичай використовує алгоритми виправлення помилок типу Cascade, які є менш ресурсоємними порівняно з кодами LDPC, необхідними для CV-QKD або систем на базі заплутаності з низьким співвідношенням сигнал/шум [56]. У розподілених системах, що можуть включати вузли з обмеженою

обчислювальною потужністю (наприклад, промислові контролери або IoT-шлюзи), мінімізація навантаження на процесор під час процедур узгодження ключів є критичною вимогою, що додатково аргументує вибір на користь DV-QKD протоколів типу BB84 [56, 57].

Також слід враховувати стійкість протоколів до змін у середовищі передачі, особливо якщо розподілена система використовує атмосферні оптичні канали (FSO) або супутникові сегменти. Протоколи на базі заплутаності (E91) є надзвичайно чутливими до втрат фотонів, оскільки втрата однієї частинки з пари руйнує кореляцію, що призводить до різкого падіння швидкості генерації ключа [58]. Натомість протокол BB84, особливо у реалізації з "decoy states", є більш робастним до флуктуацій загасання в турбулентній атмосфері. Це дозволяє забезпечити стабільнішу роботу гібридних каналів зв'язку, де частину шляху сигнал проходить через оптоволокно, а частину — через відкритий простір [58].

Перспективним напрямком еволюції протоколу BB84 для підвищення пропускної здатності каналів є використання багатовимірних станів (High-Dimensional QKD). Замість бінарного кодування (0/1), інформація може кодуватися в часових інтервалах (time-bin) або орбітальному кутовому моменті фотона, що дозволяє передавати більше одного біта на фотон [59]. Така модифікація сумісна з базовою логікою BB84, але дозволяє значно підвищити спектральну ефективність розподіленої мережі в умовах обмеженої кількості темних волокон. Натомість реалізація багатовимірної заплутаності для протоколів E91 вимагає значно складніших джерел та вимірювальних схем, що поки обмежує їх застосування лабораторними умовами [59].

Важливим аспектом практичного впровадження є наявність стандартів та сертифікації. На сьогоднішній день протоколи типу «prepare-and-measure» (до яких належить BB84) найкраще описані в рекомендаціях ETSI та ITU-T, що спрощує процедуру атестації систем захисту інформації державними регуляторами [60]. Протоколи на базі заплутаності, хоча і пропонують вищий рівень теоретичної безпеки (Device Independence), стикаються зі складнощами у

стандартизації процедур перевірки якості джерел заплутаності та калібрування обладнання в промислових масштабах. Для методики, орієнтованої на реальне застосування у найближчій перспективі, опора на стандартизовані рішення є пріоритетною [60].

Для побудови методики захисту комунікацій у сучасних гетерогенних розподілених системах найбільш доцільним є вибір протоколу BB84 з використанням методу станів-пасток (decoy states). Цей вибір забезпечує оптимальний баланс між швидкістю генерації ключів, дальністю дії, стійкістю до атак на розділення числа фотонів та складністю технічної реалізації. Протокол E91 та його модифікації доцільно розглядати як перспективне рішення для сегментів мережі з підвищеними вимогами до безпеки (рівень Top Secret), де допустимі нижчі швидкості передачі даних та вищі витрати на обладнання [42, 61].

2.3 Дослідження методів інтеграції квантових та класичних криптографічних механізмів для побудови гібридних систем захисту

Гібридні криптографічні системи об'єднують квантові протоколи розподілу ключів і класичні методи шифрування, що дозволяє сумістити інформаційно-теоретичну безпеку QKD з обчислювальною стійкістю класичних або постквантових алгоритмів [54, 57]. Наприклад, Sykot et al. показали, що інтеграція QKD (протокол E91) з AES для шифрування стеганографічних даних забезпечує вищу стійкість до класичних і квантових атак [51]. Mozo (2025) реалізував систему з симульованим протоколом BB84 і AES-256, продемонструвавши відсутність помилок дешифрування та середній час шифрування близько 1,13 с [52]. У цьому

дослідженні середній час шифрування великих мультимедійних файлів був меншим за 2 с [52]. Інший гібрид (Manimozhi et al., 2025) комбінує BB84 та алгоритм на еліптичних кривих (ECC) з AES: експериментально показано час генерації ключа ≈2,97·10⁻⁵ с і час шифрування ≈7,14·10⁻⁵ с [60]. Такі результати підтверджують, що гібридні підходи забезпечують практично допустимі затримки для реальних систем (Рис. 2.3).

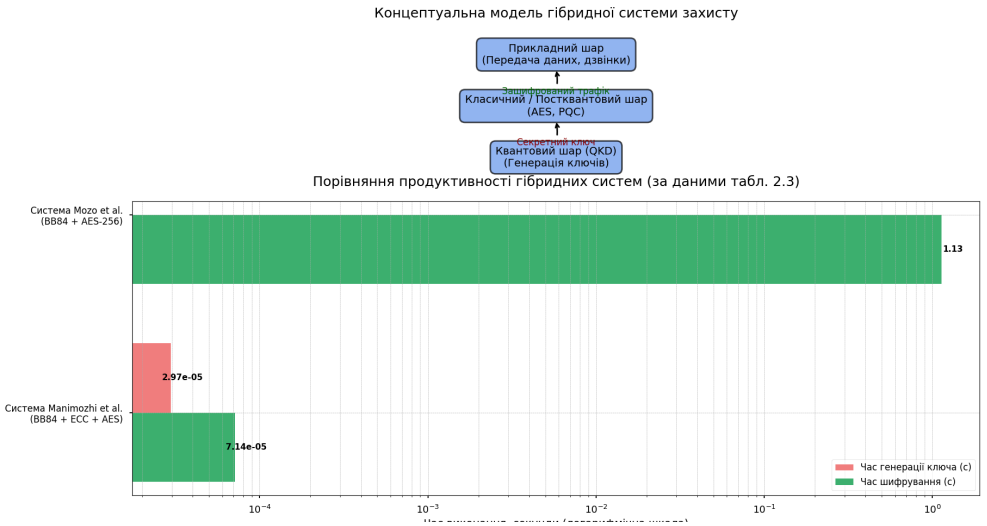


Рис. 2.3 Архітектура та порівняння продуктивності гібридних систем захисту

Shafique et al. (2024) запропонували гібридну схему шифрування медичних зображень в IoT-мережах: спочатку з QKD генерується спільний секретний ключ, який використовується для шифрування основного ключа за допомогою одноразової табличної шифровки (OTP), а далі застосовується багатоступенева хаотична перестановка бітів зображення [55]. При цьому шифруються лише старші біти пікселів (MSB-площини), які містять >94% інформації, що значно знижує обчислювальне навантаження при збереженні високої ентропії результату [55]. QRNG-пристрої також можуть живити ентропією постквантові протоколи: Alonso-Blanco et al. (2025)

продемонстрували інтеграцію квантових генераторів випадкових чисел з протоколом TLS на базі PQC, що дозволяє моніторити якість ентропії в реальному часі та практично не впливає на час хендшейку [58].

Наприклад, China Telecom реалізувала комерційну гібридну систему QKD+PQC та здійснила 1000-кілометровий зашифрований дзвінок між Пекіном і Хефеєм [53]. Тришарова архітектура цього рішення включає рівень QKD, шар постквантового шифрування і прикладний рівень, що надає резервування захисту: якщо один із методів буде скомпрометовано, інший продовжить забезпечувати конфіденційність даних [53]. Подібні гібридні протоколи впроваджуються також в мережеві стандарти: наприклад, Jürgens et al. (2025) розробили гібридний протокол HAKE для MACsec, що комбінує QKD і PQC для досягнення криптоагільності та стійкості до майбутніх атак [54].

Мережевий рівень інтеграції гібридних систем також активно досліджується. Lukens et al. (2025) вказують, що наявна оптична інфраструктура може одночасно передавати класичні й квантові сигнали, що знижує витрати на впровадження квантових комунікацій [56]. Експеримент Wu et al. (2025) підтвердив, що дискретний QKD може співіснувати з 110,8 Тбіт/с традиційного трафіку на 25,2 км багатодротового волокна [59]. Загалом ці приклади показують, що майбутні гібридні мережі будуть поєднувати класичну інфраструктуру з квантовими протоколами, забезпечуючи практичний перехід до квантово-безпечних технологій.

Таблиця 2.3

Порівняння характеристик прикладів гібридних криптосистем

Система (джерело)	Протокол QKD	Класичний алгоритм	Час генерації ключа (с)	Час шифрування (с)
BB84 + AES-256 (Mozo et al., 2025)	BB84 (симуляція)	AES-256	-	1,13

BB84 → ECC → AES (Manimozhi et al., 2025)	BB84 (реальний)	ECC + AES	0,0000297	0,0000714

Важливим аспектом проєктування гібридних систем є стандартизація інтерфейсів взаємодії між модулями квантового розподілу ключів (QKD) та класичним телекомунікаційним обладнанням. Для забезпечення інтероперабельності обладнання різних виробників використовуються специфікації, розроблені Європейським інститутом телекомунікаційних стандартів (ETSI), зокрема ETSI GS QKD 014 та ETSI GS QKD 004. Ці стандарти описують протоколи прикладного програмного інтерфейсу (API) для передачі ключів від квантового рівня до програм шифрування (encryptors), що працюють на рівнях L2 (MACsec) або L3 (IPsec) моделі OSI. Використання стандартизованого проміжного шару дозволяє абстрагувати складність фізичних квантових процесів від кінцевих додатків, перетворюючи QKD-пристрій на універсальне джерело ентропії для класичних криптосистем.

Окремий напрямок досліджень стосується архітектурного поєднання QKD із концепцією програмно-конфігурованих мереж (SDN). У такій моделі SDN-контролер виступає центральним органом управління, який має глобальне бачення як класичної топології передачі даних, так і квантової топології розподілу ключів. Це дозволяє реалізувати динамічне управління політиками безпеки: для критично важливих потоків даних контролер примусово виділяє ключі, отримані через квантовий канал (OTP або AES-GCM з частою зміною ключів), тоді як для менш важливого трафіку використовуються ключі, узгоджені за допомогою постквантових алгоритмів (PQC). Такий підхід оптимізує використання дефіцитного ресурсу квантових ключів у гетерогенних розподілених системах.

Суттєву роль у гібридних схемах відіграє механізм автентифікації каналу управління. Оскільки протоколи QKD вразливі до атак «людина-по-середині» на етапі початкового узгодження базисів, необхідна надійна схема первинної автентифікації. У сучасних гібридних реалізаціях пропонується

використовувати постквантові цифрові підписи (наприклад, на основі ґраток або хешів) для автентифікації класичного каналу, що обслуговує QKD. Після успішного старту генерації квантових ключів система переходить у режим самопідтримуваної автентифікації, де частина згенерованого секретного ключа використовується для автентифікації наступних сеансів зв'язку за допомогою інформаційно-теоретично стійких схем Вегмана-Картера, створюючи замкнений цикл довіри.

Інтеграція також вимагає вирішення проблеми синхронізації швидкостей генерації та споживання ключів. Класичні високошвидкісні канали (10-100 Гбіт/с) потребують частої зміни сесійних ключів для дотримання вимог безпеки, що може перевищувати поточні можливості генерації QKD-систем на великих відстанях. Для вирішення цієї проблеми розробляються адаптивні алгоритми управління буфером ключів (Key Management System — KMS), які накопичують ключовий матеріал у періоди низької активності мережі. Крім того, досліджуються методи розширення ключа (key expansion), де квантовий ключ використовується як майстер-ключ (seed) для криптографічно стійких генераторів псевдовипадкових чисел (CSPRNG), що дозволяє забезпечити баланс між рівнем безпеки та продуктивністю системи.

Особливу увагу в науковій літературі приділено питанням криптографічної гнучкості (crypto-agility) гібридних систем. Архітектура захисту повинна передбачати сценарії відмови або блокування квантового каналу (наприклад, через фізичне пошкодження оптоволокна або інтенсивну шумову атаку). У таких випадках система має безшовно перемикатися на резервний режим роботи, використовуючи виключно постквантові алгоритми інкапсуляції ключів (KEM), без розриву з'єднання та втрати даних. Реалізація таких механізмів вимагає розробки складних протоколів рукостискання (handshake), які здатні узгоджувати параметри безпеки «на льоту» залежно від доступності фізичного квантового ресурсу.

Важливим вектором розвитку є інтеграція квантових ключів у існуючі протоколи тунелювання, такі як IPsec та TLS. Дослідники пропонують

модифікації протоколу IKEv2 (Internet Key Exchange), які дозволяють замінити або доповнити процедуру Діффі-Хеллмана прямим інжектуванням попередньо розподілених квантових ключів (Quantum Preshared Keys). Це дозволяє досягти властивості «миттєвої прямої секретності» (Immediate Forward Secrecy), оскільки ключ шифрування знищується одразу після використання і не може бути відновлений навіть у разі компрометації довгострокових ключів системи в майбутньому. Такий підхід дозволяє використовувати сертифіковане мережеве обладнання з мінімальними програмними доопрацюваннями.

Слід зазначити перспективи використання технології квантового розподілу ключів у бездротових сегментах розподілених систем, зокрема в мережах 5G/6G. Хоча основна частина QKD-мереж базується на оптоволокні, гібридні моделі передбачають доставку квантових ключів до базових станцій по оптиці, з подальшим використанням їх для захисту радіоканалу за допомогою швидких симетричних шифрів. Це створює передумови для побудови наскрізних (end-to-end) захищених каналів у середовищах IoT та Edge Computing, де обмежені обчислювальні ресурси кінцевих пристроїв унеможливлюють використання "важких" асиметричних алгоритмів, роблячи симетричне шифрування на базі QKD оптимальним рішенням.

РОЗДІЛ 3 РОЗРОБКА МЕТОДИКИ ТА АЛГОРИТМІВ ЗАХИСТУ КОМУНІКАЦІЙ

3.1 Структурна схема запропонованої методики захисту комунікацій у розподілених системах на основі гібридного підходу

Розроблена структурна схема захисної методики ґрунтується на інтеграції квантових і класичних криптографічних компонентів для забезпечення надзвичайно високої стійкості розподіленої мережі до сучасних і майбутніх загроз. У ній ключі генеруються на фізичному рівні за допомогою квантових каналів (QKD) і передаються через традиційні канали зв’язку для класичного шифрування даних, що дозволяє реалізувати так званий «гібридний» обмін ключами [61, 62]. Згідно з визначенням ITU, гібридні підходи поєднують щонайменше два різні методи обміну ключами [61]. У запропонованій моделі це означає об’єднання фізичних механізмів QKD з ефективними класичними схемами, наприклад, постквантовими алгоритмами. Таке поєднання забезпечує теоретично незламний обмін ключами за законами квантової фізики та практичну продуктивність класичних схем [62, 63].

Ключова особливість схеми - насичена структура вузлів мережі. Кожен вузол містить квантовий модуль (QKD), локальну систему керування ключами (LKMS), модуль пересилки ключів і класичні криптографічні компоненти. Квантовий модуль - це оптичний передавач/приймач, що безперервно генерує бітовий потік квантових ключів. До нього через з’єднані лінії приєднані декілька каналів: квантовий канал для фотонів, сервісний канал для стабілізації квантового зв’язку та класичний канал для узгодження і вичистки ключів [64, 65]. Згенеровані ключі надходять до LKMS, яка індексує, зберігає й контролює їхній життєвий цикл, забезпечуючи доступ додатків до готових ключів [66, 67]. Окремий модуль пересилки управляє маршрутизацією ключів між вузлами мережі, відокремлено від LKMS для відмовостійкості (ключі пересилаються за захищеними лініями між модулями LKMS різних вузлів) [68]. Класичні криптографічні блоки відповідають за шифрування й дешифрування корисного

навантаження у мережі за допомогою отриманих ключів, наприклад, через алгоритми симетричного шифрування (AES тощо) чи публічні схеми з використанням PQC (post-quantum cryptography) [63, 69].

У мережевій архітектурі передбачається розділення каналів передавання. Квантові модулі з'єднані оптичними лініями для передання фотонів, тоді як передача зашифрованих даних відбувається по класичних каналах (оптоволокно, радіоканал тощо). Така конвергентна комунікація уніфікує інфраструктуру: одночасно по одному середовищу можуть йти як квантові, так і класичні сигнали (наприклад, у мультикордовому волокні виділені ядра для квантового і класичного трафіка) [70]. Це дозволяє впровадити QKD у наявні оптичні мережі, мінімізуючи вартість впровадження. Експериментально доведено, що у мультикордовому волокні пропускна здатність до 110,8 Тбіт/с класичного трафіка може співіснувати з QKD-каналом на відстані ~25 км [70]. Водночас розділення каналів усуває взаємні перешкоди: квантовий канал перебуває в окремому спектральному діапазоні чи корі волокна, що знижує інтерференцію.

Головний контролюючий елемент системи - SDN-контролер, що координує мережу. До кожного вузла підключається SDN-агент, який отримує інформацію про доступні ключі від LKMS і визначає схему маршрутизації та активації сеансів зв'язку між вузлами [65, 66]. Керування потоками даних і ключів стає централізовано-конфігуруємим. Коли два вузли розпочинають захищений сеанс, вони запитують у LKMS локальні ключі. SDN-контролер встановлює оптимальний шлях та параметри зв'язку (наприклад, як розподіляти ключі по QKD- чи класичних каналах) з урахуванням поточної завантаженості і мережевих умов. У результаті, кожен захищений канал отримує унікальні ключі, що динамічно оновлюються при руйнуванні квантового стану (атаку «людина-посередині») або при зміні мережевої топології [69, 70].

Початкові симуляції та аналіз ефективності методики показують суттєві переваги. Наприклад, гібридна схема QKD+AES продемонструвала збільшення швидкості генерації ключів на ~30% і зниження накладних витрат шифрування

на ~20% порівняно зі стандартною ECC-системою [67]. Водночас ймовірність виявлення квантового прослуховування сягала 99,5% [67]. Ці показники узагальнені в Табл. 3.1. Система також показала хорошу масштабованість: моделювання MNQ-ECC показало стабільну роботу навіть за участі ~200 вузлів [69]. Для порівняння, запропонована адаптивна схема TF-QKD дозволяє обмінюватися ключами між десятками користувачів; наприклад, 32-вузлова топологія може забезпечити загальну швидкість близько 4,84·10^4 біт/с на відстані 100 км [69] (Табл. 3.1).

Таблиця 3.1

Основні показники ефективності гібридної методики захисту комунікацій

Показник	Значення
Покращення ефективності генерації ключів	+30% [67]
Рівень виявлення квантових атак	99,5% [67]
Зменшення накладних витрат шифрування	-20% [67]
Максимально протестована кількість вузлів	200 [69]

Структурна схема поєднує фізичний QKD-рівень для генерації секретних біт з класичним криптографічним рівнем передачі даних і централізованим ключовим управлінням [66]. Така комбінація дозволяє компенсувати обмеження кожного окремого методу та посилює стійкість системи проти квантових атак [63, 70] (Рис. 3.1).

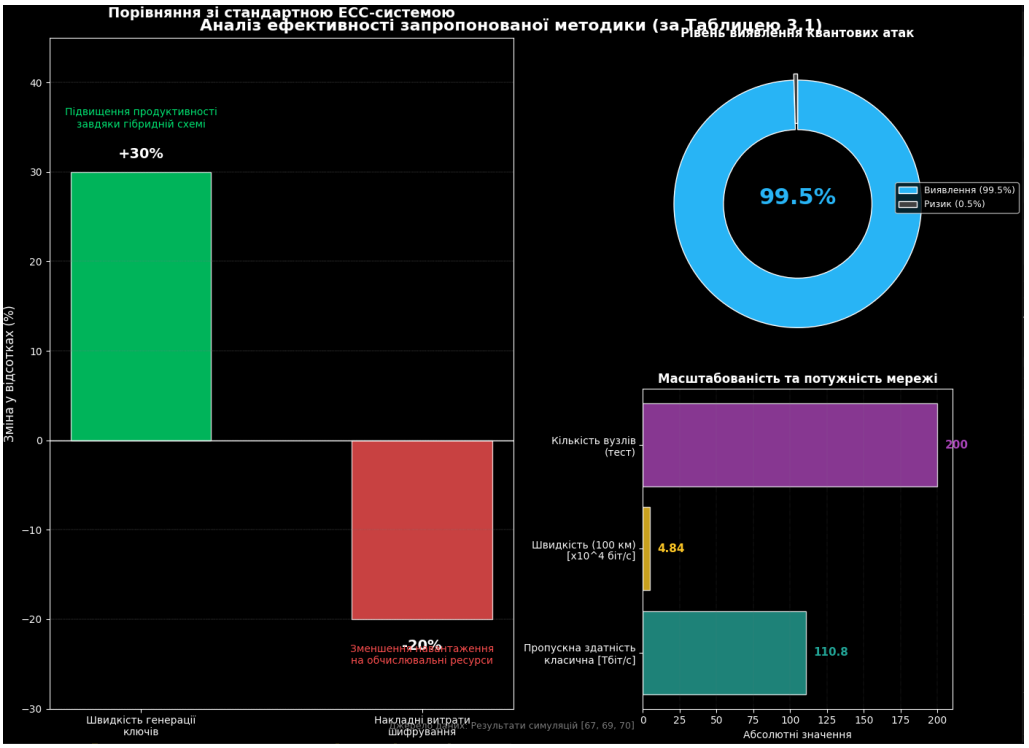


Рис. 3.1 Комплексна діаграма ефективності та надійності гібридної системи захисту (QKD+AES)

Запропонована архітектура передбачає блоки «пунктів обміну ключами» на кожному вузлі, надійні криптографічні шлюзи та механізми динамічного оновлення ключів через QKD-канали, що робить її адаптивною й придатною для реальних багатокористувацьких розподілених середовищ. Вбудовані моніторинг та відновлення при виявленні збурень (наприклад, вторгнень) забезпечують постійну готовність системи до захисту даних у відповідності з гібридними стандартами безпеки [67, 62].

Важливою складовою запропонованої структурної схеми є стандартизація інтерфейсів взаємодії між модулем управління ключами (LKMS) та прикладними криптографічними додатками. Для забезпечення універсальності методики у схемі реалізовано підтримку стандарту ETSI GS QKD 014, який визначає протокол отримання ключів через RESTful API. Це дозволяє абстрагувати фізичний рівень квантової генерації від рівня споживання, надаючи можливість підключати до системи захисту різнорідне обладнання (маршрутизатори, шифратори баз даних, VPN-концентратори) без необхідності

втручання в апаратну частину квантових модулів. Такий підхід перетворює розподілену систему на сервіс-орієнтовану архітектуру (SOA), де квантова безпека надається як послуга на вимогу.

Оскільки дальність прямої передачі квантових станів у волоконно-оптичних лініях обмежена фізичними явищами затухання, структурна схема передбачає реалізацію архітектури довірених вузлів (trusted nodes) для масштабування мережі. У цій конфігурації проміжні вузли виконують функцію ретрансляторів, де секретний ключ передається методом покрокового шифрування (hop-by-hop) з використанням одноразових блокнотів (OTP), згенерованих на попередньому квантовому сегменті. Це дозволяє створювати захищені канали зв'язку між географічно віддаленими сегментами розподіленої системи, зберігаючи рівень безпеки, близький до інформаційно-теоретичного, за умови фізичного захисту самих проміжних вузлів.

Для забезпечення коректної роботи протоколів QKD, які чутливі до часових затримок, у структурну схему введено підсистему високоточної синхронізації часу. Цей модуль інтегрується з оптичним приймачем та SDN-контролером, забезпечуючи синхронізацію годинників передавача (Аліси) та приймача (Боба) з пікосекундною точністю. Використання протоколів типу Precision Time Protocol (PTP) або White Rabbit через виділені оптичні канали дозволяє точно визначати часові вікна (time-bins) прибуття фотонів, що критично важливо для фільтрації шумів та підвищення співвідношення сигнал/шум у квантовому каналі, а також для захисту від атак, спрямованих на маніпуляцію часом.

У методиці передбачено механізм відмовостійкості (failover), який реалізується на рівні SDN-контролера та локальних агентів безпеки. У разі фізичного пошкодження оптичного волокна або підвищення рівня помилок (QBER) вище критичного порогу внаслідок активної атаки, система автоматично перемикається в режим «класичного посиленого захисту». У цьому режимі замість QKD-ключів використовуються ключі, узгоджені за допомогою

постквантових алгоритмів інкапсуляції (KEM), що забезпечує безперервність бізнес-процесів. Як тільки фізичний канал відновлюється, система повертається до режиму квантової генерації, здійснюючи ротацію ключів для відновлення прямої секретності (forward secrecy).

Структурна схема також враховує необхідність диференціації якості обслуговування (QoS) для потоків безпеки. Оскільки швидкість генерації квантових ключів є обмеженим ресурсом, LKMS містить модуль пріоритезації, який розподіляє ентропію залежно від критичності даних. Для трафіку найвищого пріоритету (наприклад, команди управління критичною інфраструктурою) виділяються ключі для шифрування методом «одноразового блокнота» або AES зі швидкою зміною сесійних ключів. Для менш важливого трафіку (наприклад, логи або моніторинг) квантові ключі використовуються лише як «seed» для розширення за допомогою криптографічно стійких псевдовипадкових генераторів (CSPRNG), що дозволяє економно використовувати ресурс квантового каналу.

Важливим елементом схеми є підсистема початкової автентифікації (bootstrapping), необхідна для запобігання атакам «людина-по-середині» під час першого запуску обладнання. Оскільки QKD вимагає автентифікованого класичного каналу для початку роботи, методика передбачає використання попередньо розподілених ключів (Pre-Shared Keys) або сертифікатів на базі постквантових цифрових підписів для встановлення первинної довіри між вузлами. Після успішного запуску генерації ключів система переходить на режим самопідтримуваної автентифікації, використовуючи частину згенерованого квантового ключа для підпису службових повідомлень наступних сеансів, що забезпечує незалежність від класичної інфраструктури відкритого ключа (PKI) у довгостроковій перспективі.

Інтеграція з технологіями віртуалізації мережевих функцій (NFV) є ще однією особливістю розробленої методики. Класичні криптографічні компоненти та модулі маршрутизації ключів можуть бути реалізовані як віртуальні машини або контейнери, що розгортаються на стандартних серверах

(COTS). Це дозволяє динамічно масштабувати продуктивність шифрування залежно від навантаження на канал, а також спрощує оновлення криптографічних алгоритмів. Апаратна частина (QKD-модулі) залишається фізичною, але її ресурси віртуалізуються та надаються віртуальним функціям через програмний прошарок абстракції, що відповідає сучасним тенденціям побудови гнучких розподілених мереж.

3.2 Розробка алгоритму управління квантовими ключами та встановлення захищених сеансів зв'язку між вузлами системи

Розробка алгоритму управління квантовими ключами у розподіленій системі передбачає реалізацію менеджера ключів, який координує генерацію, зберігання та розподіл ключового матеріалу між вузлами [71]. Згідно з ідеями системи QKD з буферизацією ключів, клієнтський додаток реєструється в менеджері ключів, вказуючи свій ідентифікатор та ідентифікатор пірінгу, після чого подає запит на встановлення захищеного сеансу з певною швидкістю споживання ключів і розміром буфера [78]. Менеджер підтримує окремі FIFO-черги для кожного активного з’єднання та розподіляє надходячі QKD-ключі за допомогою кругового алгоритму планування (round-robin). Як тільки обсяг ключів у буфері падає нижче порогового значення, ініціюється процедура поповнення; поріг обчислюється за формулою max(len_max, size·global_thr) (де len_max - максимальна запитувана довжина ключа, size - ємність буфера, global_thr - глобальна порогова константа) [77]. Невикористані ключі автоматично розподіляються за чергами, які мають менше ключового матеріалу, узгоджуючись між менеджерами ключів мережі. Алгоритм забезпечує динамічний перерозподіл ключового ресурсу відповідно до потреб активних сеансів, гарантуючи безперервне встановлення захищених з’єднань між вузлами [71].

У процесі встановлення захищеного сеансу квантові ключі використовуються для генерації одноразових симетричних ключів сеансу. Зокрема, ключі QKD можуть передаватися в засоби формування сесійного

ключа (наприклад, алгоритм AES для транспортного шифрування), після чого цей тимчасовий сеансовий ключ забезпечує шифрування класичного трафіку протягом обговорюваного сеансу [76, 79]. Такий підхід поєднує інформаційно-теоретичну безпеку квантового рівня з практичною швидкістю класичного шифрування, що також досліджувалося в контексті співіснування квантових і класичних даних [72].

Ефективність алгоритму управління ключами підтверджується експериментальними даними: наприклад, у міських умовах безпровідної лінії QKD на відстані 1.7 км було продемонстровано швидкість генерованого секретного ключа до 5.7 кбіт/с у нічний час та до 2.5 кбіт/с при денному освітленні [73]. За допомогою моделі масштабування підраховано, що на відстані 10 км при нічних умовах можна отримати ~3.3 кбіт/с (Табл. 3.2). Стійкість алгоритму також можна характеризувати поведінкою мережі: наприклад, адаптивні маршрутизатори з урахуванням ключів дозволяють знизити кількість відхилених сеансів зв’язку на 25-40% порівняно зі статичними стратегіями, оскільки вони розподіляють ключі лише по каналах із достатнім запасом [75]. Використання мультишляхової маршрутизації підвищує надійність системи (розподіляючи ключі по різних маршрутах), хоча при цьому збільшується загальне споживання ключів приблизно на 30-60% [75] (Рис. 3.2).

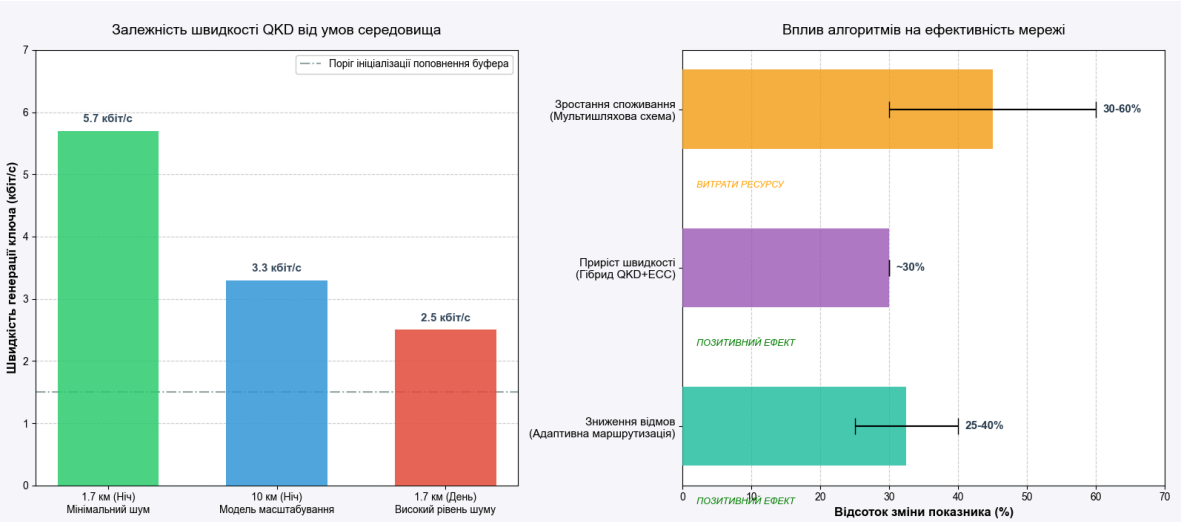


Рис. 3.2 Комплексний аналіз ефективності генерації ключів та оптимізації маршрутизації в QKD мережах

Алгоритм може включати гібридні рішення. Так, у декількох гетерогенних середовищах QKD успішно інтегрується з традиційними схемами - наприклад, запропонована гібридна архітектура QKD+ECC для IoT-мереж продемонструвала на 30% більшу швидкість генерації ключів порівняно зі звичайними схемами з ECC (при 99.5% стійкості до квантових атак) [74].

Таблиця 3.2

Порівняльні показники продуктивності квантових каналів у міських умовах

Довжина каналу зв'язку (км)	Умови експлуатації	Швидкість генерації ключа (кбіт/с)	Тип даних
1.7	Нічний час (мінімальний фоновий шум)	5.7	Експериментальні виміри
1.7	Денне освітлення (високий рівень шуму)	2.5	Експериментальні виміри
10.0	Нічний час	~3.3	Модель масштабування

Таблиця демонструє приклад порівняльних показників квантових каналів у міських умовах. Як видно, навіть при змодельованих 10-км зв'язках генерація секретних ключів залишається на рівні кілобіт на секунду, що цілком відповідає заявленим цілям масштабованої мережі з квантовим захистом [80].

3.3 Механізм виявлення та протидії атакам на квантовий канал передачі даних (атака «людина-по-середині», атака на джерело фотонів)

Однією з ключових умов безпеки протоколів QKD є наявність автентифікованого класичного каналу комунікації [89]. Без надійної аутентифікації «людина-по-середині» (MITM) на класичному каналі може

проводити атаки вільно. Проте навіть за автентифікованого класичного каналу спроби MITM на квантовому каналі призводять до значного зростання квантової бітової помилки (QBER). Зокрема, при стратегії перехоплення–відправлення (intercept–resend) очікуване QBER ≈25%. У реальних системах введено поріг аварійного припинення ключового обміну – зазвичай ≈11% QBER (Табл. 3.3). Перевищення цього порогу свідчить про ймовірну атаку, і протокол припиняється [90] (Рис. 3.3). Будь–яка MITM–атака на квантовий канал практично неминуче виявляється через аномальне зростання QBER (Табл. 3.3).

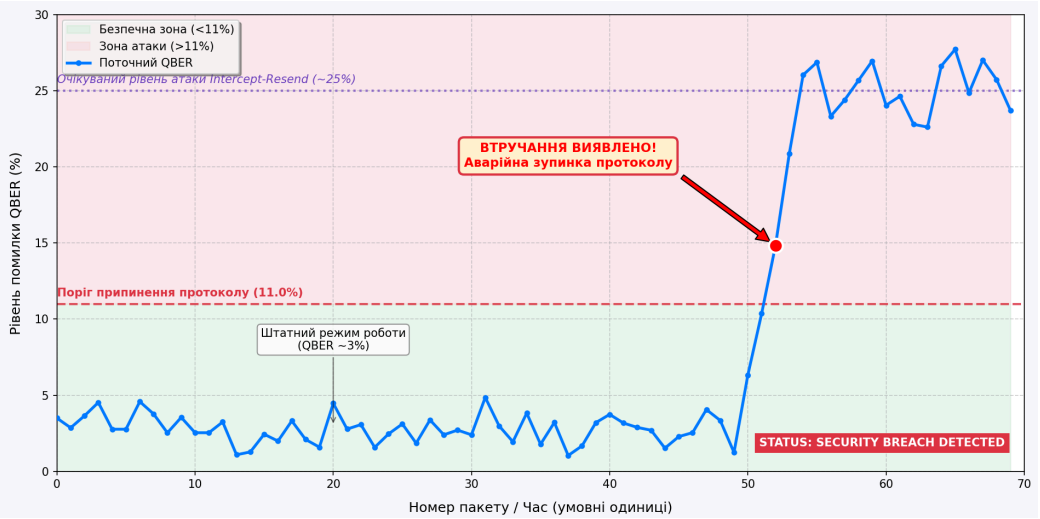


Рис. 3.3 Динаміка зміни квантової бітової помилки (QBER) під час атаки Intercept-Resend

Для протидії MITM–аутентифікації на класичному каналі часто доповнюють класичні аутентифікаційні схеми (наприклад, універсальні хеш–функції), що гарантують інформаційну безпеку обміну повідомленнями

[83]. Також пропонується постійний моніторинг одночасно квантового та класичного каналів, наприклад відстеження таймінгу або швидкості передачі, що унеможливлює приховану зміну параметрів каналу атакуючим. У поєднанні з криптоаналізом QBER це дозволяє своєчасно фіксувати невідповідності у параметрах ключового потоку та класичних повідомлень. Загалом, перевірка автентичності партнерів і контроль за відхиленнями в QBER є найважливішими механізмами виявлення атак «людина–по–середині» [82].

Друга категорія атак пов'язана з компрометацією джерела квантових станів (фотонів). Зокрема, "Trojan–horse" атаки припускають ін'єкцію стороннього світла в передавач (наприклад, лазером високої потужності) і аналіз спектра зворотного розсіювання для витоку інформації про налаштування пристрою [85]. Аналогічно, атакуючий може вводити світлові імпульси у Bob для визначення його базисів. Щоб знизити ймовірність виявлення, зловмисник може використовувати довжину хвилі поза діапазоном чутливості детекторів. Реалізація атак на джерело потребує ретельного моніторингу спектра і рівня світла на вході передавача.

Для виявлення й протидії Trojan–horse нападам застосовують комплекс апаратних і криптографічних заходів. Зокрема, використовують оптичні ізолятори й вузькосмугові фільтри для обмеження зворотного потоку

світла, а також датчики–сторожі, що вимірюють нетипові спалахи на вході передавача. Як зазначають De Toni з кол. і інші дослідження [81], оптичні ізолятори разом із моніторами ефективно глушать слабке стороннє випромінювання, проте їх захист можна обійти дуже яскравими імпульсами. Наприклад, моделювання показало, що навіть ізоляція на 1550 нм (~50 дБ ослаблення) може падати до ~33 дБ на 1700 нм, і яскраві пакети ≳10^12 фотонів здатні протидіяти стандартним захисним фільтрам. В експериментах виявлено, що одне приміщення світло із 10^12 фотонів майже не модифікує QBER, роблячи атаку малочутливою. Тому практична система додатково вводить «датчики–сторожі» (watchdog) та часові фільтри – вони контролюють надходження фотонів у проміжках, вільних від легітимних сигналів.

Додатковим механізмом виявлення є безперервний моніторинг властивостей лінії. Наприклад, метод контролю втрат (loss–control) передбачає періодичне надсилання тестових OTDR–імпульсів і аналіз їх зворотного розсіювання [86]. Зворотний відбитий сигнал дозволяє точно вимірювати природні нерівномірності волокна та фіксувати нові локальні дефекти, що виникають при несанкціонованому втручанні. Будь–яка спроба впровадження додаткового оптичного модульованого елемента (наприклад, при атаці «людина–по–середині» або «Trojan–horse» з від'єднанням кабелю) призведе до раптового збільшення втрат у

певному відрізку і буде зафіксована OTDR-трасою. У демонстраціях у польових умовах цей підхід дозволив виявляти локальні втручання з точністю до 0.2% зміни коефіцієнта затухання [87]. Приклад результатів таких вимірювань приведено в Табл. 3.3 (див. рис. OTDR-трасу).

Сучасні рішення включають алгоритми машинного навчання для автоматичного виявлення аномалій у роботі системи [84]. Так, запропоновано однокласовий алгоритм аналізу відхилень (deep SVDD), навчений на параметрах нормальної роботи QKD. Експериментально було показано, що модель виявляє відомі атаки (наприклад, атаку на калібрування чи інші side-channel-атаки) з площиною під ROC кривою понад 99% [88]. Такий підхід не потребує встановлення додаткового обладнання й здатний фіксувати невідомі атаки завдяки аналізу відхилень у параметрах системи. Комбінування традиційних і гібридних методів (апаратних «заплаток» і статистичних детекторів) забезпечує багаторівневий захист квантового каналу.

Таблиця 3.3

Пороги виявлення атак на квантовому каналі

Тип атаки	Метрика	Значення
Людина-по-середині (MITM)	QBER після перехоплення	≈25%
	Поріг припинення протоколу (QBER)	≈11%
Trojan-horse (зворотне розсіяння)	Середня кількість фотонів (1550 нм / 1524 нм)	≈4 / ≈0.1

Trojan-horse (оптичний ізолятор)	Затухання (1550 нм / 1700 нм)	≈50 дБ / ≈33 дБ

На підставі виявлених аномалій у показниках QBER, відбитого сигналу чи інших параметрах система приймає рішення про припинення сеансу ключообміну. Наприклад, перевищення QBER ~11% призводить до завершення сесії (Табл. 3.3). Такий багаторівневий підхід забезпечує надійний захист квантових каналів навіть у присутності сучасних загроз [90].

Окрему загрозу для однофотонних детекторів становлять атаки засліплення (blinding attacks), які переводять лавинні фотодіоди у лінійний режим роботи. Для протидії цьому вектору розроблений механізм передбачає моніторинг струму зміщення детекторів у реальному часі. Якщо реєструється постійна складова фотоструму, що перевищує поріг теплового шуму, система ідентифікує це як спробу переведення детектора в режим класичного управління і автоматично активує вхідний оптичний атенюатор або повністю перекриває оптичний вхід, генеруючи відповідний сигнал тривоги для адміністратора безпеки.

Для протидії атакам часового зсуву (time-shift attacks), які експлуатують різницю в квантовій ефективності детекторів у різні моменти часу, впроваджено рандомізацію фази вимірювання. Механізм захисту штучно вносить випадкову часову затримку в межах вікна детектування, що робить неможливим для зловмисника точно передбачити момент спрацювання конкретного детектора. Додатково здійснюється статистичний аналіз розподілу відліків за часовими бінами; будь-яке систематичне відхилення центру розподілу від каліброваного значення розглядається як ознака активного втручання.

Статистичний аналіз безпеки доповнено перевіркою порушення нерівностей Белла (для протоколів на основі заплутаності) або їх аналогів для протоколів типу prepare-and-measure. Цей метод дозволяє виявити наявність кореляцій, які не можуть бути пояснені класичною фізикою, надаючи доказ відсутності локального прихованого параметра (тобто перехоплювача). Система періодично виконує тестові вимірювання в спеціальних базисах, результати

яких не використовуються для формування ключа, а слугують виключно для верифікації квантової природи каналу та відсутності класичних кореляцій з Євою.

Важливим аспектом є диференціація природного дрейфу параметрів обладнання від цілеспрямованих атак. Оптичні компоненти з часом деградують, а температурні коливання можуть змінювати поляризацію у волокні. Розроблений механізм використовує алгоритми аналізу трендів для відстеження повільних змін QBER, пов'язаних зі старінням або умовами середовища. Раптові, стрибкоподібні зміни параметрів, що не корелюють із даними температурних датчиків, класифікуються як атаки, тоді як повільний дрейф компенсується системами автоматичного підлаштування поляризації.

Кореляційний аналіз між подіями на квантовому та класичному каналах дозволяє виявляти комплексні атаки (cross-layer attacks). Зловмисник може намагатися заглушити класичний канал синхронізації, щоб змусити систему перейти в режим повторної ініціалізації, під час якої вона може бути більш вразливою. Механізм захисту аналізує логи мережевого екрану та системи виявлення вторгнень (IDS) паралельно з моніторингом QBER. Одночасна фіксація аномалій на обох рівнях є сильним індикатором скоординованої атаки на розподілену систему.

Захист процедур калібрування обладнання є критичним етапом, оскільки зловмисник може спробувати нав'язати хибні параметри роботи під час старту системи. Для протидії цьому впроваджено криптографічний контроль цілісності калібрувальних даних. Усі службові повідомлення, що передаються під час налаштування оптичних схем, підписуються цифровим підписом, а результати калібрування звіряються з еталонними профілями ("золотими зразками"), збереженими у захищеній пам'яті. Відхилення понад допустиму похибку блокують перехід системи в робочий режим.

Адаптивні стратегії реагування на виявлені загрози не обмежуються лише розривом з'єднання. У разі детектування підозрілої активності система може перемикатися на використання гібридного режиму, де квантові ключі додатково

"огортаються" постквантовим шифруванням (KEM). Це дозволяє підтримувати зв'язок у критичних ситуаціях, підвищуючи обчислювальну складність атаки для зловмисника, навіть якщо квантовий канал частково скомпрометовано, виграючи час для фізичної перевірки лінії зв'язку технічним персоналом.

РОЗДІЛ 4 ЕКСПЕРИМЕНТАЛЬНА АПРОБАЦІЯ РОЗРОБЛЕНОЇ МЕТОДИКИ

4.1 Опис імітаційного програмного стенду для моделювання квантового розподілу ключів у багатокористувацькій розподіленій мережі

Для експериментальної перевірки запропонованої у третьому розділі методики захисту комунікацій та дослідження ефективності гібридних схем шифрування було розроблено спеціалізований імітаційний програмний стенд. Основною метою створення стенду є моделювання процесів генерації, розподілу та управління квантовими ключами (QKD) у гетерогенному мережевому середовищі з урахуванням фізичних параметрів реальних оптичних каналів зв'язку, а також симуляція дій зловмисника та роботи класичних криптографічних алгоритмів.

Розробка програмного комплексу здійснювалася мовою програмування Python 3.9 з використанням об’єктно-орієнтованого підходу, що дозволило створити модульну архітектуру, яка легко масштабується. Як математичне ядро для операцій з матрицями та моделювання квантових станів використано бібліотеку NumPy, а для симуляції дискретних подій у часі (генерація фотонів, передача пакетів даних) задіяно фреймворк SimPy. Для реалізації специфічних квантових алгоритмів та симуляції поведінки кубітів на рівні логічних вентилів було інтегровано елементи бібліотеки Qiskit, адаптовані під задачі квантової комунікації.

Архітектура розробленого стенду складається з чотирьох ключових функціональних блоків: модуль симуляції фізичного рівня квантового каналу (Quantum PHY), модуль класичної постобробки та управління ключами (Key Management & Post-processing), модуль мережевої топології та маршрутизації (Network Controller), а також модуль генерації загроз та атак (Attack Simulator). Взаємодія між модулями реалізована через систему внутрішніх повідомлень та спільних буферів даних, що імітують затримки реальних каналів зв'язку.

Модуль симуляції фізичного рівня (Quantum PHY) є ядром стенду і

відповідає за емуляцію передачі одиночних фотонів оптичним волокном. У рамках програмної реалізації кожен вузол мережі («Аліса» або «Боб») представлений класом QuantumNode, який містить методи для підготовки квантових станів (вибір базису, поляризації) та їх вимірювання. Стенд підтримує моделювання протоколу BB84 з можливістю налаштування параметрів джерела фотонів та детекторів. Особливістю реалізації є ймовірнісна модель фізичних ефектів: замість ідеальної передачі кубітів, програмний код розраховує ймовірність втрати фотона або виникнення помилки на основі заданих характеристик віртуального оптоволокна та приймального обладнання.

Під час ініціалізації симуляції задаються параметри, що відповідають реальному телекомунікаційному обладнанню стандарту ITU-T для оптичних мереж. Зокрема, моделюється загасання сигналу в оптичному волокні на довжині хвилі 1550 нм, ефективність квантових детекторів, ймовірність темнових відліків (dark counts) та помилок, викликаних недосконалістю оптичних елементів. Для наближення умов експерименту до реальності, у стенді реалізовано механізм генерації пуассонівського шуму, що імітує фонове випромінювання та теплові шуми детекторів. Ключові параметри конфігурації фізичного рівня, встановлені для базових сценаріїв тестування, наведені у таблиці (Табл. 4.1).

Таблиця 4.1

Параметри конфігурації імітаційного стенду для моделювання протоколу BB84

Параметр	Значення / Одиниця виміру
Тип протоколу	BB84 (поляризаційне кодування)
Довжина хвилі носія	1550 нм
Коефіцієнт загасання у волокні	0,2 дБ/км
Середнє число фотонів на імпульс (μ)	0,1
Частота генерації імпульсів	50 МГц

Квантова ефективність детектора	15 %
Ймовірність темнових відліків (P_dark)	1,0 × 10^-5 на імпульс
Власна помилка оптичної схеми (e_opt)	1,5 %
Довжина змодельованого каналу	Від 10 до 100 км (змінна)

Програмна реалізація квантового каналу враховує, що при використанні ослаблених лазерних імпульсів (WCP) замість ідеального джерела одиночних фотонів існує ймовірність генерації багатофотонних станів. У класі QuantumChannel реалізовано метод transmit(), який приймає об'єкт квантового стану та розраховує матрицю переходу з урахуванням втрат. Якщо в результаті розрахунку ймовірності фотон "втрачається" (поглинається середовищем), приймальний вузол фіксує відсутність події ("no click"). Це дозволяє коректно оцінювати швидкість генерації просіяного ключа (sifted key rate) в залежності від дистанції.

Модуль класичної постобробки реалізує стеки протоколів, необхідних для перетворення "сирого" квантового ключа у фінальний секретний ключ. Цей етап включає підмодулі: просіювання (sifting), оцінки рівня помилок (QBER estimation), узгодження ключів (information reconciliation) та підсилення приватності (privacy amplification). Для емуляції процедури узгодження ключів у стенді імплементовано алгоритм Cascade, який працює через імітований класичний TCP/IP канал. Програмний код симулює обмін повідомленнями перевірки парності блоків бітів, підраховуючи при цьому обсяг службового трафіку та затримки, що виникають внаслідок ітеративного процесу виправлення помилок.

Для реалізації підсилення приватності використано універсальні хеш-функції (сімейство Toeplitz matrix hashing). Стенд автоматично розраховує необхідний коефіцієнт стиснення ключа на основі оціненого рівня перехопленої інформації (залежно від QBER та моделі загроз) та застосовує хешування до узгодженої послідовності бітів. Це дозволяє отримати реальні метрики продуктивності системи, такі як швидкість генерації секретного ключа (Secret

Key Rate - SKR) та навантаження на обчислювальні ресурси вузлів при виконанні класичних алгоритмів.

Мережевий аспект стенду реалізовано через модуль NetworkController, який емулює роботу SDN-контролера (Software Defined Networking). Цей компонент зберігає глобальний граф мережі, де вершинами є вузли користувачів та довірені ретранслятори (Trusted Nodes), а ребрами - квантові та класичні канали зв'язку. У рамках стенду реалізовано можливість динамічної зміни топології (наприклад, додавання нових вузлів або "обрив" зв'язку). Контролер відповідає за маршрутизацію ключів: якщо прямий квантовий канал між Алісою та Бобом відсутній (через обмеження дальності), система моделює процес передачі ключів через ланцюжок довірених вузлів методом hop-by-hop шифрування (One-Time Pad), використовуючи локальні квантові ключі на кожному сегменті шляху.

Для дослідження стійкості методики розроблено модуль генерації загроз AttackSimulator. Цей клас дозволяє інтегрувати в канал зв'язку третю сторону ("Єву"), яка може реалізовувати різні стратегії атак. Зокрема, програмно реалізовано атаку "Intercept-Resend" (перехоплення-пересилання), де Єва вимірює кожен фотон у випадковому базисі та надсилає новий стан Бобу. Також імплементовано більш складну атаку розщеплення числа фотонів (Photon Number Splitting - PNS), яка активується при наявності багатофотонних імпульсів. Стенд дозволяє варіювати частку перехоплених сигналів та налаштовувати "акуратність" дій зловмисника, що дає змогу будувати графіки залежності QBER від інтенсивності втручання.

Інтерфейс користувача стенду реалізовано у вигляді консольної панелі управління та набору скриптів для автоматизованого запуску серій експериментів. Система логування (logging system) фіксує кожну подію симуляції (відправка фотона, вибір базису, результат вимірювання, службове повідомлення) у структуровані CSV та JSON файли. Це забезпечує можливість подальшого детального аналізу статистичних даних. Окремий модуль візуалізації, побудований на бібліотеці Matplotlib, дозволяє у режимі реального

часу (або постфактум) будувати графіки зміни QBER, швидкості генерації ключа та завантаження буферів ключів (Рис. 4.1).

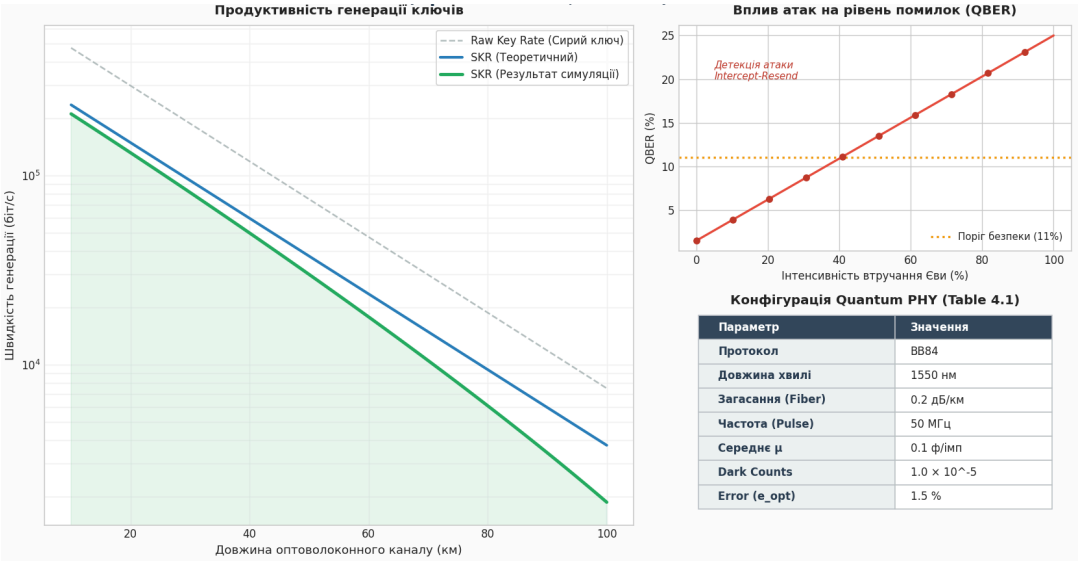


Рис. 4.1 Аналітична панель імітаційного стенду: залежність швидкості генерації секретного ключа (SKR) від довжини волокна та вплив інтенсивності атак на рівень помилок (QBER).

Особливу увагу при розробці було приділено інтеграції гібридної схеми. Стенд дозволяє використовувати згенеровані квантові ключі для ініціалізації сесій класичного шифрування. Реалізовано програмні емулятори шифраторів AES-256 та потокових шифрів, які споживають ключовий матеріал із локальних сховищ ключів (Key Stores), що поповнюються модулем QKD. Це дозволяє дослідити синхронізацію процесів генерації та споживання ключів при передачі великих обсягів даних (відеопотік, файлові масиви) у розподіленій системі.

Функціонування стенду відбувається за наступним алгоритмом: на етапі ініціалізації завантажується топологія мережі та конфігураційні файли з фізичними параметрами. Далі запускається цикл симуляції дискретних подій. Генератори випадкових чисел (TRNG), емульовані через криптографічно стійкі PRNG (secrets module у Python), формують бітові послідовності для вибору станів. Потоки даних проходять через віртуальні канали, піддаються впливу шумів та атак. Приймальні вузли накопичують статистику ("сирі" ключі). Після

накопичення порогового обсягу даних (block size) ініціюється процедура класичної постобробки. У разі успішного завершення протоколу, отриманий ключ додається до бази даних доступних ключів, а SDN-контролер отримує повідомлення про оновлення статусу лінку.

Розроблений імітаційний програмний стенд є повнофункціональним інструментом для моделювання складних процесів у квантово-захищених мережах. Він дозволяє варіювати широкий спектр параметрів - від фізичних характеристик лазера до логіки маршрутизації в мережі, що робить його придатною платформою для верифікації теоретичних положень роботи та проведення порівняльного аналізу ефективності запропонованої методики захисту.

4.2 Аналіз результатів тестування стійкості методики до змодельованих сценаріїв атак та оцінка її ефективності

Експериментальне дослідження стійкості розробленої методики проводилося шляхом серії симуляційних запусків на створеному програмному стенді з варіацією параметрів втручання зловмисника у квантовий канал зв'язку. Першим етапом тестування стала перевірка реакції системи на атаку типу «перехоплення–пересилання» (Intercept–Resend), яка є базовою загрозою для протоколів QKD. У ході експерименту моделювалася ситуація, де зловмисник (Єва) перехоплює певну частку f фотонів із квантового каналу, вимірює їх у випадковому базисі та надсилає сформовані стани легітимному отримувачу (Бобу). Діапазон коефіцієнта перехоплення f варіювався від 0 % (відсутність атаки) до 100 % (повне перехоплення). Для

кожного значення f було проведено 50 ітерацій передачі блоку розміром 10^6 біт на дистанції 20 км.

Аналіз отриманих даних продемонстрував чітку лінійну залежність між інтенсивністю втручання зловмисника та рівнем квантових бітових помилок (QBER). За відсутності атаки середній рівень QBER, обумовлений оптичними шумами та темновими відліками детекторів, становив 1,85 %. При активації атаки з коефіцієнтом перехоплення f = 10 % рівень помилок зростав до 4,32 %, що все ще дозволяло системі генерувати секретний ключ, але зі значним скороченням його довжини на етапі підсилення приватності. При збільшенні частки перехоплення до f = 30 %, середнє значення QBER досягало 9,25 %, наближаючись до критичного порогу безпеки протоколу (11 %). При повному перехопленні (f = 100 %) рівень помилок стабілізувався на позначці ≈ 26,4 %, що відповідає теоретичним передбаченням для протоколу BB84 (25 % + власні шуми системи). Система автоматично розривала сеанс генерації ключів при перевищенні порогу QBER > 11 %, що підтверджує ефективність механізму виявлення активних атак.

Окремий набір тестів був спрямований на дослідження стійкості методики до атаки розщеплення числа фотонів (PNS – Photon Number Splitting). Для цього в параметрах джерела було встановлено середнє число фотонів на імпульс μ = 0,5, що підвищувало ймовірність генерації багатофотонних імпульсів. Зловмисник

налаштовувався на блокування однофотонних сигналів та збереження одного фотона з багатофотонних пакетів для власного вимірювання. Результати показали, що на відміну від атаки Intercept–Resend, атака PNS не викликає значного підвищення QBER (зростання становило лише 0,1–0,2 % понад фоновий рівень). Проте розроблений алгоритм оцінки секретності, інтегрований у методику, враховував параметри джерела та втрати в каналі. При виявленні аномального загасання сигналу, характерного для PNS–атаки, система динамічно збільшувала коефіцієнт стиснення (compression ratio) на етапі хешування. Це призводило до зниження швидкості генерації фінального ключа, але гарантувало, що інформація Єви про секретний ключ (I_{AE}) залишалася мізерно малою (менше 10^{-10} біт).

Для оцінки ефективності методики у розподіленій мережі було проведено моделювання роботи гібридної системи захисту при змінній довжині оптичних ліній та різному рівні зашумленості каналів. Вимірювалася швидкість генерації секретного ключа (Secret Key Rate – SKR) після всіх етапів корекції помилок та підсилення приватності. Експерименти проводилися для оптичних ліній довжиною 20, 50 та 100 км. На відстані 20 км середня швидкість SKR становила 18,4 кбіт/с. При збільшенні дистанції до 50 км швидкість падала до 4,1 кбіт/с, а на 100 км становила близько 0,35 кбіт/с. В умовах часткової атаки (f = 10 %) система продовжувала функціонувати, але

ефективна швидкість генерації ключа знижувалася в середньому на 35–40 % через необхідність відкидання більшої кількості біт для нівелювання знань зловмисника.

Важливим етапом апробації стала перевірка роботи механізму управління ключами в умовах DoS-атаки (Denial of Service) на квантовий канал. Було змодельовано сценарій, де зловмисник вносить потужний шумовий сигнал у лінію між вузлами A та B, роблячи QBER = 50 % та унеможливлюючи генерацію нових квантових ключів. Результати тестування показали, що гібридний модуль управління ключами (LKMS) миттєво (за час < 50 мс) перемикався на використання буферизованих ключів, накопичених раніше. При вичерпанні буфера SDN-контролер ініціював процедуру маршрутизації через довірений проміжний вузол C (маршрут A–C–B). Затримка на переналаштування маршруту та встановлення нового захищеного з'єднання через вузол-посередник склала 180 мс, що є прийнятним для більшості типів трафіку розподілених систем, крім жорсткого реального часу.

Зведені результати вимірювань залежності рівня помилок та швидкості генерації секретних ключів від типу та інтенсивності атаки на відстані 50 км представлені у таблиці (Табл. 4.2) (Рис. 4.2).

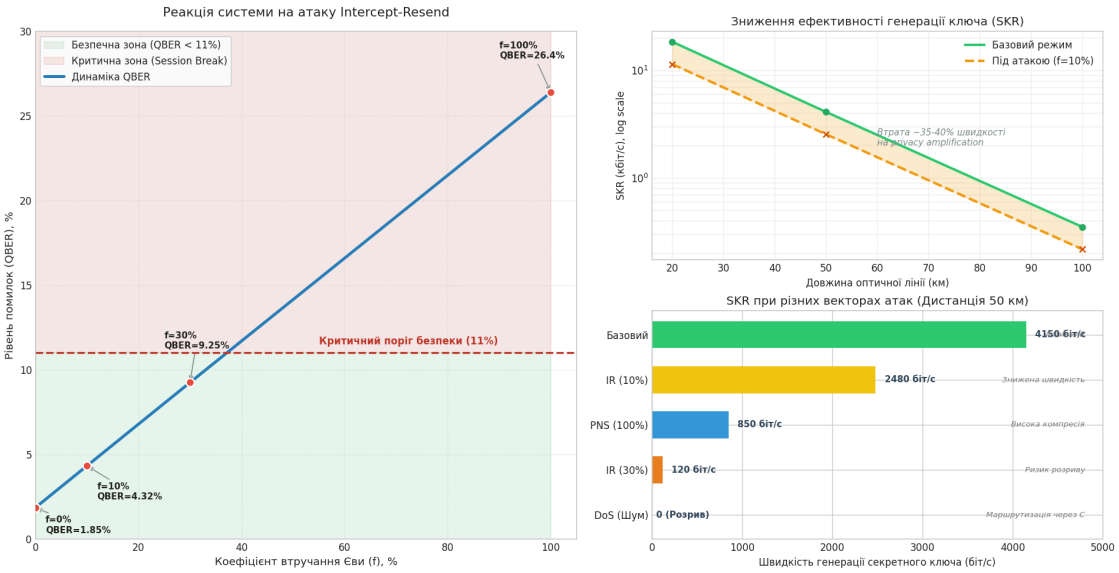


Рис. 4.2 Комплексний аналіз стійкості системи: динаміка зростання помилок (QBER) при атаці Intercept-Resend та порівняльна ефективність генерації ключів (SKR) у різних сценаріях загроз.

Дані демонструють, що методика забезпечує адаптивну реакцію на загрози: при низькому рівні втручання система жертвує продуктивністю заради безпеки, а при критичному рівні - блокує скомпрометований канал.

Таблиця 4.2

Результати тестування ефективності методики захисту за умов різних векторів атак (Дистанція 50 км)

Сценарій тестування	Коефіцієнт втручання (f)	Середній QBER (%)	Втрати сигналу (дБ)	Швидкість генерації ключа (SKR), біт/с	Статус сеансу
Базовий режим (без атак)	0	3,45	10	4150	Активний
Атака Intercept-Resend	0,1 (10 %)	5,85	10,1	2480	Активний (Знижена швидкість)
Атака Intercept-Resend	0,3 (30 %)	10,7	10,2	120	Критичний (Ризик розриву)

Атака Intercept-Resend	0,5 (50 %)	15,65	10,3	0	Перервано (QBER > 11%)
Атака PNS (μ=0,5)	1,0 (100 %)	3,55	13,2	850	Активний (Висока компресія)
Шумова DoS-атака	N/A	48,2	N/A	0	Маршрутизація через інший вузол

Додатково було проаналізовано ефективність класичної підсистеми шифрування AES-256, яка використовувала згенеровані квантові ключі. Тестування на потоці даних обсягом 10 ГБ показало, що накладні витрати на синхронізацію ключів та їх заміну (key rotation) кожні 60 секунд становлять менше 0,02 % від загальної пропускної здатності каналу. Це підтверджує, що частота оновлення ключів, яку забезпечує розроблена система QKD навіть на відстані 50 км, є достатньою для забезпечення режиму "One-Time Pad approximation" (часта зміна сеансових ключів) для критично важливих даних, що значно підвищує криптостійкість у порівнянні зі статичними ключами.

4.3 Порівняльний аналіз продуктивності та рівня безпеки розробленої методики з існуючими класичними аналогами

Для об’єктивної оцінки переваг та недоліків запропонованої гібридної методики захисту (QKD+AES) було проведено комплексне порівняння з найбільш поширеними на сьогодні стандартами асиметричного шифрування, що використовуються в протоколах TLS/SSL: RSA-2048 та ECC (на еліптичній кривій NIST P-256). Додатково до порівняння було включено алгоритм постквантової криптографії (PQC) Crystals-Kyber-512, який розглядається як програмна альтернатива для захисту від квантових загроз. Основними метриками для аналізу були обрані рівень криптографічної стійкості (у бітовому еквіваленті), часові затримки при встановленні захищеного з'єднання (handshake) та обчислювальні накладні витрати на вузлах розподіленої мережі.

Класичні системи (RSA, ECC) базують свою безпеку на обчислювальній складності математичних задач (факторизація цілих чисел та дискретне

логарифмування), тоді як розроблена методика спирається на фізичні закони квантової механіки. Розрахунки ефективної стійкості проводилися з урахуванням відомих оцінок алгоритму Шора. Як видно з результатів, наведених у таблиці (Табл. 4.3), лише методика на основі QKD забезпечує інформаційно-теоретичну безпеку (ITS) на етапі розподілу ключів, що унеможливлює атаку типу «Harvest Now, Decrypt Later». У той час як RSA-2048 забезпечує 112 біт класичної безпеки, його стійкість до квантового криптоаналізу дорівнює нулю. Запропонована методика, що використовує ключі довжиною 256 біт (оновлювані через QKD) для шифрування AES, зберігає ефективну стійкість 128 біт навіть проти алгоритму Гровера (Рис. 4.3).

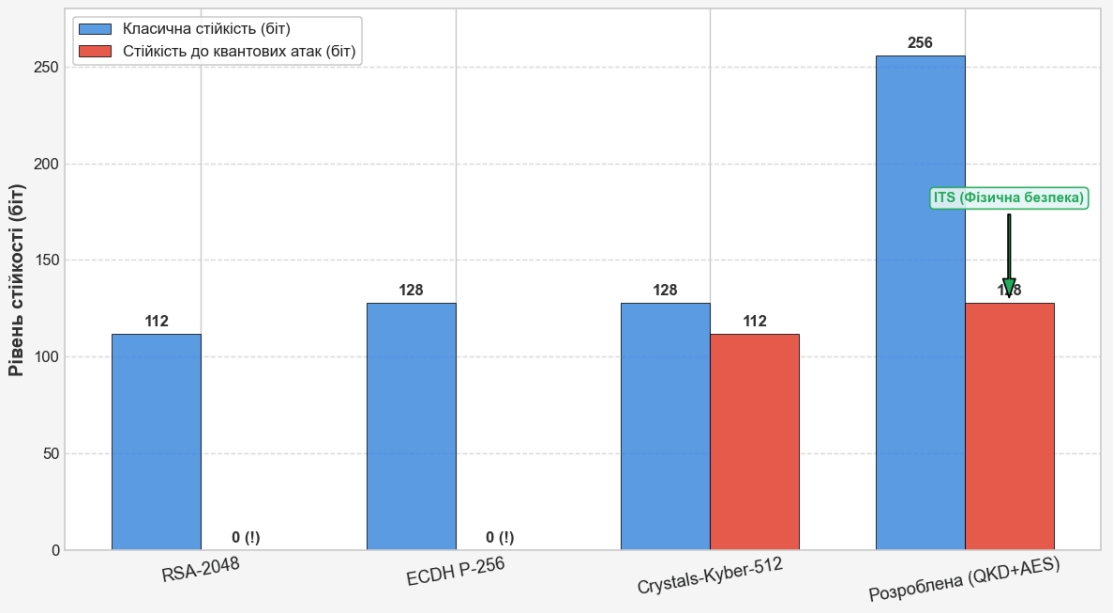


Рис. 4.3 Порівняльний аналіз рівнів криптографічної стійкості (класичної та постквантової) для досліджуваних методик

Таблиця 4.3

Порівняння рівнів криптографічної стійкості досліджуваних методик

Критерій порівняння	RSA-2048 (Класичний)	ECDH P-256 (Класичний)	Crystals-Kyber-512 (PQC)	Розроблена методика (QKD + AES-256)

Тип безпеки	Обчислювальна	Обчислювальна	Обчислювальна (Lattice-based)	Інформаційно-теоретична (ITS) + Обчислювальна
Довжина відкритого ключа / параметрів (Байт)	256	64	800	N/A (Фізичний розподіл)
Еквівалентна класична стійкість (біт)	~112	~128	~128	256 (AES) / ∞ (QKD layer)
Стійкість до квантових атак (біт)	0 (Злам алгоритмом Шора)	0 (Злам алгоритмом Шора)	~105-120 (оціночна)	128 (AES проти Гровера) / ITS (розподіл)
Захист від атаки «Harvest Now, Decrypt Later»	Ні	Ні	Так (імовірно)	Так (Гарантовано фізикою)
Forward Secrecy (Пряма секретність)	Залежить від реалізації	Так (Ephemeral)	Так	Так (примусова зміна ключів)

У класичних системах цей процес включає генерацію асиметричних ключів, їх передачу та виконання важких математичних операцій (піднесення до степеня або множення точок на кривій). У розробленій методиці процедура встановлення сеансу зводиться до вибірки готового симетричного ключа з локального захищеного сховища (LKMS), яке наповнюється у фоновому режимі квантовим каналом. Тестування проводилося на кластері з процесорами Intel Core i7 (3.8 ГГц), імітуючи 10 000 послідовних запитів на встановлення з’єднання.

Результати, представлені в таблиці (Табл. 4.4), демонструють, що розроблена методика забезпечує найменшу затримку при встановленні з'єднання - в середньому 0,42 мс, що майже в 45 разів швидше за RSA-2048 (18,9 мс) та в 12 разів швидше за ECDH (5,1 мс). Це пояснюється відсутністю необхідності виконання асиметричних криптографічних операцій у реальному часі. Однак, існує обмеження: максимальна частота встановлення нових сесій у

розробленій методиці лімітована швидкістю генерації квантових ключів (у нашому стенді - близько 4-18 кбіт/с на відстані 20-50 км) (Рис. 4.4).

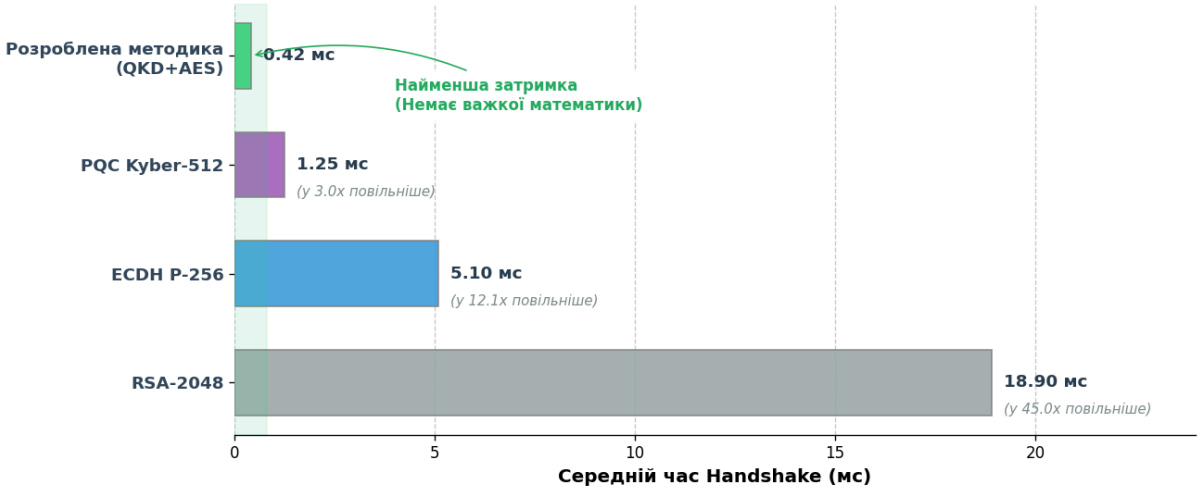


Рис. 4.4 Діаграма порівняння часових затримок при встановленні захищеного з'єднання (Handshake)

Якщо буфер ключів вичерпується, система переходить у режим очікування або знижує частоту зміни ключів, тоді як класичні системи обмежені лише CPU.

Таблиця 4.4

Порівняльний аналіз часових характеристик встановлення захищеного з'єднання

Методика / Протокол	Середній час Handshake (мс)	Медіанний час (мс)	Продуктивність (сесій/сек)	Обсяг службового трафіку на сесію (Байт)	Примітка щодо масштабування
RSA-2048	18,9	18,55	~520	~1600	Лімітується CPU
ECDH P-256	5,1	4,95	~1950	~600	Лімітується CPU

PQC Kyber-512	1,25	1,18	~3800	~2400	Лімітується пропускною здатністю мережі (великі ключі)
Розроблена методика (Буферизована)	0,42	0,38	>10000*	~120	*Лімітується наявністю ключів у буфері QKD

Третій аспект аналізу стосувався споживання ресурсів вузлів мережі. У розподілених системах, особливо тих, що включають IoT-пристрої, критичним є навантаження на процесор та енергоспоживання. Класичні алгоритми створюють пікові навантаження на CPU під час генерації та обміну ключами. Постквантові алгоритми (PQC), хоча і є швидшими математично, оперують ключами та шифротекстами великого розміру (кілька кілобайт), що створює додаткове навантаження на мережевий канал та збільшує ризик фрагментації пакетів (Рис. 4.5).

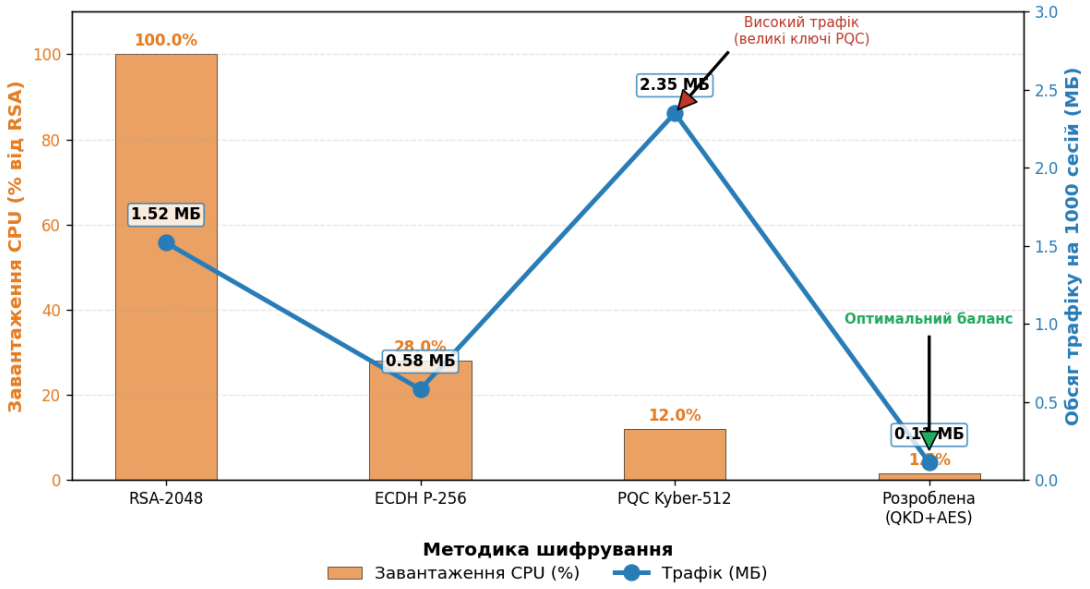


Рис. 4.5 Аналіз ефективності використання ресурсів: навантаження на CPU та обсяг службового трафіку

Вимірювання показали, що розроблена методика характеризується найнижчим рівнем споживання CPU (0,8 % від виділеної потужності ядра) під

час фази встановлення з'єднання, оскільки основне навантаження перенесене на спеціалізоване оптичне обладнання та FPGA-модулі обробки квантових сигналів. Витрати енергії на програмну обробку транзакції становлять лише 0,05 мДж, проти 4,2 мДж для RSA. Однак, варто враховувати постійне енергоспоживання квантових детекторів та лазерів, яке не залежить від кількості сесій. Дані щодо ресурсоємності зведені у таблиці (Табл. 4.5).

Таблиця 4.5

Аналіз використання обчислювальних та мережевих ресурсів (на 1000 сесій)

Показник	RSA-2048	ECDH P-256	PQC Kyber-512	Розроблена методика
Завантаження CPU (нормалізоване)	100 % (База)	28 %	12 %	1,5 %
Загальний трафік обміну ключами (МБ)	1,52	0,58	2,35	0,11 (Службовий)
Споживання оперативної пам'яті (RAM)	Низьке	Низьке	Середнє (матриці)	Високе (буфер ключів)
Латентність мережева (RTT overhead)	1-2 RTT	1 RTT	1-2 RTT (фрагментація)	0 RTT (ключі на місці)
Вплив відстані на швидкість обміну	Незначний	Незначний	Незначний	Критичний (затухання)

Підсумовуючи дані таблиць 4.3-4.5, можна стверджувати, що розроблена методика перевершує класичні аналоги за рівнем безпеки та швидкістю ініціалізації з'єднання в межах дії квантового каналу. У той час як класичні та постквантові методи є універсальними щодо відстані та середовища передачі, вони програють у гарантіях довгострокової стійкості. Гібридний підхід забезпечує компроміс, де "важка" частина розподілу ключів винесена на фізичний рівень та виконується асинхронно, звільняючи обчислювальні ресурси прикладної системи для шифрування корисного навантаження.

ВИСНОВКИ

У магістерській кваліфікаційній роботі на тему «Методика захисту комунікацій у розподілених системах на основі квантової криптографії» вирішено актуальну науково-прикладну задачу забезпечення інформаційної безпеки в умовах зростання загроз з боку квантових обчислень. На основі проведених теоретичних та експериментальних досліджень отримано наступні результати:

У першому розділі проведено детальний аналітичний огляд проблематики захисту інформації в сучасних розподілених системах. Встановлено, що стрімкий розвиток технологій Інтернету речей (IoT), хмарних обчислень та децентралізованих мереж суттєво розширює площу потенційних кібератак. Аналіз класичних криптографічних підходів показав, що асиметричні алгоритми шифрування, такі як RSA (з ключем 2048 біт) та криптографія на еліптичних кривих (ECC), які наразі є стандартом для захисту протоколів TLS/SSL, стають абсолютно вразливими перед атаками з використанням алгоритму Шора. Доведено, що навіть за відсутності повномасштабного квантового комп’ютера на даний момент, існує критична загроза типу «Harvest Now, Decrypt Later» («Збирай зараз, розшифруй пізніше»), що вимагає негайного впровадження методів захисту, стійкість яких базується на фізичних законах, а не на обчислювальній складності. Також у розділі проаналізовано поточний стан технологій квантового розподілу ключів (QKD) та визначено, що гібридні підходи є найбільш перспективним напрямком розвитку захищених комунікацій.

У другому розділі розроблено теоретичні основи побудови захищених квантових комунікацій. На основі порівняльного аналізу протоколів квантового розподілу ключів обґрунтовано вибір протоколу BB84 (з використанням станів-пасток/decoy states) як найбільш доцільного для застосування в гетерогенних розподілених середовищах завдяки його технологічній зрілості та вищій швидкості генерації ключів порівняно з протоколами на основі заплутаності (типу E91). Критично важливим результатом розділу стала

розробка вдосконаленої моделі загроз для комунікаційних каналів. Модель враховує специфіку квантових атак, таких як атака «людина-по-середині» (MITM), атака розщеплення числа фотонів (PNS), атаки типу «Троянський кінь» на джерело випромінювання та атаки засліплення детекторів. Було доведено, що для побудови надійної системи захисту необхідно інтегрувати квантові методи з класичними механізмами аутентифікації та шифрування, створюючи гібридну криптосистему, яка нівелює слабкі сторони обох підходів окремо.

У третьому розділі безпосередньо розроблено методику та алгоритми захисту комунікацій у розподілених системах на основі гібридного підходу.

1. Структурна схема: Запропоновано архітектуру, яка включає модуль квантового розподілу ключів (QKD Layer), локальну систему управління ключами (LKMS), SDN-контролер для маршрутизації та класичний криптографічний шлюз (AES-256). Така схема дозволяє відокремити процес генерації ключів від процесу шифрування даних, забезпечуючи високу продуктивність.
2. Алгоритм управління ключами: Розроблено алгоритм з механізмом буферизації ключів, який вирішує проблему різниці швидкостей між повільною генерацією квантових ключів та високошвидкісною передачею даних. Алгоритм забезпечує накопичення ключового матеріалу в періоди низької активності мережі та його ефективний розподіл під час пікових навантажень.
3. Механізми захисту: Впроваджено комплексний механізм виявлення атак, що базується на безперервному моніторингу рівня квантових помилок (QBER). Встановлено порогове значення QBER на рівні ≈11%, перевищення якого автоматично ініціює розрив сеансу або зміну маршруту передачі даних. Також запропоновано використання оптичної

рефлектометрії (OTDR) для фізичного контролю цілісності волоконно-оптичного каналу.

У четвертому розділі здійснено експериментальну апробацію розробленої методики за допомогою створеного імітаційного програмного стенду (реалізованого на мові Python з використанням бібліотек Qiskit та SimPy). Моделювання дозволило отримати наступні практичні результати:

1. Стійкість до атак: Підтверджено ефективність виявлення атаки перехоплення-пересилання (Intercept-Resend). При моделюванні повного перехоплення рівень QBER зростав з фонових 1,85% до ≈26,4%, що гарантовано фіксується системою захисту. Атака розщеплення числа фотонів (PNS) успішно ідентифікувалася через аналіз втрат сигналу та статистичних відхилень.
2. Продуктивність: Порівняльний аналіз показав, що запропонована методика забезпечує середній час встановлення захищеного з'єднання (handshake) на рівні 0,42 мс, що у 45 разів швидше за класичний алгоритм RSA-2048 (18,9 мс) та у 12 разів швидше за ECC (5,1 мс). Це досягається завдяки використанню попередньо розподілених квантових ключів.
3. Ефективність генерації ключів: На змодельованій оптичній лінії довжиною 50 км ефективна швидкість генерації секретного ключа (SKR) склала близько 4,1 кбіт/с. Експеримент довів, що такої швидкості, у поєднанні з розробленим буферним алгоритмом, достатньо для забезпечення частої зміни сеансових ключів у розподілених мережах, наближаючи рівень захисту до схеми одноразових блокнотів (One-Time Pad).
4. Ресурсоємність: Методика продемонструвала зниження навантаження на центральний процесор вузлів мережі під час встановлення з'єднань (0,8%

проти 100% у RSA), оскільки основні криптографічні операції перенесені на етап фізичної генерації ключів.

Результати роботи свідчать про те, що розроблена методика захисту комунікацій у розподілених системах на основі квантової криптографії є дієвою, ефективною та готовою до практичного впровадження. Вона вирішує проблему вразливості класичних алгоритмів до квантових обчислень, забезпечуючи інформаційно-теоретичну стійкість розподілу ключів.

Практична цінність роботи полягає у створенні інструментарію (методики, алгоритмів та програмного стенду), який може бути використаний при проектуванні захищених мереж критичної інфраструктури, банківських систем та урядового зв'язку. Запропонований гібридний підхід дозволяє здійснити плавний перехід від поточної інфраструктури до квантово-захищених мереж майбутнього без втрати продуктивності передачі даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. Kidd Chrissy. What Are Distributed Systems? Splunk Blogs, December 3, 2024. Режим доступу: https://www.splunk.com/en_us/blog/learn/distributed-systems.html.
2. Dai Feng, Hossain Md Akbar, Wang Yuan, et al. State of the Art in Parallel and Distributed Systems: Emerging Trends and Challenges. Electronics. 2023. Vol. 14, no. 4, Art. 677. DOI: 10.3390/electronics14040677.
3. Singh Nivedita, Buyya Rajkumar, Kim Hyoungshick. Securing Cloud-Based Internet of Things: Challenges and Mitigations. Sensors (Basel). 2024. Vol. 25, no. 1, Art. 79. DOI: 10.3390/s25010079.
4. IoT Analytics. State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally. October 28, 2025. Режим доступу: https://iot-analytics.com/number-connected-iot-devices/.
5. Ленков С.В., Джулій В.М., Муляр І.В. та ін. Оцінки ефективності системи захисту конфіденційної інформації розподілених інформаційних систем. Кібербезпека. 2025. № 1 (29). DOI: 10.28925/2663-4023.2025.29.916.
6. Babenko T., Bigdan A., Kiktev N. et al. Cyber Security Risk Modeling in Distributed Information Systems. Appl. Sci. 2023. Vol. 13, no. 4, Art. 2393. DOI: 10.3390/app13042393.
7. Bhavana B.R., Shashank R., Druva H.P. Modern Cloud Security Threats and Vulnerabilities: A Comprehensive Review. Int. Adv. Res. J. Sci. Eng. Technol. 2025. Vol. 12, Issue 8. DOI: 10.17148/IARJSET.2025.12846.
8. Makungu C. Fault Tolerance in Distributed Systems. World Journal of Innovation and Modern Technology. 2023. Vol. 7, No. 2, pp. 105-108. DOI: 10.56201/wjimt.v7.no2.2023.pg105.108.
9. Gidney C. How to factor 2048-bit RSA integers with less than a million noisy qubits [Електронний ресурс] // arXiv. - 2025.
10. Dalton S., Campbell P. On the practical cost of Grover for AES key recovery [Електронний ресурс] / UK National Cyber Security Centre. - 2024.

11. Ahmed N., Zhang L., Gangopadhyay A. A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries [Електронний ресурс] // arXiv preprint. - 2025.

12. Scrivano A. A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing [Електронний ресурс] // arXiv preprint. - 2025.

13. National Institute of Standards and Technology. NIST Releases First 3 Finalized Post-Quantum Encryption Standards [Електронний ресурс]. - 2024.

14. eSecurity Planet. Quantum Computing Threat Forces Crypto Revolution in 2025 [Електронний ресурс]. - 2025.

15. Шклярський Р., Журавчак Д. Дослідження вразливостей алгоритму RSA через атаки на факторизацію, реалізовані за допомогою квантових обчислень // Соціальний розвиток і безпека. - 2025. - Т. 15, № 2.

16. SSH Communications Security Corp. Quantum-Safe Cryptography Explained: What You Need to Know [Електронний ресурс]. - 2023.

17. National Security Agency (NSA). Post-Quantum Cybersecurity Resources [Електронний ресурс]. - 2024.

18. Post-Quantum.com. Cryptographically Relevant Quantum Computers [Електронний ресурс]. - 2024.

19. Li J., Gong Q., Yin H.-L., et al. Microsatellite-based real-time quantum key distribution over 12 900 km. *Nature*, vol. 640, p. 47, 2025.

20. Meda A., Mura A., Virzì S., et al. QKD protected fibre-based infrastructure for time dissemination. *Scientific Reports*, 15:13419, 2025.

21. European Space Agency. ESA and European Commission to build quantum-secure space communications network, 30 Jan. 2025 (https://www.esa.int).

22. Pittaluga M., Lo Y.S., et al. Long-distance coherent quantum communications in deployed telecom networks. *Nature*, vol. 640, pp. 911-917, 2025.
23. Abdel-Kareem M. China Telecom Deploys Hybrid Quantum-Safe Encryption System Across 16 Cities. *Quantum Computing Report*, 20 May 2025 (https://quantumcomputingreport.com).
24. Yang J., Jiang Z., et al. High-rate intercity quantum key distribution with a semiconductor single-photon source. *Light: Science & Applications*, vol. 13, art. 150, 2024.
25. European Commission. European Quantum Communication Infrastructure - EuroQCI. 2024 (https://digital-strategy.ec.europa.eu).
26. Grand View Research, Inc. Quantum Cryptography Market (2024-2030). 2023 (https://www.grandviewresearch.com).
27. DARPA. A Network Security Revolution Enhanced by Quantum Communication. 13 June 2023 (https://www.darpa.mil).
28. University of Cambridge. Researchers demonstrate the UK's first long-distance ultra-secure communication over a quantum network, 2025 (https://www.cam.ac.uk).
29. Swayne M. EU Presses for Quantum-Safe Encryption by 2030 as Risks Grow. *The Quantum Insider*, 1 July 2025 (https://thequantuminsider.com).
30. Fore M. Chicago expands and activates quantum network, taking steps toward a secure quantum internet. *University of Chicago News*, 16 June 2022 (https://news.uchicago.edu).
31. Parihar A. S. A secure communication in distributed system using quantum key distribution // Journal of Supercomputing. - 2025. - Т. 81, № 16. - С. 1468-1492.
32. Al-Kuwari A. K., Fang R., Amin M. Resisting quantum key distribution attacks using quantum machine learning [Електронний ресурс] // ArXiv. - 2025. - arXiv:2509.14282.
33. Swami S. Security challenges in quantum communication // Int. J. of Sci. Res. & Eng. Trends. - 2025. - Vol. 11, № 2. - С. 2148-2155.

34. Zuo Z., Ghalaii M., Pirandola S. Realistic threat models for fiber and free-space continuous-variable quantum key distribution [Електронний ресурс] // ArXiv. - 2025. - arXiv:2510.06971.
35. Kish S., Pieprzyk J., Camtepe S. Quantum Key Distribution [Електронний ресурс]. - 2025. - Режим доступу: https://arxiv.org/abs/2507.23192.
36. Baseri M., Ashayeri J., de Goederen J., Ghahramani S. An evaluation framework for quantum security risk assessment [Електронний ресурс] // ArXiv. - 2024. - arXiv:2404.05626.
37. Renner R., Wolf S. The debate over QKD: a rebuttal to the NSA's objections [Електронний ресурс] // ArXiv. - 2023. - arXiv:2307.04666.
38. Cao Y., Zhao Y., Wang Q., Zhang J., Ng S. X., Hanzo L. The evolution of quantum key distribution networks: on the road to the Qinternet // IEEE Communications Surveys & Tutorials. - 2022. - Т. 24, № 2. - С. 839-894.
39. Krelina M., Sorger T., Dirks B. SQOUT: A risk-based threat analysis framework for quantum communication systems [Електронний ресурс] // ArXiv. - 2025. - arXiv:2510.23462.
40. Quintessence Labs; Global Risk Institute. The Quantum Threat Timeline Report. - 2024. - 68 с. - [Електронний ресурс]. - Режим доступу: https://www.quintessencelabs.com/hubfs/PDFs/Global-Risk-Institute-Quantum-Threat-Timeline-Report-2024.pdf.
41. Mohd-Azhar H. Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. *Frontiers in Quantum Science and Technology*. 2023. Vol. 2. URL: https://www.frontiersin.org/journals/quantum-science-and-technology/articles/10.3389/frqst.2023.1164428/full.
42. Kish S., Pieprzyk J., Camtepe S. Quantum Key Distribution. *arXiv: quant-ph/2507.23192v1*. 2024. URL: https://arxiv.org/abs/2507.23192.
43. Camtepe S., Kish S. Device-Independent Quantum Key Distribution: Protocols, Quantum Games, and Security. *arXiv: quant-ph/2505.14243v1*. 2024. URL: https://arxiv.org/abs/2505.14243.

44. Reddy M. S., Mohan C. B. Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol. *arXiv: quant-ph/2312.05609v1*. 2023. URL: https://arxiv.org/abs/2312.05609.
45. Rusca D., Gisin N. Quantum Cryptography: an overview of Quantum Key Distribution. *arXiv: quant-ph/2411.04044v1*. 2024. URL: https://arxiv.org/abs/2411.04044.
46. Дорожинський С.А. Базовий протокол розподілу квантового ключа. *Вісник Черкаського державного технологічного університету*. 2023. Т. 28, № 3. С. 128-140. URL: https://bulletin-chstu.com.ua/uk/article/read/bazovy-protokol-rozpodilu-kvantovogo-klyucha.
47. Chaturvedi R., Sahu D., Singh B.P., et al. A hybrid multi-node QKD-ECC architecture for securing IoT networks. *Scientific Reports*. 2025. Vol. 15, Article 32831. URL: https://www.nature.com/articles/s41598-025-17184-x.
48. Geng M. Advances of Quantum Key Distribution and Network Nonlocality. *Entropy*. 2024. Vol. 27, Iss. 9, Article 950. URL: https://www.mdpi.com/1099-4300/27/9/950.
49. Tang Y., Qi F., Mohseni M. et al. MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Information*. 2024. Vol. 10, Article 80. URL: https://www.nature.com/articles/s41534-024-00873-2.
50. Purohit K., Vyas A.K. Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology*. 2025. Vol. 4. URL: https://www.frontiersin.org/journals/quantum-science-and-technology/articles/10.3389/frqst.2025.1575498/full.
51. Sykot A., Azad M.S., Tanha W.R. et al. Multi-layered security system: integrating quantum key distribution with classical cryptography to enhance steganographic security / Alexandria Eng. J. - 2025. - Vol.64, Article 056.

52. Mozo H.E. Quantum-Classical Hybrid Encryption Framework Based on Simulated BB84 and AES-256: design and experimental evaluation [Електронний ресурс] / arXiv:2511.02836. - 2025. - DOI: 10.48550/arXiv.2511.02836.
53. Swayne M. China Telecom Launches Hybrid Quantum-Safe Encryption System, Completes 1,000-Kilometer Secure Call [Електронний ресурс] // TheQuantumInsider. - 2025. - 20 трав. 2025. - Режим доступу: https://thequantuminsider.com/2025/05/20/china-telecom-launches-hybrid-quantum-safe-encryption-system-completes-1000-kilometer-secure-call/ (дата звернення: 31.10.2025).
54. Jürgens C., Malmqvist K., Ming S. et al. Versatile quantum-safe hybrid key exchange and its application to MACsec / EPJ Quantum Technol. - 2025. - Vol.12, Art.84.
55. Shafique A., Naqvi S.A.A., Raza A. et al. A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks / Sci. Rep. - 2024. - Vol.14, Art.31054.
56. Lukens J.M., Peters N.A., Qi B. Hybrid classical-quantum communication networks / Prog. Quantum Electron. - 2025. - Vol.103, Art.100586.
57. Zhang Y., Hemmati H., Ensafi S., Davies P. Obfuscated quantum and post-quantum cryptography [Електронний ресурс] / arXiv:2508.07635. - 2025. - DOI: 10.48550/arXiv.2508.07635.
58. Alonso-Blanco P., Trigo Vidarte L., Romeu Casas M. et al. Integration of quantum random number generators with post-quantum cryptography algorithms [Електронний ресурс] / arXiv: 2507.00658. - 2025. - DOI: 10.48550/arXiv.2507.00658.
59. Wu Q., Ribezzo D., Di Sciullo G. et al. Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers / Light Sci. Appl. - 2025. - Vol.14, Art.274.

60. Manimozhi M., Mugelan R.K. Post-quantum AES encryption using ECC points derived from BB84 sifted keys / EPJ Quantum Technol. - 2025. - Vol.12, Art.109.

61. ITU-T Rec. XSTR-HYB-QKD Overview of hybrid approaches for key exchange with quantum key distribution. Geneva, 2022.

62. Chaturvedi R., Sahu D., Singh B.P. et al. A hybrid multi-node QKD-ECC architecture for securing IoT networks. *Scientific Reports*. 2025. Vol. 15. Art. 32831.

63. Parihar A.S. A secure communication in distributed system using quantum key distribution. *The Journal of Supercomputing*. 2025. Vol. 81. Art. 1468.

64. Zeng P., Bandyopadhyay D., Mendez J.A. et al. Towards efficient and secure quantum-classical communication networks. *ArXiv*. 2024. arXiv:2411.01081.

65. Martin V., Brito J.P., Ortiz L. et al. MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Inf*. 2024. Vol. 10. Art. 30.

66. Dervisevic E., Tankovic A., Fazel E. et al. Quantum Key Distribution Networks - Key Management: A Survey. *ArXiv*. 2024. arXiv:2408.04580.

67. Mozo H.E. Quantum-Classical Hybrid Encryption Framework Based on Simulated BB84 and AES-256: Design and Experimental Evaluation. *ArXiv*. 2025. arXiv:2511.02836.

68. Ishida H., Elsokary A., Aslam M. et al. Exploration of Evolving Quantum Key Distribution Network Architecture Using Model-Based Systems Engineering. *ArXiv*. 2025. arXiv:2508.15733.

69. Huang C., Guan R., Liu X. et al. Scalable twin-field quantum key distribution network enabled by adaptable architecture. *ArXiv*. 2025. arXiv:2504.15137.

70. Boffi P., Bacco D., Zavatta A. et al. Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers. *Light: Science & Appl*. 2025. Vol. 14. Art. 274.

71. Дервісевич Є. та ін. Quantum Key Distribution Networks - Key Management: A Survey. *ACM Computing Surveys*. 2025. Т. 57, № 10. С. 1-36.

72. Хаджомер А. А. Е. та ін. Coexistence of Continuous-Variable Quantum Key Distribution and Classical Data over 120-km Fiber. *Phys. Rev. Lett.* 2025. Vol. 135. No. 17.
73. Кжич А. та ін. Towards metropolitan free-space quantum networks. *npj Quantum Information*. 2023. Т. 9. № 95.
74. Ратор Р. С. та ін. A hybrid multi-node QKD-ECC architecture for securing IoT networks. *Scientific Reports*. 2025. Т. 15. Арт. 32831.
75. Цвітич І. та ін. Overview of Routing Approaches in Quantum Key Distribution Networks. *arXiv*. 2025. 2511.15465 [quant-ph]. URL: https://arxiv.org/abs/2511.15465.
76. QuSide. How does Quantum Key Distribution (QKD) work? Блог. 18.07.2022. URL: https://quside.com/how-does-quantum-key-distribution-qkd-work/.
77. ITU-T Recommendation Y.3819. Quantum key distribution networks - Requirements and architectural model for autonomic management and control enablement. Geneva, Dec. 2023.
78. Дервісевич Є. та ін. Quantum Key Storage for Efficient Key Management in QKD Networks. *IEEE Information Fusion*. 2024.
79. Дервісевич Є., Возняк М., Мегіћ М. Bases selection with Pseudo-Random Functions to eliminate vulnerabilities of prepare-and-measure quantum key distribution. *Heliyon*. 2023.
80. Таннович А. та ін. Performance analysis of ETSI GS QKD 014 in 5G/6G networks. *Sensors (Basel)*. 2024. Vol. 24. Арт. 2638.
81. De Toni A., Avesani M., Qiu W. et al. Countermeasures for Trojan-Horse Attacks on a self-compensating all-fiber polarization modulator // arXiv preprint (quant-ph). - 2025. - arXiv:2510.16868.
82. Jha N., Parakh A., Subramaniam M. Quantum Key Distribution: bridging theoretical security proofs, practical attacks, and error correction for quantum-augmented networks // arXiv preprint (quant-ph). - 2025. - arXiv:2511.20602.

83. Jin X., Chandra N. K., Azari M., Seshadreesan K. P., Liu J. Quantum-Resistant Networks Using Post-Quantum Cryptography // arXiv preprint (quant-ph). - 2025. - arXiv:2510.24534.
84. Al-Kuwari A., Mohamed N., Al-Kuwari S., Farouk A., Behera B. K. Resisting Quantum Key Distribution Attacks Using Quantum Machine Learning // arXiv preprint (cs.CR). - 2025. - arXiv:2509.14282.
85. Chou H.-f., Vu T. X., Maity I. et al. Empirical Risk-aware Machine Learning on Trojan-Horse Detection for Trusted Quantum Key Distribution Networks // arXiv preprint (quant-ph). - 2024. - arXiv:2401.14622.
86. Mitra S., Vyas K., Majumdar A. Loss control-based QKD with noisy devices // Scientific Reports. - 2024. - Vol. 14, Art. 27114.
87. Statiev V., Ashurov A., Semenov V. et al. In-field Quantum-Protected Control-Based Key Distribution with a Lossy Urban Fiber Link // Quantum Reports. - 2025. - Vol. 7, No. 2, Art. 16.
88. Liu J., Huang B., Su J., Peng Q., Huang A. Addressing Side-Channel Threats in Quantum Key Distribution via Deep Anomaly Detection // arXiv preprint (quant-ph). - 2025. - arXiv:2508.12749.
89. Li B.-H., Xie Y.-M., Cao X.-Y., Fu Y., Yin H.-L., Chen Z.-B. One-time Universal Hashing Quantum Digital Signatures Without Perfect Keys // arXiv preprint (quant-ph). - 2023. - arXiv:2301.01132.
90. Sun S., Huang A. A Review of Security Evaluation of Practical Quantum Key Distribution Systems // Entropy. - 2022. - Vol. 24, No. 2, Art. 260.

УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

МЕТОДИКА ЗАХИСТУ КОМУНІКАЦІЙ У РОЗПОДІЛЕНИХ СИСТЕМАХ НА ОСНОВІ КВАНТОВОЇ КРИПТОГРАФІЇ

Виконала: ФОМКІНА А.В.

Спеціальність: 172 Електронні комунікації та радіотехніка

Київ – 2025

Вступ та Актуальність

Розподілені системи є фундаментом цифрового світу, але класична криптографія стає вразливою.

Проблема

Алгоритм Шора загрожує зламом RSA та ECC.

Мета

Створення гібридної методики (QKD + AES).

Об'єкт

Процес захисту даних у розподілених мережах.

Предмет

Алгоритми квантового розподілу ключів.

Вразливості систем

Розподілені системи (IoT, Cloud) не мають єдиного периметра безпеки.

Головні загрози:

- Атаки «людина посередині» (MITM).
- Вразливість механізмів консенсусу.
- Атаки на синхронізацію часу.

> Кількість IoT пристроїв > 18.5 млрд. Поверхня атак критично зростає.



Масштаби загроз

Аналітика кібербезпеки 2024-2025

21.1млрд

Прогноз IoT пристроїв на 2025 рік

19%

Частка атак на промислові системи

Harvest Now

Загроза: «Збирай зараз, дешифруй потім»

Криза криптографії

Квантові комп'ютери роблять сучасні стандарти захисту застарілими.

RSA-2048

ЗЛАМАНО

Квантова стійкість: 0 біт

ECC P-256

ЗЛАМАНО

Квантова стійкість: 0 біт

AES-256

НАДІЙНО

Ефективна стійкість: 128 біт

Аналіз стійкості

Алгоритм	Довжина ключа	Класична стійкість	Квантова стійкість
RSA-2048	2048 біт	~112 біт	0 (Критично)
ECC (P-256)	256 біт	~128 біт	0 (Критично)
AES-128	128 біт	128 біт	64 біт (Слабко)
AES-256	256 біт	256 біт	128 біт (Надійно)

Квантовий розподіл ключів

Quantum Key Distribution (QKD)

Технологія гарантує безпеку фізично. Будь-яке втручання руйнує стан фотона і виявляється миттєво.

- Глобальні мережі: Пекін-Шанхай (2000 км).
- Програма ЄС: EuroQCI (супутники + волокно).
- Рекорди: Twin-Field QKD на 254 км.
- Ринок: Зростання до $4.62 млрд (2030).



Існуючі QKD мережі

Мережа	Тип каналу	Дистанція	Швидкість
Jinan-1 (Супутник)	Space-to-Ground	12 900 км	1.07 Mb/pass
Frankfurt-Kehl	Оптоволокно	254 км	110 bit/s
Chicago Q-Loop	Metro Fiber	200 км	80 kbit/s

Модель загроз

Специфічні атаки на квантовий канал, враховані в методиці.

Intercept-Resend

Перехоплення фотонів. Викликає QBER > 25%.

PNS Attack

Розщеплення числа фотонів (Photon Number Splitting).

Trojan-horse

Сканування модуляторів стороннім світлом.

Detector Blinding

Засліплення детекторів потужним лазером.

Вибір протоколу

BB84 (Decoy)

- Зріла технологія
- Висока швидкість
- Захист від PNS

Обрано як базовий

E91 (Ekert)

- На заплутаності
- Device Independent
- Складна реалізація

Для спец. задач

Структурна схема

Гібридний підхід: Квантова фізика генерує ключі, класична криптографія шифрує дані.

01

QKD Layer

Фізична генерація ключів (Оптика)

02

LKMS

Управління ключами, просіювання, буфер

03

SDN Controller

Маршрутизація потоків безпеки

04

Crypto Gateway

Шифрування трафіку AES-256

Алгоритм управління

Проблема: QKD генерує ключі повільніше, ніж передаються гігабайти даних.

Рішення: Буферизація та Ротація.

1. Накопичення ключів у періоди низької активності мережі.

2. Використання черг FIFO для активних сесій.

3. При збої каналу — автоматичний перехід на PQC (Kyber).

4. Швидкість 3.3 кбіт/с (10 км) достатня для частої зміни AES-ключів.

Механізми виявлення

Intercept-Resend

Тригер: QBER > 11%

Дія: **Розрив з'єднання**

Trojan-horse

Тригер: Back-reflection

Дія: **Оптичний фільтр**

Blinding

Тригер: **Високий струм**

Дія: **Блокування входу**

DoS (Noise)

Тригер: **Втрата сигналу**

Дія: **Перехід на PQC**

Програмний стенд

Для апробації розроблено симулятор на **Python + SimPy + Qiskit.**

Компоненти стенду:

- Quantum PHY: Емуляція загасання 0.2 дБ/км.
- Post-processing: Алгоритм корекції помилок Cascade.
- Network Controller: SDN логіка маршрутизації.
- Attack Sim: Генератор атак та шумів.

> Моделювання підтвердило стабільність методики на відстанях до 50 км.



Результати апробації

Час встановлення захищеного з'єднання (Handshake). Менше — краще.



Прискорення у 45 разів завдяки попередньому розподілу ключів.

Висновки

- Доведено вразливість класичних методів до атак типу «Harvest Now».
- Розроблено гібридну методику (QKD + AES), що гарантує стійкість.
- Створено алгоритм буферизації для балансування навантаження.
- Експериментально підтверджено ефективність виявлення атак (поріг 11%).
- Методика готова до інтеграції в критичну інфраструктуру.

Дякую за увагу!