Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)

Кафедра Фізичних основ електронної техніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

КВАНТОВА КРИПТОГРАФІЯ ВОЛОКОННИХ
ТА ВІДКРИТИХ СИСТЕМ ЗВ'ЯЗКУ
(тема)

Виконав:
здобувач 4 року навчання,
групи МТІОЛС-21-1
Михайло ГУТОВСЬКИЙ
(власне ім'я, прізвище)

Спеціальність 152 Метрологія та
інформаційно-вимірювальна техніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна

Освітня програма «Інженерія
оптоінформаційних та лазерних систем»
(повна назва освітньої програми)

Керівник проф. каф. ФОЕТ Юрій КУРСЬКИЙ
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ФОЕТ _____ Олександр ГНАТЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії

Кафедра Фізичних основ електронної техніки

Рівень вищої освіти перший (бакалаврський)

Спеціальність 152 Метрологія та інформаційно-вимірювальна техніка
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма «Інженерія оптоінформаційних та лазерних систем»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Гутовському Михайлу Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Квантова криптографія волоконних та відкритих систем зв'язку

затверджена наказом університету від « 23 » травня 2025р. № 408 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 23 червня 2025 р.

3. Вихідні дані до роботи Фізико-математичні основи квантової криптографій; токоли квантового розподілу ключів; квантова криптографія в оптоволоконних лініях зв'язку; квантова кріптографія в відкритих лініях зв'язку.

4. Перелік питань, що потрібно опрацювати в роботі:
1. Розкрити основні принципи квантової механіки, що лежать в основі квантової криптографії 2. Описати протоколи квантового розподілу ключів та принцип їх дії. 3. Проаналізувати переваги та обмеження використання волоконно-оптичних ліній у квантовому зв'язку. 4. Порівняти волоконні та відкриті канали передавання в контексті реалізації квантової криптографії.

5. Перелік графічного матеріалу із зазначенням кресленików, схем, плакатів, комп'ютерних ілюстрацій
Демонстраційний матеріал – 13 слайдів.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Інформаційно-тематичний пошук та огляд літературних джерел про квантову криптографію	06.05.25–15.05.25	Виконано
2	Дослідження фізико-математичні основи квантовой криптографії	16.05.25–22.05.25	Виконано
3	Дослідження особливості використаня квантової криптографії в оптоволоконних та відкритих систем	23.05.25–28.05.25	Виконано
4	Дослідження тенденцій розвитку систем квантової кріптографії	29.05.25–01.06.25	Виконано
5	Оформлення пояснювальної записки	02.06.25–10.06.25	Виконано
6	Оформлення демонстраційних матеріалів	11.06.25–13.06.25	Виконано
7	Проходження нормоконтролю та перевірки на академічний плагіат	14.06.25–20.06.25	Виконано
8	Отримання відгуку та рецензії	21.06.25–22.06.25	Виконано
9	Підготовка та захист кваліфікаційної роботи	23.06.25–24.06.25	Виконано

Дата видачі завдання 05 травня 2025 р.

Студент _____
(підпис)

Керівник роботи _____ проф. каф. ФОЕТ Юрій КУРСЬКИЙ
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 53 с., 15 рис., 4 табл., 14 джерел, 1 додаток.

КВАНТОВА КРИПТОГРАФІЯ, КВАНТОВИЙ СТАН, КОЛАПС ХВИЛЬОВОЇ ФУНКЦІЇ, КУБІТ, ОПТИЧНЕ ВОЛОКНО, ПОЛЯРИЗАЦІЯ, ПРИНЦИП НЕВИЗНАЧЕНОСТІ.

Об’єкт дослідження – технологія квантовоїй криптографії.

Метою кваліфікаційної роботи є дослідження принципів квантової криптографії та її використаня в оптично волоконних та відкритих системах звязку, а також опис протоколи квантового розподілу ключів та принцип їх дії.

Метод дослідження – теоретичний.

Для досягнення мети в роботі поставлено та вирішено наступні завдання.

1. Дослідити фізико-математичні основи квантової криптографій.
2. Дослідити особливості використаня квантовой криптографій в оптоволоконних та відкритих системах зв’язку.

ABSTRACT

Explanatory note of the qualification work: 53 pp., 15 figures, 4 tables, 14 sources, 1 applications.

QUANTUM CRYPTOGRAPHY, QUANTUM STATE, WAVEFUNCTION COLLAPSE, QUBIT, OPTICAL FIBER, POLARIZATION, UNCERTAINTY PRINCIP.

The object of research is quantum cryptography technology.

The purpose of this thesis is to study the principles of quantum cryptography and its use in optical fiber and open communication systems, as well as to describe quantum key distribution protocols and how they work.

The research method is theoretical.

To achieve the goal, the following tasks were set and solved in the work.

1. To study the physical and mathematical foundations of quantum cryptography.

2. To study the features of the use of quantum cryptography in fiber optic and open communication systems.

ЗМІСТ

ВСТУП

У сучасному світі, де обсяги переданої інформації зростають експоненційно, питання безпеки комунікацій стає надзвичайно актуальним. Класичні криптографічні методи, що базуються на складності математичних задач и кількості вариацый, вже сьогодні перебувають під загрозою з боку стрімкого розвитку обчислювальних технологій, зокрема у галузі квантових комп'ютерів та квантових обчислень. У цьому контексті квантова криптографія виступає як перспективна альтернатива, що забезпечує принципово новий рівень захисту інформації.

Согодні розглядається реалізація застосування квантової криптографії у волоконно-оптичних та відкритих системах зв'язку. Завдяки властивостям квантової механіки, таким як суперпозиція, заплутаність та принцип невизначеності, стає можливою реалізація протоколів безпечного обміну ключами, що гарантують виявлення будь-якої спроби несанкціонованого доступу к информацый.

У даній роботі розглядаються основи квантової криптографії, її реалізація в оптичних системах зв'язку, а також порівнюються переваги та виклики, пов'язані з використанням волоконних і відкритих каналів для передавання інформації.

Метою кваліфікаційної роботи є дослідження фізичних принципів, оптично волоконних та відкритих систем, а також тенденції розвитку систем квантової криптографії.

Для досягнення мети в роботі поставлено низку завдань, в межах теми, у яких потрібно досліджувати, аналізувати. Потрібно визначити основні напрямки розвитку технологій квантової криптографії.

Розвиток сучасних технологій квантової криптографії є стрімким та в край необхідним. В свою чергу це вказує на те, що дослідження цих систем, та слідкування за новими розробками є наявною необхідністю.

1 ФІЗИКО-МАТЕМАТИЧНІ ОСНОВИ КВАНТОВОЇ КРИПТОГРАФІЇ

1.1 Суперпозиція та кубіт

Согодні застосуваня квантовой кріптограіфй не є необхідністю, оскільки на момент нинішнього часу традиційного шифрування даних було достатньо для підтримання безпечного зв'язку в більшості ситуацій, пов'язаних з кібербезпекою. Однак розвиток квантових обчислень створює потенційну загрозу навіть для найбезпечніших традиційних криптографічних алгоритмів. У зв'язку з цим виникає необхідність розробити й реалізувати методи для квантової криптографії, щоб бути готовим до того, що традиційні методи шифрування стануть неприйнятними для забезпечення збереження інформації.

На відміну від традиційної криптографії, яка побудована на математиці і спирається на складність та малу теорему Ферма, яка стверджує що якщо p – просте число, a – ціле число, яке не ділиться на p то:

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.1}$$

Квантова криптографія побудована на законах фізики, саме на основних законах квантової фізики. Зокрема, квантова криптографія спирається на унікальні принципи квантової механіки. Головним принципом квантової механіки, на якому заснована квантова криптографія, є принцип суперпозицій [1].

Для роботи з квантовою суперпозицію потрібно зрозуміти, що вона ґрунтується на рівнянні Шредінгера – це диференційне рівняння в частинних похідних, яке описує хвильову функцію нерелятивістської квантово-механічної системи:

$$i\hbar \frac{\partial}{\partial \mathrm{t}} \Psi(x,t) = \hat{\mathrm{H}}\Psi(x,t), \tag{1.2}$$

де $\Psi(x,t)$ – хвильова функція (амплітуда ймовірності);

i – уявна одиниця;

$\hbar$ – приведена стала Планка;

$\widehat{H}$ – оператор гамільтоніану (представляє повну енергію: кінетичну та потенційну);

x – координата;

t – час.

Слід визначити що квантова суперпозиція – це фундаментальний принцип квантової механіки, який стверджує, що лінійні комбінації розв'язків рівняння Шредінгера також є розв'язками рівняння Шредінгера. Це випливає з того, що рівняння Шредінгера є лінійним диференціальним рівнянням за часом і положенням. Точніше, стан системи задається лінійною комбінацією всіх власних функцій що описує цю систему.

Для простого розуміння суперпозицій можна проаналізувати експеримент із проходом світла через фільтри з різною поляризацією. Для того щоб спостерігати ефект суперпозиції, можливо встаннвити кілька фільтрів по-різному. Світло, яке проходить крізь горизонтальний фільтр, матиме сто відсотковій шанс пройти крізь другий горизонтальний фільтр, тобто пройде крізь нього повністю. Якщо змінювати положення цього фільтра повертаючи його до вертикальної орієнтації, ймовірність проходження світла через обидва фільтри неухильно зменшується. Половина світла пройде, коли фільтр досягне діагоналі 45 %, і жодне світло не пройде, коли фільтр стоїть вертикально як показано на рисунку 1.1.

Але коли додамо діогональний фільтр між горизонтальним і вертикальним фільтрами це дозволяє деякому світлу проходити через всю систему як показано на рисунку 1.2. Це також результат суперпозиції. Новий фільтр пропускає 50 % світла, що проходить через горизонтальний фільтр. Потім, оскільки новий фільтр також є діагональним по відношенню до вертикального фільтра, вертикальний фільтр пропускатиме 50 % світла.

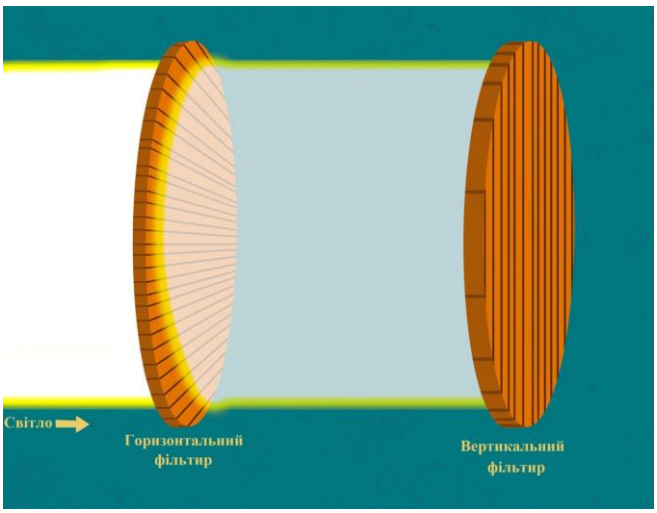

Рисунок 1.1 – Світло не проходить через горизонтальний фільтр, за яким слідує вертикальний фільтр

Тому що діагональний фільтр як би скидає суперпозицію світла, роблячи його більш схильним до вертикальної поляризації, що дозволяє частині світла повністю пройти всю систему фільтрів [2].

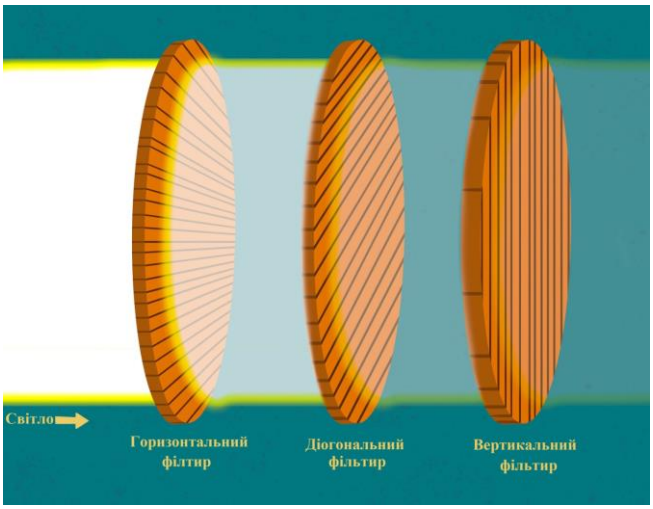

Рисунок 1.2 – Частина світла проходить через горизонтальний фільтр, за яким послідовно слідують діагональний і вертикальний фільтри

З цього можливо проаналізувати як працює і можливість впливати на супер позицію. Але для квантової криптографії, не тільки потрібно взаємодіяти з фізичними частинками, а й передати інформацію. У класичній цифровій системі основною одиницею інформації є біт, який може набувати лише одного з двох станів — «0» або «1». У квантовій інформаційній науці його аналогом є кубіт, який володіє принципово іншими властивостями. Кубіт – це елементарна одиниця квантової інформації, що здатна перебувати не тільки в стані «0» або «1», а й у суперпозиції цих двох станів одночасно.

Кубіт – це дворівнева квантово-механічна система, одна з найпростіших квантових систем, що відображає особливості квантової механіки. У класичній системі біт мав би перебувати в тому чи іншому стані. Однак квантова механіка дозволяє кубіту перебувати в когерентній суперпозиції кількох станів одночасно – властивість, яка є фундаментальною для квантової механіки та квантових обчислень.

Чистий стан кубіта – це когерентна суперпозиція базисних станів. Це означає, що один кубіт (ψ) можна описати лінійною комбінацією $|0\rangle$ і $|1\rangle$. Математично кубіт описується як вектор у двовимірному комплексному гільбертовому просторі:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \qquad (1.3)$$

де $|0\rangle$ та $|1\rangle$ – базисні стани;

α і β — комплексні коефіцієнти.

Сфера Блоха використовується в квантовій механіці для геометричного зображення простору чистих станів квантовомеханічної дворівневої системи як зазначено на рисунку 1.3, названа на честь фізика Фелікса Блоха.

Сфера Блоха є одиничною двовимірною сферою, кожна пара діаметрально протилежних точок якої відповідають взаємно ортогональним векторам стану. Зокрема, північний і південний полюси сфери Блоха

вважаються такими, що відповідають базисним векторам |0⟩ та |1⟩, які в свою чергу можуть відповідати, наприклад, двом спіновим станам електрона. Однак, слід зазначити, що подібний вибір точок є довільним. Точки на поверхні сфери відповідають чистим станам квантової системи, в той час як точки всередині сфери репрезентують мішані стани. Взагалі сфера Блоха може бути узагальнена на N-рівневі квантові системи, але така візуалізація є менш наочною та корисною.

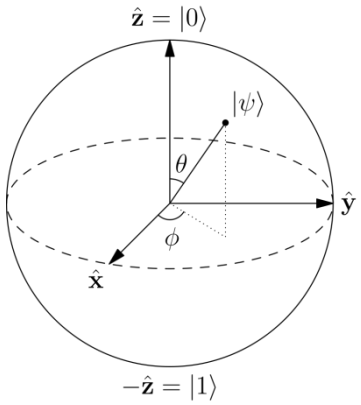

Рисунок 1.3 – Сфера Блоха

Коли проводитися вимірювання цього кубіту у стандартному базисі, згідно з правилом Борна, ймовірність результату |0⟩ зі значенням «0» є $|\alpha|^2$ та ймовірність результату |1⟩ зі значенням «1» є $|\beta|^2$. Оскільки абсолютні квадрати амплітуд дорівнюють ймовірностям, то з цього випливає, що α і β повинна бути обмежена згідно з другою аксіомою теорії ймовірностей рівнянням:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.4}$$

Амплітуди ймовірностей, α і β, кодують більше, ніж просто ймовірності результатів вимірювання; відносна фаза між α і β, відповідає за

квантову інтерференцію. Ця здатність кубіта перебувати в суперпозиції надає квантовим системам значно вищу гнучкість і потужність у порівнянні з класичними які спираються на послідовний та суворий математичний порядок дій. В основі більшості квантових протоколів шифрування, лежить саме передавання та маніпуляція кубітами у вигляді окремих фотонів з певною поляризацією [3].

1.2 Квантове вимірювання та принцип невизначеності

Однією з найважливіших особливостей квантових систем є те, що процес вимірювання істотно впливає на стан об’єкта, що дозволяє відстежувати втручання у процес ззовні. На відміну від класичної фізики, де спостереження не змінює стану системи, у квантовій механіці вимірювання призводить до колапсу хвильової функції – тобто, квантовий об’єкт переходить із суперпозиції можливих станів (1.2) до одного конкретного результату, кубит прийняв «0» або «1».

Сформульований німецьким фізиком і лауреатом Нобелівської премії Вернером Гейзенбергом у 1927 році, принцип невизначеності стверджує, що неможливо знайти положення і швидкість частинки, наприклад, фотона або електрона, з ідеальною точністю; чим більше інформації відомо про положення частинки, тим менше інформації відомо про її швидкість, і навпаки, що не дозволяє отримати точну інформацію про всі властивості частки одночасно [4].

Хоча принцип невизначеності Гейзенберга добре відомий у квантовій фізиці, подібний принцип невизначеності також застосовується до проблем чистої математики та класичної фізики – по суті, будь-який об'єкт з хвилеподібними властивостями буде піддаватися впливу цього принципу. Квантові об'єкти є особливими, оскільки всі вони демонструють хвилеподібні властивості за самою природою квантової теорії, що дуже ускладнює роботу з такими об'єктами, оскільки це призводить до того, що частки будуть

втрачати стан суперпозицій не тільки при втручанні ззовні людей, а й природних факторів, які впливатимуть на точність та ефективність передачі інформацій аж до повної її втрати.

Це означає, що до моменту вимірювання стан частинки не визначений однозначно – вона перебуває у поєднанні кількох можливих станів. Але як тільки здійснюється спостереження, цей стан «обирається» випадковим чином згідно з ймовірностями, заданими квантовою амплітудою. Саме ця властивість лежить в основі невідворотності зміни стану при спробі підслуховування в квантовій криптографії.

Принцип невизначеності, також відомий як принцип невизначеності Гейзенберга, є фундаментальним поняттям у квантовій механіці. Він відіграє в ньому дуже важливу роль і формально виражається співвідношенням:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}, \tag{1.5}$$

де Δx— невизначеність положення;

Δp — невизначеність імпульсі.

Принцип стверджує, що існує межа точності, з якою можуть бути одночасно відомі певні пари фізичних властивостей, таких як положення та імпульс. Іншими словами, чим точніше вимірюється одна властивість, тим менш точно може бути відома інша властивість.

Система може перебувати в стані, в якому вона не має чітко визначеного значення величини, яку зазвичай очікуємо від класичної системи – точного положення і точного імпульсу, або, у випадку частинок зі спіном, чітко визначеної компоненти спіну в будь-якому напрямку. І з усього вище перерахованого можна дійти висновків, що коли проводиться вимірювання певної величини, стан системи перетворюється на такий, в якому ця величина справді є добре визначеною. Те, що відбувається з хвильовою функцією, яка описує систему, коли це відбувається, називається «колапс хвильової функції» що випливає з вищезазначеного закону невизначеності Гейзенберга.

Таки чином ключовою властивістю, що лежить в основі безпеки квантових протоколів, є колапс хвильової функції при вимірюванні. В квантовій механіці частинка, наприклад фотон, до моменту вимірювання перебуває у стані суперпозиції – вона може бути водночас у кількох можливих станах. Однак, коли проводиться спостереження або вимірювання, ця суперпозиція миттєво руйнується, і система переходить у один конкретний стан – цей процес і називається колапсом хвильової функції.

У контексті квантової криптографії це явище має надзвичайно важливе практичне значення. В протоколах передача інформації відбувається у вигляді окремих фотонів, які кодуються в певному поляризаційному стані. Якщо зловмисник намагається перехопити цей фотон і провести вимірювання без знання правильного базису, його дія змінює стан фотона, спричиняючи коллапсу хвильової функції, що впливає на кінцевий результат. У результаті такі втручання можна виявити за допомогою статистичного аналізу помилок у переданому ключі.

Це робить будь-яке несанкціоноване втручання принципово неможливим без помітних наслідків, що забезпечує базову фізичну безпеку квантових мереж на рівні, недосяжному для класичних засобів шифрування.

При спробі обійти це може виникнути спокуса інтерпретувати цю дуже дивну поведінку субмікроскопічних систем в термінах так званих «прихованих змінних». Це припущення, що частинка справді має і положення, і імпульс, і компонент спіну як у напрямку *z*, так і в напрямку *x*, але експериментатор не знає, якими є значення будь-якої з цих величин, доки не проведе експеримент з її вимірювання, не є дійсним. Джон Белл показав, що цей постулат дає результати, які не узгоджуються з передбаченнями квантової механіки. На субмікроскопічному рівні система просто не володіє цими величинами і що акт вимірювання – або взаємодія системи з макроскопічним середовищем – змінює хвильову функцію та впливає на стан частки.

Тобто колапс хвильової функції – це механізм, в якому система, взаємодіючи з навколишнім середовищем, перетворюється з суперпозиції станів у певний стан з чітко визначеним значенням заданої вимірюваної величини. Саме властивість хвилі призводити до інтерференції породжує дивне явище, яке дозволяє квантовій системі одночасно мати кілька значень певної вимірюваної властивості. Ця властивість називається «когерентність» і пов'язана з тим, що фази двох хвиль, які інтерферують, мають бути «заблоковані» так, щоб між ними існувала постійна різниця фаз, яка і породжує цю інтерференцію. Процес розблокування цієї фази – так, щоб різниця фаз двох хвиль була випадковою – відомий як «декогеренція», і зараз вважається, що це механізм, який призводить до колапсу хвильової функції. Коли відбувається декогеренція, втрачається квантова властивість суперпозиції станів з багатьма різними можливими значеннями для даної величини - хвильова функція розпадається на хвильову функцію для стану, в якому ця величина дійсно чітко визначена і має унікальне значення.

Монохроматичне світло або інше монохроматичне електромагнітне випромінювання, або частинки з однаковим імпульсом, що використовуються в експерименті Юнга з подвійною щілиною, можуть інтерферувати, оскільки падаюча хвиля є когерентною, тобто хвильовий фронт на подвійній щілині має піки і спади одночасно – вони зчеплені за фазою. Якщо щось трапляється, щоб рандомізувати фази хвиль, що падають на обидві щілини, інтерференція втрачається. Спроба визначити, через яку щілину пройшов фотон або електрон, є прикладом збурення системи, що призводить до декогеренції і, як наслідок, втрати інтерференційної картини [5].

1.3 Поляризація фотонів та квантовий розподіл ключів

Поляризація фотонів – це фундаментальна концепція, яка використовується у квантовому розподілі ключів. Це квантово-механічний опис класичної поляризованої синусоїдальної плоскої електромагнітної

хвилі. Окремий фотон можна описати як такий, що має праву або ліву кругову поляризацію, або їх суперпозицію. Еквівалентно, фотон можна описати як такий, що має горизонтальну або вертикальну лінійну поляризацію, або їх суперпозицію.

Квантовий розподіл ключів використовує принципи квантової механіки для генерації секретного ключа через квантовий канал, і ця процедура є повністю безпечною завдяки законам квантовий фізики. Властива випадковість квантових станів та їх вимірювань забезпечує випадковість у створенні ключа. Крім того, QKD використовує теорему про неможливість клонування, де квантові стани не можуть бути клоновані, тому цей ключ є унікальним. Крім того, принцип невизначеності Гейзенберга, робить процес квантового розподілу ключів стійким до спроб перехоплення та ретрансляції з боку шахрайського користувача. За допомогою принципу Гейзенберга виявляється існування підслуховувача, оскільки спроба виміряти квантові стани спровокує зміни у квантовій системі, і обидві сторони, які спілкуються, виявлять підслуховувача.

Припустимо, що існують два користувачі, «Аліса» і «Боб», які хочуть обмінюватися інформацією і повинні згенерувати секретний ключ. Протокол розподілу квантового ключа складається з двох фаз. Перша фаза квантової передачі, на якій відправник і одержувач надсилають і вимірюють квантові стани або просто вимірюють їх, і друга фаза пост-обробки, на якій бітові рядки, згенеровані на квантовій фазі, повертаються в пару безпечних ключів. Для процедури квантового розподілу ключів необхідна наявність двох каналів, квантового каналу і класичного каналу, де відбувається процес обміну повідомленнями. У квантовому каналі передається промінь фотонів, кодуючи кожен фотон методом поляризації [6].

Основними перевагами виеористаня квантового росподілу ключів є:

– безпека: QKD базується на принципах квантової механіки і вважається однією з найбезпечніших форм шифрування. Вона стійка до прослуховування, що є головною проблемою традиційних методів

шифрування, оскільки будь-яка спроба прослуховування процесу розподілу ключів буде виявлена;

– квантова стійкість: QKD вважається квантово-стійким, що означає, що він захищений від атак квантових комп'ютерів, тоді як традиційні методи шифрування, такі як симетричне та асиметричне шифрування, будуть зламані потужністю квантових комп'ютерів;

– розподіл ключів: У QKD процес розподілу ключів є безпечним і не залежить від безпечного початкового каналу, який необхідний у традиційних методах шифрування. Це робить його більш придатним для використання в середовищах, де безпечний початковий канал недоступний.

Загальний протокол розподілу квантових ключів за принципом «підготуй і виміряй» можна розділити на два основні етапи: квантова комунікація та класична постобробка. Під час квантової комунікації відправник «Аліса» кодує екземпляри випадкової класичної змінної α у неортогональні квантові стани. Ці стани надсилаються квантовим каналом, який контролюється підслуховувачем «Євою», що намагається викрасти закодовану інформацію. Лінійність квантової механіки забороняє здійснити досконале клонування, тому «Єва» може отримати лише часткову інформацію, порушуючи квантові сигнали. На виході каналу зв'язку приймач «Боб» вимірює вхідні сигнали і отримує випадкову класичну величину β. Після декількох використань каналу «Аліса» і «Боб» обмінюються вихідними даними, які описуються двома корельованими змінними α і β.

Віддалені сторони використовують частину вихідних даних для оцінки параметрів каналу, таких як його пропускна здатність і рівень шуму. Цей етап оцінки параметрів важливий для того, щоб оцінити обсяг постобробки для вилучення приватного спільного ключа з решти даних. Залежно від цієї інформації, вони фактично виконують етап виправлення помилок, який дозволяє виявити і усунути помилки, після чого слідує етап посилення конфіденційності, який дозволяє зменшити вкрадену «Євою» інформацію до незначної кількості. Кінцевим результатом є секретний ключ.

Залежно від того, яку змінну вгадано, буде спостерігатися пряме або зворотне узгодження. При прямому узгодженні саме «Боб» обробляє свої результати, щоб зробити висновок про кодування «Аліси». Ця процедура зазвичай здійснюється за допомогою прямого класичного зв'язку від «Аліси» до «Боба». На противагу цьому, в RR «Аліса» обробляє свою змінну кодування для того, щоб вивести результати «Боба». Ця процедура зазвичай супроводжується останнім раундом зворотної класичної комунікації від «Боба» до «Аліси». Звичайно, в більш загальному випадку можна розглядати двосторонні процедури, в яких видобуванню ключа допомагають прямі і зворотні класичні комунікації, які можуть навіть чергуватися з різними раундами комунікації в протоколі.

Поляризація фотонів є основою всього процесу шифрування інформації та розподілу квантового ключа. Отримаємо те що ми досягаємо за допомогою поляризації світла, полягає в геометричній орієнтації коливань електромагнітного поля, пов'язаних з його хвилею. Слід зосередити аналіз на двох типах базисів поляризації: прямолінійний базис і діагональний базис. Отже, класичний біт кодується в поляризації фотона, і це досягається за допомогою фільтрів або кристалів.

Іноді протоколи квантового розподілу ключів формулюють у представленні на основі заплутаності. Це означає, що підготовка Алісою вхідного ансамблю станів замінюється заплутаним станом ψ_{AB}, частина якого вимірюється «Алісою». Вимірювання на частині *A* має наслідком умовну підготовку стану на частині *B*. Результат вимірювання співпадає з класичною змінною, закодованою у підготовлених станах. Таке представлення є особливо корисним для вивчення протоколів квантового розподілу ключів, оскільки їх формулювання підготовки та вимірювання замінюється формулюванням на основі заплутаності для оцінки безпеки та отримання швидкості секретного ключа [4].

1.4 Протоколи квантового розподілу ключів

1.4.1 Протокол BB84

У 1984 році Чарльз Беннетт (Charles Bennett) і Жиль Брассар (Gilles Brassard) запропонували перший протокол квантового розподілу ключів, відомий як BB84, названий так тому, що зібрав перші літери їхніх прізвищ та дату публікацій. Протокол BB84 – це криптографічна схема, за допомогою якої можна закодувати класичні біти в кубіти, він був детально проаналізований і реалізований за весь час свого існування. Крім того, було розроблено багато варіацій BB84 та інших протоколів квантового розподілу ключів. Як завжди припустимо ситуацію, що є дві сторони, «Аліса» і «Боб», які хочуть обмінятися секретним ключем і спілкуватися на відстані, але за ними стежить потенційний підслуховувач «Єва».

Ми можемо проаналізувати структуру протоколу BB84 та зрозуміти, як він влаштований (рис. 1.4). Протокол складається з двох каналів, квантового і класичного. Квантовий канал – це той, де відбувається квантова передача, а саме дві сторони готують, надсилають і вимірюють свої квантові стани. Квантовий канал не є безпечним, оскільки шахрайський користувач може отримати доступ до інформації або перервати зв'язок, використовуючи методи, засновані на квантовій механіці. Класичний канал – це коли «Аліса» та «Боб» спілкуються, надсилаючи один одному класичні повідомлення, тобто перетворюють бітові рядки, які вони отримали у квантовому каналі, у безпечні ключі. «Єва» може мати доступ до класичного каналу, тобто вона може слухати розмову, але не може змінити повідомлення, якими обмінюються «Аліса» і «Боб» [6].

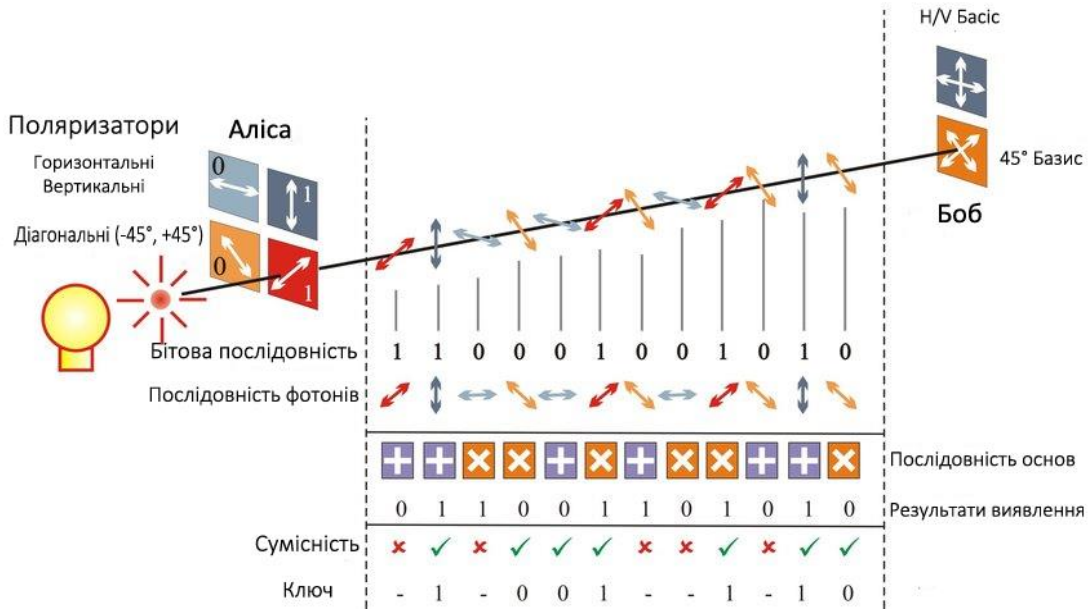

Рисунок 1.4 – Обмін ключами в протоколі BB84, реалізований за допомогою поляризації фотонів

Бази поляризації, які використовуються в BB84, є прямолінійними:

$$\oplus = \{|0\rangle, |1\rangle\} \tag{1.6}$$

і діагональний базис

$$\otimes = \{|+\rangle, |-\rangle\}, \tag{1.7}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{1.8}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1.9}$$

Ці два базиси є взаємно незміщеними, тобто коли, наприклад, при вимірюванні цього фотона, який був діагонально поляризований за допомогою прямолінійного базису, ми отримуємо абсолютно випадковий результат, тобто спостерігач не можемо витягти жодної інформації. У таблиці 1.1 продемонстровано, як можна закодувати біт у поляризації фотона.

Таблиця 1.1 – Біти кодування

Основа	Біт «0»	Біт «1»
$\oplus$	$\xrightarrow[0^o]{} \|0\rangle$	$\xrightarrow[90^o]{} \|1\rangle$
$\otimes$	$\xrightarrow[45^o]{} \|+\rangle$	$\xrightarrow[-45^o]{} \|-\rangle$

Протокол BB84 має дві фази:

Фаза №1. Квантова передача:

– «Аліса» вибирає бітовий рядок $a = (a_1, \dots, a_n)$ і випадкова комбінація основ $s \in \{\oplus,\otimes\}^n$ де $n > N$;

– «Аліса» кодує свій бітовий рядок за допомогою вибраних нею основ у поляризовані фотони і надсилає фотон «Бобу»;

– «Боб» отримує фотони «Аліси» і вибирає базис ($\oplus$ або $\otimes$) вимірює кожен з них і отримує класичні біти. Боб отримує бітовий рядок $b = (b_1, \dots, b_n)$. Ця пара $a = (a_1, \dots, a_n)$ та $b = (b_1, \dots, b_n)$ називається необробленою парою ключів.

Фаза №2. Класична пост-обробка:

– етап просіювання. «Боб» оголошує у відкритому доступі бази, які він використав. «Аліса» порівнює вибрані нею основи з основами «Боба» і вибирає випадки, у яких їхні вибори збігаються. Обидві сторони відкидають всі біти, для яких основи кодування та вимірювання відрізняються;

– крок оцінки параметрів. «Аліса» і «Боб» намагаються вгадати частку позицій і, де a і b не збігаються, тобто частоту помилок у квантовому каналі. «Боб» випадковим чином відкриває деякі біти свого ключа, і якщо немає підслуховування, то ці біти збігаються з бітами «Аліси», і вона погоджується з ними. Якщо є спроба підслуховування, то існує висока ймовірність помилки, і обидві сторони переривають протокол;

– на останньому кроці «Аліса» і «Боб» виконують узгодження інформації, тобто стирають всі помилки в своїх бітових рядках, і тому вони мають однакові рядки, а для посилення конфіденційності вони видаляють будь-яке знання про ключ, яке має підслуховувач [7].

В таблиці 1.2 приведено протокол BB84 без присутності підслуховувача.

Таблиця 1.2 – Протокол BB84 без присутності підслуховувача

Біти «Аліси»	1	0	1	0	0	1	0	1
Основа «Аліси»	⊗	⊗	⊗	⊕	⊕	⊕	⊗	⊕
Стани «Аліси»	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$
Основа «Боба»	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊕
Просіяний ключ		0			0			1

1.4.2 Протокол E91

У 1991 році був запропонований протополь квантового росподілу ключів, який базується на квантовій заплутаності, протокол E91. Ідея полягає в схемі квантового розподілу ключів за допомогою станів, які існують у квантовій заплутаності, явищі, яке було проаналізовано Ейнштейном, Подольським і Розеном. Припустимо, що у нас є пара частинок, які називаються ЕПР, і при наявності інформації про значення вимірювання однієї з них, тоді можливо отримає інформацію про значення вимірювання і для іншої. Протокол E91 QKD використовує джерело, яке виробляє пари частинок, що перебувають у стані квантової заплутаності, і ці пари розподіляються між Алісою і Бобом, двома сторонами, які спілкуються. «Аліса» і «Боб» мають доступ до класичного каналу, де вони можуть надсилати класичні повідомлення один одному і де підслуховувач може прослуховувати спілкування.

У протоколі Екерта джерело, до якого мають доступ «Аліса» і «Боб», розподіляє між ними заплутані пари кубітів, стани яких мають вигляд:

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle). \qquad (1.10)$$

Схема використовує дві різні основи $\oplus = \{|\,0\rangle, |\,1\rangle\}$ та $\otimes = \{|\,+\rangle, |\,-\rangle\}$. Протокол E91 можна описати:

– джерело виробляє пару фотонів, які знаходяться в стані квантової заплутаності, і посилає першу частинку $|\,\psi^+\rangle_A$ Алісі та другому $|\,\psi^+\rangle_B$ до Боба.

– дві сторони випадковим чином обирають один із основу $\oplus$, $\otimes$ для вимірювання частки, яку вони отримали, і записують свої вимірювання. Через класичний канал вони транслюють основу вимірювання, яку вони використовували;

– «Аліса» та «Боб» поділяють вимірювання на дві окремі групи: групу, для якої вони використовували різну основу вимірювання, і групу, яка використовувала ту саму основу вимірювання. «Аліса» та «Боб» відкидають усі вимірювання, у яких один або обидва з них взагалі не змогли зареєструвати частинку;

– перша група, де вони використовують різну основу вимірювань, може виявити підслуховувач, як якщо існує бітова помилка, підслуховувач виявленol;

– якщо «Аліса» та «Боб» впевнені, що квантовий канал безпечний, другу групу можна використовувати як необроблені ключі. Вони виконують виправлення помилок і посилення конфіденційності, щоб перетворити відсіяний ключ на спільний секретний ключ [7].

Основою є $\oplus = \{|\,0\rangle, |\,1\rangle\}$ та $\otimes = \{|\,+\rangle, |\,-\rangle\}$ і 8 кубітів, які знаходяться в стані квантової заплутаності $\frac{1}{\sqrt{2}}(|\,1\rangle\,|\,-\rangle + |\,1\rangle\,|\,+\rangle)$, $\frac{1}{\sqrt{2}}(|\,1\rangle\,|\,-\rangle - |\,0\rangle\,|\,+\rangle)$,

$\frac{1}{\sqrt{2}}(|0\rangle|-\rangle+|0\rangle|+\rangle)$, $\frac{1}{\sqrt{2}}(|1\rangle|-\rangle-|0\rangle|+\rangle)$. Реалізацію протоколу наведено в таблиці 1.3.

Таблиця 1.3 – Протокол E91

Отримані фотони	$\|1\rangle\|-\rangle$	$\|1\rangle\|-\rangle$	$\|0\rangle\|-\rangle$	$\|1\rangle\|+\rangle$
Основа «Аліси»	$\oplus$	$\otimes$	$\oplus$	$\otimes$
Заміри «Аліси»	1	0	0	1
Отримані фотони	$\|1\rangle\|+\rangle$	$\|0\rangle\|-\rangle$	$\|0\rangle\|+\rangle$	$\|0\rangle\|+\rangle$
Основа «Боба»	$\otimes$	$\otimes$	$\otimes$	$\otimes$
Виміри «Боба»	1	0	1	1
Ключ		0		1

1.4.3 Протокол B92

Пізніше у 1992 році вже самостійно тільки Чарльз Беннетт представив новий протокол квантового розподілу ключів, який також названий за його прізвищами та датою публікацій. Цей протокол по суті є варіантом протоколу BB84, з основною відмінністю в тому, що B92 використовує два стани поляризації, замість чотирьох, які використовуються в протоколі BB84. Це протокол з двома неортогональними квантовими станами, і завдяки його архітектурі можна виявити підслуховування.

Завдяки своїй спрощеній структурі B92 легше реалізується у певних типах обладнання і може бути стійкішим до деяких технічних обмежень, таких як вирівнювання базисів. Проте його менш стійка природа до шуму порівняно з BB84 вимагає додаткових засобів обробки даних, зокрема посиленої фільтрації та узгодження.

B92 – це схема QKD, яка використовує поляризовані фотони для спілкування двох сторін, «Аліси» та «Боба», через два канали. Один класичний публічний канал, до якого може отримати доступ шахрайський користувач, і один квантовий канал. Як і BB84, протокол B92 має дві фази,

квантову передачу, яка відбувається у квантовому каналі, і другу фазу, яка відбувається у класичному каналі. Етапи протоколу B92:

– «Аліса» вибирає бітовий рядок $a = (a_1, \dots, a_n)$ і кодує значення кожного біта, a_i, $i \in \{1, \dots, n\}$, 0 як $|0\rangle$ і 1 як $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$;

– «Аліса» відправляє свої кубіти «Бобу», який генерує бітовий рядок $b = (b_1, \dots, b_n)$ і вибирає основу $\oplus$ для $b_i = 0$ і основа $\otimes$ для $b_i = 1$;

– «Боб» вимірює результати і з них формує ще один бітовий рядок s: якщо Боб отримує результат –1, то i біт s дорівнює $s_i = 0$, і якщо Боб отримає результат +1, то $s_i = 1$;

– потім через публічний канал «Боб» оголошує s, а b тримає в таємниці;

– «Аліса» та «Боб» вибирають лише пари бітів $[a_i, b_i]$ для яких $s_i = 1$ [7].

Дискретний приклад реалізації протоколу B92 приведено в таблиці 1.4.

Таблиця 1.4 – Дискретний приклад реалізації протоколу B92

Відправлені біти «Аліса» (a_i)	0	0	0	0	1	1	1	1
Поляризація базісу «Аліси»	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
Вибрані біти «Боб» (b_i)	0	0	1	1	0	0	1	1
Основа «Боба»	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$
Результат виміру «Боб»	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Значення s	0	–	0	1	0	1	0	–

1.4.4 Протокол квантового розподілу ключів SARG04

У 2004 році було запропоновано новий протокол квантового розподілу ключів, варіацію протоколу BB84. SARG04 розроблений шляхом зміни

кодування інформації в BB84, щоб стати більш стійким до атак з використанням фотонно-числового розщеплення. Перша фаза протоколу SARG04 повністю збігається з першою фазою протоколу BB84, Проте протоколи відрізняються другої фазі класичної процедурі просіювання.

На другому етапі «Аліса» не оголошує базиси, як це відбувається у протоколі BB84, які вона використовує для кодування бітів. Вона обирає пару неортогональних станів для кожного надісланого кубіта і оголошує ці два стани, помічаючи, який з них правильний. Боб знає, що отриманий ним кубіт був в одному з двох станів, які оголосила Аліса. Отже, щоб дізнатися секретний біт, Боб повинен мати достатньо інформації, щоб розрізнити ці два стани. Боб проводить вимірювання і, якщо його вимірювання відповідає оголошеним станам, оголошує, що біт недійсний. Це відбувається тому, що Боб не може визначити, який з двох станів є правильним. Якщо один зі станів не відповідає його вимірам, Боб оголошує біт дійсним, оскільки він може відновити біт секретного ключа.

У протоколі SARG04 ми маємо чотири набори $a_1 = (|0\rangle, |+\rangle)$, $a_2 = (|0\rangle, |-\rangle)$, $a_3 = (|1\rangle, |+\rangle)$, $a_4 = (|1\rangle, |-\rangle)$:

– «Аліса» відправляє стан $|0\rangle$ двома фотонними імпульсами з випадково вибраного набору;

– «Аліса» показує набір $a_1 = (|0\rangle, |+\rangle)$ і записує «0» як секретний біт;

– якщо «Боб» вимірює стан в основі $\oplus = \{|0\rangle, |1\rangle\}$, можливим результатом буде $|0\rangle$.

У зв'язку з тим, що такий результат також можливий, якщо переданий стан був $|1\rangle$, «Боб» оголошує біт недійсним. Якщо «Боб» вимірює стан в основі $\otimes = \{|+\rangle, |-\rangle\}$, то він отримує $|1\rangle$ або $|\text{-}\rangle$ з ймовірністю $\frac{1}{5}$. Якщо його результат $|1\rangle$ узгоджується з обома станами і якщо є $|\text{-}\rangle$, «Боб» впевнений, що стан «Аліси» $|0\rangle$ оскільки цей результат ніколи не може бути отриманий від держави $|1\rangle$. Тоді «Боб» знає, що секретний біт дорівнює 0, і оголошує, що біт дійсний [7].

У цьому прикладі «Єва» отримує |0⟩ використовуючи $\oplus = \{|0\rangle, |1\rangle\}$ основа та заходи |+⟩ або |-⟩ з $\frac{1}{2}$ ймовірністю. Отже, вона не може визначити стан за результатом вимірювання у двофотонних імпульсах. Перевага протоколу SARG04 над протоколом BB84 полягає в тому, що відправник, «Аліса», ніколи не оголошує свої бази кодування. Отже, шахрайський користувач, «Єва», повинна зберігати більше фотонів, щоб отримати достовірну інформацію про секретні біти, а це підвищує ймовірність її виявлення.

1.4.4 Порівняльний аналіз протоколів

Протокол BB84 використовує чотири стани поляризації фотонів. Ці стани відносяться до двох взаємонезалежних баз. Пошук і виправлення помилок виконується за допомогою класичного публічного каналу, який не повинен бути конфіденційним, а лише автентифікованим. Для виявлення дій зловмисників у протоколі BB84 використовується процедура контролю помилок, а для забезпечення безумовної безпеки використовується процедура посилення конфіденційності.

E91 відноситься до протоколів QKD, що використовують заплутані стани. У цьому протоколі використовуються заплутані пари кубітів, які перебувають у синглет-стані. Перехоплення кубітів між «Алісою» та «Бобом» не дає «Єві» жодної інформації, оскільки там немає закодованої інформації. Інформація з'являється лише після того, як законні користувачі проводять вимірювання та спілкуються через класичний публічний аутентифікований канал. Проте на цей протокол все ж можливі атаки з використанням додаткових квантових систем.

Інший тип протоколів QKD – це протоколи, що використовують фазове кодування: наприклад, протокол B92, що використовує сильні опорні імпульси. Однак, при заданому рівні помилок, зловмисник може отримати

більше інформації про ключ шифрування в протоколі B92, ніж в протоколі BB84. Таким чином, безпека протоколу B92 нижча, ніж безпека протоколу BB84.

Протокол SARG04 не сильно відрізняється від оригінального протоколу BB84 . Основна відмінність стосується не «квантової» частини протоколу, а «класичної» процедури відбору ключів, яка відбувається після квантового перенесення. Таке вдосконалення дозволяє підвищити захист від атак з розділенням кількості фотонів. Протокол SARG04 на практиці має вищу швидкість генерації ключів, ніж протокол BB84.

Найпопулярнішим у застосуванні залишається протокол BB84 завдяки своїй універсальності. Інші популярні протоколи можуть показувати кращі результати в деяких ситуаціях, але вони більш складні в реалізації або мають знижену безпеку. Все це робить їх більш спеціалізованими, ефективність кожного протоколу може дуже сильно варіюватися від поставленого завдання [8].

2 КВАНТОВА КРІПТОГРАФІЯ В ОПТОВОЛОКОННИХ ЛІНІЯХ ЗВ'ЯЗКУ

2.1 Особливості оптоволоконних ліній для квантової передачі

Одним із найефективніших способів впровадження квантової криптографії є волоконно-оптичні лінії зв'язку, що забезпечують передачу з малими втратами та високу стабільність для передавання квантової інформації. Така інтеграція квантових технологій в наявні волоконно-оптичні мережі не тільки підвищує безпеку передавання даних, а й прокладає шлях для розроблення перспективних систем зв'язку, здатних протистояти навіть атакам на основі квантових комп'ютерів.

Існують кілька використовуваних стандартів на розміри оптоволокна, вимірювальну техніку і два стандарти телекомунікаційних оптичних мереж. Існують деякі особливості оптичних волокон, які необхідно враховувати під час розроблення квантових криптографічних систем.

Випромінювання поширюється у волокні завдяки наявності профілю показника заломлення поперек перерізу оптоволокна. Світло утримується у волокні за рахунок ефекту повного внутрішнього відбиття. У волокні може існувати кілька мод. Моди, по суті, є різними розв'язаннями рівняння Максвелла для хвилеводу і визначаються частотою і поляризацією світла.

Якщо серцевина досить велика, то у волокні може існувати багато хвилеводних мод. Такі волокна називають багатомодовими і діаметр їхньої серцевини зазвичай дорівнює 50 мкм. Окремий фотон взаємодіє з таким набором мод як із незамкненою системою. Отже, багатомодове волокно не є відповідним квантовим каналом. Якщо ж діаметр серцевини малий порівняно з довжиною хвилі, то у волокні поширюється одна хвилеводна мода. Одномодові волокна добре підходять для передачі одиночних фотонів. Наприклад, оптична фаза на виході волокна може стійко залежати від фази на вході. Таким чином, одномодове волокно з циліндричною симетрією може бути ідеальним квантовим каналом. Насправді оптичні волокна мають певні

порушення симетрії. Це призводить до зняття виродження мод за поляризацією і набуття ними різних постійних поширення. Подібний ефект викликається хроматичною дисперсією.

Але в одномодових волокнах виникають поляризаційні ефекти, які є джерелом помилок для будь-яких комунікаційних схем, як класичних, так і квантових. Ефект двопроменезаломлення в сучасних оптоволокнах досить малий, щоб впливати на класичний канал зв'язку, але для квантового каналу навіть дуже мале двопроменезаломлення необхідно брати до уваги. Усі реалізації квантового зв'язку, засновані на оптоволокні, стикаються з цією проблемою. Облік поляризаційних ефектів важливий не тільки для систем, заснованих на кодуванні поляризації, а й для систем, заснованих на кодуванні фази. Розглянемо основні чотири поляризаційні ефекти. ефект геометричної фази, двопроменезаломлення, дисперсію мод за поляризацією, залежність втрат від поляризації.

1. Ефект геометричної фази. Геометрична фаза виникатиме при адіабатичній зміні параметрів системи, що здійснює рух по циклу. Під час поширення поляризованого світла волокном, замкнутим у петлю, адіабатичній зміні піддається хвильовий вектор. Наприклад, якщо у волокно ввести вертикально поляризоване світло, то чи збережеться на виході напрямок поляризації? У принципі можна простежити зміну лінійної поляризації вздовж такого волокна і визначити кут, на який повертається вектор поляризації. Якщо петля залишається на площині, то поляризація не змінюється. Якщо ж петля замикається внаслідок тривимірної конфігурації, то під час паралельного перенесення поляризація змінюється на величину окресленого тілесного кута, яка і є геометричною фазою. Схожі міркування зберігаються і для еліптичної поляризації. У міру поширення дві кругові поляризації, що є власними станами, набувають протилежних геометричних фаз. Наявність геометричної фази не є критичною для квантової комунікації. Для її подолання Алісі та Бобу необхідно спочатку повернути свої системи на деякий кут. Якщо зміни геометричної фази відбуваються повільно, то їх

можливо відстежити і ввести в схему комунікації за допомогою активного зворотного зв'язку. Однак якщо зміни відбуваються занадто швидко, то зв'язок може бути перервано.

2 Двопроменезаломлення. Навіть одномодовий хвилевід, строго кажучи, не є одномодовим, оскільки він може підтримувати дві вироджені моди, що переважно поляризовані у двох ортогональних напрямках. За ідеальних умов досконалої циліндричної геометрії та ізотропії речовини ортогонально поляризовані моди не взаємодіють. Однак у реальних умовах малі відхилення від циліндричної геометрії або малі флуктуації в анізотропії речовини призводять до змішування двох поляризаційних станів, знімаючи виродження мод. Постійні поширення стають різними для мод, поляризованих у *x*- і *y*-напрямках. Ця властивість називається двопроменевим заломленням мод. Існують оптоволокна, що зберігають стан поляризації. У них навмисно створюється сильне двопроменезаломлення, так що малі випадкові флуктуації двопроменезаломлення істотно не впливають на поляризацію світла. Один зі способів створення сильного двопроменезаломлення полягає в порушенні циліндричної симетрії та створення оптоволокон з еліптичною формою серцевини або підкладки. В іншому методі двопроменезаломлення викликається статичними пружними напруженнями. Якщо ефект двопроменезаломлення є стійким у часі, то «Аліса» і «Боб» можуть його компенсувати. Так, ефект двопроменезаломлення є схожим з ефектом геометричної фази і на додаток до нього може впливати на еліптичність світла. Стійкість ефекту вимагає повільної зміни температурного режиму і механічних напружень.

3 Дисперсія мод за поляризацією призводить до наявності двох різних групових швидкостей для ортогонально поляризованих мод. Дві групові швидкості локально створюються двопроменевим заломленням. В оптичних волокнах локальна дисперсія приблизно дорівнює фазовій дисперсії. За порядком вона становить кілька пікосекунд на кілометр. Оптичний імпульс локально розподіляється за «швидкою» і «повільною»

модою. Але оскільки двопроменезаломлення мале, ці моди слабо взаємодіють. Навіть малі неоднорідності у хвилеводі спричиняють перекачування енергії зі швидкої моди в повільну і навпаки. Дисперсія мод за поляризацією схожа з випадковим блуканням і наростає пропорційно квадратному кореню з довжини волокна. Довжина взаємодії мод варіюється від декількох до сотень метрів залежно від типу волокна. За сильної взаємодії мод зменшується дисперсія мод за поляризацією, оскільки моди не встигають далеко піти одна від одної. У сучасних оптоволокнах взаємодія мод збільшується штучно в процесі виготовлення. Дисперсія поляризації описується статистичним розподілом затримок. Спричинена цим ефектом деполяризація схожа з процесом втрати когерентності. Щоб уникнути цього ефекту, у квантових каналах зв'язку використовують лазерні імпульси з часом когерентності більшим, ніж найбільший із часів затримки.

4 Залежністю втрат від поляризації можна знехтувати для оптоволокон, але вона може виявитися суттєвою в таких оптичних компонентах, як фазові модулятори. Зокрема, деякі оптичні хвилеводи підтримують тільки одну поляризацію. Сама по собі залежність втрат від поляризації є стійкою, але в разі накладення двопроменезаломлення можуть виникнути флуктуації. Залежність втрат від поляризації не описується унітарним перетворенням у просторі станів поляризації. Також не зберігається скалярний добуток. Зокрема, неортогональні стани можуть перейти в ортогональні з деякими втратами. Зазначимо, що ця обставина може бути використана для перехоплення інформації [9].

2.2 Особливості квантових розподілів ключів для оптоволоконних ліній

Технічні особливості використовуваних засобів і каналів зв'язку призводять до необхідності внесення змін в описані раніше протоколи для того, щоб зробити їх безпечними.

З технологічного погляду надзвичайно важко створити імпульс світла, що містить тільки один фотон. Набагато легше створити когерентний імпульс, що є суперпозицією квантових станів з 0, 1, 2 ... фотонами. Якщо середнє число фотонів в імпульсі досить мале: $\mu \ll 1$, то існує ймовірність порядку $\mu^2/2$ того, що перехоплювач зможе розділити імпульс на два і більше фотонів, виміряти один із них, пропускаючи інші до «Боба». Це дасть йому змогу дізнатися фіксовану частку тих бітів, які є в «Аліси» і у «Боба», без внесення будь-яких помилок. Така індивідуальна атака має назву атаки ділення числа фотонів (ДЧФ-атаки), і основне завдання полягає у визначенні самого факту наявності такої атаки.

Розглянемо ситуацію «Аліса» використовує в протоколі BB84 імпульси, що містять одиничний фотон з імовірністю 90 %, а більшу кількість фотонів – з імовірністю 10 %. Крім того, невідомо, коли саме випускаються кілька фотонів замість одного. Приймемо також, що втрати каналу передавання l дорівнюють, наприклад, 90 % або що він має пропускну спроможність, у, рівну 10 %. Тут $y = 1 - l$ і y відповідає p_{exp} у роботі. Приймемо також, що «Боб» використовує доступні на практиці детектори, які не розрізняють число фотонів. Метод перехоплення, який використовує «Єва», такий: вона вимірює кількість фотонів у кожному імпульсі і блокує імпульси з одним фотоном. Коли фотонів більше, вона ділить сигнал, залишаючи собі одну частину, і відправляючи другу через ідеальний канал «Бобу». Як зазвичай, припускається, що «Єва» має необмежені технологічні та обчислювальні здібності, обмежені лише законами природи. Тоді «Боб» спостерігає, як і очікується, лише 10 % імпульсів. Однак Єва може отримати повну інформацію про ключ, вимірюючи кожен зі збережених фотонів у відповідному базисі, інформація про який передається незахищеним каналом «Алісою». Для стратегії Єви ми приймаємо, як зазвичай, найсприятливіше для неї припущення – усі багатофотонні імпульси використовуються для ДЧФ-атаки. У цьому випадку можна бачити, що якщо пропускна спроможність у менша за ймовірність генерації сигналу з більшим за

одиницю числом фотонів p_{multi}, протокол повністю відкритий для перехоплення за допомогою ДЧФ-атаки. Інакше кажучи, для забезпечення безпеки протоколу пропускна здатність у має перевищувати ймовірність генерації сигналу з числом фотонів, більшим за одиницю, p_{multi}:

$$y > p_{multi}. \tag{2.1}$$

2.3 Квантовий зв'язок в існуючій волоконно-оптичній мережі

Усі вимоги до оптичного аолокуну для квантового зв'язку мають на увазі, що потребуватимуть абсолютно нової інфраструктури, але сучасні дослідження продемонстрували, що насправді є можливість інтегрування квантової системи зв'язку в наявні сьогодні оптоволоконні мережі.

Оптоволоконна інфраструктура і телекомунікаційні технології, що лежать в основі Інтернету, широко використовуються дослідниками, які прагнуть розробити квантові мережі, здатні до таких застосувань, як квантово-розширена криптографія, зондування і мережеві квантові обчислення. Однак, оскільки більшість існуючої оптоволоконної інфраструктури заповнена звичайним телекомунікаційним трафіком, а також через економічну вартість оренди або встановлення нового волокна, можливість реалізації квантових мереж у великих масштабах буде залежати від здатності поширювати квантові сигнали в тому ж самому волокні, що і класичні сигнали високої потужності.

Квантові і класичні сигнали можуть легко передаватися по одному волокну за допомогою мультиплексування з поділом по довжині хвилі. Однак, вперше було показано, що шумові фотони від непружного розсіювання потужного класичного світла можуть заважати виявленню квантових сигналів, часто на субфотонному рівні. Серед потенційних джерел шуму спонтанне комбінаційне розсіювання є найбільш домінуючим завдяки своєму широкосмуговому спектру, а це означає, що шум ніколи не можна

повністю запобігти. Без ретельного проектування виникає компроміс між можливостями звичайних і квантових мереж.

Вивчення квантово-класичного співіснування має довгу історію з багатьма експериментами, проведеними для додатків з використанням джерел слабких когерентних станів, заплутаних пар фотонів, вимірювань стану Белла на слабких когерентних станах, неперервних змінних і стисненого світла. Хоча в цих дослідженнях були досягнуті значні досягнення і розуміння, всі експерименти на сьогоднішній день були зосереджені на системах, які безпосередньо передають квантову інформацію між вузлами мережі. Однак багато квантових додатків наступного покоління потребують безтілесної передачі квантових станів між користувачами. Завдяки нелокальним властивостям квантової заплутаності, квантова телепортація дозволяє передавати квантовий стан між двома віддаленими фізичними системами без необхідності прямої передачі. Вона відіграє фундаментальну роль у таких передових додатках, як квантові реле, квантові ретранслятори, мережеві квантові комп'ютери та інші додатки у квантовій науці і техніці.

Концептуальну схему показано на рисунку 2.1. «Аліса» генерує один фотон для кодування квантового стану (1.3) що вона хоче телепортувати до «Боба». Фотон «Аліси» мультиплексується в оптичне волокно довжиною L_{AC} для спільного поширення з класичним сигналом зв'язку до вузла вимірювання стану дзвону в Чарлі. Класичний сигнал демультиплексується безпосередньо перед вимірюванням стану дзвону, а потім знову мультиплексується, щоб обійти вузол Чарлі. Після цього класичний сигнал рухається по іншому волокну довжиноюL_{BC}, зустрічно поширюється відносно одного фотона із заплутаної пари фотонів у стані дзвона, що генерується у вузлі «Боба». Під час вимірювання дзвонового стану у Чарлі обидва фотони незворотно знищуються детектуванням, тоді як інший фотон Боба із заплутаної пари проектується на стан $|\varphi\rangle_B = \sigma\,|\varphi\rangle_A$, де σ – унітарна операція, яка є унікальною для результату вимірювання стану дзвоника і

може бути класично передана «Бобу» для відновлення стану «Аліси» або фізичним застосуванням унітарної операції, або врахуванням її при постобробці даних [10].

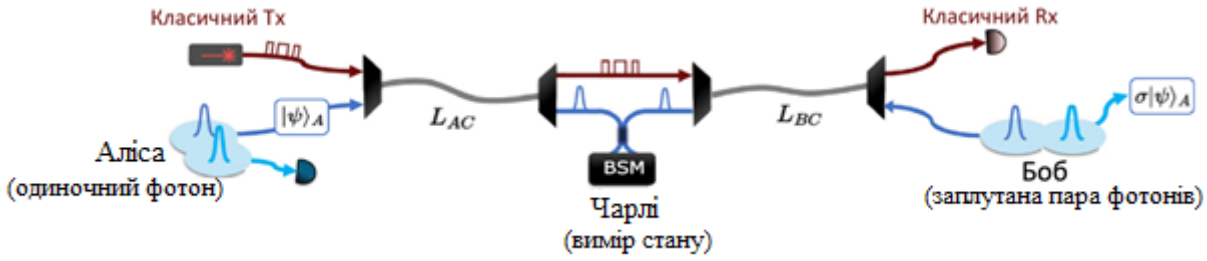

Рисунок 2.1 – Квантова кріптографія в оптоволоконних лініях зв'язку

2.4 Затуханя сигналу та збереження поляризації у волокні

Надзвичайно низьке загасання або втрати при передачі в оптичних волокнах є одним з найважливіших факторів, що зумовили їх широке визнання як середовища передачі. Передача сигналу в оптичних волокнах, як і в металевих провідниках, зазвичай позначається абревіатурою *dB*. Децибел (*dB*) є зручним способом порівняння двох різних рівнів потужності, наприклад, P_1 і P_2. Він визначається як:

$$dB = 10\log_{10}\frac{P_1}{P_2}. \tag{2.1}$$

Загасання оптичного волокна є вимірюванням втрати світла між входом і виходом. Загальне загасання є сумою всіх втрат. Отже, це сума поглинання матеріалу, розсіювання Релея у волокні та недосконалості хвилеводу. Є й інші фактори, які також можуть спричинити втрату світла, наприклад витік світла, коли волокно піддається мікрозгинанню. Загасання обмежує відстань, яку сигнал може пройти по волокну, перш ніж він стане занадто слабким для виявлення.

Будь-який матеріал поглинає світло на певних довжинах хвиль, що відповідають електронним і коливальним резонансам, пов'язаним з конкретними молекулами. Для молекул кремнезему електронні резонанси відбуваються в ультрафіолетовій області (довжина хвилі < 0,4 мкм), тоді як коливальні резонанси відбуваються в інфрачервоній області (довжина хвил $\lambda > 7$ мкм). Через аморфну природу плавленого кремнезему ці резонанси мають форму смуг поглинання, хвости яких простягаються в видиму область. На рисунку 2.2 показано, що внутрішнє поглинання матеріалу для кремнезему в діапазоні довжин хвиль від 0,8 мкм до ~1,6 мкм становить менше 0,1 дБ/км. Фактично, воно становить менше 0,03 дБ/км в діапазоні довжин хвиль від 1,3 до 1,6 мкм, який зазвичай використовується для систем світлових хвиль [11].

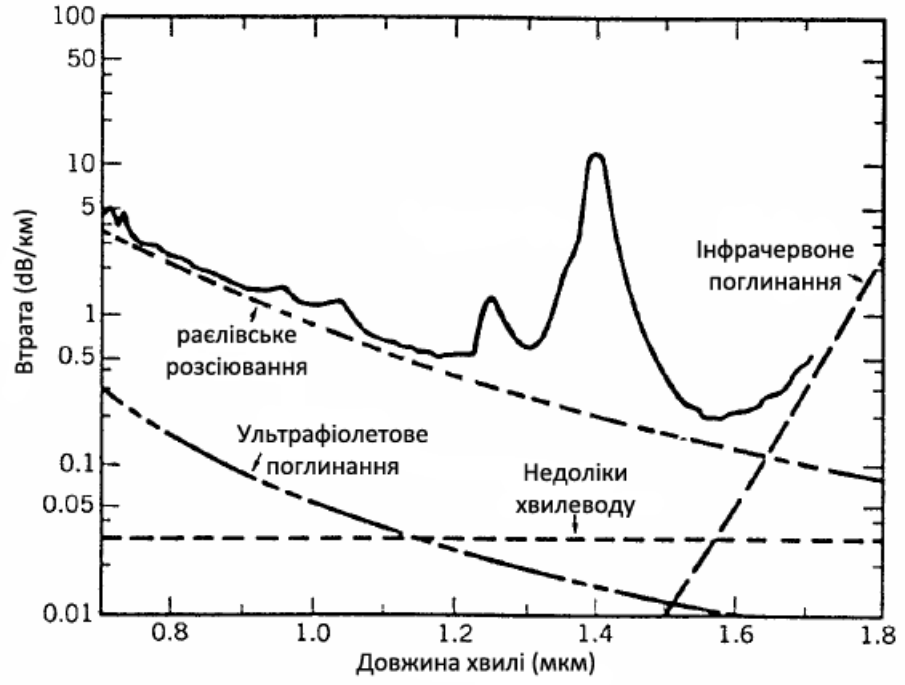

Рисунок 2.2 – Графік загасання сигналу у волокні

Оптичні волокна завжди виявляють певний ступінь двопроменезаломлення, навіть якщо вони мають кругово симетричну конструкцію, оскільки на практиці завжди існує певний механічний стрес або

інший ефект, який порушує симетрію. Як наслідок, поляризація світла, що поширюється у волокні, поступово змінюється неконтрольованим чином, що також залежить від будь-якого вигину волокна та його температури.

Зазначену проблему можна вирішити за допомогою волокна, що зберігає поляризацію, яке не є волокном без двопроменезаломлення, а навпаки, спеціальним волокном із сильним вбудованим двопроменезаломленням. За умови, що поляризація світла, що запускається в волокно, вирівняна з однією з осей двозаломлення, цей стан поляризації буде збережений навіть у разі вигину волокна. Фізичний принцип, що лежить в основі цього, можна зрозуміти з точки зору когерентного з'єднання режимів. Постійні поширення двох режимів поляризації значно відрізняються через сильне двозаломлення, так що відносна фаза таких режимів, що поширюються разом, швидко зміщується. Тому будь-яке порушення вздовж волокна може ефективно з'єднати обидва режими тільки в тому випадку, якщо воно має значну просторову компоненту Фур'є з хвильовим числом, яке відповідає різниці констант поширення двох режимів поляризації. Якщо ця різниця достатньо велика, звичайні порушення у волокні змінюються занадто повільно, щоб забезпечити ефективне з'єднання режимів. У кількісному вираженні довжина поляризаційного биття повинна бути значно коротшою за типову довжину, на якій змінюється паразитна двопроменезаломлення.

Поширеним методом отримання сильного двозаломлення є включення двох (не обов'язково циліндричних) стрижнів напруги зі зміненим складом скла (зазвичай це скло, леговане бором, з іншим ступенем теплового розширення) у преформу з протилежних боків серцевини (рис. 2.3). Коли волокно (так зване волокно PANDA) витягується з такої преформи, елементи напруги викликають певне механічне напруження з чітко визначеною орієнтацією. За допомогою інших технік можна виготовляти волокна типу «метелик», де елементи напруги мають іншу форму і наближаються до серцевини волокна, що дозволяє досягти сильнішого двозаломлення. Інший варіант цього підходу полягає в тому, щоб навколо серцевини мати еліптичну

оболонку з іншого скла; це призводить до отримання волокна з еліптичним шаром напруги. Можна також поєднувати обидва методи.

Рисунок 2.3 – Волокно PANDA, що зберігає поляризацію (ліворуч), та волокно «метелик» (праворуч). Вбудовані елементи напруги, виготовлені з іншого типу скла, показані темнішим сірим кольором

Інша техніка, яка не покладається на механічне навантаження, полягає у використанні еліптичного сердечника, що викликає так зване формове двозаломлення. Тут сама еліптична форма, навіть без будь-якого механічного навантаження, створює певний рівень формового двозаломлення.

У фотонному кристалічному волокні дуже сильне двозаломлення можна отримати за допомогою асиметричного розташування повітряних отворів, але також можна використовувати елементи напруги. У будь-якому випадку довжина поляризаційного биття може бути настільки малою, що додаткові ефекти напруги можуть спричинити лише низький рівень змішування станів поляризації. Контраст індексу може бути в кілька разів більшим за 10^{-3}, тоді як у повністю скляних PM-волокнах він зазвичай становить лише кілька разів 10^{-4} [12].

3 РЕАЛІЗАЦІЯ В ВІДКРИТИХ ЛІНІЯХ ЗВ'ЯЗКУ

3.1 Особливості відкритих ліній для квантової передачі

Фотони, що поширюються у відкритому просторі, не зазнають явища двопроменезаломлення. Тому ці середовища краще, ніж оптоволокно підходять для поляризаційного кодування. Однак атмосфера призводить до інших шумових впливів.

Відкритий простір надає широкі можливості для передачі фотонів різних довжин хвиль, будучи альтернативою оптичному волокну. В якості генераторів і приймачів випромінювання в даному випадку також використовуються лазери і фотодетектори. Сучасні системи бездротової передачі даних здатні передавати світлові сигнали на відстань у кілька кілометрів зі швидкістю до 160 Гбіт/с.

Як і у випадку з оптичним волокном, найбільша ефективність передавання досягається для фотонів певних енергій, як показано на рисунку 3.1.

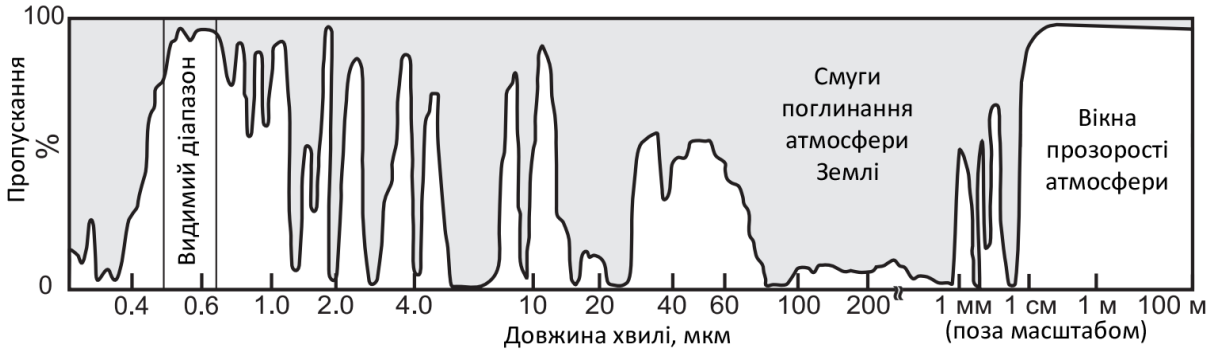

Рисунок 3.1 – Прозорість земної атмосфери для випромінювання різної довжини хвилі

Найпрозорішою є земна атмосфера для випромінювання з довжиною хвилі понад 1 см. На жаль, практична реалізація протоколів квантової криптографії з використанням фотонів сантиметрового діапазону неможлива через малу величину енергії фотона і, отже, неможливість його ефективного

детектування, тому найвідповіднішими є два спектральні вікна: від 0,3 мкм до 1,3 мкм та від 1,5 мкм до 1,8 мкм, тим паче, що генератори й приймачі фотонів у даних діапазонах добре розроблені й широко застосовуються під час передачі фотонів за допомогою оптичного волокна.

Під час передання фотонів через атмосферу існують чотири основні види втрат:

– дифракційні втрати призводять до збільшення діаметра світлового пучка зі збільшенням відстані передач;

– статичні атмосферні втрати виникають і за відсутності турбулентності атмосфери і являють собою процеси розсіювання і поглинання корисного сигналу. Причому дощ або легкий туман ускладнює, або навіть унеможливлює передачу сигналу. Загасання сигналу в цьому разі залежить також і від кута його поширення відносно зеніту і змінюється від 3 % до 5 % при зміні кута від 0º до 50º;

– турбулентність атмосфери може призводити до низки негативних ефектів: збільшення діаметра світлового пучка подібно до того, як це відбувається внаслідок дифракційних втрат, відхилення світлового пучка, когерентні втрати, коливання інтенсивності пучка близько його середнього значення;

– оптичні втрати пов'язані з використанням телескопів для приймання-передавання сигналу: діаметр прийнятого пучка може бути надто великим, унаслідок чого можливі втрати.

У разі поодиноких фотонів додатковою проблемою є фонове випромінювання, тому важливим елементом практичних схем є синхронізація між приймачем і передавачем, щоб фотодетектор вмикався тільки на короткий час у момент приходу чергового фотона для зменшення ймовірності реєстрації сторонніх фотонів.

Очевидно, що слабкі однофотонні сигнали будуть значною мірою схильні до описаних перешкод, тому різко знизиться швидкість і відстань ефективної передачі. Щоб розв'язати цю проблему, було запропоновано

схеми квантової криптографії, що використовують супутники на різних орбітах від 300 км до 30 000 км. Ефективність передачі в даному випадку зростає через те, що щільність атмосфери падає з ростом висоти над Землею, і втрати при досягненні фотоном супутника, що знаходиться на 300-кілометровій орбіті, можна порівняти з втратами при проходженні від 10 км до15 км біля поверхні планети. На сьогоднішній день кільком групам вже вдалося досить ефективно передати поодинокі фотони у відкритому просторі на 7,8 км і 13 км [9].

3.2 Затуханя сигналу в відкритому просторі

Розглянемо відповідні ефекти для властивостей передачі в оптичному спектрі від 500 нм до 2 мкм. Це поглинання та розсіювання аерозолями, пов'язаними з поверхнею землі (нижче 10 км висоти), та аерозолями вулканічного попелу (вище 10 км), розсіювання біполярними молекулами (так зване розсіювання Релея) та частотно-специфічне поглинання фотонів різними молекулами та їх ізотопами. В результаті отримуємо чотири ефекти ослаблення сигналу, які необхідно підсумувати для оцінки загальної пропускання. Програми моделювання дозволяють обчислити різні коефіцієнти ослаблення для певної висоти та моделі. Коефіцієнт ослаблення в 1/км визначає силу поглинання в певному місці (визначеному його висотою над рівнем моря) та на певній частоті. Існують різні визначення пропускання, що відносяться до коефіцієнта ослаблення α з натурального логарифму та а з декадного логарифму. Загальна частка пропускання T ($0 < T < 1$) оптичної потужності через довжину атмосферного шляху L розраховується відповідно до закону Бера-Ламберта:

$$T = e^{-\int_0^L a(h)dz}, \tag{3.1}$$

$$T = 10^{-\int_0^L a(h)dz}. \tag{3.2}$$

Коефіцієнт α пов'язаний з десятичним коефіцієнтом загасання a за формулою $a = \alpha \log 10e \approx 0{,}4343 \cdot \alpha$:

$$A[dB] = 10 \log_{10} e^{-\int_0^L a(h)dz} \approx -4{,}343 \times \int_0^L a(h)dz. \quad (3.3)$$

Ефект молекулярного поглинання базується на здатності молекули поглинати фотони на різних рівнях енергії електронів. Ці енергетичні рівні дещо змінюються за положенням і шириною залежно від температури, тиску та ізотопу елемента. Розширення під тиском і температурою на нижчих висотах призводить до спектрально ширших ліній молекулярного поглинання, як зображено на прикладі лінії CO_2 на рисунку 3.2. Тут спектральна ширина поглинання на землі.

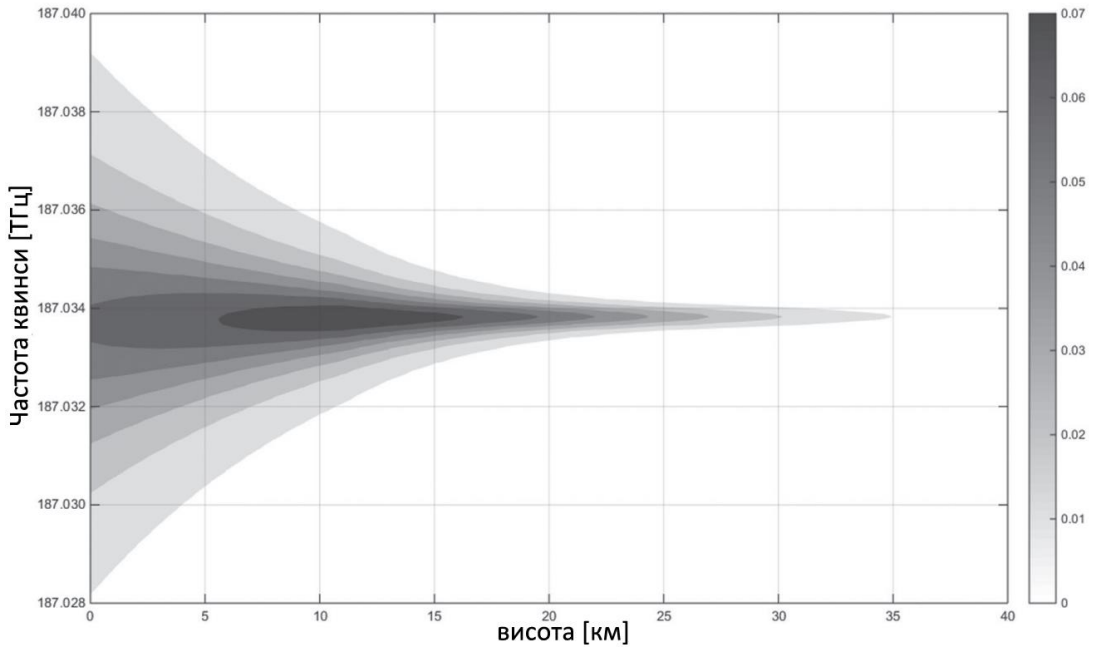

Рисунок 3.2 – Приклад залежності однакового коефіцієнта поглинання від висоти від розширення тиску і температури

Рівень становить близько 5 ГГц, а на висоті понад 20 км він знижується до рівня нижче 1 ГГц. В результаті цих ефектів коефіцієнт спектрального

поглинання на осі є найвищим на висоті від 6 км до 16 км. Найбільш релевантними молекулами в нашому спектральному діапазоні, що нас цікавить, є H_2O і CO_2. На рисунку 3.3 зображено типові форми коефіцієнтів поглинання на висоті 3 км.

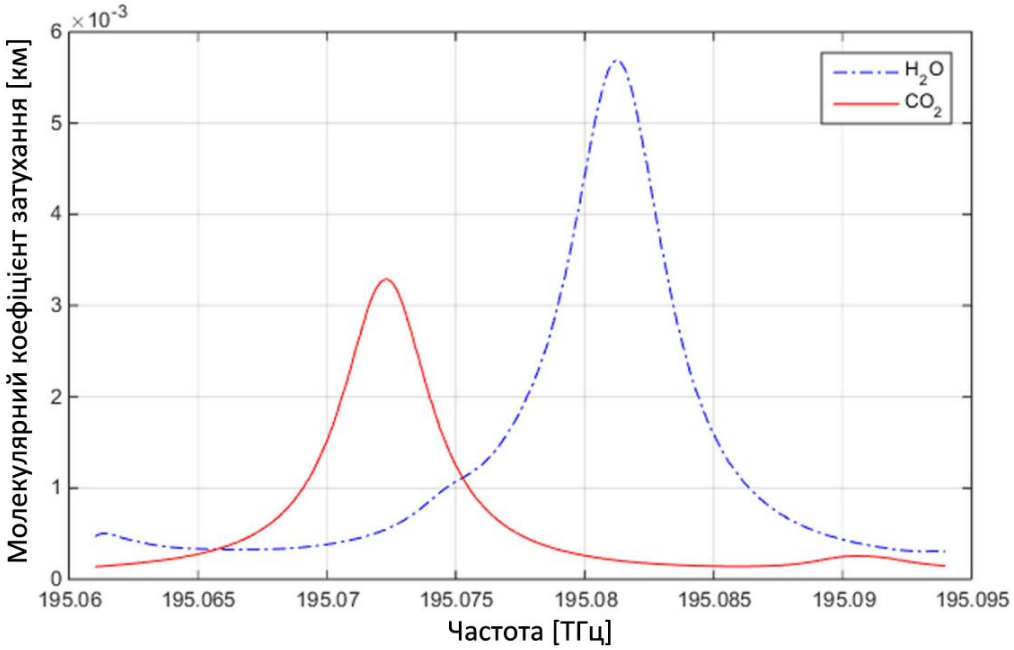

Рисунок 3.3 – Коефіцієнти поглинання двох типових ліній поглинання, водяною парою та вуглекислим газом, обидві на висоті 3 км

Хоча об'ємне співвідношення CO_2 залишається досить постійним на різних висотах, кількість води різко зменшується з висотою. На рисунку 3.4 показано об'ємне співвідношення молекул H_2O залежно від висоти. Більшість молекул води присутні нижче 10 км, і їх кількість значно вища для тропічних атмосферних моделей порівняно з іншими. На рисунку показано об'ємне співвідношення інших молекул (N_2, O_2, CO та CO_2). Для деяких типів молекул об'ємне співвідношення не змінюється істотно з висотою, як у випадку з CO_2 або O_2.

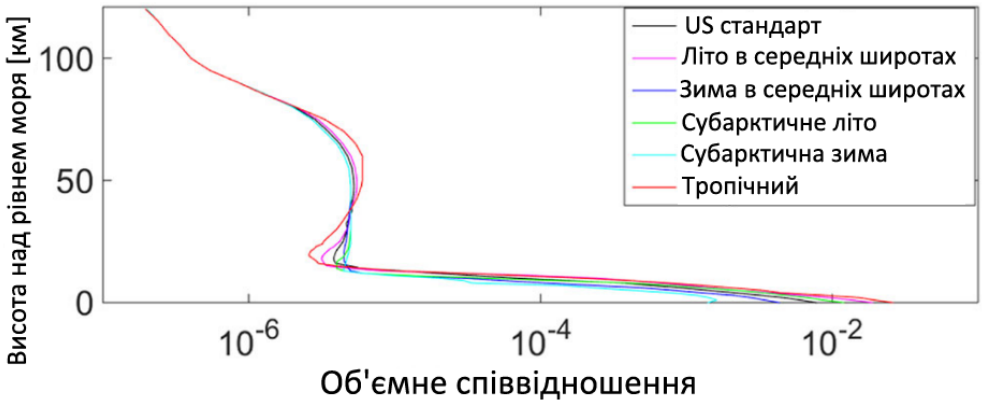

Рисунок 3.4 – Об'ємне співвідношення молекул H2O залежно від висоти над рівнем моря для різних атмосферних моделей

На рисунку 3.5 показано суму всіх коефіцієнтів молекулярного поглинання на рівні моря для різних частот. Періодичні максимуми молекулярних ліній поглинання, спричинені головним чином водяною парою та вуглекислим газом (від 900 нм до980 нм; від 1110 нм до1160 нм; від 1330 нм до 1520 нм; від 1760 нм до 1990 нм тощо), чергуються з вікнами пропускання (рис. 3.6). Видима область «A», 740–810 нм «B», 836–890 нм «C», 990–1080 нм «D», 1220–1300 нм «E», 1530–1690 нм «F». На щастя, спектри пропускання оптичних високошвидкісних волоконно-оптичних систем передачі майже збігаються з одним з атмосферних вікон «F», що робить ці компоненти найбільш корисними для оптичної передачі через атмосферу [9].

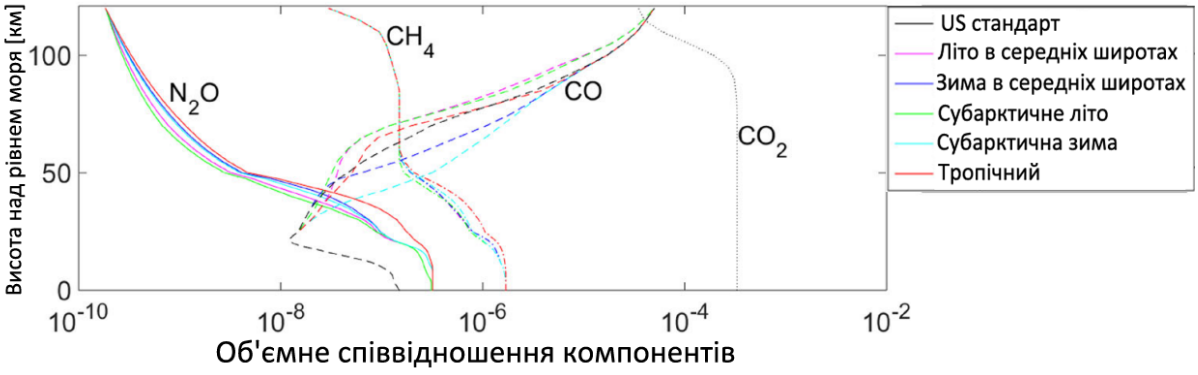

Рисунок 3.5 – Об'ємне співвідношення N2O, CH4, CO та CO2 залежно від висоти над рівнем моря для різних атмосферних моделей

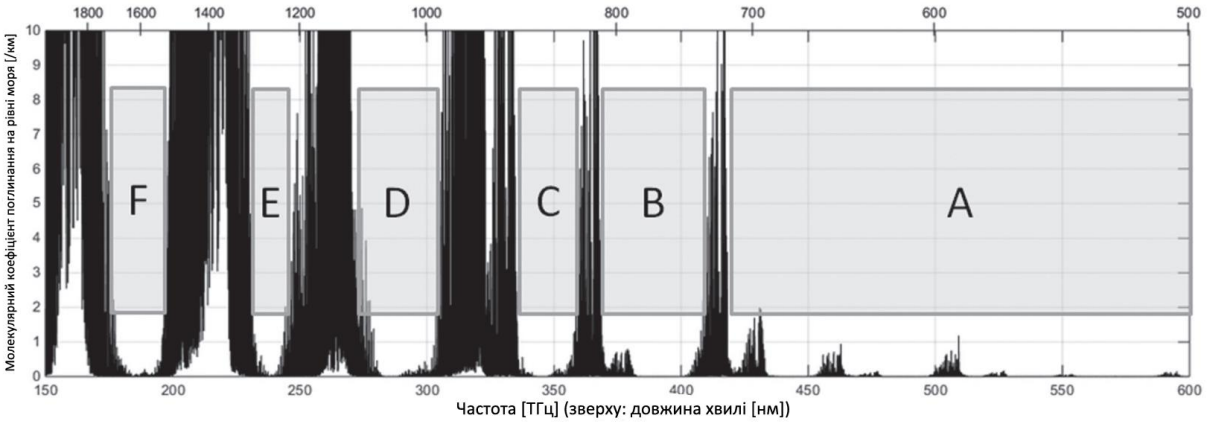

Рисунок 3.6 – Спектр суми всіх коефіцієнтів молекулярного поглинання на рівні моря, що визначає типові вікна пропускання лазерного випромінювання. Не враховується поглинання та розсіювання аерозолів

3.3 Досягнення в області квантової криптографії

Як видно з попередніх досліджень, квантова криптографія розвивається у двох напрямках: оптоволоконних і відкритих систем зв'язку. Обидва підходи мають переваги і обмеження, на наш погляд, перспективним є метод, який об'єднує обидва підходи. Сьогодні розвиваються нові методи, які демонструють приклад використання для побудови з'єднань для квантового розподілення ключів у міських умовах на коротких відстанях, де прокладання нового оптичного волокна є надто дорогим, щоб бути практичним, наприклад, «між будівлями в міських районах або через дороги загального користування». Квантовий розподіл ключів в оптичному волокні безперешкодно з'єднується з оптичною бездротовою технологією, де закодовані інфрачервоні, ультрафіолетові або видимі світлові сигнали передаються на короткі відстані у вільному просторі, зберігаючи при цьому квантове шифрування.

Прикладом такого застосування є тест, проведений 19 березня 2024 року японські компанії Toshiba Digital Solutions Corp. і SoftBank Corp. оголосили про демонстрацію інтеграції безпечних квантових комунікацій з

короткостроковою оптичною бездротовою комунікацією. У спільному прес-релізі компанії заявили, що продемонстрована конфігурація, в якій система квантового розподілу ключів Toshiba була розгорнута в оптичному бездротовому тестовому середовищі SoftBank, забезпечила «новий, економічно ефективний і своєчасний метод розгортання безпечних мереж квантового розподілу ключів в міських умовах».

Демонстрація була організована шляхом підключення передавача та приймача Toshiba QKD до оптичного бездротового тестового середовища, яке вже було розгорнуто в SoftBank. У ході подальших випробувань обидві компанії підтвердили, що стабільні квантові ключі можуть бути згенеровані та передані через систему, навіть якщо оптична бездротова передача була включена до ланцюга, схема показана на рисунку 3.7.

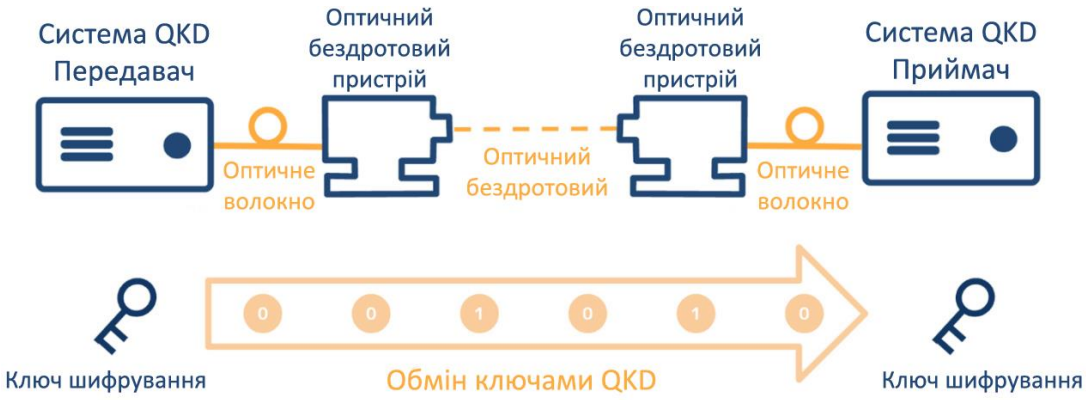

Рисунок 3.7 – Схема гібридної оптично-волоконної/оптично-бездротової установки

Саме такі гібридні оптоволоконні/оптико-бездротові системи можуть виявитися перспективним напрямком для практичного розгортання ліній квантової передачі даних.

Були встановлені рекорди з швидкості безперервного безпечного ключа для системи QKD, яка становить 13,7 Мб/с на відстані 10 км по оптоволокну. Компанія Toshiba досягла найвищої в світі швидкості розподілу квантових ключів, розробивши високошвидкісні детектори та електроніку для

реєстрації фотонних сигналів, а також нові, більш швидкі методи постобробки сигналів для отримання секретного ключа. Нові методи включають реалізацію етапів виправлення помилок та посилення конфіденційності в апаратному забезпеченні, що значно покращує швидкість постобробки та долає вузьке місце в поточних програмних реалізаціях.

Крім того, був продемонстрований новий протокол під назвою Twin-Field QKD, який дозволяє розширити діапазон зв'язку до понад 500 км оптоволокна. Це забезпечує захист конфіденційних даних, що передаються в оптичних мережах між містами, дозволяючи створити безпечний зв'язок між такими містами, як Лондон, Париж, Брюссель, Амстердам і Дублін.

У Twin-Field QKD світлові імпульси надсилаються з обох кінців волокна до центрального місця, де відбувається детекція фотона. За умови, що неможливо визначити, з якого кінця волокна прийшов фотон, ця техніка ефективно подвоює відстань передачі при заданій швидкості. Хоча традиційні системи можна з'єднати між собою для збільшення загальної відстані передачі, це вимагає, щоб проміжні станції знаходилися в безпечному місці. На відміну від цього, для безпеки Twin-Field QKD не потрібна фізична охорона центрального місця. Це дозволило б, наприклад, банку в Лондоні переміщати надзвичайно конфіденційні дані клієнтів до центру обробки даних в Лідсі в межах існуючої традиційної оптоволоконної мережі без побоювання, що дані будуть скомпрометовані.

Також були передові досягнення в галузі технології активної стабілізації, яка дозволяє системі безперервно розподіляти ключовий матеріал навіть у найскладніших умовах експлуатації без втручання користувача. Це дозволяє уникнути необхідності повторної калібрування системи через зміни довжини волокон, викликані температурою.

Ініціювання системи продемонстрована на рисунку 3.8, також здійснюється автоматично, що забезпечує просту експлуатацію «під ключ». Система успішно продемонструвала свою ефективність у ході декількох польових випробувань у мережі. Система може використовуватися для

широкого спектру криптографічних застосувань, наприклад, для шифрування або автентифікації конфіденційних документів, повідомлень або транзакцій. Програмний інтерфейс надає користувачеві доступ до ключового матеріалу.

Система також проста в управлінні, запуск здійснюється автоматично, а інтуїтивно зрозумілий інтерфейс програмування надає користувачеві доступ до ключових матеріалів. Технологія включає в себе передову технологію активної стабілізації, яка дозволяє системі безперервно розподіляти ключовий матеріал навіть у найскладніших умовах експлуатації без втручання користувача. Це дозволяє уникнути необхідності повторної калібрування системи через зміни довжини волокон, викликані температурою [13, 14].

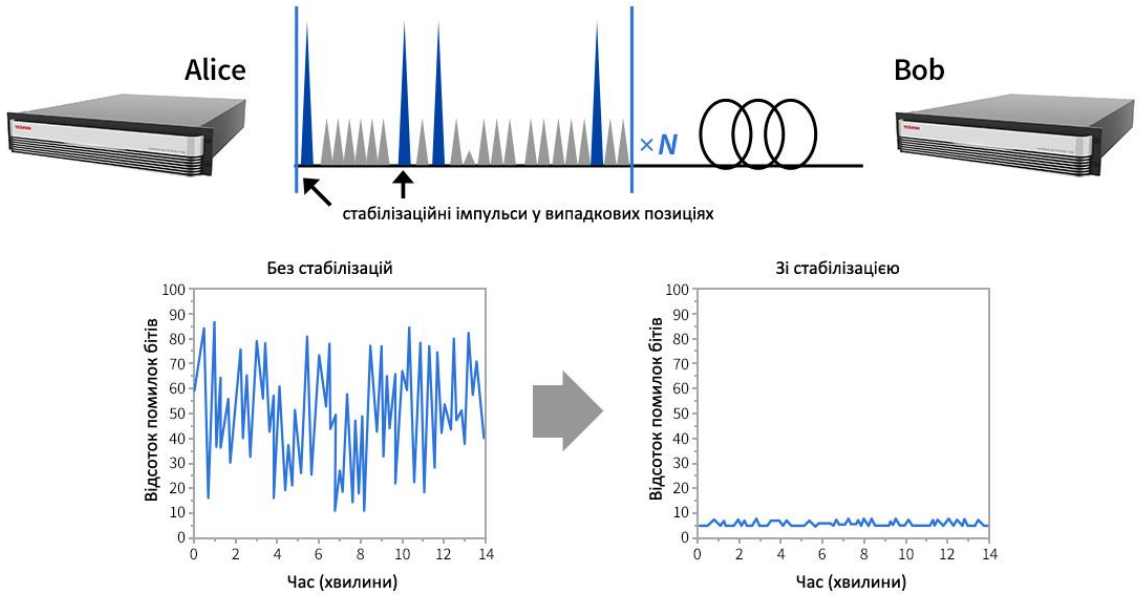

Рисунок 3.8 – Стабільність розподілу квантового ключа з високою швидкістю передачі даних на встановленому волокні

ВИСНОВКИ

Розкриваючи тему кваліфікаційної роботи, було опрацьовано тематичну літературу і інші інформаційні джерела, які поглиблюють знання, розширюють можливості сприйняття та засвоєння матеріалу. Створення необхідної бази знань, є най необхіднішим процесом навчання.

У виконаній кваліфікаційної роботі, була досягнута мета – визначено дослідження принципів квантовой криптографій, та їй використаня в оптично волоконних та відкритих системах звязку, а також тенденції розвитку систем квантової криптографії.

Для досягнення мети були вирішені такі завдання як, дослідження фізико-математичні основи квантової криптографій. Проаналізовані особливості використаня квантовой криптографій в оптоволоконних та відкритих системах зв’язку. Було визначено основні напрямки розвитку технологій оптичної томографії. Були розглянуті основні протоколи квантового розподілу ключів, реалізація даних протоколів, порівняння для визначення областей їх застосування в квантовій криптографії. Реалізація в оптоволоконних лініях, технічні обмеження, реалізація збереження поляризації фатонів, розрахунки загасання сигналу при передачі. Також використання відкритих ліній зв'язку, їх реалізація і технічні складнощі реалізації та вплив атмосферних факторів на загасання сигналу. Досліджено можливості об'єднання цих двох методів для реалізації перспективної мережі для квантової передачі даних.

Значні досягнення сьогодення в технічному плані і розвитку квантових обчислень, майже щоденно підіймають планку важливості цих систем для забезпечення інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Schneider J., Smalley I. What is quantum cryptography? // IBM 01 December 2023. URL: https://www.ibm.com/think/topics/quantum-cryptography (дата звернення10.05.2025 р.)

2. What Is Superposition and Why Is It Important? URL: https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition (дата звернення 10.05.2025).

3. Schneider J., Smalley I. What is a qubit? // IBM 28 February 2024. https://www.ibm.com/think/topics/qubit (дата звернення 11.05.2025).

4. Pirandola S., Andersen U. L., Banchi L., Berta M. et al. Wallden Advances in quantum cryptography // Advances in Optics and Photonics. 2020. Vol. 12, No. 4. P. 1012–1236.

5. Hilgevoord J., Uffink J. The Uncertainty Principle // Stanford Encyclopedia of Philosophy. 2016. URL: https://plato.stanford.edu/entries/qt-uncertainty/ (дата звернення 11.05.2025).

6. Mavroeidis V., Vishi K., Dominik M., Jøsang A. The Impact of Quantum Computing on Present CryptograVphy researchgate // International Journal of Advanced Computer Science and Applications . 2018. Vol. 9, No 3.

7. Sabani M. Savvas I. Poulakis D. Quantum Key Distribution: Basic Protocols and Threats: Proceedings of the 26th Pan-Hellenic Conference on Informatics/ November 25–27, 2022. New York, NY, USA. P. 383–388.

8. Sergiy O. Gnatyuk Comparative analysis of quantum key distribution systems researchgate // Science-based technologies. 2013. Vol. 17, No 1

9. Giggenbach D., Shrestha A. Atmospheric absorption and scattering impact on optical satellite-ground links // International Journal of Satellite Communications and Networking. 2021. Vol. 40. No 2. P. 157–176.

10. M. Thomas I., Yeh H., Chen J., Mambretti J., Kohlert S., Kanter P. Kumar Quantum teleportation coexisting with classical communications in optical fiber // Optica publishimg group.2024. Vol. 11. Issue 12. P. 1700-1707.

11. Optical Fiber Attenuation. URL:https://www.fiberoptics4sale.com/blogs/archive-posts/95052294-optical-fiber-attenuation (дата звернення 02.06.2025).

12. Dr. Rüdiger Paschotta. Polarization-maintaining Fibers rp-photonics. . URL: https://www.rp-photonics.com/polarization_maintaining_fibers.html (дата звернення 02.06.2025).

13. Toshiba, SoftBank Demonstrate Optical Wireless QKD URL: https://www.optica-opn.org/home/industry/2024/march/toshiba_softbank_demonstrate_optical_wireless_qkd (дата звернення 08.06.2025).

14. Гнатенко О., Одаренко Є., Курський Ю. Лазерні, оптико-електронні прилади та системи. Ч. 4. // Інформаційно-вимірювальні технології. Волоконно-оптичні гіроскопи. Україна. 2024. С. 1–30.