НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи
фахового молодшого бакалавра

на тему: **Аналіз технології квантових комунікацій та перспектив її впровадження на практиці**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Занько Сергій Олександрович

Керівник	_____ (підпис)	Володимир ПЛІШ
Нормоконтролер	_____ (підпис)	Володимир ПЛІШ
Рецензент	_____ (підпис)	Анатолій РОМАНЮК
Голова ЕК	_____ (підпис)	Андрій ВАХ
Члени ЕК	_____ (підпис)	Ігор ТИБЕЛЬ
	_____ (підпис)	Володимир ПЛІШ

Дипломна робота захищена в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія	***Телекомунікації***
Освітньо-професійний ступінь	***Фаховий молодший бакалавр***
Освітньо-професійна програма	***Телекомунікації та комп'ютерні технології***
Спеціальність	***172 Телекомунікації та радіотехніка***

ЗАТВЕРДЖУЮ
Завідувач відділення
«Телекомунікацій та
комп'ютерних технологій»
_____ Ігор ТИБЕЛЬ
« 25 » квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ ЗДОБУВАЧУ

Занько Сергію Олександровичу
(прізвище, ім'я та по батькові)

1.Тема роботи *Аналіз технології квантових комунікацій та перспектив її впровадження на практиці*

керівник роботи *Володимир ПЛІШ викладач вищої категорії, викладач-методист*
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом директора від " 20 " березня 2025 року № 20-СТ

2. Строк подання студентом роботи "10" червня 2025 року

3. Вихідні дані до роботи *3.1 Проаналізувати сполучення квантових частинок, що знаходяться у стані заплутаності;*

3.2 Розглянути телепортацію за допомогою квантів;

3.3 Проаналізувати алгоритми в квантовій обчислювальній парадигмі;

3.4 Створиння схеми квантової мережі.

4. Зміст розрахунково-пояснювальної записки

4.1 Обмін інформацією за допомогою квантових систем.

4.2 Принципи функціонування квантових систем та мереж

4.3 Засоби забезпечення безпеки в квантовому середовищі

4.4 Розвиток сучасних систем квантової комунікації

4.5Техніко-економічне обгрунтування.

4.6 Охорона праці та безпека життедіяльності

5. Перелік графічного матеріалу

5.1.	*Проходження світла через два та три фільтра*
5.2.	*Схема квантової комунікації*
5.3.	*Кодування бітів за допомогою поляризації фотона*
5.4.	*Формування криптографічного ключа за допомогою протоколу BB84*
5.5	*Створення криптографічного ключа за протоколом шести станів*

6. Консультанти розділів дипломної роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	Завдання отримав
Техніко-економічне обґрунтовування	*Мар'яна СМУК викладач вищої категорії*	*25.04.2025р.*	*25.04.2025р*
Охорона праці та безпека життєдіяльності	*Олена МЕЛЬНИКОВА викладач першої категорії*	*25.04.2025р.*	*25.04.2025р.*

7. Дата видачі завдання « 25» квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання	Примітка
1	*Вступ. Обмін інформацією за допомогою квантових систем.*	*25.04-01.05*	
2	*Принципи функціонування квантових систем та мереж*	*02.05-08.05*	
3	*Засоби забезпечення безпеки в квантовому середовищі*	*09.05-15.05*	
4	*Розвиток сучасних систем квантової комунікації*	*16.05-22.05*	
5	*Техніко – економічне обґрунтування*	*23.05-29.05*	
6	*Охорона праці та безпека життєдіяльності*	*30.05-03.06*	
7	*Висновки*	*04.06-05.06*	
8	*Підготовка графічного матеріалу.*	*06.06-09.06*	

Здобувач _____ *Сергій ЗАНЬКО*
(підпис) (ім'я, прізвище)

Керівник роботи _____ *Володимир ПЛІШ*
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина дипломної роботи: 69 с., 8 рис., 2 табл., 15 джерел.

Об’єкт дослідження – квантові системи зв'язку.

Мета роботи – розкриття основних принципів квантової комунікації.

Метод дослідження – аналітичний з використанням комп’ютерних технологій.

У дипломній роботі розглянуто основні елементи, що використовуються в квантових системах зв'язку, такі як квантова заплутаність, квантова суперпозиція та квантова телепортація, а також принципи, на яких ґрунтується робота квантових систем зв'язку, зокрема, принципи квантової заплутаності, квантової суперпозиції та квантової телепортації. Описано концепцію квантової криптографії та її важливість для забезпечення безпеки в квантових системах зв'язку.

КВАНТОВА ЗАПЛУТАНІСТЬ, КВАНТОВА СУПЕРПОЗИЦІЯ, КВАНТОВА ТЕЛЕПОРТАЦІЯ, КВАНТОВА КРИПТОГРАФІЯ, КВАНТОВИЙ РОЗПОДІЛКЛЮЧА, ПРОТОКОЛ BB84, ПРОТОКОЛЕ91

ЗМІСТ

ВСТУП

У сучасному інформаційному суспільстві, де безпека та ефективність обміну конфіденційною інформацією стають надзвичайно важливими завданнями, квантові комунікаційні системи виступають як перспективний інструмент, спроможний забезпечити новий рівень захисту та ефективності. Сучасний стан справ у галузі криптографії свідчить про зростання вразливостей традиційних методів передачі інформації через швидко розвиваючіся обчислювальні здатності потенційних загроз.

В цьому контексті квантові комунікаційні системи виходять за рамки стандартних підходів, використовуючи принципи квантової фізики для створення безпечних та ефективних засобів обміну інформацією. Однією з ключових переваг цих систем є використання протоколів квантової криптографії, зокрема квантового розподілу ключа, які забезпечують неперевершену рівень безпеки через неможливість перехоплення квантових станів.

Крім того, квантові комунікаційні системи відкривають нові перспективи у сфері обчислень та обробки інформації. Здатність квантових комп'ютерів паралельно обробляти величезні обсяги даних відкриває двері до швидкого та ефективного розв'язання складних завдань у різних галузях, таких як фармація, медицина, фінанси та інші.

Однак, не дивлячись на перспективність цих технологій, важливо враховувати практичні виклики та проблеми, що виникають у процесі їх розвитку. З врахуванням швидкого темпу технологічного прогресу та збільшення доступності експериментальних платформ, висвітлення та вирішення цих аспектів стає важливим завданням для науковців та інженерів в даній області.

У даній дипломній роботі досліджуються та аналізуються ключові аспекти квантових комунікаційних систем, їхні переваги та виклики, а також перспективи застосування у різних галузях.

1 ОБМІН ІНФОРМАЦІЄЮ ЗА ДОПОМОГОЮ КВАНТОВИХ СИСТЕМ

1.1 Сполучення квантових частинок, що знаходяться у стані заплутаності

Квантові системи слідують за принципами квантової механіки, яка описує поведінку частинок на мікроскопічному рівні. У порівнянні з класичними системами, що підлягають класичній фізиці, квантові системи діють відповідно до принципів квантової механіки, яка вводить унікальні характеристики, такі як суперпозиція, заплутаність і квантова невизначеність. Квантова комунікація передбачає переміщення квантової інформації, закодованої в конкретному стані, з одного місця на інше, а не в бітах.

Основу квантових систем становлять мікрочастинки, такі як електрони, фотони та атоми, іхню поведінку описує хвильова функція. Ця функція представляє розподіл ймовірностей можливих станів, які може займати квантова система, використовуючи невизначеність, характерну для квантової механіки.

Однією з основних задач квантового зв'язку є забезпечення безпеки інформаційних каналів за допомогою квантової криптографії. Класичні криптографічні методи можуть бути ламані швидкими обчислювальними алгоритмами, тоді як квантова криптографія використовує принципи квантової механіки для гарантії непроникної захисту інформації. Зокрема, квантова криптографія використовує заплутані квантові стани, унеможливлюючи перехоплення інформації без виявлення втручання, і застосування її забезпечує надійний захист інформаційних каналів від зловмисників.

Одним з ключових принципів квантових систем є суперпозиція, що виявляється можливістю квантової системи існувати в кількох станах одночасно. Наприклад, електрон може одночасно обертатися вгору і вниз, поки його не виміряють або спостерігають, після чого він знаходиться в конкретному стані. Ця властивість відрізняє квантові системи від класичних, де об'єкт може перебувати

лише в одному стані.

Заплутаність є ще однією важливою характеристикою квантових систем. Це явище виникає, коли дві або більше квантові частинки стають взаємозалежними так, що стан однієї частинки нерозривно пов'язаний із станом іншої, незалежно від відстані між ними. Цей нелокальний зв'язок має суттєві наслідки для квантового зв'язку та квантових обчислень.

Також характерною властивістю квантових систем є невизначеність. Згідно з цим принципом, існує фундаментальне обмеження точності, з якою можна виміряти певні пари фізичних властивостей, таких як положення та імпульс. Ця невизначеність становить фундаментальний аспект квантових систем і встановлює обмеження на передбачуваність і точність вимірювань квантових явищ.

Квантова заплутаність – явище, що полягає в тому, що властивості однієї частинки в парі залежать від властивостей іншої частинки, незалежно від відстані чи перешкод між ними. Наприклад, електрони чи фотони можуть мати різні атрибути, такі як напрям обертання, і вимірювання однієї частинки миттєво надає інформацію про іншу.

Це явище, відоме як "квантова заплутаність" і часто описуване Альбертом Ейнштейном як "моторошна дія на відстані", викликає сумніви та зацікавленість вчених. Спочатку існував скептицизм до реальності квантової заплутаності, але завдяки прогресу в експериментальних технологіях і дослідженням таких вчених, як Ален Аспект, Джон Клаузер і Антон Зейлінгер, які отримали Нобелівську премію, фізики стали більш відкритими до цього явища.

Для глибшого розуміння квантової заплутаності важливо освоїти концепцію квантової суперпозиції. Це означає, що частинки можуть перебувати в декількох станах одночасно. Наприклад, спін частинки може бути одночасно "вгору" і "вниз", поки не відбудеться вимірювання. Хоча середні результати можна передбачити, результат конкретного вимірювання залишається непередбачуваним.

У 1935 році Ейнштейн, Подольський і Розен висунули уявний експеримент,

відомий як парадокс ЕПР, для того щоб підкреслити уявну абсурдність квантової заплутаності. Вони розглядали розпад частинок пі-мезонів, які мали протилежний спін і віддалялися одна від одної. Таким чином, якщо спін електрона вимірюється напрямленим вгору, то спін позитрона вимірюється напрямленим вниз, і навпаки, навіть якщо частинки знаходяться на відстані мільярдів миль одна від одної.

Це б сталося нормальним, якщо б спін електрона завжди вказував вгору, а спін позитрона завжди вниз. Проте, завдяки квантовій механіці, спін кожної частинки одночасно вказує вгору і вниз, доки не виміряється. Лише під час вимірювання квантовий стан спіну "згортається" у вказаному напрямку, миттєво впливаючи на іншу частинку і змушуючи її спін приймати протилежне значення. Такий ефект віддаль демонструє, наскільки непередбачуваним і здивувальним може бути пов'язаність квантових станів.

У 1930-х роках фізики пропонували альтернативні інтерпретації квантової заплутаності, такі як існування прихованих змінних, які визначають стан частинки до вимірювання. Проте, на той час відсутні були технології та точні методи вимірювання, необхідні для перевірки цих теорій. Лише у 1960-х роках Джон Белл сформулював відому нерівність, відому як нерівність Белла, щоб дослідити життєздатність теорій прихованих змінних.

Експерименти, проведені лауреатами Нобелівської премії 2022 року, зокрема Аленом Аспектом, використовуючи заплутані фотони, переконливо продемонстрували порушення нерівності Белла. Ці експерименти розвіяли сумніви у існуванні прихованих змінних і підтвердили достовірність квантової механіки. Згідно з результатами, об’єкти можуть демонструвати кореляції на значних відстанях, що класична фізика не в змозі пояснити. Таким чином, експериментально підтверджено, що квантова заплутаність є реальним та необхідним явищем у фізичному світі.

Найважливіше полягає в тому, що квантова заплутаність не порушує теорію відносності, яка забороняє спілкування на швидкості, вищій за світло. Кореляція, яку спостерігають під час вимірювань між заплутаними частинками на величезних відстанях, не означає передачу інформації між ними [3].

Згідно з принципами теорії відносності Альберта Ейнштейна, події чи взаємодії не можуть поширюватися швидше за світло, і це обмеження залишається справедливим навіть у випадку квантової заплутаності. Таким чином, незважаючи на дивовижні кореляції між заплутаними частинками, жодна інформація не передається між ними зі швидкістю, вищою за світло. Це узгодження між квантовою механікою та теорією відносності сприяє глибшому розумінню природи квантових явищ та їх відповідності фундаментальним законам всесвіту.

В даний час фізики продовжують досліджувати квантову заплутаність і її потенційне практичне застосування. Хоча квантова механіка може точно передбачити ймовірності вимірювань, багато дослідників все ще сумніваються, чи забезпечує вона повний опис реальності.

1.2 Суперпозиція квантів

Порівняльний приклад із світу поверхні ставка може допомогти у розумінні концепції квантової суперпозиції. Під час ставкової поверхні одночасно рухаються хвилі, які розтікаються в різних напрямках. Після взаємного перетинання цих хвиль утворюється складний малюнок. У квантовій фізиці, частинки, такі як електрони та фотони, проявляють хвилеподібну поведінку і можуть існувати в кількох станах одночасно, об'єднуючись і створюючи накладені стани.

В той час, як хвилі на поверхні ставка виникають фізично внаслідок руху води, квантові хвилі виражаються математично за допомогою рівнянь, які описують ймовірність існування частинки в певному стані або з певними властивостями. Ці математичні рівняння вказують на ймовірність знаходження електрона з певною швидкістю чи в певному місці. У стані суперпозиції різні стани електрона розглядаються як різні можливості, кожна з яких має власну ймовірність спостереження.

Наприклад, електрон може бути в суперпозиції двох швидкостей чи

існувати в двох місцях одночасно, поки не відбудеться вимірювання, яке фіксує конкретний стан. Таким чином, концепція квантової суперпозиції розширює наше розуміння про те, як частинки можуть існувати і взаємодіяти в квантовому світі.

Концепцію квантової суперпозиції може бути складно візуалізувати, тому використовують аналогії для пояснення, такі як монета, яка одночасно є орлом і решкою, або відомий мисленнєвий експеримент кота Шредінгера. Один із сценаріїв цього експерименту включає кота, якого поміщають у закриту коробку з отрутою, що має рівні шанси бути смертельною чи несмертельною протягом години. До моменту відкриття коробки та спостереження, кіт вважається живим і мертвим одночасно. Шредінгер використав цей приклад, щоб підкреслити парадоксальну природу квантової фізики.

Математично суперпозицію можна уявити як рівняння з кількома можливими дійсними рішеннями. Наприклад, розв'язуючи рівняння $x^2 = 4$, можна отримати два можливих значення для x: 2 або -2. Обидва рішення є правильними. У квантових системах хвильові функції складніші, але принцип суперпозиції залишається застосовним.

Використовуючи концепцію суперпозиції та математичний підхід до квантових систем, дослідники можуть розширити розуміння квантових явищ. Це розуміння є важливим для розвитку та використання квантових технологій, які мають значний потенціал у майбутньому.

Суперпозицію було експериментально підтверджено різними демонстраціями. Один із прикладів - використання світлофільтрів, які блокують певні поляризації світла, такі як ті у сонцезахисних окулярах чи фільтрах камер. Звичайне світло містить хвилі різної поляризації від різних джерел, і ці хвилі можуть утворювати суперпозицію поляризованих станів. За допомогою фільтра, що пропускає лише світло певної поляризації, можна ефективно блокувати відбиті відблиски.

Суперпозиція стає очевидною, коли ми вивчаємо додаткові властивості світла за допомогою кількох фільтрів. Коли світло проходить через горизонтальний фільтр, ймовірність того, що воно пройде через інший

горизонтальний фільтр, становить 100%, оскільки обидва фільтри вирівняні рис. 1.1. Проте, коли другий фільтр повертається у вертикальне положення, ймовірність проходження світла через обидва фільтри зменшується. При діагональному положенні 45 градусів половина світла проходить, а коли фільтр повертається у повністю вертикальне положення, світло не пройде. Без суперпозиції навіть невелике обертання другого фільтра може призвести до повного блокування світла.

Цей ефект відображає принципи квантової механіки, де суперпозиція дозволяє частинцям існувати в різних станах одночасно. Такий підхід до вивчення властивостей світла і фільтрів відкриває шлях для розуміння багатофакторних взаємодій та відображення сложності квантових явищ у світлі..

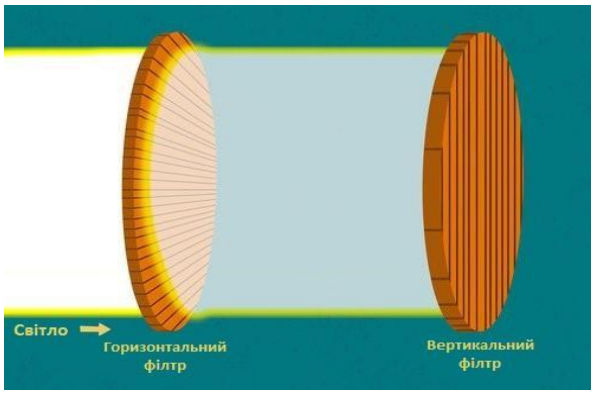

Рисунок 1.1 – Проходження світла через два фільтра

Впровадження діагонального фільтра між горизонтальним і вертикальним фільтрами визначає можливість проходження певної кількості світла через систему. Це явище зумовлене суперпозицією. Діагональний фільтр пропускає 50% горизонтально поляризованого світла. З огляду на те, що діагональний фільтр розташований під кутом щодо вертикального фільтра, останній також пропускає 50% світла.

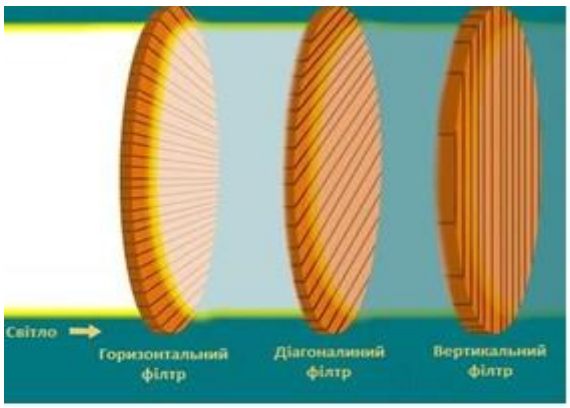

Рисунок 1.2 –Проходження світла через три фільтра

Ця послідовність, починаючи з горизонтального фільтра, далі через діагональний і закінчуючи вертикальним, ілюструє, як світло може частково пройти через комбінацію фільтрів завдяки явищу суперпозиції [5].

1.3 Телепортація за допомогою квантів

Квантова телепортація є фундаментальним квантовим явищем, що базується на принципах квантової механіки. Основна ідея полягає в передачі квантового стану одного об'єкта на інший об'єкт, використовуючи квантову сполученість між ними.

Процес квантової телепортації включає три взаємопов'язані частини: квантове сполучення, вимірювання та передачу класичної інформації. Основною умовою для успішної телепортації є наявність попередньо створеної пари заплутаних (сполучених) частинок або кубітів.

Коли стан одного кубіту змінюється, стан іншого кубіту, незалежно від відстані між ними, теж миттєво змінюється відповідно до принципів квантової сполученості. Застосовуючи вимірювання та передачу класичної інформації, стан першого кубіту може бути точно відтворений на другому кубіті, який може знаходитися в іншому місці.

Цей процес не передбачає переміщення реальних об'єктів, але дозволяє передавати квантовий стан частинок через великі відстані без прямого контакту

між ними. Квантова телепортація має важливі застосування в області квантових обчислень, криптографії та забезпечення безпеки квантового зв'язку. Процес квантової телепортації зазвичай включає два етапи: квантове сполучення і вимірювання [6].

На першому етапі відправник і одержувач створюють пару частинок, які перебувають у квантово сполученому стані. Наприклад, це може бути пара фотонів із спінами, що взаємодіють у стані спіну-знижування або стані спіну-піднімання. Ця взаємодія створює сполученість між фотонами, незалежно від їхньої фізичної відстані один від одного.

Після цього, на другому етапі, виконується вимірювання на одному з фотонів, що належить сполученій парі. Результат вимірювання передається класичним каналом до одержувача, який застосовує відповідні операції до свого фотона для відновлення квантового стану, що був переданий відправником. Цей процес дозволяє передавати квантовий стан з одного місця на інше, не переміщуючи фізично сам об'єкт.

Використання супутників, як у випадку з супутником Micius, дозволяє досягти передачі квантової інформації на великі відстані, що відкриває перспективи для розвитку квантових комунікаційних мереж та квантового обчислення.

Важливо відзначити, що квантова телепортація не передбачає миттєвого передачі інформації, оскільки для виконання процесу все ще необхідна класична інформація. Швидкість передачі квантової інформації обмежена швидкістю світла і не може перевищувати її.

2 ПРИНЦИПИ ФУНКЦІОНУВАННЯ КВАНТОВИХ СИСТЕМ ТА МЕРЕЖ

2.1 Обчислення на квантових принципах

Квантова наука вносить революцію у світ фізики і приводить до значного прогресу в порівнянні з існуючими технологіями. Застосування принципів та теорій квантової науки демонструє суттєвий розвиток, зокрема у комунікаційному секторі, де вона відкриває нові перспективи для майбутніх систем зв'язку.

Важливо відзначити, що квантові системи наразі перебувають на етапі активного дослідження, і їх практичне впровадження вимагає подальшого часу для розвитку технологій і подолання технічних викликів. Наприклад, необхідно посилити стабільність та якість квантових систем, забезпечити їх масштабованість та знизити вартість виробництва. Однак високий попит на квантові системи свідчить про їхній потенціал для революційних змін у різних галузях.

Квантова наука розкриває нові горизонти для розуміння світу і ефективного використання його ресурсів.

В 1982 році Річард фон Нейман висунув ідею використання принципів квантової фізики для створення квантового комп'ютера. Однак початкове бачення цього квантового комп'ютера не полягало в його використанні як загального обчислювального пристрою, але як інструмент для моделювання складних фізичних систем.

Класичні комп'ютери зіткнулися з серйозними труднощами при спробі моделювати квантові системи. Їхні обчислювальні можливості недостатньо для точних розрахунків взаємодії між великою кількістю частинок. Крім того, обсяг пам'яті класичних комп'ютерів не вистачає для зберігання повної інформації про квантовий стан таких систем.

Таким чином, виникла ідея моделювати одну квантову систему іншою. У квантовій механіці принцип суперпозиції відіграє ключову роль. Цей принцип стверджує, що якщо фізична система може мати два стани - логічний нуль і

логічну одиницю, вона також може існувати в довільних суперпозиціях, представляючи квантовий стан системи в гільбертовому просторі.

Квантові обчислення можуть вирішувати ряд проблем та давати нові можливості, зокрема у сфері фізичного моделювання. Наприклад, вони можуть бути використані для дослідження властивостей молекул, що має важливе застосування в розробці нових неорганічних світлодіодів для передових дисплеїв. Такі завдання є складними та вимагають значних розрахунків, експериментів та інвестицій. З використанням квантових обчислень можна ефективно зменшити витрати, зокрема уникнути дорогих та трудомістких фізичних експериментів.

Віртуальне моделювання на квантових комп'ютерах може надати цінну інформацію про життєздатність та властивості молекулярних структур, ефективно використовуючи ресурси та заощаджуючи час, який зазвичай витрачається на невдачі експериментів. Хоча наразі квантові комп'ютери можуть імітувати лише основні молекули, спостерігається тенденція до розширення їхніх можливостей для фізичного, хімічного та біологічного моделювання.

При вимірюваннях у квантовій системі, зокрема при маніпуляціях з кубітами, набір квантових дворівневих систем служить пам'яттю. Ці кубіти можуть приймати різні фізичні форми, а їхні стани нуль і одиниця можуть чітко розрізнятися та маніпулюватися квантовим комп'ютером. Важливо відзначити, що суперпозиції не можна спостерігати безпосередньо в експерименті, і можливі лише два результати - нуль і один. Коефіцієнт суперпозиції визначає ймовірність отримання кожного з результатів, відображаючи фундаментальну ймовірність у квантовій теорії [7].

2.2 Біти в квантових системах та їх характеристики

В квантових обчисленнях кубіт виконує роль основної одиниці інформації, аналогічно до біта у класичних обчисленнях. Відмінність полягає в його унікальних квантових властивостях.

У квантовому комп'ютері можна використовувати елементарні частинки, такі як електрони або фотони, де їхні заряди або поляризації слугують представленням 0 та/або 1. Поведінка цих частинок становить основу квантових обчислень.

Коли частинка використовується як кубіт, її поміщають у контрольоване середовище для захисту від зовнішніх впливів, наприклад, у магнітному полі чи в спеціалізованих схемах, які ізолюють від зовнішнього середовища, часто розташовуючи їх у холодильних відсіках для мінімізації субатомних порушень.

Дослідники експериментують з різними методами створення середовища, в якому кубіти можуть маніпулювати та вимірюватися без зовнішніх впливів. Наприклад, в одному з підходів електрон утримують у електромагнітному полі, контролюючи його спін і ізолюючи від зовнішніх впливів.

Зміна стану спіну електрона за допомогою енергетичного імпульсу, постачаного лазером чи іншим джерелом, надає можливість присвоїти кубіту значення 0 або 1, аналогічно біту в класичних обчисленнях. Проте квантові обчислення дозволяють здійснювати значно більше завдяки унікальним властивостям кубіту.

Відповідно до квантового закону, частинка, коли не спостерігається, знаходиться у стані переплетення. У цьому стані вона вчиняє, начебто одночасно знаходиться в станах спрямованого вгору та спрямованого вниз спіну. Електрон існує у стані ймовірності, представленому математично дробами від 0 до 1, і лишається у цьому стані до моменту вимірювання та спостереження.

Властивість переплетення визначає здатність квантового комп'ютера існувати в декількох станах одночасно. Кількість можливих станів зростає експоненційно зі збільшенням кількості кубітів. Можливі стани представлені як 2^n, де n – кількість кубітів. Це забезпечує квантовому комп'ютеру потенційну виразність та обчислювальну потужність, яка виходить за рамки можливостей класичних обчислювальних систем.

Таблиця 2.1– Кількість можливих станів кубітів

Кількість кубітів	Кількість можливих станів
2	4
5	32
10	1024
50	1,126×10^15
100	1,268×10^30

Квантовий комп'ютер може виконувати набагато більше завдань з використанням своїх кубітів, порівняно з класичним комп'ютером, що має таку ж кількість бітів. Наприклад, дворозрядний регістр у класичному комп'ютері може утримувати тільки одну з чотирьох можливих двійкових конфігурацій (00, 01, 10 або 11) у будь-який момент часу. З іншого боку, двохкубітовий регістр у квантовому комп'ютері може зберігати всі чотири числа одночасно, і зі збільшенням кількості кубітів кількість можливих станів продовжує зростати [8].

2.3 Алгоритми в квантовій обчислювальній парадигмі

У класичних обчисленнях алгоритми виконуються послідовно на звичайних комп'ютерах. Однак у сфері квантових обчислень використовують квантові алгоритми, які можуть використовувати унікальні властивості квантових систем.

Квантові алгоритми можуть використовувати суперпозицію та заплутаність, що дозволяє їм обробляти інформацію паралельно та ефективно вирішувати певні класи завдань. Найвідомішим прикладом квантового алгоритму є алгоритм Шора для факторизації, який може значно прискорити розв'язання проблем, які класичні комп'ютери обробляли б надто довго. Квантові алгоритми відкривають нові можливості для обчислень у тих випадках, де класичні методи досягають обмежень ефективності.

Термін "квантовий алгоритм" вказує на використання квантових явищ у принаймні одному етапі обчислення. Такі алгоритми спеціально використовують суперпозицію та заплутаність, дві ключові квантові властивості, що надають квантовим комп'ютерам обчислювальні переваги над класичними.

Суперпозиція дозволяє квантовим бітам (кубітам) існувати у багатьох станах одночасно, а заплутаність полегшує встановлення кореляцій між квантовими частинками, навіть якщо вони знаходяться на великих відстанях одна від одної. Ці властивості розширюють обчислювальні можливості квантових алгоритмів, дозволяючи їм вирішувати деякі задачі значно швидше, ніж це можливо на класичних комп'ютерах.

Квантові алгоритми використовують квантові властивості для вирішення конкретних класів задач і мають потенціал експоненціального прискорення порівняно з класичними алгоритмами. Найвідоміші приклади цього потенціалу включають алгоритм Шора для розкладання чисел і алгоритм Гровера для ефективного пошуку в базі даних.

Алгоритм Шора, наприклад, може швидко факторизувати великі числа, що є трудомістким завданням для класичних комп'ютерів, особливо при великих числах, які використовуються у криптографії. Алгоритм Гровера дозволяє здійснювати пошук в невпорядкованих базах даних значно ефективніше, ніж класичні алгоритми[9].

Ці алгоритми відкривають нові перспективи в області обчислень, забезпечуючи можливість розв'язання завдань, які раніше були важкі або неможливі для виконання звичайними методами.

2.4 Складові квантової мережі

Квантові мережі грають ключову роль у розвитку квантових обчислень і квантових комунікацій. Однією з їх ключових функцій є передача квантової інформації між квантовими процесорами, яка дозволяє взаємодіяти з квантовими системами та виконувати операції, які були б неможливі на класичних комп'ютерах.

Квантові процесори в межах цих мереж представляють собою ключові складові, здатні виконувати квантові логічні вентилі та інші операції з використанням кубітів. Ці компактні квантові комп'ютери відкривають

можливості для вирішення складних завдань, що включають швидке та ефективне моделювання квантових систем, завдяки паралельним обчисленням та використанню квантової сполучності.

Концепція мережевих квантових обчислень, або розподілених квантових обчислень, полягає в установленні зв'язків між квантовими процесорами за допомогою квантових мереж, що дозволяє передавати кубіти між ними. Це створює кластер квантової обчислювальної потужності, який забезпечує загальну обчислювальну потужність більшого розмаху.

Ідея використання мережі квантових процесорів аналогічна створенню комп'ютерних кластерів у класичних обчисленнях. Об'єднуючи менш потужні квантові процесори, можна створити більш потужний і надійний обчислювальний кластер. Однак на даний момент важливо відзначити, що квантові процесори поки що реалізовані на дуже короткі відстані через виклики, пов'язані зі збереженням інформації та квантовою декогеренцією на великих відстанях.

Квантові мережі включають ключові компоненти, аналогічні їх класичним контрагентам. Спочатку це кінцеві вузли, які виступають в якості пунктів виконання програм. Робота квантових мереж подібна до функціонування квантових процесорів, які можуть включати в себе різну кількість кубітів, залежно від потреб конкретного застосунку. Деякі вимагають квантових процесорів із кількома кубітами та квантовою пам'яттю на кінцевих вузлах.

Другий компонент – це лінії зв'язку для передачі кубітів між вузлами. Використання стандартних телекомунікаційних волокон можливе для квантового зв'язку. У мережевих квантових обчисленнях, де квантові процесори знаходяться на коротких відстанях, довжини хвиль вибираються відповідно до конкретної апаратної платформи квантового процесора.

Щодо третього аспекту, для оптимізації використання комунікаційної інфраструктури необхідні оптичні комутатори. Вони направляють кубіти до відповідних квантових процесорів для оптимальної ефективності. Однак ці оптичні комутатори повинні підтримувати квантову когерентність, що вносить додаткові виклики порівняно зі звичайними оптичними комутаторами.

У кінцевому рахунку, для перенесення кубітів на значні відстані важливі квантові ретранслятори, які розташовані між кінцевими вузлами. З урахуванням того, що кубіти не можуть бути скопійовані, класичне посилення сигналу виявляється неможливим. Таким чином, квантові ретранслятори стають важливою складовою для забезпечення ефективного транспортування квантової інформації на великі відстані в квантових мережах.

Крім того, кінцеві вузли виконують подвійну функцію у отриманні та передачі інформації. Для квантового розподілу ключів можна використовувати телекомунікаційні лазери та параметричне понижувальне перетворення, в поєднанні з фотодетекторами. У таких випадках кінцеві вузли можуть представляти собою відносно прості пристрої, що складаються переважно з дільників променя та фотодетекторів.

Однак для багатьох протоколів важливі більш складні кінцеві вузли, які можуть виконувати розширені функції обробки та діяти як квантові повторювачі. Їхня вагома перевага полягає в здатності зберігати та ретранслювати квантову інформацію, не порушуючи основний квантовий стан. Збережений квантовий стан може бути виражений через відносний спін електрона в магнітному полі або енергетичний стан електрона.

Один із підходів до створення таких складних кінцевих вузлів включає використання центрів забарвлення в алмазі, таких як азотна вакансія. Ця система представляє собою компактний квантовий процесор із кількома кубітами, здатний працювати при кімнатних температурах. У цій системі вже були успішно проведені експерименти з демонстрацією дрібномасштабних квантових алгоритмів, квантової корекції помилок, заплутаності двох і трьох квантових процесорів і детермінованої квантової телепортації.

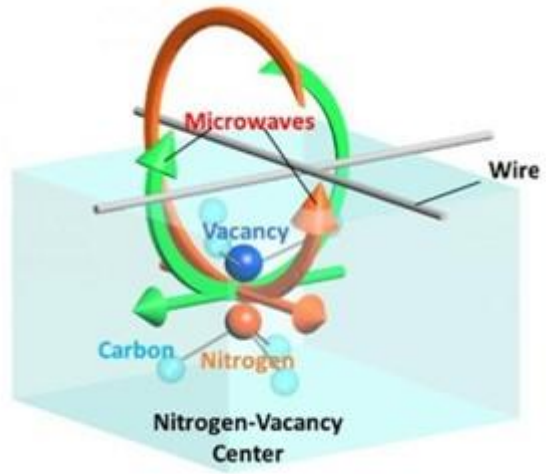

Рисунок 2.1–Центр забарвлення в алмазі

Інша потенційна платформа для кінцевих вузлів ґрунтується на іонних пастках, які використовують радіочастотні магнітні поля та лазери. У мережі захоплених іонів різних видів фотони сплутані з батьківським атомом та використовуються для встановлення зв’язку між різними вузлами. Квантова електродинаміка резонатора також є ефективним методом досягнення цієї мети. Унійфотонні квантові стани можуть бути перенесені в атомні квантові стани та з них, що зберігаються в окремих атомах в оптичних порожнинах. Це дозволяє передавати квантові стани між окремими атомами за допомогою оптичного волокна, а також створювати віддалену переплутаність між віддаленими атомами.

Лінії зв'язку в квантових мережах можуть бути реалізовані на фізичному рівні за допомогою оптичних мереж та кубітів, які базуються на фотонах. Оптичні мережі виявляються переважним вибором для покриття великих відстаней через їхню меншу чутливість до декогерентності. Вони також використовують існуючу інфраструктуру оптоволокна.

Волоконно-оптичні мережі:

– З використанням існуючого телекомунікаційного волокна можна створити оптичні мережі аналогічно до традиційного телекомунікаційного обладнання.

– Ці мережі можуть працювати як з одномодовим, так і з багатомодовим волокном, забезпечуючи підвищену точність зв’язку.

– Для генерації фотонів може використовуватися телекомунікаційний лазер, який сильно послаблюється, і лавинні фотодетектори використовуються для прийому.

– Можлива передача неквантових сигналів синхронізації та керування через мультиплексування телекомунікаційного волокна.

– Вже були досягнуті успіхи у передачі заплутаної квантової пам’яті через довгі оптоволоконні кабелі.

Мережа вільного простору:

– Аналогічно волоконно-оптичним мережам, але вимагає прямої видимості між сторонами.

– Зазвичай може підтримувати вищі швидкості передачі та уникати проблем оптичних волокон.

– Проте, вона більш сприйнятлива до екологічних збурень на великих відстанях.

Мережі у вільному космосі:

– Включають передачу квантової інформації через атмосферу або вакуум.

– Використовують супутники для забезпечення зв'язку на великі відстані.

– Досягнення включають передачу заплутаності на відстані 1203 км та обмін фотонами між супутниками на відстані 20000 км.

Ці технології розширюють можливості квантових мереж і дозволяють використовувати їх на різних відстанях та у різних середовищах.

Квантовий повторювач відіграє важливу роль у забезпеченні наскрізної передачі кубітів у квантовій мережі. Це досягається шляхом встановлення квантової заплутаності та використання квантової телепортації. Нижче розглядаються основні аспекти та застосування квантового повторювача в квантових мережах.

Значення для розповсюдження квантових ключів:

– У протоколах розповсюдження квантових ключів, де безпека забезпечується перевіркою заплутаності, квантовий повторювач грає важливу роль.

– Навіть якщо квантовий повторювач не є абсолютно надійним, перевірка заплутаності все одно дозволяє надійно шифрувати інформацію між відправником і одержувачем.

Наскрізна передача кубітів:

– Квантові повторювачі дозволяють встановлювати заплутаність між віддаленими вузлами без фізичного надсилання заплутаного кубіта на всю відстань.

– Квантова мережа може складатися з коротких зв'язків, охоплюючи десятки чи сотні кілометрів, і встановлювати заплутаність на великих відстанях.

Механізми виправлення помилок:

– Квантові повторювачі можуть використовувати методи виправлення помилок для збереження та ретрансляції квантової інформації.

– Використання методів виправлення помилок вимагає великої кількості кубітів, що залишається викликом через поточні технологічні обмеження.

Застосування в квантовому розподілі ключів:

– В контексті квантового розподілу ключів, квантові повторювачі можуть використовуватися для забезпечення безпечної передачі класичних рядків бітів.

– Традиційні коди виправлення помилок можуть бути застосовані до бітового рядка перед його передачею в квантовій мережі.

Враховуючи ці аспекти, квантові повторювачі стають важливим елементом квантових мереж, що дозволяє реалізацію безпечної та ефективної передачі квантової інформації.

2.5 Створення схеми квантової мережі

Розробка є найскладнішим аспектом будь-якої сучасної технологічної системи. Якщо концепція не є ефективною або простою, це може призвести до того, що технологія не матиме перспектив у майбутньому. Таким чином, в розробці квантових комунікаційних мереж важливо ретельно враховувати всі можливі труднощі, щоб забезпечити їх успішну реалізацію.

У цьому контексті особливо важливо враховувати, що квантові технології вносять нові виклики, такі як квантові взаємодії та заплутаність, які не є характерними для класичних систем. Планування та розробка квантових комунікаційних мереж має враховувати ці особливості, а також забезпечити ефективність, надійність та безпеку в обраних сценаріях використання.

Крім того, уникнення зайвого ускладнення концепцій та імплементацій є ключовим для забезпечення швидкого прийняття та успіху квантових комунікаційних технологій в індустріальних та наукових областях. Правильне вирішення цих аспектів може визначити успішність та виробничу реалізацію квантових комунікацій в майбутньому.– Безпека. Аспекти безпеки повинні бути ретельно враховані у квантовій мережі. Запобігання проникненню та злому інформації є критично важливим. Квантові мережі використовують принципово нові методи захисту інформації, такі як квантова криптографія, яка використовує властивості квантової механіки для конфіденційної передачі даних. Забезпечення абсолютної безпеки інформації у квантових мережах є одним із ключових аспектів їхнього проектування.

Успішна реалізація квантових мереж визначається декількома ключовими аспектами:

– Економічна ефективність. Вартість будівництва та експлуатації повинна бути прийнятною для користувачів і бізнес-сектору. Постійне вдосконалення технологій виробництва компонентів, розробка компактних та енергоефективних пристроїв, ефективне використання ресурсів.

– Високошвидкісне та стабільне з’єднання. Мінімізація затримок розповсюдження сигналу та стабільне з’єднання в будь-якому середовищі. Розробка високошвидкісних комунікаційних каналів, протоколів та мережевої архітектури.

– Просте апаратне забезпечення. Максимально спрощене проектування апаратури для забезпечення широкої доступності та надійності. Легке впровадження і обслуговування квантових пристроїв для прискорення розвитку технології.

– Маштабованість. Здатність масштабувати мережі для обробки великих обсягів даних та зростаючих потреб користувачів. Розробка архітектури мережі, що дозволяє додавати нові квантові процесори та ресурси, підтримка паралельних обчислень та розподіленої обробки даних.

– Корекція помилок. Розробка алгоритмів корекції помилок для виявлення та виправлення негативного впливу шуму та взаємодії з оточуючим середовищем. Забезпечення точності та достовірності обробки квантової інформації. [10].

Забезпечення криптографічної безпеки є важливим аспектом усього процесу комунікації від передавача до приймача. Запропонована архітектура комунікації в основному зосереджується на використанні квантового каналу від кінця до кінця, управлінні мережею та протоколах квантового криптографічного обміну ключами. На рис. 2.2 показана схема квантової комунікації від передавача до приймача, де кожен етап процесу взаємодії зашифрований для забезпечення високого рівня безпеки.

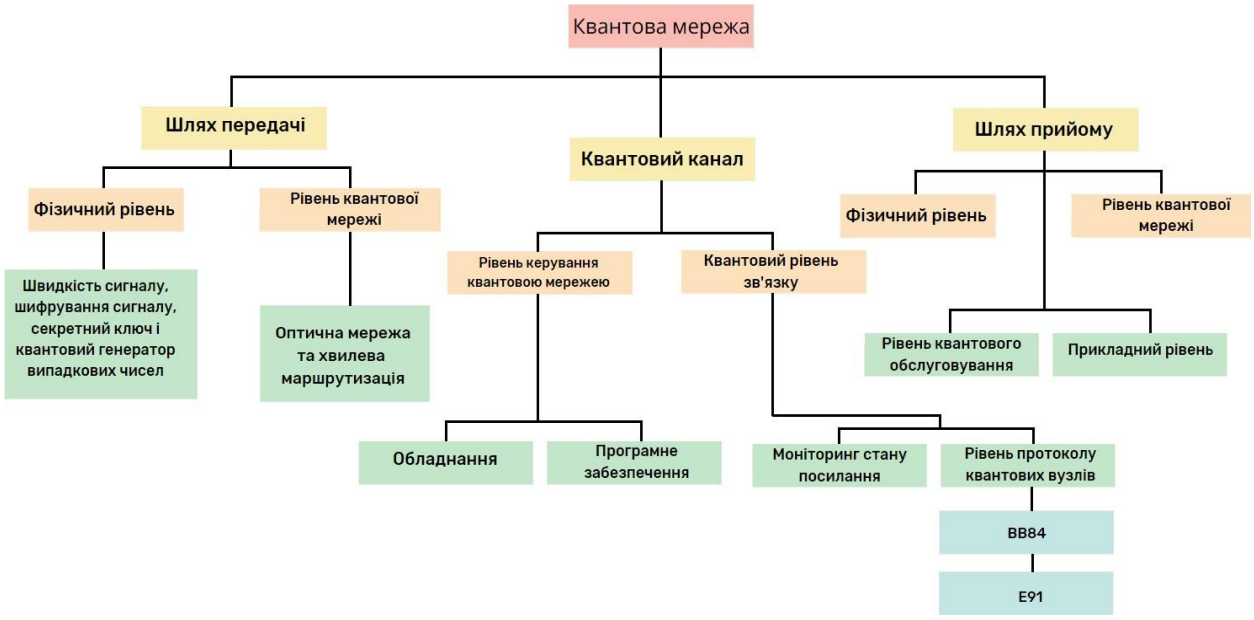

Рисунок 2.2 – Схема квантової комунікації

Передачу інформації розділено на два рівні:

– квантовий фізичний рівень;

– квантовий мережевий рівень.

На квантовому фізичному вузлі два вузли взаємодіють, враховуючи фізичне з'єднання, швидкість сигналу, шифрування сигналу, криптографічну генерацію випадкових квантових чисел та генерацію сплетеності.

На квантовому мережевому рівні передача сплетеності та традиційне маршрутизування хвиль виконуються за допомогою мережі, визначеної програмним забезпеченням. Апаратне та програмне керування є основними функціями управління квантовою мережею. Ключові протоколи включають протоколи багатовимірного квантового зв'язку, протоколи розподілу секретної інформації, а також протоколи шести станів, які відповідають за контроль помилок.

Шлях прийому також розділено на два рівні: квантовий сервісний рівень, що базується на розподілі сплетеності, і прикладний рівень.

3 ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В КВАНТОВОМУ СЕРЕДОВИЩІ

3.1 Протоколи квантового розподілу ключів

Відновлення та збереження особистої безпеки стає однією з головних турбот для користувачів у світі, що швидко розвивається, незалежно від того, які пристрої вони використовують. Разом із стрімким розвитком інформаційних технологій та поширенням Інтернету з'являються нові загрози та ризики, пов'язані з захистом особистих даних, комунікацій та конфіденційної інформації.

Квантова криптографія стає ключовим напрямком, який прагне надати відповіді на виклики та вирішити проблеми, пов'язані із забезпеченням конфіденційності даних при використанні квантових технологій. Застосування цих технологій стало можливим завдяки науковим відкриттям та сучасним досягненням, які дозволяють вирішити складні обчислювальні завдання.

Квантова криптографія використовує принципи квантової механіки для створення систем, які забезпечують абсолютну конфіденційність передачі даних. Зокрема, квантовий обмін ключів виключає можливість неповідомленого перехоплення ключа, оскільки будь-яка спроба взаємодії з квантовим станом призведе до його зміни, що буде помічено відразу.

Класичні криптографічні методи, які стали стандартом безпеки протягом тривалого часу, виявилися вразливими до потенційних загроз, що можуть виникнути в результаті розвитку квантових комп'ютерів. Основною метою досліджень у галузі квантової криптографії є розробка алгоритмів та протоколів, стійких до квантових обчислень.

Квантова криптографія використовує принципи квантової механіки для забезпечення безпеки при шифруванні. Завдяки квантовим механізмам, інтегрованим у шифрування, рівень безпеки значно посилюється, і ніхто не може отримати доступ до даних, які спільно використовуються та захищаються цією системою.

Використання фотонів як носіїв інформації є особливо ефективним, оскільки вони можуть існувати одночасно в кількох станах, а будь-яка спроба спостерігати чи змінити їх квантові властивості вимагає взаємодії, що робить неможливим створення непомічених копій.

Навіть за наявності великої обчислювальної потужності квантових комп'ютерів, зламати квантовий ключ залишається великим викликом, оскільки наразі відсутні конкретні докази або демонстрації теоретичної можливості обійти цей рівень безпеки. [11].

Квантовий розподіл ключів (КРК) представляє собою безпечний метод обміну ключами для шифрування, де сторони можуть обмінюватися ключами, відомими тільки їм, використовуючи унікальні властивості квантової фізики. Цей підхід забезпечує перевірену та гарантовану безпеку.

У системі КРК обидві сторони можуть генерувати та спільно використовувати ключі для шифрування та дешифрування повідомлень. На відміну від традиційних методів розподілу ключів, що базуються на шифрах відкритих ключів, які використовують складні математичні розрахунки, КРК використовує квантові властивості для забезпечення безпеки.

Традиційні методи розподілу ключів можуть стикатися з проблемами, такими як розвиток стратегій атак, використання слабких генераторів випадкових чисел та зростання обчислювальної потужності комп'ютерів. Розвиток квантових обчислень також створює загрозу для багатьох існуючих методів шифрування з відкритим ключем, тому КРК виявляється обіцяючим рішенням для забезпечення високого рівня безпеки в цьому контексті.

Квантовий розподіл ключів (КРК) відрізняється від традиційних методів розподілу ключів тим, що використовує квантові системи, базовані на фундаментальних законах квантової механіки, замість виключного застосування математики. Наприклад, теорема про заборону клонування встановлює, що неможливо створити ідентичні копії невідомого квантового стану, що запобігає зловмисникам просто копіювати дані, як це можливо в звичайних системах передачі інформації. Крім того, спроба зловмисника спостерігати або

маніпулювати системою призводить до змін у квантових властивостях, що може бути виявлено. Цей процес забезпечує високий рівень безпеки, а його ефективність не залежить від збільшення потужності обчислювачів

Рисунок 3.1 – Взаємодія в квантовому протоколі розподілу ключів

Квантовий розподіл ключів забезпечує безпеку через передачу фотонів, які представляють собою окремі частинки світла, по волоконно-оптичних кабелях між сторонами. Кожен фотон має випадковий квантовий стан, утворюючи потік одиниць і нулів. При досягненні приймального кінця, фотон вибирає шлях до колектора фотонів, проходячи через розсіювач променя випадковим чином. Після цього приймач повідомляє відправника про послідовність відправлених фотонів, яку можна порівняти з записами випромінювача.

Фотони, які були неправильно зібрані, відкидаються, залишаючи певну послідовність бітів, яку можна використовувати як ключ для шифрування даних. Корекція помилок та наступні етапи обробки виправляють будь-які помилки або витоки інформації. Додаткові кроки обробки, такі як відкладене посилення конфіденційності, додатково гарантують, що будь-яке потенційне знання, отримане підслуховувачем про остаточний секретний ключ, буде вилучено.

Квантовий розподіл ключів охоплює різні типи, з двома основними категоріями – це протоколи підготовки та вимірювання і протоколи на основі заплутування. Протоколи підготовки та вимірювання зосереджені на вимірюванні невідомих квантових станів, що дозволяє виявляти спроби прослуховування та оцінювати потенційне перехоплення даних. Протоколи на основі заплутування використовують квантові стани, коли два об'єкти з'єднані, що призводить до об'єднаного квантового стану. Концепція заплутаності передбачає, що

вимірювання одного об'єкта впливає на інший. Таким чином, якщо перехоплювач втручається в раніше довірений вузол, інші сторони-учасники дізнаються про втручання.

Використання квантової заплутаності або суперпозиції в акті спостереження фотонів у квантовому розподілі ключів вносить зміни в систему, зроблюючи будь-яке вторгнення виявленим. Однак квантовий розподіл ключів стикається з трьома основними проблемами:

1. Інтеграція в існуючу інфраструктуру. Впровадження систем квантового розподілу ключів в поточну інфраструктуру представляє собою складне завдання. Навіть якщо теоретично це є безпечним процесом, практичні проблеми виникають через недосконаліть інструментів, таких як детектори одиночних фотонів, які можуть створити вразливості в системі безпеки. Тому впровадження потребує ретельного аналізу безпеки.

2. Обмеження відстані. Волоконно-оптичні кабелі, хоч і є високоефективними для передачі квантової інформації, мають свої обмеження щодо відстані, на яку може бути ефективно поширена квантова інформація.

Сучасні стандартні волоконно-оптичні кабелі, як правило, мають обмеження радіусу дії, який становить приблизно 100 км. Однак, деякі дослідження та розробки спрямовані на розширення цього діапазону. Наприклад, Женевський університет розробив систему, яка дозволяє передавати фотони на відстань до 307 км за ідеальних умов.

Крім того, компанія Quantum Xchange вивела на ринок мережу в США, яка пропонує позасмугову доставку квантових ключів і здатна працювати на необмежені відстані. Ця технологія використовується для забезпечення безпеки комунікацій і може бути ефективною навіть на великих відстанях, де традиційні волоконно-оптичні кабелі можуть виявлятися менш ефективними.

3. Вимога до каналу автентифікації. Квантовий розподіл ключів передбачає наявність класичного каналу автентифікації зв'язку заздалегідь. Це означає, що користувачі повинні вже обмінятися симетричним ключем для забезпечення певного рівня безпеки. Важливо відзначити, що розширені стандарти шифрування

можуть забезпечити достатній захист, незалежно від квантового розподілу ключів. Однак зі зростанням поширеності квантових комп'ютерів зростає ризик їх використання зловмисниками для злому поточних методів шифрування, що робить квантовий розподіл ключів актуальним для забезпечення довгострокової безпеки.

Незважаючи на теоретичну безпеку, практична реалізація квантових розподілів ключів може впроваджувати вразливості, які можуть скомпрометувати їх безпеку. У реальних програмах було виявлено методи, які можуть зламати такі системи. Наприклад, навіть не дивлячись на те, що протокол BB84 був розроблений з метою забезпечення безпеки, досягнення ідеальної реалізації залишається викликом.

Одним з таких методів атаки є атака із зміною відображення фази, метою якої є створення прихованої точки входу для перехоплювачів. Ця атака використовує потребу сторін дозволяти сигналам входити та виходити з їхніх пристроїв, використовуючи методи, що зазвичай застосовуються в комерційних системах квантового розподілу ключів.

Атака поділу кількості фотонів використовує вразливість у процесі передачі квантових фотонів, де, в ідеальному сценарії, повинен передаватися лише один фотон від користувача до отримувача. Однак на практиці можуть відбуватися надсилання додаткових фотонів, які можуть бути перехоплені без виявлення. З метою протидії цьому типу атаки, було введено удосконалення протоколу BB84, відоме як стан КРК.

Техніка стану КРК передбачає включення набору сигналів-приманок поряд із запланованими сигналами BB84. Це дозволяє обом сторонам, які здійснюють обмін квантовими фотонами, виявити присутність можливого перехоплювача. Спостерігаючи реакцію на сигнали-приманки, учасники можуть виявити будь-яку недійсність чи втручання в квантовому обміні. Це покращення спрямоване на підвищення надійності і безпеки квантових протоколів передачі ключів, зменшуючи ймовірність успішної атаки поділу кількості фотонів. [12].

Протокол BB84, представлений у 1984 році Чарльзом Беннетом і Жильом Брассаром, є важливим квантовим протоколом, що ґрунтується на принципі невизначеності Гейзенберга. Цей принцип стверджує, що в квантовій системі неможливо точно визначити одночасно дві властивості - положення та імпульс. Квантова криптографія успішно використовує цей принцип, застосовуючи поляризацію фотонів, які можуть передаватися по волоконно-оптичних лініях, у різних базах, як сполучені властивості.

Протокол BB84 отримав свою назву на честь своїх авторів та року публікації, і він став одним із найвизначніших квантових протоколів. Його успішність полягає в тому, що він забезпечує безпеку передачі квантових ключів через віддаль та може виявити будь-які спроби перехоплення чи вторгнення.

Багато інших квантових протоколів, побудованих на основі BB84, розглядаються як його аналоги і використовують ті ж самі принципи для забезпечення безпеки обміну квантовими ключами.

У протоколі BB84 Емелі може передавати випадковий секретний ключ Марку, відправляючи послідовність фотонів, в яких закритий ключ закодовано з використанням їхньої поляризації. Теорема про заборону клонування гарантує, що Емелі не зможе виміряти ці фотони та передати їх Марку, не порушивши стан фотонів помітним чином.

Важливо відзначити, що зазначене твердження є вірним лише за умови відсутності помилок у квантовому каналі. Якщо канал чутливий до помилок, можуть виникати випадки, коли Емелі та Марк не зможуть виявити присутність Лізи.

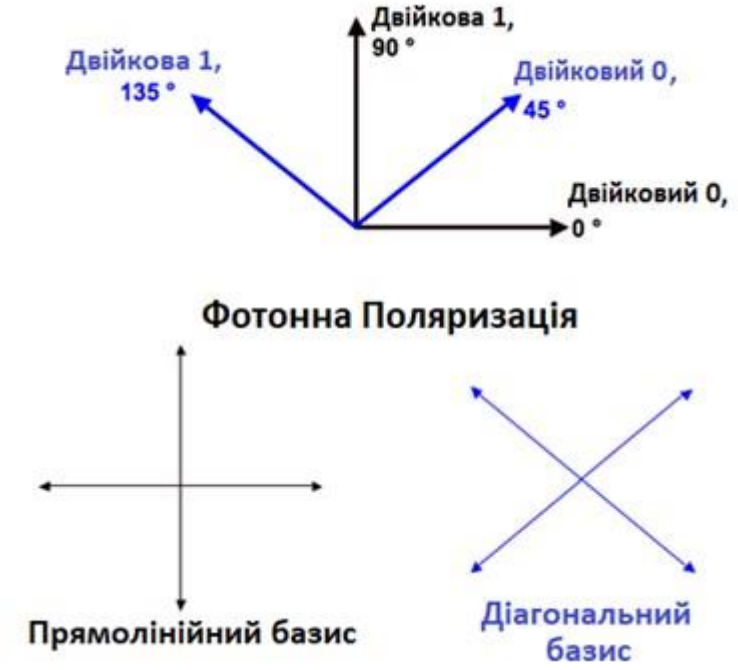

Рисунок 3.2 – Кодування бітів за допомогою поляризації фотона

Протокол BB84 - це квантовий криптографічний протокол, призначений для безпечного обміну криптографічними ключами між Емелі та Марком через квантовий канал. Протокол використовує властивості квантових систем для забезпечення конфіденційності передачі даних.

У протоколі BB84, Емелі та Марк використовують два різних базиси для вимірювання поляризації фотонів. Значення поляризації для двійкового 0 та двійкового 1 визначаються наступним чином:

– 0° для прямолінійного базису та 45° для діагонального базису представляють двійковий 0.

– 90° для прямолінійного базису та 135° для діагонального базису представляють двійковий 1.

Процес передачі даних починається тим, що Емелі випадковим чином генерує два рядки - один для бітів, які вона хоче передати, та інший для відповідних базисів (прямолінійних або діагональних). Далі вона посилає фотон для кожного біта з визначеною поляризацією, що відповідає вибраному базису, через квантовий канал до Марка.

Марк, незалежно, вибирає власні базиси для вимірювання поляризації отриманих фотонів. Якщо обраний Марком базис збігається з базисом Емелі для даного фотона, він може визначити положення поляризації та отримати біт з передачі. У випадку несумісності базисів результат вимірювання стає випадковим.

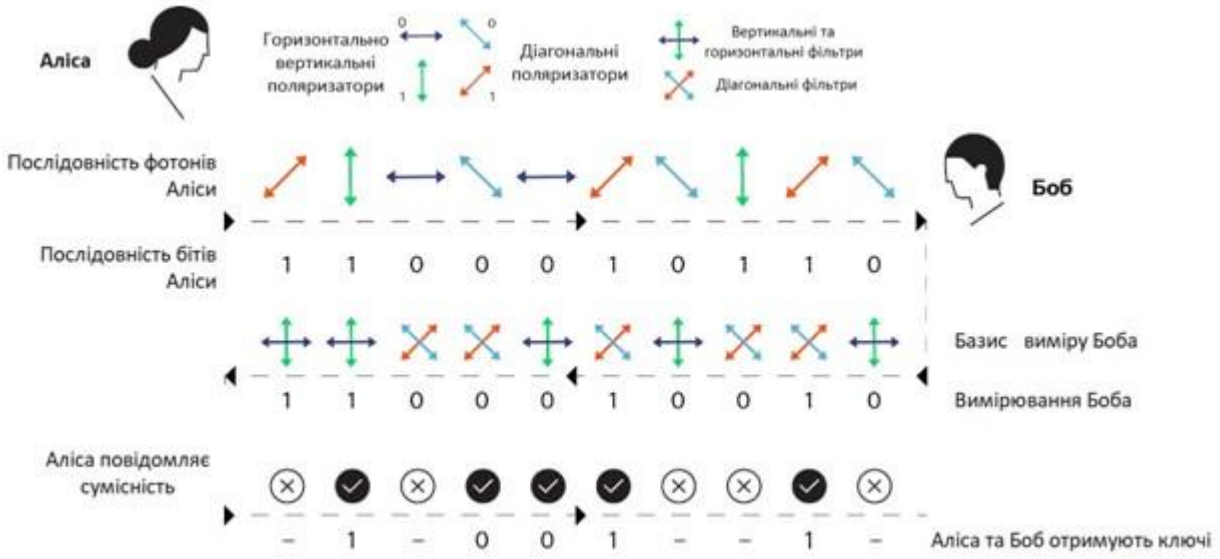

Рисунок 3.3 – Формування криптографічного ключа за допомогою протоколу BB84

На другому етапі Емелі та Марк взаємодіють через традиційний відкритий канал. Марк розповідає Емелі про методи, які він використовував для вимірювання кожного фотона, тоді як Емелі повідомляє Марка про те, які базиси вона використовувала для вимірювань, де її вимірювання співпадають з закодованими бітами. Потім вони відкидають біти, виміряні в різних базисах. Результатом є зміщений ключ - ідентичний бітовий рядок, який є спільним для Емелі та Марка.

Щоб виявити можливу присутність Лізи, Емелі та Марк можуть порівняти підмножину бітів зі зміщеного ключа. Якщо виявляється будь-яка розбіжність у порівнянні бітів, це свідчить про можливий втручання Лізи.

Розглянемо ситуацію, коли Ліза успішно перехоплює деякі фотони, що передаються квантовим каналом. Навіть при використанні однакових базисів відбувається збіг лише на один біт, що вказує на наявність Лізи в каналі. У такому випадку Емелі та Марку слід повторно передавати фотони, використовуючи інший квантовий канал [13].

Протокол із шістьма станами представляє собою специфікацію протоколу з дискретними змінними, що застосовується у квантовому розподілі ключів. На відміну від протоколу BB84, цей протокол спроектований з урахуванням шумових каналів. Відповідно до проведених досліджень, протокол із шістьма станами вносить вищий рівень помилок при спробах прослуховування. Ця підвищена помилковість сприяє виявленню будь-якого несанкціонованого доступу, оскільки прослуховувач повинен правильно вибрати відповідну базу із трьох можливих.

Дослідження підтверджує, що системи великої розмірності, як ті, що використовуються в протоколі із шістьма станами, забезпечують вищий рівень безпеки. Реалізація протоколу можлива без використання квантового комп'ютера і може бути здійснена виключно за допомогою оптичних технологій [14].

Початковий етап протоколу передбачає генерацію випадкового рядка кубітів Емелі. Вона кодує ці кубіти випадковим чином, використовуючи одну з трьох баз, і відправляє їх Марку через безпечний квантовий канал. Кожна база використовується з однаковою ймовірністю 1/3. При отриманні рядка кубітів, Марк також випадковим чином вибирає одну з трьох баз для вимірювання кожного кубіта. Спілкуючись через класичний, але автентифікований канал, Емелі та Марк відкидають вимірювання, де використана база для вимірювання відрізняється від бази кодування. Стани кубітів, де база кодування збігається з базою вимірювання, використовуються для отримання секретного ключа.

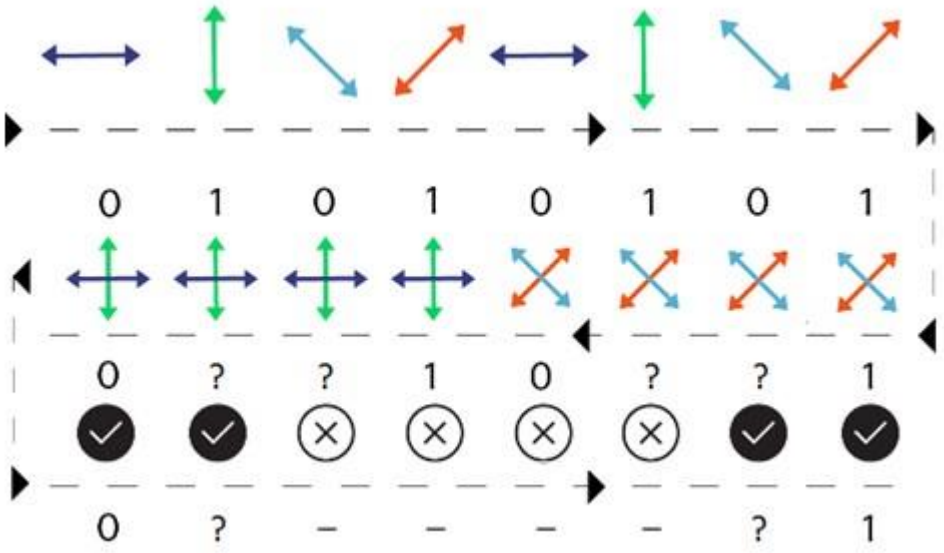

Рисунок 3.4 – Створення криптографічного ключа за протоколом шести станів

Протокол E91 використовує заплутані пари фотонів для створення безпечного каналу зв'язку між Емелі та Марком. Ці заплутані пари можуть бути створені будь-ким із сторін, включаючи Емелі, Марка чи навіть потенційного підслуховувача Лізу. Гарантія розподілу полягає в тому, що Емелі та Марк мають по одному фотону з кожної пари.

Протокол E91 базується на двох ключових властивостях заплутаності. По-перше, заплутані стани демонструють ідеальну кореляцію, тобто коли Емелі і Марка вимірюють вертикальну чи горизонтальну поляризацію своїх частинок, результати завжди збігаються зі 100% ймовірністю. Однак самі результати вимірювань є абсолютно випадковими, і тому Емелі не може передбачити, яку поляризацію вона спостережує і яку побачить Марк. По-друге, будь-яка спроба Лізи підслухати спілкування порушує кореляцію між заплутаними фотонами, яку можуть виявити Емелі та Марк.

Схожий на протокол BB84, протокол передбачає приватний процес вимірювання перед виявленням присутності Лізи. На етапі вимірювання Емелі вимірює кожен фотон, використовуючи одну із заздалегідь визначених баз. Вибір баз залишається конфіденційним до завершення вимірювань. Фотони розподіляються на дві групи: одна група містить фотони, які були виміряні Емелі

та Марко на одній базі, тоді як друга група включає решту фотонів. Щоб виявити підслуховування, обчислюється тестова статистика, використовуючи коефіцієнти кореляції між базами Емелі та Марка. У випадку максимально заплутаних фотонів тестова статистика набуде певного значення. Відхилення від цього очікуваного значення свідчить про втручання Лізив локальний реалізм і порушення теореми Белла. У випадку успішного протоколу перша група фотонів може бути використана для генерації безпечних ключів [15].

3.2 Переваги та недоліки квантової криптографі

Недоліки квантового шифрування:

– Складність реалізації. Реалізація квантового шифрування вимагає високоточних технологій та спеціалізованого обладнання. На даний момент технології, необхідні для ефективної роботи квантових систем, досить дорогі та складні у виготовленні.

– Вразливість до атак з боку квантових обчислювачів. Існує концепція квантових обчислювачів, які можуть потенційно ламати певні алгоритми квантового шифрування. Хоча на сьогоднішній день це ще лише теоретична загроза, необхідно враховувати можливі ризики, пов'язані з розвитком цих обчислювачів.

– Обмеженість дальніх відстаней передачі. Квантове шифрування вимагає фізично заплутаних фотонів для передачі інформації. Однак велика дальність передачі фотонів може вплинути на ефективність системи через втрату сигналу.

– Питання про зберігання та стабільність кубітів. Зберігання квантових інформаційних одиниць (кубітів) виявляється складним завданням через взаємодію з оточуючим середовищем, що може призвести до втрати квантової стабільності.

– Висока вартість інфраструктури. Впровадження квантового шифрування вимагає значних витрат на створення та підтримку відповідної інфраструктури, яка б забезпечувала безперебійну роботу систем.

– Потреба в постійному вдосконаленні. Швидкий розвиток технологій може вимагати постійного вдосконалення квантових систем для підтримки високого рівня безпеки та конкурентоспроможності.

Переваги квантового шифрування:

– Покращена безпека зв’язку. Квантова криптографія пропонує вищий рівень безпеки зв’язку порівняно з традиційними методами шифрування. Її основа ґрунтується на законах квантової фізики, що забезпечує сильний захист для обміну даними.

– Різноманітні методи безпеки. Квантові обчислення та фізика відкривають широкий спектр різних методів безпеки, які були обговорені раніше в розділах, що стосуються заплутаності. Поточні дослідження та розробки можуть виявити додаткові методи в майбутньому.

– Непорушність ключів шифрування. В квантовому шифруванні використовуються квантові властивості частинок для генерації та передачі ключів шифрування. Це забезпечує непорушність ключів від прослуховування або підміни, оскільки будь-яка спроба перехоплення або зміни квантового стану частинок буде помічена, і комунікаційні сторони можуть виявити такі спроби.

– Широкий спектр застосувань. Квантове шифрування може бути успішно застосоване в різних галузях, таких як фінанси, комунікації, урядові структури, облік та зберігання даних, медицина. Це дозволяє використовувати його в різних сферах життя, де безпека даних є критично важливою.

3.3 Обмеження та труднощі, які виникають у квантових комунікаційних системах

Розвиток квантових технологій викликає значний інтерес і призводить до ряду важливих досягнень та перспективних проектів. Ці нові можливості створюють нові технологічні галузі та перспективи для подальшого впровадження в різні сфери життя.

Наприклад, Кембриджська дослідницька лабораторія Toshiba досягла революційного прориву в області квантової комунікації. Успішно демонструючи передачу квантової інформації через оптичні волокна з довжиною понад 600 км, вони створили можливість для квантово-захищеної передачі інформації між містами. Це відкриття наближає нас до реалізації глобального квантового інтернету.

Глобальний квантовий інтернет передбачає об'єднання квантових комп'ютерів через міжміські квантові канали зв'язку. Така інфраструктура може вирішити складні завдання оптимізації в хмарних обчисленнях, створити точну глобальну систему часу та забезпечити високозахищені глобальні комунікації.

Так, ефективна передача квантових бітів чи кубітів по довгих оптичних волокнах є однією з ключових технологічних викликів у створенні квантового інтернету. Кубіти, які використовуються для квантового обміну інформацією, мають властивість крихкості, що робить їх вразливими до зовнішніх збурень.

Одним із основних факторів, які впливають на ефективність передачі квантових бітів, є коливання температури. Зміни температури можуть викликати розширення та звуження оптичних волокон, що в свою чергу може порушити стан квантових бітів, передаваних слабкими оптичними імпульсами.

Інноваційна технологія "дводіапазонної" стабілізації, впроваджена компанією Toshiba, є значним кроком у вирішенні проблем передачі квантових бітів через довгі оптичні волокна. Цей метод використовує два оптичних опорних сигнали на різних довжинах хвиль для мінімізації коливань фази на значній відстані волокна.

Перший опорний сигнал призначений для запобігання швидким коливанням, тим самим забезпечуючи стабільність передачі в умовах змін температури та інших факторів. Другий сигнал синхронізує оптичні кубіти та точно налаштовує фазу, що важливо для збереження цілісності переданої інформації.

Це нововведення дозволяє досягти надзвичайної стабільності, зберігаючи оптичну фазу квантових сигналів з нанометровою точністю навіть після

розповсюдження через великі відстані оптичного волокна (сотні кілометрів). Такий підхід є критичним для успішної передачі квантових бітів на великі відстані та викорінення проблем, пов'язаних із збуреннями середовища.

Такі досягнення в розвитку квантового зв'язку на великій відстані є вражаючими і відкривають нові перспективи для безпечної квантової передачі інформації в глобальному масштабі. Технологія дводіапазонної стабілізації, яку впроваджує Toshiba, виявляється ключовою у подоланні технічних обмежень та збільшенні відстані для квантового розподілу ключів (КРК).

Зазвичай торгові системи КРК мають обмеження приблизно 100-200 км оптичного волокна. Однак впровадження протоколу Twin Field і технології дводіапазонної стабілізації дозволяє Toshiba подолати це обмеження. Протокол Twin Field був спроектований для збільшення відстані КРК, і завдяки технології дводіапазонної стабілізації компанія успішно впроваджує його на довгих відстанях.

Результатом цього є можливість реалізації квантового розподілу ключів на вражаючій відстані в 600 км. Це відкриває можливість для безпечної обміну квантовими ключами між великими географічними областями, наближаючи нас до мети глобального квантового зв'язку.

Такий прорив в розвитку квантового розподілу ключів, як використання технології дводіапазонної стабілізації компанією Toshiba, відкриває широкі можливості для розширення відстані квантового зв'язку і застосування цих методів до різних протоколів і програм квантового зв'язку. Це важливий крок, який сприяє розвитку безпечних та надійних квантових мереж.

Покращення в передачі квантових бітів на великі відстані дозволяє подолати попередні обмеження і полегшує зв'язок між містами, країнами і навіть континентами, не залежачи від надійних проміжних вузлів. Це важливо для розвитку глобального квантового зв'язку, який має великий потенціал в різних сферах, включаючи безпеку комунікацій, обчислення та передачу інформації.

Крім того, створення платформи для послуг квантової інформаційної технології показує широкий вектор інтересів компанії. Ця платформа може

сприяти не лише безпечному глобальному зв'язку, але й трансформаційним технологіям, таким як хмарні квантові обчислення та розподілене квантове зондування. Це свідчить про те, що квантові технології можуть вирішувати складні завдання і приводити до інновацій в різних галузях.

Ці події є вражаючими кроками вперед у розвитку квантових технологій і квантового зв'язку та відкривають нові горизонти для впровадження інновацій у сфері безпеки зв'язку та технологій космічного зв'язку.

Успішне встановлення промислової квантово-захищеної мережі в Великобританії з використанням мультиплексної сумісності Toshiba є важливим кроком у напрямку ефективного та безпечного квантового зв'язку. Можливість передавати дані та квантові ключі по одному волокну без потреби у встановленні додаткової інфраструктури для розподілу ключів робить цей підхід привабливим для практичного впровадження в реальних умовах.

Супутник квантового зв'язку Китайської академії наук, який був запущений у 2016 році, є іншим значущим досягненням. Цей супутник успішно подолав розрив між квантовими технологіями та космічним зв'язком, виконавши ряд новаторських демонстрацій. Це відкриває перспективу для майбутнього розвитку квантового космічного зв'язку, що може охоплювати всю планету та впливати на подальший розвиток космічних та квантових технологій..

Проблема втрат світла при передачі квантового зв'язку на великій відстані дійсно єскладною технічною задачею, і вона виникає з ряду фізичних обмежень. В класичних оптичних системах втрати світла можуть бути компенсовані за допомогою оптичних підсилювачів, що не є ефективним для квантового зв'язку через його чутливість до втрат квантової інформації при підсилених фотонах.

Дослідники шукають різні шляхи розв'язання цієї проблеми, і одним із напрямків є розробка квантових ретрансляторів. Ці пристрої призначені для підсилення квантової інформації без спотворень. Однак їхнє впровадження для міжконтинентального квантового зв'язку залишається в далекому майбутньому через технічні та вартісні виклики.

Наразі одним з рішень є використання оптичного каналу вільного космосу, який з'єднує низькоорбітальні супутники з поверхнею Землі. Цей підхід має перевагу, оскільки фотони подорожують через практично вакуумне середовище з мінімальним поглибленням і розсіюванням, за винятком нижньої частини атмосфери. Такий метод може стати кроком у напрямку подолання обмежень міжконтинентального квантового зв'язку та розширенням можливостей для безпечної передачі квантових ключів на великі відстані.

Передача світла від супутника до Землі дійсно постає з низкою труднощів. Однією з основних проблем є постійне вирівнювання телескопів супутника та наземних станцій для оптимізації передачі сигналу. Цей процес може бути нарушений атмосферними умовами, що призводить до випадкових відхилень та спотворень світлових променів. Крім того, супутник і наземна станція повинні синхронізувати свої годинники для точної ідентифікації фотонів сигналу на основі часу їх приходу.

Супутник Micius вирішує ці проблеми за допомогою інтерферометра, в якому фотони "накачування" розщеплюються нелінійним кристалом на пари заплутаних фотонів. Шляхи інтерферометра призводять до сплутування станів поляризації пар фотонів. Супутник може випромінювати понад 5 мільйонів заплутаних пар фотонів на секунду, які потім передаються на наземні станції.

Після запуску на орбіту висотою 500 км супутник Micius успішно провів серію демонстрацій у співпраці з наземними станціями на різних континентах. Одним із ключових досягнень була демонстрація розподілу заплутаності на великій відстані. У 2017 році експеримент показав, що заплутані фотони з пари можуть бути розділені та передані на дві станції, розташовані на відстані 1200 км одна від одної в Китаї, зберігаючи при цьому їх заплутаність. Цей прорив більш ніж удвічі перевищив попередній рекорд відстані, досягнутий за допомогою оптичних волокон.

Лише через 10 днів після запуску Micius також продемонстрував квантовий розподіл ключів між супутником і наземною станцією поблизу Пекіна. Використовуючи протокол BB84, він успішно поділився приблизно 300

кілобітами випадкового ключа за 273 секунди, що було достатньо для щоденного обміну 256-бітним ключем.

Використовуючи систему квантового розподілу ключів (КРК), супутник Micius розповсюдив 100 кілобайт захищених ключів на наземні станції в Китаї та Австрії. Ці ключі були використані для захисту 75-хвилинної відеоконференції між Пекіном і Віднем за допомогою 128-бітних ключів. Однак дослідники прагнули досягти заснованого на заплутаності квантового розподілу ключів між двома наземними станціями, не покладаючись на це припущення. Завдяки різноманітним удосконаленням системи, вони змогли досягти цієї мети, увімкнувши КРК між двома наземними станціями, розділеними на відстані понад 1100 км. Однак досягнутий безпечний ключ становив лише 6 біт, що було достатньо для демонстрації технології, але не практично для реальних додатків. Для розробки життєздатної системи супутника з подвійною наземною станцією знадобляться більш ефективні канали зв’язку та підвищена швидкість генерації заплутаних фотонів.

Останні роки свідчать про рост інтересу до квантового машинного навчання (КМН) в контексті обробки великих обсягів даних у додатках 5G і 6G. Зростання розмірів даних у цих додатках викликало проблеми з обчислювальною потужністю та часом при використанні традиційних методів машинного навчання. Квантові обчислення обіцяють вирішити ці проблеми, забезпечуючи вищу швидкість та більш ефективне вирішення складних завдань.

КМН використовує принципи квантової фізики, такі як квантова суперпозиція та заплутаність, для виконання обчислювальних завдань. Науковці також досліджують оптимізацію мереж 5G/6G, поєднуючи машинне навчання з квантовими обчисленнями. Це означає розробку методів, які використовують квантові принципи у процесах навчання та висновків, а також адаптацію класичних алгоритмів до квантово-сумісної мови.

Розробка алгоритмів квантового контролю включає перегляд традиційних методів машинного навчання у контексті квантового середовища. Вчені використовують етапи попередньої обробки для адаптації даних навколишнього

середовища до вхідних даних для квантових комп’ютерів. Останні роки принесли значний прогрес в алгоритмах квантового машинного навчання, що внесло вагомий вклад у різні галузі досліджень.

Однак декогеренція квантових станів є значущою проблемою. Це явище виникає внаслідок взаємодії квантових систем із зовнішнім середовищем, призводячи до втрати квантової надгнучкості та змін в квантовому стані. Декогеренція може бути спричинена тепловими ефектами, коливаннями фононів, взаємодією з електромагнітним випромінюванням та іншими факторами.

Дослідники працюють над розробкою методів контролю та управління квантовими станами для підтримки їх стабільності в умовах декогеренції. Це може включати в себе застосування методів корекції помилок, адаптивних стратегій та нових алгоритмів для ефективного контролю над квантовими бітами.

Окрім цього, важливим аспектом є розробка квантових апаратів, які мають високу устійкість до декогеренції. Винаходження нових матеріалів та архітектур, що дозволяють зберігати квантову інформацію без значної деградації, є великим викликом для вчених у цій області. Розвиток таких устійких систем є ключовим для подальшого успіху квантових обчислень та інших застосувань квантової технології.

Також, разом із збільшенням кількості кубітів, зростає складність управління їх взаємодією та забезпечення стабільності квантового обчислювального процесу. Проблема утримання кубітів у стані заплутаності та уникнення декогеренції є ключовою для досягнення ефективної роботи квантового комп'ютера.

Зараз існують різноманітні підходи до розв'язання цих питань. Наприклад, використання квантових бітів, які базуються на особливих об'єктах або структурах, таких як топологічні кубіти, може сприяти збереженню стабільності квантових станів. Також, розробка нових методів управління та корекції помилок важлива для забезпечення точності обчислень.

Ще однією перспективою є використання квантових мереж, де кілька малих квантових процесорів можуть працювати разом. Це може полегшити управління

та збереження стабільності великої кількості квантових бітів, але також вимагатиме розробки нових методів синхронізації та координації між цими процесорами.

Точна, розробка високоякісного квантового обладнання є ключовим елементом у впровадженні квантових обчислень та інших квантових технологій. Одним з важливих викликів є збереження квантової стабільності і подолання декогеренції кубітів, що може виникати внаслідок взаємодії з навколишнім середовищем.

Розробка програмного забезпечення для квантових комп'ютерів включає ряд викликів і вимагає нових підходів до програмування. Одним з ключових аспектів є створення мов програмування та інструментів оптимізації, спрямованих на ефективне використання квантових обчислювальних ресурсів. Також, інтерфейси програмування (API) мають надавати доступ до функціональності квантового апаратного забезпечення.

Нові концепції та підходи до розробки квантових алгоритмів вимагають від програмістів усвідомлення принципів квантової фізики та їх впливу на обчислення. Для цього можуть бути потрібні нові методи навчання та навички.

Розробка ефективних API для взаємодії з квантовим апаратним забезпеченням є важливою, оскільки вони визначають можливості програмістів у роботі з квантовим обладнанням. Це охоплює створення інтерфейсів для керування кубітами, виконання квантових гейтів та отримання результатів обчислень.

Бібліотеки квантових алгоритмів і стандартні модулі грають важливу роль у полегшенні розробки складних квантових програм. Їх розвиток сприяє стандартизації та робить квантове програмування більш доступним і зрозумілим для широкого кола розробників.

Співпраця між різними галузями, включаючи квантову фізику, комп'ютерну науку та математику, є важливою для успішного розвитку програмного забезпечення для квантових комп'ютерів.

Розробка стандартів та протоколів грає ключову роль у стандартизації квантових систем, сприяючи сумісності між платформами та рішеннями. Основні напрямки цього процесу включають апаратне забезпечення, програмне забезпечення та комунікаційні протоколи.

Стандарти для апаратного забезпечення визначають специфікації компонентів квантових систем, таких як кубіти, зчитувачі та детектори. Це сприяє розробці сумісного обладнання, яке легко інтегрується з різними програмними рішеннями.

Стандарти програмного забезпечення визначають специфікації для мов програмування, компіляторів, оптимізаторів та інструментів розробки квантових алгоритмів. Це сприяє створенню програм, які легко адаптуються до різних квантових платформ та архітектур.

Стандарти комунікаційних протоколів визначають специфікації для передачі даних між квантовими системами та зовнішніми пристроями. Це включає протоколи обміну даними, протоколи керування та протоколи забезпечення безпеки.

Бенчмаркінг визначається як ще один важливий аспект розвитку квантових обчислень. Це передбачає створення стандартних тестів та метрик для оцінки продуктивності квантових систем. Бенчмарки допомагають визначити ефективність та якість різних реалізацій квантових обчислень, сприяючи удосконаленню технологій та алгоритмів.

Узагальнюючи, ці стандарти та протоколи сприятимуть стабільному розвитку квантових обчислень, підвищать сумісність між системами та забезпечать надійність та ефективність використання квантових ресурсів.

3.4 Застосування квантової комунікації в майбутньому та потенціал у різних сферах

Квантовий зв'язок для захисту представляє собою інноваційний напрямок в оборонній сфері, спрямований на забезпечення високого рівня конфіденційності

та цілісності важливої інформації. Основні аспекти квантового зв'язку для захисту включають:

– Квантовий розподіл ключів. Використання квантового розподілу ключів для безпечного обміну ключами між військовими об'єктами, такими як супутники, літаки та транспортні засоби. Забезпечення захищеного каналу зв'язку, що є імунним до перехоплення чи вторгнення.

– Захист від шпигунства. Квантова комунікація забезпечує захист від шпигунської діяльності та перехоплення важливої військової інформації. Квантові стани не можуть бути перехоплені без помітного впливу на передачу даних, що робить їх ідеальними для створення захищеного зв'язку між військовими об'єктами.

– Квантовий радар. Використання квантових технологій для розробки квантових радарів з високою роздільною здатністю та точністю визначення об'єктів у просторі. Корисно для військових операцій, зокрема для виявлення та слідкування за наземними, повітряними або морськими об'єктами.

– Квантове глушіння. Розробка систем квантового глушіння, які перешкоджають ворожим радарам та комунікаційним системам.

Використання квантових технологій для створення ефективних засобів електронної боротьби.

Використання нової квантової технології для вирішення фінансових проблем, зокрема тих, що пов'язані з невизначеністю та обмеженою оптимізацією, надає значні переваги тим, хто приймає її в першу чергу. Це дозволяє розраховувати можливості динамічного арбітражу, недоступні для конкурентів. Крім того, квантові обчислення, серед інших переваг, можуть забезпечити більшу відповідність вимогам, використовувати дані про поведінку для підвищення залученості клієнтів та забезпечити швидшу реакцію на нестабільність ринку.

Ключовою перевагою квантових обчислень є величезний простір рішень, який на порядки перевершує той, що доступний традиційним комп'ютерам, навіть найпотужнішим. У класичних обчисленнях подвоєння обчислювальної потужності вимагає подвоєння кількості транзисторів, які працюють над

проблемою. Однак у квантових обчисленнях додавання всього одного кубіта може приблизно подвоїти обчислювальну потужність.

Хоча до широкого комерційного застосування може залишитися кілька років, очікується, що квантові обчислення нададуть проривні продукти та послуги, які ефективно вирішуватимуть конкретні бізнес-проблеми протягом трьох-п'яти років.

Крім того, можливості квантових обчислень відкривають нові перспективи для трансформації операційних процесів у сфері фінансових послуг. Ця технологія має потенціал змінити підхід до різних аспектів, таких як:

– Управління казначейством, торгівля та стратегії управління активами.

– Оптимізація бізнес-процесів, включаючи ефективне управління ризиками.

У галузі фінансових послуг конкретні застосування квантових обчислень можна розглядати у трьох ключових напрямках: націлене прогнозування, оптимізація торгівлі та аналіз ризиків.

Хмарні обчислення надають користувачам можливість використовувати ресурси для обчислень і зберігання даних, переховуючи їх на комп'ютерах або серверах, що розташовані у центрах обробки даних, а не локально на їхніх власних персональних комп'ютерах. Зазвичай користувачі отримують доступ до цих центрів обробки даних через мережеве підключення, таке як інтернет. Квантова хмара працює на аналогічному принципі, але забезпечує доступ до квантових комп'ютерів, а не звичайних.

Сліпі квантові обчислення відкривають можливість користувачам використовувати квантові комп'ютери через квантову хмару, приховуючи структуру та алгоритми своїх обчислень від квантового комп'ютера. Іншими словами, квантовий комп'ютер залишається "сліпим" до даних і обчислень користувачів.

Підключившись до квантової хмари через мережу з функціями збереження конфіденційності, користувачі можуть комбінувати квантові обчислення з квантовим зв'язком. Це гарантує, що їхні дані та квантові обчислення залишаються повністю "сліпими". Завдяки анонімному квантовому зв'язку дані

користувача стають практично недоступними для будь-кого в мережі, включаючи інших користувачів і сам квантовий комп'ютер.

Сліпі квантові обчислення мають як свої переваги, так і ризики. З одного боку, вони можуть значно підвищити безпеку та захист конфіденційних даних для урядових і неурядових організацій, захищаючи інформацію та приховуючи чутливі проблеми від розголошення.

Однак існують серйозні наслідки та потенційні загрози, пов'язані зі сліпими квантовими обчисленнями. Сполучений "сліпий" аспект із великими обчислювальними ресурсами квантових обчислень може стати метою зловживання злочинцями та терористами, які потенційно можуть використовувати цю технологію для розробки нових видів зброї, зламу державних систем даних або підриву економіки через злам протоколів шифрування.

Розподілені квантові обчислення використовують концепцію розподілених обчислень, де завдання розбиваються на менші частини і розподіляються між кількома віддаленими квантовими комп'ютерами, які функціонують як єдина система. Ця мережева архітектура дозволяє квантовим комп'ютерам співпрацювати над вирішенням складних проблем, використовуючи їхні унікальні характеристики.

Аналогія з лазерами може вказати на те, що, хоча квантові комп'ютери можуть не замінити традиційні обчислювальні системи, вони відкривають нові можливості у різних галузях. Подібно до того, як лазери знайшли застосування в хірургії очей та лазерному друку, квантові комп'ютери можуть мати непередбачувані застосування, які перейдуть за межі поточних обчислювальних концепцій.

Окрім потенційного використання для зламу шифрування в Інтернеті, існує безліч інших застосувань квантових комп'ютерів, які зараз можуть залишатися поза межами нашого уявлення. Деякі організації навіть надають відкритий доступ до квантових комп'ютерів через Інтернет, сприяючи дослідженню нових програм і розвитку інноваційних ідей щодо використання цієї трансформаційної технології.

4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок капітальних витрат на розробку

Капітальні витрати на розробку становлять:

$$К=К1+К2 \quad (4.1)$$

де: К1– витрати на розробку, грн.;

К2– витрати на налагодження і дослідну експлуатацію програмного засобу на ПК, грн.;

4.2 Складові структури витрат на розробку

Складові структури витрат на розробку та реалізацію розробки розраховуються за формулою:

$$К1=Зз+Нз+Ві, \quad (4.2)$$

де: Зз – загальна зарплата розробників, грн;

Нз – нарахування на зарплату, грн;

Ві – інші витрати, грн;

Для проведення розрахунків зарплати (Зз) необхідно визначити спеціальність робітників, чисельність робітників і трудомісткість цих робіт. Для розробки проектного рішення потрібно чотири спеціалісти розробники:

– Керівник проекту(К);

–Студент-дипломник(СД);

– Консультант з економічне ї частини(КЕ);

– Консультант з охорони праці(КОП);

Згідно з штатним розписом сума витрат на оплату праці робітників, з 01.01.2025р. складає:

– Керівник (викладач вищої категорії) – 107,93 грн/год;

– Консультант з економічної частини (викладач вищої категорії) – 107,93 грн/год;

– Консультант з охорони праці(викладач першої категорії) 93,70 грн/год;

– Час витрачений керівником – tk = 14 годин.

– Час витрачений консультантом з охорони праці – tko= 1 година.

– Час витрачений консультантом з економічної частини–tke = 1 година.

– Час витрачений студентом дипломником tc = 3×50= 150 годин.

Витрати на оплату праці керівника проекту:

Ск = 14 роб.год.× 107,93 грн.год.=1511,02 грн.

Витрати на оплату праці консультанта з економічної частини:

Ске = 1 роб.год.×107,93грн.год.= 107,93 грн.

Витрати на оплату праці консультанта з охорони праці :

Ско = 1 роб.год×93,70грн.год.= 93,70грн.

Денна оплата студента дипломника :

1510/173=8,73 грн.

1510 – стипендія

173 – місячний фонд робочого часу, годин.

Витрати на оплату праці студента дипломника

Сс = 8,73×150= 1310 грн.

Витрати на оплату праці робітників проектустановлять

Зз= Ск+Ске+Ско+Сс= 1511,02 +107,93 +93,70 +1310= 3022,65 грн.

Нарахування на зарплату визначаються в розмірі 22% від фонду оплати праці

Нз = Зз×22% = (3022,65 ×22)/100 = 664,98 грн.

де 22 – норматив нарахування на зарплату, %

Інші витрати Ві відображають витрати які, не враховані в попередніх статтях витрат. Ці витрати розраховуються згідно структури витрат(5%)

Ві = 0.05×(Зз+Нз)= 0.05×(3022,65 +664,98)=1843,93 грн.

К1 = Зз+Нз+Ві= 3022,65 +664,98 +1843,93 =5578,56 грн.

4.3 Витрати на відлагодження розробки

Витрати на від лагодження та дослідну експлуатацію розробки

$$К2 = Sм\text{-}г. \times t \quad (4.3)$$

де Sм-г. – вартість однієї машино-години роботи конкретно ПК, грн./год.;

t–машинний час, витрачений на накладку та дослідну експлуатацію програмного засобу, год.

Вартісь 1 машинно-години роботи ПК розраховуємо за складовими витрат на таку роботу:

$$Sм\text{-}г =(А+Ен)/Фд \quad (4.4)$$

де А – амортизація використаного ПК, грн;

Ен – вартість електроенергії, яку споживає ПК, грн.;

Фд – дійсний час від лагодження програми, год.;

Розрахунок складових вартості 1 машино-години роботи ПК:

а) амортизація ПК становить

А= (Кт×На)/100 = (670,31 ×15%)/100= 100,55 грн.

Де Кт – вартість використання ПК, грн..

На – норма амортизації (На=15%)

Кт = (Кс×Тексп)/Твик = (14625×2,2)/48= 670,31 грн.

де Кс – вартість компютероної системи,грн.

Тексп – період експлуатації системи 2.2 місяців(50 робочих днів)

Твик – термін корисного використання 4 роки (48 місяців):

Кс= Ркомп×Р$ = 500×41,00=14625 грн.

де Ркомп –вартість комп'ютерної системи у доларах США;

Р$ – курс долара США по курсу НБУ на момент купівлі системи.

б) вартість використання електроенергії розраховується за формулою:

Ен = (Р×Тф)×Фд×Квик=(0,25 ×5,60)×150×0,8=154,8грн.

де Р – потужність обчислювальної системи, кВт (Р=0,25)

Квик – коефіцієнт використання ПК

Тф – ціна за 1кВт/год.,грн..(Тф = 5,16 грн.)

Фд – дійсний час від лагодження програми

Фд = пр.д.×Тсер= 50р.дн.×3год. = 150год.

Де пр.д. – кількість робочих днів ПК

Тсер = 3 год – середній щоденний час роботи ПК

Отже вартість 1 машино-години роботи і від лагодження на ПК становить

Sм-г=(100,55+154,8)/150= 1,70 грн.

Таким чином сумарні витрати на від лагодження і дослідну експлуатацію проектного рішення становлять:

К2=Sм-г×Фд= 1.70×150=255 грн.

Отже, капітальні витрати на розробку проектного рішення за формулою становлять:

К=К1+К2 = 5578,56 + 255 = 5833,56 грн.

Загальний кошторис витрат на розробку проектного рішення приведений в таблиці 4.1

Таблиця 4.1 – Кошторис витрат на розробку проектного рішення

Складові елементи витрат	Умовне позначення	Сума витрат, грн
Витрати на оплату праці	Зз	3022,65
Нарахування на зарплату	Нз	664,98
Інші витрати	Ві	1843,93
Разом	К1	5578,56
Витрати на відлагодження	К2	255
Разом К=К1+К2	К	5833,56

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ

5.1 Загальні положення

Визначення поняття охорони праці дається в ст. 1 Закону України від 14 жовтня 1992 р. «Про охорону праці». Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. В поняття охорони праці входять і всі ті заходи, що спеціально призначені для створення особливих полегшених умов праці для жінок і неповнолітніх, а також працівників зі зниженою працездатністю. Охорону праці і здоров'я громадян віднесено до пріоритетних напрямків соціальної політики України. Так, Конституція України одним з основних соціальних прав громадян визначає право кожного на належні, безпечні й здорові умови праці, встановлює, що використання праці жінок і неповнолітніх на небезпечних для їхнього здоров'я роботах забороняється. Завдання охорони праці:

– проектування підприємств, технологічних процесів і конструювання обладнання з обов'язковим виконанням вимог охорони праці;

– знаходження оптимальних співвідношень між різними факторами виробничого середовища, що дозволяє забезпечити мінімум несприятливого впливу їх на здоров'я працівників;

– розробка конкретних заходів щодо покращення умов праці та забезпечення її безпеки на основі застосування у виробництві новітніх досягнень науки і техніки;

– застосування раціональних засобів захисту працівників від впливу несприятливих факторів виробничого середовища, а також втілення організаційних заходів, які нейтралізують або послаблюють ступінь їх впливу на організм людини;

– розробка та застосування методів і засобів оцінки ефективності заходів з охорони праці, що плануються і здійснюються.

5.2 Організація охорони праці на підприємстві

На сучасному етапі науково-технічного розвитку нашої держави питання охорони праці на підприємствах є одним із найактуальніших.

Належна організація охорони праці, яка відповідає вимогам нормативно-правових актів, є основним заходом профілактики та запобігання виробничому травматизму й професійній захворюваності. Крім того, кожним трудовим договором передбачаються зобов’язання роботодавця щодо забезпечення найманих працівників безпечними умовами праці.

Законодавство України покладає на всіх роботодавців обов'язок щодо забезпечення безпечних і нешкідливих умов праці. Витрати на охорону праці на підприємстві згідно зі ст. 19 Закону повинні становити не менше 0,5% від фонду оплати праці за попередній рік, а за невиконання законодавства про охорону праці до підприємства можуть бути застосовані санкції аж до заборони його експлуатації.

Для того щоб не поставити під загрозу існування підприємства, роботодавцю необхідно:

– створити службу охорони праці.

Згідно зі ст. 15 Закону така служба обов'язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці, затвердженого наказом Держкомітету з нагляду за охороною праці від 15.11.2004 № 255. На підставі цього документа також має бути розроблено Положення про службу охорони праці цього підприємства, визначено структуру такої служби, її чисельність, основні завдання, функції та права її працівників. На підприємствах із кількістю працівників менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку.

– Розробити та затвердити на підприємстві положення, інструкції та інші акти з охорони праці.

Обов'язок роботодавця стосовно розробки та затвердження документів, які повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майдан-чиках і робочих місцях, передбачений ст. 13 Закону про охорону праці.

– Організувати проведення інструктажів з питань охорони праці.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 КЗпП зобов'язаний проінформувати його під розпис про умови праці, наявні на його робочому місці, у тому числі про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров'я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

– Забезпечити навчання і перевірку знань з питань охорони праці.

Згідно зі ст. 18 Закону працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, проходять спеціальне навчання і перевірку знань відповідних нормативно-правових актів з охорони праці. Таке навчання з питань охорони праці може проводитись як безпосередньо на підприємстві, так і навчальним центром.

– Подбати про проведення медичних оглядів.

Згідно зі ст. 169 КЗпП роботодавець зобов'язаний за свої кошти організувати проведення попереднього (при прийнятті на роботу) та періодичних (протягом трудової діяльності) медоглядів працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі. Також він зобов'язаний проводити щорічний обов'язковий медогляд осіб віком до 21 року.

– Забезпечити працівників засобами індивідуального захисту.

На роботах із шкідливими й небезпечними умовами праці, а також на роботах, пов'язаних із забрудненням або несприятливими температурними умовами, працівникам згідно зі ст. 164 КЗпП необхідно безкоштовно видавати спеціальний одяг, взуття та інші ЗІЗ.

– Провести атестацію робочих місць.

На підприємствах, де технологічний процес, використовуване обладнання, сировина, матеріали є потенційними джерелами шкідливих і небезпечних виробничих факторів, які можуть негативно впливати на стан здоров'я працюючих, повинна проводитись атестація робочих місць за умовами праці. Така атестація повинна проводитися атестаційною комісією, склад і повноваження якої визначаються наказом по підприємству в строки, передбачені колективним договором, але не рідше одного разу на 5 років. Порядок проведення такої атестації передбачений постановою КМУ від 01.08.1992 № 442. Відомості про результати атестації заносяться в картку умов праці.

– Налагодити облік нещасних випадків.

Згідно зі ст. 22 Закону «Про охорону праці» роботодавець зобов'язаний організувати розслідування та вести облік нещасних випадків, професійних захворювань і аварій у порядку, встановленому постановою КМУ від 30.11.2011 № 1232. За результатами такого розслідування роботодавець повинен складати акт за формою Н-5 (якщо нещасний випадок визнано таким, що не пов'язаний з виробництвом) або Н-1 (якщо він визнаний пов'язаним з виробництвом). Один із примірників повинен видатися потерпілому або іншій зацікавленій особі не пізніше трьох днів з моменту закінчення розслідування.

5.3 Заходи безпеки на робочому місці

Конструкція робочого місця, його розміри та взаємне розташування його елементів повинні відповідати антропометричним, фізіологічним І психофізіологічним характеристикам людини, а також характеру роботи.

Організація робочих місць повинна забезпечувати стійке положення та вільність рухів працівника, безпеку виконання трудових операції виключати або допускати лише в деяких випадках роботу в незручну позиціях, котрі зумовлюють підвищену втомлюваність.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого; всі необхідні для роботи предмети повинні знаходитись поряд з працівником, але не заважати йому;

– ті предмети, котрими користуються частіше, розташовуються ближче, ніж ті предмети, котрими користуються рідше;

– предмети, котрі беруть лівою рукою, повинні знаходитись зліва а ті предмети, котрі беруть правою рукою, повинні знаходитись справа;

– якщо використовують обидві руки, то місце розташування інструментів вибирається з врахуванням зручності захоплювання його двома руками;

– небезпечніше, з точки зору можливості травмування обладнання повинне розташовуватись вище, ніж менш небезпечне. Однак слід враховувати, що важкі предмети під час роботи зручніше опускати, ніж піднімати.

5.4 Санітарно-гігієнічні вимоги

Санітарно-гігієнічні вимоги до умов праці під час виконання роботи мають відповідати визначеним нормативам:

– параметри мікроклімату у приміщенні забезпечували комфортне самопочуття організму. Параметри мікроклімату закритих приміщень унормовані за санітарні норми ДСН 3.3.6.042-99.

– освітлення приміщень та робочих місць забезпечене відповідно до встановлених вимог. Відносно вікна робоче місце розміщено так, що природне світло збоку, переважно з лівого та забезпечувало коефіцієнт природної освітленості не нижче 1,5 %. Освітленість за штучного освітлення в площині робочої поверхні становила 300 – 500 Лк. Відношення яскравості робочих поверхонь було 3:1, а яскравість робочих поверхонь і стін (іншого обладнання) – 5:1. Використана система вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

– Дотримані вимоги до рівнів шуму та вібрації. Було дотримано допустимих рівнів звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях встановлені санітарними нормами виробничого 17 шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

– Надходження свіжого повітря регульоване, виходячи із відповідних нормативних.

– Передбачений захист від шуму та вібрацій.

Дотримані заходи особистої гігієни на робочому місці (підтримання чистоти, миття рук тощо). Заходи особистої гігієни на робочому місці передбачають щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього трудового розпорядку.

ВИСНОВКИ

Проведений аналіз сучасних квантових систем зв'язку у рамках бакалаврської роботи свідчить про великий потенціал цих технологій у різних сферах застосування, зокрема в криптографії, обчислювальній технології та безпеці мереж. Результати опрацювання дозволили визначити квантові системи зв'язку як перспективний напрямок розвитку комунікаційних технологій.

Сучасні квантові системи використовують унікальні явища квантової механіки, такі як квантова заплутаність та квантова суперпозиція, для передачі та обробки інформації. Квантові біти, квантові процесори, лінії зв'язку та квантові повторювачі становлять основу цих систем, забезпечуючи створення, передачу та рецепцію квантових сигналів.

Необхідно врахувати, що, незважаючи на потужні можливості, сучасні квантові системи зв'язку викликають виклики, такі як складність реалізації, чутливість до шуму та високі витрати. Розв'язання цих проблем вимагатиме подальших досліджень, розробок та тісної співпраці між науковими, промисловими та урядовими секторами.

Загалом, результати роботи підтверджують важливість подальшого розвитку квантових технологій у сфері зв'язку та підкреслюють їхню обіцяючу роль у майбутньому розвитку інформаційних технологій.

ПЕРЕЛІК ПОСИЛАНЬ

1. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/
2. https://scienceexchange.caltech.edu/topics/quantum-science explained/entanglement
3. https://scitechdaily.com/what-is-quantum-entanglement-a-physicist-explains-einsteins-spooky-action-at-a-distance/
4. https://theconversation.com/explainer-what-is-wave-particle-duality-7414
5. https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition
6. https://en.wikipedia.org/wiki/Quantum_teleportation
7. С.Е.Остапов,Ю.Г Добровольський Квантова інформатика та квантові обчислення. - Чернівці: ЧНУ, 2021. – 69-73 с.
8. Nielsen,M.QuantumComputationandQuantumInformation/M.Nielsen, I.Chuang—2001.Vol.1.3—P.16-17.
9. https://en.wikipedia.org/wiki/Quantum_algorithm
10. https://esolangs.org/wiki/Quantum_Dimensions
11. TanX.TheoryandPracticeofCryptographyandNetworkSecurity Protocols and Technologies / X. Tan — 2013. P. 35-36.
12. PadamvathiV.QuantumCryptographyandQuantumKeyDistribution Protocols / B. Vardhan, A Krishna — 2016, P. 556–559.
13. https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5
14. Kato,G.SecurityofSixStateQuantumKeyDistributionProtocolwith Threshold Detectors / G. Kato, K. Tamaki — 2016. Vol. 6— P. 1-2.
15. https://en.wikipedia.org/wiki/Quantum_key_distribution.

КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ