

УДК 004.056(075.8)

канд. техн. наук Данилюк І. А. ORCID: 0000-0003-0955-0108 (ВІТІ ім. Героїв Крут)
Лазута Р. Г. ORCID: 0000-0002-8584-1110 (ВІТІ ім. Героїв Крут)
Куцаєв В. В. ORCID: 0000-0001-8213-4739 (ВІТІ ім. Героїв Крут)
Цимбал І. В. ORCID: 0000-0001-7294-3794 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ ПЕРСПЕКТИВ ЗАСТОСУВАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Стрімкий розвиток квантових технологій відкриває нові можливості для військової сфери, зокрема у галузях кібербезпеки, комунікацій, навігації, розвідки та моделювання складних бойових сценаріїв. У статті проведено аналіз сучасного стану досліджень у сфері квантових обчислень, квантової криптографії, квантових датчиків і сенсорик, а також їхнього потенційного застосування для підвищення боєздатності Збройних Сил України. Розглянуто можливості використання квантових алгоритмів для розв'язання складних оптимізаційних завдань, що можуть бути корисними у військовій логістиці, управлінні військовими ресурсами та прогнозуванні загроз.

Окрему увагу приділено перспективам впровадження квантових технологій для створення захищених каналів зв'язку, що унеможливлюють несанкціоноване перехоплення інформації, а також для розробки нових систем навігації, які не залежать від супутникових сигналів і здатні працювати в умовах радіоелектронної боротьби. У роботі також розглянуто основні виклики, що стоять перед впровадженням квантових технологій у військову сферу, зокрема технічні, фінансові та організаційні бар'єри.

На основі проведеного аналізу визначено ключові напрями подальших досліджень, що сприятимуть ефективному впровадженню квантових технологій у сферу оборони України. Запропоновано підходи до створення інноваційної стратегії розвитку квантових технологій у військовій сфері, яка передбачає як наукові дослідження, так і практичну реалізацію їхніх результатів у військових інформаційних системах, системах зв'язку та засобах розвідки.

Ключові слова: квантові технології, квантові обчислення, квантовий зв'язок, квантові сенсори, квантова суперпозиція, квантова запутаність, квантовий генератор випадкових чисел.

I. Danyliuk, R. Lazuta, V. Kutsaiev, I. Tsymbal. Research into the prospects of application of quantum technologies in the Armed Forces of Ukraine

The rapid development of quantum technologies opens up new opportunities for the military sphere, in particular in the fields of cybersecurity, communications, navigation, intelligence and modelling of complex combat scenarios. The article analyses the current state of research in the field of quantum computing, quantum cryptography, quantum sensors and sensors, as well as their potential application to increase the combat capability of the Armed Forces of Ukraine. The possibilities of using quantum algorithms to solve complex optimization problems that can be useful in military logistics, military resource management and threat forecasting are considered.

Particular attention is paid to the prospects for the implementation of quantum technologies to create secure communication channels that prevent unauthorized interception of information, as well as for the development of new navigation systems that do not depend on satellite signals and are capable of operating in electronic warfare conditions. The paper also examines the main challenges facing the introduction of quantum technologies into the military sphere, in particular technical, financial and organizational barriers.

Based on the analysis, key areas of further research have been identified that will contribute to the effective introduction of quantum technologies into the defense sector of Ukraine. Approaches to creating an innovative strategy for the development of quantum technologies in the military sphere, which involves both scientific research and the practical implementation of their results in military information systems, communication systems and intelligence means, have been proposed.

Keywords: quantum technologies, quantum computing, quantum communication, quantum sensors, quantum superposition, quantum entanglement, quantum random number generator.

Вступ

За останнє десятиліття квантові технології стали однією з найдинамічніших галузей наукових досліджень, що підтверджується значним зростанням кількості публікацій та міжнародних дослідницьких проєктів. Дослідження у сфері квантових обчислень уже продемонстрували можливість квантової переваги, коли квантові процесори перевершують

класичні суперкомп'ютери у виконанні спеціалізованих обчислювальних задач. Водночас у квантовій криптографії досягнуто значного прогресу, зокрема реалізовано практичні системи квантової комунікації, що підтверджено успішними експериментами в різних країнах.

Значна увага приділяється і підготовці квантових спеціалістів, що знайшло відображення у зростанні кількості освітніх програм, курсів та досліджень, присвячених методикам навчання у цій сфері. Проведені роботи підкреслюють важливість міждисциплінарного підходу, що включає знання з фізики, математики, комп'ютерних наук та інженерії, а також необхідність розвитку лабораторної інфраструктури й тісної співпраці між науковими установами та промисловістю. Усі ці аспекти активно досліджуються та відображені в численних наукових публікаціях, що висвітлюють сучасний стан і перспективи розвитку квантових технологій.

Аналіз публікацій за темою дослідження

У роботі [1] викладено історію квантових обчислень, основи квантової інформації, квантові алгоритми та квантові криптографічні системи.

У роботі [2] авторами запропоновано послідовний виклад фізичних основ і математичного апарату квантової механіки та їх застосування до різних задач, що є гарною основою для початкової підготовки військових квантофахівців.

Робота [3] представляє квантовий алгоритм розпізнавання оптичних образів на растрових зображеннях, який реалізується на основі квантових логічних елементів Тоффолі та оператора Гровера. Показано, що реалізація квантового алгоритму розпізнавання образів дає змогу порівняно із класичними алгоритмами експоненційно скоротити обсяг необхідної пам'яті та поліноміально зменшити час виконання алгоритму внаслідок реалізації квантового паралелізму. Автори вважають, що застосування схожих алгоритмів надасть можливість використати квантовий комп'ютер, складений з 1–2 млн. кубітів, який буде здатен розв'язувати складні питання планування, розвідки, логістики, криптографії в інтересах Збройних Сил України.

У роботі [4] автори розглядають проблеми квантових обчислень, квантові алгоритми Шора, Гровера та квантове перетворення Фур'є, що також є основою для сучасних досліджень, стосовно використання квантових технологій в Збройних Сил України.

У роботі [5] автори розглядають фотонні системи з однокубітними квантовими обчисленнями, що може стати корисним при підготовці військових квантофахівців.

У роботі [6] пропонується нове ефективне перетворення великого об'єму неструктурованих текстових даних на просторову. Це дозволить здійснювати конверсію великих наборів текстової інформації, таких як звіти, замовлення, листи й інші документи, на точкові класи просторових об'єктів у географічних інформаційних системах. Для опрацювання цієї проблеми у новому перспективному підході авторами пропонується поєднання гібридних квантово-класичних нейронних мереж із геоінформаційними технологіями.

У роботі [7] викладено питання, які стосуються нестационарного та стаціонарного рівнянь Шредінгера, фізичного змісту хвильової функції. Проаналізовано співвідношення невизначеностей Гайзенберга та принцип доповнювальності Бора. Це надає можливість військовим квантофахівцям ефективно опанувати принципи фізики квантових частинок та приєднатись до використання квантових технологій в інтересах Сил оборони України.

У роботі [8] викладено основи виконання квантових розрахунків за допомогою квантових процесорів, із суттєвим використанням їх квантових властивостей. У роботі розглянуто поняття розрахунку функцій, складності алгоритмів, класичної та квантової машин Тюринга, квантових бітів, квантових логічних елементів, квантових обчислювальних мереж. З'ясовано, на яких ефектах ґрунтується надефективність квантових комп'ютерів порівняно з класичними. Наведено приклади ефективних квантових алгоритмів.

У роботі [9] викладено основні положення та методи квантової механіки, які необхідні для більш глибокої підготовки до опанування та застосування можливостей застосування квантових технологій у Збройних Силах України.

У роботі [10] запропоновано узагальнення булевих операцій для квантових обчислень, а також розглянуто 9 квантових операцій додатково до 7-ми класичних. Отримано повний набір 16 однокубітних операцій, що відповідає кількості базових станів 16-кубітного квантового процесора, що дозволить підвищити продуктивність квантових обчислень у цифрових симуляторах квантових процесорів, з точки зору паралельності обчислень та скорочення програмного коду. Дані дослідження можуть бути використані для підготовки квантофахівців-програмістів на квантових засобах інформаційних технологій або квантових симуляторах.

У роботі [11] висвітлено сучасні проблеми створення стандартів перспективних криптографічних перетворень та хід їх вирішення, які необхідні для аналізу криптографічної стійкості алгоритмів, у тому числі і квантових, що може бути використано для аналізу стійкості постквантових алгоритмів.

Таким чином, проведений аналіз літератури, зокрема робіт [1–11], надає достатнє підґрунтя для підготовки військових квантофахівців до ефективного використання сучасних інноваційних квантових технологій у військовій сфері. Це стосується квантових обчислень, квантового зв'язку та квантових сенсорів, що, у свою чергу, сприятиме підвищенню боєздатності Збройних Сил України.

Метою статті є дослідження сучасного стану квантових технологій у контексті можливості використання квантових технологій і підготовки квантофахівців в інтересах Збройних Сил України для підвищення їх боєздатності.

Основна частина

Аналіз сучасного стану досліджень у сфері квантових обчислень, необхідний для підвищення боєздатності Збройних Сил України

Квантові обчислення є однією з найперспективніших технологій, що здатна радикально змінити підхід до вирішення складних завдань у військовій сфері. Уряди провідних країн світу, включно із США, Китаєм, Великобританією та країнами ЄС, активно фінансують дослідження та розробки в галузі квантових технологій для оборонного сектору. Зокрема, військові програми зосереджені на застосуванні квантових обчислень для оптимізації військових операцій, розробки нових систем шифрування та моделювання складних фізичних процесів.

Одним із ключових напрямів є використання квантових алгоритмів для військової логістики та планування бойових дій [8]. Такі алгоритми, як квантовий відпал (Quantum Annealing), уже тестуються оборонними агентствами США та Великобританії для вирішення задач оптимального розподілу ресурсів [12]. Наприклад, Агентство перспективних дослідницьких проєктів оборони США (DARPA) фінансує проєкти, спрямовані на інтеграцію квантових обчислень у військове управління.

Квантові комп'ютери також мають значний потенціал у сфері криптографії. Використання алгоритму Шора дозволяє розкласти великі числа на прості множники експоненційно швидше, ніж класичні алгоритми, що ставить під загрозу традиційні криптографічні методи, такі як RSA. У відповідь військові відомства активно розробляють квантостійкі алгоритми шифрування, які здатні забезпечити безпечний зв'язок навіть у разі появи потужних квантових обчислювальних систем [4].

Ще один перспективний напрямок досліджень – це квантові сенсори, які можуть забезпечити високоточне визначення положення військової техніки без використання супутникових систем. У 2022 році Міністерство оборони Великобританії заявило про успішні випробування квантових інерціальних навігаційних систем, які дозволяють

кораблям і підводним човнам орієнтуватися без GPS. Такі розробки є критично важливими в умовах радіоелектронної боротьби, коли традиційні навігаційні засоби можуть бути виведені з ладу.

Китай також активно розвиває військові квантові технології. У 2017 році країна запустила супутник *Micius*, який здійснив першу у світі квантову телепортацію та захищену передачу інформації між віддаленими точками. Це демонструє потенціал квантової комунікації для створення нерозшифровуваних каналів зв'язку між військовими об'єктами.

Таким чином, сучасні дослідження в галузі квантових обчислень у військовій сфері перебувають на стадії активного розвитку. Провідні держави спрямовують значні ресурси на інтеграцію цих технологій у свої оборонні стратегії, що створює нові виклики та можливості для України. Подальші дослідження та інвестиції у квантові обчислення можуть стати важливим чинником зміцнення обороноздатності нашої держави. У контексті підвищення боєздатності Збройних Сил України. Ці технології відкривають можливості для оптимізації логістики, розробки нових систем озброєння, аналізу великих даних та забезпечення кібербезпеки. Сучасний стан досліджень у цій сфері демонструє значний прогрес, однак потребує адаптації до специфічних потреб військової сфери, особливо в умовах війни.

Перш за все, потрібно звернути увагу на відмінність теоретичних основ квантових обчислень від сучасних класичних, що суттєво впливає на вирішення проблемних питань.

Квантові комп'ютери базуються на принципах квантової механіки, таких як суперпозиція, запутаність та інтерференція, порівняно з класичними бітами, які мають значення 0 або 1.

Кубіти – квантові біти [1–5] можуть перебувати в суперпозиції станів [2] згідно з виразом (1):

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

де α та β – комплексні амплітуди, що задовольняють умові нормалізації (2):

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2)$$

Суперпозиція. Принцип суперпозиції дозволяє квантовому комп'ютеру одночасно обробляти велику кількість станів, що суттєво прискорює виконання складних обчислювальних задач [2].

Другою ключовою властивістю є квантова **запутаність**, яка забезпечує миттєву кореляцію між кубітами незалежно від відстані [1–5]. Якщо два кубіти знаходяться у запутаному стані, їх хвильова функція має вигляд (3):

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (3)$$

Ця особливість використовується у квантовій криптографії для забезпечення безпечного зв'язку, а також у військових інформаційних системах.

Квантова інтерференція. Ще однією важливою властивістю є квантова інтерференція, яка відіграє ключову роль у роботі квантових алгоритмів. Використання оператора Унітарного перетворення дозволяє маніпулювати станами кубітів за допомогою квантових вентилів. Наприклад, квантове перетворення Фур'є, яке використовується в алгоритмі Шора для факторизації чисел [4], визначається виразом (4):

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i x k / N} |k\rangle. \quad (4)$$

Цей механізм дозволяє вирішувати криптографічні задачі експоненційно швидше за класичні методи, що є важливим у військовій сфері для розробки нових засобів шифрування та дешифрування інформації.

Таким чином, завдяки принципам суперпозиції, запутаності та інтерференції, квантові обчислення відкривають нові можливості для оптимізації військових операцій, забезпечення безпеки комунікацій і швидкої обробки великих масивів даних.

Квантова перевага. Авторами було досліджено, проаналізовано та встановлено, що на глобальному рівні лідерами у сфері квантових обчислень є компанії Google, IBM, D-Wave, Microsoft та Intel. У 2019 році Google оголосила про досягнення «квантової переваги» з їхнім процесором Sycamore, який виконав задачу за 200 секунд, що для класичного суперкомп'ютера потребувало б 10 тис. років. Час виконання задачі для квантового комп'ютера можна оцінити згідно з виразом (5):

$$T_q = O(2^n/p), \quad (5)$$

де n – кількість кубітів;

p – кількість паралельних квантових операцій.

Для класичних суперкомп'ютерів час обчислення такої самої задачі визначається виразом (6):

$$T_c = O(2^n P), \quad (6)$$

де P – кількість класичних процесорів, що працюють паралельно.

У випадку експерименту Google процесор Sycamore мав 53 кубіти та виконав задачу вибірки випадкових чисел у квантовій системі за 200 секунд. Для класичного суперкомп'ютера ця задача має експоненційну складність, що призводить до оцінки часу (7):

$$T_c \approx 10^4 \text{ років}. \quad (7)$$

Цей результат підтверджує значну перевагу квантових обчислень у специфічних класах задач, таких як моделювання квантових систем і оптимізаційні завдання.

Компанія IBM [5], у свою чергу, розвиває підхід до квантових обчислень на основі гібридних систем, де класичні алгоритми доповнюються квантовими прискорювачами. Основною метою є зниження рівня квантового шуму, який моделюється рівнянням (8):

$$\varepsilon = e^{-\lambda t}, \quad (8)$$

де λ – коефіцієнт затухання кубітного стану;

t – час виконання обчислень.

Зменшення цього шуму є ключовою проблемою для масштабування квантових процесорів.

Компанія D-Wave розвиває інший підхід – квантове відпалювання (Quantum Annealing), який використовується для оптимізаційних задач. Його математична модель описується гамільтоніаном (9):

$$H(t) = A(t)H_i + B(t)H_j, \quad (9)$$

де H_i – початковий гамільтоніан;

H_j – фінальний гамільтоніан;

$A(t)$ та $B(t)$ – функції часу, які поступово змінюються так, щоб система еволюціонувала до розв'язку задачі.

Квантовий комп'ютер Microsoft в рамках Azure Quantum працює на основі топологічного кубіту, що використовує майоранові квазічастинки для підвищення стабільності квантових обчислень. Квантові стани в такій системі описуються хвильовою функцією Ψ , що еволюціонує згідно з рівнянням Шредінгера (10):

$$i\hbar \frac{\partial}{\partial t} \Psi(t) = H\Psi(t), \quad (10)$$

де H — гамільтоніан системи.

В основі квантових операцій лежать унітарні перетворення, які забезпечують когерентну еволюцію кубітів (11):

$$U = e^{-iHt\hbar}. \quad (11)$$

Microsoft також використовує гібридну квантово-класичну обчислювальну модель, де квантові алгоритми, такі як квантовий алгоритм Гровера, використовуються для пошуку в неупорядкованих базах даних, де складність відповідає виразу квадратичного прискорення (12):

$$O = (\sqrt{N}), \quad (12)$$

де N – розмірність бази даних.

Також використовується квантовий алгоритм Шора для факторизації чисел, де складність O відповідає виразу (13):

$$O = ((\log N)^3). \quad (13)$$

Розрахунки інтегруються з класичними обчисленнями через платформу Azure Quantum. Це дозволяє ефективно вирішувати задачі оптимізації, криптографії та симуляції фізичних процесів, використовуючи різні апаратні реалізації, включаючи іонні пастки, надпровідникові кубіти та перспективні топологічні процесори, що може бути використано для підвищення обороноздатності держави.

Компанія Intel розробила квантовий комп'ютер, заснований на технології кремнієвих спінових кубітів, які використовують спин електрона у квантовій точці як носій інформації. Динаміка квантового стану таких кубітів описується рівнянням Шредінгера (14):

$$i\hbar \frac{\partial}{\partial t} \Psi(t) = H\Psi, \quad (14)$$

де гамільтоніан системи має вигляд (15):

$$H = g\mu_B B S_z + J S_1 \cdot S_2, \quad (15)$$

де g – фактор Ланде;

μ_B – магнетон Бора;

B – зовнішнє магнітне поле;

J – обмінна взаємодія між спінами кубітів;

S_2 – оператор спіну.

Intel використовує технологію Horse Ridge, яка дозволяє ефективно керувати квантовими станами при температурі $< 1\text{K}$, що спрощує масштабування квантових систем.

Перспективи використання у Збройних Силах включають криптографічні операції (захист інформації за допомогою постквантових алгоритмів), оптимізацію логістичних процесів (швидкий розподіл ресурсів у реальному часі) та аналіз великих даних для розвідки (квантові алгоритми прискорюють розпізнавання об'єктів на супутникових знімках). Використання квантових технологій Intel може значно підвищити ефективність обчислень у військовій сфері, забезпечуючи перевагу в інформаційних і стратегічних операціях.

Таким чином, технологічно розвинені країни світу намагаються втілювати принципи квантової технології для підвищення якісного та ефективного розвитку своїх Збройних сил.

Автори намагалися вивчити досвід розвинутих країн світу та визначитися з можливими основними напрямками, які зможуть підвищити ефективність використання Збройних Сил України для досягнення перемоги у сучасній війні, в першу чергу, з метою збереження особового складу.

Квантові технології можуть значно покращити точність та швидкість прогнозування загроз завдяки застосуванню квантових алгоритмів для аналізу великих масивів даних, розпізнавання закономірностей та моделювання складних систем.

Проведено аналіз можливостей використання досягнень квантових технологій у військовій галузі та визначено напрямки використання квантових технологій для підвищення ефективності використання військових ресурсів (людських та матеріальних), що набуває особливої потреби в сучасних умовах війни проти рф.

Оптимізаційні завдання відіграють ключову роль у військовій сфері, оскільки дозволяють підвищити ефективність логістики, управління військовими ресурсами, розподілу сил та планування бойових операцій. Традиційні методи часто стикаються з обмеженнями обчислювальної потужності при розв'язанні задач великої розмірності, що ускладнює швидкий аналіз бойової обстановки. У цьому контексті квантові алгоритми відкривають нові перспективи, оскільки здатні значно прискорювати розв'язання складних комбінаторних задач.

Квантові технології можуть бути використані для розв'язання складних оптимізаційних завдань, що можуть бути корисними у військовій логістиці, управлінні військовими ресурсами та прогнозуванні загроз.

Проаналізовано основні можливі напрямки оптимізації військових стратегій, які можливо вирішити за допомогою використання квантових технологій.

Одним із найперспективніших напрямів є використання квантового відпалу (Quantum Annealing) для розв'язання задач маршрутизації та розподілу ресурсів. Такі задачі можуть бути сформульовані у вигляді задачі квадратичного двоїстого програмування (Quadratic Unconstrained Binary Optimization, QUBO) (16):

$$H(x) = \sum_i Q_{ii}x_i + \sum_{i,j} Q_{ij}x_ix_j, \quad (16)$$

де x_i – двійкові змінні (0 або 1), що представляють вибір конкретного маршруту чи ресурсу;

Q_{ii} та Q_{ij} – коефіцієнти, що відображають вагу та взаємозв'язки між змінними.

Квантові пристрої, такі як D-Wave, здатні знаходити глобальний мінімум функції, що дозволяє оптимально розподіляти ресурси в реальному часі.

Таким чином, оптимізація логістичних операцій щодо розподілу ресурсів у бойових умовах можна сформулювати у вигляді задачі квадратичного двоїстого програмування (QUBO). При цьому оптимізація військових перевезень може бути розв'язана за допомогою алгоритму квантового відпалу, де транспортна задача формулюється наступним чином (17):

$$\min \sum_{i=1}^m \sum_{j=1}^n c_{ij}x_{ij} \quad (17)$$

за умов:

$$\begin{aligned}\sum_{j=1}^n x_{ij} &= a_i, i = 1, 2, \dots, m, \\ \sum_{i=1}^m x_{ij} &= b_j, j = 1, 2, \dots, n,\end{aligned}$$

де c_{ij} – вартість транспортування військових ресурсів між пунктами ii та jj ;

x_{ij} – кількість ресурсів, що транспортується;

a_i – запаси у відправних пунктах;

b_j – потреби в пунктах призначення.

Квантові алгоритми можуть швидко знаходити рішення подібних задач навіть при великій кількості змінних.

Даний метод може бути застосований для розподілу військових підрозділів, маршрутизації техніки та обчислення оптимального використання пального.

Ще одним перспективним напрямком застосування квантових технологій авторами був запропонований квантовий пошук у військовій розвідці. Для його реалізації запропоновано використовувати алгоритм Гровера для пошуку в невпорядкованих базах даних. Цей алгоритм здатний прискорювати виявлення критично важливих цілей. Часова складність класичного пошуку складає, тоді як алгоритм Гровера виконує пошук за складності $O(\sqrt{N})$. Основний оператор алгоритму описується наступним рівнянням (18) [5]:

$$U = (2|\psi\rangle\langle\psi| - I)O, \quad (18)$$

де $|\psi\rangle$ – початковий стан суперпозиції;

O – оператор пошуку;

I – одиничний оператор.

Таким чином, автори пропонують використовувати алгоритм Гровера для аналізу великих обсягів розвідувальної інформації, значно скорочуючи час на обробку даних [4; 5].

Ще одним із можливих ключових напрямків, на думку авторів, є використання нейромереж і методів машинного навчання для аналізу даних розвідки при використанні квантових алгоритмів. Наприклад, Варіаційний квантовий алгоритм наближення (VQE) та Квантова підтримка векторних машин (QSVM), можуть значно прискорити обробку великих розвідувальних даних.

Класичне оновлення параметрів у нейромережах описується градієнтним спуском (19):

$$\Theta_{t+1} = \Theta_t - \eta \nabla L(\Theta_t), \quad (19)$$

де η – швидкість навчання;

Θ_t – функція втрат;

$\nabla L(\Theta_t)$ – градієнт функції втрат.

Запропоновані квантові алгоритми можуть пришвидшити цей процес завдяки швидкому розрахунку квантових градієнтів та експоненційному масштабуванню обчислювальних можливостей.

Ще одним можливим варіантом використання квантових технологій є моделювання можливих дій противника за допомогою квантових стохастичних алгоритмів [8].

Для прогнозування можливої поведінки противника можна використовувати квантову Марковську модель, яка визначається рівнянням еволюції (20):

$$\rho(t) = e^{-iHt} \rho(0) e^{iHt}, \quad (20)$$

де $\rho(t)$ – щільнісний оператор стану системи;
 H – гамільтоніан, що описує динаміку змін;
 t – час.

Ця модель дозволяє аналізувати ймовірності різних сценаріїв розвитку подій та визначати оптимальні стратегії реагування.

Автори вважають, що застосування квантових алгоритмів [8] у прогнозуванні загроз відкриває нові можливості для військової аналітики, зменшуючи час обчислень та покращуючи точність оцінки ризиків. У подальшому військові аналітики зможуть швидше реагувати на нові загрози, оптимізувати використання ресурсів та розробляти ефективні оборонні стратегії.

Таким чином, застосування квантових алгоритмів у військових оптимізаційних задачах дозволяє значно підвищити ефективність логістичних операцій, аналіз розвідувальних даних та управління ресурсами. Подальші дослідження в цій сфері сприятимуть швидшому впровадженню квантових технологій у Збройні Сили України.

Наступною областю впровадження квантових технологій у військову галузь є використання квантових алгоритмів для криптографії та військового зв'язку [8].

Традиційна криптографія базується на факторизації великих чисел, що є складним завданням для класичних комп'ютерів. Однак алгоритм Шора дозволяє розкласти число N на прості множники за час згідно з виразом (21) [4]:

$$T = O((\log N)^3), \quad (21)$$

що експоненційно швидше за класичні методи. Це загрожує безпеці існуючих криптографічних протоколів.

Телепортація. Для захищеного зв'язку військові досліджують квантову телепортацію, яка базується на передачі квантового стану між двома віддаленими точками за допомогою сплутаних кубітів. Основна формула квантової телепортації виглядає так (22) [1; 2]:

$$|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle. \quad (22)$$

Після передачі квантового стану між точками А і В можна створювати нерозшифровані канали зв'язку.

Перспективи впровадження квантових технологій для створення захищених каналів зв'язку.

Сучасний розвиток інформаційних технологій ставить перед суспільством нові виклики у сфері кібербезпеки, зокрема щодо захисту даних від несанкціонованого доступу. Традиційні методи шифрування, такі як RSA або AES, базуються на обчислювальній складності певних математичних задач (наприклад, факторизації великих чисел). Проте поява квантових комп'ютерів, здатних реалізовувати алгоритм Шора [4], загрожує зламати ці системи за поліноміальний час $O((\log N)^2(\log \log N)(\log \log \log N))$, де N – число, яке потрібно факторизувати. У цьому контексті квантові технології відкривають нові горизонти у сфері інформаційної безпеки, зокрема у створенні захищених каналів зв'язку, що унеможливають несанкціоноване перехоплення інформації. Основою таких систем є принципи квантової механіки, які гарантують безпеку передачі даних завдяки унікальним властивостям квантових станів. Авторами пропонується впровадження квантових технологій, таких як квантова криптографія та квантовий розподіл ключів (Quantum Key Distribution, QKD) для забезпечення конфіденційності зв'язку.

Одним із ключових принципів квантової криптографії є використання квантової суперпозиції та запутаності [1]. Квантовий стан частинки, наприклад, фотона [5], може перебувати у суперпозиції станів $|0\rangle$ та $|1\rangle$, що описується виразами (23) та (24):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (23)$$

$$|\alpha|^2 + |\beta|^2 = 1, \quad (24)$$

де α і β – комплексні амплітуди.

При спробі вимірювання цього стану сторонньою особою (перехоплювачем) квантовий стан колапсує до одного з базисних станів, що порушує початкову інформацію та робить перехоплення помітним для легітимних користувачів.

Найвідомішим протоколом QKD є BB84, запропонований Чарльзом Беннеттом і Жилем Brassarом у 1984 році. У цьому протоколі відправник (А) кодує біти ключа у поляризаційних станах фотонів, наприклад, горизонтальному ($|H\rangle$) або вертикальному ($|V\rangle$), а також у діагональних базисах (25) та (26):

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, \quad (25)$$

$$|A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}. \quad (26)$$

Отримувач (Б) випадково обирає базис для вимірювання. Після передачі отримувач (А) та відправник (Б) порівнюють базиси через відкритий канал і зберігають лише ті біти, де базиси збіглися. Будь-яке втручання, наприклад, вимірювання посередником (В), вносить помилки, які виявляються через перевірку підмножини бітів. Рівень помилок у ключі (Quantum Bit Error Rate, *QBER*) розраховується виразом (27):

$$QBER = \frac{D}{DD}, \quad (27)$$

де D – кількість помилок;

DD – загальна кількість бітів.

Якщо *QBER* перевищує певний поріг (зазвичай 11 % для BB84), це свідчить про присутність перехоплювача.

Перспективи впровадження квантових технологій включають інтеграцію QKD у сучасні оптоволоконні мережі та супутникові системи зв'язку. Наприклад, китайський супутник *Micius* у 2017 році продемонстрував успішну передачу квантового ключа на відстань понад 1200 км. Це стало проривом у глобальній квантовій комунікації, що використовує супутниковий зв'язок для передачі ключів між континентами. Ключова перевага полягає в тому, що будь-яка спроба перехоплення квантового сигналу змінює його стан, що описується принципом клонування квантових станів: жодна квантова система не може бути скопійована без порушення оригіналу (теорема про заборону клонування). Однак існують і виклики: висока вартість обладнання, обмеження дальності передачі через втрати у волокнах (приблизно 0,2 дБ/км для стандартних оптоволоконних ліній), які описуються законом Бугера – Ламберта – Бера, який описує залежність інтенсивності світла від товщини середовища та концентрації поглинаючої речовини при його проходженні через поглинаюче середовище. Його математичний вираз має вигляд (28):

$$I = I_0 e^{-\alpha L}, \quad (28)$$

або у логарифмічній формі (29):

$$A = \log \frac{I_0}{I} = \varepsilon c L, \quad (29)$$

де I_0 – початкова інтенсивність світла;

α – коефіцієнт поглинання середовища;

I – інтенсивність світла після проходження середовища;

L – товщина поглинаючого шару;

A – оптична густина (абсорбція);

ε – молярний коефіцієнт поглинання (залежить від довжини хвилі світла речовини);

c – концентрація поглинаючої речовини.

Практичне застосування закону Бугера – Ламберта – Бера може бути використане у спектроскопії, аналітичній хімії та біофізиці для визначення концентрації речовин у розчинах. У військовій сфері він застосовується для аналізу диму, газів та забруднень в атмосфері, а також у лазерних технологіях, зокрема для оцінки ефективності маскувальних аерозолів та оптичного виявлення хімічних речовин.

Для зменшення втрат активно розробляються квантові повторювачі (quantum repeaters), які використовують запутані фотони для подовження дистанції передачі (телепортацію квантового стану) [1; 2].

У майбутньому вдосконалення квантових повторювачів, які використовують квантову телепортацію для подолання втрат сигналу, може розширити масштабність таких систем. Процес телепортації квантового стану описується оператором запутаності, наприклад, для стану Белла [1; 7; 9] виглядає, як у виразі (30):

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad (30)$$

де стан однієї частинки передається іншій через спільний запутаний стан і класичний канал зв'язку.

Ще одним видом використання квантових технологій може бути квантовий зв'язок, в основу якого покладена квантова сплутаність (заплутаність) [1–8] – це квантовомеханічне явище, коли існує взаємозв'язок та залежність між квантовими частками, навіть рознесеними у просторі. Головним при цьому є використання так званих сплутаних квантових станів [5–8]. На рисунку 1 зображено процес утворення зв'язаних частинок фотона шляхом їх пропускання скрізь кристал бета-барата-барія світового потоку або одного фотону.

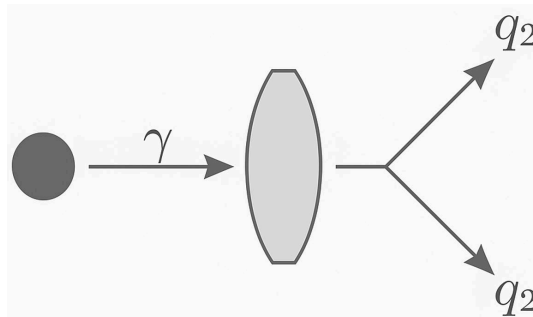


Рис. 1. Графічне представлення процесу утворення заплутаних кубітів (фотонів) шляхом їх розкладання в лінії

На рисунку 2 пояснюється процес вимірювання стану частки. Зв'язані або заплутані квантові частки захоплюються в пастку, яка вимірює їх стан, але далі ці частки вже не поширюються.

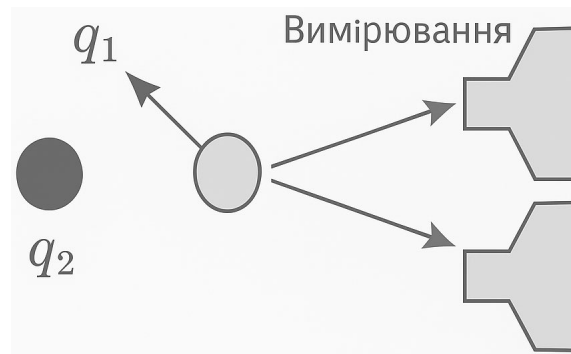


Рис. 2. Графічне представлення вимірювання (та руйнування) стану заплутаних кубітів спеціальними пастками

Рисунок 3 пояснює, як крізь канал, побудований на основі заплутаних частинок *A*, *B*, передається інформаційна частка *C*.

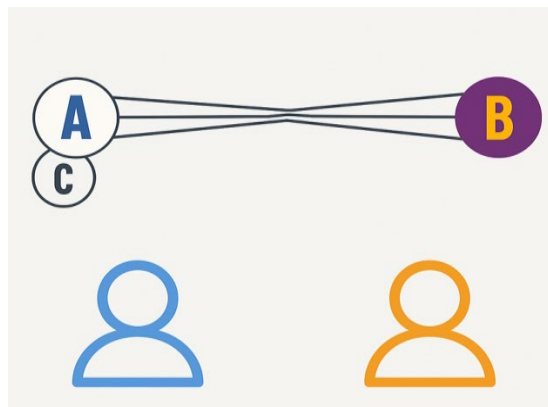


Рис. 3. Принцип передачі даних каналом, утвореним між пов'язаними частками *A*, *B*

Квантовий генератор випадкових чисел (КГВЧ). Однією із важливих складових криптографічних систем є генератори псевдовипадкових чисел, необхідні для створення ключів шифрування. КГВЧ використовує квантові явища, такі як суперпозиція і заплутаність, для створення чисел, які є абсолютно випадковими і не підлягають детермінізму, забезпечуючи високий рівень ентропії і непередбачуваності, що є критично важливим для криптографії та інших безпекових застосувань, особливо у військовій сфері. На рисунку 4 визначено принцип утворення потоку випадкових чисел за рахунок утворення та контролю збуджених станів квантових часток. Очікувано, що Збройні сили використовують КГВЧ для здійснення більш надійного захисту інформації.

Перспективним для військового використання є *квантовий датчик Рідберга (КДР)*, який здатен перевершити можливості сучасних засобів електроніки за чутливістю, смугою пропускання і частотним діапазоном. Це в перспективі надасть можливість розробити нові ефективні засоби радіоелектронної боротьби. Рисунок 5 пояснює принцип роботи квантових часток у різноманітних сенсорах або засобах, реалізуючи квантові датчики.

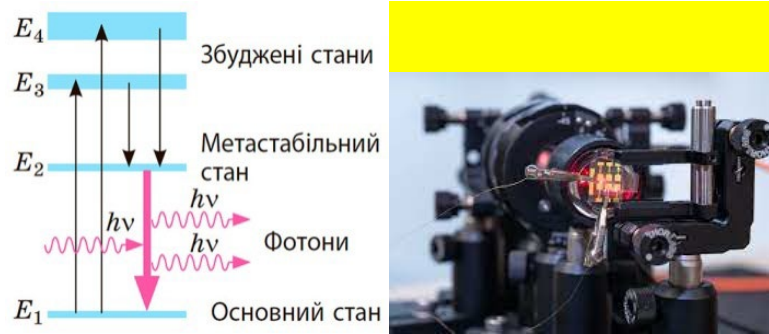


Рис. 4. Принцип роботи квантового генератора випадкових чисел

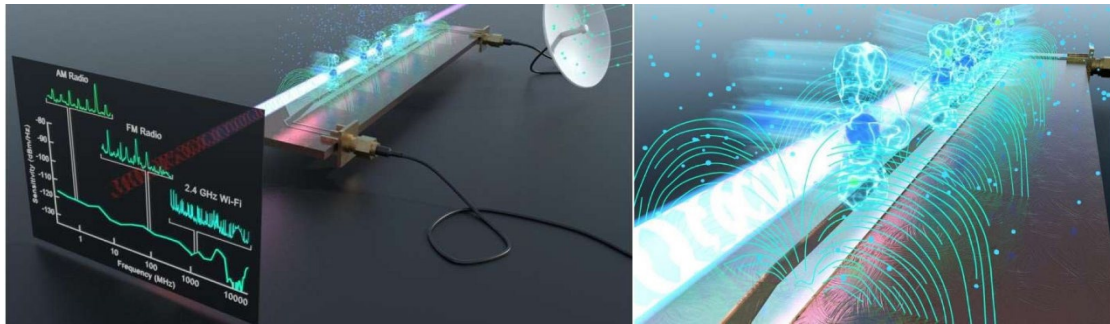


Рис. 5. Надчутливі квантові датчики

КДР здатен вловлювати й аналізувати весь спектр радіочастотних сигналів та допоможе виявити ворожі електронні засоби. КДР здатен фіксувати від нульової частоти до 19 ГГц, АМ- та FM-хвилі, Bluetooth, Wi-Fi та інші сигнали зв'язку. Наразі застосовують лазерні промені для створення атомів Рідберга, зовнішні електрони яких знаходяться у високозбудженому стані. Це робить датчик надчутливим до широкого діапазону сигналів у радіочастотному спектрі.

КДР значно перевищує сучасну електроніку за чутливістю, смугою пропускання і частотним діапазоном. Таким чином, можливо розробити військові засоби радіоелектронної боротьби та виявлення засобів зв'язку в разі ефективнішими, що є частиною стратегії модернізації армії.

Кульмінацією розвитку військового квантового зв'язку стане створення військового квантового Інтернету, коли передача буде здійснюватися у вигляді кубітів між розподіленими квантовими процесорами. Надалі військові побудують квантовий зв'язок між командними пунктами та вузлами управління, використовуючи субатомні частинки, такі як фотони [5], для передачі інформації на принципах квантової механіки. Квантова криптографія забезпечить таємність даних, тому що ці частинки неможливо знищити, скопіювати або відслідкувати. Квантовий розподіл ключів передбачає передачу ключової інформації заплутаними фотонами, що унеможливає перехоплення даних, тому що при їх вимірюванні вони руйнуються. Рисунок 6 відображає схему утворення глобального квантового Інтернету на основі супутникової мережі.

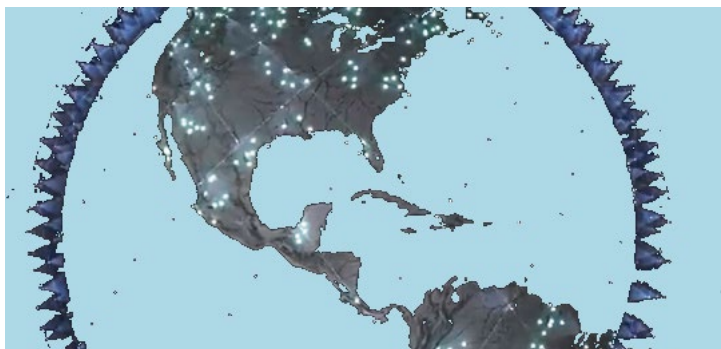


Рис. 6. Принцип формування та роботи глобального квантового Інтернету

Квантова телепортація [2–7] дозволить передавання квантового стану від однієї частинки до іншої на відстані без фізичного переміщення самої частинки. У квантовій телепортації не передається сама інформація чи матеріал, а лише квантовий стан, що робить її важливою для майбутніх технологій, зокрема для квантової комунікації та обчислень[1; 10; 11]. Рисунок 7 дає уяву про принципи роботи квантової телепортації на основі супутникових каналів зв'язку, утвореними між заплутаними частками.

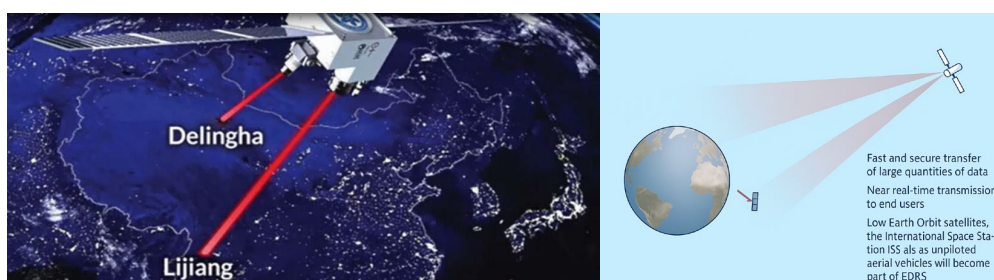


Рис. 7. Принципи роботи квантової телепортації на базі утворених супутникових каналів між заплутаними частками

Квантова телепортація є фундаментальною технологією для створення захищених каналів зв'язку у військовій галузі. Вона дозволить передавати квантовий стан між віддаленими військовими об'єктами без фізичного переміщення носія інформації. Основна ідея базується на квантовій заплутаності, що дозволяє миттєво передавати інформацію. У майбутньому квантові технології можуть стати основою військових мереж зв'язку, стійких до атак квантових комп'ютерів, які здатні зламувати традиційні криптосистеми (RSA, ECC) за допомогою алгоритму Шора [4–7]. Таким чином, впровадження квантових каналів зв'язку обіцяє революцію в кібербезпеці, забезпечуючи абсолютну конфіденційність передачі даних.

Перспективним напрямком автори статті вважають використання квантових сенсорів та військової навігації.

Наприклад, традиційні GPS-системи можуть бути заблоковані радіоелектронною боротьбою. Альтернативою є квантові інерціальні сенсори, що базуються на принципі атомної інтерферометрії. Основне рівняння руху квантових частинок у такій системі має вигляд (31):

$$S = \int L dt, \quad (31)$$

де S – дія;

L – лагранжіан;

dt – елемент часу.

У квантовій механіці лагранжіан можна представити у вигляді (32):

$$L = \frac{1}{2}mv^2 - \mathcal{V}, \quad (32)$$

де m – маса атома;

v – швидкість атома;

$\mathcal{V}$ – потенціальна енергія в системі.

Завдяки вимірюванню фазового зсуву між хвильовими функціями атомів можна з високою точністю визначати параметри руху, включаючи прискорення та кутову швидкість.

Квантові інерціальні сенсори забезпечують надвисоку точність визначення координат, що дозволяє військовим об'єктам, таким як підводні човни, безпілотники та ракетні комплекси, автономно орієнтуватися без використання GPS. Точність таких систем може сягати нанометрів на секунду, що значно перевершує традиційні інерціальні навігаційні системи.

Крім того, квантові сенсори можуть працювати в умовах, де традиційні системи втрачають ефективність, наприклад, під водою, у глибоких підземних тунелях або в середовищі із сильними радіоперешкодами.

Таким чином, застосування квантових сенсорів у військовій навігації відкриває нові можливості для Збройних сил, що забезпечує незалежність від супутникових систем (наприклад, нещодавній випадок відключення функціонування супутникової системи Starlink під час проведення бойових дій Збройними Силами України в окупованому Криму та в Курській операції) та підвищує точність автономного руху військової техніки. Це робить квантові технології критично важливим напрямом розвитку оборонних систем майбутнього.

Висновки

Таким чином, використання квантових технологій демонструє значний прогрес і потенціал для застосування у військових галузях, таких як зв'язок, криптографія та оптимізація військових операцій. Інтеграція квантових технологій у військову сферу може докорінно змінити принципи ведення бойових дій, забезпечуючи технологічну перевагу над супротивником.

У майбутньому для повноцінного використання квантових технологій у секторі оборони України необхідно продовжувати дослідження, створювати необхідну матеріально-технічну базу та подальше впровадження підготовки професійних і досвідчених квантофахівців, що передбачає розробку сучасних освітніх програм у галузі квантової фізики, обчислень та безпеки, використання в освітньому процесі інноваційних методів та забезпечення новітніми технічними засобами.

З огляду на стрімкий розвиток квантових технологій, держави, які першими зможуть ефективно їх інтегрувати у військову інфраструктуру, отримають стратегічну перевагу у майбутніх конфліктах та значно змінять власну обороноздатність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карлаш Г. Ю. Квантові інформаційні системи: навч. посіб. для спеціальності «Прикладна фізика та наноматеріали». Київ, 2018. С. 12, 18, 33.
2. Вакарчук І. О. Квантова механіка: підруч. / І. О. Вакарчук. 4-те вид., доп. Львів: ЛНУ ім. Івана Франка, 2012. С. 747–749.
3. Павлишенко Б. Квантовий алгоритм розпізнавання образів на растрових зображеннях // Львівський національний університет ім. Івана Франка. Львів. Серія Фіз. 2010. Вип. 45. С. 24–30.

4. Крохмальський Т. Є. Вступ до квантових обчислень: навч. посіб. Львів: ЛНУ ім. Івана Франка, 2018. С. 107–120.
5. Філоненко Є. О., Корольок Д. В. Фотонні системи з однокубітними квантовими обчисленнями. Київ: Кафедра мікроелектроніки НТУ України «КПІ ім. Ігоря Сікорського», Факультет електроніки. Київ, 2021. С. 44–45, 50–51, 107–120.
6. Старовойт Тетяна, Зайченко Юрій. Гібридна квантово-вдосконалена модель штучного інтелекту в задачі автоматичного розпізнавання та швидкого перетворення неструктурованої текстової інформації на просторову // *Advanced Information Technology*. 2023. № 1 (2).
7. Боровий М. О., Оліх О. Я. Фізичні основи квантової механіки. Частина 1. К.: КНУ ім. Тараса Шевченка, 2011. С. 19–22, 56–65.
8. Крохмальський Т. Квантові комп'ютери: основи й алгоритми (короткий огляд) / Т. Крохмальський // *Журн. фіз. досліджень*. 2004. Т. 8, № 4. С. 1–15.
9. Кобушкін О. П. Квантова механіка: навч. посіб. Київ, 2016. С. 1–15.
10. Будник Микола. Булеві квантові логічні операції // *Фізико-математичне моделювання та інформаційні технології*. 2023. Вип. 36. С. 38–42. URL: doi.org/10.15407/fmmit2023.36.038.
11. Горбенко І. Д., Качко О. Г., Кузнецов О. О., Потій О. В., Горбенко Ю. І., Пономар В. А., Єсіна М. В. Проблеми створення стандартів перспективних криптографічних перетворень та хід їх вирішення // *Доповідь на конференції ВІТІ, 2018* URL: <https://iit.com.ua/>.
12. Корольов В. Ю., Ходзінський О. М. Дослідження впливу параметрів квантового відпалу на якість розв'язку задачі факторизації чисел // *Cybernetics and Computer Technologies*. 2023. Вип. 1. С. 13–22. URL: <https://doi.org/10.34229/2707-451X.23.1.2>.