Received 04.02.2026 | Accepted 20.02.2026 | Published 30.03.2026

УДК 004 DOI: 10.63978/3083-6476.2026.1.4.05

Лисецький Юрій Михайлович
доктор технічних наук, доцент
Воєнна академія імені Євгенія Березняка
Київ, Україна
e-mail: Yurii.Lysetskyi@snt.ua
ORCID: 0000-0002-5080-1856

КВАНТОВІ ТЕХНОЛОГІЇ В ОБОРОНІ І БЕЗПЕЦІ

Анотація. *Досліджено квантові технології та перспективи їх використання в обороні і безпеці. Розглянуто квантові обчислення, квантовий зв'язок, квантові сенсори. Наведено основні напрямки застосування квантових обчислень у кібербезпеці: детекція та аналіз кіберзагроз, квантове шифрування, квантова криптографія, постквантова криптографія.*

Ключові слова*: квантові технології, квантові обчислення, квантові сенсори, квантовий зв'язок, квантове шифрування, квантова криптографія, кібербезпека.*

QUANTUM TECHNOLOGIES IN DEFENSE AND SECURITY

Lysetsyi Yurii
Doctor of Engineering Sciences,
associate professor
Yevhenii Bereznyak Military Academy
Kyiv, Ukraine
e-mail: Yurii.Lysetskyi@snt.ua
ORCID: 0000-0002-5080-1856

Abstract*. The article focuses on quantum technologies and the prospects for their application in the defense and security sectors. Based on an analysis of the current state of development of quantum technologies and their applications in defense and security, three main areas are identified: quantum computing, quantum communication, and quantum sensors. For each of these, a specific set of applications, advantages, and limitations is identified. It is noted that quantum computing in defense and security finds application primarily in four subfields: post-quantum cryptography, quantum cryptography, cyber threat detection, and cryptanalysis; quantum communication ensures secure information transmission by utilizing the physical properties of quantum states, particularly the principle of the impossibility of cloning a quantum state, with its primary practical application being Quantum key distribution and its promising application being the quantum internet; quantum sensors are the category of quantum technologies closest to operational deployment, as they utilize the hypersensitivity of quantum states to external disturbances to achieve measurement accuracy unattainable by classical devices. A summary of the main areas of application for quantum technologies in defense and security indicates that quantum sensors have the nearest practical implementation horizon (5–7 years), while quantum computing will have the greatest strategic impact on cryptographic infrastructure due to the threat it poses to existing asymmetric encryption algorithms—which is precisely why the transition to post-quantum standards is becoming urgent. Therefore, given the significant interest in and funding for quantum technologies from both the civilian industry and governments, it is expected that these technologies will continue to develop and new quantum applications will become available over the next five to ten years, and new advances in the development of quantum technologies may bring new opportunities for the military, but for the military to actually reap the benefits of new quantum technologies, they need to actively engage in this field and guide the development and implementation of military applications of quantum technologies.*

Keywords: *quantum technologies, quantum computing, quantum sensors, quantum communication, quantum encryption, quantum cryptography, cybersecurity.*

JEL Classification: O32, H56, L86, O33

Вступ

Квантові технології несуть з собою нові можливості як в цивільному, так і військовому застосуванні, і вони останнім часом залучили до себе великий інтерес з боку промисловості і урядів. Великі технологічні компанії витрачають сотні мільйонів доларів на науково-дослідні роботи в галузі квантових обчислень [1]. Так само, уряди визнали трансформаційний потенціал і геополітичну цінність застосувань квантової технології, і США, Європейський союз і Китай започаткували власні дослідницькі програми вартістю у мільярди доларів. Зважаючи на потенційні наслідки новітніх квантових технологій для оборони і безпеки, НАТО визначає квантові технології як один із провідних нових технологічних напрямків за впливом на оборону і безпеку.

Огляд літератури

Аналіз наукових публікацій засвідчує зростаючий інтерес дослідницької спільноти до проблематики застосування квантових технологій у сферах оборони та безпеки. Ключові напрямки досліджень охоплюють три взаємопов'язані домени: квантові обчислення та їх вплив на криптографічну інфраструктуру; квантовий зв'язок і розподіл ключів; квантові сенсори для задач розвідки та навігації.

Загальний огляд перспектив використання квантових технологій наданий у роботі Данилюка І. А. та інших [2], де систематизовано ключові напрямки квантових досліджень і сформульовано прогноз щодо їх впливу на інформаційні та комунікаційні системи. Практичні аспекти застосування квантових технологій для потреб кіберзахисту розглядаються у публікації Лисецького Ю. М., Боханченка О. С., Сурми А. І. [3], де описано конкретні сценарії протидії кіберзагрозам на основі квантових методів.

Стандартизація постквантової криптографії стала визначальною подією 2024 року. Після шестирічного міжнародного конкурсу Національний інститут стандартів і технологій США (National Institute of Standards and Technology, NIST) у серпні 2024 року опублікував три фінальні стандарти постквантових алгоритмів: FIPS 203 (ML-KEM, на основі CRYSTALS-Kyber), FIPS 204 (ML-DSA, на основі CRYSTALS-Dilithium) та FIPS 205 (SLH-DSA, на основі SPHINCS+) [4]. Ці алгоритми спираються на математичні задачі, що вважаються стійкими до квантових атак, зокрема задачі на ґратках та задачі геш-функцій, і призначені для заміни вразливих RSA (Rivest, Shamir та Adleman), DSA (Digital Signature Algorithm) та ECC (Elliptic Curve Cryptography). NIST розробляє також FIPS 206 на основі алгоритму FALCON як додатковий стандарт цифрових підписів.

Комплексний аналіз впливу квантових обчислень на кібербезпеку здійснено у публікації Саху С. та Мазумдара К. "State-of-the-art analysis of quantum cryptography: applications and future prospects" (*Frontiers in Physics*, 2024), де систематизовано загрози від алгоритмів Шора та Гровера [5] щодо асиметричних і симетричних шифрів, а також проаналізовано методи протидії – постквантову криптографію та квантовий розподіл ключів. Огляд Алі С. та інших авторів деталізує технічні та організаційні виклики впровадження PQC (Post-Quantum Cryptography) і QKD (Quantum Key Distribution) у реальних системах безпеки [6].

Проблема "Harvest Now, Decrypt Later" (HNDL) – стратегія зберігання зашифрованих даних з метою їх подальшого розкодування квантовим комп'ютером – набуває практичного значення вже сьогодні. Аналітичний центр Soufan Center у доповіді 2024 року "Quantum Computing and the Evolving Cyber Threat Landscape" фіксує свідчення

того, що державні актори вже реалізують цю стратегію [7], що надає переходу на постквантові алгоритми невідкладного, а не лише перспективного характеру. Рахункова палата США (Government Accountability Office, GAO) у доповіді "Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy" (листопад 2024) констатує, що федеральні агентства досі не сформували повноцінної стратегії протидії цим загрозам [8].

Квантовий розподіл ключів є найбільш зрілою з квантових комунікаційних технологій. Огляд "Quantum Key Distribution Networks – Key Management: A Survey" (2024 р.) систематизує топологію QKD-мереж, схеми управління ключами та інтеграцію з класичними мережами [9]. Практичні розгортання 2022–2023 років – мережа QKD JPMorgan Chase у США та приєднання HSBC до квантово-захищеної мережі в Лондоні – демонструють прийнятність технології для захисту критичної інфраструктури [10]. Водночас критичний аналіз (International Association for Cryptologic Research, IACR) у 2025 році вказує на суттєві обмеження QKD: залежність від прямого оптичного з'єднання, обмежена дальність без квантових ретрансляторів, висока вартість – через що NSA (National Security Agency) США і ряд інших регуляторів рекомендують PQC як більш практичний підхід [11].

Квантові сенсори для задач навігації та розвідки являють собою найближчий для впровадження клас квантових технологій для військового застосування. Публікація "How Quantum Sensing Will Help Solve GPS Denial in Warfare" (Lawrence Livermore National Laboratory) у 2024 році підкреслює, що квантові інерціальні сенсори на основі атомної інтерферометрії забезпечують більш ніж десятикратну перевагу за стабільністю порівняно з класичними інерціальними системами [12].

DARPA (Defense Advanced Research Projects Agency) реалізує програму Robust Quantum Sensors (RoQS), в рамках якої компанія Q-CTRL отримала контракти на 24,4 млн дол. США; у льотних випробуваннях система Ironstone Opal продемонструвала точність навігації в 111 разів вищу за класичний аналог за відсутності сигналу GPS (Global Positioning System) [12]. Defense Innovation Unit паралельно розвиває програму Transition of Quantum Sensing (TQS) для прискорення впровадження цих технологій у реальні військові платформи [13].

Аналіз квантового машинного навчання (Qt Modeling Language, QML) для задач виявлення кіберзагроз систематизовано у публікації "Quantum key distribution through quantum machine learning: a research review" (*Frontiers in Quantum Science and Technology*, 2025), де показано потенціал QML для покращення виявлення аномалій і підвищення надійності криптографічних систем [11]. Доповідь Congressional Research Service "Defense Primer: Quantum Technology" (2024 р.) підсумовує військовий потенціал усіх трьох класів квантових технологій – обчислень, зв'язку та сенсорів – і наголошує на необхідності активного залучення збройних сил до формування вимог та участі у випробуваннях [14].

Таким чином, аналіз наукової літератури підтверджує, що квантові технології перейшли від теоретичного до прикладного етапу розвитку. Ключовими дослідницькими лакунами залишаються: стратегії міграції наявних систем безпеки на постквантові стандарти в умовах обмежених ресурсів; практичні рішення для розгортання QKD на тактичному рівні (включаючи мобільні та безпровідні сценарії); та інтеграція квантових сенсорів у спільні системи управління, навігації та розвідки збройних сил.

Мета та завдання статті

Дослідження можливостей використання квантових технологій у секторі оборони і безпеки.

Методи

У процесі дослідження використовувалися загальнонаукові і спеціальні методи, а саме: системного аналізу, системно-функціональний; теоретичного узагальнення, факторних порівнянь та експертних оцінок.

Результати

На основі аналізу сучасного стану розвитку квантових технологій та їх застосувань у сфері оборони і безпеки можна виокремити три основних напрямки: *квантові обчислення, квантовий зв'язок та квантові сенсори*. Для кожного з них характерний специфічний набір застосувань, переваг і обмежень.

Напрямок 1. Квантові обчислення

Квантові обчислення здатні кардинально змінити баланс сил у кіберпросторі. В обороні і безпеці вони знаходять застосування передусім у чотирьох підгалузях: постквантовій криптографії, квантовій криптографії, детекції кіберзагроз та криптоаналізі.

Постквантова криптографія (PQC). Розробка та впровадження криптографічних алгоритмів, стійких до атак з боку квантових комп'ютерів. Після завершення стандартизаційного конкурсу NIST у 2024 році галузь отримала три перших стандарти: ML-KEM (FIPS 203), ML-DSA (FIPS 204) та SLH-DSA (FIPS 205).

Переваги: реалізується на класичному обладнанні без необхідності у квантовій апаратурі; алгоритми сумісні з наявними мережевими протоколами TLS (Transport Layer Security), SSH (Secure Shell); дозволяє захистити інформацію від стратегії "збережи зараз – розшифруй пізніше"; міграція може здійснюватись поетапно.

Недоліки: значно більший розмір ключів і підписів порівняно з RSA/ECC (наприклад, публічний ключ ML-KEM-1024 – 1568 байт проти 256 байт у ECC-256); підвищене обчислювальне навантаження на обмежені пристрої; математична стійкість нових алгоритмів не є повністю доведеною – зберігається теоретичний ризик появи нових класичних або квантових атак; перехід вимагає масштабного оновлення IT-інфраструктури, що є витратним і тривалим.

Квантова криптографія (QKD-забезпечення). Застосування принципів квантової механіки для гарантування таємності криптографічних ключів. Протоколи BB84 [15] та E91 [16] забезпечують фізично обґрунтовану неможливість непоміченого перехоплення.

Переваги: "інформаційно-теоретична" безпека (Information-Theoretical Security, ITS) – захист не залежить від обчислювальних можливостей противника; будь-яка спроба перехоплення автоматично виявляється; не потребує постійного оновлення алгоритмів.

Недоліки: потребує спеціалізованого апаратного забезпечення (одиночні фотони, кріогенні детектори); дальність без ретрансляторів обмежена ~100–300 км по оптоволокну; не захищає від атак на кінцеві вузли, а лише на канал передачі ключів; висока вартість розгортання; несумісність з радіоканалами, що критично для тактичного рівня.

Детекція та аналіз кіберзагроз на основі QML (Qt Modeling Language). Використання квантового машинного навчання для прискорення виявлення аномалій у мережевому трафіку та класифікації зловмисного програмного забезпечення.

Переваги: теоретична квадратична або експоненційна перевага в обробці великих масивів даних; потенціал для виявлення складних прихованих кореляцій; можливість прискорення задач оптимізації в системах SOC (Security Operations Center).

Недоліки: сучасні NISQ-процесори (Noisy Intermediate-Scale Quantum) ще не забезпечують стабільного переважання над класичним ML на реальних задачах безпеки; обмежена кількість кубітів не дозволяє обробляти масштаб реальних датасетів; алгоритми QML чутливі до шуму квантових обчислень; практичне впровадження у бойові системи кібербезпеки не очікується раніше кінця десятиліття.

Напрямок 2. Квантовий зв'язок

Квантовий зв'язок забезпечує захищену передачу інформації, використовуючи фізичні властивості квантових станів, зокрема принцип неможливості клонування квантового стану. Основним практичним застосуванням є QKD; перспективним – квантовий інтернет.

Квантові мережі зв'язку (QKD-мережі). Розгортання мереж для обміну криптографічними ключами між стратегічними об'єктами. Китай у 2016 році запустив перший квантовий комунікаційний супутник "Міціус" і продемонстрував міжконтинентальний QKD [2]; НАТО та США активно фінансують наземні мережі QKD.

Переваги: фізично гарантована таємність каналу розподілу ключів; захищеність від будь-яких майбутніх обчислювальних атак; виявлення підслуховування в реальному часі; супутниковий QKD усуває обмеження відстані наземних мереж.

Недоліки: наземні мережі вимагають прокладки спеціалізованої оптоволоконної інфраструктури або розгортання довірених ретрансляторів, кожен з яких є потенційною точкою компрометації; супутникові рішення залежать від погодних умов і часових вікон видимості; технологія не розрахована на мобільні або тактичні застосування; глобальна мережа QKD потребує вирішення проблеми квантових ретрансляторів, яка наразі не має масштабованого рішення.

Квантовий інтернет. Перспективна архітектура глобальної мережі взаємопов'язаних квантових комп'ютерів з ультразахищеними комунікаційними каналами.

Переваги: потенційно абсолютно захищений зв'язок між командними пунктами і платформами; можливість розподілених квантових обчислень для вирішення тактичних задач оптимізації.

Недоліки: знаходиться на ранніх стадіях досліджень; відсутність масштабованих квантових ретрансляторів є критичним бар'єром; горизонт практичного розгортання – щонайменше 10–15 років; надзвичайно висока вартість розробки і підтримки.

Напрямок 3. Квантові сенсори

Квантові сенсори є найбільш близькою до бойового впровадження категорією квантових технологій. Вони використовують надчутливість квантових станів до зовнішніх збурень для вимірювання з точністю, недосяжною для класичних приладів [17].

Квантова навігація (PNT – Positioning, Navigation, and Timing без GPS). Системи позиціонування, навігації та синхронізації часу, що не потребують зовнішніх сигналів (GPS/GNSS – Global Navigation Satellite System) і стійкі до радіоелектронної боротьби. Базуються на квантових акселерометрах (атомна інтерферометрія), квантових гіроскопах, квантових магнетометрах і квантових гравіметрах.

Переваги: повна незалежність від зовнішніх сигналів; стійкість до придушення та спуфінгу GPS, що є критичним у сучасних зонах бойових дій; досягнута точність Ironstone Opal (Q-CTRL) у 50 разів вища за традиційні GPS-системи і перевершила інші несупутникові системи (ІНС) у тестових польотах в 11 разів [18]; застосовність для підводних човнів, де GPS недоступний; пасивна робота – без випромінювання сигналів, що забезпечує прихованість.

Недоліки: поточні системи ще мають значні габарити та масу, що ускладнює розміщення на малих платформах; висока чутливість до вібрацій і механічних збурень (проблема "розгортання на рухомих платформах"); потребує попереднього завантаження детальних магнітних або гравітаційних карт місцевості; висока вартість і складність в обслуговуванні; необхідність регулярного калібрування.

Квантові радари та системи виявлення. Використання заплутаних фотонів для виявлення малопомітних об'єктів (літаків-невидимок, підводних човнів) і виявлення підземних споруд.

Переваги: теоретична здатність виявляти об'єкти зі зниженою ЕПР (ефективна площа розсіювання), недосяжні для класичних систем РЛС; можливість виявлення підводних об'єктів через гравітаційні та магнітні аномалії; розширені можливості ISR (Intelligence, Surveillance, Reconnaissance) для виявлення прихованих сил противника.

Недоліки: квантові радари дальньої дії поки що залишаються переважно теоретичною концепцією; практичні дальності виявлення суттєво обмежені втратами заплутаних фотонів у реальному середовищі; складність формування і підтримки заплутаних пар фотонів у польових умовах; чутливість до атмосферних завад.

Квантові атомні годинники та синхронізація. Еталони часу з точністю 10^{-18} для задач синхронізації розподілених мереж, точного наведення та розвідки.

Переваги: дрейф менше 0,3 наносекунди за 20 днів (зафіксовано у морських випробуваннях Vector Atomic у 2022 р.); можливість заміни рубідієвих еталонів часу на борту GPS-супутників; критична роль у забезпеченні точності систем наведення та зв'язку.

Недоліки: обмеження за розміром і енергоспоживанням для мобільного застосування; необхідність вакуумних камер та лазерних систем охолодження; чутливість до магнітних полів і вібрацій.

Узагальнення основних напрямків застосування квантових технологій в обороні і безпеці свідчить, що найближчий горизонт практичного впровадження мають квантові сенсори (5–7 років), а найбільший стратегічний вплив на криптографічну інфраструктуру матимуть квантові обчислення через загрозу існуючим алгоритмам асиметричного шифрування – саме тому перехід на постквантові стандарти набуває невідкладного характеру вже сьогодні.

Дискусія

Незважаючи на значний теоретичний і практичний потенціал квантових технологій для оборони і безпеки, їх реальне використання стикається з цілою низкою серйозних проблем, з якими фахівці у кожному з напрямків неминуче зіткнуться вже найближчими роками.

Проблеми використання квантових обчислень

Найближча і найбільш практично значуща проблема – це невизначеність щодо темпів розвитку криптографічно значимих квантових комп'ютерів (Cryptographically Relevant Quantum Computer, CRQC). Фахівцям з кібербезпеки доводиться проектувати захищені системи без точного розуміння того, коли CRQC стане реальністю. Оцінки варіюються від 5 до 20+ років, що ускладнює планування міграції. При цьому стратегія HNDL (Have Now, Decode Later) вже активна: зловмисники збирають зашифровані дані сьогодні з розрахунку на майбутнє. Це означає, що фахівці, відповідальні за захист інформації з тривалим строком конфіденційності (державна таємниця, медичні дані, фінансові записи), вже перебувають під загрозою, навіть якщо CRQC з'явиться лише через десятиліття.

Перехід на постквантові алгоритми, хоча і технічно здійсненний, є надзвичайно ресурсоємним. Фахівці стикаються з проблемою криптографічної гнучкості: системи потрібно проектувати так, щоб алгоритми можна було замінювати без повного переписування коду –адже один із чотирьох обраних NIST алгоритмів SIDH/SIKE (Supersingular Isogeny Diffie-Hellman/ Supersingular Isogeny Key Encapsulation), вже був зламаний у 2022 році ще до остаточної стандартизації. Це відкриває питання: наскільки надійні нові стандарти і що станеться, якщо один із них виявиться вразливим після масштабного впровадження? Також постає практична проблема збільшення розмірів ключів і підписів, що знижує продуктивність вбудованих систем, IoT-пристроїв і систем з обмеженою пропускною здатністю – типових для тактичного військового рівня.

Окремою проблемою є використання квантових обчислень для криптоаналізу і атак. Фахівці з кібербезпеки і контррозвідки повинні враховувати, що противники, які першими отримають CRQC, зможуть ретроактивно розкрити будь-які перехоплені зашифровані комунікації – включаючи дипломатичні переговори, розвідувальні дані та оперативні накази, що передавались протягом останніх десятиліть.

Проблеми використання квантового зв'язку (QKD)

Одна з центральних невирішених проблем – масштабованість QKD-мереж до тактичного і мобільного рівня. Наявні розгортання (JPMorgan Chase, HSBC, китайська QKD-мережа) є стаціонарними і прив'язаними до оптоволоконної інфраструктури. Для польових умов – зв'язок між рухомими штабами, тактичними підрозділами, БПЛА, морськими платформами – це рішення непридатне у поточному вигляді. Квантові ретранслятори, необхідні для подолання обмежень дальності, залишаються предметом фундаментальних досліджень і не мають готових інженерних рішень.

Проблема довірених вузлів у QKD-мережах є нетривіальною з точки зору безпеки: у мережах з ретрансляторами кожен вузол є "довіреним" і може бути скомпрометований фізично або адміністративно. Це означає, що QKD не вирішує проблему безпеки кінцевих вузлів і не усуває необхідності у традиційних засобах фізичного захисту і контролю доступу. Фахівці, що проектують захищені командні мережі, повинні усвідомлювати, що гарантії QKD стосуються виключно каналу – але не системи в цілому.

Ще одна проблема – відсутність єдиних стандартів і сертифікаційних вимог для QKD-обладнання. На відміну від PQC, де NIST провів відкритий міжнародний процес стандартизації, QKD-пристрої різних виробників (ID Quantique, Toshiba, китайські) мають різні характеристики безпеки і несумісні протоколи. Для розгортання у системах національної безпеки це становить серйозну перешкоду.

Проблеми використання квантових сенсорів

Попри найбільшу з трьох напрямків готовність до практичного застосування, квантові сенсори стикаються з критичною проблемою розгортання на рухомих платформах. Вони потребують вакуумних камер, точних лазерних систем і захисту від вібрацій – все це суперечить вимогам до габаритно-масових характеристик авіаційних, наземних і водних платформ. Програма DARPA RoQS (Robust Quantum Sensors) спеціально спрямована на подолання цього розриву, але до серійного виробництва ще далеко.

Проблема інтеграції квантових сенсорів у існуючі системи управління і бойових платформ є не менш серйозною, ніж фізична мініатюризація. Квантові навігаційні системи генерують дані у форматі, відмінному від класичних ІНС, і потребують нових алгоритмів злиття даних (sensor fusion). Взаємодія з наявними системами бойового управління (C2), цілевказання і навігації вимагатиме значних доробок програмного забезпечення і переатестації платформ. Фахівці, що відповідають за інтеграцію нових систем, зіткнуться з проблемами сумісності на всіх рівнях: апаратному, програмному і доктринальному.

Проблема картографічного забезпечення є специфічним обмеженням для квантових систем магнітної і гравітаційної навігації (MagNav, GravNav). Їх точність безпосередньо залежить від якості і деталізації відповідних карт аномалій. Актуальні глобальні магнітні і гравітаційні карти з необхідною роздільною здатністю відсутні для більшості театрів бойових дій, особливо в океанічних і полярних районах. Це означає, що ефективне використання квантової навігації вимагає значних попередніх інвестицій у картографування.

Кадрові та доктринальні проблеми

Попри технічний характер більшості вищеназваних викликів, ключовою наскрізною проблемою є катастрофічна нестача фахівців, які поєднують глибоке розуміння квантової фізики з практичними знаннями у галузі безпеки, криптографії та військових систем.

Збройні сили і спецслужби більшості країн, включаючи Україну, ще не виробили доктрин, що регламентують застосування квантових технологій, процедури їх сертифікації і обслуговування в бойових умовах, а також правила обробки інформації з урахуванням загроз HNDL. Ця доктринальна прогалина є не менш небезпечною, ніж суто технічні обмеження, адже навіть за наявності готових технологій їх некоректне або несвоєчасне застосування може знецінити очікуваний ефект.

Висновки

Отже, зважаючи на значну зацікавленість і фінансування квантових технологій з боку як цивільної промисловості, так і урядів, очікується, що ці технології будуть розвиватись і нові квантові застосування стануть доступними протягом найближчих п'яти-десяти років.

Нові досягнення в розробці квантових технологій можуть принести нові можливості для військових. Проте для того щоб військові могли фактично користуватись перевагами нових квантових технологій, важливо, щоб вони активно включились в роботу в цій сфері і скеровували розробку і запровадження військових застосувань квантових технологій. Військові можуть забезпечити значну додану вартість наявним зусиллям промисловості і науки, надавши інфраструктуру для тестування і випробувань (випробувальні центри) і доступ до військових операторів, які будуть кінцевими користувачами. Якомога більш ранні експерименти з цими технологіями не лише допоможуть їхньому подальшому розвитку, але й допоможуть військовим ознайомитись з цими технологіями і їхніми можливостями, що сприятиме майбутньому впровадженню. Більше того, активна участь в квантовій, особливо в кіберсфері. Оцінюючи свої поточні протоколи кібербезпеки, досліджуючи перспективні технології та шукаючи поради експертів, вони можуть краще екосистемі покращує розуміння військовими потенційних ризиків, зв'язаних з квантовими технологіями підготуватися до захисту від майбутніх квантових загроз.

Список використаних джерел

1. Міхель ван Амеронген Квантові технології в обороні і безпеці. URL: https://www.nato.int/docu/review/uk/articles/2021/06/03/kvantov-tehnolog-v-oboron-bezpets/index.html (дата звернення: 14.01.2026).
2. Данилюк І. А., Лазута Р. Г., Куцаєв В. В., Цимбал І. В. Дослідження перспектив застосування квантових технологій у Збройних Силах України. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2025. Вип. 7. URL: https://doi.org/10.58254/viti.7.2025.03.28; https://journal.viti.edu.ua/index.php/cicst/article/view/113.
3. Лисецький Ю. М., Боханченко О. С., Сурма А. І. Використання квантових технологій для забезпечення кіберзахисту. *30 років ВА імені Євгенія Березняка: актуальні проблеми розвідки, контррозвідки, правоохоронної діяльності в умовах широкомасштабної збройної агресії рф проти України* : наук. зб. міжвід. наук.-практ. конф. № 54 (м. Київ, 2 квітня 2024 року). Київ, 2024. С. 114–115.
4. The White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). May 4, 2022. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (дата звернення: 20.01.2026).
5. Sahu S. K., Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics.* 2024. Vol. 12. URL: https://doi.org/10.3389/fphy.2024.1456491.
6. Ali S. et al. Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity – Threats, Mitigations, and Solutions. *Computers & Electrical Engineering*. 2025. Vol. 128. Article 110649. URL: https://doi.org/10.1016/j.compeleceng.2025.110649.
7. The Soufan Center. Quantum Computing and the Evolving Cyber Threat Landscape. IntelBrief. November 15, 2024. URL: https://thesoufancenter.org/intelbrief-2024-november-15/ (дата звернення: 22.01.2026).

8. U.S. Government Accountability Office (GAO). Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy. GAO-25-107703. Washington, D.C., November 21, 2024. URL: https://www.gao.gov/products/gao-25-107703 (дата звернення: 18.01.2026).
9. Dervisevic E., Tankovic A., Fazel E., Kompella R., Fazio P., Voznak M., Mehic M. Quantum Key Distribution Networks – Key Management: A Survey. ACM Computing Surveys. 2025. URL: https://doi.org/10.1145/3730575.
10. Quantum Technologies and Cybersecurity: Threats and Defenses. PostQuantum.com. September 24, 2025. URL: https://postquantum.com/quantum-computing/quantum-cybersecurity/ (дата звернення: 22.01.2026).
11. Purohit K., Vyas A. K. Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology*. 2025. Vol. 4. Article 1575498. URL: https://doi.org/10.3389/frqst.2025.1575498.
12. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. GPS World. November 19, 2025. URL: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (дата звернення: 12.01.2026).
13. Burkey M. T. How Quantum Sensing Will Help Solve GPS Denial in Warfare. Fellow Publication. Center for Global Security Research, Lawrence Livermore National Laboratory. June 2025. LLNL-TR-2004820. URL: https://cgsr.llnl.gov/sites/cgsr/files/2025-06/Burkey_QS_final.pdf (дата звернення: 28.01.2026).
14. Sayler K. M. Defense Primer: Quantum Technology. CRS In Focus IF11836. Congressional Research Service. Washington, D.C., November 4, 2024. URL: https://www.congress.gov/crs-product/IF11836 (дата звернення: 15.01.2026).
15. Ekert A. K. Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*. 1991. Vol. 67. No. 6. P. 661–663. DOI: 10.1103/PhysRevLett.67.661.
16. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE. 1994. P. 124–134.
17. Лисецький Ю. М., Сурма А. І., Данченко О. І. Квантові технології. Нові можливості в кібербезпеці. *Вісник воєнної розвідки.* 2024. № 81. С. 44–47.
18. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. GPS World. November 19, 2025. URL: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (дата звернення: 12.01.2026).

References

1. Mikhel van Ameronhen (2021). Kvantovi tekhnolohii v oboroni i bezpetsi [Quantum technologies in defense and security]. Retrieved from: https://www.nato.int/docu/review/uk/articles/2021/06/03/kvantov-tehnolog-voboron-bezpets/index.html (accessed 14.01.2026) [in Ukrainian].
2. Danyliuk, I. A., Lazuta, R. H., Kutsaiev, V. V., & Tsymbal, I. V. (2025). Doslidzhennia perspektyv zastosuvannia kvantovykh tekhnolohii u Zbroinykh Sylakh Ukrainy [Research into the prospects of applying quantum technologies in the Armed Forces of Ukraine]. *Systemy i tekhnolohii zviazku, informatyzatsii ta kiberbezpeky*. 7. Retrieved from: https://doi.org/10.58254/viti.7.2025.03.28; https://journal.viti.edu.ua/index.php/cicst/article/view/113 [in Ukrainian].
3. Lysetskyi, Yu. M., Bokhanchenko, O. S., & Surma, A. I. (2024). Vykorystannia kvantovykh tekhnolohii dlia zabezpechennia kiberzakhystu [The use of quantum technologies to ensure cyber defense]. *30 rokiv VA imeni Yevheniia Berezniaka: aktualni problemy rozvidky, kontrrozvidky, pravookhoronnoi diialnosti v umovakh shyrokomasshtabnoi zbroinoi ahresii rf proty Ukrainy*: nauk. zb. mizhvid. nauk.-prakt. konf. 54 (pp. 114–115). Kyiv [in Ukrainian].
4. The White House. (2022). National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). Retrieved from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed 20.01.2026).
5. Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics,* 12. Retrieved from: https://doi.org/10.3389/fphy.2024.1456491.
6. Ali, S. & et al. (2025). Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity – Threats, Mitigations, and Solutions. *Computers & Electrical Engineering*, 128. Article 110649. Retrieved from: https://doi.org/10.1016/j.compeleceng.2025.110649.
7. The Soufan Center. (2024). Quantum Computing and the Evolving Cyber Threat Landscape. IntelBrief. Retrieved from: https://thesoufancenter.org/intelbrief-2024-november-15/ (accessed 22.01.2026).

8. U.S. Government Accountability Office (GAO). (2024). Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy. GAO-25-107703. Washington, D.C. Retrieved from: https://www.gao.gov/products/gao-25-107703 (accessed 18.01.2026).
9. Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum Key Distribution Networks – Key Management: A Survey. ACM Computing Surveys. Retrieved from: https://doi.org/10.1145/3730575.
10. Quantum Technologies and Cybersecurity: Threats and Defenses. (2025). PostQuantum.com. Retrieved from: https://postquantum.com/quantum-computing/quantum-cybersecurity/ (accessed 22.01.2026).
11. Purohit, K., & Vyas, A. K. (2025). Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology*, 4. Article 1575498. Retrieved from: https://doi.org/10.3389/frqst.2025.1575498.
12. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. (2025). GPS World. Retrieved from: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (accessed 12.01.2026).
13. Burkey, M. T. (2025). How Quantum Sensing Will Help Solve GPS Denial in Warfare. Fellow Publication. Center for Global Security Research, Lawrence Livermore National Laboratory. LLNL-TR-2004820. Retrieved from: https://cgsr.llnl.gov/sites/cgsr/files/2025-06/Burkey_QS_final.pdf (accessed 28.01.2026).
14. Sayler, K. M. (2024). Defense Primer: Quantum Technology. CRS In Focus IF11836. Congressional Research Service. Washington, D.C. Retrieved from: https://www.congress.gov/crs-product/IF11836 (дата звернення: 15.01.2026).
15. Ekert, A. K. (1991). Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67, 6, 661–663. Retrieved from: https://doi.org/10.1103/PhysRevLett.67.661.
16. Shor, P. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE, 124-134.
17. Lysetskyi, Yu. M., Surma, A. I., & Danchenko, O. I. (2024). Kvantovi tekhnolohii. Novi mozhlyvosti v kiberbezpetsi [Quantum technologies. New opportunities in cybersecurity]. *Visnyk voiennoi rozvidky*, 81, 44-47 [in Ukrainian].
18. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. (2025). GPS World. Retrieved from: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (accessed 12.01.2026).