

Андрій ТРИСТАН,
д-р техн. наук, професор, заступник начальника з наукової роботи
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки, Україна
ORCID 0000-0002-2137-5712

andr.tristan@gmail.com

Володимир ЛАРІН,
канд. техн. наук, доцент, начальник науково-організаційного відділу
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки, Україна
ORCID 0000-0003-0771-2660

lv83@ukr.net

Вікторія ГМИРЯ,
канд. екон. наук, доцент, провідний науковий співробітник
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки, Україна
ORCID 0000-0003-3070-0158

viktoryagmirya@ukr.net

КВАНТОВІ ТЕХНОЛОГІЇ ЯК НЕВІД'ЄМНА СКЛАДОВА ІННОВАЦІЙНОЇ ЕКОСИСТЕМИ У СФЕРІ ЗАХИСТУ ТА БЕЗПЕКИ

Анотація. Квантові технології відіграють важливу роль у забезпеченні захисту і безпеки країни в сучасних глобалізаційних умовах. Квантові технології дійсно мають потенціал стати переломними у сфері оборони і безпеки. Хоча перспективи квантових технологій дуже захоплюючі, їхнє застосування також може породжувати нові виклики і загрози, такі як квантова комп'ютерна атака або розробка квантових збройних систем. Тому важливо, щоб країни і міжнародні організації спільно працювали над розробкою правових, етичних і технічних рамок для використання квантових технологій у сфері оборони і безпеки.

Ключові слова. Інноваційна екосистема, квантові технології, захист і безпека

Актуальність. Інноваційна екосистема – це синергія держави, підприємницького та дослідницького середовища, спрямована на колективні дії у сфері створення потоків знань, підтримку технологічного розвитку й комерціалізації інновацій [1].

Мета світової інноваційної екосистеми визначається не лише потребою в створенні сприятливого середовища для розвитку та впровадження інновацій, а й захистом прав на інтелектуальну власність та збалансованою політикою щодо доступності нових технологій.

Забезпечення умов для глобальних інноваційних проєктів у визнаних сферах знань, таких як ІТ, енергетика, біотехнології та нанотехнології, сприяє просуванню суспільства та розвитку економіки. Однак це повинно відбуватися в рамках міжнародних стандартів та законодавства, які забезпечують баланс між відкритістю нових технологій та захистом прав та інтересів власників інтелектуальної власності.

Постановка завдання. Розвиток і підтримка світової системи патентування грає ключову роль у цьому процесі, сприяючи стимулюванню інновацій та захисту винаходів. Такий підхід допомагає створити сприятливу екосистему для розвитку та впровадження новаторських ідей, забезпечуючи одночасно захист прав винахідників і здійснюючи контроль над розповсюдженням та використанням технологій. Тому питання використання квантових технологій не лише в цивільній сфері, а й у секторі безпеки і оборони набуває важливого значення.

Результати дослідження. Концепція інноваційної екосистеми виокремлює ключові складові, необхідні для створення сприятливого середовища для інноваційної діяльності. Людський капітал визначається не лише кількістю, а й якістю знань, компетенціями та мотивацією людей. Капітал відносин вказує на важливість спільного бачення, довіри та

впевненості між учасниками екосистеми. Структурний капітал, у свою чергу, охоплює організації та інфраструктуру, які сприяють розвитку та впровадженню інновацій.

Ця концепція може служити основою для розвитку стратегій урядів, бізнесу та громадських організацій з метою сприяння інноваціям. Вона покликана стимулювати співпрацю між різними галузями та стейкхолдерами для досягнення спільних цілей у сфері інновацій.

Співпраця між Україною та НАТО в сфері інновацій, зокрема у розвитку квантових технологій, може бути дуже перспективною. Квантові технології вважаються одними з найбільш перспективних у світі сучасних технологій через їх потенціал змінювати парадигми у багатьох галузях, включаючи обчислювальну та криптографію.

Україна, з своїм великим потенціалом у галузі наукових досліджень та інженерної компетентності, може активно долучитися до розвитку квантових технологій. Співпраця з НАТО в цьому напрямку може допомогти Україні отримати доступ до новітніх наукових розробок, технологічних знань та фінансування, що сприятиме її технологічному розвитку та конкурентоспроможності.

Крім того, така співпраця може сприяти інтеграції України у міжнародні інноваційні мережі та підвищенню її статусу на міжнародній арені. Разом з тим, це може стимулювати розвиток внутрішніх інноваційних екосистем та сприяти створенню нових робочих місць у високотехнологічних секторах економіки.

Квантові технології можуть принести нові можливості як для цивільних, так і для військових цілей. Квантові технології отримали значний інтерес з боку промислових виробників і урядів країн в останні роки [2]. Великі технологічні компанії, такі як IBM, Google і Microsoft, витрачають сотні мільйонів доларів на дослідження і розробки в галузі квантових обчислень у боротьбі за «квантову перевагу». Уряди розвинених країн також визнали трансформаційний потенціал і геополітичну цінність застосування квантових технологій. Сполучені Штати Америки, Європейський Союз і Китай створили власні дослідницькі програми вартістю понад 1 мільярд доларів кожна [3].

Покращене розуміння фундаментальних квантових принципів стало поштовхом до розвитку квантових технологій наступного покоління – квантові сенсори, квантовий зв'язок та квантові обчислення.

Квантові сенсори ґрунтуються на ультрахолодних атомах або фотонах, якими обережно маніпулюють за допомогою суперпозиції або зчеплення у конкретних «квантових станах» [4]. Квантові сенсори відкривають перед нами безліч нових можливостей у різних сферах, включаючи військові цілі. Вони дають змогу вимірювати навіть дуже малі розбіжності у різних властивостях, що робить їх надзвичайно корисними для виявлення та вимірювання різноманітних параметрів.

У військових цілях квантові сенсори можуть мати велике значення. Наприклад, вони можуть допомогти в розвитку систем розвідки та нагляду, забезпечуючи більш точне та чутливе зондування навколишнього середовища. Це може включати виявлення підземних структур або виявлення змін у геологічних формаціях, які можуть свідчити про можливі воєнні загрози.

Крім того, квантові сенсори можуть забезпечити вдосконалені системи навігації та мапування для військових додатків, що може бути критичним для здійснення операцій у складних умовах, таких як гірський рельєф або в густому лісі.

Такі технології можуть також забезпечити значний внесок у розвиток автономних систем, які можуть виявити широке застосування в військових цілях, включаючи розвідку, безпілотний транспорт та системи безпеки.

В цілому, розвиток квантових сенсорів може покращити здатність військових сил до виявлення та реагування на загрози, забезпечуючи перевагу в бойових умовах.

Хоча квантові технології можуть здаватися технологіями далекого майбутнього, перші квантові датчики насправді вже доступні на ринку (наприклад, атомні годинники та гравіметри). Забігаючи наперед, можна очікувати, що протягом наступних п'яти-семи

років з'явиться більше застосувань квантового зондування, зокрема, квантові пристрої позиціонування, навігації і синхронізації (PNT) та квантові радіолокаційні технології.

Квантовий зв'язок відкриває нові можливості для безпечної передачі даних, які не можуть бути перехоплені чи скомпрометовані зловмисниками. Це досягається завдяки використанню властивостей квантових частинок, таких як квантовий стан, квантова надмірність та неперервність станів. Квантовий зв'язок може забезпечити велику стійкість до вторгнень і викрадень даних, що робить його привабливим для використання в сферах, де конфіденційність і безпека даних є вирішальними.

Квантовий розподіл ключів (QKD) є одним з перших застосувань квантового зв'язку. Він використовує квантові частинки для обміну криптографічними ключами, які використовуються для шифрування та розшифрування даних. Цей процес гарантує, що ключі не можуть бути перехоплені або зламані під час передачі, оскільки будь-яка спроба перехоплення змінить стан квантових частинок і буде виявлена.

Широкі експерименти в галузі QKD демонструють потенціал цієї технології як для земного, так і для космічного зв'язку. Використання квантового зв'язку в космосі відкриває нові перспективи для безпечної та надійної комунікації на великі відстані, що може мати важливе значення для сучасних і майбутніх космічних місій, включаючи космічну експлорацію, супутникову зв'язок та оборонні цілі.

Першопрохідцем в даному напрямку був Китай, який запустив у 2016 році перший у світі квантовий науковий супутник «Міціус», який відтоді продемонстрував міжконтинентальний зв'язок «земля-супутник» і «супутник-земля», забезпечивши відеоконференцію між Пекіном і Віднем [5].

Розвиток квантового інтернету потенційно відкриває нову еру для комунікацій та обчислень, переносячи людство з класичної інформаційної епохи в еру, де квантові властивості матеріалів використовуються для зберігання, обробки та передачі інформації.

Однією з ключових складових квантового інтернету є квантові комп'ютери, які використовують квантові біти або кубіти замість класичних бінарних бітів. Квантові комп'ютери мають потенціал виконувати обчислення на непорівнянно вищому рівні швидкості та ефективності порівняно з класичними комп'ютерами. Вони можуть бути особливо корисними для моделювання складних систем, оптимізації задач та розв'язання криптографічних завдань.

Підтримка квантового інтернету вимагає інтеграції квантових комп'ютерів з мережею квантового зв'язку, яка забезпечує безпечну передачу квантової інформації між різними вузлами мережі. Квантовий зв'язок, заснований на законі квантової механіки, надає механізми для захисту від несанкціонованого доступу до переданих даних.

Подальший розвиток квантового інтернету потребує не лише вдосконалення квантових комп'ютерів і квантового зв'язку, але й розробки комплексного стеку програмного забезпечення, включаючи інтернет-протоколи та алгоритми шифрування, спеціально призначені для квантового середовища.

Існує низка застосувань, де квантові комп'ютери будуть особливо трансформаційними:

- моделювання фізичних систем для розробки нових матеріалів;
- розв'язання складних оптимізаційних задач у ланцюгах поставок, логістиці та фінансах;
- поєднання зі штучним інтелектом для прискорення комп'ютерного навчання;
- факторизація цілих чисел, що дозволяє розшифровувати найпоширеніші протоколи кібербезпеки (наприклад, RSA, асиметричний алгоритм шифрування, який використовується для безпечної передачі даних).

Великі технологічні компанії, такі як IBM, Google і Microsoft, змагаються за «квантову перевагу», яка полягає в тому, що квантовому комп'ютеру вдається вирішити проблему, яку жоден класичний комп'ютер не може вирішити за будь-який можливий проміжок часу.

Яку роль квантові технології відіграють для оборони і безпеки.

Квантові сенсори в сфері оборони та безпеки мають потенціал стати переважними засобами виявлення та навігації, забезпечуючи нові можливості для вирішення військових та безпекових завдань.

По-перше, квантові сенсори можуть бути використані для виявлення субмарин та літаків-невидимок. Будучи надзвичайно чутливими до мінімальних змін в навколишньому середовищі, квантові сенсори можуть допомогти виявити навіть найменші зміни у рельєфі морського дна або атмосферних умовах, що може вказувати на присутність підводних човнів або невидимих літаків.

Далі, квантові пристрої PNT (Positioning, Navigation, and Timing) можуть забезпечувати надійну і високоточну навігацію без необхідності у зовнішній прив'язці, такий як GPS. Це особливо важливо для підводних човнів, які часто опиняються у ситуаціях, де сигнал GPS не доступний. Квантові пристрої PNT можуть надавати незалежну систему навігації, що дозволяє їм ефективно виконувати завдання в будь-яких умовах.

Ці технології мають потенціал перетворити підхід до виявлення та навігації у військовій та безпековій сферах, забезпечуючи нові можливості для ефективного захисту національних інтересів та забезпечення безпеки населення країни.

Так, розвиток квантових технологій, зокрема квантових сенсорів, має потенціал стати вирішальним напрямком не лише у військовій сфері, але й у цивільному секторі. Зважаючи на широкий спектр застосувань цих технологій, від зв'язку до обчислень до зондування, цивільний сектор також активно зацікавлений у їхньому використанні.

Проте військова сфера має специфічні потреби та вимоги, які можуть вимагати розробки спеціалізованих квантових технологій. Наприклад, квантові PNT та квантовий радар можуть бути критичними для військових операцій, де точність, швидкість та безпека навігації та виявлення є надзвичайно важливими.

Фінансування, підтримка та спрямування досліджень і розробок в галузі квантових технологій військовою сферою може допомогти прискорити їхній розвиток та перетворити потенційні застосування в реальність. Такий підхід може сприяти не лише вдосконаленню військових можливостей, але й сприяти розвитку цивільних застосувань квантових технологій, що має великий економічний та соціальний потенціал.

По-друге, «квантова загроза» з боку квантового обчислення, як було зазначено, факторизація цілих чисел – це один із типів проблем, які квантові комп'ютери можуть розв'язувати особливо ефективно. Більшість цифрової інфраструктури і практично все, що здійснюється онлайн: відеоконференція, розсилка електронної пошти або онлайн доступ до банківських рахунків – зашифровано за допомогою криптографічних протоколів на основі того, що розв'язати проблему такого зразка факторизації цілих чисел важко (наприклад, алгоритм RSA) [6]. Хоча придатні для практичного використання квантові комп'ютери все ще потребують розробки, квантовий алгоритм для розв'язання цих проблем і розшифрування цифрової комунікації, тобто алгоритм Шора, був винайдений в 1994 році і очікує на квантовий комп'ютер, який зможе ним користуватись [7].

Справді, зростання квантових технологій створює нові виклики і можливості, як для цивільного суспільства, так і для військових структур. Надзвичайно важливо, щоб керівники в різних секторах розуміли ці виклики і готувалися до них.

Перехід до «квантово-стійкої» криптографії і захищеної цифрової інфраструктури є надзвичайно важливим для забезпечення безпеки і конфіденційності в умовах зростаючої загрози квантового обчислення. Квантовий зв'язок, такий як квантова телепортація, може забезпечити високий рівень безпеки передачі інформації, що стане невід'ємною складовою цифрової інфраструктури майбутнього.

Однак, разом із цим, необхідно враховувати потенціальні загрози безпеки, пов'язані з квантовими технологіями, і розробляти відповідні заходи для їх запобігання та протистояння. Крім того, важливо підтримувати та спрямовувати дослідження і розробки в галузі квантових технологій, як у цивільному, так і військовому секторах, з метою максимізації їхнього потенціалу та забезпечення безпеки та стабільності.

Висновок. Так, розвиток квантових технологій відкриває широкі можливості для військових застосувань, які можуть значно поліпшити оборонні можливості та забезпечити перевагу на полі бою. Проте для того, щоб максимально використовувати потенціал цих технологій, необхідно активно співпрацювати та координувати зусилля між різними країнами та інституціями.

Важливо, щоб країни Європейського союзу та країни члени НАТО виявили зацікавленість і зобов'язання в розробці та впровадженні військових застосувань квантових технологій. Це може включати співпрацю з великими технологічними компаніями, а також активне взаємодію зі стартапами, університетами та науково-дослідними інститутами.

Стартапи та університети можуть відігравати ключову роль у розвитку інноваційних рішень та нових технологій у цій області. Вони часто мають гнучкіші структури та можуть швидше реалізувати новаторські ідеї. У той же час, великі технологічні компанії можуть забезпечити необхідні ресурси та експертизу для розвитку та впровадження квантових технологій у військові застосування.

Спільна робота між цими гравцями може сприяти розвитку нових військових технологій, що базуються на квантових принципах, та забезпечити важливу перевагу у сфері безпеки та оборони.

Список використаних джерел

1. МОН проводить опитування щодо змін у інноваційній екосистемі серед учасників процесу її створення. URL: <https://mon.gov.ua/ua/news/mon-provodi-opituvannya-shodo-zmin-u-innovacijnij-ekosistemi-sered-uchasnikiv-procesu-yi-yi-stvorenniya> (дата звернення 10.04.2024)
2. The realist's guide to quantum technology and national security <https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html> (дата звернення 10.04.2024)
3. Sensing the future of quantum. <https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html> (дата звернення 10.04.2024)
4. National security and technology regulation. <https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html> (дата звернення 10.04.2024)
5. National agenda on quantum technology: the Netherlands as an international centre for Quantum Technology. URL: <https://qutech.nl/2019/09/16/national-agenda-on-quantum-technology-the-netherlands-as-an-international-centre-for-quantum-technology/> (дата звернення 10.04.2024)
6. RSA (cryptosystem). URL: [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem)) (дата звернення 10.04.2024)
7. Shor's algorithm URL: https://en.wikipedia.org/wiki/Shor%27s_algorithm (дата звернення 10.04.2024)

Andrii TRYSTAN,

Dr of Technical Sciences, professor, Deputy Head of the Institute for Scientific Work,
State Research Institute of Testing and Certification of Weapons and Military Equipment, Ukraine

Volodymyr LARIN,

Ph.D. in Engineering, Associate Professor, Head of Scientific and Organizational Department,
State Research Institute of Testing and Certification of Weapons and Military Equipment, Ukraine

Viktoriia HMYRIA,

Ph.D. in Economics, Associate Professor, Leading Researcher
State Research Institute of Testing and Certification of Weapons and Military Equipment, Ukraine

QUANTUM TECHNOLOGIES AS AN INTEGRAL PART OF THE INNOVATIVE ECOSYSTEM IN THE FIELD OF DEFENCE AND SECURITY

Abstract. Quantum technologies play an important role in ensuring the country's defence and security in the current globalized environment. Quantum technologies have the potential to become a game-changer in the field of defence and security. While the prospects of quantum technologies are very exciting, their application can also give rise to new challenges and threats, such as quantum computer attack or the development of quantum weapons systems. Therefore, it is important that countries and international organizations work together to develop legal, ethical and technical frameworks for the use of quantum technologies in defence and security.

Keywords. innovation ecosystem, quantum technologies, defence and security