

# Квантові технології: майбутнє, що вже настало

*Павло Бурдяк, аналітик напрямку “Незалежні медіа”*



**2026**

*Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного фонду «Відродження» в рамках спільної ініціативи «Вступаємо в ЄС разом». Матеріал представляє позицію авторів і не обов'язково відображає позицію Європейського Союзу чи Міжнародного фонду «Відродження».*

*Є така теорія: якщо хто-небудь коли-небудь дізнається, для чого насправді потрібен Всесвіт і чому він взагалі існує, то він миттєво зникне й буде замінений чимось ще більш дивним і незрозумілим. Але є й інша теорія — що це вже сталося.*

Дуглас Адамс, "Путівник по Галактиці для космотуристів"

Британський письменник-сатирик Дуглас Адамс у своєму культовому романі "Путівник по Галактиці для космотуристів" жартував про природу Всесвіту, але його слова напрочуд влучно описують людську природу і науку. Кожного разу, коли людство вважає, що розуміє світ, з'являється щось нове, ще дивніше та складніше. Так було з гравітацією Ньютона, яку перевернув Ейнштейн. Так сталося з класичною фізикою, якій кинула виклик квантова механіка. І так відбувається знову: коли ми думаємо, що оволоділи технологіями штучного інтелекту, світ робить новий крок у невідомий (чи маловідомий) квантовий вимір.

Квантові технології – це наступний стрибок в цій нескінченній подорожі людства до розуміння реальності. Вони використовують найпарадоксальніші явища квантової механіки – суперпозицію, заплутаність – щоб розв'язувати завдання, які не під силу технологіям, заснованим на принципах класичної фізики. Але, як і у романі Адамса, коли ми знаходимо одну нову відповідь, виникає десять нових запитань. Запитань, на які ми не те що не можемо відповісти, а які ми ще не можемо навіть зрозуміти. Як [вказав](#) видатний фізик і лауреат Нобелівської премії Річард Фейнман: "Ніхто не розуміє квантову механіку", навіть фізики – тим не менш, вона стає основою технологій, які змінюють світ.

Період наступних 5-10 років – це вікно можливостей. Квантові технології вплинуть на кібербезпеку, оборону, медицину, енергетику та інші сфери критичної інфраструктури. Європейський Союз і країни-члени уже [вклали](#) щонайменше €11 мільярдів у розвиток цих технологій. США, Велика Британія та Китай роблять те саме. Україна також може і повинна брати активну участь у розробці національних та європейських стандартів, захищати свою критичну інфраструктуру від квантових викликів та позиціонувати себе як інноваційного партнера у європейській квантовій екосистемі.

Цей аналітичний матеріал розповідає історію квантових технологій: що це таке, як вони виникли, які можливості та загрози вони несуть, як світ готується до їх приходу і найголовніше – як Україна повинна діяти прямо зараз, щоб не залишитися позаду.

## Зміст

<i>Перша квантова революція: як все починалося.....</i>	<i>4</i>
<i>Квантовість починається там, де світ стає “зернистим” і “розмитим”.....</i>	<i>5</i>
<i>Від першої квантової революції до другої: коли теорія перетворюється на інженерію.....</i>	<i>8</i>
<i>Квантове сенсування: як ми навчилися чути шепіт Всесвіту.....</i>	<i>10</i>
<i>Квантові обчислення і пошук відповіді на найважливіше питання Всесвіту.....</i>	<i>12</i>
<i>Квантова комунікація як місток для квантового світу.....</i>	<i>14</i>
<i>Квантова архітектура Європейського Союзу: побудова цифрового суверенітету.....</i>	<i>15</i>
<i>Європейська квантова стратегія – закріпити лідерство до 2030 року..</i>	<i>16</i>
<i>Грядущий Квантовий акт як законодавчий фундамент регулювання квантових технологій в ЄС.....</i>	<i>17</i>
<i>Програма “Флагман квантових технологій”.....</i>	<i>17</i>
<i>EuroHPC JU: квантові прискорювачі для суперкомп'ютерів.....</i>	<i>18</i>
<i>EuroQCI: захищені квантові комунікації від Лісабона до Таллінна.....</i>	<i>19</i>
<i>Постквантова криптографія як базовий стандарт захисту даних у квантову епоху.....</i>	<i>19</i>
<i>Квантовий “іспит” для України у контексті євроінтеграції.....</i>	<i>21</i>
<i>Стратегічні орієнтири для України: короткостроковий, середньостроковий та довгостроковий горизонти.....</i>	<i>23</i>

## Перша квантова революція: як все починалося

На початку ХХ століття класична фізика здавалася майже завершеною наукою. Ньютонівська механіка пояснювала рух планет і маятників, рівняння Максвелла описували електромагнітні хвилі, термодинаміка розкривала природу тепла. Здавалося, що залишалось лише заповнити кілька прогалин – і картина світу стане повною. Але саме ці кілька "прогалин" виявилися прірвою.

Квантова революція у фізиці розпочалася непомітно. У 1900 році німецький фізик Макс Планк [намагався](#) пояснити природу випромінювання нагрітого абсолютного чорного тіла. [Абсолютне чорне тіло](#) – це тіло, яке повністю поглинає проміння (усіх довжин хвиль), що падає на нього. Планк [припустив](#), що енергія випромінюється і поглинається не безперервно, як це тоді передбачала класична фізика (так званий [парадокс "ультрафіолетової катастрофи"](#)), а окремими порціями – квантами. І хоча сам Планк за освітою й способом мислення залишався типовим представником класичної фізики, [скептично](#) ставився до першочергових результатів своєї роботи й називав своє відкриття "актом відчаю", його напрацювання стали відправним пунктом в історії розвитку квантової механіки. У 1919 році Макс Планк [отримав](#) Нобелівську премію з фізики за відкриття квантів енергії.

У 1905 році Альберт Ейнштейн розвинув напрацювання Планка, щоб [пояснити фотоефект](#) (вивільнення електронів від зв'язку з атомами речовини під дією світла). Він [висунув](#) гіпотезу, що світло має не просто хвильову природу, як це вважали на той час, а складається з потоку окремих частинок – квантів світла (фотонів). Фотони є ключовим елементом сучасних технологій, таких як лазери, оптоволокло та фотоніка. У 1921 році Ейнштейну [присудили](#) Нобелівську премію з фізики "за його заслуги в галузі теоретичної фізики, а особливо за відкриття закону фотоефекту". Протягом наступних років інші дослідники продовжували розвивати теорію квантової механіки. Нільс Бор [запропонував](#) квантову модель атома, яку згодом узагальнив Арнольд Зоммерфельд на системи з декількома ступенями вільності (умови квантування Бора-Зоммерфельда). Луї де Бройль [висунув](#) гіпотезу, що не тільки світло (фотони) має хвильові властивості, але й усі елементарні частинки (так званий "корпускулярно-хвильовий дуалізм").

Та основи квантової механіки [заклали](#) у 1920-х роках вчені Вернер Гейзенберг і Ервін Шрödінгер. У 1925 році Гейзенберг з'ясував, що поведінку частинок у квантовому світі неможливо точно передбачити на основі класичних законів фізики, і запропонував матричну квантову механіку, яка базувалася на ймовірності можливих станів системи. А кілька роками пізніше Гейзенберг сформулював знаменитий принцип невизначеності, який проголосив неможливість одночасного точного вимірювання положення та імпульсу частинки.

Цей принцип став наріжним каменем квантової механіки, підкреслюючи, що невизначеність на мікрорівні є фундаментальною властивістю самої природи, а не обмеженням проведених експериментів чи застосованих інструментів.

У 1926 році Ервін Шрєдінгер винайшов рівняння, відповідно до якого кожна частинка має хвильову природу, а її поведінка визначається через хвильову функцію, що містить інформацію про всі можливі стани частинки. Так була відкрита так звана "хвильова квантова механіка". Та згодом виявилось, що матрична квантова механіка Гейзенберга і хвильова квантова механіка Шрєдінгера – це не дві різні механіки, а лише дві різні мови, які описують одне й те ж явище, лише іншими словами. Це було підтверджено в роботах Поля Дірака, який об'єднав ці підходи в єдину квантову механіку.

Так зародилася квантова механіка – фундаментальна теорія у фізиці, що описує поведінку матерії та енергії на атомному та субатомному рівнях.

### **Квантовість починається там, де світ стає “зернистим” і “розмитим”**

Якщо класична фізика описує рух і взаємодію того, що ми здатні спостерігати напряду (падіння волейбольного м'яча чи руху зірки в небі), то квантова – поведінку “цеглинок” матерії та енергії: фотонів (квантів світла), електронів, кварків тощо. Зручна аналогія – цифрове зображення: поки ви дивитеся на фото здалеку, бачите цілісну картинку; якщо ж сильно “наблизити”, виявиться, що вона складається з пікселів. Так само і з матерією: на дуже малих масштабах вона складається з “квантів” – також немовби з пікселів. Але на відміну від пікселя, квантова частинка не має чітко визначеного місця: ми можемо говорити лише про те, де її найімовірніше знайти. Це як лінія, проведена олівцем: здалеку вона видається рівною, а зблизька видно, що край розмитий.

“Розмитість” квантової механіки породжує унікальні принципи, які спантеличили перших фізиків у цій сфері, і які сучасні науковці все ще намагаються осягнути. Їх важливо розуміти, оскільки на них базується розвиток квантових технологій. А саме, до таких принципів квантової механіки належать:

1. **Корпускулярно-хвильовий дуалізм:** дуже малі частинки можуть проявлятися як хвилі або як частинки – залежно від того, як ми їх спостерігаємо.

Приклад із повсякденного життя – світло. Коли воно проходить крізь дрібні краплі води, проявляється його хвильова природа й виникають знайомі нам візерунки на кшталт веселки. А коли світло падає на сонячну панель, ми спостерігаємо, як енергія фотонів надходить

«порціями» (як тверді кулі, що вдаряються об екран), і сприймаємо їх як частинки.

1. **Суперпозиція:** у квантовому світі частинка може одночасно бути в кількох можливих станах. Нам важко це зрозуміти, бо на макроскопічному рівні об'єкти мають чіткі властивості: вони знаходяться в одному місці, мають визначений стан, явно "включені" або "вимкнені". Але на рівні атомів і частинок все інакше. Квантові об'єкти можуть одночасно перебувати у кількох станах – це явище і називається суперпозицією. Щоб краще зрозуміти цю особливість квантової механіки, можна провести аналогію з музичними інструментами. Музичні інструменти можуть видавати багато нот (тонів, вібрацій або частот) одночасно. Схожим чином суперпозиція дозволяє частинкам існувати в декількох «станах» одночасно.
2. **Принцип невизначеності Гейзенберга:** невизначеність присутня в будь-яких вимірюваннях, але на квантовому рівні вона стає дуже помітною.

Щоб щось виміряти, треба якось “доторкнутися” до об'єкта – тобто взаємодіяти з ним. Наприклад, ми бачимо міську ратушу у фізичному світі, бо на неї падає світло, а фотони відбиваються і потрапляють нам в очі. Для ратуші це майже нічого не змінює: енергії фотона замало, щоб зрушити будівлю.

Але якщо “об'єкт” – не такий великий, як ратуша, а крихітний, як електрон, то той самий фотон стає для нього відчутним “поштовхом”. Тобто сам факт вимірювання (взаємодії) змінює стан частинки.

У цьому й суть принципу невизначеності Гейзенберга: через те, що вимірювання неминуче впливає на квантовий об'єкт, є деякі величини, які не можна виміряти одночасно з високою точністю – наприклад, точне місце і точний імпульс, або точний час і точну енергію.

1. **Заплутаність:** два об'єкти можуть бути настільки пов'язані, що стан одного миттєво впливає на стан іншого, незалежно від відстані між ними.

Поширеною аналогією для розуміння квантової заплутаності двох фотонів є дві “заплутані” монети. Так, уявімо, що Анна і Василь перебувають на відстані 300 тисяч кілометрів один від одного й мають “пару” особливих “заплутаних” квантових монет. Кожен підкидає свою монету й записує результат – “орел” або “решка”. Для Анни результат щоразу виглядає випадковим (приблизно 50/50), і для Василя так само. Але коли вони потім порівнюють записи, виявляється дивна закономірність: їхні результати завжди узгоджені – якщо в Анни випав “орел”, то у Василя “решка”, якщо в Анни “решка” – у Василя “орел”.

Сенс аналогії в тому, що випадковість проявляється лише “наодинці”: Анна не знає наперед, що випадде, і Василь теж. Але після порівняння видно, що їхні результати не незалежні – між ними щоразу є чітка відповідність і взаємозалежність, яку можна перевірити, попри відстань у 300 тисяч кілометрів.

1. **Спін:** це [базова](#) властивість частинки, як маса або заряд, яка впливає на її поведінку та взаємодію з іншими частинками. Спін не дає частинкам речовини “злипатися” в одному місці. Через це електрони в атомі змушені “розкладатися по місцях”, атоми стають стабільними, а речовина має форму й об’єм.

Тобто стіл твердий, а ваше тіло не провалюється крізь підлогу – частково завдяки цій властивості.

1. **Тунелювання:** це явище, коли частинка [може](#) з певною ймовірністю “прослизнути” крізь енергетичний бар’єр і опинитися по інший бік, хоча за класичними законами їй бракувало б енергії, щоб його подолати. Причина в тому, що квантова частинка описується хвильовою функцією: вона не “сидить” в одній точці, а має певну ймовірність бути в різних місцях. Якщо бар’єр тонкий, частина цієї “ймовірності” може проникнути крізь нього – і тоді інколи частинка виявляється з іншого боку.
2. **Когерентність і декогерентність.** Когерентність [описує](#) стабільність квантової системи. Декогерентність – це коли квантовий стан “ламається” [через](#) небажані контакти з довкіллям.

Квантові стани дуже крихкі: якщо частинка в суперпозиції випадково взаємодіє з теплом, повітрям, електромагнітними завадами чи іншими частинками, суперпозиція починає зникати так, ніби систему “поміряли”. Через це квантова система перестає поводитися “по-квантовому” і стає більш “звичайною” (класичною). Саме тому в квантових технологіях так багато уваги ізоляції, охолодженню, вакууму тощо.

Згадані квантові концепції докорінно змінили наше уявлення про природу на найглибшому рівні – і це швидко вийшло за межі підручників. Так, наприклад, коли стало [зрозуміло](#), що електрон може поводитися як хвиля, з’явилося пояснення періодичної таблиці, хімічних зв’язків і поведінки електронів у твердих тілах – а звідти вирости фізика напівпровідників і вся індустрія мікрочипів, що лягла в основу комп’ютерів і “класичних” інформаційно-комунікаційних технологій. На них тримаються цифрові економіки сьогодні. А коли світло почали описувати як потік частинок (фотонів), з’явилася можливість коректно пояснити фотоефект і створити практичні речі на кшталт сонячних елементів, копіювальних апаратів, лазерів тощо. Ці та інші винаходи (як-от глобальна система позиціонування GPS, ядерна енергетика) часто [називають](#) плодами “першої квантової революції”.

Вплив “першої квантової революції” відчутний не лише в гаджетах і мережах, а й у безпосередній якості життя. Яскравий приклад – [медицина](#): магнітно-резонансна томографія (МРТ) та позитронно-емісійна томографія (ПЕТ) радикально підсилили діагностику, бо дозволяють безопераційно отримувати дуже детальні зображення внутрішніх структур і функцій органів. Тобто квантова фізика “вийшла” з лабораторій не тільки в процесори, а й у лікарні – у вигляді технологій, які буквально рятують життя, допомагаючи виявляти хвороби точніше й раніше.

Загалом же, до кінця ХХ століття перша квантова революція принесла набір базових технологій, на яких стоїть сучасне суспільство, і заклала фундамент сучасної інформаційної епохи.

### **Від першої квантової революції до другої: коли теорія перетворюється на інженерію**

Якщо перша квантова революція дала людству нові правила, за якими працює фізична реальність, то друга взяла ці правила і почала перетворювати їх на нові технології.

У першій революції ми могли описати періодичну таблицю, але не створювали нові атоми “під замовлення”. Ми могли пояснити, як поведуться метали чи напівпровідники, але не могли маніпулювати їхніми станами чи контролювати їх.

Друга революція – це момент, коли [з’являється](#) такий контроль: ми створюємо штучні “атоми” (наприклад, квантові точки, які забезпечують високу яскравість, якісну передачу кольору та енергоефективність, що робить їх основою сучасних QLED-дисплеїв), проєктуємо їхні електронні й оптичні властивості, і навіть навмисно робимо стани когерентності або заплутаності, які в природі трапляються рідко або не існують у такому вигляді. Саме ці створені людиною квантові стани дають нові можливості для створення надчутливих сенсорів, нових способів зв’язку, точних вимірювальних пристроїв, а також адаптації принципово іншого підходу до здійснення обчислень. Тобто квантова механіка як наука вже зріла, а от квантова інженерія як технологія – тільки стає на ноги, і це й є ядро другої квантової революції.

Впродовж останніх десятиліть [з’явився](#) новий напрям – квантова інформатика та технології (Quantum Information Science and Technology, QIST). Суть цього напрямку в тому, що квантові принципи тут використовують з метою інженерії: не лише щоб пояснювати, як працюють матеріали чи прилади, а щоб саме на основі квантових принципів записувати, вимірювати, обробляти і передавати інформацію. Тобто якщо під час першої квантової революції квантова механіка допомагала створювати технології на базі класичної

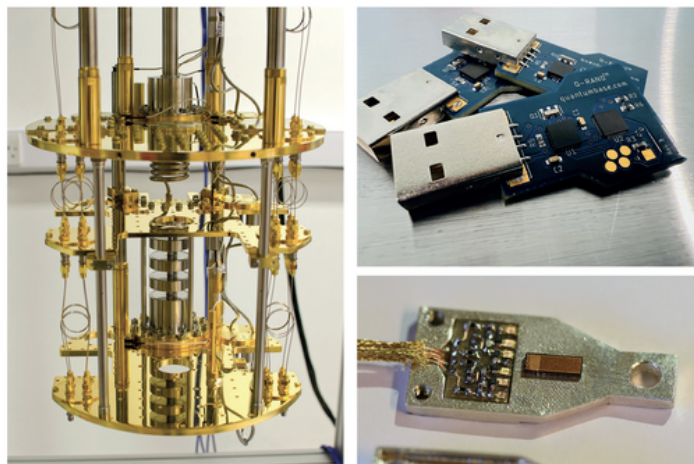
електроніки, то під час другої – квантові принципи стають наріжним каменем нових технологій.

Коли люди чують “нові квантові технології”, у голові зазвичай одразу спалахує один образ – квантовий комп’ютер. Десь миготіло в новинах, хтось сказав “зламає весь інтернет”, і все: квантові технології = квантові комп’ютери. Насправді ж квантові комп’ютери – лише один із прикладів квантових технологій (про це ще поговоримо згодом).

Загалом же виділяють три основні сфери розвитку квантових технологій у період другої квантової революції:

1. **Квантове сенсування (quantum sensing)** – це надточні вимірювання фізичних величин (наприклад, часу, магнітних полів або освітленості) з чутливістю та точністю, яких не дають звичайні датчики.
2. **Квантові обчислення (quantum computing)** – це спроба розв’язувати задачі (зокрема за допомогою згаданих квантових комп’ютерів), які для найпотужніших сучасних комп’ютерів є надто складними або практично недосяжними.
3. **Квантові комунікації (quantum communication)** – це спроби використовувати квантові властивості частинок, щоб кодувати й передавати інформацію, будувати мережі квантових пристроїв і посилювати цифрову безпеку.

Пристрій квантового обчислення (ліворуч), квантові сенсори (внизу праворуч) та пристрої безпеки (вгорі праворуч).



Джерело: Центр квантових технологій Ланкастерського університету.  
Отримано з [доповіді](#) Роба Янга

Далі розглянемо кожну із цих сфер окремо – що вже працює, що ще “на підході”, та які можливості й ризики це створює.

## Квантове сенсування: як ми навчилися чути шепіт Всесвіту

Уявіть, що ви намагаєтеся почути кроки kota в центрі головного залізничного вокзалу в Києві в годину пік, щоб з'ясувати, в якому місці він зараз перебуває. Для наших вух це майже неможливе завдання: гуркіт потягів та сотні голосів просто розмивають делікатний звук котячих лапок у суцільний сірий шум. Але з цим завданням можуть справитися квантові сенсори. Вони не просто функціонують як "покращений слух". Вони вимірюють дуже конкретний "слід" kota – мікросміни фізичних величин під час його руху (наприклад, крихітні зміни прискорення або магнітного/гравітаційного поля) – і тому можуть відсікати більшість фонового шуму, який збиває наші класичні сенсори.

Чому квантові сенсори такі точні? Відповідь – у [масштабі](#). Класичні датчики вимірюють колективну поведінку великої кількості атомів одразу – як натовп на тому ж вокзалі, де голос одного губиться в загальному гулі. Квантові сенсори натомість "слухають" окремі атоми – і саме ця різниця дає експоненційно вищу точність, повноту й ефективність вимірювань.

Ще одна суттєва [перевага](#) квантових сенсорів, яка особливо актуальна в епоху гібридних воєн і кібератак: квантові сенсори принципово стійкіші до заглушення й електромагнітних завад. Класичні датчики – світлові, звукові, радіочастотні – вразливі до перешкод: їх можна заглушити, збити з пантелику, обдурити. Квантовий сенсор працює на рівні, де такі перешкоди значно складніше створити.

Квантові сенсори розвивають (а подекуди вже й використовують) у низці [сфер](#), як-от:

- **Атомні годинники.** На відміну від звичайних годинників, які працюють на основі механічних деталей або електричних сигналів, атомні годинники вимірюють час на основі постійних і передбачуваних коливань атомів.
- **Квантові гравіметри.** Це прилади, що вимірюють силу гравітаційних полів за допомогою атомів. Атоми ідеально підходять для точних вимірювань, оскільки їхня точна маса відома, на відміну від штучних об'єктів у класичних гравіметрах, маса яких може змінюватися під час виготовлення або інших маніпуляцій.
- **Квантові інерційні датчики/сенсори.** Це пристрої, що використовують квантові частинки, такі як атоми або іони, для виявлення змін положення, швидкості та напрямку. Вони забезпечують більш надійні дані навіть у середовищах, де традиційні системи можуть мати труднощі, наприклад, на великій глибині під водою, під землею або в густо забудованих міських районах без належного доступу до сигналів GPS. Це сприяє виробленню значно точніших гіроскопів і пристроїв навігації.

- **Квантові магнітометри.** Це пристрої, що використовують частинки, такі як електрони або атоми, для вимірювання сили магнітних полів.
- **Квантові електрометри.** Це пристрої, що використовують атоми для вимірювання сили електричних полів (радіочастот). Вони можуть вимірювати широкий діапазон частот, що робить їх універсальними для різних технологічних застосувань.
- **Фотонні детектори.** Це пристрої, що використовують фотони та їхні квантові властивості для виявлення та аналізу найслабших джерел світла. Вони мають широке застосування: від камер і телескопів до наукових експериментів. Коли ж фотонні детектори використовують не просто для фіксації “є світло/немає світла”, а для відновлення просторової картини – тобто для побудови зображення – ми переходимо до квантової візуалізації. Очікується, що вона поліпшить супутникове зондування, дозволить виявляти об’єкти поза прямою лінією видимості (так звана “примарна” візуалізація), а також потенційно підсилить протидію стелс-технологіям, спрямованим на зниження помітності військової техніки у радіолокаційному, інфрачервоному та інших діапазонах (концепція “квантового радара”).

Разом із тим, поруч із своїми перевагами, квантові сенсори можуть створити нові [виклики](#). Це стосується насамперед стеження і проникнення в приватний простір, адже квантові сенсори потенційно можуть “бачити” крізь одяг, будівлі, породу та інші матеріали значно краще, ніж нинішні технології. Окремий вектор ризику – квантові магнітні сенсори: зловмисники можуть потенційно використовувати їх для перехоплення сигналів near-field communication (NFC) на відстані, наприклад, щоб отримати платіжну інформацію з банківських карток або смартфонів.

Та навіть у випадку легітимного збору даних за допомогою квантових сенсорів виникають виклики щодо безпеки й збереження цих даних, а також щодо інформування осіб про збір даних. Адже зібрані дані можуть бути настільки складними, що особам важко буде зрозуміти, що саме збирається, як це буде використано та які наслідки матиме використання – і це підриває класичну модель “інформованої згоди”.

Щоб ці ризики не стали “платою за прогрес”, потрібне випереджальне врядування: ще до масового впровадження квантових сенсорів варто переглянути правила, які регулюють нагляд і обробку персональних даних, та чітко визначити межі допустимого використання нових квантових інструментів. Паралельно квантові сенсорні системи мають розроблятися за принципом *privacy-by-design* (мінімізація збору даних, контроль доступу, безпечне зберігання), а застосування у чутливих сферах – супроводжуватися прозорістю й зрозумілими для людей процедурами згоди.

## Квантові обчислення і пошук відповіді на найважливіше питання Всесвіту

7,5 МІЛЬЙОНІВ РОКІВ – саме стільки часу знадобилося суперкомп'ютеру Deep Thought, щоб знайти відповідь на “найважливіше питання Життя, Всесвіту і Всього” у романі Адамса "Путівник по Галактиці для космотуристів". І суперкомп'ютер дав відповідь, яка збила всіх з пантелику: “42”.

Коли творці суперкомп'ютера отримали такий результат, перед ними постала проблема: можливо, “42” – це і відповідь на “найважливіше питання Життя, Всесвіту і Всього”, але ж як звучить це найважливіше питання? Deep Thought виявився безсилий. Для того, щоб дізнатися правильне питання, потрібен був новий, ще потужніший комп'ютер, і ще більше часу...

Історія Адамса, бодай жартівлива, метафорично висвітлює реальну проблему, з якою обчислювальні машини стикаються сьогодні. Класичні комп'ютери можуть відповідати на багато питань – але лише на ті, для яких в них достатньо часу, щоб знайти відповідь. Якщо ж питання надто складне і потребує перевірки незліченної кількості варіантів, класичні комп'ютери пасуть задніх. Для таких операцій потрібні потужніші обчислювальні машини.

Розглянемо конкретний приклад. Багато критично важливої інформації в світі – державні таємниці, військові секрети, банківські дані, медичні записи людей, особиста кореспонденція – захищена сучасним криптографічним шифруванням. Щоб зламати шифрування "в лоб" (перевіривши всі можливі комбінації), залежно від типу шифрування, класичному комп'ютеру [знадобиться](#) тисячі чи навіть мільярди років обчислень.

Та ця ситуація кардинально змінюється з появою квантових технологій.

Завдяки своїм унікальним властивостям – суперпозиції та заплутаності – вони можуть опрацьовувати багато можливих станів системи в одному обчислювальному процесі, а не послідовно, як це роблять звичні нам комп'ютери. Якщо класичний комп'ютер працює з бітами (кожен біт – це або 0, або 1), то [квантовий](#) комп'ютер працює з кубітами – квантовими бітами, які завдяки суперпозиції можуть бути в комбінації станів 0 і 1. Більше того, квантова заплутаність дозволяє кубітам взаємодіяти між собою: коли кубіти заплутані, стан одного кубіта стає тісно пов'язаним зі станом іншого. Унікальні властивості суперпозиції та заплутаності дозволяють квантовим комп'ютерам вирішувати певні складні задачі, які є важкими або навіть нерозв'язними для класичних комп'ютерів. Те, на що класичним комп'ютерам потрібно тисячі років, квантові комп'ютери можуть зробити за години, хвилини чи навіть [секунди](#). Вони розв'язуватимуть завдання, на які класичні комп'ютери просто не спроможні відповісти. Квантові комп'ютери не обов'язково

знайдуть “найважливіше питання Життя, Всесвіту і Всього”, але зможуть розв'язувати запити зі швидкістю, яка змінить архітектуру нашого цифрового світу.

Важливий нюанс: коли ми говоримо про “квантові обчислення”, то повинні розуміти, що йдеться не про один конкретний квантовий комп'ютер. Залежно від типу і призначення, [розрізняють](#):

- Квантові емулятори (Quantum emulators) – коли квантові алгоритми запускають на звичайних комп'ютерах, щоб протестувати ідею без справжнього квантового заліза (але це швидко впирається в обмеження).
- Квантові анелери (Quantum annealers) – спеціалізовані пристрої, які добре розв'язують вузький клас задач оптимізації, але не є “універсальними”.
- Квантові симулятори (Quantum simulators) – також спеціалізовані установки для моделювання конкретних квантових процесів у природі (корисні, наприклад, у хімії та матеріалознавстві).
- Універсальні квантові комп'ютери загального призначення (Universal quantum computers) – ті, що виконують обчислення через квантові операції (гейти) і теоретично можуть запускати будь-які квантові алгоритми.

Якщо говорити про виклики, експерти [азначають](#), що завдяки новим квантовим алгоритмам (як-от [алгоритм Шора](#)) квантові комп'ютери вже за 5-10 років стануть достатньо потужними, щоб зламати класичні системи шифрування даних. Це може поставити під загрозу державні таємниці, військову інформацію, фінансові дані та приватні деталі мільйонів чи навіть мільярдів людей. Для держави, яка веде боротьбу за своє існування в умовах гібридної війни, – це критична загроза, до якої потрібно бути готовими.

Але це також і можливість. Крім того, що квантові комп'ютери можуть зламати класичне шифрування, вони також можуть допомогти створити безпечніші моделі захисту даних, які будуть не по зубах зловмисникам (про це детальніше в наступному розділі). Вони також можуть прискорити розробку ліків, оптимізувати енергомережі, змінити фінансову індустрію і багато іншого.

У відповідь на прийдешні загрози держави вже почали будувати правові та стандартні рамки переходу до постквантового захисту: американський NIST [фіналізував](#) стандарти постквантової криптографії, Єврокомісія [рекомендувала](#) країнам розробити узгоджені національні дорожні карти та опублікувала спільну дорожню карту переходу на постквантову криптографію, а британський NCSC [визначив](#) етапи переходу на нові системи безпеки до 2035 року.

Для держави це означає не чекати на “квантовий апокаліпсис”, а діяти зараз: закріпити вимоги криптостійкості в регулюванні критичної

інфраструктури та держсектору, запровадити обов'язкову інвентаризацію криптографії в системах і продуктах, вимоги crypto-agility у держзакупівлях, і поетапний перехід на постквантові або гібридні схеми для даних з довгим строком секретності (бо їх можуть перехопити вже сьогодні і розшифрувати згодом, коли технічні можливості квантових комп'ютерів це дозволятимуть).

## Квантова комунікація як місток для квантового світу

Квантова комунікація [використовує](#) квантові властивості частинок, щоб кодувати й передавати інформацію. Її ключова ідея – становлення квантових мереж, які могли б з'єднувати між собою віддалені квантові сенсори та квантові обчислювальні пристрої і забезпечувати обмін даними між ними.

Один із найбільш перспективних сценаріїв – розподілене квантове сенсування: мережа взаємопов'язаних сенсорів, які діляться заплутаними (entangled) квантовими станами, може робити вимірювання точніше й ефективніше, ніж окремий сенсор. Аналогічно, квантові мережі потенційно підтримують розподілені квантові обчислення, коли кілька квантових процесорів працюють разом над задачами, які “не під силу” одному пристрою.

Найвідоміша практична “вітрина” квантової комунікації сьогодні – квантовий розподіл ключів (QKD, quantum key distribution). Сучасна криптографія спирається на класичні біти як для передачі секретних ключів, так і для обміну зашифрованими даними, тоді як QKD формує секретні ключі, закодовані в кубітах, і передає їх квантовою мережею, щоб посилити безпеку. На відміну від “класичного” підходу, де стійкість шифрування ґрунтується на складності математичних задач, QKD прагне спиратися на фізичні закони: кубіти дуже чутливі до спостереження, і будь-яка спроба перехоплення руйнує квантовий стан (декогеренція) та створює помітні помилки. Отже, користувач може виявити спробу перехоплення, а дані, які намагалися вкрати чи підслухати, стають непридатними для використання.

Коли ми говоримо про технічні аспекти безпеки у контексті квантових технологій, важливо не плутати терміни, які звучать схоже, але означають різні речі. Це стосується насамперед квантової криптографії (quantum cryptography) і постквантової криптографії (post-quantum cryptography, PQC).

Так, квантова криптографія (quantum cryptography) [використовує](#) властивості квантової фізики для забезпечення нових протоколів і стандартів безпеки. Найвідоміший її приклад – вищезгаданий квантовий розподіл ключів (quantum key distribution, QKD).

Та квантову криптографію (quantum cryptography) слід [відрізнити](#) від постквантової криптографії (post-quantum cryptography, PQC). Остання

стосується розробки криптографічних рішень, які мають бути стійкими до потенційних атак квантових комп'ютерів і можуть працювати на сучасних (неквантових) пристроях (сервери, телефони, маршрутизатори). Відповідно, постквантове шифрування не потребує квантового обладнання – це, по суті, оновлення криптографії в нашому звичному цифровому світі. І ця опція є більш реалістичною для впровадження у короткостроковій перспективі. Про неї детальніше розповімо далі у розділі “Постквантова криптографія як базовий стандарт захисту даних у квантову епоху”.

Якщо ж говорити про впровадження і масову комерціалізацію саме квантового розподілу ключів (quantum key distribution, QKD) як елемента квантової криптографії (quantum cryptography), до цього ще далеко: квантові комунікаційні мережі мають подолати інженерні та “польові” бар'єри розгортання. QKD вже тестували у волокні, радіочастотному спектрі та через супутникові ретрансляції, але кожен канал має свої обмеження; зокрема, практичні реалізації часто обмежувалися відстанями близько 100 км, а сценарії “космос–земля” давали змішані результати. Тому паралельно розробляють квантові повторювачі (quantum repeaters) – проміжні вузли мережі, які мають подовжувати дальність передачі квантової інформації. Попри ці виклики, пілотні QKD-мережі вже створювали й випробовували у Великій Британії, Нідерландах, США та Китаї – як ранній сигнал того, що напрям виходить із лабораторій у реальну інфраструктуру.

Однією із [ключових](#) проблем, пов'язаних із запровадженням нових стандартів криптографії, є тривалість переходу на них. Це займає роки й навіть десятиліття. Причина не в тому, що “потрібно просто оновити програму”, а в масштабі: криптографія вшита буквально всюди – у веб-з'єднання, месенджери, банківські картки, VPN, хмари, урядові мережі, підписи документів, блокчейн тощо. Тому заміна алгоритмів означає ланцюжок змін у протоколах, сертифікатах, обладнанні, вимогах до сумісності, закупівлях і навичках людей, а широке впровадження нових систем може тривати десятки років.

Тому починати підготовку і розробляти дорожню карту переходу на нові стандарти треба вже зараз, щоб не довелося латати діри кібербезпеки під час кризи.

## **Квантова архітектура Європейського Союзу: побудова цифрового суверенітету**

За останні роки квантові технології в Європейському Союзі перестали бути нішевою темою для фізиків і стали частиною широкої політики цифрового суверенітету, економічної безпеки та технологічної конкурентоспроможності. Єврокомісія [прогнозує](#), що до 2040 року глобальний сектор квантових технологій може перевищити €155 млрд і створити тисячі висококваліфікованих робочих місць у країнах ЄС. Для Брюсселя це сигнал: або Європа очолить другу квантову революцію,

або вона знову опиниться в ролі користувача чужих технологій, намагаючись наздогнати США та Китай у гонці, де швидкість обчислень вимірюється вже не гігагерцями, а станами заплутаності.

Наразі Єврокомісія прямо [описує](#) квант як сферу, де ЄС має наукову силу, але ризикує програти на етапі масштабування та комерціалізації – зокрема через фрагментацію ініціатив між державами-членами й дефіцит приватного капіталу.

Та щоб виправити ситуацію і закріпити за собою роль лідера у сфері розвитку квантових технологій, ЄС реалізовує низку великих програм та інвестицій. Так, за останні п'ять років ЄС і держави-члени разом [вклали](#) понад €11 млрд у квантові технології. При цьому майже €2 млрд припадає на інвестиції на рівні ЄС, а понад €9 млрд – на бюджети держав-членів.

### **Європейська квантова стратегія – закріпити лідерство до 2030 року**

Ключовим документом, що визначає сьогоднішній вектор ЄС у квантовій сфері, є [Квантова стратегія \(Quantum Europe Strategy\)](#), представлена Єврокомісією у липні 2025 року. Її мета – зробити Європейський Союз глобальним лідером у сфері квантових технологій до 2030 року, збудувавши стійку та суверенну квантову екосистему, здатну стимулювати розвиток стартапів, перетворювати наукові прориви на прикладні рішення і зміцнювати наукове лідерство Європи.

Стратегія охоплює **п'ять ключових напрямів**. **Перший** – дослідження та інновації: консолідація ресурсів і компетенцій по всій Європі, щоб зберегти лідерство в квантовій науці й довести його до промислового використання. **Другий** – квантова інфраструктура: розвиток масштабованих, скоординованих хабів для виробництва, проектування й розробки прикладних рішень. **Третій** – зміцнення квантової екосистеми: інвестиції в стартапи та scale-up компанії, захист ланцюгів постачання й промисловий розвиток. **Четвертий** – квантові технології подвійного призначення (космос, безпека й оборона): інтеграція надійних квантових рішень у відповідні стратегії ЄС. **П'ятий** – квантові навички: формування різноманітної та висококласної робочої сили через узгоджені освітні програми й мобільність талантів усередині ЄС.

Серед конкретних запланованих кроків:

- запуск "Ініціативи з досліджень та інновацій квантової Європи" як спільного проєкту ЄС і держав-членів;
- створення Центру квантового проектування та шести пілотних ліній для виробництва квантових чипів (із публічним фінансуванням до €50 млн) для комерціалізації прототипів;

- запуск пілотного проєкту Європейського квантового інтернету;
- розширення мережі кластерів квантових компетенцій і створення Європейської академії квантових навичок у 2026 році;
- розробка дорожньої карти квантових технологій у космосі спільно з Європейським космічним агентством.

Для реалізації стратегії буде створено Вищу консультативну раду з провідних науковців і фахівців у сфері квантових технологій, включно з лауреатами Нобелівської премії. Такі мультистейкхолдерські установи є важливими, адже ані уряди, ані академія поодиноці не впораються з масштабом трансформації – тільки спільними зусиллями можна досягнути позитивного результату.

### **Грядущий Квантовий акт як законодавчий фундамент регулювання квантових технологій в ЄС**

Після стратегії ЄС готує наступний крок – [Квантовий акт ЄС \(Quantum Act\)](#), який Комісія планує представити у другому кварталі 2026 року.

Передбачається, що документ матиме три основні цілі:

- посилити дослідження та інновації;
- масштабувати промислову спроможність, включно з пілотними лініями й дизайн-інфраструктурою;
- зміцнити стійкість ланцюгів постачання й запровадити механізми управління (governance) у квантовій сфері.

Важлива деталь: Квантовий акт ЄС задуманий не як “дублювання” інших правових рамок, а як доповнення до вже наявних великих актів та ініціатив – Акт про чипи (**Chips Act**), Європейське спільне підприємство з високопродуктивних обчислень (**EuroHPC**) та Інфраструктура для забезпечення стійкості, взаємозв'язку та безпеки за допомогою супутників (**IRIS<sup>2</sup>**). Тобто ЄС поступово зшиває квантові технології з мікроелектронікою, суперкомп'ютерами і захищеним зв'язком в одну логіку технологічного суверенітету.

### **Програма “Флагман квантових технологій”**

Щоб зрозуміти нинішню квантову політику ЄС, варто пам'ятати: Брюссель закладав квантовий “фундамент” задовго до Квантової стратегії 2025 року та Квантового Акту 2026. Одним із центральних елементів була програма [“Флагман квантових технологій”](#) (Quantum Technologies Flagship), запущена у 2018-му як масштабна, довгострокова (більше десяти років) ініціатива з очікуваним бюджетом близько €1 млрд.

Мета програми – перевести європейські дослідження про квантові технології у практичну площину і знайти їм промислове/комерційне застосування, а також посилити співпрацю між університетами, індустрією та державним сектором.

Програма фінансує чотири квантові напрями:

- квантові обчислення;
- квантові симуляції;
- квантові комунікації;
- квантові сенсори і метрологія.

Окрім того, фінансування отримують дослідження в галузі фундаментальних наук, що лежать в основі квантових технологій, а також освітні та міжнародні кооперативні заходи в галузі квантових технологій.

У стартовій фазі (2018–2022) програма профінансувала 24 проєкти із загальним бюджетом €152 млн, до яких залучила понад 1 600 дослідників.

Нова фаза програми (що фінансується у межах Horizon Europe) вже триває: її бюджет перевищує €400 млн і охоплює понад двадцять нових проєктів, спрямованих на наближення наукових результатів до промислового використання. Додаткове фінансування здійснюється через програму “Цифрова Європа” (Digital Europe Programme), щоб зміцнити стратегічні цифрові спроможності Союзу. Для формування проєктних пріоритетів було розроблено Стратегічну програму досліджень (Strategic Research Agenda), до формування якої долучилися понад 2 000 європейських експертів з квантових технологій.

Довгострокове бачення програми “Флагман квантових технологій” – створення “квантового інтернету”, де комп'ютери, симулятори й сенсори будуть з'єднані квантовими комунікаційними мережами.

### ***EuroHPC JU: квантові прискорювачі для суперкомп'ютерів***

Паралельний напрям інфраструктурної політики ЄС – розгортання фізичних квантових систем у межах [Європейського спільного підприємства з високопродуктивних обчислень](#) (European High Performance Computing Joint Undertaking, EuroHPC JU). Ідея полягає в тому, щоб інтегрувати квантові комп'ютери (які функціонуватимуть як прискорювачі) із суперкомп'ютерами EuroHPC, створивши так звані “гібридні” електронно-обчислювальні машини, де поєднані сильні сторони квантових і класичних обчислень.

У жовтні 2022 року EuroHPC JU оголосило про вибір шести місць в ЄС для розміщення перших європейських квантових комп'ютерів, які будуть інтегровані в суперкомп'ютери EuroHPC – у Чехії, Німеччині, Іспанії, Франції, Італії та Польщі.

Це був перший крок до розгортання європейської інфраструктури квантових обчислень, яка має бути доступна європейським

користувачам з наукових та промислових кіл через хмару на некомерційній основі. Ця інфраструктура буде призначена для прискорення процесу створення нових знань та пошуку рішень глобальних суспільних викликів. Завдяки своїй величезній обчислювальній потужності вона буде вирішувати складні проблеми моделювання та оптимізації, особливо в галузі розробки матеріалів, відкриття ліків, прогнозування погоди, транспорту та інших реальних проблем, що мають велике значення для промисловості та суспільства.

Перший квантовий комп'ютер, придбаний EuroHPC, був введений в експлуатацію в Познані (Польща) в червні 2025 року. У вересні 2025 року EuroHPC ввів в експлуатацію свій другий квантовий комп'ютер "VLQ" в Оставі (Чехія). Ці події є важливим кроком вперед у розгортанні найсучаснішої європейської інфраструктури квантових обчислень.

### ***EuroQCI: захищені квантові комунікації від Лісабона до Таллінна***

Квантова політика ЄС – це не лише розвиток квантових комп'ютерів. Це також і побудова європейської інфраструктури захищених комунікацій у цифровому просторі із квантовим "шаром" безпеки. Для цього започаткували ініціативу [Європейська інфраструктура квантової комунікації](#) (European Quantum Communication Infrastructure, EuroQCI)

З 2019 до 2021 року всі 27 держав-членів підписали декларацію EuroQCI, погодившись спільно – разом із Єврокомісією та за технічної підтримки Європейського космічного агентства (ESA) – спроектувати й розгорнути цю інфраструктуру.

EuroQCI поєднує два основні елементи інфраструктури: наземний – волоконно-оптичні мережі, що з'єднують стратегічні вузли на національному й транскордонному рівні, та космічний – супутникова складова, інтегрована з IRIS<sup>2</sup>, новою загальноєвропейською системою захищеного зв'язку. Принципова ідея – не замінити наявний інтернет, а додати до теперішньої комунікаційної інфраструктури додатковий рівень захисту на основі законів квантової фізики (передусім квантового розподілу ключів, QKD), таким чином захистивши урядові установи, дата-центри, лікарні, енергомережі та інші критичні системи.

Комісія прямо пов'язує EuroQCI з цифровим суверенітетом ЄС та цілями Digital Decade 2030, розглядаючи його як один із головних стовпів Стратегії кібербезпеки ЄС на наступні десятиліття.

### ***Постквантова криптографія як базовий стандарт захисту даних у квантову епоху***

Окремою віхою квантової політики ЄС є підготовка до моменту, коли квантові обчислення ставитимуть під загрозу класичні криптографічні алгоритми. Єврокомісія прямо [називає](#) квантові обчислення загрозою

для криптографії, яка захищає конфіденційність і автентичність даних, та підкреслює: відповіддю має бути своєчасний, комплексний і скоординований перехід на постквантову криптографію (Post-Quantum Cryptography, PQC).

Перший відчутний крок у цьому було зроблено у квітні 2024 року, коли Комісія опублікувала [Рекомендацію щодо координованої дорожньої карти переходу до PQC](#) (Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography). Документ не зобов'язував, але задав політичний стандарт: держави-члени мають розробити всеохопну стратегію впровадження PQC, із чіткими цілями, віхами і таймлайнами, щоб перехід відбувався синхронно між країнами та їхніми публічними секторами. У рекомендації також прямо закладена ідея гібридного підходу: у перехідний період PQC може поєднуватися з чинними криптографічними методами або з квантовим розподілом ключів (QKD) – тобто з тією технологічною лінією, яку ЄС паралельно розвиває через EuroQCI.

Наступний важливий крок – затвердження у червні 2025 року [Координованої дорожньої карти щодо переходу до постквантової криптографії](#) (Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography). Це вже була не загальна рекомендація, а узгоджена рамка реалізації переходу до постквантової криптографії.

Комісія прямо вказує: усі держави-члени мають розпочати перехід на постквантову криптографію до кінця 2026 року, а захист критичної інфраструктури має бути переведений на постквантову криптографію “якнайшвидше”, але не пізніше кінця 2030 року. Це переводить тему квантових технологій з “чогось далекого у майбутньому” в режим державного планування “вже тут і зараз”: інвентаризація криптографії, план міграції, пріоритизація систем критичної інфраструктури та уніфікація підходів у державному секторі.

Якщо зібрати всі вищезгадані елементи квантової політики ЄС в одну картину, можна побачити, що це не “одна програма”, а ціла зв'язка інструментів і проєктів різних типів:

- **Європейська квантова стратегія (Quantum Europe Strategy, 2025)** задає політичну мету до 2030 року й визначає п'ять пріоритетних стовпів розвитку квантових технологій.
- **Майбутній Квантовий акт ЄС (Quantum Act, 2026)** має закріпити governance, підсилити R&I та “проштовхнути” промислове масштабування і стійкість ланцюгів постачання.
- **Програма “Флагман квантових технологій” (Quantum Technologies Flagship, з 2018)** підтримує довгострокову дослідницько-інноваційну траєкторію, з фокусом на чотири прикладні сфери застосування квантових технологій.

- **EuroHPC** перетворює квантові обчислення на доступну інфраструктуру через гібридні зв'язки з суперкомп'ютерами та розгортання цих систем у кількох країнах.
- **EuroQCI** вибудовує контур квантово-захищених комунікацій із наземним і космічним сегментами.
- **Постквантова криптографія** розробляє стандарти захисту даних у квантову епоху.

## Квантовий “іспит” для України у контексті євроінтеграції

Активний розвиток квантової політики ЄС – це черговий дзвіночок, що квантові технології перестали бути "технологіями майбутнього", а вже сьогодні потребують уваги держави, дослідників та компаній.

Перше, що важливо розуміти: ЄС формує не лише науковий порядок денний, а й інституційний контур – через спільні ініціативи, інфраструктурні проекти та координацію між державами. Це означає, що країнам-кандидатам (які хочуть бути інтегрованими в європейський цифровий та технологічний простір) доведеться поступово підлаштовуватися під європейські підходи: у стандартах, у пріоритетах фінансування, у вимогах до кіберстійкості, а з часом – і в правилах, що стосуються квантових технологій.

Для України, яка рухається шляхом вступу до ЄС, це означає просту річ: або ми допомагаємо розробляти і впроваджувати технічні та правові правила гри щодо квантових технологій уже зараз, або потім будемо дорого і болісно реагувати на квантові інциденти і нашвидкоруч “підганяти” свої системи під готові європейські стандарти.

І тут з'являється важливий практичний інструмент “впливу до вступу”. Національні регулятори можуть брати участь у публічних консультаціях ЄС та надсилати коментарі щодо свого бачення стандартів розвитку квантових технологій. Таким чином можна впливати на те, які саме пріоритети та вимоги закладатимуться в майбутні європейські політики й стандарти, ще до того, як вони стануть “обов'язковою реальністю” для ринку. Наприклад, Єврокомісія відкривала [збір коментарів](#) (call for evidence) для майбутнього EU Quantum Act і прямо запрошувала до участі органи влади, інфраструктурних операторів, бізнес, науку та організації зі стандартизації – тобто тих, хто потім і застосовуватиме практичні правила екосистеми. Окремо Єврокомісія проводить [публічні консультації](#) щодо європейської стандартизації як такої, і це теж канал, через який можна “підсвітити” позицію України або сектора.

Окрім цього, європейська квантова стратегія прямо показує економічну логіку – ЄС хоче, щоб квантова сфера стала індустрією, а не лише академічною темою, і визнає проблему нестачі приватного капіталу в європейських квантових компаніях. ЄС ставить мету суттєво збільшити частку глобального приватного фінансування квантових

технологій. Для України це означає, що якщо ми хочемо, щоб українські стартапи та інженерні команди були “всередині” майбутніх ланцюгів доданої вартості, треба вчасно вбудовуватися в європейські проєкти, партнерства та рамки фінансування – інакше ми залишимося лише споживачами готових рішень.

Українські організації також можуть співпрацювати з європейськими партнерами задля участі у програмах Horizon Europe, Digital Europe Programme та інших, які виділяють кошти на проєкти з розвитку інфраструктури і прикладних цифрових спроможностей, зокрема квантових ініціатив.

Наступний важливий аспект (і, можливо, найпрактичніший для України вже зараз): квантовий порядок денний ЄС безпосередньо зачіпає технічні стандарти кібербезпеки у контексті переходу до постквантової криптографії (PQC). Для України це важливо щонайменше з трьох причин:

- сумісність з європейськими технічними безпековими практиками. Чим ближче ми до спільного цифрового простору Європи, тим частіше українські державні системи, банки, оператори зв'язку, енергетика і оборонні структури мають обмінюватися даними, які повинні бути захищені на рівні очікуваних європейських стандартів постквантової криптографії. Відставання тут означає не тільки вразливість, а й бар'єри для інтеграції.
- тривалість переходу на нові стандарти. Перехід на нову криптографію зазвичай займає роки – і запізнення потім означатиме дорогий “аварійний” перехід.
- безпека даних. Особливо гостро це звучить в умовах війни. Українські дані і комунікації мають “довгий строк цінності”: розвіддані, персональні масиви, реєстри, документообіг, медичні записи, фінансові транзакції. Якщо противник збирає “класично” зашифровані дані сьогодні, він може намагатися дешифрувати їх завтра, коли квантові технології дозволять це зробити (“[harvest now decrypt later](#)”, HNDL) – і саме тому перехід до квантово-стійких механізмів шифрування має бути частиною загальної політики кіберстійкості, а не реакцією “після інциденту”. В цьому сенсі ЄС задає темп, під який Україні раціонально підлаштовуватися, щоб не залишитися з криптографічною спадщиною, яку потім доведеться ламати через коліно у найгірший момент.

Врешті-решт, людський капітал і освіта щодо квантових технологій стають не менш важливими, ніж “залізо”. ЄС у своїй квантовій стратегії окремо виділяє квантові навички як один із центральних напрямів політики. В Україні вже є [приклад](#) освітніх і наукових активностей у цій темі – зокрема, університетські ініціативи й публічні події, присвячені квантовим дослідженням та освіті. Але для євроінтеграційної логіки важливо, щоб це не залишалось набором ізольованих ініціатив. ЄС робить ставку на мережі, кластери й

узгоджені програми підготовки кадрів, і саме в такий формат Україні доведеться “входити”, якщо ми хочемо бути сумісними з європейськими підходами.

Показово, що Україна вже [починає](#) заходити у європейську PQC-практику: у 2026–2028 роках РНБО та Київський авіаційний інститут візьмуть участь у проєкті QARC (Quantum-Resistant Cryptography in Practice), який під егідою [Horizon Europe](#) має тестувати й впроваджувати постквантову криптографію в реальних системах і середовищах.

Але участь в одному проєкті не замінює державної політики: без власних рамок, плану переходу та вимог до критичної інфраструктури Україна ризикує залишитися “пасажиром” у чужій системі, а не повноцінним гравцем із власними правилами.

Таким чином, Україна опиняється на своєрідному роздоріжжі. З одного боку, є формальні можливості для участі у публічних консультаціях та проєктах ЄС, є наукові кадри й перші освітні програми. З іншого – бракує системної державної уваги до квантових технологій: відсутня національна стратегія, регуляторний простір не адаптований до специфіки цієї сфери, а фінансування досліджень залишається фрагментованим. Досвід ЄС – де навіть найбільші країни визнали необхідність координації та спільних інвестицій – показує: поодиноці цей технологічний перехід не виграти. Для України це означає, що починати потрібно вже зараз – з діалогу з партнерами, розробки стандартів і поступової побудови власної квантової компетенції як складової євроінтеграції.

## **Стратегічні орієнтири для України: короткостроковий, середньостроковий та довгостроковий горизонти**

### **Короткострокові цілі (1-2 роки)**

1. Розробка національної стратегії квантових технологій. Україна повинна розробити комплексну національну стратегію, яка визначатиме цілі, інвестиції та структури управління і напрямки розвитку квантових технологій.
2. Дорожня карта і початок міграції до постквантової криптографії (PQC), насамперед це стосується критичної інфраструктури. Варто розпочати аудит всіх систем критичної інфраструктури, які залежать від криптографії, та розробити план переходу до постквантової криптографії. Європейська комісія рекомендує починати цей процес якнайшвидше, оскільки повна міграція займатиме роки.
3. Розгортання освітніх програм з квантових технологій. Розпочати інтеграцію тем з квантових технологій у вищих навчальних закладах, запровадження більшої кількості програм, що готуватимуть фахівців у квантових технологіях, квантовій

криптографії та кібербезпеці.

4. Моніторинг змін і підходів ЄС. Активно стежити за розробкою стандартів у ЄС, готуватися до їх впровадження і надавати свої коментарі.

### **Середньострокові цілі (3-5 років)**

1. Активна участь у європейських дослідницьких проєктах. Подавати заявки на фінансування через Horizon Europe та інші програми для реалізації дослідницьких проєктів у квантовій комунікації, квантових обчисленнях, квантовому сенсингу, квантовій безпеці та інших сферах.
2. Підготовка нормативно-правової бази для регулювання квантових технологій. Розробити законодавство, що регулює розвиток квантових технологій в Україні, з близькою координацією з ЄС. Це може включати вимоги до технічних та процедурних стандартів безпеки, стандарти тестування та сертифікації, вимоги щодо безпеки даних, зібраних квантовими технологіями тощо.
3. Інвестування у дослідницьку інфраструктуру. Встановити дослідницькі центри або лабораторії в акредитованих закладах, спеціалізованих на квантових технологіях. Це не обов'язково повинно включати розробку власного квантового комп'ютера (це дорого), а скоріше розробку експертизи в використанні хмарних квантових сервісів, квантових емуляторів, квантових анелерів, квантових симуляторів.
4. Залучення приватного сектора. Сприяти розвитку українських стартапів у квантовій сфері.

### **Довгострокові цілі (5-10+ років)**

1. Позиціонування як частини європейської екосистеми. До того часу, коли Україна формально вступить до ЄС, вона вже повинна мати встановлені дослідницькі партнерства, технічні спеціалізації та розвинену індустрію у квантовій сфері.
2. Розроблення власної компетентності. Хоча Україна не обов'язково розроблятиме власні квантові комп'ютери, вона могла б розвивати глибоку компетентність у специфічних областях, таких як квантова криптографія чи квантові сенсори, і визначати потенціал їхнього застосування у сфері безпеки й оборони.
3. Інноваційне лідерство у квантовій безпеці. Позиціонувати Україну як глобального лідера у квантовій кібербезпеці та постквантовій криптографії як площини, де Україна має сильну мотивацію та спеціалізацію завдяки своїй історії боротьби з кіберзагрозами.

Водночас як у романі Адамса вже нам потрібні не лише якісні технічні рішення, а мудрість, аби ставити правильні запитання. Які саме квантові технології нам треба пріоритетно розвивати? Які нормативно-правові рамки потрібно оновити чи встановити? Як

захистити себе від можливих загроз? Як скористатися перевагами другої квантової революції? Як позиціонувати Україну в цій новій системі координат? Ці запитання мають лунати в залах парламенту, у корпоративних офісах, у науково-дослідницьких установах вже сьогодні, а не коли друга квантова революція докорінно змінить світ.

*Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного фонду «Відродження» в рамках спільної ініціативи «Вступаємо в ЄС разом». Матеріал представляє позицію авторів і не обов'язково відображає позицію Європейського Союзу чи Міжнародного фонду «Відродження».*

*Міжнародний фонд «Відродження» – одна з найбільших благодійних фондаций в Україні, що з 1990-го року допомагає розвивати в Україні Відкрите Суспільство на основі цінностей свободи, поваги прав людини і демократії. За час своєї діяльності Фонд підтримав понад 20 тисяч проектів на суму понад 365 мільйонів доларів США.*

*Сайт: [www.irf.ua](http://www.irf.ua)*

*Facebook: [www.fb.com/irf.ukraine](http://www.fb.com/irf.ukraine)*

*Європейський Союз – це економічний і політичний союз 27 європейських країн. Він заснований на цінностях поваги до людської гідності, свободи, демократії, рівності, верховенства права та поваги до прав людини, зокрема прав осіб, що належать до меншин. ЄС діє на глобальному рівні для сприяння сталому розвитку суспільств, довкілля та економік, щоб кожен міг отримати з цього користь.*