ФІНАНСИ. БАНКІВСЬКА СПРАВА ТА СТРАХУВАННЯ

DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-99-107
УДК 336.71:004
JEL Classification: G21

Яніна Василівна Белінська
доктор економічних наук, професор,
професор кафедри економічної політики маркетингу та бізнес-аналітики
Державний податковий університет (Ірпінь, Україна)
E-mail: 071065@ukr.net. **ORCID**: https://orcid.org/0000-0002-9685-0434
Scopus Author ID: 36068854900

Юлія Михайлівна Коваленко
доктор економічних наук, професор,
в.о. завідувача кафедри фінансів, обліку та оподаткування
Державний університет "Київський авіаційний інститут» (Київ, Україна)
E-mail: kovalenko0202@ukr.net. **ORCID**: https://orcid.org/0000-0002-5678-3185
ResearcherID: H-4742-2018

ВПЛИВ КВАНТОВИХ ОБЧИСЛЕНЬ НА СТІЙКІСТЬ БАНКІВСЬКОГО СЕКТОРУ В УМОВАХ НАДЗВИЧАЙНИХ ПОДІЙ

Анотація*. У сучасному світі фінансовий сектор перебуває під впливом великого спектра надзвичайних подій, від ринкових шоків і геополітичної напруженості до пандемій та кібератак. Останнім часом особливу увагу привертає вплив технологій ШІ та квантових обчислень на фінансовий сектор. Стаття присвячена аналізу можливих сфер впливу квантових технологій на фінансову сферу загалом та стійкість фінансових установ зокрема. Проаналізовані загрози й можливості квантових обчислень, зокрема потенціал покращання оцінки фінансових ризиків, у тому числі підвищення точності стрес-тестування, управління портфелями та ціноутворення деривативів, а також потенціал квантового машинного навчання для виявлення шахрайства. Серед викликів виділено загрозу зламу існуючих криптографічних алгоритмів, що захищають конфіденційні дані, у вигляді атак типу «збережи зараз, розшифруй пізніше», що створює виклики для онлайн банкінгу, платіжних операцій та корпоративних комунікацій.*

Ключові слова: *надзвичайні події; банки; квантові обчислення; операційна стійкість; фінансовий сектор; кібербезпека; управління ризиками; машинне навчання; ШІ.*
Рис.: 2. Табл.: 1. Бібл.: 8.

Постановка проблеми. У сучасному світі фінансовий сектор економіки стикається зі зростаючою кількістю надзвичайних подій. Ці події охоплюють широкий спектр непередбачуваних і руйнівних явищ, включаючи фінансові ринкові шоки, природні катаклізми, геополітичну напруженість, пандемії та кібератаки. Вони відрізняються за своєю природою, але мають значний негативний вплив на фінансові компанії. Останнім часом поширення технологій ШІ та квантових обчислень можна прирівняти до статусу надзвичайної події, вплив якої на стабільність фінансової системи дотепер не достатньо вивчений. Разом з очікуваним «квадратичним» прискоренням обчислень за допомогою квантових комп'ютерів, що спроможне кардинально підвищити точність оцінок ризиків, прогнозів та прийняття рішень, зростає вірогідність зламу схем шифрування даних, що є суттєвою загрозою фінансовій стабільності банків і потребує розробки стратегії захисту від неї вже на поточному етапі.

Аналіз останніх досліджень та публікацій. Проблемою впливу надзвичайних подій на стан банківської системи та заходами протидії їм фінансових установ займаються багато науковців. Системний підхід до становлення і розвитку банківської

системи України свого часу розвинув О. Дзюблюк у своїй ґрунтовній праці [1]. Питаннями банківського нагляду займається В. Міщенко та С. Науменкова [2]. Особливості функціонування банківської системи під час війни в Україні дослідили Ю. Заволока, О. Кузьменко, В. Кузьменко [3], регулярно аналізують фахівці НБУ [4].

У сучасному глобалізованому світі фінансові мережі настільки взаємопов'язані, що надзвичайно важко точно оцінити довгостроковий вплив потенційних фінансових обвалів, таких як стрибки цін на активи. Р. Орус та інші [5] визначили, що математична проблема прогнозування наслідків руйнівної події не може бути розв'язана класичними алгоритмами навіть для невеликої мережі, що складається з 20-30 фінансових установ і організацій. Це зайняло б більше часу, ніж вік всесвіту. У цьому випадку А. Абусалах та інші [6] вважають більш ефективним використання квантового підходу до аналізу системного ризику у фінансових мережах. У своїй роботі вони продемонстрували, як методи квантових обчислень можуть досить точно «оцифрувати» стійкість фінансових систем. Квантові методи управління ризиками розвиваються швидкими темпами, але залежать від швидкості розширення можливостей квантових комп'ютерів [7]. Науковці очікують, що подальші дослідження дозволять розробити нові квантові алгоритми прогнозування несприятливих подій [8]. Збільшення частоти появи та складності прояву цих подій підкреслює потребу в підвищенні операційної стійкості банківського сектору.

Посилюється увага науковців до технологій криптографії, значення яких істотно зросло в епоху цифровізації для захисту даних клієнтів, проте їхній вплив на стабільність фінансової системи дотепер недостатньо вивчений. Ван Метер та інші виявили, що сучасні криптографія і схеми шифрування, що захищають дані споживачів фінансових послуг та звітність банків, базуються на математичних проблемах, які не можуть бути розв'язані за допомогою класичних комп'ютерів, але потенційно можуть бути вирішені квантовим комп’ютером [9]. Загроза зламу схем шифрування вимагає розробки стратегії її запобігання вже на поточному етапі, адже зловмисники можуть використовувати можливість перехоплювати та зберігати дані сьогодні з наміром розшифрувати їх у майбутньому, коли квантові комп’ютери стануть широко доступними («harvest now, decrypt later» (HNDL) attacks) [10].

Виділення недосліджених частин загальної потреби. Незважаючи на активне дослідження і розробку алгоритмів дій банків в умовах надзвичайних подій, потужний трансформаційний вплив інформаційних та квантових технологій вимагає підвищеної уваги до потенціалу їхніх позитивних і негативних проявів у фінансовій сфері. За підвищеної уваги до впливу надзвичайних подій, насамперед інформаційних та квантових технологій на фінансовий сектор, їх швидкий прогрес зумовлює постійну зміну технологій, що відкриває простір для досліджень.

Мета статті – дослідити позитивний вплив і ризики поширення квантових технологій в умовах зростаючої кількості надзвичайних подій на стійкість банківського сектору, включаючи загрози для сучасної криптографії та конфіденційності даних.

Виклад основного матеріалу. Надзвичайні події можуть мати різноманітний характер і кожна з яких створює унікальні виклики для банківського сектору. Розуміння специфіки цих викликів є першим кроком до розробки ефективних стратегій підтримки стійкості банків в поточному та в довгостроковому періоді.

Традиційно до надзвичайних подій належать такі (табл. 1).

Таблиця 1

Види і характеристики надзвичайних подій

Вид	Характеристика наслідків	Приклад
Фінансові кризи	Системні збої, що призводять до падіння цін на активи, масових дефолтів та нестачі ліквідності, спричиняючи паніку серед вкладників	2008-2009 рр. – фундаментальні проблеми ліквідності, різке скорочення кредитування
	Швидкий та значний відтік депозитів, посилений технологіями та соціальними медіа, слабкими місцями бізнес-моделей, недоліками управління процентними та ризиками ліквідності, а також незбалансованою структурою активів.	2023 рік – Silicon Valley Bank (SVB), Signature Bank та First Republic Bank
Природні катаклізми	Значні економічні збитки та результативні збої в діяльності глобальних фінансових установ, що мають системний характер. Кризові явища поширюються через глобальні банківські мережі, включаючи канали зниження транскордонного кредитування, тиск на якість активів, адекватність капіталу та ризик ліквідності	Землетруси, урагани та повені
Пандемії	Стрес та волатильність на фінансових ринках і в економіці. Зростання кредитних ризиків через неспроможність позичальників обслуговувати борги, процентних ризиків, пов'язаних зі зменшенням чистої процентної маржі. Зростання депозитів внаслідок панічних настроїв і підвищеної потреби у заощадженнях та відносного надлишку ліквідності через експансіоністську політику. Перехід до цифрового банкінгу та віддаленої роботи, що трансформує банківське обслуговування та інфраструктуру.	Криза COVID-19
Геополітичні ризики	Складна мережа викликів, які можуть негативно вплинути на фінансові ринки, перешкоджати транскордонним операціям та підірвати довіру інвесторів через канали підвищеного кредитного ризику, зменшити інвестиційні можливості та змінити регулювання. Оскільки банки працюють у глобальному середовищі вони залежать від стабільності та безпеки країн, у яких вони працюють.	Арабська весна, війна в Україні, напруженість на Близькому Сході та потенційні торговельні суперечки США і Китаєм
Кіберзагрози	Фішингові атаки, що під маскуванням викрадають облікові дані; шкідливе програмне забезпечення (програми-вимагачі), які шифрують дані та вимагають викуп; атаки типу «відмова в обслуговуванні», які перевантажують системи банку, блокуючи доступ користувачів до послуг. Це шкодить репутації, веде до регуляторних штрафів, втрати довіру клієнтів.	У 2023 р. обсяг кібератак на банківську галузь зріс на 125 % порівняно з 2022 р., що засвідчує її статус основної мішені для кіберзлочинців

***Джерело**: складено авторами.*

Для ефективного реагування банків на надзвичайні події напрацьований комплексний підхід, що ґрунтується на концепціях операційної стійкості банків та безперервності бізнесу. Операційна стійкість банку визначається як здатність проводити критично важливі операції під час надзвичайних збоїв, таких як пандемії, кіберінциденти, технологічні збої або стихійні лиха. Вона передбачає не лише здатність банку витримувати кризові подій та відновлюватися після них, а і проактивно готуватися до кризових епізодів, адаптуватися до негативних тенденцій, вчасно реагувати на події та вчитися на помилках. Безперервність бізнесу (ББ) є складовою операційної стійкості банків, що базується на алгоритмі планування дій під час

кризових збоїв і забезпеченні безперервності виконання критично важливих функцій організації під час та після надзвичайної події [11]. Загалом планування безперервності бізнесу має тактичний характер, визначаючи, яким чином організація продовжуватиме функціонувати в умовах кризи. Відновлення після кризових подій (катастроф) (ВПК) є ще одним важливим компонентом операційної стійкості банків, що охоплює відновлення критичних систем, додатків та даних після кризового інциденту. ВПК зосереджується на короткостроковому відновленні, тоді як ББ охоплює довгострокове відновлення. У межах удосконалення підходу до безперервності бізнесу, банки інтегрували геополітичні ризики у свої системи ризик менеджменту й посилили заходи з кібербезпеки. Це покращило надійність практик підтримки функціонування банків у надзвичайних умовах для збереження їхньої стійкості.

У сучасних умовах фінансової цифровізації поширення інформаційних технологій ламає усталену схему дій банку в надзвичайних ситуаціях через надвисоку швидкість поширення і завеликий обсяг інформації, а також не традиційність проявів і специфіку впливу цифрових інновацій. Зокрема, впровадження блокчейну в банківській справі через його складність стикається з викликами щодо необхідності спеціалізованих знань та технічної експертизи, а також проблемами масштабованості та труднощів взаємодії з існуючою фінансовою інфраструктурою. Так, унаслідок посилення залежності від інформаційних технологій вразливість до кризових подій у мобільному банкінгу зросла на 42 % у 2023 році, а 58 % фінансових організацій повідомили про загрозу безпеки хмарних середовищ, при цьому інциденти, пов'язані з API, зросли на 47 % [11].

Специфіка викликів з боку цифрових, інформаційних, а останнім часом і квантових технологій вимагає особливих методів реагування. Для цього банки дедалі частіше використовують хмарні технології, що стали ключовим рушієм розвитку операційної ефективності в банківському секторі. Використання хмарних рішень для відновлення після катастроф (DR) має значні переваги порівняно з традиційними підходами, включаючи низькі початкові витрати, швидку масштабованість, автоматизовані процеси перемикання між процесами, а також скорочення цільових показників часу відновлення (RTO) та цільових показників точки відновлення (RPO) [12]. Хмарні провайдери пропонують вбудовані інструменти оркестрації на платформі, що автоматизує процеси аварійного перемикання та відновлення роботи, спрощуючи робочі процеси та зменшуючи кількість ручних помилок. Використання хмарних технологій покращує процес ухвалення рішень, продуктивність антикризових дій і зміцнює кібербезпеку, дозволяючи банкам використовувати веб- та мобільні продукти для управління транзакціями та коригувати/оптимізувати розміщення ресурсів під час пікових навантажень на установу без надмірних інвестицій в інфраструктуру.

Попри вагомі переваги, впровадження хмарних технологій у банківській сфері породжує низку викликів, таких як необхідність відповідності регуляторним вимогам та їх оновленням, труднощі інтеграції інноваційних технологій із застарілими системами, контроль за постачальниками та необхідність розробки комплексної стратегії хмарної безпеки.

Останнім часом за силою непередбачуваності як позитивних, так і негативних проявів хмарні технології поступаються місцем квантовим обчисленням, які хоча все ще перебувають на експериментальній стадії, мають потенціал глибокого трансформаційного впливу на фінансову систему.

Використання таких базових понять квантової теорії, як суперпозиція та заплутаність дозволяють квантовому комп'ютеру (КК) виконувати обчислення радикально новими способами порівняно з класичними комп'ютерами. Квантова перевага – це нова віха використання КК для розв'язання проблем, які жоден класичний комп'ютер не може розв'язати в реалістичні терміни. Хоча деякі дослідницькі групи стверджують, що вони вже досягли квантової переваги, багато експертів вважають, що практичний квантовий комп'ютер (КК) з'явиться ще через багато років, а деякі вважають, що він може ніколи не бути реалізований [13]. На основі опитування провідних світових експертів у галузі квантових обчислень Моска та Піані [7] оцінюють, що криптографічно релевантний КК може з'явитися протягом п'яти-тридцяти років.

Однією зі сфер, де квантові технології можуть бути корисними для підвищення операційної стійкості банків, є запобігання надзвичайним подіям завдяки кардинальному покращанню оцінки фінансових ризиків і проведенню більш точних стрес-тестів. Сфера застосування квантових обчислень включає процеси від симуляцій ризиків до оцінки системного ризику. У деяких випадках квантові комп'ютери здатні виконувати завдання, які недосяжні для традиційних комп'ютерів, що може змінити спосіб моделювання фінансових подій та пом'якшення фінансових ризиків. Очікується, що квантові алгоритми управління ризиками забезпечать квадратичне прискорення процесу ухвалення рішень у порівнянні з класичними алгоритмами.

Використання потенціалу виконання складних квантових обчислень із безпрецедентною швидкістю дозволяє покращити управління ризиками, Так, зі збільшенням розміру вхідних даних для проблеми, найкращі класичні алгоритми вимагають експоненціально зростаючої кількості кроків, тоді як квантові алгоритми, розроблені для оцінки ризиків у портфелях фінансових активів потребують лінійного збільшення кількості кроків. Так, Еггер та інші оцінили, що квантовий комп'ютер міг би виконати розрахунки VaR для портфеля з 1 мільйона активів за 30 хвилин [14]. Це залежить від кількох факторів, таких як кількість сценаріїв, складність портфеля, обрана методологія VaR та ефективність реалізованих алгоритмів. Натомість за використання традиційних обчислень ці розрахунки можуть зайняти декілька годин.

Так само алгоритми квантових обчислень можуть бути використані для прискорення ціноутворення, наприклад, фінансових деривативів. Фахівці порівняли квантові, класичні та напівквантові схеми і виявили, що квантові методи дозволяють квадратично прискорити ці процеси та вимагають менше ресурсів, ніж наявні методи [15]. Завдяки безпрецедентній точності та швидкості квантові обчислення можуть використовуватися у сфері інвестиційної діяльності та управління портфелем активів. Більш точні результати симуляцій та аналізу можуть суттєво покращити інвестиційні стратегії. Очікується, що в майбутньому штучний інтелект (ШІ) та машинне навчання знайдуть широке застосування в механізмах виявлення шахрайства, платежів та розрахунків, а також макромоделювання.

Таким чином, у довгостроковому періоді наслідки квантових обчислень будуть трансформаційними для фінансової сфери. Хоча багато дослідників концентруються «лише» на прискореній роботі квантового комп'ютера, його важливим наслідком може бути виконання таких обчислювальних завдань, які сьогодні ще нездійсненні за допомогою класичних комп'ютерів. «Квантова» революція в обробці даних та алгоритмічних розрахунках спроможна забезпечити стійкість фінансової

системи завдяки можливості прораховувати велику кількість варіантів розвитку подій та підвищенню точності та швидкості оцінок ризиків, оптимізації управління портфелями, вдосконаленню макроаналізу та виявленню шахрайства.

З другого боку, квантові комп'ютери розглядаються як серйозна загроза фінансовій стабільності через їхню здатність зламувати деякі з найбільш широко використовуваних криптографічних алгоритмів, таких як AES, RSA та ECC [9]. Якщо це стане масовим явищем, зловмисники, включаючи ворожі держави або злочинні підприємства, можуть використовувати квантові комп'ютери для атаки на банки та інші об'єкти критичної інфраструктури з метою крадіжки даних, заподіяння репутаційної шкоди та руйнації конфіденційності клієнтів.

Для зниження цих потенційних ризиків Центральні банки та регулятори вже розпочали розробку та вжиття заходів [10]. Національний інститут стандартів і технологій (NIST) розробляє постквантові криптографічні алгоритми, а такі органи, як G7 Cyber Expert Group, моніторять розвиток квантових обчислень та заохочують співпрацю між зацікавленими сторонами. Банк міжнародних розрахунків (BIS) розпочав Проєкт Leap для вивчення сфери квантових обчислень з позиції фінансової безпеки. Загалом банкам рекомендується вже на поточному етапі зайнятися розробкою переліку активів та сфер використання криптографії для адаптації до майбутніх змін [8].

Таким чином, хоча нині безпосередні переваги використання квантових обчислень у системі заходів протидії банків надзвичайним подіям є досить скромними, їхній потенціал фундаментальних трансформацій обчислювальних можливостей фінансових установ, віддзеркалює широкомасштабність впливу технологічної еволюції на сучасні фінансові стратегії.

Висновки та пропозиції. На сучасному етапі фінансові установи стикаються з широким спектром надзвичайних подій, від фінансових криз до кібератак, що вимагає відповідних безпекових заходів. Цифровізація фінансових послуг, зокрема розвиток мобільного банкінгу та використання хмарних технологій, трансформують традиційні підходи до управління ризиками та алгоритму відновлення після катастроф. Хоча хмарні рішення надають значні переваги у швидкості, масштабованості та автоматизації дій, вони породжують і нові виклики. У цьому контексті квантові обчислення є подвійним викликом: вони загрожують зламом сучасної криптографії та конфіденційних даних через атаки типу «збережи зараз, розшифруй пізніше» та водночас пропонують безпрецедентні можливості щодо покращання оцінки фінансових ризиків, стрес-тестування, управління інвестиційними портфелями та виявлення шахрайства за допомогою квантових обчислень, що вирішують задачі, недоступні для класичних комп'ютерів.

У відповідь на ці виклики, фінансовий сектор, зокрема центральні банки та регулятори, активно впроваджують заходи для використання квантово-стійкої (постквантової) криптографії. Це вимагає значних інвестицій та адаптації регуляторних рамок, і банківська система має бути готовою до цих фундаментальних змін.

Список використаних джерел

1. Банківська система України: становлення і розвиток в умовах глобалізації економічних процесів : монографія / за ред. О. В. Дзюблюка. – Тернопіль : Вектор, 2012. – 462 с.

2. Міщенко В. І. Банківський нагляд : підручник / В. І. Міщенко, С. В. Науменкова. – Київ : Центр наукових досліджень НБУ, 2010. – 497 с.

3. Заволока Ю. Робота банківської системи та валютного ринку в умовах війни [Електронний ресурс] / Ю. Заволока, О. Кузьменко, В. Кузьменко // Економіка та суспільство. – 2023. – Вип. 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-3.

4. Стан фінансового сектору України та заходів НБУ з підтримки його безперебійного функціонування в умовах воєнного стану // Національний банк України. – 2022. – Режим доступу: https://bank.gov.ua/ua/news/all/stan-finansovogo-sektoru-ukrayini-ta-zahodi-nbu-z-pidtrimki-yogo-bezperebiynogo-funktsionuvannya-v-umovah-voyennogo-stanu.

5. Orus R. Forecasting financial crashes with quantum computing / R. Orus, S. Mugel, E. Lizaro // arXiv. – 2019. – 1810.07690.

6. Aboussalah A. M. Quantum computing reduces systemic risk in financial networks / A. M. Aboussalah, C. Chi, C.-G. Lee // Scientific Reports. – 2023. – Vol. 13, no. 3990.

7. Mosca M. Quantum threat timeline report 2023 / M. Mosca, M. Piani. – Global Risk Institute and evolutionQ Inc., 2023.

8. Quantum computing and the financial system: spooky action at a distance? / J. Deodoro, M. Gorbanyov, M. Malaika, T. S. Sedik // IMF Working Papers. – 2021. – No. 2021/071.

9. Van Meter R. Architecture-dependent execution time of Shor's algorithm / R. Van Meter, K. Itoh, T. Ladd // Controllable quantum states: mesoscopic superconductivity and spintronics (MS+S2006). – 2008. – P. 183–188.

10. Cyber risk in central banking / S. Doerr, L. Gambacorta, T. Leach, B. Legros, D. Whyte // BIS Working Papers. – 2022. – No 1039.

11. Quantum computing and the financial system: opportunities and risks [Elecntronuc resource] / R. Auer, A. Dupont, L. Gambacorta, J. S. Park, K. Takahashi, A. Valko // Monetary and Economic Department BIS Papers. – 2024. – No 149. – Pp. 1–33. – Accessed mode: https://www.bis.org/publ/bppdf/bispap149.pdf.

12. Bova F., Goldfarb A., Melko R. Quantum computing is coming. What can it do?/ F. Bova, A. Goldfarb, R. Melko. – Harvard Business Review, July 2021.

13. Dyakonov M. The case against quantum computing [Elecntronuc resource] / M. Dyakonov // IEEE Spectrum. – 2018. – Accessed mode: https://spectrum.ieee.org/the-case-against-quantum-computing.

14. Quantum computing for finance: state-of-the-art and future prospects / D. Egger, C. Gambella, J. Marecek et al. // IEEE Transactions on Quantum Engineering. – 2020. – Vol. 1, no. 3101724.

15. Towards quantum advantage in financial market risk using quantum gradient algorithms / N. Stamatopoulos, G. Mazzola, S. Woerner, W. Zeng // Quantum. – 2022. – Vol. 6. – P. 770.

Reference

1. Dzyublyuk, O. V. (2012). *Bankivska systema Ukrayiny: stanovlennya i rozvytok v umovakh hlobalizatsiyi ekonomichnykh protsesiv [The banking system of Ukraine: formation and development in the context of globalization of economic processes].* Vektor.

2. Mishchenko, V. I., Naumenkova, S. V. (2010). *Bankivskyi nahlyad [Banking supervision]*. Tsentr naukovykh doslidzhen NBU.

3. Zavoloka, Yu., Kuzmenko, O., Kuzmenko, V. (2023). Robota bankivskoi systemy ta valyutnoho rynku v umovakh viyny [Operation of the banking system and the currency market in wartime]. *Ekonomika ta suspilstvo – Economy and Society, 50.* https://doi.org/10.32782/2524-0072/2023-50-3.

4. *Natsionalnyi bank Ukrainy [National Bank of Ukraine]*. (2022). Stan finansovoho sektoru Ukrayiny ta zakhodiv NBU z pidtrymky yoho bezperebiynoho funktsionuvannya v umovakh voyennoho stanu [The state of the financial sector of Ukraine and the measures of the NBU to support its uninterrupted functioning in conditions of martial law]. https://bank.gov.ua/ua/news/all/stan-finansovogo-sektoru-ukrayini-ta-zahodi-nbu-z-pidtrimki-yogo-bezperebiynogo-funktsionuvannya-v-umovah-voyennogo-stanu.

5. Orus, R., Mugel, S., Lizaro, E. (2019). Forecasting financial crashes with quantum computing. *arXiv*. 1810.07690.

6. Aboussalah, A. M., Chi, C., Lee, C.-G. (2023). Quantum computing reduces systemic risk in financial networks. *Scientific Reports, 13*(3990).

7. Mosca, M., Piani, M. (2023). Quantum threat timeline report 2023. *Global Risk Institute and evolutionQ Inc.*

8. Deodoro, J., Gorbanyov, M., Malaika, M., Sedik, T. S. (2021). Quantum computing and the financial system: spooky action at a distance? *IMF Working Papers*. No. 2021/071.

9. Van Meter, R., Itoh, K., Ladd, T. (2008). Architecture-dependent execution time of Shor's algorithm. *Controllable quantum states: mesoscopic superconductivity and spintronics (MS+S2006)* (pp. 183–188).

10. Doerr, S., Gambacorta, L., Leach, T., Legros, B., Whyte, D. (2022). Cyber risk in central banking. *BIS Working Papers*, No 1039.

11. Auer, R., Dupont, A., Gambacorta, L., Park, J. S., Takahashi, K., Valko, A. (2024). Quantum computing and the financial system: opportunities and risks. *Monetary and Economic Department BIS Papers*, No 149, 1–33. https://www.bis.org/publ/bppdf/bispap149.pdf.

12. Bova, F., Goldfarb, A., Melko, R. (July, 2021). *Quantum computing is coming. What can it do?* Harvard Business Review.

13. Dyakonov, M. (2018). The case against quantum computing. *IEEE Spectrum.* https://spectrum.ieee.org/the-case-against-quantum-computing.

14. Egger, D., Gambella, C., Marecek, J. (2020). Quantum computing for finance: state-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering, 1*(3101724).

15. Stamatopoulos, N., Mazzola, G., Woerner, S., Zeng, W. (2022). Towards quantum advantage in financial market risk using quantum gradient algorithms. *Quantum*, *6*, 770.

Отримано 08.06.2025

UDC 336.71:004
JEL Classification: G21

Yanina Belinska

Doctor of Economics, Professor,
Professor of the Department of Economic Policy, Marketing and Business Analytics
State Tax University (Irpin, Ukraine)
E-mail: 071065@ukr.net. **ORCID**: https://orcid.org/0000-0002-9685-0434
Scopus Author ID: 36068854900

Yuliia Kovalenko

Doctor of Economics, Professor, Head of the Department of Finance, Accounting and Taxation
State University "Kyiv Aviation Institute" (Kyiv, Ukraine)
E-mail: kovalenko0202@ukr.net. **ORCID**: https://orcid.org/0000-0002-5678-3185
ResearcherID: H-4742-2018

THE IMPACT OF QUANTUM COMPUTING ON THE STABILITY OF THE BANKING SECTOR IN THE CONDITIONS OF EXTRAORDINARY EVENTS

Abstract*. In the modern world, the financial sector faces a wide range of extraordinary events, from market shocks and geopolitical tensions to pandemics and cyberattacks. These diverse challenges significantly impact banks. Recently, particular attention has been drawn to the influence of artificial intelligence (AI) and quantum computing (QC)*

technologies on the stability of the financial system. This article analyzes the potential areas of impact of quantum technologies on the financial sphere in general and the resilience of financial institutions in particular.It's determined that quantum technologies can simultaneously pose both threats and new opportunities. Specifically, the article analyzes the potential of quantum technologies to break existing cryptographic algorithms that protect the confidential data of financial institutions' clients. This threat is exacerbated by the possibility of "harvest now, decrypt later" attacks, where malicious actors intercept data today with the intention of decrypting it in the future. This presents challenges and threats for online/mobile banking, payment operations, and corporate communications. Among the positive impacts of quantum technologies on banking, the article highlights improved financial risk assessment, particularly enhanced accuracy in stress testing, portfolio management, and derivatives pricing, by solving problems inaccessible to classical computing. The potential of quantum machine learning for fraud detection is also noted. Attention is given to the financial sector's response to these challenges. Initiatives for developing quantum-resistant (post-quantum) cryptography are considered as the primary method for mitigating the risks associated with the proliferation of quantum computing, along with new cryptographic protocols and quantum key distribution as a new opportunity to enhance security. The article emphasizes the responsibility of central banks in forming quantum-readiness strategies, including investments in post-quantum cryptography, expertise development, and the adaptation of regulatory frameworks. The conclusion drawn is that although the immediate benefits of quantum technologies may be modest, their long-term transformative potential for the financial sector is immense.

Keywords: extraordinary events, banks, quantum computing, operational resilience, financial sector, cybersecurity, risk management, machine learning, AI.

Fig.: 2. Table: 1. References: 8.

Бібліографічний опис для цитування:

Белінська Я. В., Коваленко Ю. М. Вплив квантових обчислень на стійкість банківського сектору в умовах надзвичайних подій. *Науковий вісник Полісся*. 2025. № 1(30). С. 99-107. DOI: https://doi.org/10.25140/2410-9576-2025-1(30)99-107.