УДК 004.932:519.676.8:004.5

Фесенко Т.М., к.т.н., доцент
Національний університет
«Полтавська політехніка ім. Юрія Кондратюка»

КВАНТОВО-КЛАСИЧНІ ГІБРИДНІ АЛГОРИТМИ РОЗВ’ЯЗУВАННЯ НЕЛІНІЙНИХ ЗАДАЧ У ВИСОКОПРОДУКТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні електронно-комунікаційні системи оборонного та кібербезпекового призначення функціонують в умовах багатофакторної динамічної невизначеності. При цьому їх формування здійснюється під впливом активних деструктивних дій противника, стохастичних флуктуацій параметрів каналів зв’язку, варіативності топології мереж, а також обмеженості обчислювальних, енергетичних і часових ресурсів. Для таких систем характерними є жорсткі вимоги до латентності обробки даних, гарантованої доступності сервісів та забезпечення криптографічної стійкості в умовах адаптивних атак. Невизначеність має як структурний, так і параметричний характер, що зумовлює необхідність використання формалізованих моделей із врахуванням нелінійної динаміки, стохастичних збурень і часткової спостережуваності станів.

Значна частина прикладних завдань, зокрема захист транспортних мереж, адаптивного розподілу мережевих ресурсів, ідентифікації та прогнозування кіберзагроз, а також синтезу й оптимізації криптографічних протоколів формалізується у вигляді багатокритеріальних нелінійних задач оптимізації або задач керування високої розмірності [1]. Такі постановки часто супроводжуються наявністю обмежень типу реального часу, невипуклих функціоналів якості та складних кореляційних залежностей між параметрами, що суттєво ускладнює застосування традиційних детермінованих або лінійних методів аналізу. У результаті виникає потреба в обчислювальних підходах, здатних ефективно працювати з великими просторами станів і забезпечувати прискорений пошук квазіоптимальних рішень.

У цьому контексті перспективним напрямом є використання квантово-класичних гібридних алгоритмів [2], зокрема варіаційних підходів, які передбачають інтеграцію квантових обчислювальних модулів у контур класичної високопродуктивної інфраструктури. Архітектурно такі рішення реалізуються за принципом розподілу обчислювального навантаження, тоді як класична підсистема здійснює

параметричну оптимізацію, агрегацію результатів, контроль збіжності та інтеграцію з прикладними сервісами.

Застосування гібридних алгоритмів дозволяє поєднати потенційні обчислювальні переваги квантових примітивів, зокрема паралелізм у просторі станів і можливість апроксимації складних нелінійних залежностей із надійністю, масштабованістю, керованістю та відпрацьованими механізмами відмовостійкості класичних платформ. Зазначене створює передумови для підвищення ефективності розв’язання задач криптоаналізу, оптимізації параметрів протоколів постквантового захисту, адаптивного керування трафіком у надщільних мережах та формування прогнозних моделей кіберзагроз в умовах обмеженого часу реагування.

Нехай ***стан інформаційної системи*** спеціальних користувачів описується вектором фазових змінних

$$\mathbf{x} \in \mathrm{X} \subset \mathbb{R}^{n}, \tag{1}$$

компоненти якого відображають ключові параметри функціонування системи а саме, конфігурацію мережевої інфраструктури, поточні режими криптографічних механізмів, характеристики трафіку, рівень завантаження обчислювальних ресурсів, а також індикатори виявлених аномалій або загроз. Така векторна репрезентація дозволяє формалізувати систему як багатовимірний динамічний об’єкт із внутрішніми нелінійними зв’язками та обмеженнями.

Зовнішні збурення, кіберзагрози, навмисні деструктивні впливи та випадкові шумові компоненти описуються вектором параметрів

$$\boldsymbol{\xi} \in \Xi, \tag{2}$$

який моделює стохастичні флуктуації каналів зв’язку, зміну інтенсивності атак, перехідні процеси в мережі та інші фактори невизначеності.

Задача оптимізації функціонування формулюється у вигляді мінімізації нелінійного функціоналу якості:

$$\min_{\mathbf{x}\in \mathrm{X}} J(\mathbf{x}, \boldsymbol{\xi}), \tag{3}$$

де функціонал $J(\cdot)$ відображає багатокритеріальний компроміс між показниками інформаційної безпеки, структурної та функціональної стійкості, часової затримки обробки, пропускної здатності та ресурсної ефективності. Саме це зумовлює доцільність застосування методів глобальної або квазіглобальної оптимізації, у тому числі гібридних квантово-класичних підходів, для забезпечення адаптивного та стійкого функціонування системи в умовах активної протидії.

Квантово-класична гібридна параметризація. У гібридному підході вектор $\mathbf{x}$ параметризується через квантовий стан:

$$|\psi(\boldsymbol{\theta})\rangle = U(\boldsymbol{\theta})\,|\psi_0\rangle \ , \tag{4}$$

де $U(\boldsymbol{\theta})$ – параметризований квантовий оператор,

$\boldsymbol{\theta} \in \square^{\mathrm{n}}$ – вектор варіаційних параметрів,

$|\psi_0$ – початковий стан.

Цільова функція подається у вигляді математичного сподівання спостережуваного оператора:

$$\mathrm{L}(\boldsymbol{\theta}, \boldsymbol{\xi}) = \langle \psi(\boldsymbol{\theta}) \,|\, \hat{O}(\boldsymbol{\xi}) \,|\, \psi(\boldsymbol{\theta}) \rangle + \lambda \mathrm{R}(\boldsymbol{\theta}) \,, \tag{5}$$

де $\hat{O}$ – оператор вартості, що кодує критерії безпеки та ефективності,

$\mathrm{R}(\boldsymbol{\theta})$ – регуляризуючий функціонал, що враховує обмеження ресурсів,

λ – коефіцієнт балансування.

Нелінійна динаміка гібридного алгоритму. Ітеративна еволюція алгоритму описується нелінійним рекурентним співвідношенням:

$$\boldsymbol{\theta}_{k+1} = \boldsymbol{\theta}_k - \eta_k \mathrm{G}\left(\nabla_{\boldsymbol{\theta}} \mathrm{L}(\boldsymbol{\theta}_k), \mathbf{y}_k\right) \tag{6}$$

де $\mathbf{y}_k$ – вектор результатів квантових вимірювань,

η_k – адаптивний крок оптимізації,

$\mathrm{G}(\cdot)$ – нелінійний оператор оновлення, що враховує стохастичні та апаратні ефекти.

Нелінійність алгоритму зумовлена залежністю оператора оновлення від результатів вимірювань і поточного стану оптимізаційного процесу, що формує замкнений квантово-класичний контур зворотного зв'язку.

У перспективі квантово-класичні гібридні алгоритми можуть розглядатися як основні складові інтегрованих обчислювальних контурів підтримки прийняття рішень в умовах активної протидії, динамічної невизначеності та ресурсних обмежень [3]. Зазначені контури потенційно здатні забезпечити ефективну обробку високорозмірних і комбінаторно складних конфігурацій, а також оцінити криптографічну стійкість та оптимізувати параметри захищених каналів зв'язку.

За цих умов класична складова алгоритму передбачає інтеграцію результатів квантових обчислень у мережеві та обчислювальні інфраструктури, системи аналізу загроз та механізми адаптивного керування ресурсами. Саме наявність нелінійного контуру зворотного

зв’язку формує ефективну динаміку системи, у якій результати квантових вимірювань безпосередньо впливають на параметри класичних процедур [4]. Це забезпечує оперативну адаптацію до активних кібер і радіоелектронних впливів, змін топології мережі та деградації каналів зв’язку.

Отже, запропонована математична модель нелінійних квантово-класичних гібридних алгоритмів формує чіткий теоретичний фундамент для формалізованого опису та систематичного аналізу складних інформаційних процесів у високопродуктивних системах оборонного та кібербезпекового призначення. Модель забезпечує узгоджене представлення взаємодії квантових і класичних обчислювальних компонентів, дозволяє досліджувати властивості стійкості, адаптивності та ефективності алгоритмів, а також створює методологічну основу для проєктування адаптивних обчислювальних систем нового покоління [5], здатних працювати в умовах динамічних загроз, обмежених ресурсів та оперативних змін обстановки.

Список використаних джерел

1. NIST: Post-Quantum Cryptography (PQC) Project і NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://csrc.nist.gov/projects/post-quantum-cryptography.

2. Живило, Є., & Кучма, Ю. (2025). DEEP LEARNING-МОДЕЛЬ ПРОГНОЗУВАННЯ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 589–601. https://doi.org/10.28925/2663-4023.2025.31.1050

3. Zhyvylo, Ye., & Kuchma, Yu. Practical application and vulnerabilities of the Hill Cipher in a modern context. Systems of Control, Navigation and Communication. 2025. № 4 (78). С. 66–69. DOI: https://doi.org/10.26906/SUNZ.2025.4.066

4. Zhyvylo, Y., & Kuchma, Y. (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. Collection “Information Technology and Security”, 13(2), 162–177. https://doi.org/10.20535/2411-1031.2025.13.2.344591

5. Фесенко, Т., & Калашнікова, Ю. (2025). ФЕДЕРАТИВНА GNN-ХАІ МОДЕЛЬ ПРОГНОЗУ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У ZERO TRUST-СЕРЕДОВИЩІ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 602–619. https://doi.org/10.28925/2663-4023.2025.31.1049