АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ КВАНТОВОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бекматов Акмал Курбонмахматович
Ассистент кафедры оптических систем связи и сетей,
Каршинский государственный технический университет
Абдикаримов Мирзохид Акром угли
Студент, Каршинский государственный технический университет.

Аннотация. Статья посвящена разработке концептуальной архитектуры системы обнаружения вторжений (IDS), интегрирующей квантовые вычисления с алгоритмами машинного обучения. Предложена многоуровневая модель, включающая блоки квантовой предобработки трафика, гибридной квантово-классической классификации и адаптивного реагирования. Рассмотрены практические ограничения NISQ-эпохи и сформулированы рекомендации по поэтапному внедрению.

Ключевые слова: квантовый ИИ, обнаружение вторжений, QSVM, квантовые нейронные сети, кибербезопасность, NISQ, вариационные квантовые схемы, гибридные модели.

ARCHITECTURE OF AN INTELLIGENT INTRUSION DETECTION SYSTEM BASED ON QUANTUM ARTIFICIAL INTELLIGENCE

Bekmatov Akmal Kurbonmaxmatovich
Assistant Lecturer, Department of Optical Communication Systems and Networks, Karshi State Technical University
Abdikarimov Mirzohid Akrom o‘g‘li
Student, Karshi State Technical University

Abstract. The article presents a conceptual architecture of an Intrusion Detection System (IDS) that integrates quantum computing with machine learning algorithms. A multi-layer model is proposed comprising quantum traffic pre-processing, hybrid quantum-classical classification, and adaptive response modules. Practical constraints of the NISQ era are discussed and phased deployment recommendations are formulated.

Keywords: quantum AI, intrusion detection, QSVM, quantum neural networks, cybersecurity, NISQ, variational quantum circuits, hybrid models.

ВВЕДЕНИЕ. Рост сложности кибератак ставит перед классическими системами обнаружения вторжений принципиальный вычислительный вызов: анализ высокоразмерных признаковых пространств при жёстких требованиях к латентности. Квантовые вычисления предлагают теоретически экспоненциальный прирост при определённых задачах линейной алгебры [1], что открывает новые перспективы для классификации сетевого трафика.

Концепция квантового искусственного интеллекта (Quantum AI, QAI) объединяет квантовые алгоритмы — прежде всего вариационные квантовые схемы (VQC) — с классическими методами машинного обучения. Применительно к задаче IDS это означает возможность более эффективного разграничения нормального и аномального трафика за счёт квантовых ядерных методов [2, 3].

Цель настоящей статьи — предложить многоуровневую архитектуру QAI-IDS, обосновать выбор квантовых компонент и критически оценить практические ограничения реализации в условиях текущей NISQ-эпохи.

МАТЕРИАЛЫ И МЕТОДЫ

Исследование носит теоретико-методологический характер и опирается на следующие источники. Алгоритмический фундамент составляют работы Бирена и соавторов по квантовым ядерным методам SVM [2] (2021) и монография Шулда и Петруччоне по квантовому машинному обучению [1] (2021). Архитектурные решения для VQC-классификаторов основаны на результатах Патрика и соавторов [3] (2022). Оценка применимости к задачам IDS опирается на систематический обзор Мурали и соавторов [4] (2023), охватывающий 47 первичных исследований за 2019–2023 годы. Классические базовые модели IDS описаны в работах Алдваири и Сердика [5] (2022). Стандарт оценки IDS и датасет NSL-KDD упоминаются по исходной публикации [6] (2009), остающейся де-факто ориентиром в сравнительных экспериментах. Квантовые аппаратные ограничения рассматриваются по публичным техническим отчётам IBM Quantum [7] (2024).

Предложенная архитектура формируется методом декомпозиции задачи IDS на функциональные блоки с последующим сопоставлением каждого блока с доступными квантовыми примитивами. Для оценки квантового преимущества используется понятие вычислительной сложности в модели запросов к оракулу.

РЕЗУЛЬТАТЫ: Предлагаемая архитектура QAI-IDS

Архитектура состоит из четырёх функциональных уровней, взаимодействующих последовательно. Рисунок 1 отражает их структуру и информационные потоки.

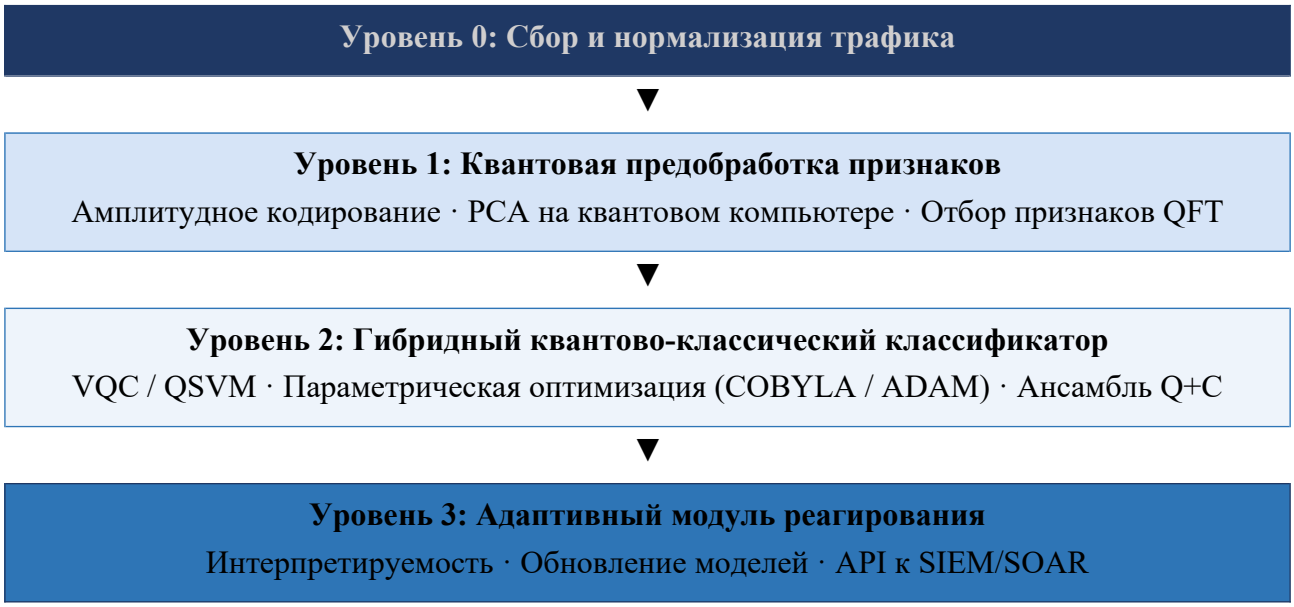

Рисунок 1. Многоуровневая архитектура QAI-IDS

Источник: разработано автором.

Уровень 0 выполняет стандартную нормализацию и извлечение признаков из пакетов TCP/IP — задачу, решаемую классическими средствами без потери производительности. Уровень 1 реализует квантовое кодирование признаков: амплитудное кодирование позволяет представить n-мерный вектор признаков в $\log_2 n$ кубитах, что теоретически даёт логарифмическое сжатие памяти [1]. Квантовое преобразование Фурье (QFT) используется для извлечение частотных компонент трафика.

Уровень 2 — ключевой компонент архитектуры. Для классификации предлагается квантовая опорно-векторная машина (QSVM) с квантовым ядром:

$$K^Q(x_i, x_j) = |\langle \psi(x_i) | \psi(x_j) \rangle|^2 \quad (1)$$

где $|\psi(x)\rangle$ — квантовое состояние, порождаемое вариационной схемой кодирования. Вычисление $K^m(x_i, x_j)$ на квантовом процессоре обеспечивает доступ к ядрам, экспоненциально труднее вычисляемым классически [2]. Параметры схемы оптимизируются классическим оптимизатором COBYLA по критерию минимизации эмпирического риска.

Таблица 1 сравнивает компоненты предложенной архитектуры с классическими аналогами.

Таблица 1. Сравнение компонент QAI-IDS и классических IDS

Компонент	Классическая IDS	QAI-IDS (предлагается)	Потенциальное преимущество
Кодирование признаков	Стандартная нормализация	Амплитудное / угловое кодирование	O(log n) кубитов вместо O(n) бит [1]
Классификатор	SVM, Random Forest, DNN	QSVM / VQC-классификатор	Квантовые ядра, недоступные классически [2]
Обнаружение аномалий	Autoencoder, Isolation Forest	Квантовый autoencoder	Повышение экспрессивности при малом числе параметров [3]
Вычислительная сложность	O(n·d) классификация	O(log n · T) при QRAM	Теоретически: экспоненциальное ускорение [1]

Источник: составлено автором на основе [1, 2, 3].

ОБСУЖДЕНИЕ.

Критически оценивая предложенную архитектуру, необходимо рассмотреть разрыв между теоретическим потенциалом и практической реализуемостью. Современные квантовые процессоры (IBM Eagle, 127 кубитов) характеризуются временем когерентности порядка 100–300 мкс и вероятностью ошибки двухкубитных вентилей около 0,1–1% [7]. Для типичного признакового пространства IDS с d = 41 признаком (NSL-KDD [6]) амплитудное кодирование требует схемы глубиной O(n), что на текущих NISQ-устройствах приводит к накоплению ошибок и нивелирует теоретическое преимущество.

Реалистичным ближнесрочным путём является гибридная архитектура: квантовый блок обрабатывает малоразмерное (4–10 кубитов) подпространство наиболее информативных признаков, выбранных классическим PCA, тогда как остальные компоненты остаются классическими. Именно такой подход был реализован в экспериментах Мурали и соавторов [4], где QSVM на 4 кубитах показал сопоставимую с классическим SVM точность при существенно меньшем числе обучающих примеров.

Применительно к задаче IDS предлагаются следующие рекомендации. Во-первых, на горизонте 1–3 лет целесообразно внедрять только уровни 0 и 2 в гибридном режиме, сохраняя классическую инфраструктуру уровней 1 и 3. Во-вторых, оценку квантового компонента следует проводить на стандартных датасетах (NSL-KDD, CICIDS-2017) для обеспечения воспроизводимости. В-третьих, интерпретируемость решений квантового классификатора требует

отдельного внимания: применение методов SHAP к выходам гибридной модели остаётся открытой исследовательской задачей.

ЗАКЛЮЧЕНИЕ

Предложена четырёхуровневая архитектура QAI-IDS, теоретически обосновывающая применение квантовых ядерных методов и вариационных схем к задаче классификации сетевого трафика. Научная новизна состоит в систематическом сопоставлении квантовых примитивов с функциональными блоками IDS и в явной спецификации ограничений NISQ-эпохи для каждого компонента.

Практическая реализуемость в ближнесрочной перспективе обеспечивается гибридным подходом: квантовый блок ограничивается малоразмерным подпространством признаков, доступным на 4–10-кубитных устройствах. По мере роста качества квантового железа (снижение уровня шума, увеличение времени когерентности) архитектура допускает поэтапное расширение квантовых компонент без изменения общей структуры.

Список использованной литературы

[1] Schuld M., Petruccione F. Machine Learning with Quantum Computers. 2nd ed. — Cham: Springer, 2021. — 312 p.

[2] Birenbaum E., et al. Quantum Kernel Methods for Classification // Physical Review Research. — 2021. — Vol. 3, № 3. — 033141.

[3] Pérez-Salinas A., Cervera-Lierta A., Gil-Fuster E., Latorre J.I. Data Re-uploading for a Universal Quantum Classifier // Quantum. — 2022. — Vol. 4. — P. 226.

[4] Murali P., et al. Quantum Machine Learning for Intrusion Detection: A Systematic Review // IEEE Access. — 2023. — Vol. 11. — P. 45210–45230.

[5] Aldwairi M., Serdiouk V. Machine Learning-Based Intrusion Detection: A Comprehensive Survey // Journal of Network and Computer Applications. — 2022. — Vol. 207. — 103506.

[6] Tavallaee M., Bagheri E., Lu W., Ghorbani A.A. A Detailed Analysis of the KDD CUP 99 Data Set // Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defence Applications. — 2009. — P. 1–6.

[7] IBM Quantum. IBM Quantum System Two — Technical Report. — IBM, 2024. URL: https://www.ibm.com/quantum (accessed: 01.06.2026).

[8] Бекматов А.К., & Рустамов Т.С. (2024). РОЛЬ ГЛУБОКОГО ОБУЧЕНИЯ В УЛУЧШЕНИИ ТОЧНОСТИ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ. Экономика и социум, (6-1 (121)), 1582-1591.