МОДЕЛЬ ЦИФРОВОЙ ПЛАТФОРМЫ ДЛЯ АНАЛИЗА УСТОЙЧИВОСТИ К КВАНТОВЫМ УГРОЗАМ

Ларина М.В[1]., Скиба В.Ю[2].

Ключевые слова: *кибербезопасность, квантовое превосходство, квантовая устойчивость, пост-квантовая криптография, мониторинг угроз, квантово-устойчивая аутентификация, концептуальная модель платформы, схемы шифрования, стандарты NIST PQC.*

Аннотация

Цель работы *— выявить слабые стороны цифровых платформ с учетом развития квантовых технологий и разработать концептуальную модель цифровой платформы, обладающей устойчивостью к квантовым атакам.*

Методы *исследования: системный анализ современных платформ, классификация, синтез и интеграции квантово-устойчивых решений, проектирование цифровой платформы с многоуровневой архитектурой, сравнительный анализ постквантовых криптографических алгоритмов, стандартизированных NIST. В основу модели заложены принципы адаптации к появляющимся вызовам в области кибербезопасности.*

Результаты исследования: предложены модель взаимодействия элементов цифровой экосистемы и концептуальная модель платформы, включающая в себя многоуровневую системы защиты, в основе которой лежит постквантовая криптография, квантово-устойчивая аутентификация и динамический мониторинг угроз. Разработанные модели могут быть использованы при развитии цифровых платформ, а также при проектировании новых безопасных платформ в финансовом секторе, государственном управлении и критической информационной инфраструктуре. Приведены результаты сравнительного анализа алгоритмов CRYSTALS-KYBER, HQC, CRYSTALS-DILITHIUM, FALCON и SPHINCS+. Выводы исследования подчеркивают необходимость заблаговременного внедрения постквантовых технологий для минимизации рисков.

Научная новизна: *представленная модель цифровой платформы демонстрирует комплексное решение проблемы обеспечения квантовой устойчивости за счет комплексного применения компонент, предусматривающих использование алгоритмов пост-квантовой криптографии, элементов машинного обучения и механизмов управления рисками.*

Практическая значимость: *разработанные модели цифровой платформы и взаимодействия элементов цифровой экосистемы позволяют решать такие задачи, как синтез квантовоустойчивых цифровых платформ и анализ устойчивости функционирования цифровых платформ в условиях наличия квантовых угроз.*

DOI: 10.24412/1994-1404-2025-3-00-02

Введение

Термин «экосистема» в цифровых технологиях предполагает наличие совокупности взаимосвязанных сервисов, способных легко масштабироваться, обеспечивать эффективный обмен и обработку больших объемов данных. А также данные сервисы объединены общими технологическими решениями.

В современном мире цифровые экосистемы и платформы могут быть подвержены различным вызовам в сфере информационной безопасности, в том числе вызовам, которые связаны с развитием квантовых технологий. По данным компании Positive Technologies[3] общее количество инцидентов информационной безопасности возросло в среднем на 15%, если сравнивать показатели по кварталам за 2023 и 2024 года (рис. 1).

[3] Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года. URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id1 (дата обращения: 12.09.2025).

[1] ***Ларина Мария Васильевна,*** *лаборант-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», федеральная территория «Сириус», Краснодарский край, Российская Федерация. ORCID: 0009-0009-7826-0180.*

E-mail: larina.mv@talantiuspeh.ru

[2] ***Скиба Владимир Юрьевич,*** *доктор технических наук, старший научный сотрудник, главный инженер-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», федеральная территория «Сириус», Краснодарский край, Российская Федерация. ORCID: 0000-0002-9805-7800.*

E-mail: skiba.vy@talantiuspeh.ru

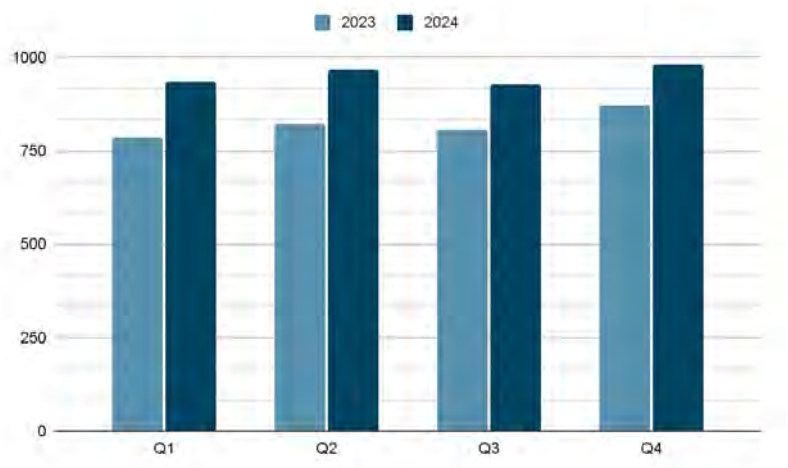

Рис. 1. Количество инцидентов по кварталам в 2023 — 2024 гг.

Прогресс в сфере квантовых вычислений порождает как положительные результаты, так и отрицательные — в виде новых угроз для традиционных криптографических алгоритмов. Эти факты требуют привлечения особого внимания к разработке новых методов по защите цифровых платформ и экосистем, а также — необходимость внесения изменений в их архитектуру. Ядро подобных экосистем составляют технологии, следовательно, разработка квантовых сетей и компьютеров скорее всего приведет к значительной трансформации.

Квантовые вычислительные системы способны осуществлять действия, на данный момент недоступные классическим, например такие как реализация алгоритма Гровера (ускоренный поиск в базах данных) или алгоритм Шора (взлом криптографических схем). Данные алгоритмы подробно изучены в работе [1], они были использованы в качестве методов исследования при оценивании квантовой устойчивости блокчейн-платформ. Все большее распространение получают квантовые коммуникации, они предоставляют возможность защищенной передачи данных на основе квантовых состояний фотонов, при этом любая попытка перехвата информации или прослушивания моментально выявляется. Анализ развития квантовых коммуникаций в России, США, Китае и Японии проведен в [2]. В [3] предложена Концепция обеспечения устойчивости функционирования цифровых платформ и блокчейн-экосистем в условиях появления квантовых угроз, предусматривающая комплексное применение различных методов и моделей, а также проведения исследований достигнутого уровня устойчивости.

В данной статье представлена модель цифровой платформы, реализация которой позволит обеспечить устойчивость к квантовым угрозам. Она сочетает в себе методы пост-квантовой криптографии (алгоритмы на решетках, протоколы распределенных ключей и хеш-функции) с формальными методами проверки безопасности.

Постановка задачи

На данный момент комплексный подход к оценке устойчивости цифровых экосистем к квантовым угрозам остается не реализованным в полной мере. Многие исследования в данной сфере фокусируются на отдельных аспектах защиты от различных уязвимостей, например таких как использование технологий искусственного интеллекта, пост-квантовой криптографии или мониторинга угроз [4, 5, 6], без учета системного взаимодействия компонентов модели.

При этом особое внимание при квантовых атаках требует взаимосвязь таких модулей, как аутентификация, шифрование и мониторинг, динамические свойства цифровых экосистем (автоапгрейд протоколов). Таким образом, необходимо:

- выявить особенности архитектуры и принципов работы цифровых экосистем и платформ;
- разработать модель взаимодействия элементов цифровой экосистемы;
- разработать модель цифровой платформы, устойчивой к квантовым атакам и предусматривающей применение квантово-устойчивые алгоритмы (постквантовые или квантовые алгоритмы), механизмы обнаружения и нейтрализации уязвимостей, адаптивные протоколы обновления системы;
- провести сравнительный анализ постквантовых криптографических алгоритмов, стандартизированных NIST по ключевым параметрам: реализация, безопасность, производительность, размер ключей и подписей.

При построении модели также необходимо учесть методологический документ Федеральной службы по техническому и экспортному контролю[4] (ФСТЭК России) от 5 февраля 2021 года «Методика оценки угроз безопасности информации» использован в качестве руководства.

[4] Методический документ. Методика оценки угроз безопасности информации. URL: https://rppa.pro/_media/npa/fstek_05.02.2021.pdf (дата обращения 12.09.2025).

Особенности архитектуры и принципов работы цифровых экосистем и платформ

Термин «цифровая экосистема» введен американским ученым Джеймсом Муром в 1993 году [7]. Под цифровой экосистемой он понимал сложное цифровое пространство, сеть множества взаимосвязанных сервисов и технологических компонентов, объединенных общими стандартами и протоколами.

В 2002 году группой европейских исследователей выдвинута Концепция цифровых бизнес-экосистем. В их понимании цифровая экосистема — это распределенная адаптивная система, которой свойственны такие природные качества, как самоорганизация, масштабируемость и устойчивость [8].

В качестве основных принципов работы цифровых экосистем следует отметить ориентацию на пользователя, масштабируемость и динамику. Сервисы и платформы объединены друг с другом и построены с учетом возможности дальнейшего масштабирования. Функционирование стандартной цифровой экосистемы можно представить в виде следующей последовательности процессов:

1. Идентификация, аутентификация и авторизация пользователя в системе.
2. Сбор данных (действия пользователя, логи, API, транзакции).
3. Интеграция данных и обработка (объединение данных из разных источников в одну точку сбора, удаление дубликатов и приведение к единому формату).
4. Хранение различных типов данных (в исходном формате, обработанные, операционные данные).
5. Анализ данных (возможно с применением моделей машинного обучения).
6. Использование данных в различных процессах.
7. Получение обратной связи от пользователей или программ.

Эффективность цифровых экосистем зависит напрямую от архитектуры платформ (рис. 2), входящих в их состав. Представленная укрупненная архитектура стандартной цифровой платформы представляет собой доработанную архитектуру из [9], в которую авторами внесены уточнения некоторых уровней и добавлен новый уровень, связанный с обеспечением безопасности цифровых платформ. При проектировании каждая компонента платформы требует особого внимания, очень важно учесть требования к масштабируемости и отказоустойчивости системы в целом.

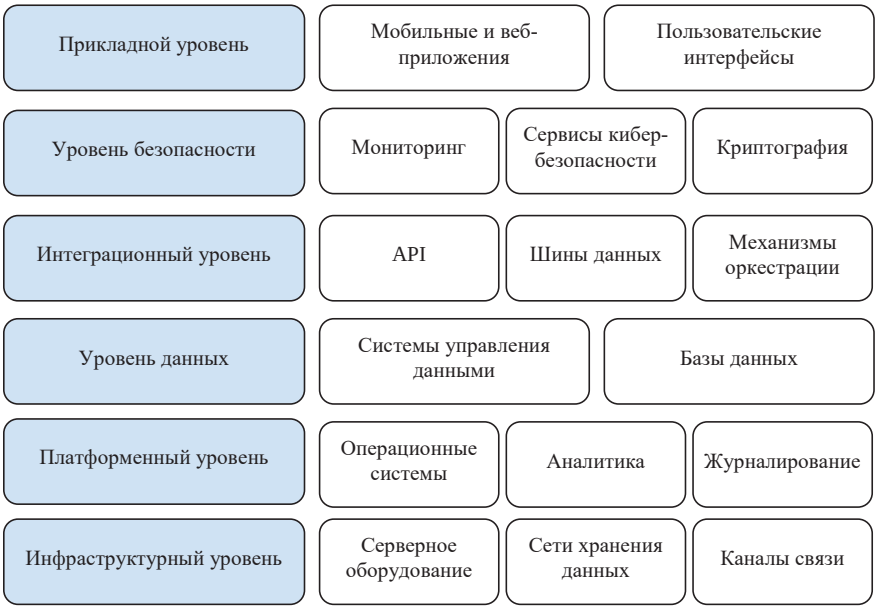

Рис. 2. Укрупненная архитектура стандартной цифровой платформы

Анализ данной архитектуры позволяет выделить основные свойства цифровых экосистем.

Главное из них — это модульность, система должна быть разделена на независимые компоненты, отдельные микросервисы, которые в случае квантовых или обычных угроз будет проще восстановить, в отличии от монолитной архитектуры.

Второе свойство — это асинхронность взаимодействия между сервисами, которая позволяет поддерживать гибкость при работе.

API-first подход является следующим свойством и подразумевает под собой разработку через интерфейсы для более удобного представления.

И заключительное свойство, которым должна обладать цифровая экосистема, — это горизонтальное масштабирование, возможность добавление новых узлов для повышения производительности или отказоустойчивости.

Указанные особенности следует учитывать при разработке стандартных или типовых моделей цифровых

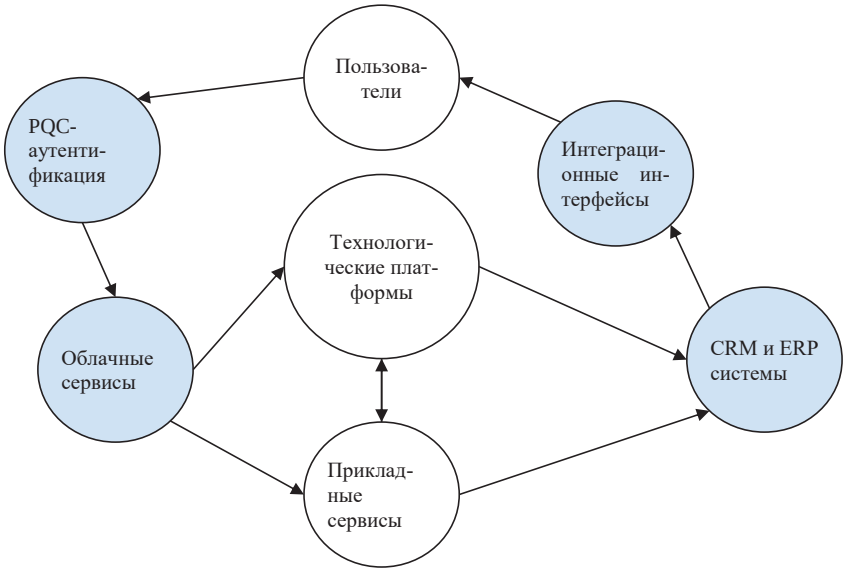

Рис. 3. Модель взаимодействия ключевых элементов цифровой экосистемы

экосистем и платформ, в том числе и для решения следующих задач:

- синтеза (или проектирования, создания или развития, модернизации) конкретных цифровых платформ, их интеграции в цифровые экосистемы;
- анализа (или сертификации, верификации и т.д.) защищенности и устойчивости функционирования, в том числе в условиях наличия квантовых угроз.

При этом стандартная и типовые модели цифровой платформы также должны учитывать применение квантовых технологий и квантовых алгоритмов, то есть использование как минимум одного квантового вычислительного модуля (или его эмулятора), что позволит решать задачи синтеза и анализа применения квантовых алгоритмов для цифровых платформ, которые находятся на стадии создания или для которых запланировано дальнейшее развитие (модернизация). Учет данных квантовых технологий и квантовых алгоритмов позволит заблаговременно проводить исследования принципов квантовых вычислений, тестирования квантовых алгоритмов и обучения специалистов работе с квантовыми технологиями.

Модель взаимодействия элементов цифровой экосистемы

Рассмотрим модель взаимодействия структурных компонентов цифровой экосистемы и их описание в соответствии с выше поставленными задачами, а также уточним модель цифровой платформы, входящей в состав экосистемы. Цифровые экосистемы способны предоставить быстрый доступ к информационным ресурсам и открыть возможности интеграции сервисов из различных сфер деятельности. По данным исследования института экономической политики имени Е.Т. Гайдара[5] на 2022 год экосистемы в России находятся на стадии формирования по сравнению с мировыми. Но в условиях развития квантовых технологий важно даже на этапе зарождения стремиться обеспечить полноценную кибербезопасность на долгий срок.

Подобные экосистемы можно охарактеризовать как совокупность взаимодействующих элементов, каждый из которых отвечает за определенные функции. На рис. 3 представлена модель взаимодействия элементов в экосистеме, которая в отличии от модели, представленной в [10], дополнена авторами новыми компонентами, учитывающими необходимость обеспечения квантовой устойчивости.

В данной модели PQC-аутентификация (Post-Quantum Cryptography) выделена в качестве отдельного элемента, одной из ее главных целей является защита конфиденциальных данных и обеспечение устойчивости цифровых экосистем к квантовым уязвимостям, а также защита от неправомерных действий злоумышленников. В [11] представлены два протокола полной аутентификации для квантового распределения ключей, они базируются на пост-квантовой криптографии. Важное их отличие состоит в следующем: первый использует пост-квантовые (PQC) алгоритмы для подписи и шифрования при проверке ключа с целью исправления ошибок, а второй — только для подписи, когда осуществляется аутентификация базисного просеивания.

После успешного прохождения PQC-аутентификации через веб-интерфейс экосистемы пользователь создает запрос, который перенаправляется в облачные сервисы. Они предоставляют удаленный доступ

[5] Институт экономической политики им. Е.Т. Гайдара: Цифровые экосистемы в России: эволюция, типология, подходы к регулированию. URL: https://www.iep.ru/files/news/Issledovanie_jekosistem_Otchet.pdf (дата обращения: 12.09.2025)

к вычислительным ресурсам (IaaS) и гибко масштабируют инфраструктуру в соответствии с потребностями организации. Далее облачные сервисы загружают необходимые инструменты на технологические платформы (PaaS), являющиеся ядром цифровых экосистем. В зависимости от требований к функционалу экосистемы могут быть централизованными, децентрализованными или гибридными. Прикладные сервисы (SaaS) также входят в состав компонентов экосистем, могут быть базовыми, интегрированными или специализированными, тесно взаимодействуют с платформами.

Когда задача, поставленная пользователем, выполнилась, она переходит в обработку CRM- и ERP-системами. На этом этапе все действия защищены, и каждая операция подписывается цифровой подписью, данные дополнительно шифруются комбинацией классических и пост-квантовых алгоритмов. Затем пользователь получает обратную связь через интеграционные сервисы, все эти процессы происходят мгновенно.

Модель платформы, устойчивой к квантовым киберугрозам

Анализ моделей информационных систем на основе облачных вычислений, предложенных NIST, IBM и Microsoft проведен в [12]. Авторы пришли к выводу о том, что при разработке моделей информационных систем важно четко выделять детализированные уровни, а также значительное внимание уделять безопасности, охватывающей все уровни платформы. По итогам исследования авторы предложили эталонную модель, основанную на модели национального института стандартов и технологий США[6], но с внесением дополнений, отмеченных выше.

Действительно, в условиях стремительного развития квантовой информатики появляются новые угрозы, от которых важно защитить цифровые экосистемы и платформы, иначе это может негативно сказаться на состоянии как небольших организаций, так и значимых государственных предприятиях. В [13] по итогам анализа состояния объектов критической информационной инфраструктуры таможенных органов Российской Федерации предложено выделить три основных направления решения проблемы обеспечения квантовой устойчивости и отмечено, что создание полностью квантовой модели информационных систем представляет отдаленную перспективу.

Для построения модели цифровой платформы, содержащей в себе элементы квантовых технологий, необходимо понимать, какие этапы включает в себя процесс квантовых вычислений. В соответствии с [14] процесс нначинается с подготовки данных, далее идет подготовка схемы квантовых вычислений и ее загрузка вместе с данными в квантовый процессор. После этого процессор выполняет вычисления, получает результаты в виде новых данных и интерпретирует их.

В связи с этим авторы настоящей работы предлагают с целью обеспечения безопасности на всех ее уровнях новую уточненную Модель цифровой платформы с внедрением квантовых технологий (рис. 4), в которой выделены конкретные уровни в соответствии с укрупненной архитектурой стандартной цифровой платформы (рис. 2). Разработанная модель объединила в себе традиционные и новые методы на пост-квантовых алгоритмах.

На прикладном уровне пользователю доступны инструменты для анализа и защиты от квантовых угроз. Симулятор квантовых атак предназначен для моделирования потенциальных ситуаций взлома, а модуль визуализации рисков — для предоставления наглядных отчетов и рекомендаций по улучшению мер защиты. Аналитический модуль с поддержкой машинного обучения осуществляет детекцию аномалий в онлайн-режиме. Также на данном уровне предложены инструменты разработки с PQC-библиотеками, которые позволят внедрить квантовые технологии в код приложений, тем самым повысить их устойчивость. Функция автоапгрейда протоколов обеспечивает своевременное обновление криптографических механизмов в соответствии с рекомендациями и последними стандартами безопасности.

Уровень безопасности выделен как отдельный уровень и главная его цель — это проведение аутентификации для новых пользователей. Система PQC-аутентификации отвечает за безопасный доступ ко всем ресурсам платформы, хеш-функции и протоколы генерации случайных чисел вносят дополнения в криптографическую защиту и тем самым создают многоуровневый барьер. Криптографические алгоритмы используют математические задачи на решетках.

Интеграционный уровень обеспечивает безопасное взаимодействие между компонентами платформы, API с гибридным шифрованием поддерживает традиционные и пост-квантовые алгоритмы, что позволяет осуществить плавный переход к новым стандартам безопасности. Механизмы оркестрации и шины данных оптимизируют передачу информации между различными сервисами и сохраняют надежный уровень защиты на всех этапах обработки данных.

На уровне данных предложено использование инновационных методов защиты информации. Системы управления базами данных основаны на криптографических протоколах, также применяется технология гомоморфного шифрования (homomorphic encryption), направленная на выполнение аналитических операций с зашифрованными данными. Это позволяет минимизировать риск компрометации данных.

[6] National Institute of Standards and Technology Special Publication 500-292. NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology / Liu F., Tong J. and other // Cloud Computing Program, Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, September 2011, 35 pp. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909505 (дата обращения 12.09.2025).

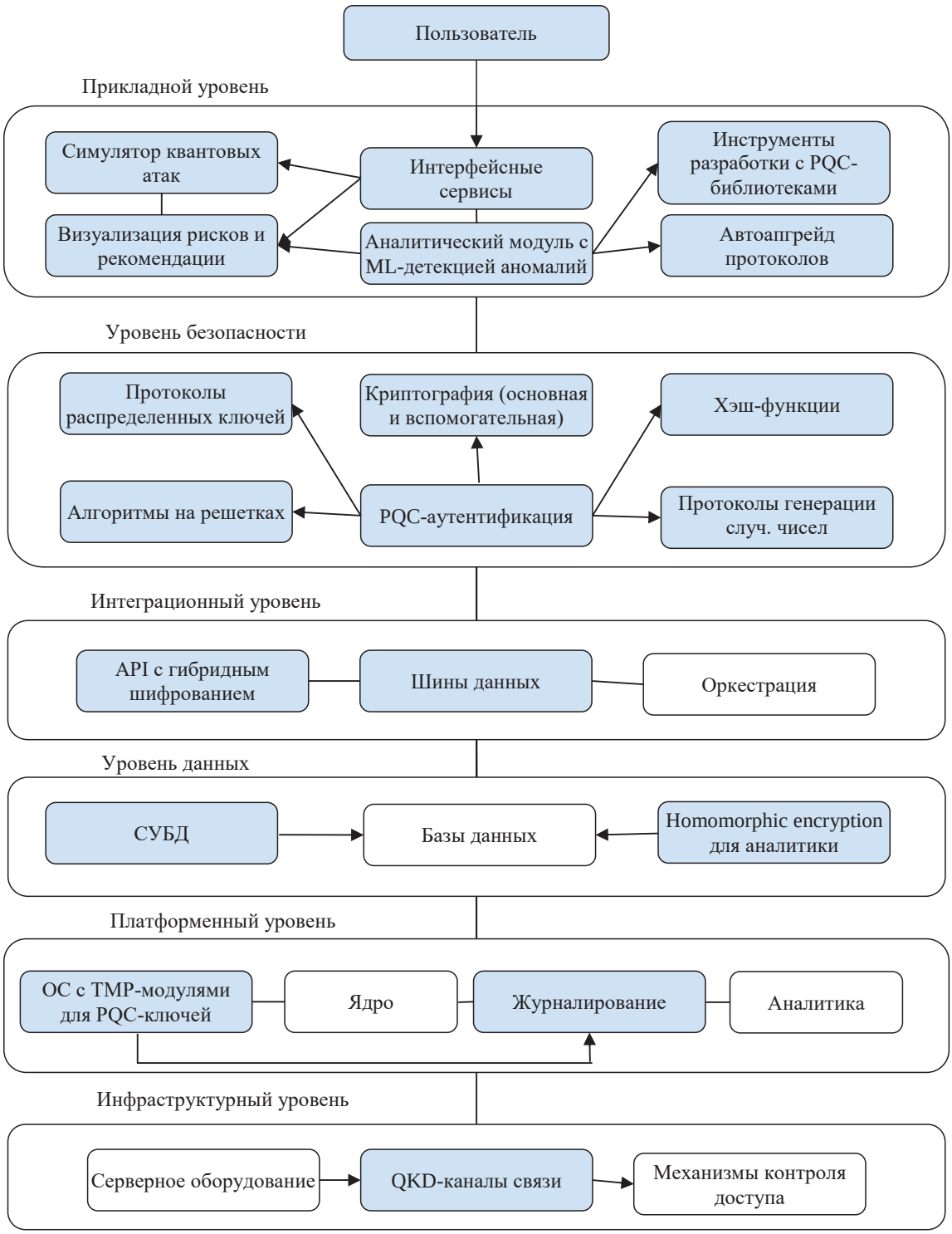

Рис. 3. Модель взаимодействия ключевых элементов цифровой экосистемы

Следующий платформенный уровень объединяет компоненты в единую систему, операционная система с TPM-модулем (Trusted Platform Module) обеспечивает безопасное хранение криптографических ключей, сертификатов и других конфиденциальных данных. Ядро платформы оптимизировано и направлено на работу с ресурсоемкими криптографическими операциями. Также необходимо видеть полную картину событий и потенциальных угроз, для этого используются системы журналирования и аналитики, они позволяют оперативно реагировать на любые инциденты.

И наконец, инфраструктурный уровень включает в себя специализированное оборудование. QKD-каналы связи (Quantum Key Distribution) отвечают за защиту передачи ключей шифрования, а механизмы контроля доступа дают доступ к критически важным данным и ресурсам только авторизованным пользователям.

Таблица 1

Кандидаты всех четырех туров конкурса NIST

1 тур	BIG QUAKE **BIKE** CFPKM **Classic McEliece** Compact LWE **CRYSTALS-DILITHIUM** **CRYSTALS-KYBER** DAGS Ding Key Exchange DME DRS DualModeMS Edon-K EMBLEM/R.EMBLEM **FALCON** **FrodoKEM** **GeMSS** Giophantus Gravity-SPHINCS Guess Again Gui HILA5 HiMQ-3	HK-17 **HQC** KCL KINDI **LAC** LAKE LEDAkem LEDApkc Lepton LIMA Lizard LOCKER LOTUS **LUOV** McNie Mersenne-756839 **MQDSS** **NewHope** NTRUEncrypt NTRU-HRSS-KEM **NTRU Prime** **NTS-KEM** Odd Manhattan	Ouroboros-R **Picnic** Post-quantum RSA Encryption Post-quantum RSA Signature pqNTRUSign pqsigRM QC-MDPC-KEM **qTESLA** RaCoSS **Rainbow** Ramstake RankSign RLCE-KEM Round2 RQC RVB **SABER** **SIKE** **SPHINCS+** SRTPI **Three Bears** Titanium WalnutDSA
2 тур	**BIKE** **Classic McEliece** **CRYSTALS-DILITHIUM** **CRYSTALS-KYBER** **FALCON** **FrodoKEM** **GeMSS** **HQC** LAC	LEDAcrypt LUOV MQDSS NewHope **NTRU** **NTRU Prime** NTS-KEM **Picnic** qTESLA	**Rainbow** ROLLO Round5 RQC **SABER** **SIKE** **SPHINCS+** Three Bears
3 тур	Шифрование с открытым ключом: **Classic McEliece** **CRYSTALS-KYBER (standard)** NTRU SABER Цифровая подпись: **CRYSTALS-DILITHIUM (standard)** **FALCON (standard)** Rainbow	Альтернатива: **BIKE** FrodoKEM **HQC** NTRU Prime **SIKE** Альтернатива: GeMSS Picnic **SPHINCS+ (standard)**	
4 тур	Базируется на коде: BIKE **HQC (standard)** Classic McEliece	Базируется на изогении: SIKE	

Таким образом, в представленной модели платформы большое внимание уделено обеспечению защиты от квантовых угроз, более детально рассмотрены уровни. Данная модель может быть использована в дальнейших исследованиях и адаптирована под конкретные задачи пользователей.

Сравнительный анализ пост-квантовых алгоритмов, стандартизированных NIST

В предложенной выше модели используются пост-квантовые алгоритмы, способствующие улучшенной защите от различного типа угроз. В 2016 Национальный Институт Стандартов и Технологий США сообщил о проведении конкурса по отбору новых пост-квантовых алгоритмов в качестве стандартов. На конкурс подано 82 заявки, 69 из них прошли отбор (20 — схемы электронной подписи и 49 — алгоритмы шифрования с открытым ключом) [15].

Конкурс проводился в 4 тура, результаты первого тура были озвучены в январе 2019 и по его итогам дальше прошло 26 алгоритмов[7].

По итогам второго тура осталось 15 алгоритмов, они были разделены на группы основных и альтернативных алгоритмов[8].

Результаты третьего тура представили в июле 2022 года[9], в качестве стандартов было выбрано 4 алгоритма, и по окончанию четвертого тура в марте 2025 года также добавили еще один стандартный алгоритм[10]:

1) шифрование с открытым ключом:
   a) CRYSTALS-KYBER (2022 год);
   b) HQC (2025 год);
2) алгоритмы цифровой подписи:
   a) CRYSTALS-DILITHIUM (2022 год);
   b) FALCON (2022 год);
   c) SPHINCS+ (2022 год).

Результаты всех туров конкурса NIST представлены в табл. 1 (жирным шрифтом выделены алгоритмы, успешно прошедшие в следующий тур).

Приведем результаты анализа пост-квантовых алгоритмов, стандартизированных NIST, по таким параметрам, как реализация, безопасность, производительность и размер ключей, а также представим общую оценку каждого алгоритма.

Алгоритмы шифрования с открытым ключом

CRYSTALS-KYBER. Это алгоритм инкапсуляции ключей, основанный на модульных решетках (module-LWE). Сначала он строится как схема шифрования с открытым ключом с безопасностью IND-CPA (неотличимость при атаке на открытый текст), а затем преобразуется в механизм инкапсуляции ключей с безопасностью IND-CCA (неотличимость при атаке на шифротекст) [16].

Базовая схема шифрования с открытым ключом основывается на проблеме MLWE. Алгоритм работает в кольце многочленов $R = Z[X]/(X^{256} + 1)$ по модулю $\mathrm{q} = 3329$.

При генерации ключей создается пара $pk = (A, b)$, где $A \in R_q^{k \times k}$ — это случайная матрица многочленов, а $b = As + e$ вычисляется через секретный вектор s и вектор ошибок e. Оба вектора $s, e \in R_q^k$ выбираются независимо из распределения χ покоэффициентно (χ — распределение на «короткие» полиномы из R_q).

NIST определяет три уровня безопасности: 1, 3 и 5; они достигаются при изменении ранга модуля k (2, 3 и 4 соответственно).

Шифрование и дешифрование демонстрирует парадигму Линднера-Пейкерта [17]. Шифрование сообщения m (256-битной строки) имеет сходство с классическими схемами на основе решеток, но есть и важные изменения.

Отправитель формирует зашифрованный текст $c = (c_1, c_2) \in R_q^k \times R_q$, где $c_1 = rA + e_1$ и $c_2 = rb + e_2 + [\frac{q}{2}] \cdot m$. Векторы многочленов $r, e_1 \in R_q^k$ и многочлен $e_2 \in R_q$, при этом все коэффициенты каждого многочлена выбираются независимо от χ, они обеспечивают возможность корректного дешифрования [16]. Данную запись $[\frac{q}{2}] \cdot m$ следует воспринимать как вектор коэффициентов одного полинома в R_q (при необходимости с дополнением).

Отметим, что при реализации CRYSTALS-KYBER применяется сжатие данных: без ущерба для безопасности уменьшается объем данных при отправлении, так как часть битов зашифрованного текста отбрасывается.

При дешифровании вычисляется промежуточное значение $v = c_2 - c_1 s$, затем каждый коэффициент полинома округляется по модулю 2, чтобы извлечь отправленную последовательность битов m [16].

Алгоритм обеспечивает безопасность на основе сложной задачи Module-LWE, устойчивой к квантовым атакам. Доказательства безопасности строго выполняются в ROM (Random Oracle Model) [18] и менее строго в QROM (Quantum Random Oracle Model). Однако повысить уровень безопасности в QROM можно путем

---

[7] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process / Alagic G., Alperin-Sheriff J. and other // National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report (IR), NISTIR 8240, January 2019, 27 pp. URL: https://doi.org/10.6028/NIST.IR.8240 (дата обращения: 12.09.2025).

[8] Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process / Alagic G., Alperin-Sheriff J. and other // National Institute of Standards and Technology, Gaithersburg, MD, NISTIR 8309, July 2020, 39 pp. URL: https://doi.org/10.6028/NIST.IR.8309 (дата обращения: 12.09.2025).

[9] Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / Alagic G., Apon D. and other // National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report (IR), NISTIR 8413-updl, July 2022, 102 pp. URL: https://doi.org/10.6028/NIST.IR.8413-upd1 (дата обращения: 12.09.2025).

[10] Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process / Alagic G., Bros M. and other // National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report (IR), NISTIR 8545, March 2025, 34 pp. URL: https://doi.org/10.6028/NIST.IR.8545 (дата обращения: 12.09.2025).

применения разделимой симулируемости (Disjoint Simulatability) [19].

Это свойство позволяет симулировать шифротекст без знания открытого текста, а значит, избежать квадратичных потерь в безопасности, характерных для преобразования Фуджисаки-Окамото. Также благодаря этому свойству получается избежать применения леммы OW2H (One Way to Hiding), приводящей к квадратичным потерям.

Таким образом, алгоритм CRYSTALS-KYBER обладает отличной производительностью в программных, аппаратных и гибридных реализациях, в отличие от NTRU и SABER (финалисты 3 тура), поэтому алгоритм выбран в качестве стандартного.

HQC. Это алгоритм инкапсуляции ключей, основанный на теории кодов исправления ошибок (квазициклических кодах, QC-MDPC), позволяет скрывать данные в шуме таким образом, чтобы только владелец секретного ключа мог эффективно расшифровать их.

HQC также использует протокол шифрования, похожий на LWE. В его реализации применяется кольцо $R = F_2[x]/(x^n - 1)$, где n — простое число, такое, что x^{n-1} имеет всего два несократимых множителя по модулю 2.

Секретный ключ представляет собой случайно выбранную пару $(x, y) \in R^2$, а открытый ключ — пару $(h, s = x + h \cdot y)$, где h выбирается случайным образом из R и используется для построения матрицы генератора $G \in F_2^{k \times n}$ [16]. Поскольку секретный ключ генерируется независимо от кода, в публичной матрице проверки четности HQC нет скрытой структуры, что обеспечивает безопасность независимо от алгоритма декодирования [23].

Чтобы зашифровать сообщение $m \in F_2^k$, отправитель случайным образом выбирает три многочлена $e, r_1, r_2 \in R$ с соответствующими весами и отправляет зашифрованный текст $c: c = (u, v) = (r_1 + h \cdot r_2, mG + s \cdot r_2 + e)$.

Чтобы расшифровать сообщение, используется алгоритм декодирования $(v - u \cdot y)$, в HQC применяется декодер на основе кодов Рида-Соломона и Рида-Мюллера (RMRS). Он имеет четко определенное минимальное расстояние d и определяемую возможность исправления ошибок $\delta = [\frac{d-1}{2}]$ [23]. Вероятность того, что зашифрованный текст содержит ошибку e такую, что $e > |\delta|$, определяется анализом в замкнутой форме и используется для определения верхней границы частоты ошибок при расшифровке.

Квазициклическая структура данного алгоритма имеет уникальные математические основы и позволяет достичь приемлемых размеров открытых ключей и зашифрованных текстов, но они все равно остаются больше, чем у других кандидатов четвертого тура[11]. Общая производительность считается удовлетворительной, но не самой оптимальной, поэтому NIST все еще рассматривает алгоритм HQC и возможно выберет его в качестве «запасного» постквантового алгоритма из-за этих особенностей.

Производительность алгоритмов CRYSTALS-KYBER и HQC при различных уровнях NIST, а также размеры секретного ключа (СК), открытого ключа (ОК) и шифротекста (ШТ) представлены в табл. 2.

Таблица 2

Производительность и размеры ключей алгоритмов CRYSTALS-KYBER[12] и HQC[13]

Параметр	Уровень NIST	Количество циклов (тыс)			Размер в байтах		
		Генерация ключа	Инкапсуляция	Декапсуляция	СК	ОК	ШТ
Kyber512	I	33,9	45,2	34,6	1 632	800	768
hqc-128	I	105	197	360	56	2 249	4 497
Kyber768	III	52,7	67,6	53,2	2 400	1 184	1 088
hqc-192	III	244	460	746	64	4 522	9 042
Kyber1024	V	73,5	73,5	79,1	3 168	1 568	1 568
hqc-256	V	4 246	844	1 410	72	7 245	14 485

Результаты сравнительного анализа алгоритмов CRYSTALS-KYBER и HQC (табл. 3) позволяет сделать следующий вывод: CRYSTALS-KYBER больше подойдет для приложений, где важны скорость, а HQC обладает менее оптимальной производительностью и подойдет для ситуаций, где важна устойчивость к атакам на основе кодовых решеток.

[11] Status Report on the Fourth Round (см. сноску 10).

[12] CRYSTALS-Kyber. Algorithm Specifications And Supporting Documentation (version 3.02) / Avanzi R., Bos J. and other // August 4, 2021, 43 pp. URL: https://www.pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf. (дата обращения: 12.09.2025).

[13] Status Report on the Fourth Round (см. сноску 10).

Таблица 3

Результаты анализа алгоритмов CRYSTALS-KYBER и HQC

Параметр	CRYSTALS-KYBER	HQC
Тип алгоритма	Основан на module-LWE	Основан на квазициклических кодах QC-MDPC
Реализация	Поддержка AVX2 для оптимизации, константное время выполнения	Оптимизированные версии на C и AVX2, константное время выполнения
Безопасность	IND-CCA2 безопасность Устойчивость к квантовым атакам	IND-CCA2 безопасность Устойчивость к квантовым атакам
Обновления	Увеличен параметр шума для Kyber512 Улучшена генерация матрицы A	Исправлены ошибки индексации
Аппаратная поддержка	Поддержка аппаратного AES/SHA-2 в «90s» варианте	Поддержка аппаратного Keccak (SHAKE)

Алгоритмы шифрования с открытым ключом

CRYSTALS-DILITHIUM. Это алгоритм цифровой подписи на основе решеток, базируется на парадигме Фиата-Шамира [16]. В его реализации используется кольцо $R_q := Z_q[X]/(X^{256}+1)$, где q — простое число $2^{23}–2^{13}+1$.

Открытый ключ формируется в виде выборки в формате Module-LWE $(A, t := As_1 + s_2)$, где A — матрица над R_q, а s_1 и s_2 — векторы ошибок над R_q.

В большинстве алгоритмов на решетках используется усеченное распределение Гаусса, DILITHIUM же применяет равномерное распределение на множестве $\{-\eta; -\eta+1; \ldots; \eta\}$, где η — небольшое положительное целое число.

CRYSTALS-DILITHIUM основан на подходе Любашевского «Фиат-Шамир с прерываниями» [20], использующем схему идентификации на решетках в три этапа. Доказывающий (prover) вычисляет вектор w содержащий старшие биты Ay (для случайного y), затем отправляет его. Проверяющий (verifier) отправляет случайный полином $c \in R_q$ с небольшими коэффициентами. Доказывающий отвечает ему вектором $z := y + cs_1$, но проблема в том, что z может содержать информацию о s_1, поэтому используется отбраковка (rejection sampling) и она гарантирует, что коэффициенты z имеют нужную величину. Проверяющий принимает подпись только, если $Az \approx w + ct$.

Преобразование Фиата-Шамира применяется для получения подписи. Отправитель генерирует значение путем хеширования обязательства w вместе с сообщением μ. В реальной схеме алгоритма используется несколько дополнений, главная из них — сжатие публичного ключа. Это происходит вследствие псевдослучайности и исключения больше половины младших битов t. Для компенсации этих битов доказывающая сторона предоставляет «подсказки» в составе каждой подписи, представляют собой некоторые условия, чтобы верификатор мог правильно выполнить описанную выше проверку.

FALCON. Это алгоритм на основе решеток, использует парадигму «хеширование и подпись». Также в его основе лежит GPV-фреймворк [21], он строит схемы подписи на решетках с функцией предварительной выборки прообразов. В данном алгоритме эффективно реализован GPV-подход для NTRU-решеток с акцентом на компактность пары (открытый ключ; подпись). В качестве секретного ключа используется набор многочленов $f, g, F, G \in Z[x]/(x^n+1)$, таких что $fG - gF \equiv q$, а в качестве открытого — $h \equiv g \cdot f^{-1}$. При корректной генерации h выглядит случайным, а матрицы

$$\begin{matrix} 1 & h \\ 0 & g \end{matrix} \text{ и } \begin{matrix} f & g \\ F & G \end{matrix}$$

порождают одну и ту же решетку.

Реализация FALCON достаточно сложная, алгоритм требует нетривиальных вычислений, в том числе вычисления с плавающей запятой и сложные структуры данных (FALCON-дерево). Из-за перечисленных факторов FALCON сложнее в реализации по сравнению с другими стандартизированными алгоритмами подписей на решетках, поэтому NIST в 2022 году рекомендовал продолжить работу по оптимизации реализации и по разработке методов проверки корректности реализации алгоритма.

Теоретическая безопасность алгоритма подтверждается доказательством устойчивости к подделкам в квантовой модели случайного оракула (QROM), основанным на сложности решения проблемы SIS (Short Integer Solution) в NTRU-решетках [22]. Как и в случае с CRYSTALS-DILITHIUM, безопасная реализация алгоритма FALCON требует защиты от атак по побочным каналам.

SPHINCS+. Это алгоритм цифровой подписи на основе хеш-функций без сохранения состояния. Его конструкция сочетает в себе применение одноразовых цифровых подписей, подписей, использующихся несколько раз, деревьев Меркла и гипердеревьев. Такой подход позволяет создать универсальную схему подписи, не требующую отслеживания состояния меж-

ду подписаниями. Алгоритм SPHINCS+ является усовершенствованной версией SPHINCS, предлагает повышенную безопасность и поддержку различных хеш-функций, включая SHA-256, SHAKE256 и Haraka.

WOTS+ (Winternitz One-Time Signature) — это один из основных компонентов алгоритма, одноразовая подпись, имеющая два параметра n — длина хеша в байтах и w — параметр Винтерница (обычно 4, 16 или 256). Длина подписи определяется по формуле

$$len = [\frac{8n}{log_2(w)}] + [\frac{log_2(len_1 \cdot (w-1))}{log_2(w)}] + 1 \quad ,$$

где $len_1 = [\frac{8n}{log_2(w)}]$.

Следующий важный компонент FORS (Forest of Random Subsets) — схема подписи для ограниченного числа сообщений. Он включает в себя k (количество деревьев) секретных значений и соответствующие пути аутентификации в k деревьях. $t = 2^a$ — количество листьев в каждом дереве (a — высота деерва).

HT (Hypertree) представляет собой иерархическую структуру из деревьев XMSS (расширенная схема Меркла), каждый слой HT подписывает корни деревьев следующего слоя, что обеспечивает масштабируемость и эффективность.

Закрытый ключ алгоритма формируется из двух основных компонентов: SK.seed —для генерации секретных ключей в схемах WOTS+ и FORS, SK.prf — для рандомизации подписей. Открытый ключ состоит из PK.root — корень гипердерева HT и основа для проверки подлинности подписей, и PK.seed — публичное начальное значение, используется при генерации масок для хеш-функций. Безопасность обеспечивается за счет комбинации секретных и публичных данных, где закрытый ключ отвечает за создание подписей, а открытый — за их верификацию.

Процесс создания подписи состоит из нескольких этапов, сначала генерируется случайное значение R при помощи функции $R = PRF_{msg}(SK.prf, OptRand, M)$, где $SK.prf$ берется из закрытого ключа, $OptRand$ — дополнительная случайная величина для повышения безопасности, M — сообщение. Затем сообщение хешируется при помощи функции $md = H_{msg}(R, PK.seed, PK.root, M)$. В результате получается хеш-значение md, оно разделяется на две части, которые используются для определения индексов в структурах FORS и гепердерева HT. Далее создается подпись FORS, которая включает в себя секретные значения и пути аутентификации, необходимые для проверки их подлинности. Алгоритм FORS подписывает часть хеш-значения md, используя секретные ключи из SK.seed. Завершающий этап — это создание подписи HT, здесь подписывается открытый ключ FORS с использованием гипердерева[14].

Производительность алгоритмов CRYSTALS-DILITHIUM, FALCON и SPHINCS+ при различных уровнях NIST, а также размеры секретного (СК)и открытого (ОК) ключей и цифровой подписи представлены в табл. 4. В алгоритме SPHINCS+ параметры подразделяются еще по типу оптимизации: s = «small» и f = «fast», такое разделение позволяет адаптировать алгоритм под разные прикладные задачи, где могут быть важны либо компактность подписей, либо быстродействие работы алгоритма.

Таблица 4

Производительность и размеры ключей *CRYSTALS*-DILITHIUM[15], FALCON[16] и SPHINCS+[17]

Параметр	Уровень NIST	Количество циклов (тыс)			Размер в байтах		
		Генерация ключа	Подписание	Проверка	СК	ОК18	Подпись
Falcon-512	I	21 445,3	829,1	144,1	7 553	897	666
SPHINCS+-128s	I	49 987,3	380 684,2	680,9	64	32	7 856
SPHINCS+-128f	I	792,5	18 642,1	1 719,8	64	32	17 088
dilithium-124	II	124	333	118,4	2 528	1 312	2 420
dilithium-186	III	256,4	529,1	179,4	4 000	1 952	3 293
SPHINCS+-192s	III	73 692,2	691 889,6	1 042,6	96	48	16 224
SPHINCS+-192f	III	1 159	30 949,2	2 369,8	96	48	35 664
dilithium-265	V	298,1	642,2	279,9	4 864	2 592	4 595
Falcon-1024	V	62 260,8	1 686,2	308,8	13 953	1 793	1 280
SPHINCS+-256s	V	49 145,6	623 454,8	1 367,4	128	64	29 792
SPHINCS+-256f	V	3 236,9	67 013,5	2 561,1	128	64	49 856

[14] SPHINCS+. Submission to the NIST post-quantum project, v.3.1 / Aumasson J., Daniel J. Bernstein and other // June 10, 2022, 63 pp. URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf (дата обращения: 12.09.2025).

[15] CRYSTALS-Dilithium. Algorithm Specifications and Supporting Documentation (Version 3.1). / Bai S., Ducas L. and other // Technical report February 8, 2021. URL: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf (дата обращения: 12.09.2025).

[16] Open Quantum Safe algorithm performance visualizations. URL: https://openquantumsafe.org/benchmarking/ (дата обращения 12.09.2025).

[17] Open Quantum Safe (см. сноску 16).

[18] Status Report on the Third Round (см. сноску 9).

Результаты сравнительного анализа алгоритмов CRYSTALS-DILITHIUM, FALCON и SPHINCS+ по различным параметрам (табл. 5) позволяют сделать следующие выводы:

CRYSTALS-DILITHIUM позволяет держать лучший баланс между скоростью и безопасностью, подойдет для систем с высокими требованиями к скорости;

FALCON создает самые компактные подписи из всех решетчатых алгоритмов, но сложен в реализации из-за арифметики с плавающей запятой, подходит для систем с ограничением по размеру подписей и для долгосрочной архивации;

SPHINCS+ единственный алгоритм с крайне большими подписями, но максимальной безопасностью на основе хешей, подходит для систем с нулевым доверием (Zero Trust) и устройств без постоянной памяти (например, одноразовые IoT-сенсоры).

Таблица 5

Результаты анализа алгоритмов CRYSTALS-DILITHIUM, FALCON и SPHINCS+

Параметр	CRYSTALS-DILITHIUM	FALCON	SPHINCS+
Тип алгоритма	Основан на решетках (module-LWE / SIS)	Основан на решетках (NTRU)	Основан на хеш-функциях (без сохранения состояния)
Реализация	Оптимизированный C / AVX2	C / AVX2 с FFT, плавающая запятая, сложная реализация	Оптимизированный C, константное время, большие подписи
Безопасность	IND-CCA2 безопасность Устойчивость к квантовым атакам, доказано в QROM	SUF-CMA безопасность Устойчивость к квантовым атакам, доказано в QROM	Устойчивость к квантовым атакам на основе хешей
Обновления	Улучшена генерация матрицы A, добавлены новые уровни безопасности	Исправлены ошибки в алгоритме сэмплирования, оптимизированы деревья	Добавлены новые параметры хеширования, улучшена производительность
Аппаратная поддержка	Поддержка аппаратного AES-NI/ SHA-2	FFT-оптимизации	Поддержка Keccak (SHA-3)

Выводы

Стремительное развитие квантовых технологий требует более надежных подходов к обеспечению безопасности. Разработка квантово-устойчивых решений, создание и реализация полностью квантовых моделей цифровых экосистем откроют новые возможности и способствуют усилению безопасности.

Анализ эталонных платформ различных компаний показал, что они не обладают достаточным уровнем защиты от новых видов угроз. Эти угрозы связаны с использованием квантовых вычислительных устройств, способных производить взлом традиционных алгоритмов за достаточно короткий промежуток времени, что ставит под угрозу все сферы нашей жизни. Поэтому необходимо заранее осуществить переход на защищенные алгоритмы, это позволит не только защитить конфиденциальную информацию, но и получить конкурентное преимущество перед другими странами.

В статье предложено две модели: модель взаимодействия элементов цифровой экосистемы и модель цифровой платформы, устойчивой к квантовым угрозам. Модель цифровой платформы демонстрирует комплексное решение проблемы, объединяет в себе алгоритмы пост-квантовой криптографии, элементы машинного обучения, защищенную архитектуру и автоматизированные механизмы управления рисками. Переход на алгоритмы, устойчивые к атакам квантовых компьютеров — это ключевое отличие представленной цифровой платформы от классических. Внедрение подобных решений требует пересмотра и внесения значительных изменений в ИТ-инфраструктуру, однако в будущем это необходимый этап трансформации.

Как перспективную задачу дальнейших исследований предлагается рассмотреть применение многоуровневой модели цифровой платформы для решения таких задач, как:

- проектирование и синтез квантово-безопасных платежных систем и защищенных блокчейн-платформ;
- проектирование и синтез цифровых экосистем для объектов критической информационной инфраструктуры;
- проектирование защищенных систем спутниковой связи.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение № 23—03 от 27.09.2024 г.)

Литература

1. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3(49). С. 2 — 22. DOI 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
2. Сухоручкина И.Н. Квантовые коммуникационные сети в инфраструктуре связи / И. Н. Сухоручкина // Россия: тенденции и перспективы развития: Ежегодник, Курск, 04 — 05 июня 2021 года. Том Выпуск 16. Часть 2. Москва: Институт научной информации по общественным наукам РАН, 2021. С. 407 — 415. EDN EMGRHT.
3. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18, № 2. P. 56 — 73. DOI 10.18721/JCSTCS.18205. EDN DCDMZF.
4. Венедюхин А.А. Пост-квантовая криптография и практика TLS в браузерах // Интернет изнутри. 2024. № 20. С. 26 — 30. EDN KIOKXY.
5. Васильева И.Н. Развитие квантовых технологий и квантовая угроза современной криптографии // Проблемы информационной безопасности в киберпространстве: Монография. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2024. С. 108 — 118. EDN MNORQF.
6. Еловская М.А. Кибербезопасность и защита данных: вызовы цифрового мира // Актуальные направления научных исследований XXI века: теория и практика. 2025. Т. 13, № 1(68). С. 117 — 127. DOI 10.34220/2308-8877-2025-13-1-117-127. EDN BZGJTP.
7. Курдюмов А.В., Свистунова Я.В. Теоретико - методологические основы формирования цифровых экосистем // Регион: системы, экономика, управление. 2024. № 3(66). С. 62 — 69. DOI 10.22394/1997-4469-2024-66-3-62-69. EDN FYDPWT.
8. Цифровые экосистемы / З.М. Казова, З.А. Иванов, Т.К. Татаров [и др.] // Инновационная экономика: информация, аналитика, прогнозы. 2024. № 2. С. 123 — 129. DOI 10.47576/2949-1894.2024.2.2.013. EDN CZOWMG.
9. Радкевич К.А. Архитектура цифровой платформы «умного» образования // Новые информационные технологии в телекоммуникациях и почтовой связи. 2021. № 1. С. 28 — 29. EDN: WLUHLJ.
10. Репина М.О. Развитие облачных технологий в России: архитектура решений и перспективы // Вопросы инновационной экономики. 2024. Т. 14, № 4. С. 1169-1190. DOI 10.18334/vinec.14.4.121856. EDN QTGBIH.
11. Азман А.В., Растамханов Р.Н., Цуканов И.Р. Аутентификация распределения квантовых ключей с помощью постквантовой криптографии // Известия Тульского государственного университета. Технические науки. 2023. № 1. С. 29 — 35. DOI 10.24412/2071-6168-2023-1-29-35. EDN: GBFOUZ.
12. Симоненкова Д.С., Велигура А.Н. Эталонные модели информационных систем, построенных с использованием технологий облачных вычислений // Безопасность информационных технологий. 2013. Т. 20, № 3. С. 28 — 32. EDN RTVBBP.
13. Скиба В.Ю., Петренко С.А., Мурзина А.А., Попова К.Р. Оценка квантовой устойчивости информационных систем таможенных органов Российской Федерации в современных условиях // Вестник Российской таможенной академии. 2024. № 4(69). С. 32 — 45. EDN: DCCFTC.
14. Поликарпов П.В., Уваров Н.К., Хомоненко А.Д. Экосистемы квантовых вычислений и перспективы использования их на транспорте // Интеллектуальные технологии на транспорте. 2021. №3(27). С. 52 — 60. DOI 10.24412/2413-2527-2021-327-52-60. EDN KQNVUN.
15. Комарова А.В., Коробейников А.Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. № 2(30). С. 58 — 68. DOI 10.21681/2311-3456-2019-2-58-68. EDN VVTEHN.
16. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решётках / Е.С. Малыгина, А.В. Куценко, С.А. Новоселов [и др.] // Дискретный анализ и исследование операций. 2023. Т. 30, № 4(158). С. 46 — 90. DOI 10.33048/daio.2023.30.771. EDN TYEMEK.
17. Lindner R., Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Kiayias A. (eds) Topics in Cryptology. CT-RSA 2011. CT-RSA 2011. Lect. Notes in Computer Science, vol 6558. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-19074-2_21.
18. Fujisaki E., Okamoto T. Secure integration of asymmetric and symmetric encryption schemes // J. of Cryptology. 2013. Vol. 26. P. 80 — 101. DOI: 10.1007/s00145-011-9114-1.
19. Saito T., Xagawa K., Yamakawa T. Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model. In: Nielsen, J., Rijmen, V. (eds) Advances in Cryptology — EUROCRYPT 2018 . EUROCRYPT 2018. Lecture Notes in Computer Science, V. 10822. Springer, Cham. DOI: 10.1007/978-3-319-78372-7_17.
20. Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In: Matsui, M. (eds) Advances in Cryptology — ASIACRYPT 2009. ASIACRYPT 2009. Lecture Notes in Computer Science, vol 5912. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-10366-7_35.
21. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions // Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing (STOC '08). Victoria, British Columbia, Canada, May 17—20, 2008. New York, NY, USA: Association for Computing Machinery, 2008. pp. 197 — 206. DOI: 10.1145/1374376.1374407.

22. Boneh D., Dagdelen Ö., Fischlin M., Lehmann A., Schaffner C., Zhandry M. Random Oracles in a Quantum World. In: Lee, D.H., Wang, X. (eds) Advances in Cryptology — ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, V. 7073. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-25385-0_3.
23. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на изогениях и кодах, исправляющих ошибки / Е.С. Малыгина, А.В. Куценко, С.А. Новоселов [и др.] // Дискретный анализ и исследование операций. 2024. Т. 31, № 1(159). С. 52 — 84. DOI 10.33048/daio.2024.31.772. EDN AXTBUU.

SECTION:
INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

MODEL OF A DIGITAL PLATFORM FOR ANALYSING RESILIENCE TO QUANTUM THREATS

Maria V. Larina, *research technician of Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Krasnodar region, Russian Federation. ORCID: 0009-0009-7826-0180.*
E-mail: larina.mv@talantiuspeh.ru

Vladimir Yu. Skiba, *Doctor of Technical Sciences, Senior Researcher, Chief Research Engineer at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius Federal Territory, Krasnodar region, Russian Federation. ORCID: 0000-0002-9805-7800.*
E-mail: skiba.vy@talantiuspeh.ru

Keywords: *cybersecurity, quantum supremacy, quantum resilience, post-quantum cryptography, threat monitoring, quantum-resilience authentication, conceptual platform model, encryption schemes, NIST PQC standards.*

Abstract

Purpose of work is to identify the weaknesses of digital platforms, taking into account the development of quantum technologies, and to develop a conceptual model of a digital platform that is resilience to quantum attacks.

Research methods: system analysis of modern platforms, classification, synthesis and integration of quantum-stable solutions, design of a digital platform with a multi-level architecture, comparative analysis of post-quantum cryptographic algorithms standardized by NIST. The model is based on the principles of adaptation to emerging challenges in the field of cybersecurity.

Results of the study: A model of interaction between elements of the digital ecosystem and a conceptual model of the platform are proposed, which includes a multi-level protection system based on post-quantum cryptography, quantum-resilience authentication and dynamic threat monitoring. The developed models can be used to describe specific information platforms in terms of the model, as well as to design new secure platforms in the financial sector, public administration, and critical information infrastructure. The results of a comparative analysis of the algorithms are presented CRYSTALS-KYBER, HQC, CRYSTALS-DILITHIUM, FALCON, and SPHINCS+ algorithms. The research results underscore the need for early adoption of post-quantum technologies to minimize risks.

Scientific novelty: the presented model of the digital platform demonstrates a comprehensive solution to the problem of ensuring quantum resilience through the integrated use of components that involve the use of post-quantum cryptography algorithms, machine learning elements and risk management mechanisms.

Practical significance: the developed models of the digital platform and interaction of elements of the digital ecosystem make it possible to solve such problems as the synthesis of quantum-resilience digital platforms and the analysis of the resilience of operation of digital platforms in the presence of quantum threats.

References

1. Petrenko A.S., Petrenko S.A. Metod ocenivanija kvantovoj ustojchivosti blokchejn-platform // Voprosy kiberbezopasnosti. 2022. № 3(49). S. 2 — 22. DOI 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
2. Suhoruchkina I.N. Kvantovye kommunikacionnye seti v infrastrukture svjazi / I. N. Suhoruchkina // Rossija: tendencii i perspektivy razvitija: Ezhegodnik, Kursk, 04 — 05 ijunja 2021 goda. Tom Vypusk 16. Chast' 2. Moskva: Institut nauchnoj informacii po obshhestvennym naukam RAN, 2021. S. 407 — 415. EDN EMGRHT.

3. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18, № 2. P. 56 — 73. DOI 10.18721/JCSTCS.18205. EDN DCDMZF.
4. Venedjuhin A.A. Post-kvantovaja kriptografija i praktika TLS v brauzerah // Internet iznutri. 2024. № 20. S. 26 — 30. EDN KIOKXY.
5. Vasil'eva I.N. Razvitie kvantovyh tehnologij i kvantovaja ugroza sovremennoj kriptografii // Problemy informacionnoj bezopasnosti v kiberprostranstve: Monografija. Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj jekonomicheskij universitet, 2024. S. 108 — 118. EDN MNORQF.
6. Elovskaja M.A. Kiberbezopasnost' i zashhita dannyh: vyzovy cifrovogo mira // Aktual'nye napravlenija nauchnyh issledovanij XXI veka: teorija i praktika. 2025. T. 13, № 1(68). S. 117 — 127. DOI 10.34220/2308-8877-2025-13-1-117-127. EDN BZGJTP.
7. Kurdjumov A.V., Svistunova Ja.V. Teoretiko - metodologicheskie osnovy formirovanija cifrovyh jekosistem // Region: sistemy, jekonomika, upravlenie. 2024. № 3(66). S. 62 — 69. DOI 10.22394/1997-4469-2024-66-3-62-69. EDN FYDPWT.
8. Cifrovye jekosistemy / Z.M. Kazova, Z.A. Ivanov, T.K. Tatarov [i dr.] // Innovacionnaja jekonomika: informacija, analitika, prognozy. 2024. № 2. S. 123 — 129. DOI 10.47576/2949-1894.2024.2.2.013. EDN CZOWMG.
9. Radkevich K.A. Arhitektura cifrovoj platformy «umnogo» obrazovanija // Novye informacionnye tehnologii v telekommunikacijah i pochtovoj svjazi. 2021. № 1. S. 28 — 29. EDN: WLUHLJ.
10. Repina M.O. Razvitie oblachnyh tehnologij v Rossii: arhitektura reshenij i perspektivy // Voprosy innovacionnoj jekonomiki. 2024. T. 14, № 4. S. 1169-1190. DOI 10.18334/vinec.14.4.121856. EDN QTGBIH.
11. Azman A.V., Rastamhanov R.N., Cukanov I.R. Autentifikacija raspredelenija kvantovyh kljuchej s pomoshh'ju post-kvantovoj kriptografii // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2023. № 1. S. 29 — 35. DOI 10.24412/2071-6168-2023-1-29-35. EDN: GBFOUZ.
12. 1Simonenkova D.S., Veligura A.N. Jetalonnye modeli informacionnyh sistem, postroennyh s ispol'zovaniem tehnologij oblachnyh vychislenij // Bezopasnost' informacionnyh tehnologij. 2013. T. 20, № 3. S. 28 — 32. EDN RTVBBP.
13. Skiba V.Ju., Petrenko S.A., Murzina A.A., Popova K.R. Ocenka kvantovoj ustojchivosti informacionnyh sistem tamozhennyh organov Rossijskoj Federacii v sovremennyh uslovijah // Vestnik Rossijskoj tamozhennoj akademii. 2024. № 4(69). S. 32 — 45. EDN: DCCFTC.
14. Polikarpov P.V., Uvarov N.K., Homonenko A.D. Jekosistemy kvantovyh vychislenij i perspektivy ispol'zovanija ih na transporte // Intellektual'nye tehnologii na transporte. 2021. №3(27). S. 52 — 60. DOI 10.24412/2413-2527-2021-327-52-60. EDN KQNVUN.
15. Komarova A.V., Korobejnikov A.G. Analiz osnovnyh sushhestvujushhih post-kvantovyh podhodov i shem jelektronnoj podpisi // Voprosy kiberbezopasnosti. 2019. № 2(30). S. 58 — 68. DOI 10.21681/2311-3456-2019-2-58-68. EDN VVTEHN.
16. Postkvantovye kriptosistemy: otkrytye voprosy i sushhestvujushhie reshenija. Kriptosistemy na reshjotkah / E.S. Malygina, A.V. Kucenko, S.A. Novoselov [i dr.] // Diskretnyj analiz i issledovanie operacij. 2023. T. 30, № 4(158). S. 46 — 90. DOI 10.33048/daio.2023.30.771. EDN TYEMEK.
17. Lindner R., Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Kiayias A. (eds) Topics in Cryptology. CT-RSA 2011. CT-RSA 2011. Lect. Notes in Computer Science, vol 6558. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-19074-2_21.
18. Fujisaki E., Okamoto T. Secure integration of asymmetric and symmetric encryption schemes // J. of Cryptology. 2013. Vol. 26. P. 80 — 101. DOI: 10.1007/s00145-011-9114-1.
19. Saito T., Xagawa K., Yamakawa T. Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model. In: Nielsen, J., Rijmen, V. (eds) Advances in Cryptology — EUROCRYPT 2018 . EUROCRYPT 2018. Lecture Notes in Computer Science, V. 10822. Springer, Cham. DOI: 10.1007/978-3-319-78372-7_17.
20. Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In: Matsui, M. (eds) Advances in Cryptology — ASIACRYPT 2009. ASIACRYPT 2009. Lecture Notes in Computer Science, vol 5912. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-10366-7_35.
21. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions // Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing (STOC '08). Victoria, British Columbia, Canada, May 17—20, 2008. New York, NY, USA: Association for Computing Machinery, 2008. pp. 197 — 206. DOI: 10.1145/1374376.1374407.
22. Boneh D., Dagdelen Ö., Fischlin M., Lehmann A., Schaffner C., Zhandry M. Random Oracles in a Quantum World. In: Lee, D.H., Wang, X. (eds) Advances in Cryptology — ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, V. 7073. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-25385-0_3.
23. Postkvantovye kriptosistemy: otkrytye voprosy i sushhestvujushhie reshenija. Kriptosistemy na izogenijah i kodah, ispravljajushhih oshibki / E.S. Malygina, A.V. Kucenko, S.A. Novoselov [i dr.] // Diskretnyj analiz i issledovanie operacij. 2024. T. 31, № 1(159). S. 52 — 84. DOI 10.33048/daio.2024.31.772. EDN AXTBUU.