О КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗВИТИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ

Ларина М.В.[1], Скиба В.Ю.[2]

Ключевые слова: *кибербезопасность, защита данных, угрозы, уязвимости, постквантовая криптография, национальная безопасность, квантовые информационные системы, гибридные информационные системы, кубиты.*

Аннотация

Цель работы *состоит в анализе и разработке уточненной классификации угроз безопасности информации для классических, гибридных и квантовых систем в условиях роста вычислительной мощности квантовых устройств.*

Методы исследования: *системный анализ* и классификация *существующих векторов атак и их влиянии на криптографическую стойкость, а также стратификация рисков по характеру воздействия и характеру возникновения с учетом архитектурных особенностей информационных систем.*

Результаты исследования: *предложена классификация угроз в виде таблицы, демонстрирующая специфические риски для трех типов информационных систем: классических, гибридных и квантовых. Установлено, что случайные угрозы, обусловленные шумами и ошибками измерений, требуют не меньшего внимания, чем преднамеренные атаки. Практическая значимость заключается в возможности использования полученной классификации для усовершенствования критической информационной инфраструктуры, повышению устойчивости государственных и коммерческих систем к серьезным киберугрозам, а также определению требований к информационным системам.*

Научная новизна: *сформирована уточненная классификация автоматизированных информационных систем (АИС) и выполнена стратификация угроз информационной безопасности в связи с развитием квантовых информационных технологий, при этом выделив два новых класса АИС: гибридные и квантовые АИС.*

Практическая значимость: *предложенная классификация АИС и стратификация угроз информационной безопасности с учетом появления новых квантовых угроз безопасности позволяет более точно оценить риски и сформировать комплексные требования к системам защиты информации перспективных информационных систем при синтезе квантово-устойчивых АИС, включая цифровые платформы и блокчейн-экосистемы, обеспечив тем самым заблаговременное внедрение квантовых алгоритмов, постквантовых алгоритмов, а также алгоритмов квантового распределения ключей.*

DOI: 10.24412/1994-1404-2026-1-00-01

Введение

По данным Gartner[3], в 2026 году на стратегию кибербезопасности будут влиять четыре мощных фактора: хаотичный рост ИИ, геополитическая напряженность, регуляторная турбулентность и ускоряющаяся эволюция угроз. Постквантовая криптография — не «когда-нибудь», а сейчас. К 2030 году квантовые вычисления могут сделать традиционную асимметричную криптографию небезопасной. Риск "harvest now, decrypt later" становится реальным.

Во многих передовых странах наблюдается появление новых научных программ, главной целью которых

[3] URL: https://resilienceforward.com/the-top-cyber-security-trends-for-2026-according-to-gartner/ (дата обращения: 12.03.2026).

[1] ***Ларина Мария Васильевна,*** *лаборант-исследователь Научного центра информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», пгт. 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, Научно-технологический университет «Сириус», пгт. Сириус, Краснодарский край, Российская Федерация, профессор кафедры ИБМ-6 МГТУ имени Н.Э. Баумана (НИУ)», г. Москва, Российская Федерация, профессор кафедры № 2 «Автоматика» НИЯИ МИФИ, г. Москва, Российская Федерация. ORCID: 0000-0002-9805-7800.*

E-mail: skiba.vy@talantiuspeh.ru

является совершенствование квантовых информационных технологий. Каждое государство стремится достичь превосходства в разработке квантовых вычислений [1].

Так, для решения задач по развитию квантовых технологий, в январе 2023 года учрежден Международный совет ассоциаций квантовой промышленности, в который вошли ассоциации следующих стран: США (The Quantum Economic Development Consortium), Канада (The Quantum Industry Canada), Япония (The Quantum Strategic Industry Alliance for Revolution) и Европейский консорциум (The Quantum Industry Consortium).

В Российской Федерации для развития квантовых технологий созданы:

- в 2020 году — консорциум «Национальная квантовая лаборатория», главной задачей которого является обеспечение глобальной конкурентоспособности российских квантовых технологий. К нему присоединились такие организации, как СП «Квант» (организация Госкорпорации Росатом), НИУ «ВШЭ», НИТУ «МИСиС», МФТИ (НИУ), Физический институт имени П.Н. Лебедева РАН, Российский квантовый центр и Фонд «Сколково»;
- в 2024 году — Квантовый консорциум предприятий и университетов по подготовке кадров в сфере квантовых информационных технологий, к которому присоединились Научно-технологический университет «Сириус» и Государственный университет «Дубна»;
- в 2025 году — сетевой Квантовый университет, соглашение о намерении создать который подписали ректоры МИФИ (НИУ), МФТИ (НИУ), НИТУ «МИСиС», МГТУ им. Н.Э. Баумана.

Проводятся исследования по созданию квантовых процессоров на базе сверхпроводников, холодных атомов, планируется запуск образовательных программ и стандартов подготовки специалистов. В 2021 году был представлен прототип на базе платформы из 20 ионов, в декабре 2024 года ученые Московского государственного университета и Российского квантового центра объявили о создании 50-кубитного ионного квантового компьютера, а в декабре 2025 года российские ученые Физического института имени П.Н. Лебедева РАН при поддержке госкорпорации Росатом создали 70-кубитный квантовый компьютер.

Таким образом, поддержка развития сферы квантовых технологий необходима для сохранения научного потенциала страны и обеспечения безопасности, важна для обеспечения технологического суверенитета и паритета в исследовании критически значимых инноваций. В то же время сто́ит подчеркнуть, что в процессе перехода к новой технологической эпохе в этой сфере появляются новые риски[4] для существующих криптографических средств защиты информации, что, в свою очередь, может угрожать информационной безопасности на национальном уровне [1—6].

В [1] предложена концепция обеспечения устойчивости функционирования цифровых платформ и блокчейн-экосистем в условиях появления квантовых угроз, предусматривающая комплексное применение различных методов и моделей, а также проведение исследований достигнутого уровня устойчивости. В соответствии с этой концепцией определена концептуальная модель квантовых угроз безопасности для DPiBE Российской Федерации на основе дополнения и развития известной методики оценки угроз безопасности ФСТЭК России и Матрицы тактики и приемов кибератак — MITRE Enterprise ATT&CK Matrix. При этом в [7] рассмотрена модель цифровой платформы, предусматривающая применение методов постквантовой криптографии (алгоритмы на решетках, протоколы распределенных ключей и хеш-функции) совместно с формальными методами проверки безопасности, элементами машинного обучения и автоматизированными механизмами управления рисками. В работах [8—11] приведены результаты исследований методов и моделей оценки устойчивости цифровых платформ и блокчейн-экосистем.

Решение задач по противодействию угрозам информационной безопасности необходимо выполнять как в рамках национальных систем предупреждения и нейтрализации угроз информационной безопасности, так и в рамках системы международной информационной безопасности[5]. В данной статье продолжены и обобщены результаты исследований, выполненных в [3, 4, 6, 12—16], которые позволили систематизировать угрозы информационной безопасности в связи с появлением квантовых угроз и уточнить классификацию автоматизированных информационных систем (далее — АИС) в условиях развития квантовых информационных технологий. Решение задачи стратификации угроз информационной безопасности в связи с развитием квантовых информационных технологий является одним из элементов комплексной технологии обеспечения устойчивости функционирования информационных систем, позволяющих на этапе проектирования (перепроектирования) конкретных информационных систем проактивно предусмотреть применение соответствующих механизмов защиты.

Позитивные и негативные аспекты развития квантовых технологий

Квантовые вычисления могут оказать значительное влияние на различные сферы жизнидеятельности. Одна из них, например, — разработка и внедрение квантовых систем искусственного интеллекта. Предпо-

[4] Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700 (дата обращения: 12.03.2026).

[5] Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия «Документоведение и архивоведение. Защита информации и информационная безопасность». 2016. № 1 (3). С. 54—72. EDN: WAIXQZ (дата обращения: 12.03.2026).

лагается, что машинный интеллект, созданный на базе квантового компьютера, будет способен выявлять более сложные закономерности, обрабатывать данные с экспоненциальной скоростью, выводить более точные прогнозы.

В январе 2024 года ученые Московского физико-технического института впервые запустили 12-кубитный квантовый процессор на основе сверхпроводников для квантового машинного обучения. Среднее время жизни кубита составило 14 микросекунд, время выполнения одной операции — около 50 наносекунд.

В декабре 2025 года[6] Физический институт имени П.Н. Лебедева Российской академии наук и корпорация «Росатом», ведущие совместный квантовый проект, в один день сообщили о достижении важного рубежа в этой перспективной области:

- представлен прототип 70-кубитного квантового компьютера на ионах иттербия. В рамках этого же эксперимента была продемонстрирована высокая точность операций: 1-кубитной — на уровне 99,98%, 2-кубитной — на уровне 96,1%;
- представлен прототип 70-кубитного квантового компьютера на ионах кальция, выполняющего 1- и 2-кубитные операции.

Таким образом, квантовые компьютеры способны быстро решать любые математические задачи и уже представляют серьезную угрозу для современных криптографических алгоритмов с открытым ключом [1, 4, 17, 18]. Высокая скорость работы обусловлена свойством квантового параллелизма — способностью кубитов пребывать во множестве различных «базисных» состояний одновременно. Осуществляется параллельная обработка 2^n возможных состояний, где n — количество кубитов.

Существующие квантовые алгоритмы, применение которых злоумышленниками может привести к нарушению безопасности информации или устойчивости функционирования информационных систем с криптографическими средствами защиты информации, можно классифицировать следующим образом.

1. Квантовые алгоритмы преобразований Фурье (алгоритм Шора и его модификации, алгоритм поиска периодичности, алгоритм квантовой оценки фазы и другие).

2. Квантовые алгоритмы моделирования квантовых систем (алгоритм Залки-Визнера, алгоритмы, основанные на квантовом отжиге, квантовые нейронные сети, квантовые машины опорных векторов и другие).

3. Алгоритмы квантового поиска (алгоритм Гровера и другие).

Питер Шор представил в 1994 году квантовый алгоритм факторизации, который производит разложение числа N при использовании O *(log N)* кубитов за время O $(log^3 N)$. В 2023 году американский ученый Одед Регев усовершенствовал алгоритм Шора и дополнил его методами многомерной криптографии. Он обобщил алгоритм на любое количество измерений, а не на два, как это было раньше. В обновленной версии квантовый компьютер использует гораздо меньше шагов для факторизации чисел. Но с появлением подобных алгоритмов становятся реальными такие угрозы, как взлом криптографических систем с открытым ключом, и другие уязвимости [17].

Алгоритм Гровера был разработан в 1996 году, он способен дать квадратичный выигрыш в решении задач перебора по сравнению с классическими методами и может быть эффективен в задачах криптоанализа. То есть решить уравнение $f(x) = y$ для логической функции f от n переменных можно за O $(N^{0,5})$ итераций (для сравнения: классический алгоритм перебора выполняется за O (N) итераций).

Через пару лет, в 1998 году, появился алгоритм Залки-Визнера, который направлен на моделирование унитарной динамики квантовой системы n частиц и позволяет решать уравнения Шредингера для сложных квантовых систем. Исследователи убеждены, что его применение возможно в квантовой химии и физике, так как алгоритм позволяет моделировать химические реакции, что в будущем, возможно, ускорит процесс создания новых лекарств и материалов.

Как отмечено в [6], результаты в области квантовой информатики наглядно демонстрируют высокий технологический потенциал квантовых технологий. Они также затрагивают проблему того, что криптографически релевантный квантовый компьютер может поставить под угрозу системы гражданской, военной связи, экономическую сферу страны, а также многие другие сферы деятельности.

В работах [2, 19] исследователи отмечают уязвимость блокчейн-технологий, поскольку квантовые компьютеры могут взломать текущие криптосистемы (например, ECDSA), что подчеркивает необходимость адаптации классификации информационных систем.

Алгоритмы совершенствуются и становятся эффективнее, это позволит открыть новые горизонты в различных сферах [20]. Но квантовые технологии могут быть использованы и в корыстных целях, их развитие может подорвать безопасность классических систем шифрования, в связи с чем возникнет необходимость перехода к новым стандартам[7]. Вышеперечисленные факты указывают на наличие реальных опасностей информационной безопасности в критически важных сферах.

Обзор угроз и уязвимостей квантовых, гибридных и классических информационных систем

Уязвимости АИС могут привести к негативным последствиям различного характера, например, таких

[6] URL: https://rg.ru/2025/12/18/rossijskie-uchenye-sozdali-70-kubitnyj-kvantovyj-kompiuter.html (дата обращения: 12.03.2026).

[7] Казарин О.В., Скиба В.Ю. Методология обеспечения проактивной безопасности компьютерных систем // Защита информации. Инсайд. 2013. № 2 (50). С. 52—60. EDN: TKJJVB (дата обращения: 12.03.2026).

Рис. 1. Уточненная классификация автоматизированных информационных систем в связи с развитием квантовых информационных технологий

как утечка конфиденциальной информации, захват аппаратных ресурсов, вывод системы из строя, которые, как следствие, могут вызвать различные техногенные или социальные катастрофы или нарушение устойчивости функционирования объектов критической инфраструктуры. В период с 1950-х до 1990-х годов обеспечение конфиденциальности информации было необходимо военным структурам и государственным учреждениям, средства защиты создавались в закрытых исследовательских организациях и находились под полным контролем спецслужб. Но в настоящее время с развитием информационных технологий и коммуникаций все изменилось, появилось больше уязвимостей, которые могут принести много вреда как обычным пользователям, так и серьезным государственным организациям [13].

При этом уже сейчас с учетом развития квантовых информационных технологий необходимо выделять три типа АИС: классические, гибридные и квантовые (рис. 1).

В начале 1950-х годов в Европе были созданы первые серийные компьютеры (Ferranti Mark), а к началу 60-х годов начали распространяться компьютерные преступления, главной целью которых являлся вывод компьютеров из строя и нелегальное проникновение в информационные системы. К 1970 г. насчитывалось более 120 000 электронно-вычислительных машин, в этот же период появились новые компьютерные вирусы, способствующие снижению производительности и отказу в обслуживании (вирус “Rabbit”, созданный в 1974 году). 1980-е и 1990-е года отличились высокими показателями по количеству громких атак и разработкой первых антивирусных сканеров. В этот же период времени началось развитие квантовых технологий, основанных на принципах квантовой механики[8].

Интернет стал доступен в 2000-е большему количеству пользователей, всё больше данных хранилось в цифровом виде, это открыло новые возможности использования уязвимостей злоумышленниками. АИС стали использоваться практически во всех сферах жизнедеятельности государства, общества и человека. С каждым годом киберпреступники развиваются и демонстрируют новые виды многовекторных атак, одновременно с этим совершенствуется сфера квантовых технологий, представляющая еще более серьезные угрозы для классических информационных систем.

В качестве основы для классификации таких АИС необходимо применять руководящие документы ФСТЭК России и ФСБ России. В рамках данной статьи будем рассматривать три подкласса:

- к1В — АИС без использования средств криптографической защиты информации (далее — СКЗИ);
- к1Б — АИС с использованием классических СКЗИ;
- к1А — АИС с использования СКЗИ, применяющие алгоритмы и методы постквантовой криптографии [21—25].

В качестве промежуточного этапа между традиционными и квантовыми АИС выступают гибридные информационные системы, сочетающие в себе элементы классических и квантовых вычислений. Ожидается, что это будут наиболее распространенные АИС. В гибридных АИС можно использовать преимущества разных типов кубитов, что позволяет добиться высокой точности и скорости квантовых процессов. Межуниверситетская квантовая сеть (МУКС) относится к данному типу информационных систем, объединяет ведущие университеты и научные организации в сфере квантовых технологий [26].

Необходимо выделить четыре типа гибридных АИС:

– АИС без использования СКЗИ;

АИС с использованием СКЗИ, предусматривающих квантовое распределение ключей [27];

[8] Dirac P.A.M. The principles of quantum mechanics. 4th ed. Oxford, 1958. P. 84.

Таблица 1

Типы гибридных АИС

№ п/п	Тип гибридной АИС	Характеристика гибридной АИС	Класс АИС
1	Без использования СКЗИ	В АИС для защиты информации не применяются криптографические механизмы. Квантовые регистры и вентили используются исключительно для обработки информации.	к2Г
2	С использованием СКЗИ, предусматривающих квантовое распределение ключей	Квантовые регистры и вентили используются как минимум для передачи криптографических ключей. Применяются классические СКЗИ, но для распределения криптографических ключей используются методы квантового распределения ключей. Быстрое обнаружение MITM-атаки («Человек посередине») [28].	к2В
3	С использованием СКЗИ, применяющих квантовые алгоритмы для генерации ключевой информации	Комбинация квантовых вентилей, квантовых регистров и управляющей электроники. Квантовые вентили отвечают за повороты, запутывание и измерение состояния кубитов. Квантовые регистры хранят кубиты и управляют ими. Управляющая электроника направляет поток информации к различным частям процессора. Кубиты используются для обработки информации, в том числе при генерации ключевой информации.	к2Б
4	С использованием СКЗИ, применяющих квантовые криптографические алгоритмы	Комбинация квантовых вентилей, квантовых регистров и управляющей электроники. Квантовые вентили отвечают за повороты, запутывание и измерение состояния кубитов. Квантовые регистры хранят кубиты и управляют ими. Управляющая электроника направляет поток информации к различным частям процессора. Кубиты используются для обработки информации, в том числе при генерации ключевой информации и при реализации квантовых криптографических алгоритмов.	к2А

– АИС с использованием СКЗИ, применяющих квантовые алгоритмы для генерации ключевой информации;
– АИС с использованием СКЗИ, применяющих квантовые криптографические алгоритмы.

Их характеристики представлены в табл. 1.

И, наконец, квантовые информационные системы — это новое направление в области вычислений, основанных на квантовой механике. В условиях роста угроз и недостаточности известных методов обеспечения безопасности, отказоустойчивости и надежности они также подвержены угрозам, которые связаны с квантовыми атаками. В то же время полностью квантовые АИС являются дальней перспективой, для их классификации в настоящее время предлагается ограничиться двумя подклассами:

– к3Б — АИС без использования СКЗИ;
– к3А — АИС с использованием квантовых СКЗИ.

Одними из основных направлений, где могут быть применены квантовые компьютеры, являются криптография и криптоанализ.

Квантовые вычислительные устройства работают на принципах квантовой механики, они могут осуществлять вычисления гораздо быстрее и эффективнее, чем обычные компьютеры. Данные факты вызывают интерес в научных сообществах и группах, различных предприятиях, привлекают внимание правительства.

Благодаря квантовым вычислениям станет возможным решение многих полезных для общества задач в медицине, аэродинамике, экономике и многих других сферах. Но что случится, если мощный квантовый компьютер попадет в руки злоумышленников? Они будут способны в короткие сроки взломать практически любую систему безопасности, что приведет к негативным последствиям, начиная с беспорядков в финансовой системе и заканчивая утечкой государственной тайны.

Авторы исследования [14] оценивают совокупную вероятность взлома RSA-2048 за 24 часа и рассуждают о реальности угроз для существующих информационных систем, в работе приведено сравнение мнений отечественных экспертов и экспертов канадского агентства Moody's. Канадские эксперты более обеспокоены данной проблемой и рекомендуют компаниям приступить к разработке стратегий защиты от квантовых угроз как можно раньше.

При этом необходимо хорошо понимать специфику и структуру угроз, поэтому предлагаем провести стратификацию угроз по характеру воздействия (активные

Таблица 2

Стратификация угроз безопасности информации в связи с возможностью применения злоумышленником квантовых компьютеров

Тип и класс АИС	Случайные угрозы	Преднамеренные угрозы	
		Пассивные	Активные
к3А, к3Б	Невыявленные ошибки при проектировании программного обеспечения; ошибки измерений; перепады температур; несоблюдение требований по эксплуатации квантового компьютера; скачки электропитания на технических средствах.	Появление специфичного для квантовых вычислителей вредоносного программного обеспечения; «ослепление» фотодетекторов мощным лазером; прослушивание и атака «человек посередине»; намеренный вызов случайных факторов; чтение конфиденциальных данных; PNS-атака.	Атаки типа «отказ в обслуживании»; кража конфиденциальной информации и результатов вычислений; атаки на квантовый Интернет; атаки на облачную инфраструктуру.
к2А, к2Б, к2В, к2Г	Невыявленные ошибки при проектировании программного обеспечения; скачки электропитания на технических средствах.	Прослушивание и атака «человек посередине»; намеренный вызов случайных факторов; чтение конфиденциальных данных; сбор метаданных.	Вывод из строя средств защиты информации; атаки на каналы передачи информации.
к1А, к1Б, к1В	Невыявленные ошибки при проектировании программного обеспечения; старение носителей информации; скачки электропитания на технических средствах.	Намеренный вызов случайных факторов; чтение конфиденциальных данных и тихий мониторинг трафика.	Быстрый взлом классических методов криптографии и шифрования, криптографических ключей; вывод из строя средств защиты информации; ускоренный поиск.

и пассивные) и природе возникновения (случайные и преднамеренные) для трех типов АИС (табл. 2).

Рассмотрим более подробно угрозы безопасности информации, которые могут возникнуть среди прочего при воздействии злоумышленника с применением квантовых компьютеров на различные АИС.

Случайные угрозы не связаны с целенаправленными действиями злоумышленников и происходят в случайный момент времени. К таким угрозам относится старение носителей информации, вследствие чего ухудшается качество данных, повреждаются файлы. Не выявленные при проектировании программного обеспечения ошибки могут возникать на этапе системного анализа или при разработке модификаций программ. Резкие перепады сетевого напряжения, которые выходят за пределы допустимых значений, также являются угрозой для стабильной работы информационных систем. Они могут возникать из-за аварийных состояний, перегрузки сети или же природных явлений.

Для квантовых компьютеров появляются новые виды случайных уязвимостей, которые могут повлиять на их работу. Одна из основных проблем — это чувствительность к внешнему воздействию. На функционирование кубитов могут повлиять даже слабые электромагнитные помехи, вследствие чего будут получены ошибочные вычисления. Чтобы минимизировать подобные ошибки, создаются сложные системы охлаждения и контроля состояния окружающей среды, кубиты охлаждают до температур, близких к абсолютному нулю (-273,15 °С). Поведение частиц при более высоких температурах предсказать затруднительно, что мешает проводить вычисления при таком энергичном состоянии кубитов. Кроме того, критически важно соблюдение всех требований по эксплуатации квантовых компьютеров: отсутствие контроля за условиями работы может привести к снижению общей производительности системы. Шумы в системе и декогеренция провоцируют появление ошибок при измерении состояния кубитов — случайных изменений квантовых состояний. Для их выявления применяют коды коррекции ошибок, которые вносят необходимые правки и сохраняют состояние суперпозиции.

Преднамеренные угрозы, связанные с неправомерными действиями злоумышленников, подразделяются на активные и пассивные.

Задачей активных уязвимостей является нарушение стабильного функционирования системы, ее структуры или состава посредством целенаправленного воздействия на информационные ресурсы. Для классических АИС квантовые вычислительные устройства представляют наибольшую опасность, угрозу информационной безопасности на глобальном уровне. Ученые предполагают, что в ближайшие пять лет квантовые компьютеры смогут превзойти классические компьютеры архитектуры фон Неймана в области решения задач криптоанализа, в том числе распространенную

систему асимметричного шифрования RSA. Ожидается, что в ближайшее время они смогут эффективно взламывать RSA с минимальной рекомендуемой международными стандартами длиной ключа 2048 битов. Новые устройства будут способны взламывать криптоалгоритмы, которые сейчас вполне устойчивы к атакам с применением обычных компьютеров и даже распределенных вычислительных сетей. В конце прошлого столетия были разработаны алгоритмы Шора и Гровера, минимизирующие стойкость асимметричных и симметричных систем шифрования, широко используемых сейчас. Алгоритм Гровера позволяет осуществлять поиск в неструктурированных данных гораздо быстрее по сравнению с классическими алгоритмами, что может угрожать системам, использующим простые методы аутентификации.

Гибридные АИС и используемые ими алгоритмы также могут быть подвержены угрозам. Для защищенного обмена данными необходимо наличие общего ключа между любой парой узлов, поэтому возникает необходимость передачи квантового ключа через несколько сегментов, называемых промежуточными доверенными узлами. У таких узлов есть существенный недостаток — появление ключа в открытом виде на каждом доверенном узле. Соответственно, необходимо обеспечить защиту аппаратуры от злоумышленников, поскольку на доверенном узле имеются квантовые ключи от соседних сегментов сети, соединенных с данным узлом. Для стабильной работы гибридных информационных сетей важно разрабатывать и использовать различные способы передачи данных, проводить мониторинг сети и управлять ключами, чтобы гарантировать безопасность передаваемой информации. Для минимизации рисков, связанных с доверенными узлами, целесообразно также использовать модели взаимодействия с выделенным модулем квантово-устойчивой аутентификации [7].

Проанализировав основные киберугрозы, связанные с квантовыми технологиями, можно заметить, что квантовые вычислительные системы имеют свои уязвимости. К активным угрозам можно отнести атаки типа «отказ в обслуживании» (DoS), при которых злоумышленники создают помехи, искажая данные. Кража ценных результатов квантовых вычислений и конфиденциальной информации — это еще одна уязвимость. По данным специалистов Positive Technologies и Qapp, программное обеспечение для квантовых вычислений имеет уязвимости высокого уровня опасности, две из которых были зафиксированы (CVE-2018-20225 и CVE-2023-36632). С развитием облачного формата ресурсов квантовых технологий у нарушителей появится мотивация к проведению атак на компании, которые поставляют облачные продукты.

Заключительный вид угроз — пассивные. Они никак не нарушают нормальную работу системы, но зачастую бывают более опасными, так как происходят без внесения видимых изменений в информационные журналы. Для классических информационных систем квантовые компьютеры могут осуществлять намеренный вызов случайных факторов, таких как сбои в работе, шумы и фоны в каналах связи, перебои с электричеством и др. Они также способны к быстрому взлому алгоритмов, что представляет угрозу для закодированных сведений и конфиденциальных данных, и тихому мониторингу трафика. К пассивным угрозам для гибридных систем можно отнести сбор метаданных о взаимодействиях в системе, злоумышленники могут отслеживать IP-адреса пользователей для дальнейшего планирования наступлений.

Атаки типа «человек посередине» (MITM-атаки, атаки на протокол аутентификации) могут проводиться для всех типов информационных систем. Суть подобных атак в том, что нарушитель с высокой точностью копирует один из узлов, старается выполнять все его функции и при этом остаться незамеченным. Сейчас расстояние между узлами квантовых сетей не превышает нескольких сотен километров, при условии, что используются наземные системы передачи данных. Поэтому для широкого использования квантовых технологий необходимо создание дополнительных промежуточных точек, которые могут стать уязвимым местом для MITM-атак. При передаче квантовых ключей между каждой парой узлов в момент их доставки доверенными узлами узел, который маскируется под легитимный, может стать получателем информации. Чтобы увеличить количество взломанных узлов, злоумышленники атакуют все доверенные узлы в определенном сегменте сети в один момент времени.

Большое расстояние между узлами квантовых сетей и помехи пока делают невозможной передачу единичных фотонов. Их количество стараются минимизировать, но в теории у нарушителей появляется возможность перехватить один фотон, считать его состояние и остальные отправить получателю. Атаки с расщеплением по числу фотонов называют PNS-атаками (Photon Number Splitting) в системах квантового распределения ключей. Отделенный фотон нарушитель сохраняет в квантовой памяти и измеряет его, но перед измерением ему нужно дождаться согласования базисов протокола квантового распределения ключей. В это время отправитель и получатель публично делятся использованными для каждого фотона базисами, что позволяет злоумышленнику измерить его без внесения ошибок, которые могли бы быть замечены.

Ослепление фотодетекторов лазером сильной мощности — это атака, позволяющая нарушителям искажать данные в системах квантового распределения ключей. Однотонный детектор получателя засвечивается лучом лазера, а затем перехватывается хакерами.

Выводы

Проведенные исследования позволили сформировать уточненную классификацию АИС и выполнить стратификацию угроз информационной безопасности в связи с развитием квантовых информационных тех-

нологий, выделив два новых класса АИС: гибридные и квантовые АИС.

Предложенная классификация АИС и стратификация угроз информационной безопасности позволяет более точно оценить риски и сформировать комплексные требования к системам защиты информации перспективных информационных систем при синтезе квантово-устойчивых АИС, включая цифровые платформы и блокчейн-экосистемы, обеспечив тем самым заблаговременное внедрение квантовых алгоритмов, постквантовых алгоритмов, а также алгоритмов квантового распределения ключей.

Как перспективные направления дальнейших исследований необходимо рассматривать применение многоуровневой модели цифровой платформы и предложенной системы стратификации при решении таких задач, как:

- проектирование и синтез квантово-безопасных платежных систем и защищенных блокчейн-платформ;
- проектирование и синтез цифровых экосистем для объектов критической информационной инфраструктуры;
- разработка методов, алгоритмов и средств проведения сертификационных испытаний, тематических испытаний или оценку устойчивости как проектируемых, так и модернизируемых информационных систем различного назначения.

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 от 27.09.2024 г. № 23—03).

Литература

1. 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.
2. 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.
3. Васильева И.Н. Развитие квантовых технологий и квантовая угроза современной криптографии // Проблемы информационной безопасности в киберпространстве : монография. СПб. : Санкт-Петербургский государственный экономический университет, 2024. С. 108—118. EDN: MNORQF.
4. 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.
5. Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity // Computing, Telecommunications and Control. 2024. Vol. 17. № 4. Pp. 16–34. DOI: 10.18721/JCSTCS.17402. EDN: TFFIFM.
6. Скиба В.Ю., Петренко С.А., Мурзина А.А., Попова К.Р. Новые виды угроз информационным системам в сфере внешнеэкономической деятельности // Вестник Российской таможенной академии. 2025. № 1 (70). С. 82—97. EDN: AEKVPB.
7. Ларина М.В., Скиба В.Ю. Модель цифровой платформы для анализа устойчивости к квантовым угрозам // Правовая информатика. 2025. № 3. С. 12—26. DOI: 10.24412/1994-1404-2025-3-00-02. EDN: NDONZQ.
8. Сундеев П.В. Метод оценки выполнения нормативных требований к защите информации // Правовая информатика. 2025. № 4. С. 4—15. DOI: 10.24412/1994-1404-2025-4-4-15. EDN: DSWFHY.
9. Ищукова Е.А. О влиянии криптографической стойкости функций хеширования на устойчивость современных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 3 (67). С. 63—71. DOI: 10.21681/2311-3456-2025-3-63-71. EDN: UUSWXP.
10. 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.
11. Ishchukova E.A., Petrenko S.A., Gnidko K.O., Nekrasov A.V. Potential Vulnerabilities of Cryptographic Primitives in Modern Blockchain Platforms // Sci. 2025. Vol. 7. No. 3. DOI: 10.3390/sci7030112. EDN: EJABCF.
12. Данеев О.В. О проблеме квантового распределения ключей: состояние и перспективы // Хроноэкономика. 2020. № 2 (23). С. 19—23. EDN: DPWLHE.
13. 13. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems // Journal of Information Security and Applications. 2021. T. 58. P. 102717. DOI: 10.1016/j.jisa.2020.102717.
14. Лукашев А.В., Шабуня В.В., Сарафанников В.С. [и др.] Тенденции повышения уязвимости современных информационных систем со стороны квантовых компьютеров // Известия Тульского государственного университета. Технические науки. 2023. № 11. С. 324—331. DOI: 10.24412/2071-6168-2023-11-324-325. EDN: ISPHEC.

15. 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.
16. Ларина М.В., Скиба В.Ю. Уточнение классификации информационных систем и угроз в условиях развития квантовых технологий // Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства : материалы XII Межд. науч.-практ. конф., Ялта, 26–29 марта 2025 г. Симферополь: ООО «Изд-во Типография «Ариал», 2025. С. 182—184. EDN: CDFVGN.
17. Петренко А.С., Романченко А.М. Перспективный метод криптоанализа на основе алгоритма Шора // Защита информации. Инсайд. 2020. № 2 (92). С. 17—23. EDN: BAFYOW.
18. Петренко А.С. Обоснование необходимости разработки постквантовых алгебраических алгоритмов ЭЦП с двумя скрытыми группами // The 2026 Symposium on Cybersecurity of the Digital Economy–CDE'26: Сборник статей X Межд. науч.-практ. конф., Иннополис, 21–23 января 2026 г. СПб. : Университет Иннополис, 2026. С. 98—107. EDN: XBTKDH.
19. Saha B., Hasan M.M. et al. Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures // arXiv preprint arXiv: 2306.11884. 2023.
20. 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.
21. Венедюхин А.А. Пост-квантовая криптография и практика TLS в браузерах // Интернет изнутри. 2024. № 20. С. 26—30. EDN: KIOKXY.
22. Азман А.В., Растамханов Р.Н., Цуканов И.Р. Аутентификация распределения квантовых ключей с помощью пост-квантовой криптографии // Известия Тульского государственного университета. Технические науки. 2023. № 1. С. 29—35. DOI: 10.24412/2071-6168-2023-1-29-35. EDN: GBFOUZ.
23. 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.
24. Малыгина Е.С., Куценко А.В., Новоселов С.А. [и др.] Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решётках // Дискретный анализ и исследование операций. 2023. Т. 30. № 4 (158). С. 46—90. DOI: 10.33048/daio.2023.30.771. EDN: TYEMEK.
25. Малыгина Е.С., Куценко А.В., Новоселов С.А. [и др.] Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на изогениях и кодах, исправляющих ошибки // Дискретный анализ и исследование операций. 2024. Т. 31. № 1 (159). С. 52—84. DOI: 10.33048/daio.2024.31.772. EDN: AXTBUU.
26. Шабанов Б.М., Овсянников А.П. О проекте межуниверситетской квантовой сети // Программные продукты и системы. 2023. № 4. С. 695—702. DOI: 10.15827/0236-235X.144.695-702. EDN: BXQDAA.
27. Сухоручкина И.Н. Квантовые коммуникационные сети в инфраструктуре связи // Россия: тенденции и перспективы развития : ежегодник, Курск, 4—5 июня 2021 г. Том Выпуск 16. Часть 2. М. : ИНИОН РАН, 2021. С. 407—415. EDN: EMGRHT.
28. Есмагамбетова Г., Актаева А., Кубигенова А. [и др.] Многофакторная аутентификация с использованием биометрических данных с квантовыми вычислениями // International Journal of Open Information Technologies. 2024. Т. 12. № 5. С. 166—176. EDN: EBMDSF.

SECTION:
INFORMATION PROTECTION METHODS AND SYSTEMS

ON THE CLASSIFICATION OF THREATS TO INFORMATION SYSTEMS IN THE CONTEXT OF THE DEVELOPMENT OF QUANTUM TECHNOLOGIES

Maria V. Larina[9], Vladimir Yu. Skiba[10]

[9] ***Maria V. Larina,*** *Research Technician at the Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius, Krasnodar region, Russian Federation. ORCID: 0009-0009-7826-0180.*
E-mail: larina.mv@talantiuspeh.ru

[10] ***Vladimir Yu. Skiba,*** *Dr.Sc. (Technology), Senior Researcher, Principal Research Engineer at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius, Krasnodar region, Russian Federation, Professor at the IBM-6 Department, Bauman Moscow State Technical University, Moscow, Russian Federation, Professor at Department № 2 "Automation", National Research Nuclear University MEPhI, Moscow, Russian Federation. ORCID: 0000-0002-9805-7800.*
E-mail: skiba.vy@talantiuspeh.ru

Keywords: *cybersecurity, data security, threats, vulnerabilities, post-quantum cryptography, national security, quantum information systems, hybrid information systems, qubits.*

Abstract

Purpose of work *is to analyze and develop a refined classification of information security threats for classical, hybrid, and quantum systems in the context of increasing the computational power of quantum devices.*

Research methods: *system analysis and classification of existing attack vectors and their impact on cryptographic resistance, as well as risk stratification based on the nature of impact and origin, taking into account the architectural features of information systems.*

Results of the study: *a classification of threats is proposed in the form of a table, demonstrating specific risks for three types of information systems: classical, hybrid, and quantum. It is established that random threats, caused by noise and measurement errors, require no less attention than intentional attacks. The practical significance lies in the possibility of using the obtained classification to improve critical information infrastructure, increase the resilience of government and commercial systems to serious cyber threats, and determine the requirements for information systems.*

Scientific novelty: *a refined classification of automated information systems has been developed, and the stratification of information security threats has been performed in connection with the development of quantum information technologies, resulting in the identification of two new classes of automated information systems: hybrid and quantum automated information systems.*

Practical significance: *the proposed classification of automated information systems and the stratification of information security threats, taking into account the emergence of new quantum security threats, allows for a more accurate assessment of risks and the formulation of comprehensive requirements for information protection systems in advanced information systems during the synthesis of quantum-resistant automated information systems, including digital platforms and blockchain ecosystems, thereby ensuring the timely implementation of quantum algorithms, post-quantum algorithms, and quantum key distribution algorithms.*

References

1. 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. No. 2. P. 56–73. DOI: 10.18721/JCSTCS.18205. EDN: DCDMZF.
2. Petrenko A.S., Petrenko S.A. Metod otsenivaniia kvantovoi ustoichivosti blokchein-platform // Voprosy kiberbezopasnosti. 2022. No. 3 (49). S. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
3. Vasil'eva I.N. Razvitie kvantovykh tekhnologii i kvantovaia ugroza sovremennoi kriptografii // Problemy informatsionnoi bezopasnosti v kiberprostranstve : monografiia. SPb. : Sankt-Peterburgskii gosudarstvennyi ekonomicheskii universitet, 2024. S. 108–118. EDN: MNORQF.
4. Skiba V.Iu., Petrenko S.A., Murzina A.A., Popova K.R. Otsenka kvantovoi ustoichivosti informatsionnykh sistem tamozhennykh organov Rossiiskoi Federatsii v sovremennykh usloviiakh // Vestnik Rossiiskoi tamozhennoi akademii. 2024. No. 4 (69). S. 32–45. EDN: DCCFTC.
5. Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity // Computing, Telecommunications and Control. 2024. Vol. 17. No. 4. Pp. 16–34. DOI: 10.18721/JCSTCS.17402. EDN: TFFIFM.
6. Skiba V.Iu., Petrenko S.A., Murzina A.A., Popova K.R. Novye vidy ugroz informatsionnym sistemam v sfere vneshneekonomicheskoi deiatel'nosti // Vestnik Rossiiskoi tamozhennoi akademii. 2025. No. 1 (70). S. 82–97. EDN: AEKVPB.
7. Larina M.V., Skiba V.Iu. Model' tsifrovoi platformy dlia analiza ustoichivosti k kvantovym ugrozam // Pravovaia informatika. 2025. No. 3. S. 12–26. DOI: 10.24412/1994-1404-2025-3-00-02. EDN: NDONZQ.
8. Sundeev P.V. Metod otsenki vypolneniia normativnykh trebovanii k zashchite informatsii // Pravovaia informatika. 2025. No. 4. S. 4–15. DOI: 10.24412/1994-1404-2025-4-4-15. EDN: DSWFHY.
9. Ishchukova E.A. O vliianii kriptograficheskoi stoikosti funktsii kheshirovaniia na ustoichivost' sovremennykh blokchein-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 3 (67). S. 63–71. DOI: 10.21681/2311-3456-2025-3-63-71. EDN: UUSWXP.
10. Petrenko A.S., Petrenko S.A. Metod otsenivaniia kvantovoi ustoichivosti blokchein-platform // Voprosy kiberbezopasnosti. 2022. No. 3 (49). S. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
11. Ishchukova E.A., Petrenko S.A., Gnidko K.O., Nekrasov A.V. Potential Vulnerabilities of Cryptographic Primitives in Modern Blockchain Platforms // Sci. 2025. Vol. 7. No. 3. DOI: 10.3390/sci7030112. EDN: EJABCF.
12. Daneev O.V. O probleme kvantovogo raspredeleniia kliuchei: sostoianie i perspektivy // Khronoekonomika. 2020. No. 2 (23). S. 19–23. EDN: DPWLHE.

13. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems // Journal of Information Security and Applications. 2021. T. 58. P. 102717. DOI: 10.1016/j.jisa.2020.102717.
14. Lukashev A.V., Shabunia V.V., Sarafannikov V.S. [i dr.] Tendentsii povysheniia uiazvimosti sovremennykh informatsionnykh sistem so storony kvantovykh komp'iuterov // Izvestiia Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2023. No. 11. S. 324–331. DOI: 10.24412/2071-6168-2023-11-324-325. EDN: ISPHEC.
15. Elovskaia M.A. Kiberbezopasnost' i zashchita dannykh: vyzovy tsifrovogo mira // Aktual'nye napravleniia nauchnykh issledovanii XXI veka: teoriia i praktika. 2025. T. 13. No. 1(68). S. 117–127. DOI: 10.34220/2308-8877-2025-13-1-117-127. EDN: BZGJTP.
16. Larina M.V., Skiba V.Iu. Utochnenie klassifikatsii informatsionnykh sistem i ugroz v usloviiakh razvitiia kvantovykh tekhnologii // Ekonomika ustoichivogo razvitiia regiona: innovatsii, finansovye aspekty, tekhnologicheskie draivery razvitiia v sfere turizma i gostepriimstva : materialy KhII Mezhd. nauch.-prakt. konf., Ialta, 26–29 marta 2025 g. Simferopol': OOO "Izd-vo Tipografiia "Arial", 2025. S. 182–184. EDN: CDFVGN.
17. Petrenko A.S., Romanchenko A.M. Perspektivnyi metod kriptoanaliza na osnove algoritma Shora // Zashchita informatsii. Insaid. 2020. No. 2 (92). S. 17–23. EDN: BAFYOW.
18. Petrenko A.S. Obosnovanie neobkhodimosti razrabotki postkvantovykh algebraicheskikh algoritmov ETsP s dvumia skrytymi gruppami // The 2026 Symposium on Cybersecurity of the Digital Economy–CDE'26: Sbornik statei X Mezhd. nauch.-prakt. konf., Innopolis, 21–23 ianvaria 2026 g. SPb. : Universitet Innopolis, 2026. S. 98–107. EDN: XBTKDH.
19. Saha B., Hasan M.M. et al. Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures // arXiv preprint arXiv: 2306.11884. 2023.
20. Polikarpov P.V., Uvarov N.K., Khomonenko A.D. Ekosistemy kvantovykh vychislenii i perspektivy ispol'zovaniia ikh na transporte // Intellektual'nye tekhnologii na transporte. 2021. No. 3 (27). S. 52–60. DOI: 10.24412/2413-2527-2021-327-52-60. EDN: KQNVUN.
21. Venediukhin A.A. Post-kvantovaia kriptografiia i praktika TLS v brauzerakh // Internet iznutri. 2024. No. 20. S. 26–30. EDN: KIOKXY.
22. Azman A.V., Rastamkhanov R.N., Tsukanov I.R. Autentifikatsiia raspredeleniia kvantovykh kliuchei s pomoshch'iu post-kvantovoi kriptografii // Izvestiia Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2023. No. 1. S. 29–35. DOI: 10.24412/2071-6168-2023-1-29-35. EDN: GBFOUZ.
23. Komarova A.V., Korobeinikov A.G. Analiz osnovnykh sushchestvuiushchikh post-kvantovykh podkhodov i skhem elektronnoi podpisi // Voprosy kiberbezopasnosti. 2019. No. 2 (30). S. 58–68. DOI: 10.21681/2311-3456-2019-2-58-68. EDN: VVTEHN.
24. Malygina E.S., Kutsenko A.V., Novoselov S.A. [i dr.] Postkvantovye kriptosistemy: otkrytye voprosy i sushchestvuiushchie resheniia. Kriptosistemy na reshetkakh // Diskretnyi analiz i issledovanie operatsii. 2023. T. 30. No. 4 (158). S. 46–90. DOI: 10.33048/daio.2023.30.771. EDN: TYEMEK.
25. Malygina E.S., Kutsenko A.V., Novoselov S.A. [i dr.] Postkvantovye kriptosistemy: otkrytye voprosy i sushchestvuiushchie resheniia. Kriptosistemy na izogeniiakh i kodakh, ispravliaiushchikh oshibki // Diskretnyi analiz i issledovanie operatsii. 2024. T. 31. No. 1 (159). S. 52–84. DOI: 10.33048/daio.2024.31.772. EDN: AXTBUU.
26. Shabanov B.M., Ovsiannikov A.P. O proekte mezhuniversitetskoi kvantovoi seti // Programmnye produkty i sistemy. 2023. No. 4. S. 695–702. DOI: 10.15827/0236-235X.144.695-702. EDN: BXQDAA.
27. Sukhoruchkina I.N. Kvantovye kommunikatsionnye seti v infrastrukture sviazi // Rossiia: tendentsii i perspektivy razvitiia : ezhegodnik, Kursk, 4–5 iiunia 2021 g. Tom Vypusk 16. Chast' 2. M. : INION RAN, 2021. S. 407–415. EDN: EMGRHT.
28. Esmagambetova G., Aktaeva A., Kubigenova A. [i dr.] Mnogofaktornaia autentifikatsiia s ispol'zovaniem biometricheskikh dannykh s kvantovymi vychisleniiami // International Journal of Open Information Technologies. 2024. T. 12. No. 5. S. 166–176. EDN: EBMDSF.