УДК 336.71

КВАНТОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ БАНКОВСКОГО БИЗНЕСА

Анна Сергеевна АВЕРИНА[1,2], соискатель

[1]Агентство по страхованию вкладов, Москва, Россия

[2]Автономная некоммерческая организация высшего образования «Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Российская Федерация

Адрес для корреспонденции: Аверина А.С., 191023, Санкт-Петербург, Невский пр., 60.

Аннотация

Цель исследования: Привлечение внимания к проблеме потери персональных данных, ценных активов в цифровой банковской бизнес-среде, а также поиск направлений усиления кибербезопасности цифрового периметра в условиях развития квантовых технологий.

Методология исследования основана на изучении научной и специализированной литературы, анализ которой позволит по-новому взглянуть на квантовые технологии с позиции внедрения в систему безопасности и подготовить теоретическую основу для активизации исследований в данном направлении. В работе были использованы общенаучные методы аналогии, обобщения, логического анализа, систематизации, которые позволили определить роль квантовых технологий в условиях расширения цифрового банковского пространства.

Результаты исследования: Проведен обзор квантовых достижений за последние 10 лет, в которых прослеживаются следующие основные тренды: квантовые вычисления, квантовые коммуникации и сети, квантовые сенсоры и метрологии. Оценка полученных результатов по разработке квантов доказала, что мир приблизился к квантовому переходу и необходимо успевать за будущими изменениями. Точечные успехи отдельных стран и компаний в квантовой тематике накапливаются и будут трансформироваться к широкому применению. Россия участвует в квантовой международной конкуренции и стремится выстроить квантово-устойчивые коммуникационные сети.

Выводы: Предложена схема построения квантово-защищенной коммуникационной сети обмена информационными потоками в цифровом пространстве финансового рынка. Есть проблема невозможности проведения квантовых и информационных потоков по одному каналу.

Оригинальность: Исследование позволяет сфокусировать внимание на происходящих изменениях в информационном пространстве и акцентировать внимание на необходимости поиска решений по усилению защиты цифровых активов банков квантовыми технологиями.

Ключевые слова

квантовая угроза, информационное пространство, банковские операции, защиты периметра, безопасность данных, цифровые активы

Для цитирования: Аверина А.С. Квантовые угрозы безопасности банковского бизнеса // Ученые записки Международного банковского института. 2021. № 1(51). С. 9–21.

5.2.4. Finance

UDC 336.71

QUANTUM THREATS TO THE SECURITY OF BANKING BUSINESS

Anna Sergeevna AVERINA[1,2], applicant

[1]Deposit Insurance Agency, Moscow, Russia

[2]Autonomous non-profit organization of higher education «International Banking Institute named after Anatoly Sobchak», Saint-Petersburg, Russia

Address for correspondence: Averina A.S., 191023, Saint-Petersburg, Nevsky pr., 60.

Abstract

The purpose of the study. To draw attention to the problem of loss of personal data, valuable assets in the digital banking business environment, as well as to search for areas to enhance the cybersecurity of the digital perimeter in the context of the development of quantum technologies.

The **research methodology** is based on the study of scientific and specialized literature, the analysis of which will allow us to take a fresh look at quantum technologies from the standpoint of implementation in the security system and prepare a theoretical basis for activating research in this area. The work used general scientific methods of analogy, generalization, logical analysis, systematization, which made it possible to determine the role of quantum technologies in the context of expanding the digital banking space.

Research results. A review of quantum achievements over the past 10 years has been conducted, in which the following main trends can be traced: quantum computing, quantum communications and networks, quantum sensors and metrology. An assessment of the results obtained in the development of quanta has proven that the world has approached the quantum transition and it is necessary to keep up with future changes. The point successes of individual countries and companies in quantum topics are accumulating and will be transformed into widespread use. Russia is participating in quantum international competition and is striving to build quantum-resistant communication networks.

Conclusions. A scheme for building a quantum-protected communication network for exchanging information flows in the digital space of the financial market is proposed. There is a problem of the impossibility of conducting quantum and information flows through one channel.

Originality. The study allows us to focus on the changes taking place in the information space and emphasize the attention the need to find solutions to enhance the protection of banks' digital assets using quantum technologies.

Keywords

quantum threat, information space, banking operations, perimeter protection, data security, digital assets.

For citation: Averina A.S. Quantum threats to the security of banking business // Proceedings of the International Banking Institute. 2025. 1 (51). pp. 9-21. (in Russ.).

Введение

Банковский бизнес активно трансформируется и интегрируется с ФинТех. Высокая конкуренция на рынке финансовых услуг требует быстрой реакции на самые незначительные изменения рыночной конъюнктуры. Это возможно только в условиях постоянно цифрового присутствия в онлайн среде с возможностью открытого взаимодействия с цифровыми партнерскими сервисами, то есть в условиях Open Banking.

Российские банки готовы к таким преобразованиям, так как уже длительное время выстраивают собственные цифровые контуры, экосистемы, платформы и расширяют свое присутствие в Интернет-пространстве. Можно отметить, что сегодня ряд крупных банков отказываются от офлайн офисов и многие банковские операции переводят в дистанционный формат. Эти процессы повышают мобильность и комфорт получения банковских услуг для клиентов и позволяют эффективно конкурировать с ФинТех. Вместе с тем параллельно нарастает другая угроза – риски потери данных и цифровых активов, размещенных в банковских Дата-центрах и на счетах клиентов.

Банковская инфраструктура отнесена к критической информационной инфраструктуре России согласно ФЗ от 26.06.2017 г. (в ред. от 10.07.2023г.) N 187-ФЗ, поэтому защищенность ее работы и безопасность хранящихся данных является задачей государственного значения[1].

Статистика кибератак доказывает высокую заинтересованность мошенников к банковскому сектору. Так, по итогам оценок кибератак

[1]Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 10.07.2023) // СПС Гарант. URL: https://base.garant.ru/71730198/.

аналитиками компании Positive Technologies за период 2 полугодие 2023 – 1 полугодие 2024 гг. чаще всего жертвами становились банковские организации – до 65% всех атак. Можно отметить, что банки в фокусе внимания мошенников как источник наиболее распространенных каналов и центров хранения цифровых активов и конфиденциальной информации. При этом из года в год количество атак растет, что свидетельствует о необходимости использования диверсифицированного подхода к защите данных. Наибольшую популярность среди хакерских атак на банковскую инфраструктуру приобрели DDoS-атаки, стремящиеся не просто выкрасть ценную информацию, а полностью дестабилизировать работу инфраструктуры. В центре внимания не только банки, но и другие объекты финансовой инфраструктуры (фондовые рынки, операторы платежных систем, фонды), обслуживающие работу экономических субъектов расчетными и платежными услугами как на внутреннем, так и на внешних финансовых рынках. Если оперировать цифрами, то можно отметить, что среди методов атак лидирует социальная инженерия – до 65%, на втором месте применение вредоносного ПО – до 56%, третье место занимает эксплуатация уязвимостей – до 25%[2].

В условиях активизации атак кибермошенников и роста информационных ресурсов представляется актуальным поиск новых направлений и решений по укреплению цифровой инфраструктуры банков и поддержанию ее работоспособности. С этой точки зрения необходимо более пристально изучать разработки ведущих IT-компаний в части расширения квантового поиска и сопутствующей ему квантовой угрозы [1, 2].

Обзор литературы

Тема данного научного исследования освещена в работах многих современных авторов, занимающихся проблемами безопасности и защиты цифровых активов в онлайн среде. Вопросы появления новых видов рисков в условиях происходящих трансформационных изменений в банковском бизнесе были затронуты в работах следующих авторов Васильев С.А., Серов Е.Р., Федотова Г.В., Шумилина О.В.

При оценке проблемы сохранения информационной устойчивости и защиты хранящихся данных автор опирался на работы таких российских и

[2]Киберугрозы финансовой отрасли: 2023-2024. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-h2-2023-h1-2024/#id1/.

иностранных ученых как Адбулмукминова Э.М., Гаджиев Н.К., Евсиков К.С., Княжев Ф.Р., Магомедов М.А., Arute F., Arya K., Babbush R., Mosca M.

Понимание нарастающей квантовой угрозы для финансового сектора экономики было сформировано на основе работ следующих исследователей Букашкин С.А., Васильев С.А., Малышев О.К., Серов Е.Р., Сурков С.В., Черепнев М.А., Jingbo Wang, Ruan Yue, Marsh S., Xilin Xue, Shor P.M., Zhihao Liu.

Методы и материалы

Исследуемая проблематика квантового перехода была изучена на основе опубликованных литературных источников различных авторов, нормативно-правовых документов, регламентирующих легальность квантовых исследований, интернет-ресурсов коммерческих компаний, развивающих квантовые разработки. Основными методами обзора и обработки имеющегося материала и генерирования новых знаний выступили общенаучные методы систематизации, логического анализа, обобщения, сравнения, описания. Для обоснования необходимости внедрения нового подхода к системе информационной безопасности цифрового периметра были использованы методы анализа и синтеза, визуализации и графического представления материала.

Квантовая международная конкуренция

Сегодня Мир находится перед новым квантовым «скачком» или Второй квантовой революцией, которая способна перевести на новый качественный уровень имеющиеся технологии и коммуникации [3]. Технологически развитые страны и крупные ФинТех компании вкладывают инвестиции в квантовые разработки, способные значительно ускорить существующие процессы передачи цифровых данных. При этом особенности квантов под названием «эффект наблюдателя», «квантовая запутанность» настолько уникальны, что в будущем позволят генерировать новые подходы и алгоритмы к защите, обладающие высокой устойчивостью и непредсказуемостью для внешних несанкционированных доступов.

Мировые технологические лидеры сегодня активно развивают квантовую тематику, фактически соревнуясь в процессе создания максимально-кубитного квантового компьютера. На рисунке 1 представлена динамика развития квантовых компьютеров с момента появления теории и настоящего времени.

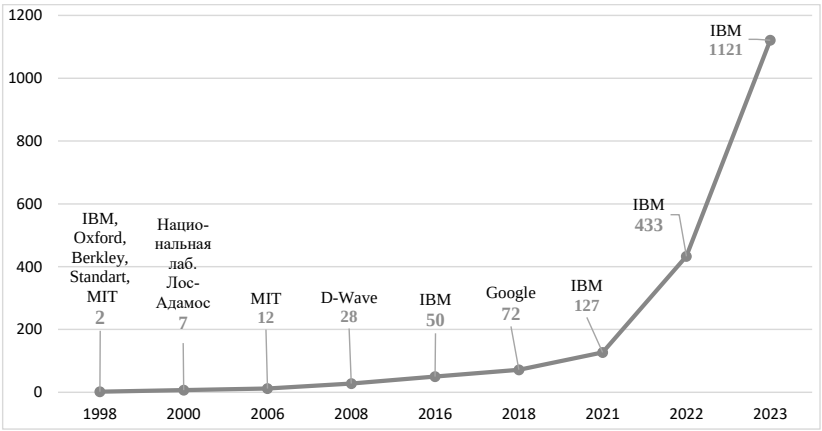

Рисунок 1 – Динамика развития квантовых компьютеров по числу кубитов
Источник: [6].

Представленная нами динамика развития квантовых технологий и усложнения операционной деятельности в кубитовом исчислении доказывает, что скорость квантовой гонки между странами нарастает за последние 2-3 года. В 2024 году лидерами квантовых исследований выступают компании IBM, Google и Rigetti, D-Wave, Xanadu30, Quantinuum31. При этом отметим, что в данной конкурентной борьбе упор сделан на достижение квантового превосходства и создание работоспособного компьютера, а также поиск практического применения данных технологий в различных сферах [4, 5].

Квантовая тематика сегодня реализуется в 24 юрисдикциях, где на государственном уровне выделяется финансирование под тематические стратегии и программы. Рассмотрим объемы инвестиций в квантовые разработки по странам в 2022 году.

Представленная диаграмма на рисунке 2 демонстрирует инвестиции 2022 года в квантовую тематику по основным юрисдикциям, для которых это направление является интересным. Общий объем мировых вложений в квантовые исследования достиг 42 млрд долл. США. В числе лидеров по тратам выступает Китай – 15,3 млрд долл. США, на втором месте страны ЕС – 8,4 млрд долл. США. Россия вложила в квантовые разработки – 0,8 млрд долл. США. [6, 7] Объемы вложений в квантовую разработку в следующих периодах будут расти, так как нарастает конкуренция между странами за лидерство и поиск эффективных решений цифрового коммуницирования и продвижения услуг.

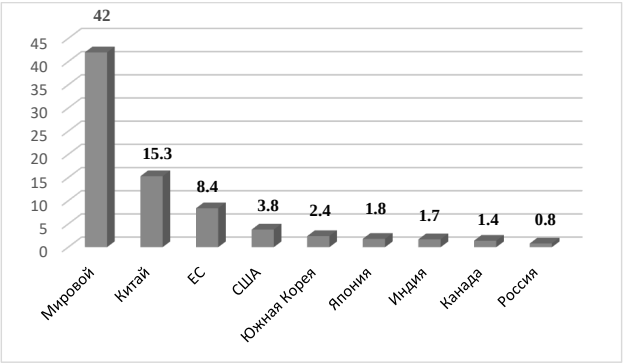

Рисунок 2 – Мировые инвестиции в квантовые исследования в 2022 году, млрд. долл. США

Источник: [6].

Очевидно, что квантовые технологии обладают колоссальным потенциалом применения в самых различных отраслях и сферах жизни. В нашем исследовании будем оценивать данные технологии с позиции усиления защиты цифровых активов и создания устойчивых коммуникационных сетей в банковских операциях [8, 9].

Квантовые исследования в России

В России квантовые исследования получили официальное обоснование в рамках нескольких официальных документов: Национальной программы развития цифровой экономики, Федеральный проект «Цифровые технологии», Государственная программа «Научно-технологическое развитие Российской Федерации», Дорожная карта развития сквозной цифровой технологии «Квантовые технологии». Все перечисленные официальные документы регламентируют необходимость поиска новых технологических решений, основанных на законах квантовой механики и состоянии суперпозиций кубитов квантового компьютера.

Российская Федерация сегодня не занимает лидирующие позиции в области квантовых вычислений, так как отечественный рынок квантовых разработок проходит этап своего становления. На период с 2020 по 2024 годы государством выделено 24,1 млрд руб., что послужило основой для формирования национального рынка квантовых решений. Дорожной картой четко определены приоритеты в области квантовых технологий: квантовые вычисления, квантовые коммуникации, квантовые сенсоры и метрологии.

Отметим, что в 2024 году в России ГК «Ростом» создан 50-кубитный ионный квантовый компьютер. Если сравнить с достижениями зарубежных компаний, можно заметить отставание отечественной квантовой отрасли. Но в данной ситуации наша страна не должна стремиться сокращать данный отрыв, а необходимо самостоятельно строить новые коммуникационные сети и технологии, основанные на специфике квантов.

Далее в развитие квантовой тематики в 2025 году в России будет запущен новый национальный проект «Экономика данных и цифровая трансформация государства», который придет на смену проекту «Цифровая экономика». В новом национальном проекте четко указано, что будут инициироваться прикладные исследования в части поиска способов применения квантовых технологий в различных практических ситуациях. Поэтому квантовые технологии уже с 2025 года могут активно внедряться в работу объектов критической информационной инфраструктуры. Остановимся на кредитных организациях.

Российские банки являются флагманами цифрового развития национальной экономики. Более того, за последние 10 лет банки выстроили собственные цифровые экосистемы, в которых аккумулированы большие данные и массивы цифровых активов. По этой причине банки включены в объекты критической инфраструктуры и должны максимально гарантировать своим клиентам и партнерам защиту информации и передачи данных через сеть Интернет.

Банки сегодня справляются с поставленной задачей, усиливая собственные службы безопасности и инвестируя большие ресурсы в технологии шифрования и защиты цифрового поля. Но нарастающая квантовая угроза заставляет их активно включаться в исследования и оценку возможностей квантовых технологий [10, 11].

С нашей точки зрения, наибольшую перспективу в финансовом секторе будут иметь технологии квантовой защиты и постквантовой криптографии. В рамках реализации Дорожной карты – создание квантовых процессоров, квантовых компьютеров, квантовых нейросетей. По нашему мнению, банковский бизнес должен включаться в квантовые разработки и максимально

адаптировать свою цифровую инфраструктуру под меняющиеся требования к ПО[3].

Так, Газпромбанк и Сбербанк активно сотрудничают с Российским квантовым центром. В 2019 году была продемонстрирована работа квантово-защищенной сети через алгоритм КРК (квантовое распределение ключей) и проведена защищенная видеоконференция между участниками. Связь была обеспечена через оптоволоконный канал с двухсторонним шифрованием, при этом ключи направлялись через оптический канал [12]. Такой механизм обеспечивает максимальную защиту и безопасную передачу данных и в будущем может быть основой в построении национальной многоузловой сети защищенной связи и коммуникаций. Представим схематично прототип данной сети (рисунок 3).

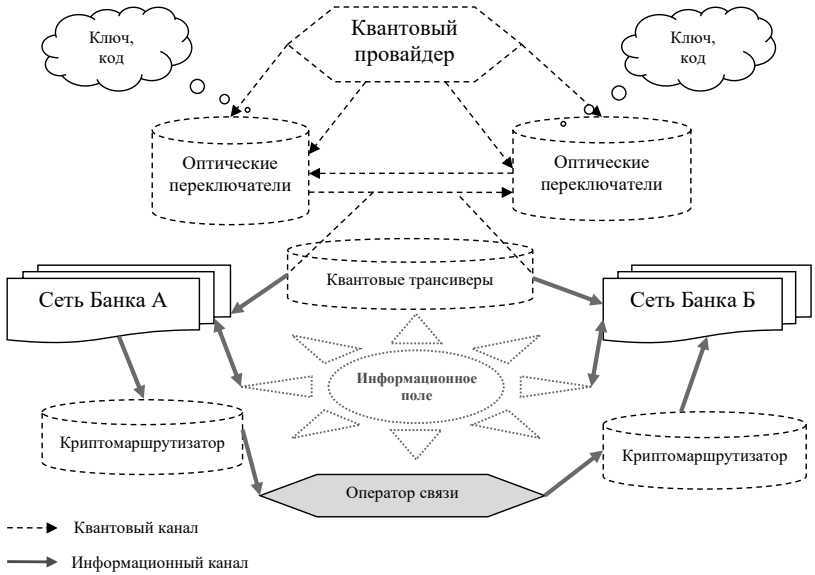

Рисунок 3 – Коммуникационная квантовая сеть обмена информацией

Источник: составлено автором.

Особенность представленной коммуникационной сети взаимодействия в финансовом информационном пространстве заключается в ее 2-уровневости. Так, существует поле квантового провайдера, который генерирует в нем

[3] Основные направления развития финансовых технологий на период 2025–2027 годов. Официальный сайт Банка России. Режим доступа: https://cbr.ru/Content/Document/File/166399/onfintech_2025-27.pdf.

квантовые ключи и передает их по своим специализированным каналам и трансиверам в цифровое бизнес-пространство. Затем уже во втором поле данные ключи применяются для передачи цифровых активов или взаимодействия между участниками рынка (в нашем примере это Банк А и Банк Б). Наличие 2 каналов связи – квантового и информационного – создает определенные неудобства, но даже в таком применении надежность квантово-распределенных ключей выше, чем криптографически-распределенных ключей. Поэтому решение проблемы сливания в один оптоволоконный канал квантовой и информационной передачи данных даст возможность не только сократить длину сети, но значительно ее бюджетировать [13].

В современных условиях создание квантовой коммуникационной сети на 50 пользователей стоит миллионы долларов, общедоступный квантовый Интернет невозможен, но технологии прогрессируют и скорость достижения новых результатов увеличивается. Построение работающего квантового компьютера ставит под угрозу всю существующую систему шифрования, так как новые возможности будут мгновенно решать задачи дискретного логарифмирования, заложенных в основу современной криптографии [14].

Итак, сегодня необходимо задуматься о наступлении квантовой эпохи в цифровом пространстве, так как внедрение таких технологий в традиционные бизнес-процессы кардинально будет менять весь процесс накопления, шифрования данных и их безопасную передачу [15]. Возможности, которые дает квантовый компьютер в решении поставленных задач и коммуницирования между субъектами гораздо выше тех, которые реализуются на данный момент посредством кремниевых компьютеров.

Субъекты экономики, которые сегодня развивают и продвигают свои услуги через информационные платформы должны учитывать грядущие изменения и трансформировать собственные технологии под изменения. Очевидно, что система криптошифрования станет бесполезной в квантовом пространстве, поэтому уже сегодня необходимо исследовать существующие решения по пост квантовой устойчивости алгоритмов и инвестировать средства в этом направлении [16].

По прогнозам консалтинговой компании, Reksoft Consulting, к 2040 году рынок квантовых вычислений составит от 110 млрд долл. США по

пессимистическому сценарию, до 258 млрд долл. США по оптимистическому сценарию развития событий, что будет составлять долю 6% мирового рынка.

Выводы

Квантовая революция неизбежна и несет в себе не только возможности, но и существенные угрозы всем работающим системам. Исследования, проводимые в данной области, доказывают, что потенциальные перспективы квантовых технологий могут вывести на новый уровень информационную экономику и по-другому выстроить онлайн-коммуникации как в бизнесе, так и в общественной жизни.

Современная проблема информационного общества – киберпреступность может получить в свое распоряжение новые эффективные решения для несанкционированных входов в цифровые контуры и платформы современных кредитных организаций, используя квантовое преимущество. Поэтому необходимо работать на опережение и уже сейчас инвестировать в перестройку применяемых технологий защиты и шифрования данных о счетах банковских клиентов.

Список источников

1. **Arute F. et al.** Quantum supremacy using a programmable superconducting processor // Nature 574. 2019. pp. 505–510. doi: 10.1038/s41586-019-1666-5.
2. **Yulin Wu. et al.** Strong quantum computational advantage using a superconducting quantum processor // Physical Review Letters. American Physical Society. 2021. No. 127. DOI: https://doi.org/10.1103/PhysRevLett.127.180501
3. **Федотова Г.В. и др.** Проблемы кибербезопасности современных цифровых систем. Коллективная монография / Под общ. науч. ред. Федотовой Г.В. – Курск: Изд-во ЗАО «Университетская книга», 2023. – 219 с.
4. **Серов Е.Р., Васильев С.А.** Ключевые тренды цифровой трансформации банковского бизнеса // Ученые записки Международного банковского института. 2022. № 2 (40). С. 201-221.
5. **Федотова Г.В., Шумилина О.В.** Банковский риск-менеджмент // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления. Материалы X международ. науч.-прак. конф. / под ред. Ю.В. Вертаковой. 2015. С. 401-405.
6. **Li G., Ding Y., Xie Y.** Towards efficient superconducting quantum processor architecture design. URL: https://arxiv.org/pdf/1911.12879.
7. **Сурков С.В., Малышев О.К.** Квантовые вычисления: взгляд в будущее. URL: https://www.reksoft.ru/blog/2024/10/17/quantum-computing-research/.

8. **Серов Е.Р., Васильев С.А.** Применение квантовых технологий в банковском бизнесе // Экономика и управление. 2023. Т. 29. № 3. С. 248-255. http://doi.org/10.35854/1998-1627-2023-3-248-255.
9. **Букашкин С.А., Черепнев М.А.** Квантовые устройства в криптографии // International Journal of Open Information Technologies. vol. 11. no. 1, 2023. pp. 104-108.
10. **Shor P.W.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput.1997. Vol. 26. № 5. P. 1484–1509.
11. **Ruan Y., Marsh S., Xue X., Liu Zh., Wang J.** The quantum approximate algorithm for solving traveling salesman problem // Computers, Materials & Continua. 2020. Vol.63. no.3. pp.1237-1247.
12. **Княжев Ф.Р.** Современные квантовые технологии для безопасного обмена данными // Столыпинский вестник. 2023. № 1. С. 189-198.
13. **Евсиков К.С.** Информационная безопасность государства в квантовую эпоху // Вестник университета имени О.Е. Кутафина. 2022. № 4. С. 47-58.
14. **Гаджиев Н.К., Магомедов М.А., Абдулмукминова Э.М.** Управление базами данных на основе облачных, квантовых, блокчейнтехнологий и технологий обработки больших данных // Журнал прикладных исследований. 2023. № 8. С. 45-50.
15. **Кудряшов В.Е., Фионов А.Н.** Проблема устойчивости современных криптосистем на фоне появления квантовых компьютеров // Интерэкспо Гео-Сибирь. 2022. Том 3. С. 109-115.
16. **Mosca M.** Cybersecurity in an era with quantum computers: Will we be ready? // IEEE Security & Privacy. 2018. Vol. 16. No. 5. P. 38-41.

References

1. **Arute F. et al.** Quantum supremacy using a programmable superconducting processor // Nature 574. 2019. pp. 505–510. doi: 10.1038/s41586-019-1666-5.
2. **Yulin Wu. et al.** Strong quantum computational advantage using a superconducting quantum processor // Physical Review Letters. American Physical Society. 2021. No. 127. DOI: https://doi.org/10.1103/PhysRevLett.127.180501
3. **Fedotova G.V. i dr.** Problemy kiberbezopasnosti sovremennykh tsifrovykh sistem. Kollektivnaya monografiya / Pod obsh. tauch. ked. Fedotovoy G.V. – Kursk: Izd-vo ZAO «Universitetskaya kniga», 2023. – 219 s.
4. **Serov Ye.R., Vasil'yev S.A.** Klyuchevyye trendy tsifrovoy transformatsii bankovskogo biznesa // Uchenyye zapiski Mezhdunarodnogo bankovskogo instituta. 2022. № 2 (40). S. 201-221.
5. **Fedotova G.V., Shumilina O.V.** Bankovskiy risk-menedzhment // Aktual'nyye problemy razvitiya khozyaystvuyushchikh sub'yektov, territoriy i sistem

regional'nogo i munitsipal'nogo upravleniya. materialy X mezhd. nauch.-prakt. konf. / pod red. Yu.V. Vertakovoy. 2015. S. 401-405.
6. **Li G., Ding Y., Xie Y.** Towards efficient superconducting quantum processor architecture design. URL: https://arxiv.org/pdf/1911.12879.
7. **Surkov S.V., Malyshev O.K.** Kvantovyye vychisleniya: vzglyad v budushcheye. URL: https://www.reksoft.ru/blog/2024/10/17/quantum-computing-research/.
8. **Serov Ye.R., Vasil'yev S.A.** Primeneniye kvantovykh tekhnologiy v bankovskom biznese // Ekonomika i upravleniye. 2023. T. 29. № 3. S. 248-255. http://doi.org/10.35854/1998-1627-2023-3-248-255.
9. **Bukashkin S.A., Cherepnev M.A.** Kvantovyye ustroystva v kriptografii // International Journal of Open Information Technologies. vol. 11, no. 1, 2023. pp.104-108.
10. **Shor P.W.** Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. Comput.1997. Vol. 26. № 5. pp. 1484–1509.
11. **Ruan Y., Marsh S., Xue X., Liu Zh., Wang J.** The quantum approximate algorithm for solving traveling salesman problem // Computers, Materials & Continua. 2020. Vol.63. no.3. pp.1237-1247.
12. **Knyazhev F.R.** Sovremennyye kvantovyye tekhnologii dlya bezopasnogo obmena dannymi // Stolypinskiy vestnik. 2023. № 1. S. 189-198.
13. **Yevsikov K.S.** Informatsionnaya bezopasnost' gosudarstva v kvantovuyu epokhu // Vestnik universiteta imeni O.Ye. Kutafina. 2022. № 4. S. 47-58.
14. **Gadzhiyev N.K., Magomedov M.A., Abdulmukminova E.M.** Upravleniye bazami dannykh na osnove oblachnykh, kvantovykh, blokcheyntekhnologiy i tekhnologiy obrabotki bol'shikh dannykh // Zhurnal prikladnykh issledovaniy. 2023. № 8. S. 45-50.
15. **Kudryashov V.Ye., Fionov A.N.** Problema ustoychivosti sovremennykh kriptosistem na fone poyavleniya kvantovykh komp'yuterov // Interekspo Geo-Sibir'. 2022. Tom 3. S. 109-115.
16. **Mosca M.** Cybersecurity in an era with quantum computers: Will we be ready? // IEEE Security & Privacy. 2018. Vol. 16. No. 5. pp. 38-41.