

УДК [316.772:530.145]:004

И.Н. Сухоручкина

Программы и проекты развития квантовых коммуникаций в России

Рассмотрены национальные программы развития квантовых коммуникаций в РФ, дорожные карты «Квантовые коммуникации», «Новые поколения узкополосной беспроводной связи для Интернета вещей и связи ближнего и среднего радиуса действия» в рамках национальной программы «Цифровая экономика РФ». Проанализированы приложения квантовой информатики, квантовые процессоры, ранжированы языки квантового программирования и протоколы квантового распределения ключей по годам. Представлены результаты разработок национальных и международных проектов сотрудничества российских исследовательских организаций, университетов, госкорпораций в области квантовых коммуникаций в РФ, включая квантовые компьютеры, квантовую криптографию, квантовое распределение ключей, квантовую телефонию, междугородние и межконтинентальные линии квантовой связи с участием РФ, Китая, Индии и ЮАР в рамках проектов БРИКС, ЕС, ООН, международных организаций, программы высшего и последилового образования по квантовым коммуникациям, важным для безопасности сетей связи.

Ключевые слова: квантовые коммуникации, квантовые технологии, квантовая криптография, квантовые компьютеры, квантовое распределение ключей, квантовый Интернет, квантовая телефония, дорожная карта развития высокотехнологичной области «Квантовые коммуникации»

DOI: 10.36535/0548-0019-2021-08-4

ВВЕДЕНИЕ

Квантовые технологии и коммуникации – перспективные и прорывные направления в области информационных технологий, цифрового развития, связи и коммуникаций XXI века в России, США, Китае, Японии и странах ЕС. В РФ квантовые коммуникации предназначаются для защиты информационно-телекоммуникационных сетей, информации финансового сектора, госорганов, высокотехнологичных компаний.

В **квантовых коммуникационных сетях** (*quantum networks*) передаваемые данные защищены благодаря применению законов квантовой механики, квантовых систем криптографии и квантовых вычислений. Безопасность передачи данных реализуется с помощью алгоритмов квантового распределения ключей (КРК, *quantum key distribution – QKD*) и волоконно-оптических систем передачи квантовых состояний фотонов. Квантовые сети развиваются после успешных экспериментов по квантовой телепортации [1]; квантовая криптография и её приложение: безопасность

связи – на стадии коммерциализации; квантовые вычисления – на стадиях гипотез, разработок и коммерциализации.

В **квантовых технологиях**, системах и устройствах используются принципы квантовой механики: 1) квантованность, дискретность уровней энергии, квантовый размерный эффект, изменение термодинамических и кинетических свойств кристалла; квантовый эффект Холла проводимости двумерного электронного газа в магнитных полях при низких температурах; 2) квантовая когерентная суперпозиция альтернативных чистых состояний систем; 3) квантовая запутанность (*quantum entanglement*) состояний двух или больше объектов; 4) квантовое туннелирование; 5) квантовый параллелизм, что позволяет квантовым компьютерам превзойти производительность классических; 6) принцип Гейзенберга неопределенности одновременного определения пары квантовых операторов системы: координаты и импульса, электрического и магнитного полей, тока и напряжения. Эти технологии реализуются в кванто-

вых коммуникациях, квантовых сетях, квантовой криптографии, квантовом распределении ключей, квантовых алгоритмах, квантовой телепортации, квантовых вычислениях, квантовых компьютерах, квантовых радарах, квантовых изображениях, квантовой визуализации, квантовой микроскопии, квантовых сенсорах, квантовой метрологии.

РАЗВИТИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ

Квантовая информатика (*quantum information science*) возникла в 1990-х гг. на стыке квантовой механики, теории алгоритмов [2] и теории информации; она изучает принципы управления динамикой квантовых систем. Приложения квантовой информатики:

- квантовая криптография;
- технологии запутанных состояний;
- компьютерное моделирование систем частиц.

Квантовые компьютеры (квантовые виртуальные машины) – модели квантовых систем применяются:

в квантовой криптографии: квантовом распределении ключей, позиционной квантовой криптографии, недоверчивой квантовой криптографии, квантовой криптографии вне зависимости от устройства, квантовом обязательстве, моделях ограниченного и зашумленного квантового хранилища, квантовом подбрасывании монеты;

в постквантовой криптографии на основе: хеш-функций, кодов исправления ошибок, решеток, многомерных квадратичных систем, шифрования с секретным ключом и на изогениях суперсингулярных эллиптических кривых;

в неструктурированном поиске: алгоритмах Шора, Гровера, Бернштейна – Вазирани, К. Залки – С. Визнера, Дойча – Йожи, Саймона, квантового счета, оценки фазы, квантовом преобразовании Фурье, квантовом сверхплотном кодировании;

в моделировании квантовых систем: имитаторах захваченных ионов, ультрахолодных симуляторах атомов, квантовых симуляторах с использованием сверхпроводящих кубитов, адиабатическом квантовом вычислении на основе квантового отжига, гамильтоновом моделировании;

в адиабатической оптимизации;

в искусственном интеллекте (ИИ), квантовом машинном обучении: моделировании линейной алгебры с квантовыми амплитудами, алгоритмах квантового машинного обучения на основе поиска Гровера, квантово-усиленном обучении с подкреплением, квантовых методах отбора проб, скрытых квантовых марковских моделях, полностью квантовом машинном обучении, квантовых алгоритмах для линейных систем уравнений, дифференцируемом программировании, квантовой томографии, квантовых нейронных сетях;

в квантовом считывании (проверке подлинности объектов) физических неклонированных функций: квантовой аутентификации сообщений и объектов, квантовых цифровых подписях, шифровании с открытым ключом, квантовом снятии отпечатков пальцев, квантовых односторонних функциях;

в квантовой визуализации: фантомном изображении, квантовом зондировании (лидарах), квантовой литографии;

в квантовой оптике: источниках одиночных фотонов на квантовых точках, квантовой метрологии, квантовых радарах, квантовых усилителях, квантовой границе Крамера – Рао, квантовой информации Фишера, квантовом шуме, квантовом отражении, квантовом стохастическом исчислении;

в моделировании молекулярных взаимодействий и химических реакций;

в квантовых алгоритмах для вычислительной биологии.

Языки квантового программирования позволяют выражать квантовые алгоритмы с использованием высокоуровневых конструкций (по годам):

Quantum pseudocode (Quantum Random Access Machine – QRAM; E. Knill, Los Alamos National Laboratory, США, 1996 г. – URL: <https://www.osti.gov/biblio/366453>);

QCL (Quantum Computation Language; B. Oemer, Венский технический университет, 2002 г. – URL: <https://arxiv.org/pdf/quant-ph/0211100.pdf>);

Q language (A. Whitney, компания Kx Systems, 2003 г. – URL: <https://code.kx.com/q/>);

Quantum lambda calculi (A. Tonder, Брауновский университет, США, 2003 г. – URL: <https://arxiv.org/abs/quant-ph/0307150>);

QPL (Quantum Physics and Logic; P. Selinger, Университет Оттавы, 2004 г. – URL: https://link.springer.com/chapter/10.1007%2F978-3-540-24754-8_1);

cQPL (P. Selinger, 2004 г. – URL: <https://www.cambridge.org/core/journals/mathematical-structures-in-computer-science/article/abs/towards-a-quantum-programming-language/54D5BCF28724CA6BE38F98DC4B6803DF>);

QML (Qt Meta Language, Qt Modeling Language; T. Altenkirch и J. Grattage, Университет Ноттингем, 2005 г. – URL: <https://ieeexplore.ieee.org/abstract/document/1509229>);

qGCL (Quantum Guarded Command Language; P. Pavan, L. Larcher, Università di Modena e Reggio Emilia; M. Cuozzo, P. Zuliani, A. Conte, STMicroelectronics, Италия, 2006 г. – URL: <https://dl.acm.org/doi/10.1109/TCAD.2003.814952>);

Quipper (версия 0.9.0.0; A.S. Green, N.J. Ross, P. Selinger, Dalhousie University, Канада; P.L.F. Lumsdaine, Институт перспективных исследований, Принстон, 2013 г. – URL: <https://dl.acm.org/doi/abs/10.1145/2491956.2462177>);

LIQUi> (Language-Integrated Quantum Operations; Microsoft Research, 2016 г. – URL: <https://www.microsoft.com/en-us/research/project/language-integrated-quantum-operations-liqui/>);

QMASM (Quantum Macro Assembler; S. Pakin, Los Alamos National Laboratory, 2016 г. – URL: <https://ieeexplore.ieee.org/document/7761637>);

Q# (Q Sharp как часть Quantum Development Kit; Microsoft, 2017 г. – URL: <https://docs.microsoft.com/en-us/azure/quantum/user-guide/>);

QPanda2 (компания HeFei Origin Quantum Computing Technology, Китай, 2017 г. – URL: <http://www.originqc.com.cn/QPanda/download.html>);

Qiskit (IBM Research, 2017 г. – URL: <https://qiskit.org/>);

Silq (B. Bichsel, M. Baader, T. Gehr, M. Vechev, компания ETH Zürich, Швейцария, 2020 г. – URL: <https://dl.acm.org/doi/10.1145/3385412.3386007>).

Квантовые процессоры основаны на схемах и квантовом отжиге. Технологии квантового компьютера: ионы в вакуумных ловушках (атомы в оптических ловушках; разработали П. Цоллер и Х.И. Сирак в 1994 г., Нобелевская премия 2009 г.);

оптические технологии: использование и детектирование генерации квантовых состояний света;

сверхпроводящие элементы: переходы Джозефсона, сверхпроводящий квантовый интерферометр (СКВИДы – SQUID, superconducting quantum interference device);

смешанные технологии: использование приготовленных запутанных состояний фотонов для управления атомными ансамблями и вычислительными сетями;

твердотельные квантовые точки на полупроводниках.

Модели квантовых компьютеров:

адиабатический квантовый компьютер на основе квантового отжига: вычисление разлагается на преобразование начального гамильтониана в конечный гамильтониан, и его состояния содержат решение;

массив квантовых вентилях: вычисление разложено на последовательность квантовых вентилях по несколько кубитов;

односторонний квантовый компьютер: вычисление разложено на последовательность однокубитных измерений запутанного начального состояния или состояния кластера;

топологический квантовый компьютер: вычисление разложено на сплетение энионов в двумерной решетке.

Реализации квантовых компьютеров:

на воздействии лазерного излучения на квантовые ямы и квантовые точки при комнатной температуре;

на захваченных ионах: кубиты реализованы внутренними состояниями захваченных ионов;

на инкапсулированных в углеродные оболочки металлических наночастицах (ИМНЧ) (URL: <http://irbis-corp.spsl.nsc.ru/fulltext/ippu/ectrudu/446.pdf>);

на квантовой электродинамике резонатора: кубиты заданы состояниями захваченных атомов, связанных с высокоточными резонаторами;

на квантовых проводах: кубиты реализованы парой квантовых проводов, соединенных квантовыми точечными контактами;

на квантовых точках (квантовый компьютер Д. Лосса – Д.П. Ди Винченцо, 1997 г.): спиновые кубиты определены спиновыми состояниями захваченных электронов;

на линейных оптических элементах: кубиты заданы обработкой состояний мод света с помощью линейных элементов (зеркал, светоделителей, фазовращателей);

на молекулярных магнитах: кубиты определены спиновыми состояниями;

на нейтральных атомах в оптических решетках: кубиты реализованы внутренними состояниями нейтральных атомов в оптической решетке;

на нелинейно-оптических квантовых компьютерах: кубиты реализованы при обработке состояний разных мод света с помощью линейных и нелинейных элементов;

на неорганических кристаллах, легированных ионами редкоземельных металлов (иттербия, тулия): кубиты заданы электронными состояниями примесей в оптических волокнах;

на основе алмаза: кубиты заданы электронными или ядерными спинами центров азотных вакансий в алмазе и взаимодействиями между резонаторами в оптических резонансных полостях в волноводах с алмазом (URL: <https://nplus1.ru/news/2016/10/15/rqc-diamond-platform>);

на основе конденсата Бозе – Эйнштейна;

на основе электронного спинового резонанса (электронного парамагнитного резонанса – ЭПР, открытого Е.К. Завойским в 1944 г., Казанский государственный университет) фуллеренов: кубиты на электронных спинах атомов или молекул в фуллеренах;

на основе ядерного магнитного резонанса (ЯМР) молекул в растворах, где кубиты созданы ядерными спинами в растворенных молекулах и исследуются с помощью радиоволн;

на пространственно-ориентированных положениях групп электронов в квантовых точках: кубиты заданы положениями электронов в двойных квантовых точках;

на сверхпроводящих электронных схемах (переходах Джозефсона): кубиты реализованы состояниями малых сверхпроводящих цепей;

на твердотельных ядерных магнито-резонансных (ЯМР) ансамблевых квантовых компьютерах Б. Кейна (1998 г.): кубиты реализованы ядерными спиновыми состояниями доноров фосфора в кремнии;

на транзисторах с захватом положительных дырок с помощью электростатических ловушек;

на электронах вблизи границы жидкого гелия: кубиты – спины электронов.

Протоколы квантового распределения ключей (по годам):

протокол неявной передачи (oblivious transfer – OT; М.О. Рэбин, Гарвардский университет, 1981 г. [3]);

BB84 (С.Н. Беннетт, IBM Research; G. Brassard, Монреальский университет, 1984 г. [4]);

E91 (протокол квантового распределения ключей с использованием электронного парамагнитного резонанса (А. Эйнштейн, В. Подольский, Н. Розен, EPR-protocol; А.К. Экерт, Оксфордский университет, 1991 г. [5]);

B92 (С.Н. Беннетт, 1992 г. [6]);

BBM92 (С.Н. Беннетт, G. Brassard, N.D. Mermin, Гарвардский университет, 1992 г. [7]);

протокол Гольденберга – Вайдмана (L. Goldenberg, L. Vaidman, Тель-Авивский университет, 1995 г. [8]);

MSZ96 (Y. Mu, J. Seberry, Y. Zheng, Университет Вуллонгонг, Австралия, 1996 г. [9]);

протокол с 6-ю состояниями (6-state protocol; Н. Вехманн-Паскуинуччи, N. Gisin, Университет Женевы, 1999 г. [10]);

дифференциальный фазовый сдвиг (differential phase-shift – DPS; К. Иноэ, Е. Вакс, Y. Yamamoto, Стэнфордский университет, японская корпорация NTT, 2002 г. [11]);

протокол состояния приманки (decoy state QKD protocol; W. Y. Hwang, Северо-Западный университет, Чикаго, 2003 г. [12]);

COW (coherent one-way; N. Gisin, Университет Женевы, 2004 г. [13]);

ARG04 (A. Acin, N. Gisin, V. Scarani, Университет Женевы, 2004 г. [14]);

SARG04 (V. Scarani, A. Acin, N. Gisin, Университет Женевы; G. Ribordy, Id-Quantique, 2004 г. [15]);

Lo05 (H.K. Lo, X. Ma, K. Chen, Университет Торонто, 2005 г. [16]);

протокол трехэтапного квантового шифрования (three-stage quantum cryptography protocol, Kak's three-stage protocol; S. Kak, Государственный университет Луизианы, 2006 г. [17]);

KMB09 (M.M. Khan, A. Beige, Университет Лидс, Великобритания; M. Murphy, Ульмский университет, Германия, 2009 г. [18]);

детектор-независимое квантовое распределение ключей (measurement-device-independent QKD – MDI-QKD; H.K. Lo, B. Qi, Университет Торонто; M. Curty, Университет Виго, Испания, 2012 г. [19]);

HDQKD (high-dimensional quantum key distribution – многомерное квантовое распределение ключей; J. Mower, Z. Zhang, P. Desjardins, C. Lee, J.H. Shapiro, D. Englund, Массачусетский технологический институт, Колумбийский университет, 2013 г. [20]).

ПРОГРАММЫ РАЗВИТИЯ КВАНТОВЫХ КОММУНИКАЦИЙ В РОССИИ

В 2013-2019 гг. уровень киберпреступности в РФ вырос в 20 раз и постоянно увеличивается: 15 % преступлений в РФ совершается с помощью информационных технологий в киберпространстве. В 2020 г. число кибератак на российские информационные порталы госорганов власти возросло в 3,5 раза [21].

В этой сфере развивается взаимодействие подразделений информационной преступности МВД РФ и ФСБ РФ и международное сотрудничество в борьбе с киберпреступностью: консультации с представителями правоохранительных органов Евросоюза и США, российско-французские встречи по противодействию киберпреступности (2019 г.) [22]. 23 ноября 2001 г. Советом Европы принята Конвенция о киберпреступности (Convention on cybercrime, ETS N 185, Будапешт, 23.11.2001, с изменениями от 28.01.2003) [23]. Разрабатывается инициированная Российской Федерацией Конвенция ООН по противодействию киберпреступности. 29 октября 2018 г. Европейская комиссия начала программу Quantum Flagship с бюджетом 1 млрд евро и 20-ю проектами в четырех областях: 1) квантовые коммуникации (проекты CiviQ, Quantum Internet Alliance, Qrange, UNIQUORN); 2) квантовое моделирование (Qombs, PASQUAN); 3) квантовая метрология и сенсоры (iqClock, MetaboliQs, macQsimal, ASTERIQS); 4) квантовые вычисления (OpenSuperQ, AQTION), а также проекты фундаментальных исследований (2D-SIPC, S2QUIP, QMiCS, SQUARE, PhoG, PhoQuS, MicroQC) [24]. 30 июля 2019 г. на 74-й сессии Генеральной Ассамблеи ООН Генеральный секретарь ООН представил доклад «Противодействие использованию информационно-коммуникационных технологий в преступных целях» [25].

1 декабря 2016 г. в Послании к Федеральному Собранию Президент РФ В.В. Путин предложил сосредоточиться на сквозных технологиях: цифровых, квантовых, робототехнике, нейротехнологиях; укреплять защиту от киберугроз, повышать устойчивость инфраструктуры, финансовой системы, госуправления; в реализации Программы цифровой экономики опираться на российские компании, научные и инжиниринговые центры [26]. 21 апреля 2021 г. в Послании к Федеральному Собранию Президент РФ отметил важность предложений РФ о международном диалоге в области кибербезопасности [27].

Национальная программа «Цифровая экономика РФ» принята в соответствии с Указом Президента РФ от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития РФ на период до 2024 г.» и утверждена 24 декабря 2018 г. на заседании президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам [28]. 10 июля 2019 г. на церемонии обмена соглашениями между правительством и крупнейшими компаниями с госучастием Президент РФ призвал гарантировать технологический суверенитет РФ в развитии перспективных и прорывных высокотехнологичных технологий связи. Подписаны соглашения между правительством РФ и ОАО «РЖД» (направление «Квантовые коммуникации»), госкорпорацией «Ростех» («Новые поколения узкополосной беспроводной связи для Интернета вещей и связи ближнего и среднего радиусов действия», «Квантовые сенсоры», «Технологии распределенного реестра»), ПАО «Сбербанк» («Искусственный интеллект»), госкорпорацией «Росатом» («Квантовые вычисления» и «Технологии создания новых материалов и веществ»), а также трехстороннее соглашение с «Ростех» и ПАО «Ростелеком» по «Беспроводной связи нового поколения». В.В. Путин отметил, что квантовые технологии и коммуникации определяют экономику РФ и мировую экономику; задача – гарантировать РФ технологический суверенитет, достойное место на перспективных рынках; государство окажет компаниям-партнерам помощь в форме финансовых, налоговых инструментов, комфортной регуляторной среды, гибких правовых режимов, разработки дорожных карт, целевых показателей, обеспеченности научно-технологической и производственной инфраструктурой [29].

10 октября 2019 г. Правительственная комиссия по цифровому развитию утвердила дорожные карты: «Квантовые технологии», «Технологии беспроводной связи», «Компоненты робототехники и сенсорики», «Технологии виртуальной и дополненной реальности», «Системы распределенного реестра», «Новые производственные технологии» [30], а также «Нейротехнологии и искусственный интеллект» [31] и выделила 850 млрд руб. на их реализацию. 19 ноября 2020 г. Правительственная комиссия по цифровому развитию утвердила дорожную карту «Мобильные сети связи пятого поколения» и 10 декабря 2020 г. – План реализации до 2024 г. в РФ Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей». Пять дорожных карт – в ведении Министерства цифрового развития, связи и массовых коммуникаций: «Квантовые коммуникации», «Кван-

товые вычисления», «Мобильные сети связи пятого поколения», «Интернет вещей», «Технологии распределенных реестров». Три дорожные карты – в ведении Министерства промышленности и торговли РФ: «Квантовые сенсоры», «Технологии распределенных реестров», «Технологии новых материалов и веществ». Госкорпорации софинансируют дорожные карты: «РЖД» – 40 % расходов по «Квантовым коммуникациям», «Росатом» – 50 % расходов по «Квантовым вычислениям», «Ростелеком» и «Ростех» – 50 % расходов по дорожной карте 5G. Остальные 50-60 % расходов финансируются из бюджета РФ [32].

4 сентября 2020 г. дорожная карта «Квантовые коммуникации» до 2024 г., разработанная «РЖД», одобрена Правительственной комиссией по цифровому развитию, использованию информационных технологий [33] и включает 120 проектов технологий оптоволоконных, атмосферных и спутниковых квантовых коммуникаций, коммерческих квантовых сетей связи и оборудования, абонентских устройств, квантового Интернета вещей, рынка и экосистемы образования, науки и промышленности РФ.

На развитие квантовых коммуникаций РФ до конца 2021 г. требуется 25 млрд руб.: 12,9 млрд руб. – из бюджета РФ, 5,3 млрд руб. – средства «РЖД», 6,5 млрд руб. – внебюджетные инвестиции. К 2024 г. рынок квантовых коммуникаций вырастет до 55 млрд руб., что составит 8 % от мирового, сформируется квантовая сеть протяженностью 10 тыс. км магистральных оптоволоконных каналов для 1 тыс. абонентов [34]. Предложены три варианта реализации квантовых сетей: 1) по действующим оптоволоконным сетям связи; 2) по открытому пространству – по сетям сотовых операторов; 3) через спутниковую связь – обмен квантовым распределением ключей между наземными станциями и орбитальными спутниками.

Национальная квантовая сеть создается как часть Евразийского квантового пути, объединяющего РФ, Китай, Индию, Турцию, со сквозной передачей квантового распределения ключей. В основе построения этой сети проекты АО «СМАРТС»: «Создание автодорожных телекоммуникационных сетей», прокладка магистральных волоконно-оптических линий связи (ВОЛС) в обочину автомобильных дорог 150 тыс. км в 85 субъектах РФ (с 2007 г.) и «Создание системы управления географически распределенными центрами обработки данных» (с 2017 г.) для контроля доступа к информационным каналам [35].

На заседании президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий 31 июля 2020 г. утверждена разработанная госкорпорацией «Росатом» с финансово-экономическим обоснованием дорожная карта «Квантовые вычисления», ее цели: создание к 2024 г. российского 100-кубитного квантового компьютера; решение инженерных задач квантовых вычислений, формирование экосистемы развития: инфраструктуры, образовательных программ, консорциумов с промышленными компаниями. Госкорпорация создала Национальную квантовую лабораторию – консорциум с участием НИУ ВШЭ, НИТУ «МИСиС», НИУ МФТИ, Физического института им.

П.Н. Лебедева РАН, Российского квантового центра и фонда «Сколково». В МГУ им. М.В. Ломоносова, МИФИ и МФТИ организованы магистерские и аспирантские программы, а также обучение старшекласников: в 2020 г. привлечены 500 школьников. Заключены контракты с ПАО «Ростелеком» и ПАО «Сбербанк».

ПРОЕКТЫ КВАНТОВЫХ КОММУНИКАЦИЙ В РОССИИ

Создание квантовых сетей ведут следующие организации.

Факультет физической и квантовой электроники МФТИ, созданный в 1964 г., осуществляет разработки: квантовых компьютеров, функциональной электроники, нанотехнологий (выпускник факультета – нобелевский лауреат К.С. Новоселов за исследование графена), нанометрологии, нейроморфных структур, микроэлектроники, твердотельной и вакуумной СВЧ-электроники [36]. 1 ноября 2018 г. МФТИ и Российский квантовый центр предложили новый способ передачи квантовой информации между разными типами кубитов посредством электромагнитного поля. 28 марта 2021 г. в лаборатории Искусственных квантовых систем МФТИ создан первый в России квантовый сопроцессор на основе 5 сверхпроводниковых кубитов – трансмонов.

На Физическом факультете МГУ им. М.В. Ломоносова в 1978 г. в результате реорганизации кафедры волновых процессов создана Кафедра квантовой электроники (до 2001 г. – квантовой радиофизики), которая ведет разработки: квантовой и статистической оптики, спектроскопии самоорганизующихся систем, нелинейной оптики поверхности и наноструктур, сканирующей зондовой микроскопии и наноэлектроники, лазерной спектроскопии водных сред и лазерной диагностики водных экосистем, лазеров УФ диапазона и квантовой оптики, теории отклика хаотических систем, туннельных процессов в наноструктурах, электронных систем с сильной корреляцией, гиперрэлеевского рассеяния света в неупорядоченных наноструктурах, сегнетоэлектрических фазовых переходов, нелинейной оптики наноструктур, а с 1996 г. – систем квантовой коммуникации при поддержке Фонда перспективных исследований (ФПИ) и ряда министерств [37]. В сентябре 2016 г. осуществлена квантовая связь в автоматической системе квантового распределения криптографических ключей на базе стандартных линий связи ПАО «Ростелеком» между Ногинском и Павловским Посадом (в Московской области) протяженностью 32 км.

Центр квантовых технологий (ЦКТ) МГУ им. М.В. Ломоносова создан в 2018 г. в рамках Национальной технологической инициативы [38] осуществляет разработки: квантовых технологий, волоконной и атмосферной квантовой криптографии, нанофотоники, квантовой оптики, нелинейной оптики, криоэлектроники, физики холодных атомов; систем квантовой криптографии, адаптированных к волоконным линиям связи, систем оптической квантовой коммуникации по открытому пространству и оптических квантовых вычислительных систем, образовательных программ и связей с промышленными ком-

паниями. В Консорциум МГУ им. М.В. Ломоносова входят Институт физики твердого тела РАН (ИФТТ РАН), Физико-технологический институт им. К.А. Валиева РАН (ФТИ РАН), Институт общей физики им. А.М. Прохорова РАН, Институт физики полупроводников им. А.В. Ржанова СО РАН, Санкт-Петербургский государственный университет, МИФИ, МГТУ им. Н.Э. Баумана, НИУ «Московский институт электронной техники», Томский государственный университет систем управления и радиоэлектроники, ФИЦ «Казанский научный центр РАН», Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова госкорпорации «Росатом», Центр компетенций Национальной технологической инициативы по направлению «Квантовые коммуникации» на базе НИТУ «МИСиС», АО «Информационные технологии и коммуникационные системы» (АО «ИнфоТеКС»), Учебный центр «ИнфоТеКС», АО «Концерн «Автоматика», ООО НТП «Криптософт» (г. Пенза), ООО «Авеста», ООО «ИД Электроника», межрегиональная общественная организация «Ассоциация защиты информации», компания «Иннопрактика» (Факультет фундаментальной медицины МГУ объединяет Центр национального интеллектуального резерва МГУ и Фонд поддержки научно-проектной деятельности молодых ученых «Национальное интеллектуальное развитие»), Саратовский НИГУ им. Н.Г. Чернышевского, технопарк «Кванториум» (г. Саратов).

29 мая 2019 г. Центр квантовых технологий МГУ им. М.В. Ломоносова и Центр научных исследований и перспективных разработок компании «Инфотекс» провели первый сеанс голосовой связи, защищенной квантовым распределением ключей, между офисами ЦКТ МГУ и «Инфотекса» с помощью первого российского квантового телефона ViPNet QSS Phone, входящего в разработанный за три года комплекс защищенной телефонии ViPNet Quantum Security System (ViPNet QSS). Российский квантовый телефон не подвержен атакам квантовых компьютеров, что подтверждено Центром компетенций Национальной технологической инициативы «Центр квантовых технологий» [39].

Математический институт им. В.А. Стеклова РАН (МИАН) разрабатывает математические методы квантовых технологий: квантовой криптографии, квантовых вычислений. Отдел математических методов квантовых технологий МИАН, созданный в 2018 г. на основе Лаборатории математических методов квантовых технологий (с 2016 г.), проводит исследования в областях квантовой криптографии, квантовой информатики, открытых квантовых систем, многочастичных квантовых систем, управления квантовыми системами, квантовой томографии, квантовой телепортации, адиабатических квантовых вычислений, неравновесной квантовой динамики, голографии и квантовой информации.

По проектам Российского научного фонда (РНФ) МИАН осуществляет проекты: «Математические методы для задач квантовых технологий и динамика открытых квантовых систем» (2017-2021 гг.), «Использование псевдослучайных генераторов в квантовой криптографии» (2018-2019 гг.), «Влияние взаимодействия с окру-

жением на информационные свойства квантовых каналов передачи данных» (2020-2022 гг.) [40].

ПАО «Ростелеком» развивает квантовые технологии связи, ОАО «РЖД» – квантовые коммуникации, госкорпорация «Росатом» – квантовые вычисления, госкорпорация «Ростех» – квантовые сенсоры. В декабре 2018 г. в проекте «Криптошифрование и квантовая защита данных» завершен 1-й этап тестирования комплексов передачи данных с гибридной квантово-классической защитой, подтверждена возможность использования квантового распределения ключей в сетях связи «Ростелекома»; в январе 2019 г. – 2-й этап испытаний квантовой защиты передачи данных. В мае 2019 г. «Ростелеком» и «Криптософт» испытали прототип первого облачного сервиса защиты передачи данных с квантовым распределением ключей, а «Ростелеком» и «ИнфоТеКС» – защиту передачи данных с квантовым распределением ключей на волоконно-оптической линии связи 58 км между дата-центром М10 «Ростелекома» (Москва) и Центром фотоники и квантовых материалов (Skoltech Center of Photonics and Quantum Materials, созданным в 2015 г. [41]) Сколковского университета науки и технологий (Сколтех, создан в 2011 г.). В сентябре 2020 г. «Ростелеком» и «Росатом» разработали волоконно-оптическую линию связи с применением квантового распределения ключей между двумя офисами «Росатома» в Москве, оборудования квантового распределения ключей ООО «КуРэйт» (QRate) и шифраторов 10 G ООО «Код Безопасности» при участии АНО «Консорциум «Телекоммуникационные технологии» и ПАО «Микрон». Сервис квантового распределения ключей для «Ростелекома» обеспечивает ключами шифрования и средствами криптографической защиты информации (СКЗИ) промышленные предприятия и банки.

ОАО «РЖД» отвечает за реализацию дорожной карты «Квантовые коммуникации» – в августе 2019 г. был создан Департамент квантовых коммуникаций «РЖД»; развиваются магистральные и городские сети квантовых коммуникаций в РФ. Квантовые сети в тысячи километров строятся с использованием промежуточных доверенных узлов через 80-120 км. На труднодоступных участках для связи двух наземных объектов используется технология спутникового квантового распределения ключей [42].

Российский квантовый центр (РКЦ, основан в 2011 г. в Инновационном центре «Сколково») разрабатывает систему квантовой связи для защищенной передачи информации банков и госорганов в телекоммуникационной сфере (твердотельные фотумножители, сверхчувствительные сенсоры, фемтосекундные лазеры) и медицине (сверхчувствительный магнитный кардиограф) [43]. В 2015 г. создана группа «Квантовые коммуникации». РКЦ и Лаборатория сверхпроводящих метаматериалов НИТУ «МИСиС» впервые в РФ произвели измерение кубита (2013 г.), совместно с исследователями МФТИ, МИСиС и ИФТТ РАН создали первый в РФ сверхпроводящий кубит (2015 г.), первый в мире квантовый блокчейн (2017 г.). РКЦ сотрудничает с компаниями: «КуРэйт» (основана в 2015 г. и ведет разработку программы обработки квантового распределения ключей

чей; испытана офисами АО «Газпромбанк»; протестирован прототип промышленной установки в ПАО «Сбербанк»; ведет серийное производство установок квантовой криптографии: детектор одиночных фотонов, квантовый генератор случайных чисел, твердотельный фотоумножитель, фемтосекундный лазер с диодной накачкой [44]), «С-Терра СиЭсПи» (S-Terra CSP, LLC; основана в 2003 г. для разработок и производства средств сетевой информационной безопасности [45]), «КриптоПро» (создана в 2000 г. для формирования средств криптографической защиты информации и инфраструктуры открытых ключей [46]), ООО «Амикон», ООО «Код Безопасности», ЗАО «Сверхпроводниковые нанотехнологии» (SCONTEL, основано в 2004 г. на основе Проблемной радиофизической лаборатории Московского педагогического государственного университета, имеет представителей в Китае, Японии и США [47]). В 2017 г. Российский квантовый центр разработал самый мощный в мире квантовый компьютер с инвестициями Google, IBM, Microsoft, Alibaba.

С 2020 г. на базовой кафедре Российского квантового центра в МФТИ организованы программы бакалавриата, магистратуры и аспирантуры, в НИТУ «МИСиС» при участии РКЦ – магистерская программа «Квантовые технологии материалов и устройств» и программа аспирантуры «Физика конденсированного состояния и квантовые технологии»; созданы устройства для квантовой криптографии, сверхпроводниковой и полупроводниковой космической электроники, разработано квантовое моделирование свойств материалов. Российский квантовый центр, Российская венчурная компания (РВК), МФТИ и Центр компетенций Национальной технологической инициативы «Квантовые коммуникации» НИТУ «МИСиС» реализуют программу «Управление проектами в сфере квантовых коммуникаций» [48].

Московский институт электроники и математики им. А.Н. Тихонова (создан в 1993 г. на базе Московского института электронного машиностроения, основанного в 1962 г.; в 2011 г. включен в НИУ ВШЭ) на кафедре квантовой оптики и телекоммуникаций ЗАО «Сконтел» (созданной в 2013 г.) ведет разработки сверхпроводниковых тонкопленочных микросхем, приемников на тонкопленочных сверхпроводниковых наноструктурах; осуществляет магистерскую программу «Нанoeлектроника и квантовые технологии» [49].

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО) создал защищенный оптический маршрутизатор (SCWQC – Subcarrier wave quantum communication system) моделированного излучения с квантовым распределением ключей на боковых частотах и внедрил его в квантовых сетях Университета ИТМО (в 2014 г.), в Казани с телеком-оператором (в 2016 г.) и в Самаре с ИТ-компанией (в 2021 г.); осуществляет международные образовательные программы «Квантовые коммуникации и фемтотехнологии» (в сотрудничестве с Университетом Рочестера, США); развивает сотрудничество с ООО «Квантовые Коммуникации», компанией «СМАРТС», ООО «Кванттелеком»

(Санкт-Петербург), ООО «Корнинг», ООО НПП «Лазерные Технологии», ООО «Лазерный Центр», компаний «Vicon-Standa», ООО «Аметист Лазер», ОАО «Комета», ОАО «ЛОМО», ОАО «ГОИ им. С.И. Вавилова» [50].

Казанский квантовый центр («КАИ-КВАНТ») Казанского НИТУ им. А.Н. Туполева – КАИ (КНИТУ-КАИ) создан в 2014 г., в лабораториях квантовой памяти и квантовых коммуникаций ведет разработки квантовых технологий, квантовых методов защиты передачи и хранения информации; волоконных и интегрально оптических однофотонных технологий, оптических методов передачи квантового распределения ключей, участвует в создании городской квантовой сети (квантовый Интернет), квантовых сетей между городами Республики Татарстан, квантовой сети на большие расстояния, квантовых повторителей на основе оптической квантовой памяти, квантовых сетей между городами РФ, квантовых вычислителей и переключателей в квантовой сети, оптического квантового компьютера для квантовых сетей. Развивает международное сотрудничество с коллегами из Франции, Китая, Южной Кореи, Саудовской Аравии, Шотландии, Канады, Индии и сотрудничество с научными организациями РФ: Университетом ИТМО (разработка оптических квантовых сетей), МГУ им. М.В. Ломоносова (нанооптическая квантовая память, с 2014 г.), РКЦ (оптоволоконные методы генерации световых полей, с 2014 г.), Физико-технологическим институтом РАН им. К.А. Валиева (основан в 1988 г., Лаборатория физических основ квантовых вычислений разрабатывает квантовые компьютеры, проводит семинары «Квантовые компьютеры») [51], сотрудничает в области оптических квантовых измерений с 2014 г.); Казанским физико-техническим институтом РАН им. Е.К. Завойского Казанского научного центра РАН; Казанским федеральным университетом (теория оптических спектров неорганических кристаллов для квантовой памяти), Институтом перспективных исследований АН РТ (оптический квантовый процессинг, квантовый компьютер, с 2010 г.); КНИТУ-КАИ (новые методы обработки сигналов) [52].

Фонд перспективных исследований с 2016 г. реализует проект «Технологии обработки информации на основе сверхпроводящих кубитов» совместно с ФГУП «ВНИИА им. Н.Л. Духова», ИФТТ РАН, РКЦ, МФТИ, МИСиС, МГУ им. Н.Э. Баумана, Новосибирским государственным техническим университетом (НГТУ НЭТИ) при поддержке Министерства науки и высшего образования РФ и госкорпорации «Росатом» [53].

Национальный исследовательский Томский государственный университет осуществляет проект «Взаимодействие закрученного света с отдельными атомами и атомными ансамблями» при финансировании РНФ (2021-2023 гг.) [54].

20 февраля 2020 г. в Министерстве экономического развития РФ объявлено о разработке проекта «Квантовая долина» в Нижегородской области [55] для создания Инновационного научно-технологического центра квантовых технологий. В реализации проекта заинтересованы 50 компаний, включая Сбербанк, «Росатом», «Ростех» и «РЖД».

29 октября 2020 г. Правительство РФ утвердило перечень технологий, на которые будет распространяться особое регулирование в упрощенных правовых режимах (регуляторных песочниц) [56], а также правовая среда для тестирования новых продуктов, снижения издержек и ускорения разработок перспективных идей. В их число вошли квантовые и производственные технологии, а также нейротехнологии и технологии искусственного интеллекта, работы с Большими Данными, робототехника и сенсорика, системы распределенного реестра, беспроводная связь, виртуальная и дополненная реальность, Интернет вещей, отраслевые цифровые технологии.

30 октября 2020 г. госкорпорация «Ростех» присоединилась к проекту создания первого в мире межконтинентального канала квантовой связи протяженностью 10 тыс. км [57] специалистами Российской Федерации, Китая, Индии и ЮАР в рамках проекта БРИКС по квантовым коммуникациям при поддержке Российского фонда фундаментальных исследований. Межконтинентальный канал квантовой связи свяжет университеты – участники проекта в ЮАР и Китае. Специалисты РФ и Индии разрабатывают волоконно-оптические волокно и коммуникации, ЮАР – головной исполнитель проекта, в Китае создают спутниковую квантовую связь. АО «Научно-производственное объединение Государственный оптический институт им. С.И. Вавилова» (ГОИ) разрабатывает лазерные системы разного назначения, включенные в перечень ведущих научно-исследовательских организаций оборонно-промышленного комплекса по направлению «Оптико-электронные приборы, системы и комплексы», утвержденный Министерством промышленности и торговли РФ 2 апреля 2009 г. ГОИ – соисполнитель научно-исследовательской работы «Спутниковая и волоконно-оптическая связь квантовых коммуникаций» по созданию волоконно-оптических элементов для формирования и трансляции оптических вихрей в приложении квантовых коммуникаций. Головной исполнитель проекта – Поволжский государственный университет телекоммуникаций и информатики – ведет исследования и подготовку специалистов по направлениям телекоммуникации, радиотехники, информатики и экономики при участии Казанского НИТУ им. А.Н. Туполева. Стоимость реализации проекта квантовой сети в 10 тыс. км до 2024 г. – 16,7 млрд руб.: 10 млрд – из федерального бюджета, 6,7 млрд – из внебюджетных источников, 5 млрд руб. выделит «РЖД». Затраты на строительство квантовых магистральных сетей к 2024 г. составят 12,8 млрд руб.; объем услуг в сети – 55 млрд руб. Разрабатываются сценарии использования квантовых технологий для передачи данных банков и госструктур, строительства безопасных систем Интернета вещей и управления беспилотными поездами.

19 ноября 2020 г. на заседании Научного совета при президиуме РАН «Квантовые технологии» по теме «Фундаментальные проблемы квантовых коммуникаций» с участием ученых 40 научных организаций РАН и других учреждений председатель Научного совета академик-секретарь Отделения нанотехнологий и информационных технологий РАН определил направления программ развития квантовых сетей в РФ.

Представлены проекты: 1) Казанский научный центр РАН: «Квантовые повторители и квантовая память»; 2) ИФТТ РАН: «Каналы утечки в квантовой криптографии»; 3) Институт проблем управления им. В.А. Трапезникова РАН и ОАО «РЖД»: «Технологии квантовых коммуникаций»; 4) МГУ им. М.В. Ломоносова: «Постквантовая криптография» и «Атмосферные и спутниковые каналы квантовых коммуникаций»; 5) МИСиС: «Ограничения скорости квантового распределения ключей»; 6) Университет ИТМО: «Компонентная база для волоконно-оптических квантовых коммуникаций»; 7) АО «ИнфоТекС»: «Доверенные узлы в сетях квантовых коммуникаций».

Техническим комитетом «Криптографическая защита информации» создана рабочая группа по созданию постквантовых криптографических механизмов, разработке и замещению импортных комплектующих в устройствах квантовой коммуникации: блоке генерации излучения, блоке регистрации излучения, блоке кодирования. Разрабатываются базовые элементы (однофотонные источники, источники перепутанных фотонов, детекторы с разрешением числа фотонов, однофотонные преобразователи частоты, квантовая память), системы на их основе со скоростью квантового распределения ключей выше предела скорости прямой передачи [58].

19 апреля 2021 г. госкорпорацией «Ростелеком» и компанией «Транстелеком» (дочерней компанией «РЖД») с использованием оборудования Санкт-Петербургского НИУ информационных технологий, механики и оптики (Университет ИТМО), Российского квантового центра, компаний «Т8», «Системы практической безопасности», «С-Терра» построена и 8 июня введена в эксплуатацию первая в Российской Федерации квантовая линия связи между Москвой и Санкт-Петербургом протяженностью 800 км. Передача квантового распределения ключей позволяет апробировать квантовые технологии и сетевую архитектуру, стандартизировать и сертифицировать оборудование, развивать сотрудничество разработчиков, операторов связи и потребителей, обеспечивать спрос со стороны финансовых, государственных и ведомственных учреждений. Строительство этой сети предусмотрено дорожной картой развития квантовых коммуникаций, разработанной корпорацией «РЖД» и утвержденной правительством летом 2020 г., тогда же утверждено и техническое задание на создание квантовой сети между дата-центрами в Москве и Твери, а в 2021 г. начались проектно-изыскательские работы и строительство квантовой сети «РЖД» на участке Москва – Удомля [59] (административный центр Удомельского городского округа Тверской области).

ОТРАЖЕНИЕ ДОКУМЕНТОВ О КВАНТОВЫХ СЕТЯХ В БАЗАХ ДАННЫХ SCOPUS, GOOGLE SCHOLAR И ВИНТИ РАН

В базе данных Scopus [60] о квантовых сетях (на 27.04.2021) отражено 329 648 документов за 1953-2021 гг.: 2021 г. – 14 587, 2020 г. – 37 795, 2019 г. – 32 937, 2010 г. – 11 588, 2000 г. – 2611, 1990 г. – 703, 1980 г. – 159, 1970 г. – 39, 1960 г. – 2, 1953 г. – 1 документ.

По странам: на 1-м месте 85 317 документов Китая, на 2-м – 76 860 США, на 5-м – 21 786 Японии, и только на 13-м – 9944 документа Российской Федерации.

По отраслям знания: по физике – 136 020 документов, по ИТ – 57 979.

По типам документов: 240 034 статьи, 47 710 докладов конференций, 25 592 обзора, 3839 книг.

По типам источников: 268 316 статей из журналов, 40 719 материалов конференций, 11 132 монографии.

Из российских авторов отражены А.И. Иванов – 181 документ (Пензенский научно-исследовательский электротехнический институт) и В.Ю. Гаврилов – 172 (Самарский государственный медицинский университет).

По языкам: на английском – 322 835 документов, на китайском – 5665, на русском – 271, на японском – 186 документов.

По названиям источников: Proceedings of SPIE (Общество оптики и фотоники – Society of Photo-Optical Instrumentation Engineers, США) – 6392 документа, Optics Express – 3453, Physical Review Letters – 3431, Lecture Notes in Computer Science, включая серии Lecture Notes in Artificial Intelligence и Lecture Notes in Bioinformatics – 2348, IEEE (Институт инженеров электротехники и электроники – Institute of Electrical and Electronics Engineers, США) Photonics Technology Letters – 1630, IEEE Access – 1469, Optics Communications – 1424, International Conference on Transparent Optical Networks – 1341, Quantum Information Processing – 936, Optical and Quantum Electronics – 912, IEEE Journal on Selected Topics in Quantum Electronics – 728, IEEE Journal of Quantum Electronics – 726, IEEE Photonics Journal – 577, Advances in Intelligent Systems and Computing – 454, IEEE Journal of Selected Topics in Quantum Electronics – 383, Communications in Computer and Information Science – 375 документов.

По организациям: Национальный научный фонд Китая (Natural Science Foundation of China) – 42 222, Китайская академия наук (Chinese Academy of Sciences) – 11 499, Министерство образования Китая (Ministry of Education of the People's Republic of China) – 9111, Японское общество развития науки (Japan Society for the Promotion of Science) – 6218, Министерство энергетики США (U.S. Department of Energy) – 5562, Токийский университет – 2919, Китайский университет науки и технологий (University of Science and Technology of China) – 2894, Пекинский университет – 2875, Российская академия наук – 2748, Стэнфордский университет – 2278, Российский фонд фундаментальных исследований – 2062, японская корпорация Nippon Telegraph and Telephone Corporation – 1935, Японское агентство науки и технологий (Japan Science and Technology Agency – JST) – 1615, МГУ им. М.В. Ломоносова – 1440, Национальный институт стандартов и технологий США (National Institute of Standards and Technology – NIST) – 1293, Российский научный фонд – 1134, Институт инженеров электротехники и электроники США (Institute of Electrical and Electronics Engineers – IEEE) – 1073, Национальный институт информационных и

коммуникационных технологий (National Institute of Information and Communications – NICT, Япония) – 960, Министерство науки и высшего образования РФ – 693 документа.

В базе данных Google Scholar по теме квантовых сетей отражены 59 авторов, по теме квантовых коммуникаций – 88 авторов [61], из них российские исследователи: В.В. Макаров (5-й в рейтинге, 5771 цитирование, 76 документов, Российский квантовый центр, МИСиС), В.В. Чистяков (40-й в рейтинге, 304 цитирования, 71 документ, Университет ИТМО), С.М. Кынев (44-й в рейтинге, 177 цитирований, 14 статей, Университет ИТМО), А.С. Мастюкова (76-я в рейтинге, 8 цитирований, 4 статьи, Российский квантовый центр, МФТИ).

В Электронном каталоге ВИНТИ РАН [62] о квантовых коммуникациях отражены 454 статьи на английском и 387 статей на русском языках и четыре монографии на русском языке.

ЗАКЛЮЧЕНИЕ

Российская Федерация, как и другие мировые технологические лидеры, развивает технологии квантового распределения ключей и реализует проект квантовой телефонии. Межконтинентальная сеть квантовой связи протяженностью 10 тыс. км развивается специалистами РФ, Китая, Индии и ЮАР в рамках проекта БРИКС по квантовым коммуникациям при поддержке Российского фонда фундаментальных исследований. Китай – лидер по масштабам внедрения технологий квантовых коммуникаций, США делают ставку на разработку постквантовых алгоритмов криптографии, более устойчивых к кибератакам. Национальный институт стандартов и технологий США (NIST) ведет стандартизацию постквантовых решений.

В реализации национальных стратегических программ и проектов разработок квантовых технологий в Российской Федерации расширяется сотрудничество разработчиков (научных организаций), потребителей (заказчиков, компаний) и поддерживающих госорганов, развивается международное сотрудничество в рамках БРИКС, ЕС, ООН, международных организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Bennett C.H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W.K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels // Physical Review Letters. – 1993. – Vol. 70. – P. 1895-1899. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.70.1895> (дата обращения: 06.05.2021).
2. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20-22 Nov. 1994 // IEEE Computer Society Press. – 1994. – P. 124-134. – URL: <https://ieeexplore.ieee.org/document/365700> (дата обращения: 06.05.2021).
3. Rabin M.O. How to exchange secrets with oblivious transfer. Technical Report // Aiken Computation Lab, Harvard University, 1981. – 26 pp. – URL:

- <https://eprint.iacr.org/2005/187.pdf> (дата обращения: 05.06.2021).
4. Bennett С.Н., Brassard G. Quantum cryptography: public key distribution and coin tossing // International conference on computers, systems and signal processing. Bangalore, India, Dec. 9-12, 1984. – Vol. 1. – P. 175-179. – URL: <https://researcher.watson.ibm.com/researcher/files/us-bennet/BV84highest.pdf> (дата обращения: 05.06.2021).
 5. Ekert А.К. Quantum cryptography based on Bell's theorem // Physical Review Letters. – 1991. – Vol. 67. – P. 661-663. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661> (дата обращения: 05.06.2021).
 6. Bennett С.Н. Quantum cryptography: uncertainty in the service of privacy // Science. – 1992. – Vol. 257, Issue 5071. – P. 752-753. – URL: <https://science.sciencemag.org/content/257/5071/752> (дата обращения: 05.06.2021).
 7. Bennett С.Н., Brassard G., Mermin N.D. Quantum cryptography without Bell's theorem // Physical Review Letters. – 1992. – Vol. 68. – P. 557-559. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.557> (дата обращения: 05.06.2021).
 8. Goldenberg L., Vaidman L. Quantum cryptography based on orthogonal states // Physical Review Letters. – 1995. – Vol. 75. – P. 1239-1243. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.75.1239>; <http://philsci-archive.pitt.edu/564/1/paradox.pdf> (дата обращения: 05.06.2021).
 9. Mu Y., Seberry J., Zheng Y. Shared cryptographic bits via quantized quadrature phase amplitudes of light // Optics Communications. – 1996. – Vol. 123, Issues 1-3. – P. 344-352. – URL: <https://www.sciencedirect.com/science/article/abs/pii/S030401895006885?via%3Dihub> (дата обращения: 05.06.2021).
 10. Bechmann-Pasquinucci H., Gisin N. Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography // Physical Review A. – 1999. – Vol. 59. – P. 4238-4248. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevA.59.4238>; <https://arxiv.org/pdf/quant-ph/9807041.pdf> (дата обращения: 05.06.2021).
 11. Inoue K., Waks E., Yamamoto Y. Differential phase shift quantum key distribution // Physical Review Letters. – 2002. – Vol. 89. – P. 037902. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.89.037902> (дата обращения: 05.06.2021).
 12. Hwang W.Y. Quantum key distribution with high loss: toward global secure communication // Physical Review Letters. – 2003. – Vol. 91. – P. 057901. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.91.057901> (дата обращения: 05.06.2021).
 13. Gisin N. Quantum gloves: physics and Information. – URL: <https://arxiv.org/pdf/quant-ph/0408095.pdf> (дата обращения: 05.06.2021).
 14. Acín A., Gisin N., Scarani V. Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks // Physical Review A. – 2004. – Vol. 69. – P. 012309. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevA.69.012309>; <https://arxiv.org/abs/quant-ph/0302037> (дата обращения: 05.06.2021).
 15. Scarani V., Acín A., Ribordy G., Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations // Physical Review Letters. – 2004. – Vol. 92. – P. 057901 – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.92.057901> (дата обращения: 05.06.2021).
 16. Lo H.K., Ma X., Chen K. Decoy state quantum key distribution // Physical Review Letters. – 2005. – Vol. 94. – P. 230504. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.94.230504>; – URL: <https://arxiv.org/pdf/quant-ph/0411004.pdf> (дата обращения: 05.06.2021).
 17. Как S. A three-stage quantum cryptography protocol // Foundations of Physics Letters. – 2006. – Vol. 19. – P. 293-296. – URL: <https://link.springer.com/article/10.1007/s10702-006-0520-9> (дата обращения: 05.06.2021).
 18. Khan M.M., Murphy M., Beige A. High error-rate quantum key distribution for long-distance communication // New Journal of Physics. – 2009. – Vol. 11. – P. 063043. – URL: <https://iopscience.iop.org/article/10.1088/1367-2630/11/6/063043/meta> (дата обращения: 05.06.2021).
 19. Lo H.K., Curty M., Qi B. Measurement-device-independent quantum key distribution // Physical Review Letters. – 2012. – Vol. 108. – P. 130503. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.108.130503> (дата обращения: 05.06.2021).
 20. Mower J., Zhang Z., Desjardins P., Lee C., Shapiro J.H., Englund D. High-dimensional quantum key distribution using dispersive optics // Physical Review A. – 2013. – Vol. 87. – P. 062322. – URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevA.87.062322> (дата обращения: 05.06.2021).
 21. Эксперт рассказал о новом способе предотвращения киберугроз. – URL: <https://iz.ru/1128985/2021-02-24/ekspert-rasskazal-o-novom-sposobe-predotvrascheniia-kiberugroz> (дата обращения: 18.04.2021).
 22. Интервью руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий СК России К.П. Комарды ИА «ТАСС». – URL: <https://sledcom.ru/press/interview/item/1529946/> (дата обращения: 18.04.2021).
 23. Совет Европы. Конвенция о преступности в сфере компьютерной информации. – URL: <https://www.alppp.ru/law/pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii---185-rus--angl-.html> (дата обращения: 18.04.2021).
 24. Quantum Flagship. – URL: <https://qt.eu/about-quantum-flagship/newsroom/flagship-kickoff-in-vienna/> (дата обращения: 07.05.2021).
 25. Противодействие использованию информационно-коммуникационных технологий в преступных целях, ООН. – URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 18.04.2021).

26. Послание Президента Федеральному Собранию 01.12.2016. – URL: <http://kremlin.ru/events/president/news/53379> (дата обращения: 21.04.2021).
27. Послание Президента Федеральному Собранию 21.04.2021. – URL: <http://kremlin.ru/events/president/news/65418> (дата обращения: 25.04.2021).
28. О национальной программе «Цифровая экономика РФ». – URL: <https://digital.ac.gov.ru/about/> (дата обращения: 02.05.2021).
29. Латухина К. Путин призвал к лидерству по технологиям будущего. – URL: <https://rg.ru/2019/07/10/putin-prizval-k-liderstvu-po-tehnologii-i-budushchego.html> (дата обращения: 19.04.2021).
30. Документы: Направление «Цифровые технологии» / Министерство цифрового развития, связи и массовых коммуникаций РФ. – URL: <https://digital.gov.ru/ru/documents/?directions=878> (дата обращения: 07.05.2021).
31. Дорожная карта развития сквозной цифровой технологии «Нейротехнологии и искусственный интеллект». – URL: <https://digital.gov.ru/uploaded/files/07102019ii.pdf> (дата обращения: 19.04.2021).
32. «Сквозные технологии» дали новые всходы. – URL: https://www.comnews.ru/content/213111/2021-02-15/2021-w07/skvozyne-tehnologii-dali-novye-vskhody?utm_source=telegram&utm_medium=general&utm_campaign=general (дата обращения: 07.05.2021).
33. Паспорт Дорожной карты развития высокотехнологичной области «Квантовые коммуникации» на период до 2024 г. – URL: <https://digital.ac.gov.ru/upload/iblock/.pdf> (дата обращения: 02.05.2021).
34. Квантовые коммуникации в России будут прокладывать «РЖД» и «Ростелеком». – URL: <https://eadaily.com/ru/news/2020/01/13/kvantovye-kommunikacii-v-rossii-budut-prokladivat-rzhd-i-rostelekom> (дата обращения: 19.04.2021).
35. От однофотонных детекторов к национальным квантовым сетям: как развиваются квантовые технологии в России? – URL: <http://1234g.ru/novosti/kvantovye-tehnologii-v-rossii> (дата обращения: 17.05.2021).
36. Факультет физической и квантовой электроники МФТИ. – URL: <https://mipt.ru/dpqe/> (дата обращения: 19.04.2021).
37. Кафедра квантовой электроники // Физический факультет МГУ им М.В. Ломоносова. – URL: <https://www.phys.msu.ru/rus/about/structure/div/div-radiophysics/chair-quantum-electronics/> (дата обращения: 17.05.2021).
38. Центр квантовых технологий МГУ им. М.В. Ломоносова. – URL: <https://quantum.msu.ru/ru/about> (дата обращения: 19.04.2021).
39. Weissberger A. Quantum Telephony Network deployed at Moscow State University using Vipnet QSS. – URL: <https://techblog.comsoc.org/2021/01/12/quantum-telephony-network-deployed-at-moscow-state-university-using-vipnet-qss/> (дата обращения: 19.04.2021).
40. Отдел математических методов квантовых технологий МИАН. – URL: http://www.mi-ras.ru/index.php?c=show_dep&id=51 (дата обращения: 19.04.2021).
41. Центр фотоники и квантовых материалов Сколтеха. – URL: <https://crei.skoltech.ru/cpqm/ru/> (дата обращения: 23.04.2021).
42. Квантовые коммуникации – это новый уровень противостояния угрозам в IT-системе «РЖД». – URL: <https://www.rzd-partner.ru/zhd-transport/interview/kvantovye-kommunikatsii-eto-novyy-uroven-protivostoyaniya-ugrozam-v-it-sisteme-rzhd/> (дата обращения: 22.04.2021).
43. Российский квантовый центр. – URL: <https://rqc.ru/about> (дата обращения: 19.04.2021).
44. QRate. – URL: <https://goqr.com/ru#about> (дата обращения: 19.04.2021).
45. S-Terra. – URL: <https://www.s-terra.ru/company/> (дата обращения: 19.04.2021).
46. КриптоПро. – URL: <https://www.cryptopro.ru/about> (дата обращения: 19.04.2021).
47. SCONTEL. – URL: <https://www.scontel.ru/ru/company/> (дата обращения: 19.04.2021).
48. Национальная технологическая инициатива. 20.35. – URL: <https://ntinews.ru/news/tsifrovaya-ekonomika/rossiyskiy-kvantovyy-tsentr-otkryl-dveridlya-studentov.html> (дата обращения: 21.04.2021).
49. Базовая кафедра квантовой оптики и телекоммуникаций НИУ ВШЭ. – URL: <https://miem.hse.ru/edu/ee/scontel/> (дата обращения: 22.04.2021).
50. Квантовые коммуникации и фемтотехнологии / Университет ИТМО. – URL: https://itmo.ru/ru/viewjper/74/kvantovye_kommunikacii_i_femtotehnologii.htm (дата обращения: 22.04.2021).
51. Семинары «Квантовые компьютеры» / ФТИАН им. К.А. Валиева РАН. – URL: <http://www.ftian.ru/seminars/?type=qj> (дата обращения: 22.04.2021).
52. Казанский квантовый центр. – URL: <https://kai.ru/quantumcenter> (дата обращения: 22.04.2021).
53. Технологии обработки информации на основе сверхпроводящих кубитов / Фонд перспективных исследований. – URL: <https://fpi.gov.ru/projects/informatsionnye-issledovaniya/liman/> (дата обращения: 23.04.2021).
54. РФФ: Проект «Взаимодействие закрученного света с отдельными атомами и атомными ансамблями». – URL: <https://rscf.ru/project/21-42-04412/> (дата обращения: 05.06.2021).
55. Инновационный центр «Квантовая долина» создадут в Нижегородской области. – URL: <https://www.niann.ru/?id=548777> (дата обращения: 31.05.2021).
56. Правительство утвердило перечень технологий для «регуляторных песочниц». – URL: <https://www.kommersant.ru/doc/4550567> (дата обращения: 19.04.2021).
57. Россия занялась созданием межконтинентального канала квантовой связи. – URL: https://www.cnews.ru/news/top/2020-10-30_rossiya_zanyalas_sozdaniem (дата обращения: 19.04.2021).

58. Научный совет при президиуме РАН «Квантовые технологии». – URL: <http://www.ras.ru/news/shownews.aspx?id=989c167f-6ca0-436c-affa-379bdbb40bae> (дата обращения: 19.04.2021).
59. «Транстелеком» построил квантовую сеть Москва – Петербург. – URL: <https://www.vedomosti.ru/technology/articles/2021/04/19/866704-transtelekom-postroil> (дата обращения: 31.05.2021).
60. Scopus. – URL: <https://www.scopus.com/> (дата обращения: 27.04.2021).
61. Google Scholar. – URL: https://scholar.google.com/citations?view_op=search_authors&hl=en&mauthor=label:quantum_communications&before_author=w2_8_2AKAAAJ&astart=0 (дата обращения: 05.06.2021).
62. Электронный каталог ВИНТИ РАН. – URL: http://catalog.viniti.ru/srch_result.aspx?IRL=QUERY+ID%3a2721255&ADV=FILTER:eARTC (дата обращения: 05.06.2021).

Материал поступил в редакцию 05.06.21.

Сведения об авторе

СУХОРУЧКИНА Ирина Николаевна – кандидат технических наук, старший научный сотрудник Технологического отделения, ВИНТИ РАН, Москва.
e-mail: insukhoruchkina@mail.ru