№20
Апрель 2024

indata
ФОНД РАЗВИТИЯ СЕТЕВЫХ ТЕХНОЛОГИЙ «ИНДАТА»

Интернет изнутри

КВАНТОВЫЕ ТЕХНОЛОГИИ

Интернет в цифрах

Применение квантовых вычислений в России и в мире

с. 8

Сети квантового распределения ключей

Новый уровень сервисов информационной безопасности национальной сети Интернет

с. 10

Квантовые коммуникации

Станут ли квантовые коммуникации новым Интернетом?

с. 20

Постквантовая криптография и практика TLS в браузерах

Постквантовая криптосистема должна появиться раньше квантового компьютера

с. 26

Управление Интернетом в 2024 году

Взаимовыгодное сотрудничество или игра с нулевой суммой?

с. 48

РосНИИРОС: как все начиналось

Рассказываем о том, как 30 лет назад появился домен .ru

с. 59

О развитии высокотехнологичного направления «Квантовые коммуникации»

Как ОАО «РЖД» создает экосистему квантовых коммуникаций в России

с. 2

Содержание:

Передовица
с. 2 О развитии высокотехнологичного направления «Квантовые коммуникации»

Интернет в цифрах
с. 8 Инфографика

Технология в деталях
с. 10 Сети квантового распределения ключей – новый уровень сервисов информационной безопасности национальной сети Интернет

с. 16 На пути к квантовому Интернету

с. 20 Квантовые коммуникации — сети квантового распределения ключей или новый Интернет?

с. 26 Постквантовая криптография и практика TLS в браузерах

Технология и рынок
с. 31 Квантовые коммуникации: «пик хайпа» или «плато продуктивности» с точки зрения дилетанта

Наука и образование
с. 38 Квантовое превосходство при решении вычислительных задач

с. 43 Квантовые коммуникации через атмосферные (космические) каналы связи

Управление Интернетом
с. 48 Управление Интернетом в 2024 году: взаимовыгодное сотрудничество или игра с нулевой суммой?

Политика
с. 54 Европейский союз на пути к цифровому суверенитету?

Исторический ракурс
с. 59 РосНИИРОС: как всё начиналось

Новости
с. 66 Новости науки и техники

с. 68 ICANN79 Community Forum: краткий обзор

Сетевое издание
Журнал **«Интернет изнутри»**
info@internetinside.ru

Выпуск №20, дата выхода:
Апрель 2024 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ЭЛ № ФС 77 – 85232 от 25.04.2023
ISSN: 2949-1967

Все статьи размещаются и индексируются в НЭБ «e-Library

Издатель: **Фонд развития сетевых технологий «ИнДата»**

Главный редактор:
Алексей Платонов

Выпускающий редактор:
Ирина Пыжова

Редакционная коллегия:
Елена Воронина
Марат Биктимиров

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Дмитрий Ивлянов

Корректор:
Наталья Рябова

Обложка разработана с использованием ресурсов сайта Freepik.com

Квантовая запутанность

Дорогой читатель,
Хотя классические компьютерные технологии и приложения достигли неимоверной сложности, основополагающие принципы остаются достаточно простыми. В конце концов, основной строительный блок – бит – может принимать два значения: 0 или 1 — есть сигнал или нет. Совсем по-другому обстоят дела в квантовых вычислениях. Базовая единица информации здесь – так называемый кубит – может находиться в состоянии 0, 1 или любой квантовой суперпозиции этих двух состояний! Парадокс заключается в том, что усложнение базовой единицы информации в конечном счёте приводит к упрощению вычислений и их масштабируемости. Это всё равно как переход от линейной алгебры к векторному исчислению, открывающий новые просторы решаемых задач!

Неудивительно, что квантовые технологии и квантовые вычисления привлекают так много внимания. Их потенциальные приложения обширны – от эффективного моделирования физических систем, например, при разработке лекарств нового поколения, финансового моделирования и машинного обучения, до криптографии, где уникальные свойства квантовой механики позволяют обеспечить защищённую передачу ключей шифрования между участниками.

В этом номере мы познакомим вас с текущим состоянием квантовой индустрии и различными аспектами квантовых технологий и приложений.

Открывает журнал статья, подготовленная редакцией журнала по материалам ОАО «РЖД» – «О развитии высокотехнологичного направления «Квантовые коммуникации». Основная тема статьи, впрочем, как и нескольких других статей – тенденции, проблематика и достижения в области квантовых коммуникаций и квантового Интернета, в особенности это применимо к квантовому распределению криптографический ключей. К раскрытию этой интересной темы подключились и другие авторы со своими статьями: Владимир Егоров, Владимир Елисеев, Алексей Сантьев, Павел Храмцов, Валерий Киселёв и Луис Ханотел. А целая группа авторов из МГУ – Андрей Деев, Александр Калинкин, Сергей Кулик, Александр Миллер, Иван Полухин – раскрывает секреты того, как можно осуществлять квантовые коммуникации через космические каналы связи.

Квантовые технологии могут использоваться не только для усиления защищённости данных, но и для взлома существующих и широко используемых криптографических алгоритмов. Поэтому важной задачей является создание и внедрение так называемой постквантовой криптографии с использованием алгоритмов, устойчивых к атакам с использованием квантовых компьютеров. Об этих алгоритмах и перспективах их использования во Всемирной паутине рассказывает Александр Венедюхин.

Вольфганг Кляйнвахтер размышляет над вопросами управления Интернетом в сегодняшних реалиях. Способно ли мировое сообщество, несмотря на все политические, экономические и культурные различия, находить общие решения для дальнейшего развития нашей цифровой среды, или Интернет будет объектом политических игр с нулевой суммой?

Этот номер журнала выходит в начале апреля, когда отмечается очень важная для развития российского Интернета дата – 7 апреля российскому национальному домену .ru исполняется 30 лет. К этому юбилею мы подготовили интервью с Алексеем Лесниковым – непосредственным участником событий 30-летней давности, который рассказывает, как рождался и развивался Рунет.

Ну и, конечно, мы продолжаем поддерживать наши традиционные разделы. В разделе «Политика» Мадина Касенова предлагает анализ стратегии Евросоюза в области квантовых технологий. А в «Новостях» мы познакомим вас с интересными фактами об Интернете и доменной индустрии.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках? Пишите нам по адресу info@internetinside.ru.

Редакция журнала

О развитии высокотехнологичного направления «Квантовые коммуникации»

Статья подготовлена редакцией журнала «Интернет изнутри» по материалам ОАО «РЖД»

Современный этап развития информационных технологий характеризуется стремлением к повышению уровня безопасности передаваемых данных. Рост числа кибератак и увеличение геополитического противостояния делают вопросы безопасности информационной инфраструктуры еще более актуальными. В связи с этим возрастает спрос на разработку и внедрение новых, более надежных технологий защиты данных, в том числе в сферах, где активно используются технологии Интернета вещей. В этом контексте особое внимание уделяется квантовым коммуникациям, представляющим собой передовую область знаний и технологий для создания защищенных каналов связи с использованием квантового распределения ключей (КРК) [1].

Развитие высокотехнологичного направления «Квантовые коммуникации» имеет критически важное значение для создания комплексной защищенной инфраструктуры цифровой экономики, в том числе для системы государственного управления, особенно с учетом возрастающих угроз в области информационной безопасности.

В России создан значительный научно-технологический задел в области технологий и оборудования квантовых коммуникаций. Задача ОАО «РЖД» как компании-лидера в деле организации экосистемы квантовых коммуникаций – трансформировать этот задел в крупные инфраструктурные проекты, обеспечить дальнейшую разработку технологий и решений, содействовать развитию экосистемы и рынка квантовых коммуникаций, что выведет Российскую Федерацию на лидирующие позиции по данному направлению в мире.

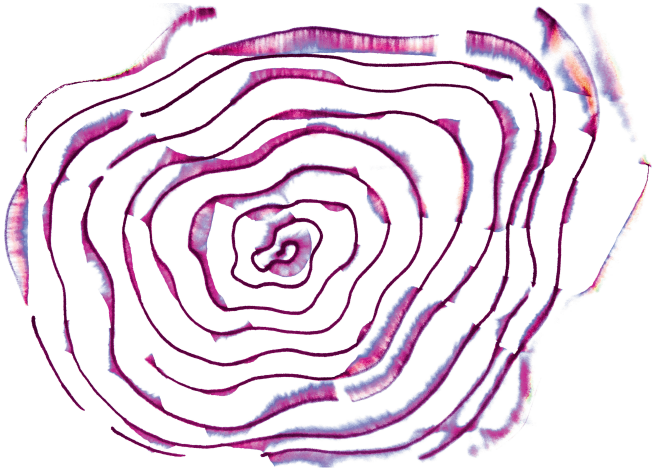
С целью развития высокотехнологичного направления «Квантовые коммуникации» между ОАО «РЖД» и правительством Российской Федерации заключены соответствующие соглашения от 10 июля 2019 г. № 88 [2] и от 29 декабря 2022 г. № 186 (рис. 1). Основным механизмом выполнения соглашения является реализация «дорожной карты» развития высокотехнологичного направления «Квантовые коммуникации» на период до 2030 года.

В настоящее время ОАО «РЖД» продолжает масштабные работы по развитию квантовых коммуникаций, решая три основные задачи: по развитию технологий, инфраструктуры и экосистемы.

Прогресс в технологиях квантовых коммуникаций способствует развитию всего высокотехнологичного направления

Рис. 1. Заключение соглашения о намерениях между Правительством Российской Федерации и ОАО «РЖД» 29 декабря 2022 г.

в целом. Сегодня большинство исследовательских и коммерческих разработок направлено на разработку квантовых сетей и их составных частей, особое внимание уделяется разработке уникальной компонентной базы и созданию аппаратуры квантового распределения ключей. При этом в последние годы наблюдается тенденция развития и создания именно пользовательских устройств и готовых решений, пригодных к использованию конечными абонентами. Это происходит по причине повышения интереса конечных потребителей к эксплуатации решений на квантовых коммуникациях.



Квантовые коммуникационные сети могут быть реализованы на основе волоконно-оптических, атмосферных и космических линий связи. Все разновидности квантовых сетей взаимосвязаны, но используются для разных целевых аудиторий потребителей и применяют разнообразные технические решения.

Оптоволоконные квантовые сети уже сегодня находятся на стадии развития, готовой к внедрению и эксплуатации после прохождения соответствующих процедур сертификации и аттестации. Технологии атмосферных оптических квантовых каналов и космической квантовой связи хотя и находятся на более ранних стадиях развития, также демонстрируют значительный потенциал.

Разработаны технические решения для магистральной инфраструктуры квантовых коммуникаций, обеспечивающих защищенную передачу данных в корпоративных сетях: архитектурные решения, оборудование, программное обеспечение, система доверенных узлов, система мониторинга.

Так, в 2024-2025 годах ожидается завершение целого ряда научно-технических проектов, направленных на разработку и создание ключевых отечественных технологий и элементной базы. Ведется работа по развитию перспективных технологий квантовых коммуникаций (квантовые повторители, протоколы на запутанных состояниях, источники однофотонных состояний и др.), а также разработке компонентной базы (оптические фильтры, детекторы одиночных фотонов и др.).

Перспективы развития квантовых коммуникаций связаны с технологиями атмосферной и спутниковой квантовой связи. Разработки в этом направлении ведутся силами целого ряда научных организаций. Созданы прототипы оборудования для атмосферной квантовой связи в Университете ИТМО, в центрах компетенций НТИ «Квантовые коммуникации» на базе НИТУ МИСиС и «Квантовые технологии» на базе МГУ им. М. В. Ломоносова.

Сформирована кооперация научно-исследовательских организаций и университетов для реализации эксперимента по отработке космической оптической линии связи и квантового канала распределения ключей. Данный проект будет включать создание и вывод на орбиту малого космического аппарата спутникового сегмента квантовой сети, а также разработку концепции космической группировки, и будет запущен в ближайшие несколько месяцев. Реализация технологии спутниковых квантовых коммуникаций объединит спутниковый и наземный сегменты квантовой сети, тем самым обеспечив бесшовное взаимодействие подключенных абонентов отечественной цифровой квантовой платформы.

Сервисы на основе сетей КРК

Технологии квантовых коммуникаций нашли применение в ряде продуктов, которые позволяют создавать сервисы на основе сетей КРК для конечных пользователей. В целом можно сказать, что происходит поэтапное движение к практическому внедрению технологии квантовых коммуникаций и возможности их коммерциализации. В РЖД была проведена работа по исследованию первоочередных задач по внедрению технологий квантовой защиты информации на инфраструктуре железнодорожного транспорта. Предполагается, что одним из первых направлений, где будут использованы технологии квантовой защиты информации, станет формирование защищенных квантовых каналов связи на полигоне Московского центрального кольца.

Следующим этапом и основной задачей после завершения процедур сертификации квантового оборудования и аттестации сетей станет предоставление коммерческих продуктов и сервисов потребителям. И уже сейчас совместно с операторами связи (ЗАО «Компания ТрансТелеКом», ПАО «Ростелеком» и др.) сформирована модель коммерциализации, проводятся пилотные подключения с целью демонстрации и тестирования технологии.

В 2023 году проведен анализ ведущих мировых компаний, опрошено более 100 потенциальных потребителей услуг в России. По результатам данных исследований появилось понимание, какие сервисы будут наиболее востребованы потенциальными клиентами. При этом сервисная модель развития рынка признана наиболее оптимальной, поскольку строительство магистральной инфраструктуры требует значительных капитальных затрат.

Существующий опыт развития технологии квантовых коммуникаций, мнение экспертного сообщества в Российской Федерации и в мире предполагают на данный момент оказание на базе квантовой сети ОАО «РЖД» двух основных видов услуг, к которым относятся:

- услуга «ключ как сервис» – передача сформированного на магистральных сегментах квантовой сети квантово-защищенного ключа оператором квантовой сети для использования клиентом (конечным потребителем или оператором более высокого уровня) на собственных средствах криптографической защиты информации (СКЗИ) (рис. 2);

- услуга по предоставлению квантово-защищенных каналов передачи данных «КВАНТ VPN» – применяется оператором ключа для оказания услуг предоставления конечным потребителям квантово-защищенного VPN, представляющего собой предоставление канала с защитой передаваемого трафика между точками оказания услуг с использованием квантово-защищенного ключа и на базе телекоммуникационной инфраструктуры предоставляющего услугу оператора (в т.ч. арендованных им каналов) (рис. 3).

Рис. 2. Схема реализации услуги «ключ как сервис» и роли участников.

Спектр применения технологий КРК может оказаться намного шире. Для выявления новых перспективных услуг необходим детальный анализ потребностей в управлении информацией в различных отраслях экономики.

В настоящее время при поддержке ОАО «РЖД» ведется или планируется разработка решений, направленных на создание сервисов квантовых коммуникаций: клиентские устройства, доверенные узлы с повышенной пропускной способностью, разработка архитектурных решений, шлюзы мультивендорного сопряжения, прикладное ПО, автоматизированная информационная система предоставления сервисов с гарантированным SLA, система учета и расчетов для сервисов квантовых коммуникаций, зонтичная система управления инцидентами 24/7.

Основными клиентами сервисов КРК станут государственные и финансовые организации, владельцы объектов критической информационной инфраструктуры в области транспорта, энергетики и ТЭК, здравоохранения, связи и др.

С целью обеспечения необходимого географического охвата создается магистральная квантовая сеть ОАО «РЖД», что позволит в перспективе снять технологический барьер для того, чтобы телеком-операторы могли оказывать клиентам, находящимся в различных регионах страны, услуги на основе технологии квантовых коммуникаций.

По итогам 2023 года протяженность квантовой сети в Российской Федерации составила более 3200 км, объединены такие города, как Москва, Санкт-Петербург, Нижний Новгород, Ростов-на-Дону, Казань и другие [3].

В текущем году к квантовой сети будут присоединены Сочи и Екатеринбург, общая протяженность сетей составит 7000 км. По итогам 2030 года планируется создание магистральной инфраструктуры, которая обеспечит необходимый и достаточный географический охват, требуемый потенциальным потребителям внутри страны.

Дальнейшим этапом развития инфраструктуры квантовых сетей станет создание многопользовательских масштабируемых сетей, построенных с использованием оборудования различных вендоров. Такого рода сети состоят из двух или более узлов, соединенных между собой оптоволоконным или атмосферным каналом связи. На каждом сегменте такой сети вырабатываются квантовые ключи, которые служат для передачи ключевой информации (симметричных секретных ключей) потребителям, в качестве которых могут выступать аппаратные или программные СКЗИ.

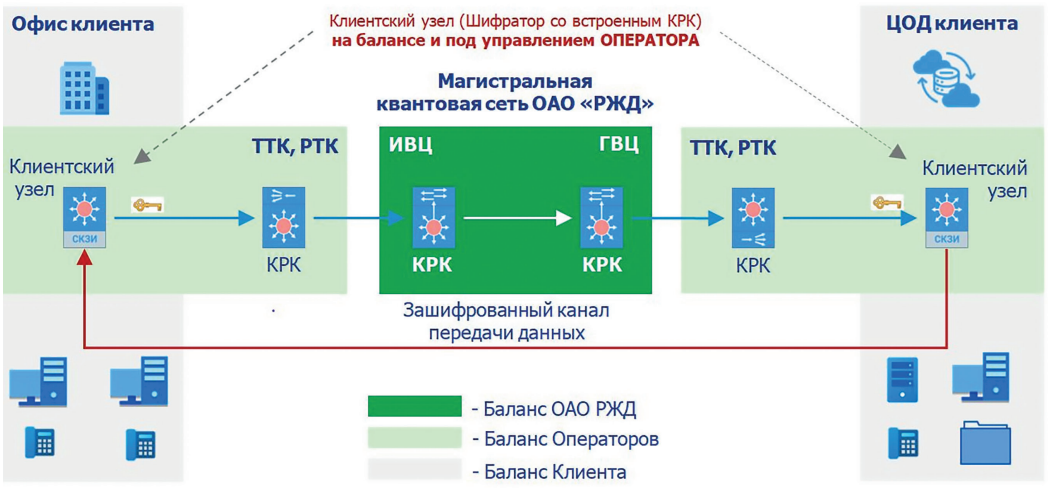
Архитектура квантовой коммуникационной сети

В рамках выполнения данной задачи ОАО «РЖД» совместно с ПАО «Ростелеком» инициировали работу по разработке архитектуры и методов построения данных сетей с учетом возникающих вопросов по сопряжению разных сегментов сети (магистральных, клиентских) в единое целое.

В настоящее время разработана 5-уровневая структура масштабируемой многопользовательской квантовой коммуникационной сети (ККС), содержащей следующие функциональные уровни (рис. 4):

- уровень формирования квантовых ключей;
- уровень распределения ключевой информации;
- коммуникационный (транспортный) уровень;
- уровень управления и мониторинга;
- уровень потребителей ключевой информации.

Поскольку квантовая связь осуществляется с помощью одиночных фотонов, то есть очень слабых оптических импульсов, потери при прохождении импульса света по оптико-волоконному кабелю ограничивают квантовую связь расстояниями порядка 100 км. Фотоны распространяются в пределах небольших участков, между которыми находятся промежуточные доверенные узлы. Такие узлы снабжены оборудова-



ОАО «РЖД»
- Обеспечение транзита квантового ключа (клиенты – Операторы)
- Мониторинг
- Управление инфраструктурой

Оператор связи
- Предоставление конечному клиенту канала передачи данных
- «Последняя миля»
- Предоставление конечным клиентам квантового оборудования
- СКЗИ

Конечный клиент
- Получение комплексной услуги Оператора по сервисному договору, включая специализированное оборудование на своей стороне

Рис. 3. Схема реализации услуги по предоставлению квантово-защищенных каналов передачи данных «КВАНТ VPN» и роли участников.

нием квантового распределения ключей, средствами криптографической защиты информации, сетевым оборудованием, системами бесперебойного питания и климатическими системами, а также системами централизованного мониторинга активного оборудования.

В дальнейшем за счет подключения к доверенным узлам телекоммуникационных операторов станет возможным реализовать последнюю милю и предложить услугу квантового распределения ключей конечному потребителю.

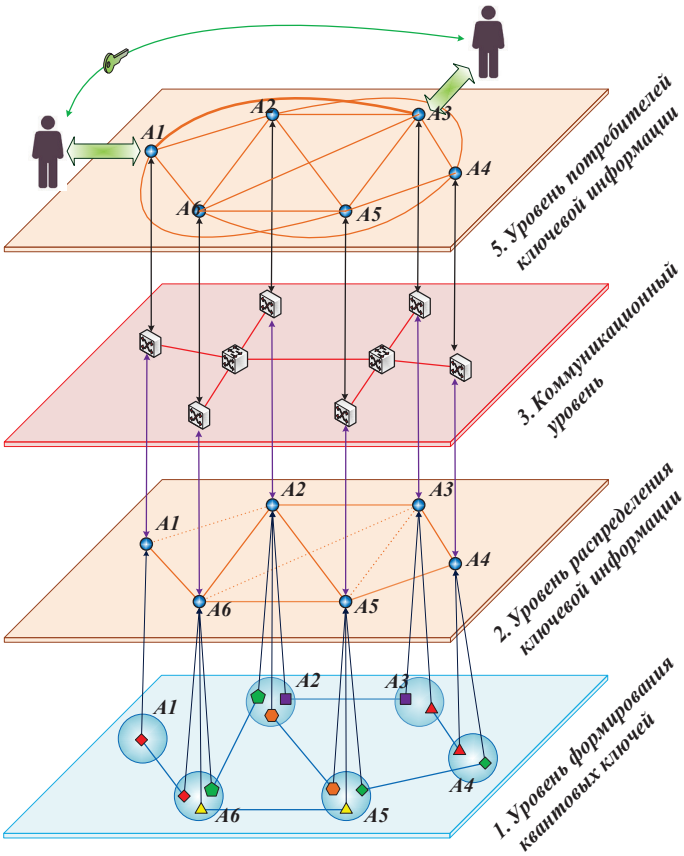


Рис. 4. Структура масштабируемой многопользовательской квантовой коммуникационной сети.

Также ведется непрерывная работа по развитию экосистемы, включая совершенствование нормативного регулирования, стандартизацию, развитие кадрового потенциала, информационное продвижение. В настоящее время реестр экосистемы уже включает более 140 организаций.

Нормативно-техническая база

Для необходимого перехода к единому пониманию сути обсуждения проблем в области квантовых коммуникаций начато формирование нормативно-технического ландшафта [4].

Утверждена Концепция регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года [5], определяющая основные подходы к развитию системы нормативного регулирования в Российской Федерации отрасли квантовых коммуникаций для обеспечения глобальной технологической конкурентоспособности.

Разработаны и утверждены приказами Росстандарта шесть предварительных национальных стандартов, которые, пройдя апробацию рынком, должны будут стать национальным регламентом [6-7]:

- «Квантовые коммуникации. Общие положения»: устанавливает общие положения в области квантовых коммуникаций.
- «Квантовые коммуникации. Термины и определения»: устанавливает термины и определения в области квантовых коммуникаций.
- «Квантовый интернет вещей. Общие положения»: устанавливает общие положения в области квантового Интернета вещей.
- «Квантовый интернет вещей. Термины и определения»: устанавливает термины и определения в области квантового Интернета вещей.

- «Квантовый интернет вещей. Типовой программно-аппаратный комплекс распределения ключей, выработанных сетью квантового распределения ключей. Архитектура»: устанавливает архитектуру типового программно-аппаратного комплекса распределения ключей, выработанных сетью КРК, и обеспечивающего защищенную доставку ключей, выработанных сетями КРК, до устройств квантового Интернета вещей, прямое подключение которых к сетям КРК технически невозможно или нецелесообразно.

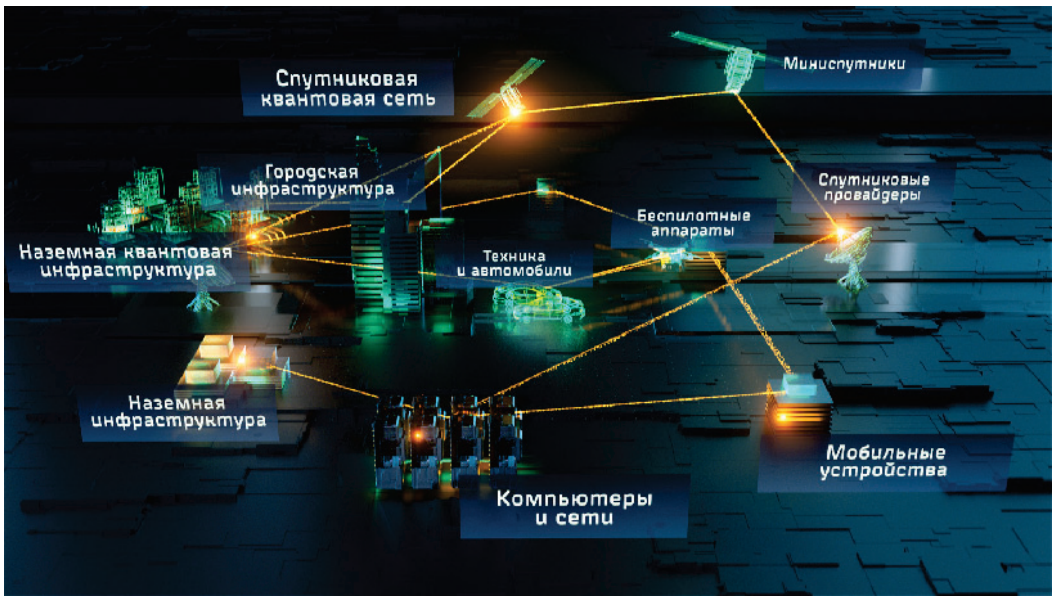


Рис. 5. Глобальная квантово-защищенная доверенная среда.

- «Квантовый интернет вещей. Типовой программно-аппаратный комплекс распределения ключей, выработанных сетью квантового распределения ключей. Интерфейсы подключения»: устанавливает требования к интерфейсам подключения типового программно-аппаратного комплекса распределения ключей, выработанных сетью КРК, в части интерфейса взаимодействия с сетью КРК, а также интерфейсов передачи квантовых и квантово-защищенных ключей на терминалы квантового Интернета вещей.

Для реализации функции стандартизации оборудования, используемого при проектировании квантовых сетей, ведутся работы по разработке Рекомендаций по стандартизации совместно с техническим комитетом по стандартизации «Криптографическая защита информации» (ТК-26).

Разработаны и утверждены рекомендации по стандартизации «Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации» [8], предназначенные для защиты передаваемых секретных ключей, случайных чисел и сервисной информации. Необходимость их разработки вызвана потребностью в обеспечении совместимости между квантово-криптографической аппаратурой выработки и распределения ключей и средствами криптографической защиты информатизации от различных производителей.

Разрабатываются Рекомендации по стандартизации, которые описывают ключевые системы, определяющие процесс создания целевых ключей квантовой криптографической системы в топологии «звезда» и произвольной топологии: «Информационная технология. Криптографическая защита информации. Ключевая система сети шифрованной связи с использованием ККС ВРК с сетевой топологией «звезда» и «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ».

Подготовка специалистов

Решение задач разработки и внедрения технологий квантовых коммуникаций требует особого внимания к вопросам подготовки специалистов с соответствующими знаниями и умениями.

В настоящее время около 30 российских вузов (МГУ им. Ломоносова, МИСиС, ИТМО, СПбГУТ им. Бонч-Бруевича, КНИТУ-КАИ и другие ведущие университеты) реализуют образовательные программы бакалавриата, магистратуры, аспирантуры в области квантовых коммуникаций и в смежных областях. На сегодняшний день подготовлено более 400 выпускников по 22 образовательным программам.

В целях обеспечения единства требований к формированию образовательных программ для подготовки высококвалифицированных специалистов в области квантовых коммуникаций и оценке их профессиональной квалификации разработаны и утверждены два профессиональных стандарта в области квантовых коммуникаций: «Специалист по монтажу и технической эксплуатации квантовых сетей» (вступил в силу с 1 марта 2023 года) [9] и «Специалист по исследованиям и разработкам в области квантовых коммуникаций» (вступил в силу с 1 сентября 2023 года) [10]. Профстандарты описывают деятельность и требования к квалификации специалистов, при этом первый стандарт включает функции по монтажу и эксплуатации линий связи и оборудования квантовых сетей, организации технического обслуживания, локализации и устранения аварий, а второй – функции лаборантов, инженеров-исследователей и научных сотрудников, а также руководителей разных уровней вплоть до главного конструктора организации, осуществляющего исследования и разработки в области квантовых коммуникаций. Также в профстандартах изложены требования к выпускникам организаций высшего и среднего профессионального образования, планирующим связать свою профессиональную деятельность с квантовыми коммуникациями.

На основании указанных профстандартов разработан и утвержден федеральный государственный образовательный стандарт среднего профессионального образования по специальности «Квантовые коммуникации» [11].

Совместно с ОАО «Межведомственный аналитический центр» в 2021-2023 годах проведена большая аналитическая работа по прогнозированию кадровых потребностей в отрасли до 2030 года. Сформированный прогноз коррелирует с текущим и планируемым темпами подготовки кадров. Согласно прогнозу к 2030 году потребуется более 1300 специалистов с профильным высшим образованием и 7000 специалистов со средним профессиональным образованием.

Одним из мероприятий «дорожной карты» является развитие системы онлайн-образования в области квантовых коммуникаций, в рамках которого предусмотрена разработка дистанционных образовательных курсов. Для изучения уже доступны восемь онлайн-курсов различной направленности и сложности.

Взгляд в будущее

Текущими задачами развития технологии и формирования нового рынка предоставления услуг и сервисов, в том числе в рамках нового национального проекта «Экономика данных», являются:

- обеспечение сертификации линейки разрабатываемого оборудования и аттестации квантовых сетей;
- создание и внедрение конкурентоспособных экономически эффективных решений;
- создание условий для развития сетей доступа и обеспечение доступности сервиса, в том числе с использованием атмосферных и космических систем квантовых коммуникаций;
- создание отраслевых решений в области квантовых коммуникаций как составляющей комплексной системы информационной безопасности на объектах критической информационной инфраструктуры, в финансовом секторе, в государственных информационных системах, в автономных системах, в здравоохранении и др.;
- внедрение технологии квантовых коммуникаций в действующую информационную инфраструктуру (рис. 5).

Последующим этапом развития планируется создание элементов квантового Интернета и переход к глобальной квантовой доверенной среде, объединяющей в себе взаимодействие наземной и космической инфраструктуры, малых спутников и летательных аппаратов, беспилотного транспорта и мобильных устройств через сеть дата-центров.

Проводимая РЖД, а также другими участниками экосистемы квантовых коммуникаций работа позволит создать комплексную защищённую инфраструктуру цифровой экономики, системы государственного управления, что особенно важно с учетом непрерывно возрастающих угроз в области информационной безопасности.

Список литературы:

[1] Развитие отдельных высокотехнологичных направлений. Белая книга // НИУ «Высшая школа экономики»: сайт. 2022. С. 93. URL: https://issek.hse.ru/mirror/pubs/share/565446894.pdf

[2] Подписаны соглашения о намерениях между правительством и крупными компаниями о развитии отдельных высокотехнологичных направлений // D-Russia.ru: сайт. 2019. 10 июля. URL: https://d-russia.ru/podpisany-soglasheniya-o-namereniyah-mezhdu-pravitelstvom-i-krupnymi-kompaniyami-o-razvitii-otdelnyh-vysokotehnologichnyh-napravlenij.html

[3] Путин спрогнозировал охват квантовых сетей железных дорог к концу 2024 года // РИА Новости: сайт. 2023. 15 декабря. URL: https://ria.ru/20231215/putin-1916051342.html

[4] Бровкина М. «Кванты: как РЖД работают над технологиями будущего» // Бюллетень Правового департамента ОАО «РЖД». 2023. № 3-4 (51-52). С. 19-26

[5] Распоряжение Правительства Российской Федерации от 11 июля 2023 г. № 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года»

[6] Приказы Федерального агентства по техническому регулированию и метрологии от 11 июля 2023 г. №№ 22-пнст, 23-пнст, 24-пнст, 25-пнст «Об утверждении предварительного национального стандарта Российской Федерации»

[7] Приказы Федерального агентства по техническому регулированию и метрологии от 29 декабря 2023 г. №№ 117-пнст, 118-пнст «Об утверждении предварительного национального стандарта Российской Федерации»

[8] Приказ Федерального агентства по техническому регулированию и метрологии от 30 ноября 2023 г. № 1510-ст «Об утверждении рекомендаций по стандартизации»

[9] Приказ Минтруда России от 24 октября 2022 г. № 685н «Об утверждении профессионального стандарта «Специалист по монтажу и технической эксплуатации квантовых сетей»

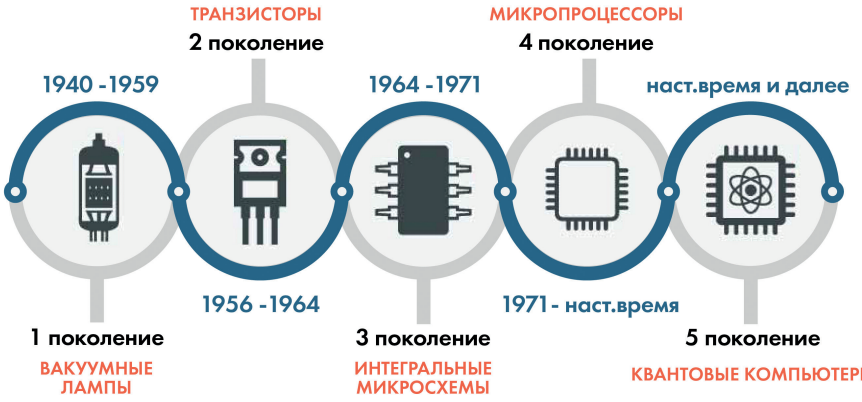
[10] Приказ Минтруда России от 25 апреля 2023 г. № 327н «Об утверждении профессионального стандарта «Специалист по исследованиям и разработкам в области квантовых коммуникаций»

[11] Приказ Минпросвещения России от 13 июля 2023 г. № 529 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.19 Квантовые коммуникации»

Интернет в цифрах

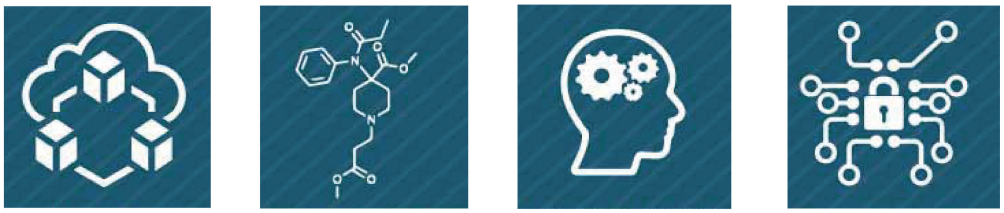
ЭТАПЫ РАЗВИТИЯ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Начало эры квантовых вычислений обеспечено технологическим переходом к компьютерной технике пятого поколения.



ПРИМЕНЕНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Вследствие наступившей огромной зависимости от больших данных, квантовый компьютер с экспоненциально более высокой скоростью вычислений будет гораздо эффективнее, чем классические вычислительные средства. Это означает, что в будущем можно решать задачи, которые ранее считались неразрешимыми, достигая таким образом «квантового превосходства».

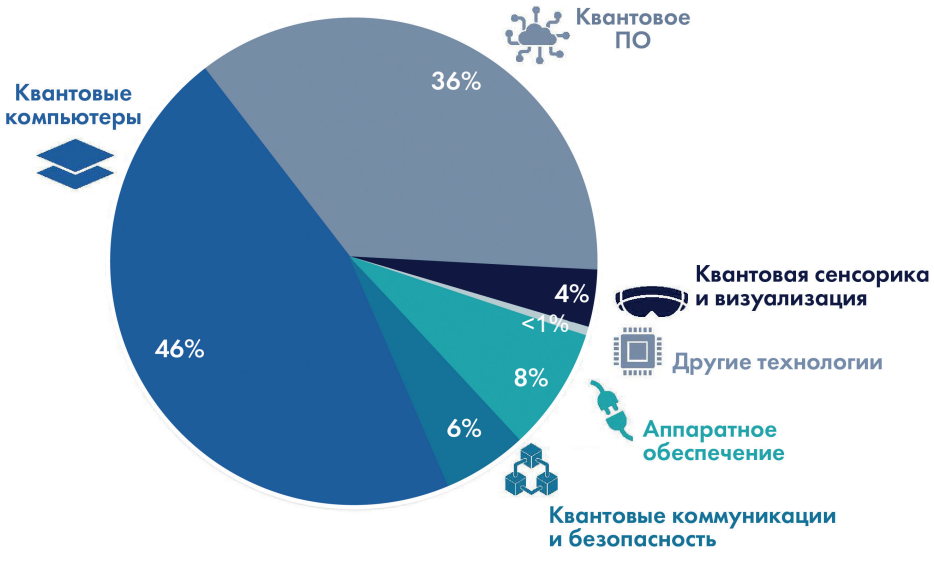


АНАЛИТИКА БОЛЬШИХ ДАННЫХ | РАЗРАБОТКА БОЛЕЕ СОВЕРШЕННЫХ ЛЕКАРСТВ | МАШИННОЕ ОБУЧЕНИЕ | КРИПТОГРАФИЯ

Источник: Pinterest

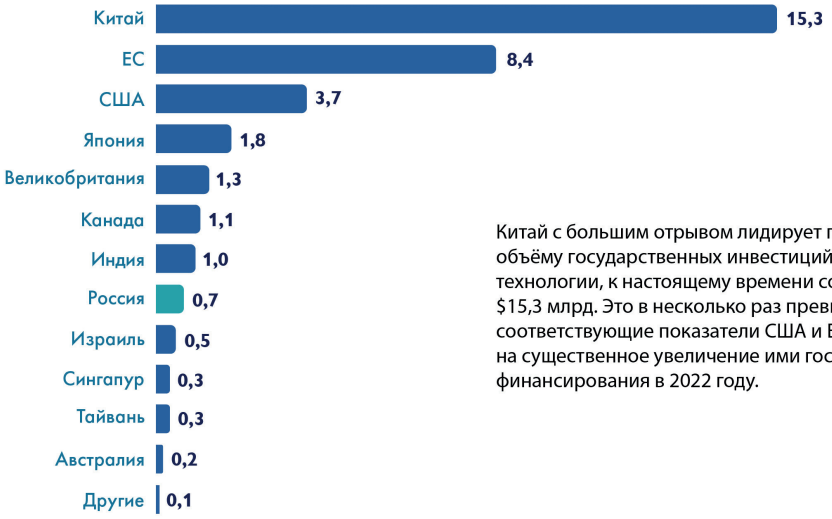
РАСПРЕДЕЛЕНИЕ ЧАСТНЫХ ИНВЕСТИЦИЙ ПО СЕКТОРАМ КВАНТОВЫХ ТЕХНОЛОГИЙ

Частные инвестиции в квантовые технологии в 2022 году суммарно достигли более $2 млрд. При этом наибольший рост наблюдался в сегментах квантовых компьютеров и программного обеспечения для них.



Источник: The Quantum Insider Quantum Technology Investment Update, February 2023 https://thequantuminsider.com

ОБЪЁМ ГОСУДАРСТВЕННОГО ФИНАНСИРОВАНИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ ПО СТРАНАМ*, $ млрд



Китай с большим отрывом лидирует по общему объёму государственных инвестиций в квантовые технологии, к настоящему времени составившему $15,3 млрд. Это в несколько раз превышает соответствующие показатели США и ЕС, несмотря на существенное увеличение ими государственного финансирования в 2022 году.

*С учётом различий инвестиционных периодов в отдельных странах

Источник: McKinsey&Company Quantum Technology Monitor, April 2023, https://www.mckinsey.com

UKRI Science and Technology Facilities Council
Hartree Centre

СУПЕРКОМПЬЮТИНГ	КВАНТОВЫЕ ВЫЧИСЛЕНИЯ
Хорошо развитые архитектура и оборудование	Архитектура в процессе разработки, отраслевых стандартов нет
Требует охлаждения в стандартном диапазоне температур	В некоторых случаях требуется ультраохлаждение
Вычисления в транзисторной (булевой) логике. Единица информации - бит, находящийся в состоянии 0 или 1	Вычисления в квантовой логике. Единица информации - кубит, может принимать состояние 0, 1 или одновременно 0 и 1 (суперпозиция)
Пропорциональное изменение скорости обработки данных	Экспоненциальное изменение скорости обработки данных

Источник: Science and Technology Facilities Council's Hartree Centre
https://blog.hartree.ac.uk

Сети квантового распределения ключей – новый уровень сервисов информационной безопасности национальной сети Интернет

Владимир Елисеев

Аннотация

В статье даются основные понятия технологии квантового распределения ключей (КРК) и необходимые понятия квантовой информатики. Перечисляются основные особенности технологии, отмечаются возможности и ограничения. Кратко приводится история развития технологии и отмечаются её основные вехи. Вводится понятие сети КРК и концепции доверенных промежуточных узлов. Рассматривается вопрос интеграции сетей КРК в инфраструктуру современных телекоммуникационных сетей. Демонстрируется мировой уровень технологических достижений систем КРК и показываются ближайшие перспективы. Исследуются возможности, предоставляемые новой технологией, отмечаются существующие технологические и регуляторные барьеры на пути её широкого внедрения.

Ключевые слова:

квантовое распределение ключей, квантовая информатика, квантовая криптография, квантовые коммуникации

Введение

Квантовое распределение ключей в плане достигнутого практического результата является одной из наиболее успешных технологий второй квантовой революции. Первая квантовая революция, последовавшая за открытиями квантовой механики в начале XX века, характеризуется появлением технологий, основанных на групповых квантовых эффектах. Наиболее яркими представителями групповых квантовых эффектов являются реакции ядерного распада и синтеза, а также полупроводниковая электроника и лазеры. Вторая квантовая революция началась в конце XX века в процессе изучения эффектов, возникающих при взаимодействии отдельных квантовых частиц. Эти эффекты сформировали понимание о квантовой информатике – науке о представлении и преобразовании информации в квантовых системах. Принято говорить о трёх китах второй квантовой революции: квантовых вычислениях, квантовых сенсорах и квантовом распределении ключей. В России эти технологии развиваются в Центре квантовых технологий МГУ [1] и нескольких других специализированных научных центрах.

В перечисленных направлениях развития квантовых технологий производятся преобразования и измерения отдельных квантовых частиц. Далее будем рассматривать квантовое распределение ключей (КРК), по-английски называемое quantum key distribution (QKD).

Квантовое распределение ключей также иногда называют квантовой криптографией, хотя в действительности собственно криптографические преобразования совершаются традиционным способом, без использования квантовых эффектов. Основной задачей, решаемой технологией КРК, является создание общего секретного ключа у двух взаимодействующих сторон, что традиционно называется распределением ключа. Для этого используется передача информации, представленной в форме квантовых состояний. Особенностями квантового представления информации являются неопределённость результата её чтения и разрушение при чтении исходного квантового состояния, несущего информацию.

С точки зрения физики, процесс чтения является измерением величины того или иного свойства физического носителя информации. Например, направление или величина намагниченности измеряется при хранении информации на магнитных лентах или дисках. При передаче электрических сигналов по металлическим проводам измеряется сила тока, а при передаче оптических сигналов измеряется их интенсивность, то есть мощность многофотонных импульсов. Классические сигналы характеризует идентичность принятой, то есть полученной в результате измерения, и переданной информации. При этом мощности сигналов достаточно для того, чтобы их измерения практически не влияли на сам сигнал: его можно многократно измерять по маршруту распространения. Конечно, на результат измерения могут влиять помехи в канале, однако при приемлемом соотношении сигнал/шум с помощью кодов исправления ошибок можно гарантировать безошибочную передачу определённого количества информации в единицу времени.

В противоположность этому, измерение неизвестного квантового состояния хотя и даёт определенный результат, однако этот результат может отличаться от того, что исходно передавалось. В чём причина этой непредсказуемости? Дело в том, что для однозначного измерения квантового состояния обеим сторонам необходимо договориться о способе представления информации – так называемом базисе. Например, при поляризационном кодировании можно договориться, что «0» кодируется горизонтально ориентированной поляризацией, а «1» – вертикально ориентированной. Назовём это крестообразным базисом. Тогда, установив горизонтально ориентированный поляризационный фильтр перед детектором, мы можем быть уверенными, что «0» вызовет срабатывание детектора, а «1» не вызовет. Если же отправитель сформирует квантовое состояние в диагональном поляризационном базисе («0» – поляризация 45 градусов, «1» – поляризация 135 градусов), то принимающая сторона, измеряя вертикально или горизонтально поляризованные фотоны, всё равно будет получать определенный ответ: «0» или «1». Мы знаем со школы, что, измеряя диагонально поляризованный свет через вертикально или горизонтально установленный поляризационный фильтр, мы получим ослабленный в два раза световой поток. На квантовом уровне это будет означать равную вероятность получить «0» или «1» при том, что отправителем был задан бит «0» или «1» в диагональном базисе. Причём не существует способа выяснить, как был поляризован одиночный фотон! К тому же, невозможно сделать копию такого фотона, что является следствием теоремы о запрете клонирования неизвестного квантового состояния.

Квантовый протокол

Оказывается, эти довольно странные особенности передачи информации в квантовом канале можно использовать для распределения секретного ключа. Для этого будем формировать базис случайно, с помощью генераторов случайных чисел (рис. 1). Допустим, «0» у нас будет крестообразным базисом, а «1» – диагональным. Далее будем кодировать в этом базисе случайный информационный бит: «0» или «1». Модулированный таким образом фотон будем передавать через подходящую среду (квантовый канал) на сторону приёмника. Там, применяя аналогичную модуляцию двумя другими случайными битами с выбором базиса и кодированного в нём бита, мы будем регистрировать на детекторе событие попадания фотона. Очевидно, что при совпадении базисов отправителя и получателя, а также информационных битов, событие попадания на детектор будет на 100% вероятным (при отсутствии потерь и помех). При различии информационных битов, но при совпадении базисных битов события попадания не будет. Это могло бы быть интерпретировано как посылка инверсного информационного бита, но фотон может не добраться до детектора просто в силу потерь в среде передачи – идеальных квантовых каналов не существует.

Гораздо более интересным является случай различия базисов отправителя и получателя. В этом случае детектор будет срабатывать или не срабатывать равновероятно, независимо от того, какой был информационный бит отправителя и какой информационный бит ожидал получатель. После детектирования события попадания фотона отправитель и получатель передают друг другу по классическому служебному каналу биты выбранных базисов. В этот момент они узнают, являлось ли срабатывание детектора признаком совпадения обоих случайно выбранных битов или это было случайное равновероятное срабатывание при различных базисах. Если базисы оказались одинаковыми, то информационный бит добавляется к формируемому секретному ключу, в противном случае сеанс передачи фотона считается неудачным, и его результаты не идут в работу. Эта процедура называется просеиванием сырого ключа.

После просеивания полученные случайные последовательности подвергаются сжатию путем применения к ним хеш-функции. Количество бит ключа становится меньше, однако вероятность того, что нарушитель в канале смог угадать квантовое состояние и, таким образом, узнать определенные биты секретного ключа, также становится меньше. Итоговая битовая строка называется общим квантовым ключом. Она совпадает у отправителя и получателя.

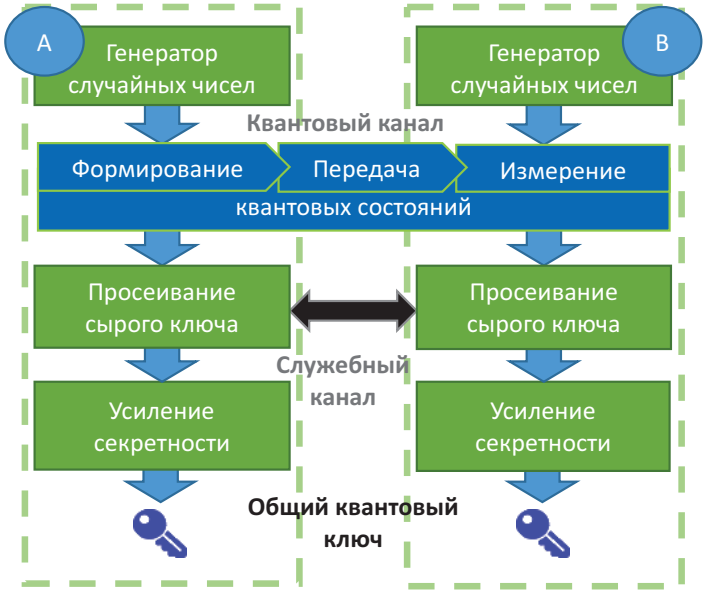


Рис. 1. Обобщённая схема реализации КРК.

Изложенное описание имеет название «квантовый протокол BB84» по имени создателей Чарльза Беннета (Charles Bennett) и Жиля Брассара (Gilles Brassard), опубликовавших его описание в 1984 году [2]. Этот протокол позволяет сформировать секретный ключ двум сторонам, не разглашающим образующие его биты для нарушителя, который может пытаться подслушивать в квантовом и служебном каналах. С тех пор были придуманы и реализованы многочисленные квантовые протоколы. Перечислим свойства, характеризующие все квантовые протоколы без исключения:

- качество (непредсказуемость, независимость) генераторов случайных чисел определяет базовую непредсказуемость квантового ключа;
- в отличие от классических телекоммуникаций квантовая информация не может обрабатываться классическими компьютерами;
- физические свойства переносчиков квантовых состояний и среды передачи ограничивают расстояние между абонентами и скорость формирования битов секретного квантового ключа;

- свойства формирователей и детекторов квантовых состояний ограничивают секретность квантового ключа и скорость его формирования;
- секретность обеспечивается только при условии априорного доверия абонентов (аутентификация служебного канала);
- потери в канале должны интерпретироваться как потенциальное присутствие нарушителя и компенсироваться с помощью усиления секретности;
- секретный ключ распределяется всегда между двумя абонентами (топология «точка-точка», независимо от варианта квантового протокола);
- все фазы формирования секретного ключа должны производиться в доверенной зоне, недоступной злоумышленнику.

Удобной средой для передачи квантовых состояний фотонами на большие расстояния является оптоволокно, используемое для телекоммуникаций. В этом случае типичным расстоянием, на котором работают современные системы КРК, является 100 км (SMF-28, потери 0,2 дБ/км, λ=1550 нм). Существует возможность совмещения КРК с λ=1310 нм и оптоволоконных линий с частотным уплотнением (CDWM, DWDM), что снижает предельное расстояние КРК до 50-60 км. Также возможно передавать квантовые состояния через атмосферу и вакуум [3], однако потенциально меньшие потери компенсируются их нестабильностью (зависимость от погоды и засветок) и геометрическим расхождением пучка света, что ограничивает расстояние между абонентами.

Системы квантового распределения ключей состоят из двух или трёх (MDI-QKD [4], TF-QKD [5]) станций, соединённых квантовым каналом. При этом квантовый ключ распределяется всегда только между двумя станциями абонентов, обладающих классическим аутентифицированным каналом. Квантовые протоколы типа MDI-QKD позволяют промежуточной станции находиться в руках нарушителя, что не влияет на секретность вырабатываемого квантового ключа. В протоколах типа TF-QKD дополнительная станция посередине обеспечивает удвоение расстояния, на котором вырабатываются квантовые ключи. С точки зрения телекоммуникаций подходы MDI-QKD и TF-QKD требуют установки средней станции в разрыв оптоволокна.

Система КРК для защиты информации

К настоящему времени системы КРК прошли длинный путь развития, за время которого увеличилась надёжность, дальность и производительность выработки квантовых ключей. Однако самым главным достижением последнего десятилетия стало практическое использование систем КРК для распределения секретных ключей, используемых в системах криптографической защиты информации (СКЗИ). Это стало возможным благодаря исследованию уязвимостей ранних систем КРК и реализации необходимых мер защиты в современных системах. В частности, в России не только разработаны требования к квантово-криптографическим системам выработки и распределения ключей (ККС ВРК) и методики проверки их соответствия, но также созданы системы КРК, уже прошедшие сертификацию [6] у национального регулятора – ФСБ России.

Классическая система КРК топологии «точка-точка» обеспечивает распределение симметричных ключей шифрования для защиты сетевого трафика (рис. 2). Такая система может использоваться для защиты канала передачи данных между основным и резервным ЦОД.

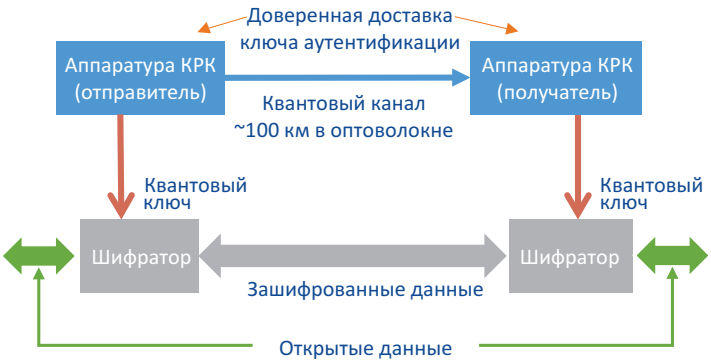


Рис. 2. Защита сетевого трафика в топологии «точка-точка» с помощью КРК.

С точки зрения специалистов по информационной безопасности КРК обеспечивает:

- новый и необычный для информационных технологий способ распределения симметричных ключей;
- защиту от внутреннего нарушителя (минимизация влияния человека на процедуру создания и распределения криптографического ключа);
- защиту от чтения вперёд/назад при раскрытии текущего ключа нарушителем;
- снижение влияния утечки по побочным каналам;
- решение проблемы контроля нагрузки на ключ.

Новая технология предлагает реализацию концепции распределённого ключевого центра, при которой отпадает необходимость в доверенных курьерах, перевозящих криптографические ключи.

Кажущиеся критическими ограничения в расстоянии и топологии КРК могут быть сняты путём построения больших географически распределённых сетей КРК с доверенными промежуточными узлами (trusted nodes). Рассмотрим особенности этого подхода ниже.

Сети КРК с доверенными промежуточными узлами

Предположим, нам необходимо снабдить ключами шифраторы, находящиеся на расстоянии, превышающем возможности КРК. В этом случае мы можем разместить один или несколько доверенных промежуточных узлов между оконечными узлами, к которым подключены шифраторы (рис. 3). Промежуточные узлы должны содержать в себе пару устройств – отправителя квантовых состояний одного сопряженного сегмента КРК и получателя квантовых состояний другого сопряжённого сегмента КРК. Оба эти устройства должны быть соединены классическим каналом, недоступным для нарушителя, поэтому такую конструкцию назовём доверенным промежуточным узлом (ДПУ).

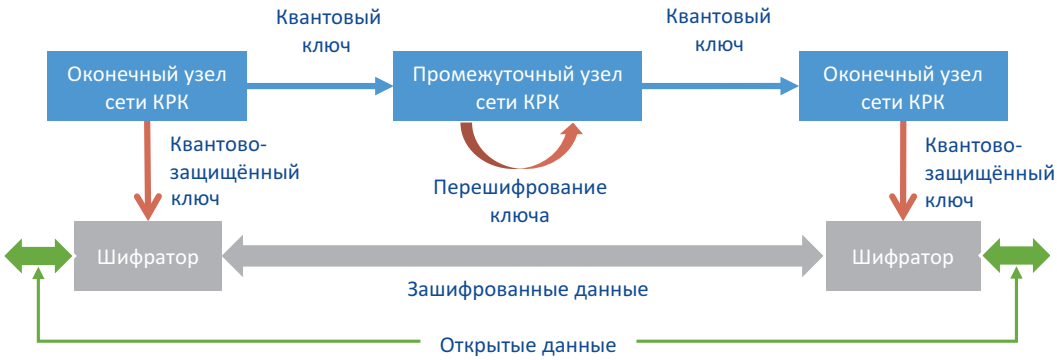


Рис. 3. Перешифрование ключа в магистральной сети КРК с ДПУ.

Для снабжения шифраторов секретными ключами на одном из оконечных узлов достаточно создать секретный ключ и передать его под защитой квантового ключа на соседний узел сети КРК по классическому каналу. Там получатель квантового состояния сможет этот ключ расшифровать, поскольку у них с отправителем общий квантовый ключ, а потом зашифровать его внутри ДПУ на квантовом ключе сопряжённого сегмента, передав далее по сети КРК. В итоге исходный секретный ключ под защитой квантовых ключей сети КРК будет доставлен до целевого оконечного узла сети, откуда его можно загрузить в шифратор. Ключ, который передаётся по сети КРК, назовём квантово-защищенным ключом (КЗК). Он не является квантовым по своему происхождению, но его секретность обеспечивается квантовыми ключами сети. Топология связи узлов в сети КРК с ДПУ может быть сколь угодно сложной: содержать кольцевые маршруты и элементы топологии «звезда». Для реализации сложных маршрутов ДПУ должны содержать в себе либо несколько модулей отправителей и получателей квантовых состояний, либо иметь в своём составе оптический коммутатор, позволяющий в режиме разделения времени вырабатывать квантовые ключи с несколькими сопряжёнными узлами сети КРК. Например, в системах КРК производства компании ID Quantique [7] используется первый подход, а в системах КРК компании «ИнфоТеКС» [8] – второй.

Современные телекоммуникационные сети основаны на широком использовании оптоволокна и вспомогательной аппаратуры, располагающейся в узлах связи и обеспечивающей подключение пользовательских устройств приёма/передачи данных, а также усиление оптического сигнала в случае его передачи на большие расстояния. Расстояние, на котором располагаются друг от друга узлы связи, редко превышает 100 км. Таким образом, структурно оптоволоконные сети хорошо подходят для развёртывания на их основе сетей КРК с ДПУ. При построении сети КРК нельзя забывать о том, что квантовые состояния невозможно «усилить», поэтому для волокон, используемых для КРК, нельзя применять волоконные и оптоэлектронные усилители сигналов, а также медиаконверторы.

Полезной особенностью ДПУ является возможность сопряжения сегментов с различными квантовыми протоколами и даже физической средой реализации квантового канала. В частности, ДПУ обеспечивают бесшовную интеграцию оптоволоконных и космических каналов КРК. Однако необходимо учитывать, что ДПУ не могут быть размещены на территории, не контролируемой владельцем сети КРК. По этой причине создание сетей КРК на основе ДПУ, расположенных в разных странах, представляет собой сомнительную с точки зрения целесообразности задачу.

Сети КРК — мировой опыт создания и применения

Лидером по масштабному применению сетей КРК является Китай. В нем более 10 лет реализуется проект построения национальной сети КРК [9]. В 2022 году сеть КРК имела протяжённость более 10 000 км и связывала сотни узлов, а также включала в себя два спутника, обеспечивающих КРК для удалённых регионов страны (рис. 4).

Рис. 4. Национальная сеть КРК Китая на 2022 год [9].

Основным практическим применением китайской сети КРК является защита коммуникаций отделений государственного банка Китая. Этим обусловлено размещение крупных ДПУ сети КРК в отделениях госбанка. Отмечаются следующие преимущества КРК:

- улучшение безопасности за счёт частой смены секретных ключей шифрования;

- снижение стоимости эксплуатации разнообразных систем банка различных производителей, использующих криптографию, без снижения уровня безопасности;
- создание случайных чисел для различных применений (ПИН-коды, одноразовые коды подтверждения, пароли и пр.) с помощью квантовых генераторов.

Кроме банковских учреждений сервисы на основе сети КРК развивают и телекоммуникационные компании. Они обеспечивают для конечных пользователей загрузку КЗК в мобильные устройства, что позволяет шифровать пользовательские данные в разных сессиях разными одноразовыми ключами.

В Южной Корее в 2022 году был реализован проект построения сети КРК для защиты данных, передаваемых между 48 государственными учреждениями [10]. Сеть была построена на инфраструктуре SK Telecom с использованием систем КРК производства ID Quantique.

В России развитие отрасли квантовых коммуникаций поручено ОАО «РЖД». Корпорация уже несколько лет финансирует широкий спектр работ по исследованиям и стандартизации в области КРК, а также строит квантовую сеть на основе систем КРК нескольких отечественных производителей. Важной движущей силой развития технологий КРК в России стали университеты. Необходимо отметить большой вклад в исследования КРК и развитие технологий МГУ имени М.В. Ломоносова, ИТМО, МФТИ, МИСИС, МТУСИ, ТУСУР, ВШЭ, ЮФУ и некоторых других вузов. В частности, в МГУ с конца 2021 года функционирует Университетская квантовая сеть [12], в Томске планируется связать все университеты города на основе сети КРК ТУСУР [13], а также есть проект создания аналогичной межуниверситетской сети в Москве с перспективой подключения к магистральной сети КРК РЖД.

В то же время вызывает удивление тот факт, что российские телекоммуникационные компании достаточно поверхностно вовлечены в работы по исследованию прикладных применений и внедрению технологии КРК. Банковская система России также достаточно инертна – кроме отдельных пилотных испытаний несколько лет назад, никаких признаков внедрения систем КРК пока не заметно. Это контрастирует с китайским опытом практических применений.

Проблематика широкого применения КРК

Достаточно актуальным вопросом, стоящим перед сообществом разработчиков и пользователей систем защиты информации, является определение сфер приоритетного применения технологии КРК. Можно выделить следующие направления внедрения КРК, которые можно было бы развивать как грамотным распределением ресурсов, так и правильной регуляторной приоритезацией:

- университеты и академические институты:
  - кадры для освоения новой сквозной технологии;
  - задел для развития квантовых сетей связи квантовых компьютеров;
- государственные информационные системы:
  - высший уровень защиты от внутреннего нарушителя и глобальных угроз;
  - инвестиции в развитие новой сквозной технологии;
  - поддержание лидерства в сфере оказания электронных госуслуг;
- критическая информационная инфраструктура (банки, телеком и крупнейшие провайдеры коммерческих электронных услуг):
  - снижение риска утечки персональных данных;
  - распределённые и отказоустойчивые криптоанклавы.

Уникальные свойства КРК в значительной степени снижают риски ИБ в защищаемых информационных системах, поэтому логично, чтобы пользователи систем КРК имели послабления при эксплуатации по сравнению с применением традиционных систем распределения ключей в СКЗИ. Некоторые государственные информационные системы, связанные с обработкой персональных данных граждан, должны быть снабжены защитой на основе КРК безусловно!

Можно выделить также некоторые технологические барьеры, не столь критичные в настоящий момент, но которые должны быть преодолены в ближайшем будущем:

- совместная работа сегментов сети КРК различных производителей;
- подключение городских, корпоративных и университетских сетей КРК к магистральной сети;
- объединение сетей КРК различной принадлежности (межсетевая передача КЗК);
- реализация КРК на космический спутник для охвата сервисом доступа к квантовым ключам удалённых регионов страны и зарубежных территорий;
- снижение стоимости владения инфраструктурой сетей КРК (адаптация к DWDM);
- снижение стоимости подключения к сети КРК (удешевление себестоимости систем КРК и увеличение их производительности);
- развитие отечественных технологий для оптоэлектронной компонентной базы систем КРК.

Более подробно вопросы, связанные с технологическими и регуляторными барьерами, а также устройство систем КРК и типовые сценарии их внедрения описаны в [14]. Новости по теме квантовых технологий, связанных с решением задач информационной безопасности, представлены на сайте [15].

Заключение

В настоящее время технология квантового распределения ключей достигла высокого уровня развития и полностью готова к применению на практике. Примеры Китая и Южной Кореи демонстрируют наиболее перспективные сферы применения КРК. Технологический уровень систем КРК в России лишь ненамного отстаёт от ведущих стран мира. Необходимо использовать накопленный научный и технологический потенциал КРК для реализации новых сервисов безопасности и снижения рисков в традиционных сферах применениях СКЗИ при шифровании больших потоков данных.

Список литературы:

[1] Центр квантовых технологий МГУ имени М.В. Ломоносова [Электронный ресурс] URL: https://quantum.msu.ru/ru (дата обращения: 06.03.2006)

[2] Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of International Conference on Computers, Systems & Signal Processing, Dec. 9-12, 1984, Bangalore, India. — IEEE, 1984. — P. 175

[3] Cheng-Zhi Peng, Yang Li et. Al. Space-ground QKD network based on a compact payload and circular orbit // Optica, 2022. Vol.9, No.8

[4] Hoi-Kwong Lo, Marcos Curty, Bing Qi. Measurement-Device-Independent Quantum Key Distribution // Physical Review Letters. — 2012-03-30. — Vol. 108, iss. 13. — P. 130503

[5] Lucamarini, M., Yuan, Z.L., Dynes, J.F. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters // Nature 557, 2018, P. 400–403

[6] Получены сертификаты ФСБ России для ViPNet QTS Lite [Электронный ресурс] // CNEWS, 29.06.2023. URL: https://safe.cnews.ru/news/line/2023-06-29_polucheny_sertifikaty_fsb (дата обращения: 06.03.2006)

[7] ID Quantique [Электронный ресурс] URL: https://www.idquantique.com (дата обращения: 06.03.2006)

[8] Квантовые криптографические системы [Электронный ресурс] // Официальный сайт компании «ИнфоТеКС». URL: https://infotecs.ru/products/filter/products_line-is-9/apply (дата обращения: 06.03.2006

[9] Wei Qi. A Brief Introduction to the Latest Progress of China's QKD Industry [Электронный ресурс] // ETSI/IQC Quantum Safe Cryptography Event, 14.02.2023. URL: https://docbox.etsi.org/workshop/2023/02_quantumsafecryptography/technicaltrack/worldtour/casquantumnetwork_qi.pdf (дата обращения: 06.03.2006)

[10] South Korea relies on ID Quantique for data security [Электронный ресурс] // The Swiss start-up news channel, 15.08.2022. URL: https://www.startupticker.ch/en/news/south-korea-relies-on-iq-quantique-for-data-security (дата обращения: 06.03.2006)

[11] Дорожная карта развития квантовых коммуникаций [Электронный ресурс] // Официальный сайт ОАО «РЖД». URL: https://company.rzd.ru/ru/9349/page/105554?id=2694#6769 (дата обращения: 06.03.2006)

[12] В МГУ заработала университетская квантовая сеть [Электронный ресурс] // ТАСС Наука. 16.12.2021. https://nauka.tass.ru/nauka/13219303 (дата обращения: 06.03.2006)

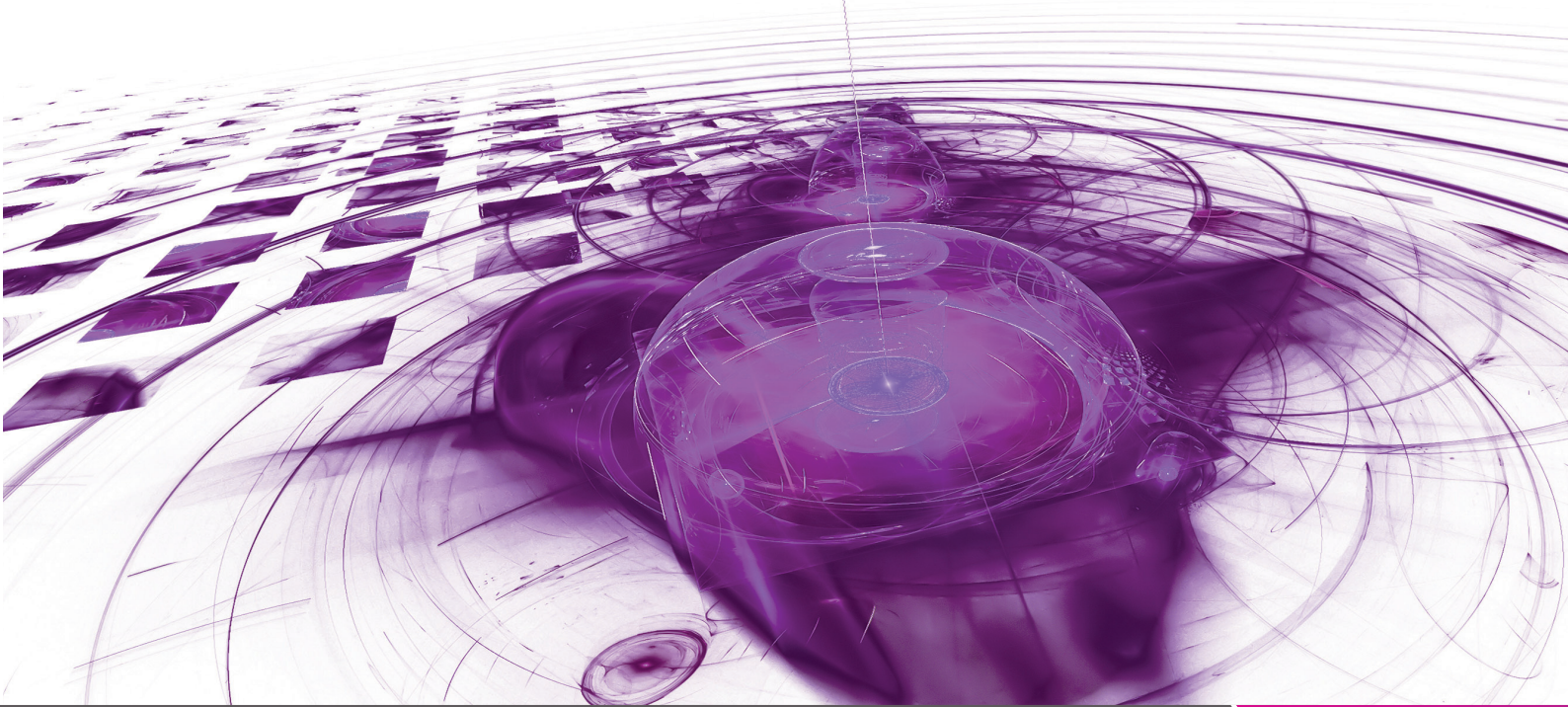
[13] ТУСУР планирует создать квантовую сеть для вузов Большого университета [Электронный ресурс] // РИА Томск 15.02.2024. URL: https://www.riatomsk.ru/article/20240215/69707 (дата обращения: 06.03.2006)

[14] Андрущенко А. С., Борисова А. В. и др. (под редакцией Втюриной А. Г., Елисеева В. Л.) Прикладные квантовые технологии для защиты информации – Москва: Медиа Группа «Авангард», 2023 – 144 стр.

[15] Квантовые технологии информационной безопасности [Электронный ресурс] URL: https://quantum-crypto.ru (дата обращения: 06.03.2006).

Об авторе

Елисеев Владимир Леонидович, компания «ИнфоТеКС», руководитель центра научных исследований и перспективных разработок, к.т.н.; Scopus Author ID: 57126912500; ResearcherID: N-5498-2014; ORCID: 0000-0002-9341-7475; SPIN-код: 9295-7442



На пути к квантовому Интернету

Владимир Егоров

Аннотация:

Коммуникационные технологии первыми из «квантовой триады» (в которую входят также вычисления и сенсоры) подходят к черте промышленного внедрения: запускаются первые магистральные квантовые сети. Следующим шагом для индустрии станет создание квантового Интернета, который объединит как абонентов-людей, так и объекты Интернета вещей. Но для этого придётся сначала решить технологическую задачу миниатюризации систем квантовой коммуникации.

Ключевые слова:

квантовый Интернет, квантовые коммуникации, квантовая рассылка ключей, фотонные интегральные схемы, Интернет вещей

Технологии квантовых коммуникаций прочно входят в нашу жизнь. Ещё пятнадцать лет назад это направление было в нашей стране экзотическим, про него знала лишь горстка специалистов в нескольких научных центрах. Сегодня в России они входят в число приоритетных «сквозных» технологий [1], которые определят научное будущее страны.

Квантовая сеть — технологическая система, включающая технические средства (расположенные в её узлах) и линии связи (квантовые и «классические» каналы), предназначенные для передачи квантовой информации. Квантовые сети могут реализовывать одну из двух функций: передача информации (например, с применением квантовой телепортации или сверхплотного кодирования) и защиты информации (с помощью протоколов квантового распределения ключей или квантовой подписи). Сети передачи квантовой информации представляют интерес в первую очередь для обмена данными по волоконно-оптическим каналам между квантовыми компьютерами. Таким образом, в будущем из них удастся составить кластеры, которые позволят добиться повышения совокупной производительности и обеспечить географически распределенную обработку информации.

Наиболее развитой субтехнологией является квантовое распределение ключей (КРК). Её суть состоит в генерации и рассылке между парой абонентов симметричных секретных ключей, используемых для шифрования, с помощью одиночных фотонов — квантов света — по оптическому волокну или атмосферному каналу. Квантовые свойства фотонов (невозможность их разделить, клонировать или повторно измерить) гарантируют такому каналу защиту от подслушивания; легитимные пользователи обнаруживают вмешательство в него по росту уровня ошибок при передаче сообщений. Отечественные коммерческие компании, такие как ООО «СМАРТС-Кванттелеком», уже предлагают первые рыночные продукты в области КРК. ОАО «Российские железные дороги», являющееся оператором «дорожной карты» по развитию квантовых коммуникаций [2], создаёт основанные на этих решениях магистральные сети КРК, соединившие Санкт-Петербург, Москву и Нижний Новгород. В 2024 году планирует продлить их на юг до Сочи через Ростов-на-Дону и на восток до Екатеринбурга через Казань [3].

Развитие технологии КРК в России в целом лежит в рамках мировых тенденций: в Европе, Китае, США и ряде других стран первым шагом тоже было строительство квантовых магистралей. Однако можно сказать, что в последнее время вектор научного развития в области сместился на пользовательские устройства и приложения. У этого есть две причины. С одной стороны, технологически магистральные системы КРК достигли своеобразного «насыщения». Поскольку в квантовых сетях нельзя использовать привычные для телекоммуникаций усилители, скорость квантовой рассылки ключей экспоненциально падает с расстоянием. И хотя в лабораторных условиях удалось передать квантовые ключи по оптическому волокну на расстояния более 1000 км [4], в реальных сетях достаточные для практических приложений параметры передачи обеспечиваются лишь на пролётах протяжённостью от 50 до 150 км. С другой стороны, из этого следует, что дальнейшая эволюция технологии КРК (в том числе снижение стоимости изделий, остающейся одним из тормозящих отрасль факторов) будет обеспечиваться за счёт масштабирования: подключения всё большего числа как можно более разнообразных абонентов.

Как построить квантовый Интернет?

Сегодня готовые к промышленной эксплуатации и проходящие сертификацию магистральные системы КРК предназначены для монтажа в серверные стойки и имеют соответствующие габариты, сравнимые с размерами магистральных шифраторов. Для того, чтобы сделать технологию КРК по-настоящему массовой, потребуется провести миниатюризацию, разработать решения для размещения на рабочих столах абонентов, на подвижных платформах (в том числе беспилотных транспортных средствах), а в долгосрочной перспективе понадобятся решения для БПЛА и даже для устройств, носимых человеком (на отдельном носителе или интегрированные, например, в смартфон). Выполнение этих задач ознаменует переход к квантовому Интернету.

Кстати, этот термин недавно стал в России официальным. В конце 2023 года Росстандартом были утверждены первые четыре предварительных национальных стандарта в области квантовых коммуникаций, включая «Квантовые коммуникации. Термины и определения» и «Квантовый Интернет. Термины и определения». Согласно им:

> «квантовый Интернет — глобальная информационная квантовая сеть, в узлах которой формируется, обрабатывается и хранится квантовая информация, и узлы которой соединены квантовыми каналами» [5];
>
> «квантовый Интернет вещей — Интернет вещей с использованием квантовых технологий» [6].

Как мы видим, это разные термины, но коммуникации играют в обоих случаях ведущую роль, связывая все элементы сети.

Квантовый Интернет в перспективе рассматривается как глобальная сеть, объединяющая распределённые квантовые вычислители, сенсоры и обеспечивающая защищённую связь между абонентами с помощью КРК. На сегодняшний день его технический облик до конца не сформировался, поэтому мы рассмотрим сценарии применения квантовых коммуникаций в более узком контексте: для приложений Интернета вещей на примере КРК как самой развитой субтехнологии. В этом случае цель будет состоять в том, чтобы обеспечить защиту каналов связи между абонентами (например, каналов управления беспилотными объектами) с помощью симметричных ключей шифрования, сгенерированных и распределённых квантовыми методами. Для этого на каждом узле потребуется разместить модули системы КРК и обеспечить их связь по квантовому каналу. Учитывая, что многие узлы квантового Интернета вещей будут мобильными объектами, этот канал должен быть не оптоволоконным, а воздушным (или гибридным).

Следует отметить, что поскольку миниатюризация КРК для размещения на подвижных объектах (особенно летающих) является непростой задачей, можно рассмотреть промежуточную ступень эволюции квантового Интернета вещей, основанную на применении квантово-защищённых ключей — секретных ключей, защита которых при передаче или хранении осуществляется с использованием квантового ключа (ключей) [5].

В этом сценарии квантовые ключи, непосредственно генерируемые системами КРК, формируются только между связанными квантовыми каналами стационарными узлами сети. После этого полученные ключи помещаются в защищённые криптоконтейнеры (формируемые также с помощью «сервисных» квантовых ключей) и передаются абонентам по обычным каналам связи. В этом случае квантовая защита при распределении ключей не достигается, но остаются другие преимущества, такие как автоматизация генерации и доставки ключей, более частое их обновление и высокое качество (в случае применения в КРК квантовых генераторов истинно случайных чисел). Более подробно данный сценарий рассматривается в [7] и [8].

Несколько перспективных сценариев представлено на рисунке 1.

Вариант 1: мобильный узел производит со стационарной рабочей станцией обмен квантовыми ключами, которые затем используются для защищённого обмена данными между ними. В качестве примера можно рассмотреть носимую человеком «Систему КРК в кармане» и квантово-защищённый банкомат. Другим примером служит эксперимент, который проводился в 2017 году в Канаде: в нём учёные осуществили сеанс КРК между летящим самолётом и наземной станцией [9].

Вариант 2: подвижная рабочая станция обменивается квантовыми ключами с несколькими летающими мобильными узлами. Аналогично варианту 1, ключи используются для защищённого обмена данными с квазистационарной (передвижной, но находящейся в состоянии остановки) рабочей станцией. Пример: беспилотный грузовик выступает в качестве передвижного центра управления роем летающих дронов, осуществляющих аэроразведку. Дроны периодически возвращаются к грузовику для подзарядки и обновления ключей. Научные группы в Китае и США уже продемонстрировали первые эксперименты с обменом квантовыми ключами между летающим дроном и станцией оператора на расстояния до 200 метров [10].

Вариант 3: летающий мобильный узел обменивается квантовыми ключами с несколькими квазистационарными узлами, доставляя на них квантовый мастер-ключ, общий для всей сети. После этого все узлы обмениваются между собой данными, зашифрованными с помощью мастер-ключа. Таким образом, дрон используется как доверенный узел связи при

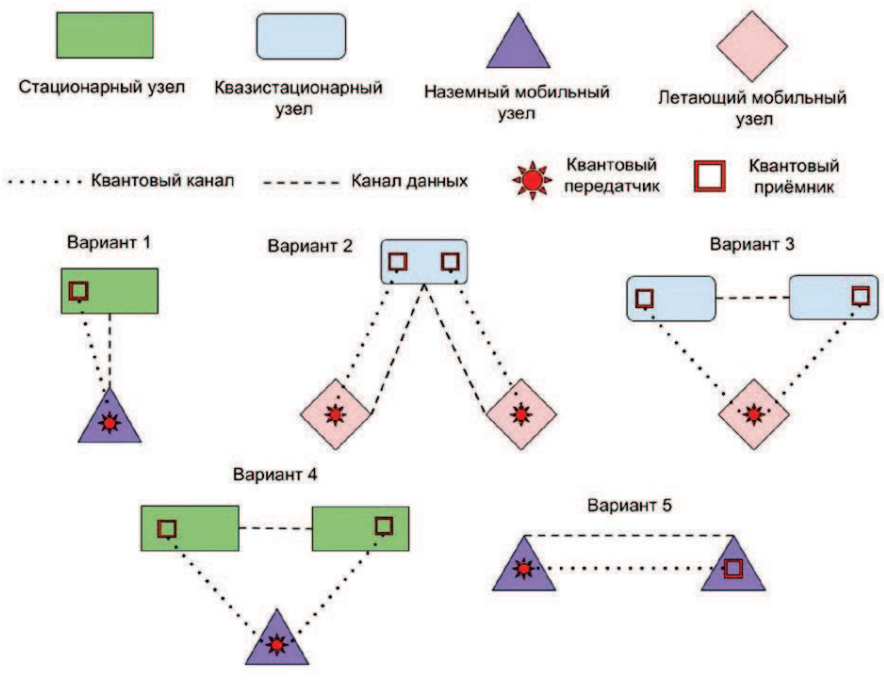


Рис. 1. Варианты построения сети квантового Интернета вещей с КРК.

обмене квантовыми ключами между несколькими подвижными станциями. Пример: дрон подлетает к беспилотному грузовику, обменивается с ним квантовым ключом K1, затем перемещается ко второму беспилотному грузовику и обменивается с ним квантовым ключом K2. Зашифровав хранящийся в памяти дрона ключ K1 с помощью сессионного ключа K2, дрон передаёт его грузовику. В результате оба грузовика смогут организовать защищённый обмен данными с применением K1, как если бы они были соединены квантовым каналом.

Вариант 4: аналогично варианту 3, но с использованием стационарных узлов. Пример: беспилотный грузовик обменивается данными с элементами умной дороги, объединенными в сеть. Квантовые ключи могут применяться для защиты канала управления и при поддержании сеанса видеосвязи с установленных на грузовик камер [11]. Другим примером может служить обмен квантовыми ключами и зашифрованной ими информацией с помощью спутника. Такая возможность была продемонстрирована Китаем: первый в мире спутник квантовой связи «Мо-Цзы» (Micius) соединил обсерватории в Вене и Пекине [12].

Вариант 5: подвижные абоненты по цепочке обмениваются квантовыми ключами и, затем, данными. Пример: обмен данными между беспилотными автопоездами, следующими колонной друг за другом.

Все вышеперечисленные примеры объединяет то, что для их реализации требуется единый набор технологий: телескопические системы для передачи квантовых сигналов по воздуху, новые архитектуры безопасности сетей Интернета вещей на основе симметричных ключей (сейчас в IoT применяются асимметричные схемы) и главное — миниатюризация систем КРК, особенно для размещения на летающих объектах.

Долгая дорога к миниатюризации

Из вышеизложенного может показаться, что квантовые технологии пока бесконечно далеки от конечных пользователей, однако это иллюзия. К примеру, смартфон Galaxy A Quantum, выпущенный компанией Samsung в 2020 году [13], имеет в составе квантовый генератор случайных чисел от швейцарской компании ID Quantique. Он предназначен для повышения защищённости устройства за счёт генерации сложных паролей.

Хотя системы КРК реализовать в столь малом объёме гораздо сложнее, чем генераторы случайных чисел, за счёт большего числа различных компонентов в их составе, в мире существуют перспективные подходы к их миниатюризации, основанные на применении фотонных интегральных схем (ФИС).

ФИС подобны электронным микросхемам, но предназначены для управления не электричеством, а оптическим излучением (в том числе одиночными фотонами, применяемыми в системах КРК). Следует отметить, что приложения ФИС выходят далеко за рамки квантовых технологий — они представляют большой интерес, к примеру, для высокоскоростных оптических трансиверов.

Подобно тому как электроника в XX веке прошла путь от ламп к транзисторам и затем микросхемам, системы КРК перешли от схем на объёмной оптике к волоконной (кроме космических систем) и сегодня начинают переходить к интегральному исполнению. Тем более, что преимущества ФИС не ограничиваются лишь снижением размеров.

Во-первых, переход на ФИС существенно повысит стабильность функционирования систем КРК. Квантовые устройства всегда демонстрируют очень высокую чувствительность к внешним условиям (изменение температуры или механические напряжения), которая резко ухудшает их характеристики. Реализация на ФИС позволит создавать системы КРК на основе компактных твердотельных элементов, существенно снизив влияние вибраций и температуры на их параметры.

Во-вторых, ФИС прекрасно подходят для массового производства. В будущем окажется возможным буквально «печатать» на литографах оптические схемы систем КРК целыми партиями вместо производства отдельных компонентов с их последующей механической сборкой, что позволит радикально снизить себестоимость.

Реализация систем КРК на ФИС стоит на «трёх китах»: оптические материалы, компоненты (волноводы, источники, приёмники, устройства управления излучением) и схемы протоколов КРК. В данном материале мы сконцентрируемся на первом аспекте.

Основные оптические материалы для реализации ФИС [14], применимых в технологии КРК, приведены в таблице. К ним относятся: кремнезём (диоксид кремния, лат. silica), кремний на изоляторе (SOI), нитрид кремния (Si_3N_4), ниобат лития ($LiNbO_3$), арсенид галлия (GaAs), фосфид индия (InP) и оксинитрид кремния (SiO_xN_y).

По таблице можно сделать вывод об отсутствии универсального решения, которое позволило бы реализовать все оптические компоненты систем КРК на единой платформе.

	SiO2 волноводы	SOI (Si на изоляторе)	Si3N4	LiNbO3 на изоляторе	GaAs	InP	SiOxNy
Контраст n	Низкий	Высокий	Средний	Средний	Низкий	Низкий	Низкий
Потери	Очень низкие	Средние, сильное двухфотонное поглощение	Низкие, слабое двухфотонное поглощение	Средние	Средние	Средние	Низкие, слабое двухфотонное поглощение
Нелинейность	Слабая X3	Сильная X3	Сильная X3	Сильная X2	Сильная X2	Сильная X2	Средняя X3
Реализация лазера	Нет	Нет	Нет	Нет	Да	Да	Нет
Реализация модулятора	Медленный	Быстрый	Медленный	Быстрый	Быстрый	Быстрый	Медленный
Реализация детектора	Нет	Да (Ge)	Нет	Нет	Да	Да	Нет
Ввод в волокно	Хороший	Плохой	Средний	Средний	Плохой	Плохой	Средний
CMOS-совместимость	Нет	Отличная	Хорошая	Нет	Нет	Нет	Хорошая

К примеру, SOI характеризуется сильным контрастом показателя преломления (волновода относительно подложки или оболочки), что позволит достичь минимальных размеров волноводов, сильную нелинейность для генерации неклассических состояний света и совместимость с CMOS-процессом (англ., «комплементарная структура металл — оксид — полупроводник»), широко применяемым в полупроводниковой промышленности для создания интегральных микросхем.

Существуют работы, в которых продемонстрирована реализация на платформе SOI лавинных фотодетекторов телекоммуникационного диапазона на основе германия. К сожалению, SOI не обладает возможностью реализовать лазер, а потому размещение на нём источников одиночных фотонов представляет трудность.

Полупроводники группы III–V (GaAs, InP), позволяющие реализовывать источники и быстрые модуляторы излучения на ФИС, демонстрируют низкий контраст показателя преломления, дороже в производстве и имеют более высокие оптические потери, что особенно важно для приёмных модулей систем КРК (поскольку по ним распространяется однофотонный сигнал, несущий информацию, в то время как в модуле отправителя среднее число фотонов, прямым образом влияющее на защищённость системы, отсчитывается от выхода из устройства).

На платформе Si_3N_4 возможно реализовать только низкочастотную модуляцию параметров оптического излучения, в то время как современные системы КРК работают на частотах кодирования сигналов (смены фазы, поляризации или других параметров) от 100 МГц до нескольких ГГц.

В связи с этим большинство решений сегодня следует гибридной парадигме, когда модули систем КРК строятся не на одной платформе, а на нескольких ФИС из разных материалов, которые затем стыкуются друг с другом. Примером может служить созданный в 2023 году в Великобритании макет системы КРК [15], применяющий чипы на InP для реализации источников излучения и модуляторов, а Si_3N_4 — интерферометра на основе волноводных компонентов. Чипы совмещались методом краевого соединения (edge coupling). В эксперименте использовались внешние детекторы одиночных фотонов, подключаемые по оптическому волокну. По оценкам авторов, данная система позволит распределять секретные ключи по волоконным каналам с потерями до 40 дБ (порядка 200 км).

К сожалению, при реализации гибридного подхода возникает проблема различий в условиях эксплуатации разных компонентов системы. К примеру, однофотонные источники излучения на основе квантовых точек и наиболее чувствительные детекторы одиночных фотонов обычно работают при криогенных температурах. В то же время, фазовые модуляторы, основанные на термооптическом или электрооптическом эффектах, предназначены для комнатной температуры и не могут работать в таких экстремальных условиях.

Гонка за миниатюризацию, а значит и за пользовательский рынок КРК, в мире пока только набирает обороты. С точки зрения архитектуры систем он включает поиск «идеальной» гибридной платформы и технологий производства, выбор компонентов, работающих при единых внешних условиях. В технологическом аспекте требуется либо обеспечить высокоточное воспроизведение характеристик ФИС при серийной фабрикации (с нанометровой точностью), либо разработать чипы с подстраиваемыми параметрами. Остаются не до конца решёнными вопросы отведения тепла и подвода управляющих оптикой электрических контактов. Потребуется также создание специализированных САПР. В современных условиях Россия берёт курс на технологический суверенитет. Квантовые технологии и фотонные интегральные схемы наверняка станут одними из элементов его фундамента.

Список литературы:

[1] Постановление правительства РФ от 2 июля 2020 г. N 974

[2] «Дорожная карта» развития высокотехнологичного направления «Квантовые коммуникации» на период до 2030 года, утверждённая президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (пункт 2 раздела IV протокола от 27 августа 2020 года № 17, пункт 1 раздела I протокола от 28 января 2022 года № 2, пункт 1 раздела IV протокола от 9 ноября 2022 года № 48)

[3] https://company.rzd.ru/ru/9401/page/78314?id=211688

[4] https://arxiv.org/abs/2303.15795

[5] ПНСТ 830-2023 Квантовые коммуникации. Термины и определения

[6] ПНСТ 832-2023 Квантовый Интернет вещей. Термины и определения

[7] ПНСТ 829-2023 Квантовые коммуникации. Общие положения

[8] ПНСТ 906-2023 Квантовый Интернет вещей. Типовой программно-аппаратный комплекс, реализующий функции системы квантового распределения ключей. Архитектура

[9] Pugh C. J. et al. Airborne demonstration of a quantum key distribution receiver payload. Quantum Science and Technology – 2017, V.2., №2

[10] https://arxiv.org/abs/2302.14012

[11] https://www.mdpi.com/2624-8921/5/4/86

[12] https://www.iqoqi-vienna.at/research/zeilinger-group/satellite-based-quantum-communication

[13] https://www.ixbt.com/news/2020/05/14/samsung-galaxy-a-quantum.html

[14] https://www.nature.com/articles/s41377-023-01173-8

[15] https://arxiv.org/abs/2308.02238

Об авторе:

Егоров Владимир Ильич, кандидат физико-математических наук,
AuthorID: 636560, SPIN-код: 8345-1128
Заместитель директора, Национальный центр квантового Интернета, ИТМО. Начальник отдела научных исследований,
ООО «СМАРТС-Квантителеком» Россия, г. Санкт-Петербург

Квантовые коммуникации — сети квантового распределения ключей или новый Интернет?

Алексей Сантьев

Аннотация:

Широкое развитие в Российской Федерации и в мире получили технологии квантовых коммуникаций. Наиболее готовым для применения в реальной инфраструктуре является технология квантовых коммуникаций. Однако в области квантовых коммуникаций помимо прикладного направления, связанного с развитием сетей квантового распределения ключей, также можно выделить исследовательское направление, связанное с разработкой концепции глобального квантового Интернета. В статье рассматриваются вопросы развития обоих технологических направлений квантовых коммуникаций и оцениваются перспективы дальнейшего развития данной отрасли.

Ключевые слова:

квантовые коммуникации, квантовое распределение ключей, квантовый Интернет, квантовая сеть, квантовый компьютер

В последние годы в Российской Федерации и во всем мире уделяется большое внимание развитию квантовых технологий [1]. Первые большие национальные программы по развитию квантовых технологий начали появляться с 2014 года, когда появилась программа развития квантовых технологий в Великобритании (UK National Quantum Technology Program). Позднее к квантовой гонке стали присоединяться такие страны, как Китай, объявивший о старте «квантовой» программы в 2016 году, Австрия с программой Quantum Austria в 2017 году, США в 2018 году (National Quantum Initiative), а также Сингапур, Швеция, Япония и Германия. Кроме того, страны Европейского союза в дополнение к существующим национальным программам в 2018 году запустили совместную десятилетнюю программу Quantum Flagship. Но хотя в прессе появляется все больше информации о достижениях и перспективах, связанных с квантовыми технологиями, не всегда понятно, что такое квантовые вычисления, квантовые коммуникации, сети квантового распределения ключей и новый квантовый Интернет.

Национальные планы по развитию квантовых технологий были сформированы и в Российской Федерации. С 2019 года действуют дорожные карты развития высокотехнологичных направлений «Квантовые вычисления» и «Квантовые коммуникации». Эти дорожные карты координируют две крупные государственные компании – квантовые вычисления закреплены за Росатомом, а за развитие квантовых коммуникаций отвечает РЖД. Обе дорожные карты сначала были утверждены правительством Российской Федерации на период с 2019 по 2024 годы, но впоследствии были расширены и продлены до 2030 года.

Дорожная карта по квантовым вычислениям направлена на создание прототипов отечественных квантовых компьютеров, в основе которых используются различные способы реализации кубитов (основных вычислительных элементов квантового компьютера). В частности, отечественные ученые используют сверхпроводниковые реализации кубитов, кубиты на ультрахолодных атомах в оптических потенциалах и ионах в оптических ловушках, а также оптические реализации кубитов. Важно отметить, что на текущий момент в мировом научном сообществе нет четкого мнения о том, на каких физических принципах должен строиться универсальный квантовый компьютер, и мы наблюдаем за процессом конкуренции различных платформ. В связи с этим развитие всех перспективных типов платформ в России потенциально позволит сократить технологическое отставание по разработке квантовых компьютеров в случае резкого прогресса платформ на одном из физических принципов. Причем речь может идти даже о проектах крупных мировых компаний, ведущих свои разработки в области квантовых вычислений, к которым относятся Google, IBM и Alibaba.

В рамках дорожной карты по квантовым коммуникациям осуществляется развитие технологии квантового распределения ключей (далее – КРК), а именно реализация инфраструктурных проектов по интеграции систем КРК в реальную телекоммуникационную инфраструктуру. В рамках таких инфраструктурных проектов ведутся работы по созданию магистральных квантовых сетей (далее – МКС) между крупными городами Российской Федерации. Так, в 2023 году на Форуме будущих технологий демонстрировалась работа сегментов МКС Москва – Санкт-Петербург, Москва – Нижний Новгород, было объявлено о планах по реализации сегментов Нижний Новгород – Казань и далее на восток, а также южного направления Москва – Сочи [6]. Кроме того, мероприятиями дорожной карты запланировано проведение дальнейших фундаментальных и прикладных исследований, которые позволят обеспечить создание новых принципов и устройств, открывающих возможности к улучшению технических характеристики систем КРК, а также развитию отечественной линейки компонентной базы квантовых коммуникаций. К таким проектам можно отнести создание устройств квантовой памяти и квантовых повторителей, фотонных интегральных схем, компактных устройств КРК, квантовых генераторов случайных чисел и так далее.

Важно отметить, что сегодня системы КРК для построения МКС находятся на очень высоком уровне готовности технологии, о чем свидетельствует появление первых сертифицированных решений. Именно поэтому с целью определения основных подходов к развитию системы нормативного регулирования в Российской Федерации отрасли квантовых коммуникаций распоряжением правительства Российской Федерации от 11 июля 2023 г. № 1858-р была утверждена «Концепция регулирования отрасли квантовых коммуникаций до 2030 года» (далее — Концепция), определяющая направления развития правовых механизмов интеграции квантовых коммуникаций в существующие сети связи, а также тенденции законодательства в сфере информационной безопасности, в том числе в отрасли государственного (муниципального) управления, критической информационной инфраструктуры, транспортной и промышленной безопасности, космической деятельности, безопасности банковских структур. При этом в качестве одной из задач Концепции выделяется необходимость поддержки отечественных производителей для обеспечения технологического суверенитета Российской Федерации в области квантовых коммуникаций.

Необходимость практического развития технологии квантового распределения ключей отмечается и в «Стратегии развития отрасли связи до 2035 года» (далее – Стратегия), утвержденной распоряжением правительства РФ от 24 ноября 2023 г. № 3339-р. В частности, в рамках первого этапа реализации Стратегии в период с 2023 по 2030 год предусматривается создание условий для предоставления услуг с использованием технологии квантового распределения ключей и ее внедрение с применением российского оборудования в интересах государственного сектора и корпораций.

По опыту автора статьи, после такого многообразия информации даже у самых подготовленных слушателей возникает множество вопросов о том, для чего именно должны использоваться квантовые коммуникации, какой реальный статус готовности технологии к ее масштабному применению, связаны ли как-то квантовые коммуникации и квантовые вычисления между собой, ограничиваются ли квантовые коммуникации только распределением ключей или можно построить квантовый Интернет между квантовыми компьютерами по аналогии с тем, как сейчас обычные компьютеры соединены между собой по Интернету. Ответы на эти вопросы будут раскрыты в последующих разделах статьи, чтобы позволить читателю сформировать понимание того, что квантовые коммуникации это и сети квантового распределения ключей, и новый квантовый Интернет.

Базовые понятия в области квантовых коммуникаций

В сентябре 2023 года в России был сделан первый шаг в области стандартизации технологии квантовых коммуникаций – появились первые предварительные национальные стандарты (ПНСТ) в области квантовых коммуникаций и квантового Интернета вещей, которые вводят термины и определения, а также описывают общие положения в данных предметных областях [2-5]. И именно в данных документах кроется ответ на вопрос, что же такое квантовые коммуникации и где находятся границы применимости данной технологии.

В соответствии с упомянутыми ПНСТ **квантовые коммуникации** представляют собой передачу информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности. Иными словами, к квантовым коммуникациям относятся все методы и способы формирования и передачи информации посредством физических систем, описываемых законами квантовой информатики. И таким образом мы можем говорить о **квантовой информации** – информации, представленной в виде состояний квантовой системы.

Как и в случае с классическими системами связи, для передачи квантовой информации необходимы каналы связи. И здесь появляется разделение на классические каналы и квантовые каналы. Под **классическим каналом** связи понимается канал связи, используемый для обмена информацией, закодированной в форме, которая позволяет прочитать и воспроизвести ее обратимым неразрушающим образом. В свою очередь, **квантовый канал** представляет собой канал связи для передачи **квантовых сигналов**, то есть сигналов, описываемых состоянием квантовой системы (**квантовым состоянием**). При этом подходы к описанию самого квантового состояния также могут отличаться в зависимости от типа квантовой системы. Наиболее часто при описании квантовых состояний речь идет о **кубите**, являющимся единицей квантовой информации. Эта единица реализуется двумя состояниями квантовой системы, находящейся в одном из состояний или в суперпозиции обоих состояний. Однако в более сложных системах могут использоваться **кудиты,** когда единица представления квантовой информации реализуется сразу несколькими состояниями квантовой системы (d-состояний, где d – произвольное целое число больше 1; при d = 2 кудит является кубитом).

Поскольку в квантовых коммуникациях используются оптические квантовые состояния, то для передачи квантовых сигналов может использоваться как стандартное телекоммуникационное оптическое волокно, так и атмосферные оптические каналы связи. Важно отметить, что в текущий момент на практике для передачи квантовых состояний в волоконно-оптических линиях связи принято использовать отдельное оптическое волокно, в котором нет других классических сигналов – такое оптическое волокно принято называть **темным волокном**.

Передачу квантовой информации осуществляет **квантовое оборудование**, представляющее собой оборудование, ключевые функциональные процессы которого основаны на использовании квантовых законов и явлений. При этом в квантовых коммуникациях чаще всего речь идет о **коммуникационном квантово-оптическом оборудовании** как подвиде квантового оборудования, использующем квантовые свойства света для обработки, хранения и передачи информации. Как правило, в таком оборудовании можно однозначно выделить **квантовый передатчик (Отправитель)**, обеспечивающий приготовление и передачу квантовых сигналов, а также **квантовый приемник (Получатель)**, обеспечивающий прием и обработку квантовых сигналов. При этом между этими двумя модулями для их функционирования необходимо обеспечить наличие квантового канала, служебного классического канала и **канала синхронизации**, используемого для передачи классических сигналов синхронизации между квантовыми передатчиком и приемником. Именно такая комбинация оборудования и каналов связи получила название **системы квантовой коммуникации**.

Квантовые коммуникации как новый квантовый Интернет

В общем смысле **квантовая (коммуникационная) сеть** представляет собой технологическую систему, включающую средства и линии связи, предназначенные для передачи квантовой информации. Иными словами, квантовая сеть представляет собой любую совокупность систем квантовой коммуникации. В силу этого в общем смысле понятие квантовой сети неразрывно связано с понятием **квантового Интернета**, который представляет собой глобальную информационную квантовую сеть, в узлах которой формируется, обрабатывается и хранится квантовая информация, и узлы которой соединены квантовыми каналами.

В таком сценарии квантовые сети могут использоваться для обеспечения связности любого квантового оборудования. В широком смысле квантовое оборудование может относиться к трем областям – квантовым вычислениям, квантовой сенсорике и самим квантовым коммуникациям. К области квантовых вычислений относятся квантовые компьютеры, и тогда квантовая сеть может использоваться для построения распределенного кластера квантовых вычислений из отдельных квантовых компьютеров. К области квантовой сенсорики относятся различные датчики, в основе которых используются квантовые законы и явления, будь то квантовые гироскопы, квантовые акселерометры или квантовые часы. В таком случае квантовая сеть может использоваться для соединения этого набора датчиков в единую сеть, например, для обеспечения распределенного мониторинга изменения состояния окружающей среды. К квантовым коммуникациям относится оборудование **квантового распределения ключей** (КРК), в таком случае квантовая сеть может применяться для формирования криптографических ключей между удаленными узлами сети.

В общем случае в составе квантовой сети можно выделить следующие базовые единицы:

- **узлы квантовой сети**, представляющие собой устройства, которые обрабатывают квантовую информацию (например, квантовые компьютеры), и связанные с ними квантовые приемники и/или квантовые передатчики;
- **узлы квантовой сети с квантовыми повторителями,** которые представляют собой комплекс устройств, расположенных в одном или нескольких узлах квантовой сети, предназначенных для ретрансляции квантового сигнала посредством распределения квантовой запутанности и квантовой телепортации;
- **узлы квантовой сети с квантовыми роутерами**, представляющие собой квантовые повторители, которые имеют несколько входов и/или выходов и обеспечивают возможность маршрутизации квантовых сигналов;
- **узлы квантовой сети с оптическими коммутаторами или оптическими объединителями**, которые предназначены для построения физической инфраструктуры передачи квантовых сигналов;
- **квантовые каналы** и **классические каналы**;
- **система управления и мониторинга квантовой сети,** обеспечивающая мониторинг статуса и управление узлами квантовой сети и входящими в них устройствами.

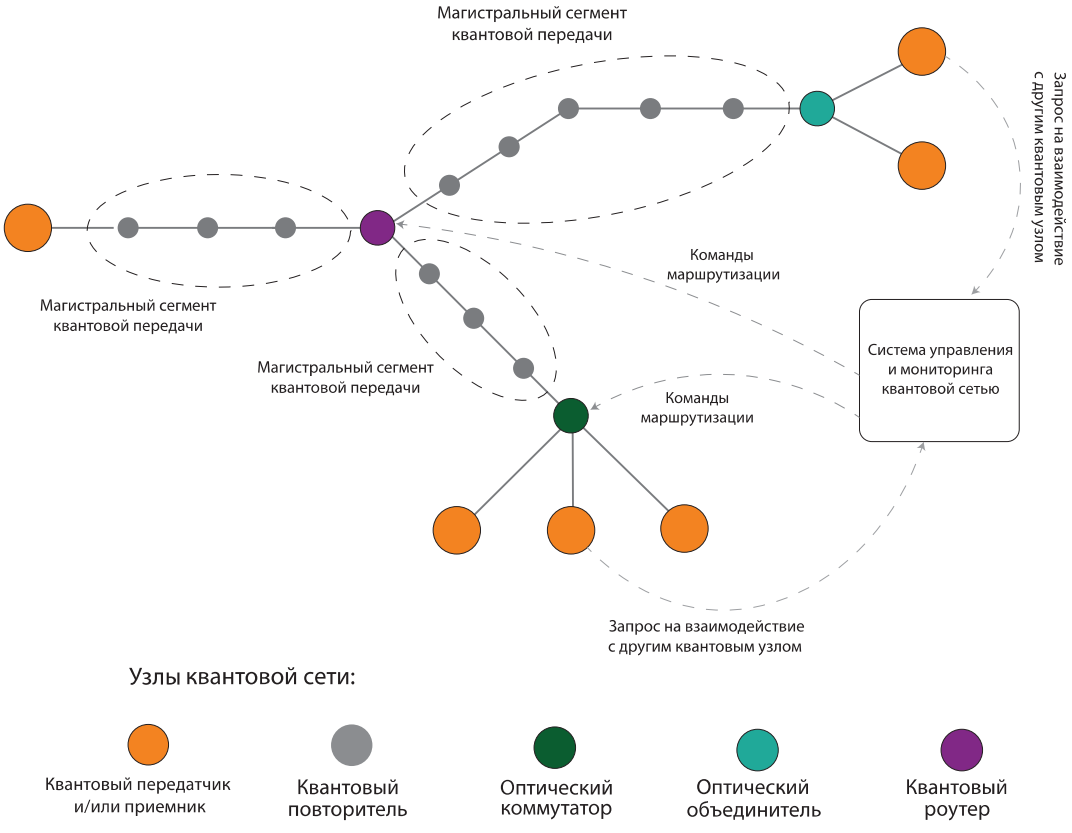


Рис. 1. Принципиальная схема произвольной квантовой сети смешанной топологии (с квантовыми повторителями и оптическими коммутаторами/объединителями).

Несколько последовательно соединенных квантовых повторителей, обеспечивающих увеличение дальности передачи квантовой информации, образуют магистральный сегмент квантовой передачи. В состав квантовой сети может входить несколько отдельных магистральных сегментов квантовой передачи. Различные магистральные сегменты квантовой передачи могут объединяться между собой с использованием квантовых роутеров или оптических коммутаторов, которые являются управляемыми элементами. В зависимости от команд маршрутизации, поступающих от системы управления и мониторинга квантовой сетью, они обеспечивают связность отдельных магистральных сегментов квантовой передачи.

С использованием квантовых повторителей и квантовых роутеров, а также оптических коммутаторов и оптических объединителей возможно построение квантовых сетей различных топологий: цепь, звезда, кольцо, дерево, смешанная топология. На рисунке 1 представлена принципиальная схема произвольной квантовой сети смешанной топологии.

Рассматриваемая структура квантовой сети позволяет обеспечить реализацию концепции **квантового Интернета вещей,** представляющего собой Интернет вещей с использованием квантовых технологий. Следует отметить, что квантовый Интернет вещей является специальным видом (подмножеством) классического Интернета вещей, и само появление нового термина и предметной области нацелено на расширение границ применения Интернета вещей, а не на его замену.

На данный момент идеи полноценного квантового Интернета и квантового Интернета вещей находятся только на этапе концептуального осмысления и проведения фундаментальных научных исследований, и мы не можем говорить о практическом внедрении этих решений в перспективе ближайших нескольких лет. Поэтому на текущий момент квантовые коммуникации не ассоциируются с такими фундаментальными приложениями и глобальными перспективами, но с учетом всего сказанного ранее можно уверенно заявлять о том, что конечной целью развития технологии квантовых коммуникаций является создание нового квантового Интернета. Причем это не противоречит тому, что сейчас под квантовыми коммуникациями все понимают реализуемые на практике **сети квантового распределения ключей** (далее – **сети КРК**).

Квантовые коммуникации как сети квантового распределения ключей

Под **сетями КРК** понимается технологическая система (квантовая сеть), включающая в себя системы КРК и линии связи и предназначенная для выработки квантовых ключей и квантово-защищённых ключей. Исходя из определения понятно, что сеть КРК состоит из набора систем КРК, которых в составе сети КРК может быть произвольное количество. Тем не менее, стоит отдельно объяснить, что же такое квантовые и квантово-защищённые ключи, и насколько они действительно «квантовые».

В первую очередь следует пояснить, что квантовый и квантово-защищённый ключ являются **секретными ключами**, определение которых также закреплено в нормативной базе в области криптографии [7]. Под секретным ключом подразумевается криптографический ключ симметричной криптосистемы, основанной на применении пар взаимосвязанных криптографических преобразований, в которой преобразования в каждой паре зависят от одного и того же секретного ключа. Важно добавить, что симметричная криптосистема может использоваться доверяющими друг другу сторонами, где для взаимодействующих пар (групп) пользователей формируются общие секретные ключи. В рассматриваемом нами случае сеть КРК является источником этих общих секретных ключей, которые впоследствии используются в классических симметричных криптосистемах. В этом смысле квантовые и квантово-защищённые ключи являются «классическими» криптографическими ключами, то есть представляют собой набор классических битов, а квантовость их природы связана лишь с методом формирования этого набора битов у двух пользователей, находящихся на разных концах прослушиваемых каналов связи.

Квантовый ключ является результатом работы системы КРК, состоящей из двух пар – модуля отправителя и модуля получателя, соединенных между собой квантовым каналом, каналом синхронизации и служебным каналом. Формирование квантового ключа осуществляется в соответствии с квантовым криптографическим протоколом выработки и распределения ключей (ККП ВРК), включающим в себя передачу и прием квантовых сигналов между модулями КРК в составе одной системы. Впоследствии квантовые ключи могут использоваться средствами криптографической защиты информации (СКЗИ), реализующими симметричные криптоалгоритмы, в том числе для обеспечения шифрования данных при их передаче по каналам связи.

Однако в силу физического ограничения на максимальную протяженность квантового канала, которая для существующих коммерческих систем КРК составляет порядка 100 км при работе по стандартному телекоммуникационному оптическому волокну, возникает необходимость формирования **квантово-защищённых ключей (КЗК)**, представляющих собой секретные ключи, защита которых при передаче или хранении осуществляется с использованием квантового ключа (ключей).

В простейшем случае метод формирования квантово-защищённых квантовых ключей подразумевает передачу формируемого в одном из целевых узлов исходного секретного ключа SK по цепочке промежуточных узлов с перешифрованием данного ключа на квантовых ключах смежных сегментов квантовой сети. Иными словами, квантовые ключи последовательно соединенных сегментов квантовой сети используются для шифрования на этих сегментах других секретных ключей, выступающих в качестве защищаемой информации. При этом в качестве исходного секретного ключа SK может выступать как произвольный криптографический ключ, получаемый с генератора случайных чисел (в том числе квантового), так и как один из квантовых ключей сегмента сети КРК, в состав которого входит целевой узел (в котором должен сформироваться квантово-защищенный ключ), при этом не используемый в качестве ключа шифрования. Пример реализации такого метода передачи квантово-защищённых ключей представлен на рисунке 2.

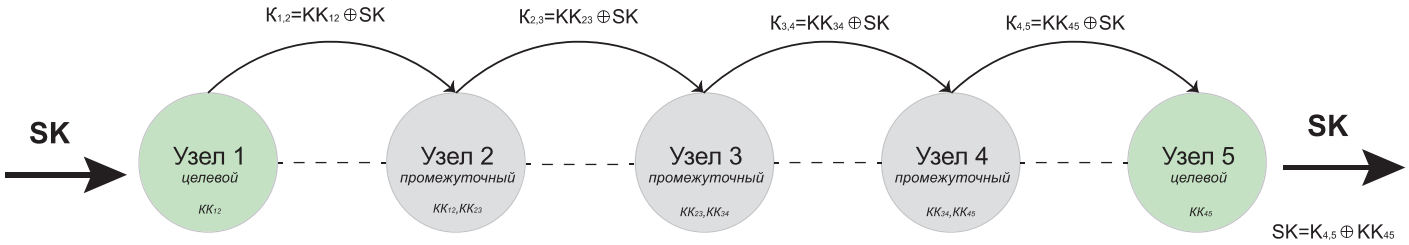


Рис. 2. Пример простейшего метода передачи квантово-защищенных ключей.

Квантово-защищённые ключи, наряду с квантовыми ключами, после формирования могут быть использованы в СКЗИ, реализующих симметричные криптоалгоритмы. При этом квантово-защищённые ключи могут быть сформированы между узлами сети, находящимися на любом расстоянии друг от друга – число сегментов сетей КРК с промежуточными узлами может быть любым. В том числе возможно построение сетей КРК различных топологий.

Еще одно важное уточнение заключается в том, что сеть КРК может выступать источником ключей для СКЗИ, находящихся в составе разных, уже существующих сетей связи, которые имеют свою каналообразующую сетевую инфраструктуру. Это значит, что маршрут передачи данных, защищаемых с использованием квантово-защищённых ключей, не обязательно должен повторять маршрут сегментов сети КРК, по которым был сформирован квантово-защищённый ключ. Более того, ситуация обратна – сеть КРК не подразумевает обязательное наличие каналов передачи пользовательских данных, а может выступать лишь дополнением к существующим сетям связи. Для удобства описания таких сетей связи в ранее упомянутых ПНСТ был введен термин **квантово-защищённые сети связи (КЗСС)**. Это сети связи, предназначенные для защищенной передачи данных с использованием квантовых ключей и/или квантово-защищённых ключей. Пример сопряжения произвольной сети КРК и двух различных КЗСС представлен на рисунке 3.

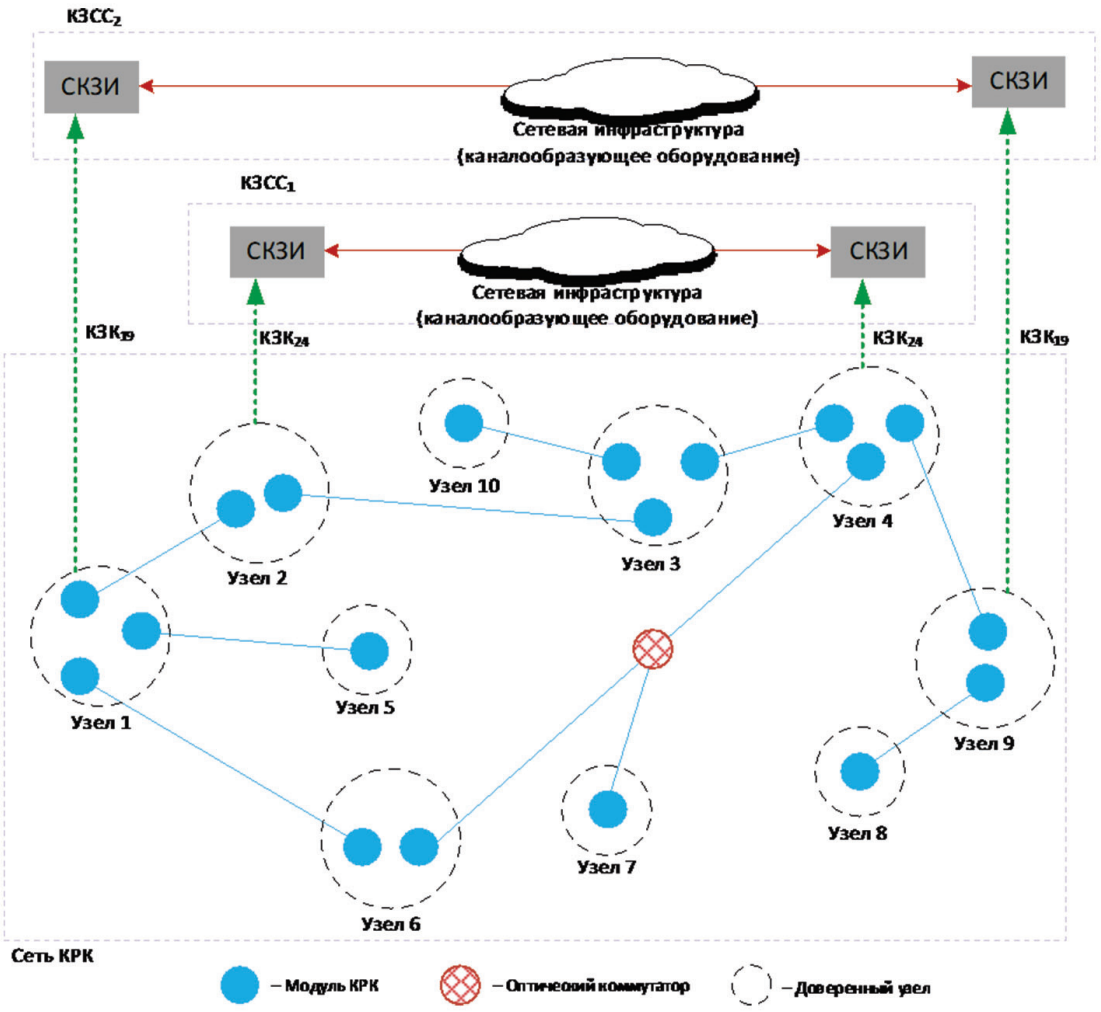


Рис. 3. Пример сопряжения произвольной сети КРК и двух различных КЗСС.

Именно на рассматриваемых здесь принципах реализуются текущие проекты по строительству сегментов магистральных квантовых сетей, которые упоминались во вводном разделе статьи. Поэтому широко обсуждаемые прикладные проекты в области квантовых коммуникаций в большей мере связаны именно с методами построения сетей КРК. Однако такая постановка вопроса также является корректной, поскольку сети КРК являются частным случаем квантовых сетей и, как следствие, одним из примеров реализации систем квантовой коммуникации.

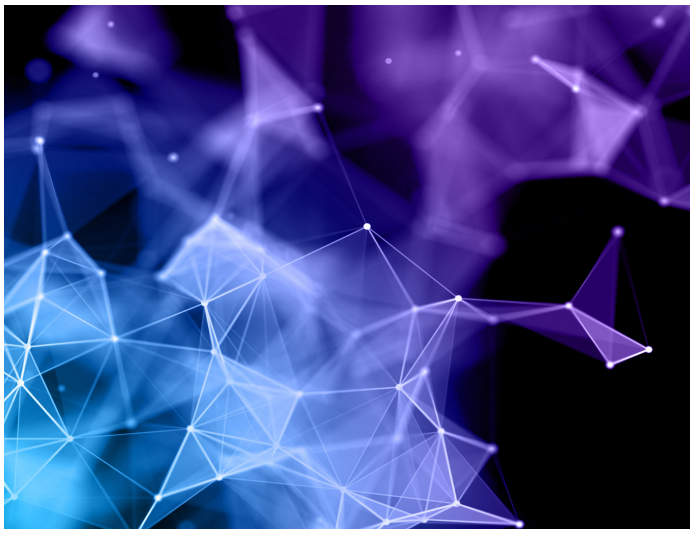
Несмотря на текущий прогресс в развитии сетей КРК, актуальным остается целый ряд прикладных вопросов, которые должны быть решены. В частности, необходимо осуществить:

- **формализацию услуг**, которые могут быть реализованы на базе сетей КРК;
- **разработку типовых сценариев применения** и предоставления сервисов, интеграции с существующими системами и сетями связи;
- **разработку ролевой модели взаимодействия** при функционировании квантовых сетей (магистральные, региональные и локальные операторы, потребители и т.д.);
- формирование набора **типовых параметров мониторинга** квантовых сетей и способов оценки **качества услуг;**
- разработку типовых **регламентов и организационно-распорядительных документов** для эксплуатации сетей КРК;
- **разработку типовых методик проведения измерений** для проверки параметров отдельных оптических и оптико-электронных компонентов систем;
- формализацию основных **подходов к оценке стойкости** к общеизвестным атакам на протоколы КРК и техническую реализацию систем КРК.

Дальнейшие горизонты

С учетом того, что технология КРК находится на высоком уровне технологической готовности, еще долгое время в глазах широкого круга общественности воплощением технологии квантовой коммуникации будут оставаться сети квантового распределения ключей. И чаще всего в ответе на вопрос «А что же такое квантовые коммуникации – сеть квантового распределения ключей или новый Интернет?» мы будем слышать первое. Но важно не забывать, что в России, как и во всем мире, уже сейчас ведутся исследования, направленные на создание глобального квантового Интернета, и что его появление не отменит необходимость существования сетей КРК, которые строятся в настоящий момент, поскольку сети КРК и квантовый Интернет являются двумя взаимно дополняющими концепциями и не только допускают, но и усиливают потенциал совместного существования.

При этом технология построения сетей КРК также требует совершенствования и реализации дополнительного комплекса мероприятий, включающих в себя как дальнейшее проведение научно-исследовательских и опытно-конструкторских работ по созданию новых образцов систем КРК и их компонентной базы, так и создание сопутствующей применению систем КРК нормативно-правовой базы.



Список литературы:

[1] Overview of Quantum Initiatives Worldwide 2023, QURECA, URL: https://qureca.com/overview-of-quantum-initiatives-worldwide-2023/

[2] ПНСТ 829–2023 «Квантовые коммуникации. Общие положения» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11 июля 2023 г. № 23-пнст)

[3] ПНСТ 830–2023 «Квантовые коммуникации. Термины и определения» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11 июля 2023 г. № 22-пнст)

[4] ПНСТ 831–2023 «Квантовый Интернет вещей. Общие положения» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11 июля 2023 г. № 23-пнст)

[5] ПНСТ 832–2023 «Квантовый Интернет вещей. Термины и определения» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11 июля 2023 г. № 24-пнст)

[6] «РЖД достроит квантовую сеть до Казани и Ростова-на-Дону». Ведомости. URL: https://www.vedomosti.ru/technology/articles/2023/07/14/985455-rzhd-dostroit-kvantovuyu

[7] ПНСТ 799–2022 «Информационные технологии. Криптографическая защита информации. Термины и определения» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 ноября 2022 г. № 124-пнст)

Об авторе:

Сантьев Алексей Альбертович, ООО «СМАРТС-Квантателеком», ведущий менеджер по развитию продуктов; SPIN-код: 9970-9568

Постквантовая криптография и практика TLS в браузерах

Александр Венедюхин

Аннотация:

Постквантовая криптография является популярным технологическим новшеством. Не так давно [1] о поддержке постквантовой схемы обмена ключами в приложении iMessage заявила компания Apple. Компания Google добавила поддержку аналогичной постквантовой криптосистемы в реализацию TLS браузера Chrome/Chromium [2]. В описании новшества Apple сказано, что постквантовая система должна быть внедрена заблаговременно, чтобы в случае появления квантового компьютера защитить ранее записанный трафик. Такая же причина названа основной и для появления постквантовой криптосистемы в браузере Google. Предполагается, что ранее записанный трафик, защищённый новой криптосистемой, квантовый компьютер раскрыть не сможет, в отличие от используемых сейчас криптосистем — которые, возможно, получится взломать. Такая защита не распространяется на трафик, записанный до добавления новых, стойких криптосистем, однако и подходящего квантового компьютера до сих пор не создано.

Ключевые слова:

квантовый компьютер, криптография, постквантовая криптография, TLS, веб-браузер

Точное значение термина «квантовый компьютер» зависит от той научно-технической области, в которой этот компьютер планируется строить и применять. Можно предложить и универсальное «вычислительное» определение: квантовый компьютер – это такой компьютер, на котором возможно эффективное исполнение квантовых алгоритмов. Ростом своей широкой популярности квантовые компьютеры как социальный феномен всецело обязаны одному вполне конкретному математическому алгоритму – предложенному в 1994 году алгоритму Шора, позволяющему ускорить решение важных для криптографии задач, в частности, задач факторизации целых чисел и дискретного логарифмирования.

Постквантовая криптография обязана своим возникновением тому, что ряд задач, традиционно считающихся вычислительно сложными, гораздо проще решить, если у вас есть квантовый компьютер. Примером является задача факторизации, с которой связана, например, оценка стойкости распространённой криптосистемы RSA. Несмотря на формальную ширину определения, на практике «постквантовыми» можно смело считать такие криптосистемы, для которых не известно методов атаки конкретно с использованием алгоритма Шора – самого знаменитого из квантовых алгоритмов и одного из самых часто упоминаемых в современной популярной литературе алгоритмов вообще (но, конечно, после алгоритма Евклида, с которым механизм применения алгоритма Шора связан математически).

Вычисление невычислимого

Сама концепция квантовых вычислений возникла значительно раньше алгоритма Шора и без всякой привязки к криптологии и взлому криптосистем. Идею использования мощности пространства квантовых состояний для аналоговых вычислений в своей печатной работе одним из первых высказал советский математик Юрий Иванович Манин – речь идет о книге «Вычислимое и невычислимое», 1980 год, «Советское радио». Но представления о «квантовой обработке информации» циркулировали среди физиков и математиков раньше, примерно с конца 60-х годов прошлого века [3]. Реализация квантовых вычислений – это обобщение понятия вычислительной сложности, приводящее к попыткам придумать способ, который позволил бы «вычислить невычислимое» без ограничений классической физики: затрат энергии и пространства.

Интерпретация фундаментальных представлений о возможности вычислить ту или иную функцию имеет большое количество чисто философских воплощений. Современное, популярное состояние данной области в применении к криптосистемам является прикладным преломлением: узкие задачи, стоящие за квантовым криптоанализом асимметричных криптосистем, вполне себе «вычислимы» и на классическом цифровом компьютере, вот только времени на поиск решения «в лоб» потребуется экспоненциально больше. Гипотетический квантовый компьютер мог бы решить эти задачи «в лоб», то есть методом полного перебора, но за обозримое время: алгоритм Шора описывает способ сворачивания «экспоненты сложности» в пространстве состояний квантовых частиц, который позволяет сразу получить полезный результат.

Такая ситуация даёт возможность находить эффективные вероятностные алгоритмы, исполняемые классическим компьютером, для многих задач. Эти алгоритмы, разумеется, эффективно решают только частные случаи сложных задач в некотором приближении к оптимальному решению, но на практике этого достаточно. Так, в случае не абсолютно стойких криптосистем ничто не запрещает успешно угадать любой секретный ключ, скажем, с трёх попыток, поскольку правиль-

ность ключа нетрудно точно проверить. При правильно выбранных параметрах криптосистемы вероятность угадать ключ довольно мала, однако и практические алгоритмы криптоанализа не просто оптимизируют полный перебор, а выстраивают именно процесс угадывания, то есть остаются эвристическими, уменьшая количество попыток подбора до практических значений.

Эффективными оказываются как более общие вероятностные алгоритмы с оптимизированным перебором (это, в частности, популярные методы ИИ – искусственного интеллекта), так и алгоритмы, подходящие только для конкретных конфигураций параметров. То есть для задач криптоанализа сейчас предлагаются более эффективные классические – не квантовые – алгоритмы, которые являются практическими. Собственно, даже алгоритм Шора остаётся вероятностным, но его особенность в универсальном методе взлома, подходящего для целого класса криптосистем и параметров.

Факторизация модулей

Традиционный пример для алгоритма Шора — RSA. Стойкость этой криптосистемы основывается на том, что вычислительно сложно находить разложение произвольных больших чисел на простые множители. Задача называется факторизацией. В RSA факторизовать требуется открытый ключ, модуль: большое число, являющееся произведением двух простых. С математическими свойствами таких разложений связаны конкретные периодические структуры, точное знание о которых позволяет быстро вычислить секретное разложение даже для больших чисел. Алгоритм Шора как раз и описывает способ нахождения соответствующего периода методами математического аппарата квантовой механики. Если этот аппарат удастся без существенных изменений перенести на достаточно мощную физическую реализацию, то получится аналоговый квантовый вычислитель, позволяющий выполнять факторизацию больших чисел «быстро». Из этого, впрочем, не следует, что «сломается вся современная криптография».

В чуть более строгой классификации алгоритм Шора относится к квантовым алгоритмам «нахождения периода» (периода функции в данном случае). Именно в этом состоит квантовая часть алгоритма, а само фактическое разложение на множители выполняется классическим компьютером (это и есть связь с алгоритмом Евклида). Другими словами, даже в теории квантового криптоанализа квантовый компьютер без классического бесполезен.

Возможность взломать RSA – в сугубо практических терминах TLS и браузеров – означает, что на основе открытого ключа можно за обозримое время вычислить секретный, нарушив защиту. Конструкция квантового «нахождения периода» переносится и на другие асимметричные криптосистемы, отличающиеся от RSA. Например, на ECDSA.

Асимметричные криптосистемы в TLS непосредственно для защиты трафика не используются, поскольку это слишком накладно в плане вычислительных ресурсов. Для защиты полезных данных в TLS (а также и в большинстве защищённых протоколов мессенджеров) используются симметричные шифры (AES, ChaCha20, «Кузнечик» и др.). Симметричные шифры страдают от известных квантовых атак не столь радикально, но это только если рассматривать симметричные шифры в максимальной общности.

Если направление атаки сузить, то и для симметричных шифров не всё так хорошо. Универсальная оценка эффективности атак на симметричные шифры силами квантовых компьютеров подразумевает полный перебор значений, то есть ситуацию «лобовой атаки», без использования каких-то особенностей конкретного алгоритма: и тут всё неплохо – квантовый алгоритм поиска (алгоритм Гровера) даёт максимально только «квадратичный» прирост, то есть 256-битный ключ как бы превращается в 128-битный, но 128 бит стойкости это всё ещё более чем достаточный уровень.

Однако для конкретных практических шифров могут быть, в теории, предложены специальные квантовые алгоритмы, ускоряющие криптоанализ конкретного шифра, ломающие именно этот шифр. Конечно, тут опять необходим универсальный квантовый компьютер, поскольку схемы, реализующие тот или иной шифр, оказываются весьма сложными. Так что теоретические возможности «квантовых атак» на симметричные шифры всё ещё оказываются весьма скромными: приблизиться к эффективности алгоритма Шора пока не получается.

В порядке очереди

Повышенная квантовая стойкость симметричных шифров делает их защиту «постквантовыми методами» далеко не первоочередной задачей: достаточно длинные ключи позволят защитить сообщения мессенджеров и трафик TLS и после гипотетического появления теоретического квантового компьютера. Однако, чтобы использовать симметричные шифры,

сторонам соединения нужны симметричные секретные ключи. В TLS, за исключением редких случаев (PSK – Pre-Shared Key), эти симметричные ключи согласуются сторонами на этапе установления соединения через незащищённый канал. Для этого служит та или иная современная реализация протокола Диффи-Хеллмана (DH), гораздо реже – всё ещё используется RSA. Все эти криптосистемы уязвимы для квантовой атаки по алгоритму Шора. (Кстати, сам протокол DH к подобному взлому устойчив, поэтому применяется в постквантовых схемах, но вот конкретный вариант базовых операций, используемый в TLS, уязвим.)

Это означает, что симметричные ключи можно раскрыть, не прибегая к взлому самих шифров – достаточно атаковать сеанс выработки симметричных ключей, проходящий в открытом виде. Поэтому самый высокий приоритет для защиты постквантовыми методами в TLS имеет именно этап согласования симметричных секретных ключей. Всё это применимо и к защищённым мессенджерам, но далее все примеры в статье будут для случая TLS.

В TLS имеется ещё один непосредственно уязвимый для квантовых атак архитектурный элемент: аутентификация узлов, или TLS-сертификаты. Предполагается, что клиент, выполнив проверку электронных подписей, связанных с сертификатом сервера, определяет, что соединяется именно с той стороной, с которой планировал (при аутентификации клиента сервером процесс аналогичный).

Квантовая атака позволяет взломать криптосистему электронной подписи и выпустить поддельные сертификаты. С точки зрения квантовых атак здесь есть одно важное отличие от описанной в предыдущем абзаце ситуации с согласованием симметричных ключей: взлом электронных подписей, используемых в сертификатах, вообще говоря, не позволяет непосредственно атаковать ранее записанные TLS-сессии, если симметричные ключи в них согласовывались по протоколу Диффи-Хеллмана для конкретного сеанса.

Взлом криптосистемы электронной подписи никак не помогает подставить подменный TLS-сертификат в сессию, которая к моменту взлома давно завершилась. Атаковать «подменным сертификатом» записанные сессии не получится, поскольку симметричные секреты в современных вариантах TLS вырабатываются с учётом так называемой прогрессивной секретности, то есть обеспечивают защиту в случае компрометации долговременного, статического серверного секретного ключа, используемого при аутентификации. Другими словами, для раскрытия записанного трафика корректной TLS-сессии взлом ключа из TLS-сертификата бесполезен, но чтобы защитить процесс обмена ключами, всё равно нужна постквантовая стойкость.

Секретность передаваемых данных желательно сохранять в течение какого-то заметного времени, поэтому и переход на постквантовые криптосистемы для обмена симметричными ключами должен произойти заранее. Тогда «неожиданно появившийся» квантовый компьютер, конечно, позволит подделать аутентификационную информацию во вновь устанавливаемых сессиях и перехватить их, но хотя бы не позволит раскрыть старый, ранее записанный трафик, так как для его защиты уже некоторое время использовались криптосистемы с постквантовой стойкостью.

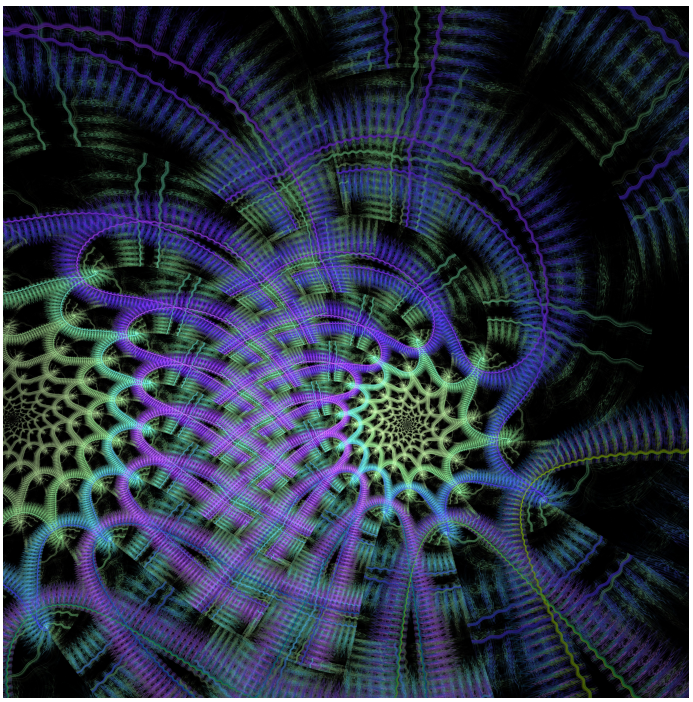
Оценки стойкости гибридов

Что же подразумевается под термином «постквантовая стойкость»? Подразумевается, что для криптосистемы, обладающей такой стойкостью, не известны квантовые алгоритмы, позволяющие взломать эту криптосистему с использованием некоторого «практического» количества ресурсов. Оценка стойкости криптосистем в теоретической криптографии вообще представляет собой отдельную сложную область, насыщенную эвристическими подходами. Оценки традиционно строятся на подсчёте вычислительных ресурсов, взятых в рамках той или иной модели: количество памяти, количество «битовых операций» и др. – подходы различаются в деталях. То же самое верно и для «постквантовой стойкости»: речь не идёт о том, что для той или иной «постквантовой криптосистемы» эффективные квантовые алгоритмы взлома невозможны в принципе, даётся лишь предположительная оценка квантово-вычислительных затрат, исходя из известных на момент исследования алгоритмов атак и их сравнения с мощностью классических атак, то есть всё это актуально для случая, когда для криптоанализа используется классический компьютер.

Например, оценки сложности квантового алгоритма Шора показывают, что затраты на взлом RSA квантовым компьютером могут находиться в области технологической достижимости. Но не более. Заметьте, это всего лишь предположение, а оценки требуемых ресурсов, если представить их в количестве квантовых элементов (кубитов и «триггеров/гейтов»), различаются буквально в тысячи раз. И тем не менее, эта квантовая сложность для RSA несравнимо меньше классической сложности взлома, отсюда делается вывод, что RSA не обладает постквантовой стойкостью для современной разрядности ключей. То же самое применимо к ECDSA (разрядность даже меньше) и к распространённым вариантам реализации протокола Диффи-Хеллмана. Оговорка про разрядность важна с практической точки зрения, поскольку задаёт нужное количество квантовых элементов. То есть оценки постквантовой стойкости базируются на том, что это именно алгоритм Шора не позволяет сломать данную криптосистему на предложенном количестве «кубитов» и «гейтов».

Наличие «постквантовой уязвимости» ничего не говорит ни о том, что классические методы атак на ту же криптосистему не могут быть улучшены, ни о том, что классический метод атаки обязательно существует. Так, для факторизации RSA-ключей алгоритм Шора работает «в лоб», как работал бы и классический компьютер – никаких алгоритмических «обходных путей» в алгоритме нет, поэтому он и не может сам по себе улучшить классические результаты факторизации. Преимущество алгоритма Шора в том, что он показывает, как перенести вычислительные затраты факторизации на квантовые схемы, где необходимый уровень этих затрат минимизируется.

Постквантовая криптосистема должна обладать и классической стойкостью – иначе смысл её применения теряется. Постквантовая стойкость никак не гарантирует наличие классической. Но у постквантовых криптосистем, несмотря на все трудности, сейчас есть большое, огромное преимущество перед квантовыми компьютерами: универсальных квантовых компьютеров с алгоритмом Шора нет ещё и на горизонте, а по-



сткванговые криптосистемы уже внедряются в качестве элемента гибридной защиты – происходит это из-за предположения, что квантовый компьютер всё же может быть создан и позволит расшифровать ранее записанный трафик.

Гибридная защита тут означает, что криптосистема с постквантовой стойкостью используется в сочетании с классической, хорошо отработанной и изученной, криптосистемой. Это исключает «обратную атаку»: если та или иная постквантовая криптосистема окажется нестойкой к классическим атакам, то защиту обеспечит классическая часть гибридной схемы.

Почему данный подход не применялся к разнотипным криптосистемам в том же TLS ранее, без требований о квантовых компьютерах? Резонный вопрос. Например, можно взять какую-нибудь экзотическую классическую криптосистему и прикрепить её к распространённой реализации классического протокола Диффи-Хеллмана (DH) без оглядки на квантовые компьютеры, чтобы, если через двадцать лет будет найден неквантовый метод эффективного взлома классического DH, записанный трафик всё ещё оказался бы защищён (улучшения вычислительных атак на классический DH за долгие годы достигнуты существенные). Такие гибридные криптосистемы существуют, но почему это не делается повсеместно, в том же TLS? Отчасти положение дел объясняется тем, что задачи, на которых строятся распространённые сейчас асимметричные криптосистемы, нередко имеют математически эквивалентную, с точки зрения сложности, структуру: то есть одну задачу можно перевести в другую «с точностью до некоторой константы» (иногда, впрочем, «константа» получается слишком большой). Навешивание же дополнительных алгоритмов может приводить к росту сложности реализации. Эта точка зрения настолько популярна, что нередко предлагается даже в случае постквантовой стойкости отказываться от гибридных схем и сразу переходить на только постквантовые. В отношении постквантовых схем это выглядит сомнительным, поскольку для новых криптосистем – а также, что важнее, для их реализаций – всё ещё не ясен практический уровень стойкости даже к классическим атакам.

Интересно, что не все криптосистемы, обладающие постквантовой стойкостью, разработаны недавно. Так, исходная асимметричная криптосистема McEliece, практические варианты которой имеют сейчас статус постквантовой стойкости, была предложена ещё в 1978 году. Конечно, в то время постквантовая стойкость не предполагалась, так как алгоритм Шора ещё не был опубликован. В McEliece такая стойкость возникает в качестве побочного эффекта, поскольку сложность обратимости ключей для этой криптосистемы базируется на задаче из теории кодирования («обращение» произвольного линейного кода с исправлением ошибок), которая для алгоритма Шора не подходит.

Собственно, если судить по конкурсным криптосистемам, отбиравшимся NIST [4] по критерию постквантовой стойкости, задачи теории кодирования используются в нескольких современных постквантовых системах. Второй весьма популярный механизм — решётки (алгебраическая структура, простейший пример которой даёт регулярная сетка из точек, расставленных по квадратным клеткам на листочке бумаги). Это, впрочем, достаточно поверхностная и тематическая оценка.

Практика браузеров

Математический аппарат, прямо связанный и с решётками, и с «помехоустойчивыми» кодами, использует постквантовая криптосистема, встроенная в TLS-стек Chrome/Chromium. Эта криптосистема относится к гибридным: классическая часть здесь – X25519, постквантовая – Kyber768.

X25519 [5] это хорошо известный вариант протокола Диффи-Хеллмана на эллиптической кривой (Curve25519, откуда и название). Kyber768 [6] – механизм «инкапсуляции ключа» (KEM – Key Encapsulation Mechanism), или асимметричная криптосистема, предназначенная для передачи общего секрета (формально, протокол Диффи-Хеллмана тоже можно переопределить как KEM-схему). Данная гибридная криптосистема известна под не менее «гибридным» названием: X25519Kyber768 [7], — а так как сейчас используется draft-версия, то полное название – X25519Kyber768drafto. Способ использования данной криптосистемы сейчас совместим только с TLS версии 1.3.

X25519Kyber768 в TLS предоставляет механизм получения общего секрета. Это развитие обязательно для TLS 1.3 протокола DH. Технически, в TLS-стеке браузера происходит следующее. TLS-соединение начинается [8] с сообщения клиента (ClientHello) в сторону сервера. Сообщение содержит параметры соединения, которые готов поддерживать клиент. Штатным ответом сервера на ClientHello является парное к нему сообщение ServerHello. В версии TLS 1.3 стороны уже на раннем этапе установления соединения согласовывают общий секрет. Этот секрет необходим для выработки симметричных ключей защиты трафика.

Используемый для согласования секрета протокол состоит в обмене открытыми частями DH с последующим вычислением секретного значения каждой из сторон.

В постквантовом варианте X25519Kyber768 заменяет для Chrome клиентскую часть ключевого обмена начального этапа TLS-соединения. То есть в ClientHello добавляются данные X25519Kyber768. Если TLS-сервер поддерживает данную криптосистему, то он извлекает клиентскую часть обмена из ClientHello и может вычислить совместимый серверный ответ (см. ниже), который передаёт в ServerHello. Схема архитектурно повторяет существующие варианты, уже используемые в TLS. Внедрение X25519Kyber768 никак не изменяет других аспектов соединения: сохраняются логика и порядок сообщений, не изменяются сертификаты и ключи к ним, используются те же симметричные шифры.

«Гибридизация» криптосистем здесь сводится к конкатенации байтов, составляющих клиентскую часть протокола Диффи-Хеллмана X25519 и открытый ключ клиента Kyber768.

На сервере данные разделяются на относящиеся к разным криптосистемам гибрида и обрабатываются отдельно. А именно: для X25519 сервер вычисляет общий секрет DH и серверный открытый ключ DH точно так же, как это делалось бы в случае «негибридной» X25519; для Kyber768 сервер генерирует общий секрет и «инкапсулирует» его, используя открытый ключ Kyber, присланный клиентом в ClientHello. В результате на сервере формируются два массива байтов, которые можно передать клиенту по открытому каналу, и два секретных массива байтов, которые служат для вычисления набора ключей симметричных шифров; эта секретная часть обмена передаётся на вход внутренней функции генерирования симметричных ключей сервера. Это и есть шаг смешивания секретов, полученный классической и постквантовой криптосистемой.

Чтобы успешно атаковать сессию, атакующему нужно взломать и классическую часть (X25519), и постквантовую (Kyber768). Если у атакующего есть квантовый компьютер, то он определяет 256 бит классической X25519, но остаются неизвестными 256 бит постквантовой Kyber768. Если квантового компьютера нет, но Kyber768 оказалась нестойкой к классическим атакам, то сохраняются 256 бит X25519. А в самом худшем варианте, когда и квантовый компьютер есть, и Kyber768 оказалась нестойкой к классическим атакам, схема скомпрометирована полностью. Однако в случае, когда обе криптосистемы оказались нестойкими к классической атаке, ничего не ухудшилось, поскольку X25519 и так повсеместно используется.

Клиент, получив серверную часть X25519Kyber768, также разделяет данные на открытую часть обмена DH X25519 и шифротекст Kyber768 с «инкапсулированным» секретом, вычисляет общий секрет DH X25519 и, используя клиентский секретный ключ, извлекает секрет Kyber768. Оба полученных значения объединяются, на основе объединённого секрета клиент вычисляет свой набор симметричных ключей. Если всё сработало правильно, то результат должен совпасть с серверным.

Чтобы получить постквантовую стойкость в описанной практической схеме, требуется дополнительно передать примерно килобайт данных для каждой из сторон: основная часть — обмен Kyber768, 1184 и 1088 байтов. По меркам постквантовых криптосистем это весьма и весьма небольшой объём данных, он сравним с типичными сейчас длинами RSA-ключей, но значительно превышает показатели DH на эллиптических кривых.

* * *

Квантовые вычисления в философском смысле – это попытка получить доступ на самом низком, самом прямом и «железячном» уровне к центральному «процессору» (ЦПУ) вселенных, то есть, к необозримому «чипу», на котором, возможно, окружающая действительность исполняется в режиме виртуализации. Это неплохо соответствует фольклорной интерпретации термина «квантовый» в отношении компьютера: элементы полупроводниковых чипов, находящихся внутри этого ящика, становились всё меньше и меньше, и вот, за гонкой нанометровых технологий, ситуация проваливается в квантовые элементы – получите квантовый компьютер. И действительно, пусть сам предполагаемый принцип квантовых вычислений не имеет ничего общего с уменьшением линейных размеров полупроводниковых вентилей и законами Мура, попытки физической реализации квантовых вычислителей уже сейчас подразумевают управление отдельными атомами. Если квантовый компьютер сделать не получится, эти наработки наверняка пригодятся для дальнейшей миниатюризации компьютеров классических. Что же касается теоретико-информационной криптографии, то она, похоже, выигрывает и тут.

Список литературы:

[1] iMessage with PQ3: The new state of the art in quantum-secure messaging at scale https://security.apple.com/blog/imessage-pq3

[2] Feature: X25519Kyber768 key encapsulation for TLS https://chromestatus.com/feature/5257822742249472

[3] Cuffaro, Michael and Amit Hagar, «Quantum Computing», The Stanford Encyclopedia of Philosophy https://plato.stanford.edu/entries/qt-quantcomp/

[4] NIST, https://csrc.nist.gov/projects/post-quantum-cryptography

[5] RFC 7748 https://datatracker.ietf.org/doc/html/rfc7748

[6] Kyber, https://pq-crystals.org/kyber

[7] IETF draft https://www.ietf.org/archive/id/draft-tls-westerbaan-xyber768d00-03.html

[8] RFC 8446 https://datatracker.ietf.org/doc/html/rfc8446

Об авторе:

Александр Анатольевич Венедюхин
ФРСТ «ИнДата», Россия, Москва

Квантовые коммуникации: «пик хайпа» или «плато продуктивности» с точки зрения дилетанта

Валерий Киселёв, Павел Храмцов

Аннотация:

В статье обсуждается «зрелость» технологии квантовой коммуникации с точки зрения теории внедрения инноваций в народное хозяйство Роджерса и кривой «хайпа» Гартнера, приведены основные ключевые вехи теории и практики квантовых коммуникаций, кратко рассмотрены некоторые особенности квантовых измерений и квантовых состояний фотонов.

Ключевые слова:

фотон, квант, квантовая спутанность, запрет клонирования, слабые измерения, уравнение Белла

Вместо введения

«Квантовые коммуникации» – чего больше в этом словосочетании? Маркетинга, хайпа – или же это словосочетание отражает физический смысл процессов будущих коммуникационных сетей?

Современный маркетинг – это зеркало, кривизной которого управляют умелые руки/головы/мозги/профессионалы (нужное подчеркнуть).

Требуемая «кривизна» задаётся типом инвестора, который обеспечивает финансовый фундамент НИР и ОКР. Даже для фундаментальных научных исследований требуется ~~«выбивать»~~ обосновывать новизну, актуальность и практическую ценность «опытов». Инвестора, в том числе и государственного, нужно увлечь грандиозностью и практической осязаемостью результатов на коротком отрезке времени.

Ещё на слуху история «холодного ядерного синтеза» (ХЯС; англ. Cold fusion), которая тянется уже более 20 лет. Есть «железо» (лабораторные установки), проводились и до сих пор проводятся международные конференции [1], но до сих пор «плазмы на лабораторном столе» (словосочетание само по себе выглядит, скажем так, странно) продемонстрировано не было. Хотя, справедливости ради следует заметить, что «горячего» управляемого ядерного синтеза тоже пока нет.

Именно по причине отделения «зёрен от плевел» – маркетинга от реальных результатов – термин «квантовые коммуникации» требует разъяснения и толкования. Вообще говоря, термин «коммуникация» имеет много значений. Вот только некоторые из них:

- У Даля – это «сообщение, путь, дороги, средства связи».
- У Ожегова – это «1. Путь сообщения, линия связи. 2. Сообщение, общение».
- В Большой советской энциклопедии – «I пути сообщения, транспорта, связи, сети подземного городского хозяйства. II Коммуникация общение. Обычно К. определяется как «передача информации» от человека к человеку».

Этот перечень источников и определений можно продолжать и дальше. Но понятно, что речь идет о среде/способе транспортировки чего-либо. Применительно к информационным

Панель «Дуализм «волна/частица»:

Дуализм волна/частица. Три электрона, попавшие в детектор после прохождения двойной щели, дали три типичные для частиц вспышки на экране. Но когда мы зарегистрировали много электронов, то обнаружили, что их распределение на экране, то есть вероятность попадания, описывается типичной для волны картиной интерференции. То есть регистрируем частицы, но вероятность регистрации описывается в конечном счёте волнами.

Дуализм «волна/частица».

коммуникациям чувствуется некий дуализм: либо «способ», либо само «сообщение» или даже «процесс» передачи информации.

Если к слову «коммуникация» добавить прилагательное «квантовая», то всё становится еще «запутаннее», не говоря уже о том, что термин «запутанные/перепутанные квантовые состояния» в теории, как, впрочем, и в реальности существуют.

Если снова обратиться к словарю Ожегова, то – «квант, квант, -а, м. В физике: наименьшее количество энергии, отдаваемое или поглощаемое физической величиной в её нестационарном состоянии. К. энергии. К. света. прил. ~овый, -ая, -ое. Квантовая теория. Квантовая электроника. К. генератор».

Собственно, вся эта терминология требует пояснения.

К счастью, в июле 2023 года Федеральным агентством по техническому регулированию были приняты предварительные национальные стандарты в области квантовых коммуникаций (ПНСТ 829 [2] — 830 [3]).

В ПНСТ 829 «квантовые коммуникации» определены как «*передача информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности*». В этом же стандарте указано, что «*в настоящее время в качестве квантовой системы для передачи информации используются фотоны, а основными системами передачи квантовой информации являются квантовые оптические системы*». Выглядит такое определение приблизительно так же, как сепульки и сепулькарии [4-6] у Лема.

Определения квантовых информационных технологий есть не только в наших предварительных стандартах (действуют до 2026 года), но в трудах международных организаций. Например, Международного союза электросвязи (International Telecommunication Union – ITU).

С сентября 2019 года в рамках этой организации образована рабочая группа FG-QIT4N, которая занимается вопросами применения квантовых информационных технологий в области связи.

В технических отчётах этой группы отмечено, что в международных стандартах нет определения терминов, относящихся к квантовым информационным технологиям, тем не менее определение словосочетания «квантовые коммуникации» есть [7]:

«5.3.1.6 quantum communication [b-ISO/IEC JTC1 AG4]: a new communication method using quantum entanglement effect for information transmission».

«Прямая передача» в этом определении отсутствует, но «спутанность» сохранилась.

Т.е. в этом определении совершенно ясно указано только на эффект «спутанности» при передаче информации.

Теперь продвинемся чуть дальше по пути разбора терминологии, а именно, вспомним об Интернете.

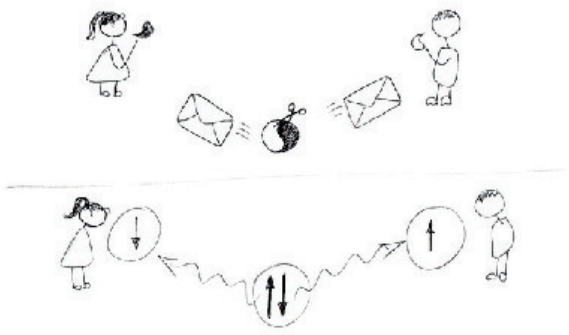
Современное понимание коммуникации в любом смысле этого термина подспудно подразумевает сеть «Интернет»., т.е. если речь зашла о неких «квантовых коммуникациях», то должен быть и «квантовый Интернет», и соответствующие ему RFC [8], которые должна выпускать соответствующая группа IETF [9].

Действительно, такая группа существует – QIRG (Quantum Internet Research Group) [10]. И эта группа выпустила два «черновика» (draft) и одно информационное RFC (RFC 9340) [11].

В этом RFC речь идёт о квантовых сетях как о сетях квантовых устройств, которые построены на фундаментальных квантовых принципах. Более того, речь не идёт о замене существующих

Панель «Определение квантовой спутанности»

Передача информации с помощью запутанных квантовых состояний. Это в целом похоже на общение по наземной почте, когда есть предварительная договорённость, что посылают, например, разрезанный пополам инь-ян, перемешав половинки. Кому какая половинка достанется — заранее не известно. Но открыв письмо, каждый адресат мгновенно знает, что получил другой. В квантовом случае ситуация похожа с точки зрения передачи информации. Рассылаются два фотона, про которые известно, например, что их суммарный момент вращения равен нулю. Зарегистрировав один фотон, адресат мгновенно знает, что получил другой. Интуиция, однако, может быть возмущена тем, что таинственный «коллапс волновой функции» происходит мгновенно, быстрее скорости света. Многие авторы называют это нарушением принципа локальности [панель «Локальность»]. В то же время, классическая интерпретация квантовой механики позволяет обойтись без мистики – есть просто два возможных исхода измерений – вниз-вверх, как на картинке, или вверх-вниз. Вероятности «оба вверх» и «оба вниз» равны нулю. Эта картина подтверждается экспериментом. Важно, что таким способом, как и в примере с письмами, нельзя обмениваться информацией между адресатами. Каждый из них, взятый в отдельности, получает случайную последовательность от общего источника, то есть никакой информации кроме того, что у другого адресата, последовательность комплементарная.



Определение квантовой спутанности.

сетей квантовыми. В нем обсуждаются принципы построения гибридов квантовых и обычных сетей.

Таким образом, можно предположить, что участники группы считают, что квантовая коммуникация — это коммуникация в квантовых сетях. Тут опять про «сепульки». Квантовый — это явно о физической технологии, из которой много чего может следовать.

Постановка исследовательских задач и описание ожидаемых результатов и эффектов в RFC 9340 выглядят грандиозно и впечатляюще.

Вот только одно «но», которое навевает «смутные сомнения», — это презентация группы на IETF 104 [12] в марте 2019 года, в которой эффект «спутывания» проиллюстрирован двумя слайдами (рис. 1):

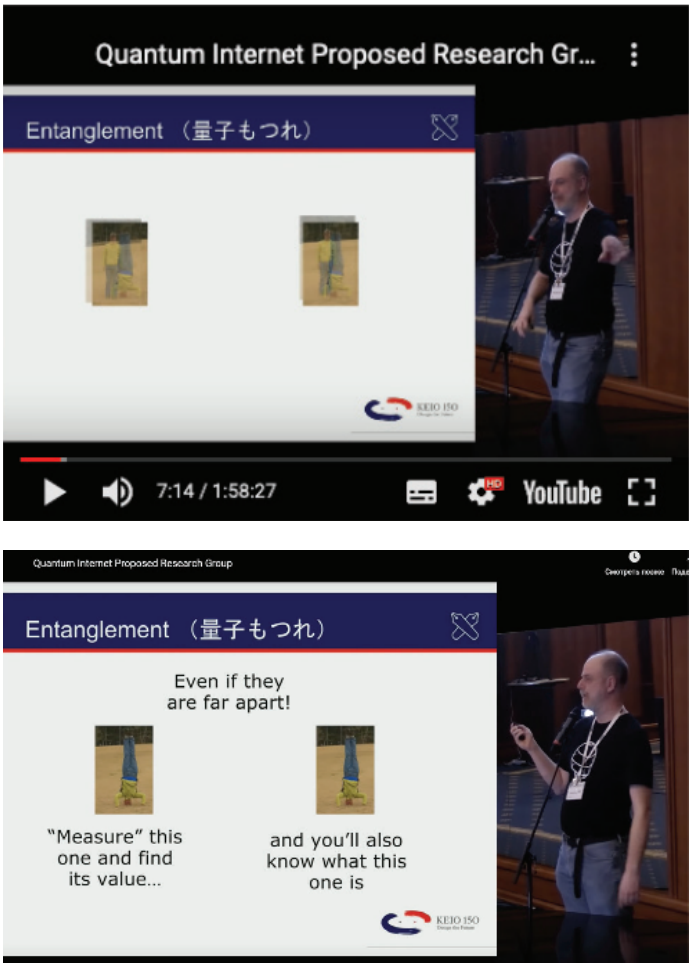


Рис. 1. Иллюстрация эффекта спутывания.

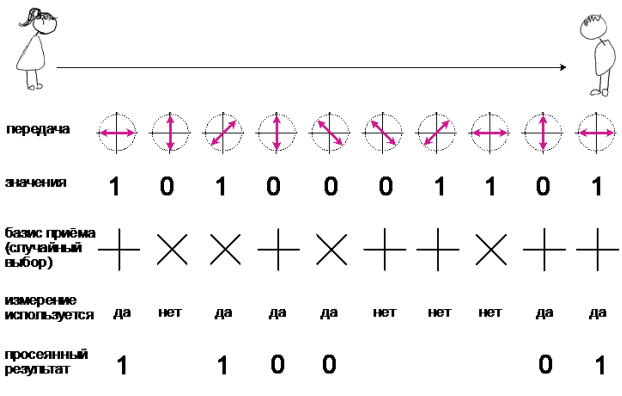
Есть ощущение, что по законам сохранения, на которых основана «спутанность», у кого-то из двух наблюдателей персонаж на слайде должен стоять твёрдо на своих ногах, если у другого он столь же твёрдо и устойчиво стоит на голове. Для результата, т.е. для определения квантового состояния это не столь существенно, но всё же...

Тем не менее, в этой презентации чётко определены границы применения квантовых коммуникаций для двух вариантов:

- «неспутанных» сетей;
- «спутанных» сетей.

Панель «Обмен ключами без «спутанности»

Первая из предложенных схем передачи информации с участием квантового канала. Фотоны передаются от А к Б. По договорённости поляризация фотона в горизонтальном направлении или под 45 градусов означает единицу, а в вертикальном или под 135 градусов — ноль. Отправитель А случайным образом выбирает одну из четырёх поляризаций фотонов. Адресат Б проводит измерение поляризации, при этом случайным образом решая, что измерять — поляризацию в вертикально-горизонтальном направлении или в направлениях 45-135 градусов. Физически это можно представить как поворот поляризатора (конечно, электронного) так, чтобы он пропускал поляризацию горизонтальную или под 45 градусов. Регистрация фотона с такой поляризацией воспринимается как единица, а поляризация вертикальная или под 135 градусов — как ноль. Назовём настройку поляризатора базисом (как в обычной векторной алгебре), соответственно, прямым или повёрнутым. Принципиально здесь то, что если фотон, например, поляризован под 45 градусов, а Б измеряет его в прямом базисе (т.е. горизонтальную поляризацию), то он получит с равными вероятностями оба возможных результата [см. панель «Квантовые измерения»]. Если же фотон создан в прямом базисе (т.е. имеет горизонтальную или вертикальную поляризацию), то результат измерения будет всегда однозначным — именно таким, каким был создан фотон. В процессе передачи Б записывает результаты измерений, сохраняя их в секрете. После передачи А сообщает Б (по открытому каналу), какой базис был использован, и Б выбрасывает все измерения в неправильно угаданном базисе. Получается т.н. просеянный результат, в котором каждое измерение однозначно. При попытке перехвата перехватчик должен послать фотон на замену измеренному, чтобы сохранить секретность, но по теореме о невозможности клонирования [см. панель «Невозможность квантового клонирования»] такие фотоны будут часто иметь неправильный базис, что скажется на статистическом разбросе результатов повторных измерений, которые должны быть однозначны. Это должен заметить Б и забраковать передачу данных (например, ключа для кодировки). Приведённая схема называется BB84 по имени создателей и году публикации [REF]. Она иллюстрирует принцип использования квантовых свойств для криптографии. В реальности используются более сложные алгоритмы.



Обмен ключами без «спутанности».

В первом случае, который, к слову сказать, реализован на практике, речь идёт о квантовом распределении ключей. Т.е. о способе безопасного обмена ключами для их использования стандартным образом на существующих публичных сетях передачи данных.

Во втором – «светлое» будущее квантового Интернета (соединение квантовых компьютеров в «квантовый Интернет»). Последнее словосочетание закавычено намеренно. Всё-таки квантовые коммуникации подразумевают коммутацию каналов, а не пакетов при передаче данных от узла к узлу сети. Впрочем, термин «Интернет» сейчас живёт сам по себе, вне контекста сетей TCP/IP.

Квантовые коммуникации в теории и на практике

В чём суть применения квантовой коммуникации в «неспутанных» сетях? Суть в том, что клонировать неопределённое квантовое состояние нельзя [13]. Это так называемая теорема «О запрете клонирования». Но, в принципе, самоклонирование [14] возможно.

В квантовых коммуникациях речь идёт, главным образом, о фотонах, а точнее, об их поляризации (состояние кубита). Считается, что пока фотон не попал на детектор, его состояние (поляризация) неизвестно. В этом утверждении содержится сильное упрощение. Вообще говоря, состояние может быть известно, например, все фотоны в определённой поляризации (прошли через поляризатор). Неизвестен в общем случае результат измерения поляризации. Этот результат вероятностный, с вероятностями, которые зависят от состояния фотона и типа измерения (например, на какую ось измеряем поляризацию [см. панель «Квантовые измерения»]).

Кроме того, фотон – это квант, т.е. он неделим. Из этого следует, что если фотон попадёт на детектор, то он поглотится, и второго такого фотона не будет. Т.е. посмотреть на такой фотон можно только один раз.

Собственно, идея построения защищённого канала передачи данных состоит в том, что между источником и легальным детектором нельзя незаметно «воткнуть» ещё один детектор.

Вообще говоря, тут есть множество сложностей. Во-первых, фотон – это не только частица, но и волна. Измеряется как частица — где стукнул, там и вспышка на экране, — но если много фотонов, то становится видно, что вероятность стукнуть имеет волновую картину.

Т.е. когда говорят о поляризации, то имеют в виду поляризацию волны. [см. панель «Дуализм волна/частица»]

Во-вторых, речь идёт о вероятностях состояний, т.е. всё очень «нечётко», ну, и, в-третьих, существует такое понятие, как «слабые измерения» [15], т.е. теоретически «подсмотреть» квантовое состояние можно, но очень осторожно. Тут проявляется что-то типа закона сохранения — «чем лучше подсмотришь, тем больше разрушишь».

Решение о наличии или отсутствии стороннего наблюдателя на канале связи принимается на основе статистики наблюдения за этим каналом, т.е. вероятность того, что ключ скомпрометирован, хоть и не равна 0, но достаточно мала.

Расстояние, на которое можно передать фотон по оптической линии связи, невелико. Это значит, что нужны доверенные узлы усиления — репитеры. Например, на наземной линии «Пекин-Шанхай» (Beijing-Shanghai Backbone Network — information security expressway) [16] установлено 32 репитера. Квантовый репитер (квантовый усилитель) – «устройство, в котором усиление электромагнитной волны происходит в

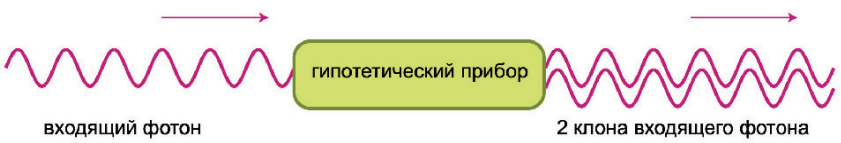
Панель «Невозможность квантового клонирования»

Клонирование подразумевает прибор, который создаёт как минимум две точные копии для любого квантового состояния входящего фотона (например, его поляризации). Ясно, что создав множество копий, можно использовать часть из них для скрытого перехвата сообщений. Менее очевидно, но гораздо более радикально то, что клонирование одного из пары запутанных фотонов [панель «Запутанные состояния»] позволило бы передавать информацию со сверхсветовой скоростью. Для этого отправитель А должен провести измерение поляризации не клонированного фотона до того, как второй фотон долетит до клонирования. Тогда клонируемые фотоны окажутся в определённом квантовом состоянии и статистика их измерений будет зависеть от измерения, проведённого отправителем, как и на панели «Квантовая линия связи». Таким образом, выбирая тип измерения, А может передать информацию Б быстрее скорости света. Идея доказательства невозможности клонирования основана на линейности квантовой механики. Клонирование возможно для заранее оговорённых базовых состояний, например, для вертикальной и горизонтальной поляризации. Соответствующая трансформация базовых состояний определяет результат действия прибора на любые состояния, однако получающиеся состояния не совпадают с требуемыми для описания двух тождественных фотонов.

Подробнее об этом:

Wootters, William; Zurek, Wojciech (1982). A Single Quantum Cannot be Cloned. Nature. 299 (5886): 802–803. Bibcode:1982Natur.299..802W. doi:10.1038/299802a0. S2CID 4339227

Dieks, Dennis (1982). Communication by EPR devices. Physics Letters A. 92 (6): 271–272. Bibcode:1982PhLA...92..271D. CiteSeerX 10.1.1.654.7183. doi:10.1016/0375-9601(82)90084-6. hdl:1874/16932



Невозможность квантового клонирования.

результате её взаимодействия с активной средой, испускающей фотоны с той же частотой, поляризацией и фазой, в том же направлении, что и усиливаемая волна.

Вообще говоря, квантовые репитеры в экспериментах китайских физиков несколько более сложные, чем описано выше. В них используются «спутанные» фотоны [17] и, соответственно, эффект «квантовой телепортации». И следует здесь также заметить, что «усиление» (фотон в нужном состоянии) происходило в 80% случаев, что считается очень неплохим результатом. В любом случае, практическая польза квантовых репитеров ограничена временем хранения фотона и эффективностью извлечения.

Тем не менее, именно на таких сетях реализован обмен секретами (ключами), которые затем используются для обычного шифрования сообщений в сетях связи общего назначения.

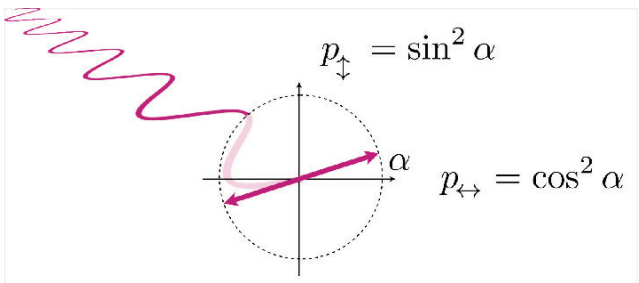
В «спутанных» сетях всё гораздо интереснее. К слову сказать, вторая часть китайского проекта – квантовая сеть с использованием спутника – это уже о «спутанных» сетях, хотя всё ещё речь идёт о безопасном обмене ключами.

Панель «Принцип локальности»

Принцип локальности в физике утверждает, что взаимодействия передаются через непосредственное окружение. Это выполняется повсеместно, от столкновений звёзд или приводных валов в автомобиле и до квантовых взаимодействий через электромагнитные и другие поля. Вся теория относительности построена на существовании максимальной скорости передачи информации – скорости света. Запутанные состояния возродили, однако, интерес к фундаментальному принципу и его экспериментальной проверке. Причина в кажущемся нарушении локальности, когда оба адресата узнают взаимно о результатах измерения, будучи разделены большим расстоянием. Выполненные до сих пор эксперименты указывают, однако, на выполнение классической интерпретации квантовой механики — она просто предсказывает вероятности измерений. В частности, вероятность получить два «иня» или два «яна» [22] [см. панель «Запутанные состояния»] равна нулю.

Панель «Квантовые измерения»

Квантовое измерение на примере поляризации фотона как поперечной электромагнитной волны. Верхняя часть рисунка: поляризация определяется углом наклона колебаний в плоскости, ортогональной направлению распространения волны. В нашем макроскопическом мире этот угол можно «увидеть» и измерить. В квантовом мире «увидеть» фотон нечем. Можно только устроить измерение проекций поляризации на произвольно выбранные оси, например, горизонтальную или вертикальную — с помощью поляризатора (нижняя часть рисунка). По основным законам квантовой механики в результате всегда получается одна из выбранных поляризаций (это похоже на знаменитый эксперимент Штерна — Герлаха). Только набрав статистику, мы увидим, что угол наклона проявляется как вероятности измерения горизонтальной и вертикальной оси. Заметим, что только угадав истинную поляризацию, мы будем получать однозначный ответ, например, можно подстроить оси так, чтобы угол наклона был равен нулю.



Квантовые измерения.

Спутанные кванты (фотоны) обладают взаимосвязанными свойствами, например, поляризацией в перпендикулярных плоскостях. Если такие частицы разнести на «приличное» расстояние, то при детектировании состояния одной из них можно «мгновенно» получить представление о состоянии другой.

Главное во всей этой истории – это нарушение «принципа локальности» [18], т.е. воздействие на одну частицу «мгновенно» (возможно, быстрее скорости света) передаётся на партнёра по «спутанности». Тут есть очень тонкий момент: информация быстрее света не распространяется. Можно мгновенно узнать, что там у партнёра, но нельзя ему передать ещё какую-нибудь дополнительную информацию. То есть фактически третье лицо кидает чёрный и белый шар, один одному адресату, а второй его партнёру по паре. Кто что получил, выясняется, когда каждый открывает свою посылку. Но это не ещё не передача информации между ними быстрее света. [см. панель «Запутанные состояния»]

Это значит, что если бы на советской космической станции «Фобос-1» [19] было бы хранилище спутанных с оставшимися на земле фотонов, то можно было бы быстро поправить ошибку программного обеспечения, и, возможно, экспедиция завершилась бы успешно.

В ранее упомянутом RFC 9340 все рассуждения по поводу сети квантовых компьютеров строятся вокруг как раз эффекта «спутанности» и так называемой квантовой телепортации, т.е. нарушения принципа локальности.

Так, рабочая группа в качестве одного из важнейших следствий реализации квантовых коммуникаций в рамках сети квантовых компьютеров называет возможность построения пространственно распределённого компьютера, ведь изменение состояния кубитов будет происходить мгновенно.

Будет или не будет – это вопрос будущего, а пока китайцы к 2022 году вывели на орбиту два спутника (первый — в 2016 году [20]). Через эти спутники должен осуществляться обмен ключами для организации безопасного информационного обмена по обычным линиям связи. Именно этому факту в основном посвящены публикации в научно-популярной литературе, например, в 3DNews.ru [21]. Однако сами авторы проекта

бОльшее внимание уделяют фундаментальному значению доказательства нарушения принципа локальности.

На спутнике размещён источник спутанных фотонов, которые принимают две китайские обсерватории, разделённые между собой расстоянием в 1203 км. Если принимать во внимание расстояние между площадками измерений через спутник, то оно варьируется от 1600 до 2400 км (зависит от положения спутника относительно этих площадок).

Китайские учёные исследовали нарушение неравенства Белла [23] и получили впечатляющие результаты, которые говорят о том, что принцип локальности нарушается. Это в свою очередь открывает «новый путь» («new avenue to both practical quantum communications and fundamental quantum optics experiments») для обмена криптографическими ключами и не только. В работе упоминается «протокол квантовой телепортации» (quantum teleportation protocol) [24], который предполагает использовать принцип спутанности для передачи данных в квантовых сетях. Правда, и здесь всё сосредоточено на измерениях нарушения неравенства Белла.

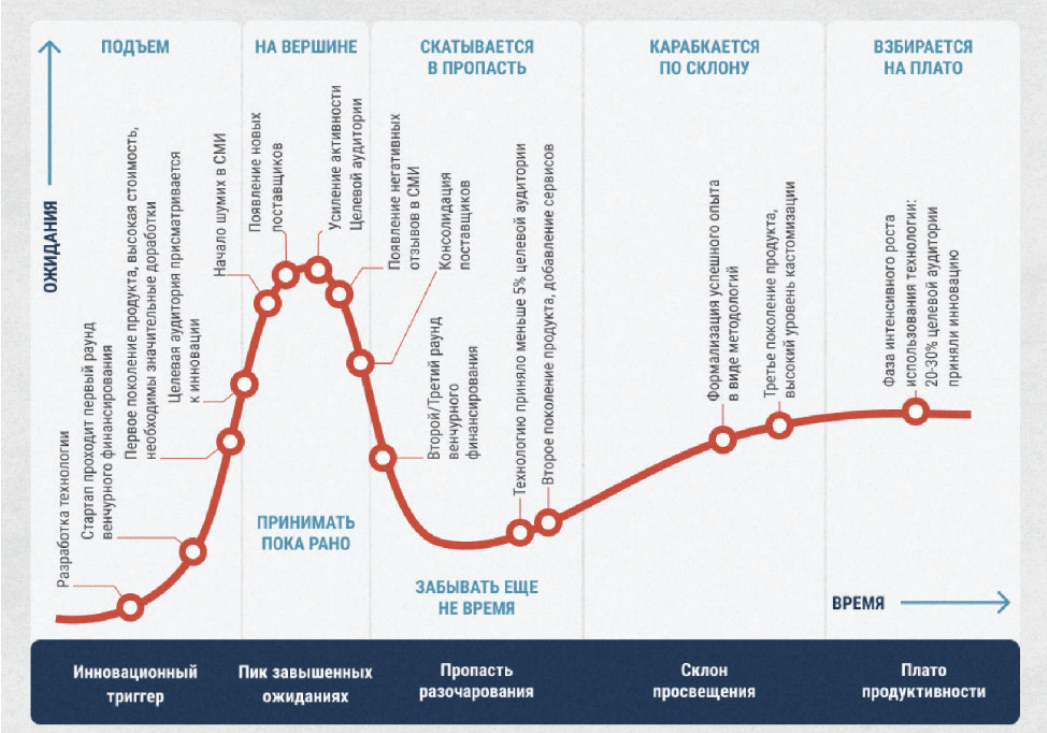


Рис. 2. Кривая зрелости технологии Гартнера [28].

Вся кривая на графике Гартнера [27] разделена на несколько периодов: технологический триггер, пик популярности, разочарование, просвещение и плато продуктивности.

Кривая призвана ориентировать инвестора по поводу того, когда пора вкладывать деньги. Рекомендовано вкладывать на периоде просвещения, чтобы максимизировать прибыль. Но периоды могут быть короткими, и можно пропустить момент (рис. 2).

Для определения места квантовых коммуникаций на этой кривой нужно определить вехи развития от идеи и теории к технологии. И определить их можно таким образом:

- V Сольвеевский конгресс (1927) «Электроны и фотоны» — Альберт Энштейн – *Бог не играет в кости.* Нильс Бор — *Эйнштейн, не указывай Богу, что ему делать [29].*
- В 1964 году Джон Белл получил новый и неожиданный для многих теоретический результат. Он доказал, что можно провести определенный эксперимент (подробности чуть позже), результаты которого позволят определить, действительно ли квантово-механические объекты описываются волновыми функциями распределения вероятностей, как они есть, или же имеется скрытый параметр, позволяющий точно описать их положение и импульс, как у ньютоновского шарика.
- Ален Аспен доказал нарушение неравенства Белла в 1982 году.
- В этом же году была сформулирована теорема о запрете клонирования.
- В 2006 году был сформулирован принцип слабых измерений.
- Эксперименты по практической реализации квантового распределения ключей на реально больших расстояниях китайцы начали в 2016.
- Нобелевскую премию по физике за обнаружение и доказательство неравенства Белла дали в 2022 году, т.е. произошло осознание масштабности вопроса.

Вместо заключения

Не только Китай занимается исследованиями в рамках квантовых коммуникаций. Европейский союз также проявляет интерес к такого сорта исследованиям. Евросоюз в рамках разработки EuroQCI (The European Quantum Communication Infrastructure Initiative) финансирует следующие проекты:

QIA – Quantum Internet Alliance [25] – разработка проекта общеевропейского квантового Интернета, основанного на запутанности, путем разработки, интеграции и демонстрации всех функциональных аппаратных и программных средств;

QSNP – Quantum Secure Networks Partnership [26] – создание устойчивой европейской экосистемы в области квантовой криптографии и связи.

В общем, если коротко, то китайцы ставят опыты и стараются превратить теорию в реальность, а европейцы пишут проспекты проектов, выделяя на это немалые деньги.

Встает резонный вопрос – насколько близко к широкому практическому внедрению находится данная технология?

Здесь мы снова вернёмся к маркетингу. А точнее, к с-образной кривой «хайпа» Гартнера, или, как ее еще называют, кривой зрелости технологии.

Сейчас у нас идет 2024 год. Два года назад китайцы запустил второй спутник, который должен решить проблему передачи данных при свете Солнца (звучит странно, но тем не менее).

Ведутся работы по конструированию источников одиночных фотонов, квантовых репитеров, детекторов и прочих «необходимых в квантовом хозяйстве» устройств.

В популярных изданиях появляются публикации о том, что «интегральные источники одиночных фотонов стали в десять раз ярче» [30], т.е. частота генерации фотонов увеличилась.

В общем, похоже, что популярность темы растёт. На кривой «хайпа» мы находимся, видимо, сразу за зоной инновационного триггера или во второй половине этой зоны. Первые версии продукта уже есть, появляются новые поставщики (свои отечественные, а не китайские).

Существует ещё один наглядный механизм для определения места инновации (новой технологии) на кривой внедрения – это s-образная кривая внедрения инновации Эверета Роджерса [31] (см. рис. 3).

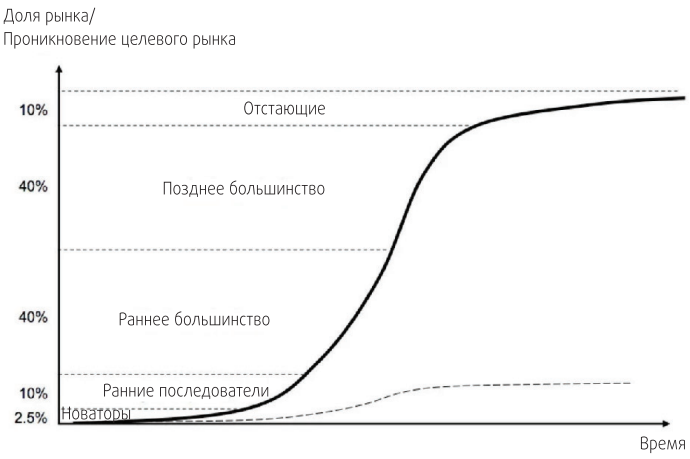


Рис. 3. S-кривая внедрения инновации Роджерса.

На этой кривой квантовые коммуникации находятся в зоне «Ранние последователи», т.е. зону новаторов (изобретателей) технология уже прошла. Первые образцы техники получены и начато ее внедрение. Но это ещё не нарастающий поток внедрений, а только самое начало – где-то ещё на грани опытов с публикациями результатов в научных журналах.

Таким образом, текущее состояние – это исследовательские и опытно-конструкторские разработки в узком диапазоне применения.

К слову сказать, притча [32] об отделении «зёрен от плевел» не предполагает экономности в тратах на исследования. Она предлагает дождаться результатов трудов.

Да, и алгоритмы пост квантовой криптографии уже существуют, если что...

Об авторах:

Киселёв Валерий Геннадьевич, профессор, Германия
Храмцов Павел Брониславович, к.т.н., доцент, научный руководитель проектов Фонда «ИнДата».

Список литературы:

[1] https://lenr-canr.org/wordpress/?page_id=2130
[2] https://protect.gost.ru/v.aspx?control=8&baseC=6&page=3&month=7&year=2023&search=&RegNum=1&DocOnPageCount=15&id=242097&pageK=BA9F9094-90B4-4365-8BDE-41BC866115DA
[3] https://protect.gost.ru/v.aspx?control=8&baseC=6&page=3&month=7&year=2023&search=&RegNum=1&DocOnPageCount=15&id=242098&pageK=88629057-99B7-4676-8705-B357183591B8
[4] https://fantlab.ru/work30920
[5] https://fantlab.ru/work3267
[6] https://www.labirint.ru/books/263732
[7] https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-QIT4N-2021-D1.1-PDF-E.pdf
[8] https://datatracker.ietf.org
[9] https://www.ietf.org
[10] https://datatracker.ietf.org/group/qirg/about
[11] https://datatracker.ietf.org/doc/rfc9340
[12] https://www.ietf.org/live/previous/live104/ietf104-qirg
[13] https://www.nature.com/articles/299802a0
[14] https://cyberleninka.ru/article/n/kvantovoe-samoklonirovanie
[15] https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.60.1351
[16] https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml
[17] https://www.nature.com/articles/s41586-021-03481-8
[18] https://www.mathnet.ru/links/f6b99653e39fe10e1a576841ff4b6274/tmf6215.pdf
[19] https://rgantd.ru/arh-docs/cosmos/k-yubileyu-zapuskov-ams-fobos-1-i-fobos-2
[20] https://www.science.org/doi/10.1126/science.aan3211
[21] https://3dnews.ru/1071045/kitay-zapustil-sputnik-kvantovoy-svyazi-novogo-pokoleniya-eto-perviy-shag-k-razvyortivaniyu-globalnoy-zashchishchyonnoy-seti
[22] Единая изначальная материя тайцзи порождает две противоположные субстанции — ян и инь, которые едины и неделимы.
[23] https://matan.math.msu.su/files/zorich/Bell's_inequality.pdf
[24] https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.80.1121
[25] https://qt.eu/projects/communication/qia
[26] https://qt.eu/projects/communication/qsnp
[27] https://trends.rbc.ru/trends/industry/64f833c29a794712449b13b2
[28] По материалам https://blog.bitobe.ru/article/krivaya-gartnera
[29] https://ru.wikipedia.org/wiki/Дискуссия_Бора_и_Эйнштейна
[30] https://nplus1.ru/news/2020/12/23/photon-source-on-chip
[31] https://books.google.ru/books?id=9U1K5LjUOwEC&pg=PR1&hl=ru&source=gbs_selected_pages&cad=1#v=onepage&q&f=false
[32] Евангелие от Матфея, Глава 13, стихи 24-30, https://radiovera.ru/rv_gospel/evangelie-ot-matfeja-glava-13-stihi-24-30

Дополнительная литература:

John Preskil, Lecture notes for physics 229, Quantum information and computation, http://theory.caltech.edu/~preskill/ph229

Nielsen-Chuang, Quantum Information and Quantum Computation, https://profmcruz.files.wordpress.com/2017/08/quantum-computation-and-quantum-information-nielsen-chuang.pdf

Килин С.Я., Квантовая информация, https://ufn.ru/ru/authors/1147/kilin-sergei-ya

Квантовое превосходство при решении вычислительных задач

Ханотел Пинзон Кристиан Луис

Аннотация

Создание квантовых компьютеров, обладающих огромным потенциалом как для развития науки, так и для улучшения качества жизни людей, представляет собой одну из наиболее важных научных и технологических задач нашего времени. В последние годы квантовая физика сделала удивительные открытия, которые обещают прорывные технологические изменения во многих практических областях, например, в метрологии, связи, вычислениях. В этой статье мы рассмотрим основные положения, которые важны для понимания принципов работы квантового компьютера, поговорим о достижениях в этой области и проблемах ближайшего будущего.

Ключевые слова:

квантовая физика, кубит, квантовый компьютер, квантовые алгоритмы, квантовое превосходство

За последнее столетие квантовая физика привела к революционным изменениям в человеческом понимании природы вокруг нас. Возникшая в начале прошлого столетия как научная теория для описания поведения микроскопических объектов и давшая ответы на многие вопросы, которые классическая физика не могла объяснить, в настоящее время квантовая физика используется для разработки и предсказания свойств новых материалов и является фундаментальным строительным блоком во многих практических приложениях, включая медицину (магнитно-резонансная томография, радиотерапия, позитронно-эмиссионная томография), ядерную энергетику, спинтронику. Лазеры и сверхпроводящие материалы, теория полупроводниковых материалов, объясняющая принцип работы транзистора, также разработаны на основе квантовой физики.

Все эти технологические разработки, возникшие на основе законов квантовой физики и относящиеся к периоду «первой квантовой революции», радикально изменили образ жизни человечества в рекордно короткие сроки. Никто и не предполагал, что открытия квантовой физики так изменят мир, в котором мы живём.

По мнению многих экспертов, на протяжении последних трёх десятилетий мир находится в процессе «второй квантовой революции» [1], поскольку на основе развития различных областей квантовой физики был сделан целый ряд открытий, которые могут полностью изменить нашу жизнь. Одним из направлений этой технологической революции является создание универсального квантового компьютера — компьютера, который работает на основе законов квантовой физики.

Но зачем нужны другие виды компьютеров, если те, что есть, работают достаточно хорошо? Как работают квантовые компьютеры? Чем они будут отличаться от уже привычных для нас компьютеров? Как квантовые компьютеры могут радикально изменить наш образ жизни? И реально ли их сконструировать?

Чтобы ответить на эти вопросы, необходимо задуматься о компьютерах, которые сейчас используются везде вокруг нас. Хотя они практически вездесущи, это не значит, что они совершенны, и, как мы покажем далее, создание квантового компьютера приведет к существенному прогрессу в области решения вычислительных задач.

Классические компьютеры

Компьютер — это устройство, позволяющее выполнять логические или арифметические операции на основе набора входных данных и серии инструкций. Примеры простейших «компьютеров» можно найти тысячи лет назад — например, таким простейшим компьютером являются счёты. В XVII веке появились первые сложные механические калькуляторы, среди них знаменитая «Паскалина». В течение XX века с развитием компьютеров произошёл потрясающий прогресс в количестве и сложности операций, которые мы можем выполнять с их помощью. Это развитие привело нас к тому, что компьютеры в современном мире распространены практически повсеместно.

Для работы любого компьютера требуется запоминающее устройство, в котором информация может передаваться машине. Основная ячейка памяти называется битом (от английского «binary digit» — двоичная единица информации), в бинарной системе исчисления бит принимает два значения: 0 и 1. Когда мы набираем текст на клавиатуре компьютера, каждое слово кодируется двоичной последовательностью. Обычно эти двоичные последовательности очень велики по длине, поэтому принято определять более крупные единицы хранения информации, такие как байты (8 бит), килобайты (1024 байта) или гигабайты (1 073 741 824 байта). Для хранения электронного письма размером около 5 килобайт требуется более 40 000 битов!

Когда у нас есть блоки памяти, в которых мы можем передавать информацию компьютеру, необходимо иметь элементы, позволяющие нам обрабатывать эту информацию и выполнять на ней алгоритмы — последовательности конкретных инструкций для решения заданной задачи. Нам также понадобится блок чтения, позволяющий извлекать информацию, полученную в результате выполнения алгоритма. Существует несколько способов создания машины с такими характеристиками, и все они эквивалентны машине Тьюринга — теоретической модели, предложенной Аланом Тьюрингом в 1936 году [2].

Среди различных теоретических моделей вычисления есть схемная модель, в которой вычисления символически представлены с помощью «проводов», передающих информацию, и последовательности логических элементов (вентилей), обрабатывающих эту информацию. Эта модель вычислений очень удобна благодаря своему структурному сходству с обычным компьютером, состоящим из сложных электрических схем. В классическом компьютере значения бита 0 и 1 соответствуют прохождению импульса электрического тока или его отсутствию.

В рамках схемной модели любая сложная вычислительная операция может быть представлена посредством последовательности действий простых логических операций (вентилей). Однобитовые логические элементы, например, логический элемент «NOT», преобразуют единицу (1) в ноль (0) и 0 в 1, что соответствует операции отрицания в математической логике. Другие вентили могут действовать над несколькими битами, например, вентиль ИЛИ («OR»), описанный в таблице 1.

Таблица 1.
Таблица истинности, связанная с логическим вентилем «OR»

a	b	OR(a,b)
0	0	0
0	1	1
1	0	1
1	1	1

Например, с помощью элементов «NOT» и «OR» можно построить следующую схему (см. рис. 1), в которой «NOT» сначала применяется к первому биту, а затем элемент «OR» применяется к полученной паре битов, создавая таким образом новую операцию (см. таблицу 2).

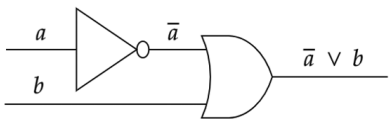


Рис. 1. Диаграммное изображение схемы, описанной выше. Для каждой из элементарных логических операций существуют свои символы.

Таблица 2. Таблица истинности, связанная с логическим вентилем, описанным на рис. 1.

a	b	OR(NOT(a),b)
0	0	1
0	1	1
1	0	0
1	1	1

Как видим, на основе последовательности простых операций мы можем разрабатывать схемы сложных вычислительных алгоритмов. В привычных для нас компьютерах логические элементы реализуются физически посредством электронных схем, состоящих из транзисторов, которые, как мы упоминали ранее, представляют собой одно из величайших достижений, созданных на основе законов квантовой физики. Согласно мнению авторов монографии [3, с.1], то, что мы сегодня живём в век информационных технологий, основано на развитии различных областей квантовой теории и синергии квантовой теории и информатики.

Сложность и количество задач, которые может решить компьютер, зависят от количества имеющихся у него транзисторов (и для конкретной задачи хороший алгоритм часто оказывается эффективнее мощной машины). В 1965 году Гордон Мур, сооснователь компании Intel, наблюдал экспоненциальный рост количества электронных компонентов в микропроцессоре и предсказал его примерное удвоение каждый год. Заметив, что этот процесс оказался менее быстрым, чем ожидалось, он скорректировал свой прогноз на каждые два года. Это предсказание известно как «закон» Мура [4]. На основе этого «закона» было верно предсказано, что за 50 лет будет пройден путь от нескольких тысяч транзисторов в микропроцессоре до сотен миллиардов, что мы сейчас и имеем.

Столь впечатляющее увеличение количества транзисторов на единицу площади стало возможным благодаря миниатюризации транзисторов: первые имели размер несколько сантиметров, а нынешние — несколько нанометров (нанометр — это одна миллионная часть миллиметра). Это также объясняет, как стало возможным обрабатывать всё возрастающие объёмы информации.

Однако эта история не может продолжаться бесконечно. Продвигаться в процессе миниатюризации становится все труднее, особенно потому, что в достигнутых нами масштабах квантовые эффекты начинают иметь большее значение. Потребности в обработке информации продолжают расти, требуя всё большего числа компьютеров большей мощности. И если невозможно удовлетворить эти потребности с помощью существующей у нас парадигмы, возможно, мы найдём решение, изменив парадигму и предложив компьютер, который, хотя и сильно отличается от известных нам компьютеров, обладает способностью удовлетворять потребности требуемой эффективности.

Решение этой проблемы необходимо не только по научным или экономическим причинам, но и по экологическим: необходимо срочно сократить загрязняющие выбросы, связанные с обработкой, хранением и передачей информации. И на основе квантовой физики есть предложения по решению этой проблемы.

Квантовые компьютеры

Впервые идея развития квантовых вычислений и создания квантового компьютера была высказана Юрием Маниным в 1980 году. В 1981 году нобелевский лауреат по физике Ричард Фейнман (Richard Feynman) выдвинул идею о том, что компьютер, основанный на правилах квантовой механики,

идеально подойдёт для моделирования физических систем. По его мнению, если квантовая физика является правильной теорией для описания природных явлений, то моделирование реального мира потребует решения уравнений квантовой механики, которая на сегодняшний день является теорией, дающей лучшие экспериментальные результаты в истории человечества!

Согласно квантовой механике, динамика поведения изолированной квантовой системы описывается нестационарным уравнением Шрёдингера — дифференциальным уравнением, которое можно решить с помощью классического компьютера только в случае составной системы из небольшого числа частиц. В случае решения данной задачи для макроскопической системы, состоящей из миллиона частиц, требуется значительное увеличение вычислительных возможностей классического компьютера, что представляется проблематичным в силу необходимости существенной миниатюризации для этого его основных компонент.

Однако, как отметил Фейнман, альтернатива всё же есть: разработать вычислительную машину, которая, в отличие от классических компьютеров, работала бы на основе законов квантовой механики. В 1980-х годах было несколько попыток построить модели машин с такими характеристиками. Например, квантовая модель машины Тьюринга, предложенная Полом Бениоффом (Paul Benioff) [5]. Хотя эта модель квантового компьютера и не увенчалась успехом, на этом примере было показано, что информация может быть закодирована на основе использования физических свойств квантовых систем. Спустя годы сам Фейнман и Дэвид Дойч (David Deutsch) разработали более надёжные модели, составляющие основу теории квантовых вычислений.

Для того чтобы понять новые аспекты, привнесённые в технику вычислений квантовыми компьютерами, важно упомянуть некоторые фундаментальные положения квантовой механики, которые противоречат нашей интуиции — во многом потому, что наша интуиция формируется посредством нашего макроскопического восприятия таких вещей как, например, суперпозиция и запутанность состояний квантовых систем, дискретизация значений физических величин, описывающих такие системы.

Квантовая суперпозиция позволяет квантовой системе находиться одновременно в произвольной комбинации разных состояний в разных положениях. Такое свойство состояний квантовой системы способствует параллельной обработке информации при квантовых вычислениях.

При квантовых вычислениях роль, аналогичную битам, играют кубиты (квантовые биты), которые помимо квантовых состояний, являющихся аналогами состояний бита «0» и «1» и обозначаемых, как |0> и |1>, могут находиться в любой их суперпозиции. Существует много способов физической реализации кубитов — на основе сверхпроводников, одиночных холодных атомов, ультра-холодных атомов в оптических решётках, ионов в ловушке, на основе фотонных чипов и интегральной оптики.

В квантовых вычислениях логические элементы представлены квантовыми вентилями, которые управляют кубитами. Таким образом, физически квантовый компьютер реализуется как система кубитов, эволюционирующая с течением времени контролируемым образом.

На основе указанных выше свойств первые алгоритмы для решения различных вычислительных задач на квантовом компьютере были предложены в конце прошлого столетия. Но, пожалуй, самый важный из алгоритмов появился в 1994 году, когда Питер Шор (Peter Shor) разработал квантовый алгоритм разложения (факторизации) на простые множители произвольного целого положительного числа [6].

Любое целое положительное число может быть единственным образом представлено в виде произведения его простых множителей. Зная простые множители некоторого числа, легко получить его значение путём их перемножения. Но обратный процесс, то есть разложение числа на простые множители, особенно в случае очень больших чисел, сложен и занимает на классических компьютерах очень много времени. Многие криптографические протоколы основаны именно на сложности решения этой задачи на обычном компьютере.

Алгоритм Шора показал, что создание полномасштабного (large-scale) квантового компьютера может поставить под угрозу конфиденциальность передаваемой информации, что вызывает глубокий интерес к его разработке как на уровне отдельных частных компаний, так и на уровне государственных организаций в разных странах мира.

Эта серия важных теоретических находок привела к необходимости построения реального квантового компьютера. Но был ли построен квантовый компьютер?

Настоящее и будущее квантовых компьютеров

Ответ на предыдущий вопрос зависит от «размера» компьютера: исследователи научились управлять системами из нескольких кубитов (используя при этом дорогие системы охлаждения и сложные экспериментальные установки), но ещё далеко до эффективного управления системами из большого числа кубитов, поскольку время жизни их состояний составляет только несколько микросекунд. Современные квантовые компьютеры имеют порядка несколько десятков или сотен кубитов, и этого достаточно для тестироваия простых квантовых алгоритмов. В конце прошлого года IBM объявила о создании квантового процессора с более чем 1000 кубитами [7].

Это правда, что квантовые компьютеры превратились из устройств в лабораториях университетов и крупных технологических компаний в реальность в различных отраслях промышленности. Существуют авиакомпании, заинтересованные в использовании квантовых компьютеров для решения сложных логистических задач [8], или даже компании, которые стремятся закодировать геном на основе квантовых алгоритмов [9]. Это первые шаги, которые позволяют рассматривать квантовые вычисления как интегрирующий элемент современных технологий и с большими надеждами на будущее: ожидается высокий рост в этой области, и это

повлечет за собой разработку новых практических приложений, например, в аэрокосмическом секторе, в области искусственного интеллекта или массовой обработки данных.

В 2019 году было продемонстрировано превосходство [10] квантового компьютера при решении вычислительной задачи, на решение которой на классическом компьютере ушли бы годы — на квантовом компьютере данная задача была решена за считанные минуты. В дальнейшем квантовое превосходство при решении вычислительных задач было продемонстрировано на разных квантовых компьютерах и в разных странах, и является в настоящее время общепризнанным. По мнению некоторых учёных, этот факт является проявлением того, что мы живём во времена «второй квантовой революции».

Последние пять лет ознаменовались значительными успехами в разработке квантовых процессоров (см. рис. 2). Университеты и компании из разных стран продвигаются вперед семимильными шагами: в 2019 году Google достигает квантового превосходства с компьютером Sycamore, состоящим из 54 кубитов, в 2020 году IBM разрабатывает свою знаменитую дорожную карту Quantum Roadmap, в 2021 году начинается бум компаний, занимающихся коммерческой разработкой квантовых компьютеров, таких как IONQ, Honeywell и Xanadu (последняя также продемонстрирует квантовое превосходство, но с компьютером, работающим с фотонами, в отличие от компьютера Sycamore от Google IA, основанного на сверхпроводниках). В конце прошлого года был запущен IBM Condor, 1121-кубитный квантовый процессор, уступивший по количеству кубитов только 1125-кубитному квантовому процессору Atom.

Одним из примеров таких компаний, заслуживающих внимания, является D-Wave. В настоящее время она производит процессоры на основе сверхпроводников с архитектурой до 5000 кубитов, что ставит её в ряд ведущих компаний на этом рынке. Следует отметить, что это не универсальный компьютер, а компьютер, предназначенный для конкретных задач и работающий по технологии, называемой квантовым отжигом, поэтому опять же количество кубитов является вводящим в заблуждение параметром. Например, у IBM Condor 1121 кубит, но это компьютер общего назначения.

Сравнивать существующие квантовые компьютеры сложно, поскольку количество кубитов — не единственный фактор, который нужно учитывать. Качество и средний срок их службы также имеют значение. Например, квантовый процессор в Университете науки и технологий Китая представляет собой 100-кубитный процессор на основе фотонов, а у канадской компании Xanadu есть процессор на основе фотонов с еще большим количеством кубитов (128!). Однако он обладает меньшей вычислительной мощностью, чем китайский 100-кубитный процессор, поскольку его кубиты менее стабильны. Что касается квантовых процессоров, работающих на ионах, то в настоящее время рекорд принадлежит процессору компании IONQ с 35 алгоритмическими кубитами.

В Российской Федерации существует большой интерес к развитию теории квантовых вычислений и разработке квантовых технологий. Не только за счёт исследований, но и за

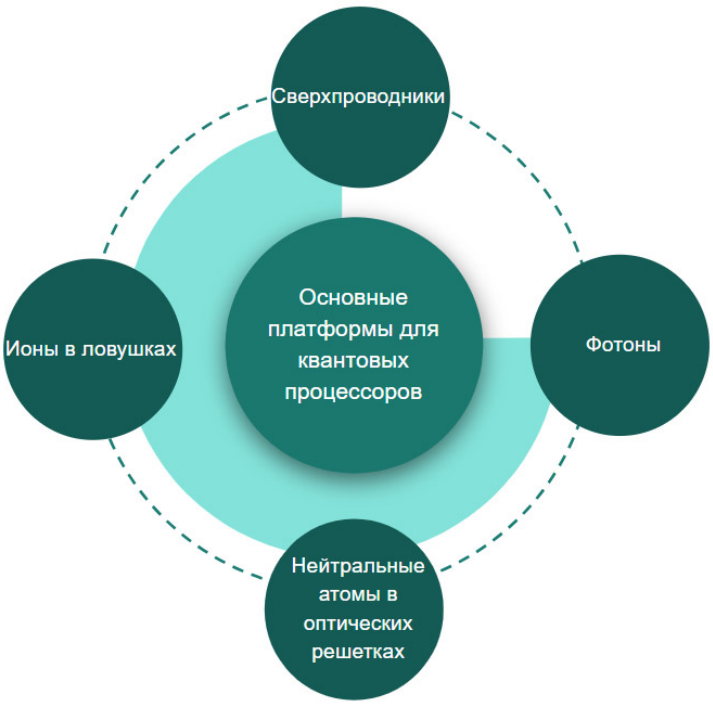


Рис. 2. Основные платформы для квантовых процессоров.

счёт консолидации компаний этого сектора. Крупные компании, такие как «Росатом», также проявили интерес к разработке квантовых компьютеров, инвестировав в эту область 24 миллиарда рублей [11]. В начале 2024 года в России был запущен первый квантовый компьютер в МФТИ [12].

С академической точки зрения существует давняя традиция исследований, отражённая в бесчисленных статьях и работах по этой теме. В рамках этих проектов можно отметить работу, проводимую в Московском институте электроники и математики им. А.Н. Тихонова НИУ ВШЭ. В рамках курса «Квантовые вычисления» студенты департамента прикладной математики приобретают навыки моделирования на квантовых процессорах, изучают основные квантовые алгоритмы и квантовые криптографические протоколы, решают на основе этого различные вычислительные задачи, исследуют также различные методы количественного определения квантовых корреляций, которые могут стать одним из фундаментальных ресурсов в задачах обработки квантовой информации.

Квантовые компьютеры как решение в борьбе с изменением климата?

В настоящее время одной из крупнейших проблем, стоящих перед человечеством, является изменение климата, вызванное глобальным потеплением. Причиной этого во многом являются чрезмерные выбросы парниковых газов в атмосферу. И многие из этих выбросов тесно связаны с использованием компьютеров: они работают на электричестве, а производство этой электроэнергии оказывает воздействие на окружающую среду.

Но так ли серьёзна проблема энергопотребления компьютеров по сравнению с автомобилями или крупными предприятиями? Эта проблема не такого же масштаба, но мы не можем сказать, что она второстепенна. Мы можем увидеть это на примере Исландии — страны с одним из самых высоких потреблений энергии на душу населения в мире. Это страна, где потребление энергии, связанное с работой компьютеров, уже превысило потребление электроэнергии в домах. Почему в такой маленькой стране, как Исландия, такое высокое потребление энергии, особенно в этом секторе? Это связано с тем, что большая часть этой энергии используется для охлаждения серверов. Крупные компании предпочитают холодные места, чтобы снизить затраты на охлаждение. Другие идеи, например, те, что изучает Microsoft, заключаются в использовании морского дна для охлаждения, но есть опасность, что это будет иметь серьёзные негативные последствия для окружающей среды.

Тревожным фактором является то, что потребление энергии, связанное с вычислительными операциями, растёт. Растёт необходимость обрабатывать, хранить и передавать всё больше информации, при этом мощность компьютеров не возрастает (закон Мура не может работать вечно!).

Одним из примеров, демонстрирующих рост потребления энергии за счет вычислительных операций, являются криптовалюты, самой популярной из которых является биткоин. Транзакция с этой криптовалютой, в отличие от обычной банковской операции, не зависит от центрального органа (банка), который одобряет транзакцию. В системе биткоина такая децентрализация подразумевает, что транзакция проверяется несколькими пользователями сети, что влечет за собой огромные затраты энергии, особенно потому, что дизайн этой серии проверок неэффективен. Потребление энергии, связанное с криптовалютами, в настоящее время эквивалентно годовому потреблению средней страны, такой как Аргентина или Таиланд, поэтому эту ситуацию следует принимать во внимание. Если бы биткоин был страной, он бы вошёл в список 30 самых энергозатратных стран!

Многие процессы на банковском уровне, логистические процессы крупных производств и моделирование различных явлений включают в себя вычислительные операции, которые, если бы их можно было решить быстро и эффективно, позволили бы снизить потребление энергии. Таким образом, функциональный квантовый компьютер может стать отличным союзником в борьбе с изменением климата. Хотя текущие разработки в области квантовых компьютеров используют дорогие системы охлаждения и сложные дорогостоящие материалы, считается, что достаточно эффективный компьютер может снизить затраты в долгосрочной перспективе: чем выше эффективность, тем меньше энергетических ресурсов ему потребуется для решения той же задачи. Задача, которая могла бы сделать квантовый компьютер доступным с экономической точки зрения и желательным с экологической точки зрения.

Создание квантовых компьютеров — сложный и дорогостоящий процесс, который сталкивается со многими проблемами на экспериментальном уровне. Например, нынешние модели постоянно требуют очень низких температур, что увеличивает затраты на эксплуатацию этих устройств. В ближайшем будущем квантовые компьютеры не будут стремиться заменить обычные компьютеры в домашних условиях, а будут использоваться в определенных стратегических отраслях, требующих больших вычислительных ресурсов, заменяя нынешние суперкомпьютеры. Для задач, решаемых в домашних условиях, необходимости в квантовых вычислениях пока нет.

Как мы видим, несмотря на большие успехи последних лет, в развитии квантовых компьютеров еще предстоит пройти долгий путь, особенно в построении хорошо управляемых моделей и упрощении существующих из-за хрупкости кубитов. В настоящее время мы наблюдаем процесс зарождения «второй квантовой революции», и, возможно, то, как она изменит нашу жизнь, находится за пределами нашего воображения!

Список литературы:

[1] Deutsch, I. H. Harnessing the power of the second quantum revolution. PRX Quantum, 1(2), 020101 (2020)

[2] Turing, A. M. On computable numbers, with an application to the Entscheidungsproblem. J. of Math, 58(345-363), 5 (1936)

[3] Benenti, G., Casati, G., Rossini, D., & Strini, G. Principles of quantum computation and information: a comprehensive textbook. World Scientific (2019)

[4] Moore, G. E. Cramming more components onto integrated circuits. Proceedings of the IEEE, 86(1), 82-85 (1998)

[5] Benioff, P. Quantum mechanical models of Turing machines that dissipate no energy. Physical Review Letters, 48(23), 1581 (1982)

[6] Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE (1994)

[7] Castelvecchi, D. IBM releases first-ever 1000-qubit quantum chip. December 2023. [Online] Available at: https://www.nature.com/articles/d41586-023-03854-1 (Consulted March 6th, 2024)

[8] Dawton, E. How Quantum Computing is Helping the Aviation Industry. July, 2023. [Online] Available at: https://medium.com/@eldawton/how-quantum-computing-is-helping-the-aviation-industry-cea8295e6db7 (Consulted March 7th, 2024)

[9] Boev, A. S. et al. Genome assembly using quantum and quantum-inspired annealing. Scientific Reports, 11(1), 13183 (2021)

[10] Arute, F. et al. Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510 (2019)

[11] Алексенко, А. В России решили создать квантовый компьютер за 24 млрд рублей. November, 2019. [Online] Available at: https://www.forbes.ru/tehnologii/386847-v-rossii-reshili-sozdat-kvantovyy-kompyuter-za-24-mlrd-rubley (Consulted March 7th, 2024)

[12] Российский 12-кубитный квантовый компьютер впервые применили для обучения нейросетей. January, 2024. [Online] Available at: https://nauka.tass.ru/nauka/19758569 (Consulted March 7th, 2024)

Об авторе:

Ханотел Пинзон Кристиан Луис, Ph.D. Scopus AuthorID: 57215610221, ResearcherID: GSN-0590-2022.
Научный сотрудник - МИЭМ НИУ-ВШЭ, Россия, г. Москва.

Квантовые коммуникации через атмосферные (космические) каналы связи

Андрей Деев, Александр Калинкин, Сергей Кулик, Александр Миллер, Иван Полухин

Аннотация

Квантовое распределение ключей – центральная технология квантовых коммуникаций, обеспечивающая принципиально новый уровень защиты информации. Особый интерес вызывает разработка систем квантово-защищенной связи для случаев, когда прокладывание оптического волокна затруднено или невозможно – на основе атмосферных (космических) каналов связи. В статье рассматриваются особенности квантовой связи на основе открытых атмосферных, включая космические, каналов коммуникаций, обсуждается текущее положение дел в указанных областях, а также перспективы развития квантовых коммуникаций.

Ключевые слова:

квантовые коммуникации, квантовое распределение ключей, открытые каналы передачи данных

Квантовые коммуникации

Квантовые коммуникации – это область знаний/техники о передаче квантовых состояний между удалёнными объектами. На основе разработок в этой области построены системы квантовой защиты информации (квантовой связи), предполагающие устойчивость как к классическим атакам, так и к атакам с использованием квантового компьютера. Наиболее развитой технологией квантовой защиты информации сегодня является квантовое распределение ключей.

Квантовое распределение ключей (КРК) позволяет двум абонентам создать общий и известный только им ключ, который абоненты могут использовать для шифрования и дешифрования сообщений уже общепринятыми классическими методами.

Для реализации КРК необходим квантовый канал связи, обладающий определёнными свойствами. Примером физической среды для построения квантового канала является сквозной оптоволоконный канал (т.н. тёмное волокно). Особый интерес вызывает разработка систем квантово-защищённой связи для случаев, когда прокладывание оптического волокна затруднено или невозможно – на основе атмосферных (космических) каналов связи. В этой области основное внимание исследователей в последние 10 лет сконцентрировано на следующих сценариях:

- КРК между мобильными и стационарными наземными или околоземными объектами;
- КРК между низкоорбитальными спутниками и наземными объектами;
- КРК между низко- и высокоорбитальными спутниками;
- создание глобальных квантовых сетей, охватывающих значительные территории.

Разработки в области КРК между мобильными и стационарными наземными или околоземными объектами принято относить к атмосферной квантовой связи, КРК между спутниками и наземными станциями – к космической квантовой связи, глобальные квантовые сети в свою очередь включают в себя несколько сегментов – «волоконно-оптические», «атмосферные» и «космические» – и являются общей перспективой развития квантовых коммуникаций.

Во всех перечисленных направлениях достигнуты определённые результаты, в основном, на уровне демонстрации возможностей [1-12].

Атмосферная квантовая связь

Построение глобальных сетей квантовых коммуникаций невозможно без подключения к защищённому доступу движущихся объектов (автомобиль, самолёт, корабль, беспилотный транспорт) и устройств Интернета вещей. Поскольку подключить магистральное оптоволокно для доставки квантовых ключей, например, к кораблю в порту, невозможно, то в качестве последней мили можно использовать оптическую беспроводную связь.

Атмосферная квантовая связь (АКС) является, по сути, квантовым распределением ключей между двумя наземными или околоземными объектами с помощью оптического излучения. Канал реализован через открытое атмосферное пространство и, с одной стороны, сочетает в себе преимущества КРК для достижения нового качества защиты передачи данных, а с другой – преимущества оптической беспроводной связи.

Спектр оптического лазерного излучения таких систем, как правило, лежит в ближнем ИК-диапазоне 785-1550 нм. Это связано с наличием в таком диапазоне большого количества источников и приемников лазерного излучения, а также наличием окон прозрачности в атмосфере. В то же время, имеются системы, которые в качестве передатчиков и приёмников используют видимый спектр оптического излучения.

Для квантового распределения ключей между двумя пользователями по АКС необходимо в пределах прямой видимости по оптическому спектру обеспечить точное совмещение квантового канала и канала синхронизации. Также необходима система наведения, которая будет точно совмещать выход лазерного излучения квантового канала и канала синхронизации между приёмником и передатчиком.

Конечных применений АКС довольно много, но мы остановимся на самых интересных из них. Первое применение – это защита управляющих каналов и каналов передачи данных для личного и общественного транспорта (в том числе и беспилотного) в умном городе. Развитие систем мобильной связи (введение сетей 5G в промышленную эксплуатацию и разработка стандарта 6G) в скором времени позволит подключать огромное количество устройств, что приведёт к обмену данными между дорожной инфраструктурой и участниками дорожного движения на протяжении всего пути, причём для беспилотного транспорта это будут управляющие каналы связи. Сейчас общение автомобиль-дорожная инфраструктура защищено с помощью PKI (Public Key Infrastructure), где основной упор делается на то, что ключи меняются настолько быстро, что злоумышленник не успевает их перехватить и расшифровать. Однако с увеличением вычислительных мощностей и появлением квантового компьютера такие атаки смогут стать успешными. АКС может защитить автомобиль, создавая для каждой поездки уникальное квантовое распределение ключей, которым уже можно защищать общение по радиочастотному каналу между системой автомобиль-дорожная инфраструктура или автомобиль-автомобиль.

Учёные из Уорикского университета в Ковентри [13] описывают развёртывание такой защищённой инфраструктуры автомобиль-умная дорога в отдельно взятом городском квартале.

Возможность АКС между двумя автомобилями была показана в докладе [14] на конференции QCRYPT2023. Две машины двигались по шоссе в одном направлении на скорости 112 км/ч и обменивались квантовыми ключами. Соотношение сигнал/шум в такой системе составило 17,4 дБ. В этом же докладе впервые продемонстрировано квантовое распределение ключей между едущей машиной и летящим рядом дроном. Система дрон-машина двигалась со скоростью 16 км/ч и средний QBER составил 6,4%.

Впервые возможность квантового распределения ключей в случае с движущимся самолётом показана в статье, вышедшей в 2013 году [4]. В 2017 году в статье канадских ученых [15] самолёт, на котором был установлен передаточный модуль, связывался с базовой станцией на земле, на которой был установлен приёмник. Расстояние от самолета до базовой станции во время полета составляло 3-10 км, скорость самолета – 260 км/ч. QBER не превышал 5%, а соотношение сигнал/шум было 3-5%.

Другой интересной работой является исследование [16], в котором демонстрировалась система дрон-дрон на расстоянии 200 метров. Особенностью АКС для БПЛА и дронов является то, что необходимо минимизировать массо-габаритные характеристики как модулей приёмника и передатчика, так и системы наведения и передачи оптического излучения. Китайские учёные смогли оптимизировать массу системы таким образом, что взлётный вес составил 11,8 кг. АКС, которая реализуется для БПЛА и дронов, очень перспективна, так как позволяет доставлять квантовое распределение ключей для удалённых объектов, не строя дорогостоящую инфраструктуру.

Космическая квантовая связь

Не стоит забывать, что прокладка оптического волокна может быть невозможна или крайне затруднена и ввиду наличия, например, протяжённого географического препятствия или в случае, когда какая-то территория принадлежит недружественному государству.

В таких условиях единственно возможным решением видится использование искусственных спутников Земли. При этом спутники могут использоваться, например, в качестве доверенных узлов между удалёнными наземными станциями. Также можно поместить на спутниках источники квантово-запутанных пар фотонов, чтобы затем разделять фотоны из каждой пары и одновременно направлять их на две наземные станции. Если при этом над фотонами провести квантовые измерения их состояний на Земле, то результаты этих измерений, вследствие квантовой запутанности, окажутся скоррелированными, хотя их и нельзя будет предсказать заранее. Это позволяет двум удалённым пользователям на Земле распределять между собой секретные ключи для шифрования.

Историю квантовых коммуникаций в космосе можно начать, наверное, с японского спутника SOCRATES, который был запущен ещё в 2014 году. Вес космического аппарата составил 48 кг. С помощью SOCRATES японские исследователи провели эксперимент по передаче из космоса на Землю оптических импульсов в двух состояниях поляризации с частотой повторения 10 МГц. Выходная мощность оптического сигнала при этом как минимум на 7 порядков превышала мощность, соответствующую однофотонному сигналу – т.е. о квантово-защищённой связи говорить тут пока не приходится. Тем не менее, этот эксперимент можно считать важной вехой в развитии квантовой связи в космосе, т.к. японские учёные показали принципиальную возможность квантового распределения ключа с использованием малого космического аппарата.

Немного позже лидерство в космической квантовой гонке перехватил Китай. В 2016 году китайские исследователи запустили на орбиту Micius, первый в мире спутник для полноценной квантовой связи. В этом же году они провели эксперимент по квантовому распределению ключа между спутником и наземной

станцией. Результаты этой работы были опубликованы в журнале Nature в 2017 году.

Примерно в это же время этим же научным коллективом был проведён менее известный, но не менее значимый эксперимент по квантовому распределению ключа между наземной станцией и квантовым передатчиком, установленным на борту китайской космической лаборатории «Тяньгун-2». Вес передатчика составлял 57,9 кг.

Позже с помощью Micius были проведены распределение квантовой запутанности и квантовая телепортация из космоса, а также другие эксперименты по квантовой физике. Несомненно, на сегодняшний день этот космический аппарат можно считать одним из самых значимых практических достижений в области космической квантовой связи. Однако стоит отметить, что вес спутника составляет 635 кг, а затраты на данный проект чрезвычайно высоки. Поэтому такой космический аппарат, как Micius, едва ли можно назвать привлекательным с коммерческой точки зрения.

Использование космических аппаратов меньших размеров может быть намного более экономически выгодным. Это могут быть, например, малые космические аппараты формата CubeSat, микро- (10-100 кг) или даже наноспутники (1-10 кг). Впрочем, некоторые исследователи рассматривают наноспутники только как промежуточный этап, который нужен для проверки работоспособности основных технических решений. При этом предполагается, что в дальнейшем основу космического сегмента глобальной квантовой сети должна составлять группировка из микроспутников. В любом случае, на данный момент ни одним участником квантовой гонки ещё не было продемонстрировано квантовое распределение ключа ни с нано-, ни с микроспутником. Однако ради справедливости стоит сказать, что летом 2022 года был анонсирован запуск второго китайского спутника для квантовой связи, Jinan 1, вес которого не превышает 100 кг. По неофициальным сообщениям коллег из Китая, этот аппарат якобы успешно работает уже с осени 2022. Тем не менее, полученные результаты, если таковые имеются, пока ещё нигде не были опубликованы.

Помимо Китая, в области космической квантовой связи сейчас активно работают исследователи в Евросоюзе, Великобритании, Канаде и Сингапуре. Европейское космическое агентство совместно с партнёрами развивает проект под названием Eagle-1. Также есть свой проект у Германии, где разрабатывают космические аппараты CUBE и QUBE-II. У исследователей из Франции и Австрии есть совместный проект Nanobob. В Великобритании квантовой спутниковой связью занимаются, в основном, в университете Стратклайда. В Канаде идёт работа над микроспутником QEYSSat, который планируют вывести на орбиту в 2024-2025 гг. Особенностью канадского проекта является распределение квантового ключа в конфигурации Земля-спутник, в то время как во всех остальных миссиях предполагается передача квантового сигнала по нисходящему каналу связи.

Сингапурские учёные занимаются исследованиями в области космической квантовой связи не менее 10 лет, и у них уже имеется успешный опыт в разработке и эксплуатации малых космических аппаратов формата CubeSat. Это аппараты Galassia и SpooQy-1, с помощью которых в условиях космоса проверяли работу источников квантово-запутанных пар фотонов. Сейчас сингапурские исследователи работают над своим следующим спутником, SpeQtral-1, который уже предусматривает возможность полноценной квантовой связи с оптической наземной станцией. Это малый космический аппарат формата 16U CubeSat, запуск которого запланирован на 2025 год.

В космической квантовой гонке Россия, несомненно, пока что отстаёт от таких стран, как Китай и Сингапур, однако некоторые достижения в этой области имеются и у нас. Так, у российских учёных есть успешный опыт в создании оптических наземных станций, позволяющих принимать квантовые состояния со спутника. В 2022 году, вместе с исследователями из Научно-технического университета Китая, они провели серию экспериментов по распределению ключа между китайским спутником Micius и российской наземной станцией [17]. Приёмная станция была изготовлена на базе телескопа с апертурой 600 мм, который расположен на территории Звенигородской обсерватории. Предварительно также было проведено квантовое распределение ключа между спутником и китайской наземной станцией, расположенной неподалёку от города Урумчи. С использованием операции «исключающее или», проведённой по команде с Земли на спутнике, наземные станции в России и в Китае получили в распоряжение секретный ключ для шифрования длиной 4 кбайт. Впоследствии российская и китайская стороны обменялись монохромными изображениями размером 256 на 64 пикселя, которые были закодированы данным ключом с помощью шифра Вернама. Общий же объём квантового ключа, распределённого между Micius и звенигородской станцией в ходе совместных экспериментов, был намного больше, чем 4 кбайт. Кроме этого, им удалось обнаружить уязвимость Micius ко взлому: речь идёт, конечно, не о квантовом протоколе как таковом – его безопасность основана на принципах физики, а лишь об уязвимости из-за несовершенства технической реализации.

Основные проблемы атмосферной и космической квантовой связи

Проблемы построения систем квантовой связи через атмосферные, включая космические каналы условно можно разделить на несколько групп.

- Выбор оптимальной длины волны. Здесь речь идёт о своеобразном компромиссе между диапазонами максимальной чувствительности доступных однофотонных детекторов (кремниевых и индий-галий-арсенидных) и окнами пропускания атмосферы, которые сильно отличаются, в зависимости от локации, а также величины дифракционного расхождения и рассеяния в оптическом канале связи и уровня шумовой засветки. Кроме того, необходимо учесть стоимость управляющих волоконно-оптических элементов и детекторов одиночных фотонов, предназначенных для различных спектральных диапазонов.
- Совместное наведение передатчика и приёмника и его удержание с необходимой точностью в течение всего времени передачи квантовых состояний. Эта проблема является наиболее специфичной с технической точки зрения по сравнению с волоконно-оптическими реализациями. В то же время, в мире известно несколько эф-

фективных её решений посредством систем активного трекинга, когда приёмная и передающая станция оснащены дополнительными (как правило, двухконтурными) поворотными устройствами, обеспечивающими точное наведение и отслеживание вибрации, поворотов и перемещений. Это ведёт к существенному удорожанию систем АКС и сложности в их практическом применении на промышленных объектах.

- Компенсация вибраций и влияния турбулентности атмосферы. Если компенсация вибраций устраняется пассивными и активными системами (см. предыдущий пункт), то турбулентность атмосферы представляет серьёзную проблему как с точки зрения внесения фазовых искажений в поперечный профиль пучка, так и в коэффициент экстинкции. Действительно, турбулентность приводит к дополнительному расплыванию пучка и увеличению его эффективного поперечного размера, который может в итоге выйти за пределы апертуры приёмной оптической системы.
- Снижение влияния фонового излучения внешней засветки, возникающей из-за свечения небесных тел, рассеяния, бликов и отражений с помощью спектральной, временной и пространственной фильтрации. Известны эксперименты по передаче и приёму квантовых состояний в режиме отдельных фотонов при дневном свете. Однако, как правило, это связано с использованием специальных бленд, одномодовых волокон, поляризаторов и, конечно, узкополосных фильтров. В конечном счете, как правило, эти устройства приводят к дополнительным потерям, что для атмосферной квантовой связи крайне нежелательно.
- Расчёт высокоапертурной оптики для уменьшения оптических потерь.
- Компенсация поляризационных искажений, хоть и малых по величине, но всё же оказывающих влияние на уровень возможных ошибок.
- Основной специфический с точки зрения обоснования защищенности протоколов квантовой связи фактор, отличающий атмосферные каналы от волоконно-оптических, – это заранее неизвестные и меняющиеся со временем потери, возникающие из-за пыли, осадков, различных взвесей и других факторов, включая преднамеренное и/или непреднамеренное попадание посторонних предметов в канал связи. Потери канала вместе с вибрацией передатчика и приёмника, а также турбулентностью приводят к росту специфических ошибок протоколов квантовой связи QBER, что ведёт к обрыву сеанса связи из-за того, что невозможно понять, идёт ли атака от злоумышленника или ошибки возросли из-за других внешних факторов.

В таблице 1 показано поглощение в атмосфере при разных погодных условиях для двух длин волн, наиболее часто используемых для атмосферного квантового распределения ключей (АКРК) [18]. Из приведённых данных видно, что при тумане или дожде поглощение возрастает на порядки, и распределение ключа на большие расстояния становится невозможным. Поэтому при проектировании линий защищённой связи на основе АКРК следует учитывать, что на практике дальность ограничивается расстоянием менее 10 км. Также важным является тот факт, что потери на длине волны 1550 нм оказываются примерно в полтора раза меньше, чем на 800 нм.

С другой стороны, поскольку оптические сигналы распространяются в свободном пространстве, между квантовым и классическим каналами отсутствуют интерференционные эффекты и влияние комбинационного рассеяния света, что характерно для волоконных линий связи. Это позволяет достаточно легко сосуществовать одновременно квантовым и классическим каналам.

Выбор оптимального протокола КРК с точки зрения безопасности и скорости генерации ключа для атмосферных каналов связи является не менее важной задачей. На сегодняшний день, пожалуй, единственным протоколом, который обеспечивает секретность при произвольных и заранее неизвестных потерях в канале связи, а также при неоднофотонном источнике, является протокол релятивистской квантовой криптографии [19-20]. Это семейство протоколов реализуется только через атмосферные каналы. Оно отличается от «классических» протоколов квантовой криптографии тем, что к ограничениям на действия злоумышленника, связанным с законами квантовой механики (запрет существования общей системы собственных функций для наблюдаемых, описываемых некоммутирующими операторами), добавляются ограничения, связанные с конечной скоростью распространения сигналов, диктуемые специальной теорией относительности. Однако реализовать такие протоколы на больших расстояниях довольно сложно, поскольку для этого необходимо использовать одномодовый приём.

Перспективы развития квантовой связи

Более или менее очевидной перспективой развития квантовых коммуникаций является создание глобальной интегрированной квантовой сети. Эта сеть будет состоять из нескольких типов сегментов: «волоконно-оптических», включающих в себя магистральные, городские и локальные сети, соединяющие абонентов на разных расстояниях с помощью оптоволокна; «атмо-

Таблица 1.
Поглощение в атмосфере при разных погодных условиях для двух длин волн, наиболее часто используемых для АКРК

Атмосферные условия	Видимость (км)	Ослабление (дБ/км)	
		Длина волны 850 нм	Длина волны 1550 нм
Чистый воздух	23	0,42	0,2
Дымка	4	2,8	1,6
Водяной пар	2	6	4
Лёгкий туман	1	13	9
Умеренный туман	0,5	28	21
Плотный туман	0,2	73	60
Дождь	0,05	309	272

сферных» сегментов, обеспечивающих квантовую связь между движущимися на- и/или околоземными объектами; а также «космического» сегмента, обеспечивающего межконтинентальную квантово-защищённую связь.

Сегодня несомненным лидером движения в сторону глобальной квантовой сети выступает Китай: именно здесь уже построена масштабная магистральная квантовая сеть, опирающаяся на локальные квантовые сети различных топологий. Именно в Китае успешно запущены низкоорбитальные спутники, которые продемонстрировали перспективы технологии в контексте создания глобальных, защищённых квантовыми ключами сетей, функционирующих на протяжённых расстояниях в тысячи километров: [21], [22].

Что же касается перспектив технологического развития систем квантовой связи по атмосферным, включая космические, каналам, то их можно разделить на три составляющие.

1. Развитие аппаратной базы, когда модули приёмника и передатчика будут оптимизированы именно под квантовую связь по атмосферным, включая космические, каналам – сейчас в основном используются модули, такие же, как и для магистральных оптоволоконных квантовых сетей.
2. Развитие протоколов передачи и архитектуры сети. Помимо аппаратной части необходимо развивать специальные протоколы именно для передачи квантового распределения ключей по атмосферным каналам. Также необходимо развивать архитектуру квантовой связи как часть глобальных квантовых коммуникаций, используя дроны, БПЛА и искусственные спутники Земли как часть глобальной сети.
3. Встраивание АКС в сети связи 6-го поколения (6G). Развитие умных городов приведёт к росту количества различных датчиков, объектов, беспилотного транспорта, которым необходим беспроводной защищённый доступ. Это может осуществить АКС: телескопические системы, передающие квантовое распределение ключей на конечные устройства, могут быть распределены в городском пространстве и таким образом защищать как каналы передачи данных, так и управляющие каналы. Такая схема должна быть заложена на этапе проектирования сетей 6G.

Об авторах:

Андрей Дмитриевич Деев, МГУ имени М.В. Ломоносова, Россия, г. Москва

Александр Александрович Калинкин, к.ф.-м.н., Центр квантовых технологий, физический факультет МГУ имени М.В. Ломоносова, Россия, г. Москва

Сергей Павлович Кулик, д.ф.-м.н., профессор, Scopus Author ID: 7005727307, Центр квантовых технологий, физический факультет МГУ имени М.В. Ломоносова, Россия, г. Москва

Александр Витальевич Миллер, Scopus Author ID: 57193204342 ООО «МЦКТ», Россия, г. Москва

Иван Сергеевич Полухин, SPIN-код: 2682-4897, Scopus Author ID: 56251826100, Университет ИТМО, Россия, г. Санкт-Петербург

Список литературы:

[1] M. Avesani et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf 7, 93 (2021)

[2] Matthew P Peloso, Ilja Gerhardt, Caleb Ho, Antía Lamas-Linares and Christian Kurtsiefer, Daylight operation of a free space, entanglement-based quantum key distribution system. New J. Phys. 11 045007 (2009)

[3] R. Ursin at al. Entanglement-based quantum communication over 144 km. Nature Physics volume 3, pages 481–486 (2007)

[4] S. Nauerth at al. Air-to-ground Quantum communication, Nature Photon. 2013

[5] J.-P. Bourgoin, B. L. Higgins, N. Gigov, at al. Free-space quantum key distribution to a moving receiver, Opt. Express v. 23, 33437 (2015)

[6] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nature Photonics, vol. 11, p. 502, 2017

[7] P Villoresi, T Jennewein, F Tamburini, M Aspelmeyer, C Bonato, R Ursin, C Pernechele, V Luceri, G Bianco, A Zeilinger, Experimental verification of the feasibility of a quantum channel between space and Earth. New J. Phys. 10 033038 (2008)

[8] Daniele Dequal, Giuseppe Vallone, Davide Bacco, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi, Experimental single-photon exchange along a space link of 7000 km. Phys. Rev. A 93, 010301(R) (2016)

[9] Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel KL Oi, Alexander Ling, Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite, Physical Review Applied 5, 054022 (2016)

[10] Ji-Gang Ren at al. Portable ground stations for space-to-ground quantum key distribution. arXiv:2205.13828v1

[11] Yehia R. et al. Connecting Quantum Cities: Simulation of a Satellite-Based Quantum Network // arXiv Prepr. arXiv2307.11606. 2023

[12] K. Günthner, Quantum-limited measurements of optical signals from a geostationary satellite, Optica, Vol. 4, No. 6, p.611, (2017)

[13] Fowler, Daniel S., Carsten Maple, and Gregory Epiphaniou, A Practical Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications. Vehicles 5.4 (2023): 1586-1604

[14] https://2023.qcrypt.net/slides/QCrypt2023TalkSlides020Conrad.pdf

[15] Pugh, Christopher J., et al. Airborne demonstration of a quantum key distribution receiver payload. Quantum Science and Technology 2.2 (2017): 024009

[16] Liu, Hua-Ying, et al. Optical-relayed entanglement distribution using drones as mobile nodes. Physical Review Letters 126.2 (2021): 020503

[17] Miller, Alexander V., et al. Vector—towards quantum key distribution with small satellites. EPJ Quantum Technology 10.1 (2023): 52

[18] A. Trichili et al., Roadmap to free space optics, JOSA B, Vol. 37, No. 11, A184-A201 (2020)

[19] I V Radchenko, K S Kravtsov, S P Kulik and S N Molotkov, Relativistic quantum cryptography, Laser Phys. Lett., vol. 11, no. 6, 065203 (2014)

[20] Konstantin Kravtsov, Igor Radchenko, Sergei Kulik, and Sergei Molotkov, Relativistic quantum key distribution system with one-way quantum communication. Scientific Reports volume 8, Article number: 6102 (2018)

[21] Y-A. Chen et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature, Vol. 589, 214 (2021)

[22] Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan, Micius quantum experiments in space. Reviews of Modern Physics, Volume 94, 035001 (2022))

Управление Интернетом в 2024 году: взаимовыгодное сотрудничество или игра с нулевой суммой?

Вольфганг Кляйнвехтер

Для всех участников глобальной экосистемы управления Интернетом список задач на 2024 год обширен. Виртуальный мир, как и реальный, переживает непростые времена. Американский ученый, один из «отцов Интернета» Винтон Серф (Vinton Cerf) когда-то утверждал, что Интернет является всего лишь отражением реального мира. Если мир находится в трудной ситуации, это неизбежно сказывается на Интернете.

Интернет в том виде, в каком он развивался на протяжении более полувека, представляет собой глобальную сеть, объединяющую тысячи сетей по всему миру для обеспечения связи между людьми в любом месте и в любое время, независимо от географических границ. Концепция «один мир, один Интернет» основана на понятии такой универсальной инфраструктуры, где все взаимосвязано и каждый зависит от другого. Мы живем в цифровую эпоху или, как отметила Группа высокого уровня по цифровому сотрудничеству ООН, в «эпоху кибервзаимозависимости» (2019 год). Взаимозависимость подразумевает, что мы все в одной лодке, независимо от того, нравимся ли мы друг другу или нет. Глобальным проблемам, таким как изменение климата или пандемии, всё равно, каких взглядов вы придерживаетесь. Если «пассажиры лодки» не могут найти общий язык для успешной навигации в бурных водах, они рискуют потонуть. И инфраструктура Интернета – это именно такая глобальная проблема.

Взаимное доверие и взаимная выгода легли в основу развития Интернета. Интернет изначально возник из идеи «совместного пользования»: если что-то подходит соседу, то это подходит и мне. Если он или она столкнется с неудачей, то у меня тоже могут возникнуть проблемы. Эта философия обоюдной пользы послужила концептуальным фундаментом для формирования глобального информационного сообщества и его институтов, таких как Общество Интернета (ISOC), Инженерный совет Интернета (IETF), корпорация ICANN и Форум по управлению Интернетом (IGF).

Но Интернет с пятью миллиардами пользователей это не то же самое, что Интернет с пятью миллионами. «Сетевой этикет», определение которому дано в RFC 1855 от 1995 года, малознаком новому поколению пользователей. Свободой Интернета злоупотребляют, а политические лидеры 2020-х вернулись к играм с нулевой суммой.

В игре с нулевой суммой, разумеется, есть победители и проигравшие. В мире взаимосвязей проблема заключается в том, что это будет пиррова победа с неизвестными последствиями. Цифровое пространство по-прежнему остается terra incognita. Даже спустя 20 лет после того, как Организация Объединенных Наций провела Всемирную встречу на высшем уровне по вопросам информационного общества (WSIS), мы до сих пор полностью не понимаем, как функционирует жизнь в безграничном киберпространстве, где присутствуют 193 суверенных государства и семь миллиардов населения. Мы все еще находимся в начале «эпохи кибервзаимозависимости».

Наступивший 2024 год покажет, способно ли мировое сообщество, несмотря на все политические, экономические и культурные различия, находить общие решения для дальнейшего развития нашей цифровой среды. В областях искусственного интеллекта, кибербезопасности, развертывания инфраструктуры, защиты конфиденциальности и свободы самовыражения есть возможности направить развитие на пользу широким слоям населения. Однако также возрастает риск втягивания Интернета в геостратегические конфликты. Киберконфликты могут выйти из-под контроля и привести к цифровым катастрофам, где все окажутся в проигрыше.

Глобальный цифровой договор (Global Digital Contract, GDC)

В 2024 году основным предметом дискуссий станет Глобальный цифровой договор (GDC). Идея создания такого договора возникла в рамках празднования 75-летия ООН: в сентябре 2020 года 193 члена ООН приняли декларацию с призывом усилить цифровое сотрудничество. В декларации отмечается, что «поскольку в современном мире от цифровых средств как никогда зависят обеспечение связи и социально-экономическое процветание, в числе первоочередных задач должны оставаться формирование общего видения цифрового сотрудничества и цифрового будущего, отражающего весь потенциал полезного использования технологий, и решение вопросов, касающихся доверия и безопасности в цифровой сфере». В рамках этого процесса Генеральный секретарь ООН Антониу Гутерриш (António Guterres) разработал общий план и предложил провести «Саммит будущего», который намечен на сентябрь 2024 года. Глобальный цифровой договор является частью этого процесса. На саммите

государства-члены ООН примут Пакт во имя будущего, а договор будет включен в виде приложения.

Составление договора обсуждается с 2022 года. Участники форумов по управлению Интернетом в Аддис-Абебе (Эфиопия) в декабре 2022 года и в Киото (Япония) в октябре 2023 года провели обширные дискуссии на эту тему. ООН опубликовала Аналитическую записку №5 (июль 2023) с соответствующим предложениями. Два сокоординатора Глобального цифрового договора – правительства Швеции и Замбии – провели большое число многосторонних консультаций и углубленных дискуссий, после чего в сентябре 2023 года опубликовали краткий исследовательский доклад. Формат «Саммита будущего» обсуждался на следующем этапе консультаций в декабре 2023 года в Нью-Йорке при поддержке правительств Германии и Намибии.

График завершающего этапа теперь утвержден. Предстоят два дополнительных раунда общественных консультаций с участием как правительств, так и неправительственных сторон, в феврале и марте 2024 года. Далее последуют три раунда межправительственных переговоров в апреле и мае. Предложения будут приниматься в письменном виде до 10 марта 2024 года. Окончательный текст планируется подготовить в июле или августе. Если все пойдет хорошо, то договор будет принят путем всеобщего одобрения 23 сентября 2024 года.

Однако все многосторонние консультации, глубокие исследования и отчеты не дают четкой картины. Множество вопросов, как с точки зрения содержания, так и процедурных аспектов, остаются открытыми. Неясно, как предложения неправительственных сторон будут учтены в межправительственных переговорах. Глобальный цифровой договор будет включать семь глав, однако непонятно, будет ли он разработан как краткое заявление с общими принципами или в виде подробного документа с конкретными рекомендациями. В процессе консультаций выявились глубокие принципиальные разногласия по таким вопросам, как искусственный интеллект, права человека и кибербезопасность. Переговорщикам будет непросто сгладить столь существенные различия с помощью общего дипломатического языка.

Кроме того, остаются неясными вопросы организации последующего этапа после GDC. Форум по управлению Интернетом (IGF) предложил себя в качестве «места приземления» для договора. Если в договоре будут отражены рекомендации, то IGF сможет осуществлять их внедрение и представлять ежегодный отчет о состоянии глобального цифрового сотрудничества перед Генеральной Ассамблеей ООН. В 2019 году Группа высокого уровня рекомендовала усилить IGF, превратив его в IGF+. Глобальный цифровой договор открывает возможность для реализации этой рекомендации. Альтернативная идея, высказанная в Аналитической записке №5, о создании Форума по цифровому сотрудничеству (DCF) не получила поддержки. DCF был широко отвергнут мировым сообществом, в том числе на форуме IGF в Киото.

Многие участники видят в GDC большие возможности, но есть и те, кто считает, что он может подорвать текущие многосторонние структуры и процедуры. Возможно возобновление споров о том, следует ли экосистеме управления Интернетом принять межправительственную поддержку. Антониу Гутерриш заявил, что «Саммит будущего» – это «возможность, которая предоставляется раз в поколение». Вероятно, эти слова верны для Пакта во имя будущего, но не относятся к дискуссии о цифровом сотрудничестве. Этот вопрос обсуждается давно, начиная с 1990-х годов. Дискуссии продолжатся и после 2030 года. Это бесконечная история, которая наверняка будет занимать будущие поколения.

На этом длительном пути выработан ряд принципов, закрепленных, в частности, в Женевской декларации принципов (2003 год), Тунисской программе (2005 год), Декларации NetMundial в Сан-Паулу (2014 год) и Дорожной карте ООН по цифровому сотрудничеству (2021 год). Недостатка в защитных механизмах не наблюдается. Глобальный цифровой договор должен опираться на это наследие, и его функция заключается в том, чтобы выявлять пробелы и формулировать рекомендации по работе с новыми вызовами, такими как искусственный интеллект, кибербезопасность и социальные сети. Кроме того, в нем будут описаны процедуры для усиленного многостороннего сотрудничества.

Экосистема управления Интернетом работает. Несмотря на свои недостатки, даже в сложные времена, такие как пандемия, существующие механизмы продолжили функционировать, обеспечив возможность удаленной работы, дистанционного обучения и онлайн-шопинга для миллиардов людей по всему миру. Нет необходимости изобретать велосипед заново. Авторы договора GDC должны внимательно перечитать письмо, которое Группа лидеров форума IGF направила Генеральному секретарю ООН Антониу Гутерришу после форума в Киото. В письме предлагалось укрепить IGF.

Всемирная встреча на высшем уровне по вопросам информационного общества (WSIS+20)

Решение о будущем IGF должно быть принято на обзорной конференции WSIS, запланированной на 2025 год (WSIS+20). Подготовка к WSIS+20 началась недавно на межсессионном заседании Комиссии ООН по науке и технике в целях развития (КНТР ООН – орган ООН, ответственный за реализацию WSIS) в ноябре 2023 года в Лиссабоне (Португалия).

Участники встречи в Лиссабоне подробно обсудили вопрос увязывания целей WSIS с Целями в области устойчивого развития ООН (ЦУР). Обзорная конференция по ЦУР запланирована на 2030 год. Было бы логичным объединить цели ЦУР и WSIS в следующем цикле развития (2030–2045) и назвать их, к примеру, «Комплексными целями развития». В таком процессе IGF+ может сыграть ключевую роль как универсальная многосторонняя платформа для обсуждений, предоставляющая необходимые возможности.

Имеет смысл опираться на действующие соглашения, особенно в условиях геостратегической напряженности, которая снижает возможность достижения консенсуса по дальнейшей работе. На встрече WSIS 1 (Женева, 2003 год) все 193 члена ООН согласились, что глобальное информационное сообщество должно быть «инклюзивным и ориентированным на людей и развитие». Они намеревались построить такое информационное общество, «в котором каждый мог бы создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими, с тем чтобы дать отдельным лицам, общинам и народам возможность в полной мере реализовать свой потенциал, содействуя своему устойчивому развитию и повышая качество своей жизни на

основе целей и принципов Устава Организации Объединенных Наций и соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека». Хорошая формулировка, которая остается актуальной и в 2024 году.

Также нет необходимости пересматривать определение управления Интернетом, как это было согласовано в Тунисской программе, принятой на встрече WSIS 2. В широкое определение управления Интернетом были включены как технические аспекты (управление критическими ресурсами Интернета и стандартами), так и вопросы общественной политики, связанные с Интернетом. Конечно, с момента встречи в Тунисе в Интернете произошли новые волны инноваций, и мы стали свидетелями еще более активного обсуждения новых подходов к управлению проблемами в цифровой среде. Появилась новая терминология, такая как «цифровое управление», «управление искусственным интеллектом», «киберуправление», «управление данными», «управление Интернетом вещей» и т.д. К сожалению, новая терминология привела к еще большей путанице.

Позитивный момент заключается в том, что широкое определение управления Интернетом, принятое на саммите в Тунисе, охватывает все аспекты управления новыми разработками, от искусственного интеллекта до Интернета вещей. Основные принципы принятого определения, такие как включение всех заинтересованных сторон в соответствующих ролях, разработка политики и принятие решений в открытых, прозрачных, инклюзивных и демократичных процессах, остаются актуальными не только для управления системой доменных имен, но и для Интернета вещей, управления данными, кибербезопасности и разработок искусственного интеллекта. Сужение термина «управление Интернетом» до технических аспектов («узкое определение») и внедрение новой терминологии для обозначения политических аспектов могут привести к терминологической путанице и борьбе за определения. Кроме того, это может способствовать фрагментации Интернета.

Искусственный интеллект

Риск возможной путаницы также присутствует в обсуждении искусственного интеллекта. В настоящее время все стремятся создать свою стратегию по ИИ. «Большая двадцатка» уже приняла принципы ИИ в 2021 году. «Большая семерка» запустила Хиросимский процесс по ИИ в 2023 году. Президент США опубликовал указ по искусственному интеллекту. Европейский союз разрабатывает законодательство по ИИ. Совет Европы работает над правовой конвенцией по ИИ, а ЮНЕСКО приняла рекомендации по этике и искусственному интеллекту. ООН создала соответствующую экспертную группу. Многие страны, включая Китай, Россию, Индию, Бразилию, ЮАР и др., обсуждают национальные стратегии в области искусственного интеллекта. Уже 10 лет в группе правительственных экспертов идут дискуссии о чувствительном вопросе смертоносных автономных систем вооружения.

Является ли это только временным трендом? И если да, то может ли ажиотаж вокруг искусственного интеллекта в 2024 году сравниться с ажиотажем вокруг интернета в 1990-х годах? Здесь существует интересное отличие. На заре Интернета аргумент «работает – не трогай» нашел широкую поддержку. В 2024 году большинство правительств и заинтересованных сторон пришли к выводу, что кое-что все же необходимо починить. Правительства и заинтересованные стороны пришли к соглашению, что искусственный интеллект нуждается в определенном регулировании. Все согласны с тем, что необходимо максимально использовать преимущества искусственного интеллекта, а риски минимизировать. Проблема лишь в том, что никто не знает, как это сделать. Ключевая задача заключается в поиске правильного баланса, но тут в игру вступает политическое противостояние.

Существуют различные точки зрения относительно того, каким должно быть регулирование. Диапазон предложений варьируется от всестороннего регулирования с четко определенными обязанностями и ответственностью (включая запреты на применение технологий искусственного интеллекта, нарушающих человеческое достоинство) до предложений о регулировании на более общих принципах с откладыванием детализации на более поздний этап, когда можно будет более тщательно оценить последствия конкретного использования.

Характерный пример этой неопределенности и размытости – Саммит по искусственному интеллекту, проведенный премьер-министром Великобритании Риши Сунаком (Rishi Sunak) в Лондоне в октябре 2023 года. В принятой Декларации Блетчли 27 правительств и ведущих интернет-компаний согласились выявлять риски искусственного интеллекта и разрабатывать соответствующие политики и необходимые регулирования, но не объяснили, как это следует делать. Участники «полны решимости поддерживать международную инклюзивную сеть научных исследований в области передовой безопасности ИИ, которая охватывает и дополняет существующее и новое многостороннее, плюрилатеральное и двустороннее сотрудничество, в том числе через существующие международные форумы и другие соответствующие инициативы, чтобы облегчить предоставление лучших научных данных для разработки политики и достижения общественного блага». Звучит неплохо, но пока это пустые слова, которые расходятся с действиями.

Теперь лондонская встреча будет проводиться в разных странах мира ежегодно. В следующий раз ее примет Сеул осенью 2024 года. Неясно, будет ли встреча по сути похожа на саммит Международного союза электросвязи по искусственному интеллекту. С 2017 года союз организует подобные саммиты под названием «ИИ во благо». Следующий саммит пройдет 30–31 мая 2024 года в Женеве (Швейцария).

Как эти международные обсуждения повлияют на законодателей национальных парламентов – вопрос открытый. На данный момент Конгресс США не смог принять законодательство по искусственному интеллекту, которое бы устраивало обе партии. В противовес Акту ЕС об искусственном интеллекте, принятому в декабре 2023 года, президент США Джо Байден опубликовал в октябре 2023 года указ на ста страницах о «безопасном, защищенном и заслуживающем доверия искусственном интеллекте». В указе говорится о создании новых стандартов безопасности искусственного интеллекта, защите конфиденциальности граждан, продвижении равенства и гражданских прав, защите интересов потребителей и работников, стимулировании инноваций и конкуренции, а также продвижении лидерства США в мире и других вопросах. Президентский указ формально не является законом, но обязателен для исполнения.

Искусственный интеллект также находится на повестке дня Торгового и технологического совета США и ЕС (ТТС). В этом нет ничего удивительного, поскольку существует множество сходств

между президентским указом США и Актом ЕС об искусственном интеллекте. Однако существуют и фундаментальные различия, которые ТТС не смог решить. ЕС предпочитает конкретные нормативы для различных приложений, придерживаясь подхода на основе анализа рисков, а США отдают предпочтение структурному подходу.

Станет ли европейский акт или указ США образцами для мирового регулирования в области искусственного интеллекта? Председатель Европейской комиссии Урсула фон дер Ляйен (Ursula von der Leyen) уверена, что «акт об искусственном интеллекте внесет значительный вклад в формирование глобальных правил и принципов для искусственного интеллекта, ориентированного на человека». Она надеется, что «брюссельский эффект», который сработал в области защиты данных с Общим регламентом по защите данных (GDPR), также проявится и в случае с искусственным интеллектом. Но и это остается под вопросом.

Законодательство ЕС в области искусственного интеллекта гораздо сложнее, чем GDPR, и еще не оформилось до конца. В 2024 году в сотрудничестве с бизнесом, научным сообществом и гражданским обществом планируется разработка специального кодекса поведения. Национальные органы по наблюдению за рынком получат надзорные полномочия и будут координироваться. Способы применения ИИ будут подлежать сертификации в соответствии с четырьмя категориями риска. Также будет создан новый Европейский офис по искусственному интеллекту.

Тем не менее, обсуждение на глобальном уровне продолжится, и ООН сыграет в этом ключевую роль. Экспертная группа ООН по искусственному интеллекту выдвинула пять принципов в качестве основных элементов для будущего глобального регулирования в своем промежуточном отчете «Управление искусственным интеллектом на благо человечества» (декабрь 2023 года). «Управление искусственным интеллектом должно осуществляться инклюзивно, на благо всех, в интересах общественности; управление искусственным интеллектом должно разрабатываться параллельно с управлением данными и содействием общей базе данных; искусственный интеллект должен быть универсальным, сетевым и основанным на адаптивном многостороннем сотрудничестве; управление искусственным интеллектом должно быть закреплено в Уставе ООН, Международном праве в области защиты прав человека и других согласованных международных обязательствах, таких как Цели устойчивого развития».

Это звучит обнадеживающе и напоминает интернет-управление 2.0, что, несомненно, неплохо. Однако как эти принципы соотносятся с быстрыми изменениями в сфере искусственного интеллекта? В первые годы Интернета программисты опережали законодателей. Есть ощущение дежавю.

Тем не менее, из истории можно извлечь урок. Одной из проблем является создание институтов, которые стремятся управлять глобальными вызовами. Тридцать лет назад новые институты включали IETF, ISOC, ICANN, Консорциум Всемирной паутины, Региональные интернет-регистратуры и другие. Все они были неправительственными организациями. Сегодня директивные органы предлагают новые межправительственные организации для управления искусственным интеллектом. На Совете Безопасности ООН Антониу Гутерриш ссылался на Международное агентство по атомной энергии как на модель. На саммите G20 председатель Еврокомиссии Урсула фон дер Ляйен предложила в качестве образца Межправительственную группу экспертов по изменению климата. Экспертная группа ООН по искусственному интеллекту рассмотрела более 20 моделей, в основном межправительственных, но еще не представила предложение в своем промежуточном отчете. Финальный отчет ожидается летом 2024 года. Если существует потребность в глобальном органе управления искусственным интеллектом, то почему бы не взять пример с многосторонних корпораций? Не следует ли создать что-то вроде ICANN для искусственного интеллекта? Более 20 лет назад покойный генеральный секретарь ООН Кофи Аннан призывал к новым подходам к разработке стратегий. Многосторонний подход к управлению Интернетом был одним из них. Если бы обсуждение искусственного интеллекта открыло новую фазу формирования новых подходов, это было бы большим шагом вперед.

К сожалению, обсуждение искусственного интеллекта все чаще сводится к геостратегическим конфликтам и военной сфере. Несмотря на то, что Акт ЕС об искусственном интеллекте и Рамочная конвенция по искусственному интеллекту Совета Европы исключают военный аспект, намечается настоящая гонка вооружений в области искусственного интеллекта, что хорошо заметно в современных военных конфликтах, в том числе на Украине и в Газе.

В зоне украинского конфликта беспилотные аппараты, подключенные к Интернету, используются как в разведывательных, так и наступательных операциях. Кибератаки на гражданские и военные объекты стали неотъемлемой частью военных действий с обеих сторон. Все подвергается проверке на полезность в борьбе с противником. Интересный пример: камеры наблюдения, установленные в крупных городах Украины для обеспечения общественной безопасности, теперь используются российскими хакерами для целей военной разведки. Камеры работают на российском программном обеспечении. С другой стороны, украинская получастная IT-армия регулярно атакует цели в России. Во время конфликта в Газе израильская армия использовала искусственный интеллект для создания системы распознавания лиц, чтобы выявлять и ликвидировать боевиков ХАМАС. Интернет фактически становится оружием.

Глобальные социальные сети все чаще используются для психологической атаки. Попытки контролировать риторику ненависти и ложную информацию через регулирование платформ пока принесли ограниченный успех. Остается вопрос, сможет ли Закон ЕС о цифровых сервисах (DSA) вызвать «брюссельский эффект» и сократить количество фейков и ксенофобских высказываний. В октябре 2023 года ЮНЕСКО приняла документ, описывающий принципы регулирования платформ, который распространяется на все 193 страны ООН. Тем не менее, юридической обязательной силы этот документ не имеет.

Растут призывы прекратить гонку в области искусственного интеллекта. Вопросы об автономных системах вооружений, использующих Интернет, впервые обсуждались на Генеральной Ассамблее ООН в октябре 2023 года. На данный момент переговоры проходят в рамках Группы правительственных экспертов по смертоносным автономным системам вооружений, но прогресса пока не видно. Четвертого декабря 2023 года в ходе 78-й Генеральной Ассамблеи ООН предложенная Австрией резолюция получила 164 голоса «за», пять голосов «против» (Россия, Индия, Мали, Нигер и Беларусь), и девять воздержались (включая Китай). Резолюция содержит мало конкретики. Генеральному

секретарю ООН просто предлагается представить подробный отчет на следующей сессии Генеральной Ассамблеи. От правительств и заинтересованных сторон ожидается, что они внесут свой вклад в отчет.

Бывший госсекретарь США Генри Киссинджер (Henry Kissinger), скончавшийся в декабре 2023 года, предостерегал от возможной военной катастрофы, связанной с использованием искусственного интеллекта, в своем эссе для *Foreign Affairs* в октябре 2023 года. Он уподобил этот риск опасности ядерной войны. «Будут ли машины со сверхчеловеческими способностями угрожать статусу человечества как хозяина Вселенной? Подрывает ли ИИ монополию отдельных стран на средства массового уничтожения? Позволит ли ИИ отдельным индивидам или небольшим группам людей создавать вирусы, способные убивать в масштабах, которые раньше были прерогативой только великих держав? Может ли ИИ разрушить средства ядерного сдерживания, которые были основой сегодняшнего мирового порядка? На данный момент никто не может с уверенностью ответить на эти вопросы. Но, изучая эти вопросы в течение последних двух лет с группой технологических лидеров, находящихся в авангарде революции искусственного интеллекта, мы пришли к выводу, что перспективы того, что неограниченное развитие ИИ создаст катастрофические последствия для Соединенных Штатов и всего мира, проявляются настолько убедительно, что мировые лидеры должны начать действовать немедленно». Киссинджер потребовал, чтобы Китай и США начали переговоры по этому вопросу, опираясь на модель переговоров США и Советского Союза об ограничении стратегических вооружений в конце 1960-х годов. Насколько военные аспекты будут освещены на консультациях по искусственному интеллекту, о которых договорились президенты США и Китая Байден и Си на встрече 15 ноября 2023 года в Сан-Франциско, еще предстоит увидеть.

Кибербезопасность и киберпреступления

В 2024 году дискуссии о кибербезопасности продолжатся в рамках Рабочей группы открытого состава (OEWG) Первого комитета Генеральной Ассамблеи (ГА) ООН и Специального комитета (АНС) Третьего комитета ГА ООН.

Рабочая группа проведет два формальных межправительственных собрания в 2024 году, а также несколько неформальных сессий с участием заинтересованных сторон. Основной задачей Рабочей группы станет внедрение нового межправительственного механизма, известного как «точки контакта». Механизм задуман по аналогии с «красным телефоном» горячей линией, установленной между США и бывшим СССР после Карибского кризиса в 1960-х годах. В случае кибератаки государства должны иметь возможность связаться с подозреваемым правительством для разъяснения ситуации. Подобный механизм был введен в ОБСЕ много лет назад и успешно работал на региональном уровне.

Однако более сложным будет обсуждение перспектив Рабочей группы. Ее мандат истекает в 2025 году. Существует общее понимание необходимости создания постоянной платформы ООН для переговоров по вопросам кибербезопасности. Однако есть два различных предложения: страны Запада выступают за запуск так называемой программы действий, сосредоточенной на внедрении 11 норм кибербезопасности, принятых Группой правительственных экспертов в 2015 году и получивших поддержку в многочисленных резолюциях ООН. Россия, Китай и некоторые другие страны выступают за придание Рабочей группе постоянного статуса с мандатом для переговоров по новым нормам и превращения рекомендательных норм в обязательную Конвенцию ООН по кибербезопасности.

Запад в целом не возражает против идеи дополнительных норм, но считает, что прежде чем переходить к следующему этапу, необходимо ясно определить, как существующие 11 норм, разработанные Группой правительственных экспертов, применяются государствами на практике. Прежде чем переходить на новый уровень, нужно иметь полную картину поведения государств в киберпространстве в соответствии с международным правом.

Двойственность ситуации заключается в том, что 78-я Генеральная Ассамблея ООН приняла оба предложения. Российский проект резолюции получил 112 голосов «за» и 52 «против» (включая всех членов ЕС, США, Японию, Австралию, Турцию, Украину и Албанию); 11 стран воздержались. Резолюция о программе действий, представленная Францией, получила 158 голосов «за» и 10 «против» (включая Китай и Россию) при 12 воздержавшихся. Будет интересно посмотреть, как эта ситуация будет развиваться на сессиях Рабочей группы в 2024 году.

Так же неясно, как неправительственные участники от бизнеса, научного сообщества, гражданского общества и технического сообщества будут участвовать в работе Рабочей группы в будущем. Проводимые между формальными заседаниями группы так называемые неформальные консультации позволяют каждому высказать свое мнение, независимо от того, признаны они Экономическим и Социальным Советом ООН как НПО или нет. Правило распространяется, например, на такие интернет-компании, как Microsoft, исследовательские институты, такие как Женевский институт цифрового миротворчества или расположенный в Гааге Глобальный форум киберэкспертизы. Однако многим НПО не разрешено участвовать в обычных заседаниях Рабочей группы. Несмотря на то, что резолюция о программе действий призывает к включению в диалог «соответствующих заинтересованных сторон» там, где это «целесообразно», сложность состоит в том, что правительства имеют право вето в определении того, что считается «целесообразным». Россия внесла в черный список более десятка НПО, включая Всемирный экономический форум (ВЭФ). В ответ Украина заблокировала участие российских институтов, таких как Московский институт международных отношений (МГИМО).

Неправительственные организации имеют упрощенный доступ к совещаниям Специального комитета по киберпреступности. Пока не известно, поможет ли это завершить переговоры весной 2024 года. Шестого ноября 2023 года председатель комитета представил новую редакцию текста Конвенции ООН о противодействии киберпреступности. Однако текст по-прежнему полон допущений. Все еще не ясно, что именно подразумевается под преступлением в киберпространстве. Незаконное вторжение в иностранные сети или нарушение блогером цензуры в конкретной стране? Западные страны предпочитают более узкое определение, в то время как автократии предпочитают более широкое. Процедуры осуществления международных онлайн-расследований и экстрадиции преступников остаются неясными. Также остается открытым вопрос, как найти баланс между обеспечением кибербезопасности и защитой прав человека в соответствии с принципами правового государства.

Последнее заседание Специального комитета пройдет в Нью-Йорке в конце января 2024 года. Если консенсус не будет достигнут, конвенция может быть принята большинством в две трети и представлена на рассмотрение Генеральной Ассамблеи этой осенью. Если Запад откажется ее подписать, то продолжит действовать Будапештская конвенция Совета Европы против киберпреступности от 2001 года.

Цифровая торговля и налоги

Ожидания относительно разработки механизмов цифровой торговли и цифрового налогообложения также невелики.

В феврале 2024 года в Абу-Даби (ОАЭ) состоялось 13-е министерское совещание Всемирной торговой организации (ВТО). В 2017 году 71 страна, представляющая 90% мировой цифровой торговли, договорились в Совместном заявлении на Всемирном экономическом форуме в Давосе начать работу по разработке соглашения вместо моратория на таможенные пошлины и сборы за трансграничный поток данных. В заявлении подчеркнуто намерение начать переговоры по торговым аспектам электронной коммерции в рамках ВТО и стремление к высоким стандартам, основанным на существующих соглашениях и структурах ВТО, с участием как можно большего числа её членов. В заявлении также отмечается признание уникальных возможностей и вызовов, стоящих перед членами ВТО, включая развивающиеся страны.

Планировалось завершить переговоры к 2020 году, но из-за принципиальных разногласий и пандемии процесс затянулся. Комитет по электронной коммерции ВТО, который совместно возглавляют Сингапур, Япония и Австралия, заявил в декабре 2023 года, что окончательное соглашение может быть достигнуто вскоре после встречи в Абу-Даби. У них есть договоренность по 13 вопросам повестки дня в трех ключевых направлениях: содействие цифровой торговле, открытие цифрового пространства и повышение доверия бизнеса и потребителей.

Однако переговоры были омрачены заявлением торгового представителя США Кэтрин Тай (Katherine Tai) от 25 октября 2023 года, в котором говорится, что США больше не заинтересованы в таком соглашении. Даже американские эксперты, такие как Фиона Александер (Fiona Alexander), которая более 20 лет вела переговоры по цифровой политике от имени Министерства торговли США в ООН, Международном союзе электросвязи, ОЭСР и ICANN, были удивлены и задались вопросом, а не отказались ли США от глобального цифрового лидерства? По мнению Александер, решение Тай противоречит обязательству администрации Байдена противостоять усилиям по расколу глобального Интернета и получению выгод от свободного потока данных, как было условлено на саммите «Большой семерки» 2023 года в Хиросиме. Китай, напротив, подтвердил свою поддержку цифрового торгового соглашения в рамках ВТО. Иными словами, здесь также наблюдается растущее непонимание.

То же можно сказать и о прогрессе в вопросах цифрового налогообложения. Два года назад «Большая двадцатка» и ОЭСР отметили важное соглашение в рамках Инклюзивной рабочей группы по минимизации утечки налогов и перераспределению прибыли. Рабочая группа включает в себя два основных принципа. Но не стоит рассчитывать на запуск цифрового налогообложения в ближайшем будущем, так как реализация этих двух принципов продвигается очень медленно. 11 октября 2023 года ОЭСР и «Большая двадцатка» согласовали Многостороннюю конвенцию о внедрении пункта «А» Первого принципа в качестве первого шага. Конвенция вступит в силу 1 июня 2024 года и за ней последуют дополнительные шаги для остальной части первого и, позднее, второго принципа. Ожидание цифровых налогов становится похоже на ожидание прихода Годо.

От сетей назад к иерархиям?

Помимо «Саммита будущего», в 2024 году нас ожидает множество встреч, на которых ведущие державы вновь обсудят ключевые проблемы неспокойного мира. Даже если вопросы, связанные с Интернетом, сейчас не имеют приоритета на встречах президентов, кибербезопасность, цифровое сотрудничество и управление Интернетом находятся в центре внимания всех форумов высокого уровня.

Саммит «Большой двадцатки» пройдет 1 декабря 2024 года в Рио-де-Жанейро (Бразилия). Саммит «Большой семерки» состоится 13–15 июня 2024 года в Апулии (Италия). В октябре 2024 года Россия примет саммит БРИКС в Казани. Казахстан председательствует в Шанхайской организации сотрудничества (ШОС) и проведет саммит ШОС в 2024 году в Астане. Также ожидаются встречи высокого уровня АСЕАН, АТЭК, ОБСЕ, ОАГ и других организаций, чья повестка неизменно включает вопросы кибербезопасности, цифрового сотрудничества и управления Интернетом.

В рамках «Большой двадцатки» существует Рабочая группа по цифровой экономике, которая планирует провести четыре встречи, включая министерскую. «Большая семерка» проводит ежегодное собрание министров цифровой сферы; ближайшее пройдет 15 марта 2024 года в Вероне (Италия). Россия объявила кибербезопасность и цифровое сотрудничество ключевыми приоритетами саммита БРИКС в Казани. Кроме пятерки первоначальных участников (Бразилия, Россия, Индия, Китай и Южная Африка) к БРИКС присоединились новые: Объединенные Арабские Эмираты, Саудовская Аравия, Египет, Эфиопия и Иран.

На самом деле, существует бесчисленный ряд и других важных экспертных встреч высокого уровня, таких как NetMundial, CyFy, CyCom, Rights Con, Lisbon WebSummit, а также встречи ICANN, IETF и форум IGF, который пройдет в Эр-Рияде (Саудовская Аравия) в декабре 2023 года. Способна ли эта «воздушная карусель управления Интернетом» ускорить поиск общих решений глобальных проблем?

Тридцать лет назад испанский социолог Мануэль Кастельс (Manuel Castells) говорил, что в сетевом обществе формирование политики переходит от «иерархий в ограниченных местах» к «сетям в безграничных пространствах». Однако в последние годы произошел сдвиг в обратном направлении – от многосторонних сетей к межправительственным иерархиям. К сожалению, это привело к усилению поляризации вместо сотрудничества. Было бы неплохо, если бы 2024 год смог повернуть этот тренд вспять.

Об авторе:

Вольфганг Кляйнвехтер, почетный профессор Орхусского университета

Европейский союз на пути к цифровому суверенитету?*

Мадина Касенова

Аннотация:

Настоящая статья продолжает рассмотрение концептуальных подходов Европейского союза («Евросоюз» или «ЕС») в части его стремления создать независимость и автономность европейской цифровой среды в контексте постановки и решения вопроса «европейского цифрового суверенитета» на уровне Евросоюза. Определение роли Евросоюза в поддержании своего «цифрового суверенитета» к 2030 году рассматривается в аспекте реализации ряда общеевропейских проектов, три из которых представлены в кратком изложении, а конкретно, «облачный суверенитет» (Cloud Sovereignty); европейская квантовая экосистема (European Quantum Ecosystem), основанная на передовых квантовых исследованиях; «Европейский Акт о чипах» (European Chip Act).

Ключевые слова:

цифровой суверенитет, цифровая среда, облачный суверенитет, квантовая экосистема

Настоящая статья продолжает рассмотрение концептуальных подходов Европейского союза в части его стремления создать независимость и автономность европейской цифровой среды в контексте постановки и решения вопроса «европейского цифрового суверенитета» на уровне Евросоюза (Digital Sovereignty for Europe / European Digital Sovereignty). Как отмечалось в предыдущей статье [1], понятие «суверенитет» в его современной интерпретации обладает т.н. цифровым измерением, что диверсифицирует его традиционное толкование и включает в содержание этого понятия комплекс взаимосвязанных вопросов – технологических, институциональных, нормативно-правовых и прочее [2]. В этом смысле не удивительно, что «европейский цифровой суверенитет» рассматривается в его различных ипостасях. Значительное число разнородных документов Евросоюза (стратегических, политико-нормативных, правовых, технологических и т.д.), которые предметно затрагивают проблематику «цифрового суверенитета», достаточно вариативно оперируют родственными понятиями, содержащими слово «суверенитет». В одних случаях «цифровой суверенитет» оценивается в дискурсе его тождественности с «технологическим суверенитетом», в других – эти понятия рассматриваются как синонимичные, но требующие разграничения, поскольку «технологический суверенитет» трактуется как способность ЕС обеспечить свою цифровую функциональную автономность посредством продвижения независимых защитных прорывных механизмов (искусственный интеллект, инновационные облачные вычисления и блокчейн, квантовая индустрия и т.д.). В некоторых документах ЕС понятие «цифровой суверенитет» трактуется как более «широкое» по содержанию и охватывающее «технологический суверенитет», «облачный суверенитет» и т.д. [3]

Как представляется, в реалиях настоящего времени едва ли можно претендовать на достаточную определенность и однозначность толкования и понимания того, что содержит в себе понятие «европейский цифровой суверенитет», принимая во внимание терминологическую вариативность его интерпретации. Однако можно констатировать как минимум два важных обстоятельства. Во-первых, потребность обеспечения стратегической автономии в цифровой сфере на уровне Евросоюза учитывает объективность как значительного экономического, социального, конкурентного доминирования GAFA (Google, Apple, Facebook, Amazon) [4], т.к. технологические ориентиры и приоритеты GAFA не всегда подчиняются европейским правилам и нормам, так и принимает во внимание все возрастающее технологическое присутствие Китая в Евросоюзе. Это присутствие расценивается как потенциальная угроза для поддержания и продвижения европейских ценностей, принципов и норм в таких областях, как защита данных, кибербезопасность, этическая разработка искусственного интеллекта и т.д. Логическим следствием является наличие в постоянной повестке Евросоюза вопросов о том, какую роль будет играть Европа в быстро меняющемся мире и что потребуется Европе, чтобы в 2030 году держать свою судьбу в своих руках; как Евросоюз может гарантировать, что Европа не превратится в среднюю державу, зажатую между США и Китаем [5]. Во-вторых, к концу 2023 года *de facto* определились некоторые итоги по ряду масштабных общеевропейских технологических, институциональных, законодательных программ и проектов, запуск которых был осуществлен в Евросоюзе после 2015 года – программа "Horizon 2020"; Европейская стратегия данных 2020 [6];

* Продолжение, начало в № 19

проекты, реализуемые в рамках 5G PPP (*5G Infrastructure Public Private Partnership* [7]); инициативы в рамках проекта «Искусственный интеллект и технологии блокчейна» [8]; разработка программ в рамках Европейского консорциума квантовой индустрии [9] и т.д.

Исходя из суммы изложенных обстоятельств, Евросоюз в настоящее время зафиксировал проблемные зоны, требующие дополнительных инвестиционных мер и финансирования, а также проведение организационных мероприятий на уровне общеевропейских институциональных механизмов для достижения целей «цифрового суверенитета», который в логике его связи с «технологическим суверенитетом» контекстно затрагивает как минимум три аспекта, которые представляют интерес и рассматриваются в кратком изложении ниже, а именно: «облачный суверенитет» (*Cloud Sovereignty*); европейская квантовая экосистема (*European Quantum Ecosystem*), основанная на передовых квантовых исследованиях; «Европейский Акт о чипах» (*European Chip Act*), вступивший в силу в конце сентября 2023 года.

Облачный суверенитет по-разному воспринимается не только на уровне Евросоюза, но также на уровне различных стран-членов ЕС и даже различным образом оценивается отдельными организациями в рамках конкретной страны-члена ЕС. Несмотря на то, что в Евросоюзе не разработано некоего единого, общепринятого определения облачного суверенитета, считается, что его следует рассматривать как безопасный путь к устойчивости и адаптивности, помогающий организациям (публичного и частного сектора) добиться большего контроля и управления своими облачными активами и ресурсами; улучшить соответствие цифровым нормативным требованиям, уменьшая зависимость от поставщиков услуг; как способ повысить эксплуатационную автономность и оперативное реагирование на рабочие нагрузки в облаке в пределах конкретной юрисдикции; как средство комплексного использования преимуществ новых технологий [10]. Такое «громоздкое» понимание облачного суверенитета отнюдь не редкость для разноплановых документов и аналитических исследований в Евросоюзе.

В более обобщенном виде облачный суверенитет характеризуется следующими параметрами:

- сумма связанных с бизнесом политических и технологических аспектов защиты и безопасности данных;
- контроль и независимость от поставщиков коммуникаций, данных, инфраструктуры, операций и программного обеспечения;
- аккумуляция управления, стратегии и технического контроля для обеспечения автономности, гибкости, надежности и соответствия цифровым нормативным требованиям [11].

Суть облачного суверенитета представлена в разработке комплексного структурированного формата с охватом всего облачного стека и в четырех различных измерениях следующих доменов: операционный суверенитет; суверенитет данных; суверенитет программного обеспечения; инфраструктура и коммуникации [12]. Этот структурированный формат облачного суверенитета применим к организациям всех отраслей, независимо от их принадлежности к частному или публичному (государственному) сектору. Кроме того, использование этого структурированного формата пригодно для оценки возможностей любой организации в области облачного суверенитета.

Облачные вычисления стали неотъемлемой частью современного цифрового ландшафта: по некоторым оценкам, к 2025 году 85% предприятий развитых стран будут использовать облачные вычисления в качестве своей основной инфраструктуры. В Евросоюзе не только на уровне общих институциональных органов ЕС, но и в странах-членах ЕС растет финансирование европейского рынка облачных вычислений и облачной среды (*Cloud Environment)*, например, согласно одному из показателей, европейские общедоступные облачные сервисы планируют затраты в размере около 150 миллиардов долларов США на облачные вычисления к концу 2024 года [13].

Операционный суверенитет (Operational Sovereignty)	Операционный суверенитет сфокусирован на предоставлении организации контроля и прозрачности операций поставщиков. Это помогает предотвратить несанкционированный доступ к данным посредством мониторинга и контроля IT-услуг и базовых элементов конфигурации, необходимых для безопасного и эффективного предоставления и эксплуатации облачных услуг, а также согласования с политиками суверенитета.
Суверенитет данных (Data Sovereignty)	Суверенитет данных — это способность организации сохранять контроль над своими данными, в том числе над тем, где и как они хранятся, как они защищаются и обрабатываются, а также кто имеет к ним доступ. Организации могут добиться полного суверенитета над данными только в том случае, если они являются собственниками данных (владеют данными). В иных случаях организации должны основываться на соглашениях и контрактах с третьими лицами, которые ограничивают степень суверенитета, которым они могут обладать.
Суверенитет программного обеспечения (Software Sovereignty)	Суверенитет программного обеспечения означает способность организации организовывать и эксплуатировать решения или ПО независимо от концепции развития продукции изготовителя. Это охватывает сохранение контроля над исходным кодом, процессами разработки и обновлениями программного обеспечения, а также возможность перехода от одного поставщика платформы к другому (т.е. переключение между поставщиками платформ). Такой открытый исходный код также обеспечивает возможность выполнения решений на разных платформах.
Инфраструктура и коммуникации (Infrastructure and communications)	Инфраструктура и коммуникации являются техническими основами суверенитета для операций с данными, а уровни программного обеспечения – средством контроля над операциями с данными. Использование открытых стандартов для инфраструктуры и коммуникаций обеспечивает максимальную адаптивность и устойчивость для перехода от одного сценария суверенитета к другому.

Следует при этом отметить, что в Евросоюзе облачный суверенитет рассматривается в некой релевантной дихотомии: обеспечение дальнейшего развития сугубо европейского облачного рынка и неизбежная технологическая связанность с глобальными участниками цифрового рынка (прежде всего с доминирующими компаниями США, а также с крупными неевропейскими технологическими компаниями) для развития партнерских отношений, учитывающих прерогативы безопасности Европы и европейские ценности. Рамки указанной дихотомии подвижны, и баланс во многом определяется доминированием так называемых гипермасштабных облаков (hyperscaler clouds) [14]. Провайдеры таких «гипермасштабных облаков», именуемые «гипермасштабными провайдерами» (Hyperscale providers), доминируют на рынке облачных вычислений и обладают обширной сетью центров обработки данных и широким спектром услуг. В число «гипермасштабных провайдеров» входит «большая тройка» американских компаний: Amazon Web Services (AWS) [15], Microsoft Azure [16] и Google Cloud Platform (GCP) [17], — которые в совокупности контролируют примерно 65% облачного рынка в целом.

С учетом доминирования «гипермасштабных провайдеров» облачных вычислений Евросоюз использует несколько подходов поддержания облачного суверенитета. Один из подходов – достижение конкурентоспособности европейских облачных вычислений на международном уровне в рамках разработанной инициативы Gaia-X [18], нацеленной на приоритетное развитие европейской облачной инфраструктуры и экосистем данных. Формально Gaia-X действует как некоммерческая ассоциация, в которой ее члены определяют архитектуру и правила, обеспечивают объединенную и безопасную инфраструктуру европейских данных, в которой пользователи сохраняют контроль над доступом к своим данным и их использованием. Это позволяет создавать связи между многими поставщиками облачных услуг в более широкой, прозрачной и справедливой экосистеме, чтобы стимулировать будущую европейскую экономику данных. Следующим подходом являются т.н. страновые инициативы, когда такие страны, как Франция и Германия, работают с национальными поставщиками облачных услуг. Пример Германии и Франции был положительно воспринят другими странами-членами ЕС, и это стимулировало развитие рынка облачных услуг и усилило контроль над данными в национальных юрисдикциях стран-членов ЕС. Еще одним подходом является содействие созданию региональных суверенных облаков (т.е. суверенного облачного пространства данных). В Германии и Испании в 2023 году размещены первые два суверенных региональных облака для Евросоюза, запуск которых осуществила и поддерживает компания Oracle Cloud Infrastructure (OCI) [19].

Облачный суверенитет является одним из инновационных инструментов, посредством которого Евросоюз решает задачу обеспечения своего «технологического суверенитета», поскольку преимущества внедрения облачных технологий оцениваются в ЕС как возможность справиться с рисками безопасности европейских учреждений государственного сектора и потребностями защиты данных широкого круга заинтересованных сторон в масштабе Европы.

Европейская квантовая экосистема (*European Quantum Ecosystem*), основанная на передовых квантовых исследованиях [20], объединяет *de facto* комплекс программ, которые реализуются институциональными структурами, созданными в Евросоюзе для развития коммерческого сектора квантовых технологий. Прежде всего необходимо отметить, что формальный импульс последовательной разработке Европейской квантовой экосистемы был дан в 2016 году, когда был принят «Квантовый манифест» (*The Quantum Manifesto*), сформулировавший общую стратегию для Европы в области квантовых технологий. Через два года (2018) вслед за Квантовым манифестом был создан Флагман квантовых технологий (*Quantum Technologies Flagship*) [21], объединивший европейские исследовательские институты, промышленность и государственные организации ЕС для консолидации передового опыта в области квантовых технологий. Основные исследовательские проекты Флагмана квантовых технологий призваны реализовать четыре ключевых направления: квантовые вычисления, квантовое моделирование, квантовая связь, квантовое зондирование и метрология.

Примечательно, что Европейская комиссия («Еврокомиссия») изначально поддерживала Флагман квантовых технологий в рамках намеченной 10-летней программы финансирования его деятельности (2018–2027 гг.) из бюджета ЕС в размере 1 миллиарда евро, и не менее 500 миллионов евро на период с 2022 по 2027 гг. Принимая во внимание этот факт, Еврокомиссия осуществляет мониторинг инициатив, исследовательских проектов и программ Флагмана квантовых технологий. В 2023 году Еврокомиссия опубликовала промежуточный отчет о результатах и конкретных достижениях квантовых исследовательских проектов Флагмана квантовых технологий [22]. Некоторые ключевые достижения, представленные в отчете Еврокомиссии, включают:

- квантовые вычисления: два стартапа, предлагающие коммерческие решения для квантовых вычислений — AQT (Австрия) и PASQAL (Франция);
- квантовую связь: соединение двух квантовых процессоров через промежуточный узел и установление общей сцепленности между несколькими автономными квантовыми процессорами, образующими квантовую сеть, публикация дорожной карты Европейской инфраструктуры квантовой связи (European Quantum Communication Infrastructure, «Euro QCI») [23], развертывание тестовых стендов для распределения квантовых ключей (quantum key distribution, QKD);
- квантовое моделирование: впервые в мире достигнуто практическое квантовое преимущество в некоторых на-

учных задачах, связанных с изучением новых материалов и фаз материи; два 100-кубитных аналоговых квантовых симулятора устанавливаются в суперкомпьютерных центрах и центрах обработки данных в рамках научно-исследовательского центра Forschungszentrum Jülich (Германия) [24] и исследовательской инфраструктуры Grand Equipment National de Calcul Intensif, GENCI (Франция) [25], что является первым шагом в развертывании общеевропейской гибридной инфраструктуры высокопроизводительных вычислений и квантового моделирования;
- квантовое зондирование: разработка одних из самых совершенных в мире квантовых сенсоров с использованием сверхчистых алмазов;
- фундаментальная квантовая наука: достижение значительного прогресса в разработке нескольких альтернативных вычислительных платформ, включая квантовые вычисления на основе фотоники.

Нацеленность Евросоюза на совершенствование платформ квантовых вычислений и моделирования практического квантового преимущества объясняет расширение институциональных структур для обеспечения широкого взаимодействия и сотрудничества на уровне ЕС по реализации программ и проектов Флагмана квантовых технологий. Об этом свидетельствует, в частности, создание в 2021 году двух организаций: Европейского совместного предприятия по высокопроизводительным вычислениям (*European High Performance Computing Joint Undertaking*, «EuroHPC JU») [26] и некоммерческого Европейского консорциума квантовой индустрии (*European Quantum Industry Consortium*, «QuIC») [27]. С точки зрения Евросоюза, развитию коммерческого сектора квантовых технологий, созданию сильной и динамичной европейской квантовой экосистемы будет способствовать совместное деятельное сотрудничество названных организаций с Европейской инфраструктурой квантовой связи (Euro QCI), а также иными инициативами, объединяющими по всей Европе предприятия малого и среднего бизнеса, крупные корпорации, инвесторов, исследовательские и технологические организации, академические институты.

«Европейский Акт о чипах» – так кратко именуется Регламент (ЕС) 2023/1781 Европейского парламента и Совета от 13 сентября 2023, устанавливающий параметры мер по укреплению европейской полупроводниковой экосистемы и изменяющий Регламент (ЕС) 2021/694 («Акт о чипах») [28]. Акт о чипах вступил в силу в сентябре 2023 года, а сфера его действия распространяется также на страны, не входящие в ЕС, но являющиеся членами Европейской экономической зоны. Принятие Акта о чипах в форме регламента, т.е. законодательного акта вторичного права ЕС, ставит этот юридический акт на самое высокое место в иерархии источников вторичного права ЕС. Регламент обладает тремя юридическими свойствами, отличающими его от других актов: он содержит нормы права, носит обязательный характер, обладает в государствах-членах силой закона и имеет прямое действие на всей территории Евросоюза. Едва ли будет преувеличением отметить, что Акт о чипах, с одной стороны, принят как некий «противовес» растущему технологическому присутствию Китая в Евросоюзе (о чем говорилось в начале настоящей статьи), с другой стороны, призван обеспечить безопасность цепочек поставок в области полупроводниковых технологий и приложений в Евросоюзе, а также удвоить текущую долю ЕС на мировом рынке полупроводниковых технологий – до 20% к 2030 году.

Полупроводники (или чипы) являются существенной основой цифрового рынка и, следовательно, определяют возможности продвижения «цифрового суверенитета». Рынок полупроводников достаточно «узок», а производство полупроводников (чипов) зависит от сложных и глобальных цепочек поставок, стабильность которых в современных условиях весьма уязвима. Акт о чипах направлен на укрепление всей стоимостной цепочки создания чипов в ЕС с учетом существующего глобального дефицита чипов и своеобразной «гонки субсидирования производства чипов» в ключевых региональных центрах. Акт о чипах, в его самом обобщенном изложении, основывается на трехкомпонентной структуре:

- поддержка крупномасштабного наращивания технологического потенциала и инноваций в экосистеме чипов ЕС;
- повышение безопасности поставок полупроводников в Евросоюзе;
- создание механизма мониторинга и реагирования на возможные кризисные ситуации.

Для реализации Акта о чипах и при возникновении кризисных ситуаций при поставках чипов Еврокомиссия наделяется широкими полномочиями, которые предусматривают применение трех типов чрезвычайных мер, а именно: запрашивать у организаций и компаний соответствующую информацию; предписывать организациям и компаниям определять приоритетность заказов на кризисную продукцию; осуществлять совместные закупки от имени государств-членов. Кроме того, Еврокомиссии в практическом плане предоставлено право налагать административные меры если организации и компании не соблюдают императивные предписания; к примеру, такие административные меры включают наложение разовых и периодических штрафных санкций в размере до 300 тысяч евро в зависимости от характера нарушения [29].

Ответы на вопросы, сформулированные в начале настоящей статьи и связанные с определением роли Евросоюза в поддержании своего «цифрового суверенитета» к 2030 году, в том числе, следует увязывать с реализацией тех проектов, которые были в кратком изложении представлены в предыдущей и настоящей статьях.

Список литературы:

[1] «Интернет изнутри» № 19 (ноябрь 2023). С. 41-44

[2] Madiega T. Towards a more resilient EU. Digital sovereignty for Europe. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[3] См., например, Digital Sovereignty Steps Towards a New System of Internet Governance. URL: https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance

[4] GAFA (иногда – GAFAM). URL: https://www.techtarget.com/whatis/definition/GAFA

[5] См. например, European Strategy and Policy Analysis System (ESPAS). Global Trends to 2030. Challenges and Choices for Europe. URL: https://espas.secure.europarl.europa.eu/orbis/system/files/generated/document/en/ESPAS_Report2019_V14.pdf

[6] 2020 European data strategy. URL: https://ec.europa.eu/commission/presscorner/api/files/attachment/862109/European_data_strategy_en.pdf.pdf

[7] 5G Infrastructure Public Private Partnership. URL:https://5g-ppp.eu

[8] Artificial Intelligence, Blockchain and Future of Europe. URL: https://www.eib.org/en/publications/online/all/ai-blockchain-and-future-of-europe-report$ The Artificial Intelligence and Blockchain Technologies initiative. URL: https://www.eif.org/what_we_do/equity/efsi/index.htm

[9] The European Quantum Industry Consortium (QuIC). URL: https://qt.eu/ecosystem/industry/quic

[10] Cloud sovereignty — Driving resilience and adaptability through cloud sovereignty. URL: https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/cloud/deloitte_article_souverainete_cloud.pdf

[11] Barroca J.G., Buxo A., Bruno Batista B.S. Cloud sovereignty: Three imperatives for the European public sector. URL: https://www2.deloitte.com/xe/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html

[12] См. подробнее, например, The cloud Sovereignty framework – four distinct dimensions. URL: https://www2.deloitte.com/xe/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html

[13] IDC, European cloud. URL: https://www.idc.com/getdoc.jsp?containerId=prEUR250293723

[14] Используется и иное название – «гиперскейлерные облака», «гиперскейлерные поставщики»

[15] Amazon Web Services https://aws.amazon.com/ru/contact-us/?nc2=h_header

[16] Microsoft Azure https://azure.microsoft.com/ru-ru

[17] Google Cloud Platform https://cloud.google.com/contact/?_gl=1*wszhg2*_up*MQ..&gclid=CjwKCAiAuYuvBhApEiwAzq_YiWU4fi22JoXiG1dlCMKCbVzgkwWfADN2b76VdSPJATusXESdlwA3fhoC-H4QAvD_BwE&gclsrc=aw.ds

[18] Janosch Delcker and Melissa Heikkila, Germany, France launch Gaia-X platform in bid for 'tech sovereignty,' https://gaia-x.eu/event/gaia-x-2023-summit

[19] Oracle Cloud Infrastructure's (OCI). URL: https://www.oracle.com/cloud/gartner-mq-strategic-cloud-platform-services-leader. См. также Scott Twaddle, Introducing Oracle's sovereign cloud regions for the European Union. URL: https://blogs.oracle.com/cloud-infrastructure/post/introducing-oracles-sovereign-cloud-regions-for-the-european-union

[20] Формирование цифрового будущего Европы. URL: https://digital-strategy.ec.europa.eu/en/policies/quantum

[21] Quantum Technologies Flagship. URL: https://qt.eu/about-quantum-flagship

[22] Quantum Tech Flagship Report. URL: https://digital-strategy.ec.europa.eu/en/news/quantum-tech-flagship-ramp-phase-report

[23] European Quantum Communication Infrastructure (EuroQCI) Initiative. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[24] Forschungszentrum Jülich. URL: https://www.fagsi.com/de/produktlinien/fagsi-procomfort/forschungszentrum-juelich/?gad_source=1&gclid=CjwKCAiAuYuvBhApEiwAzq_Yidmk3QjSKDYuhyzDnde7DJGoOJ_78hTraiM3lDRBuI5GRok1vBTGGxoCIvQQAvD_BwE

[25] Grand Equipment National de Calcul Intensif. URL: https://genci.fr/en/learn-about-genci/about-us

[26] Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1173

[27] The European Quantum Industry Consortium (QuIC). URL: https://qt.eu/ecosystem/industry/quic

[28] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.229.01.0001.01.ENG

[29] Анализ содержания Акта о чипах, см., например, URL: https://insightplus.bakermckenzie.com/bm/international-commercial-trade/international-the-european-union-chips-act-redrawing-the-european-union-semiconductor-industrys-map-with-new-opportunities-and-risks-for-nordic-companies

Об авторе:

Мадина Балташевна Касенова, доктор юридических наук, профессор кафедры теории и истории частного права ФГБН «Исследовательский центр частного права имени С.С. Алексеева при Президенте РФ»

РосНИИРОС: как всё начиналось

30-летию домена .ru посвящается

Про историю домена .ru написано достаточно много, но редакция журнала «Интернет изнутри» решила узнать из первых рук, почему именно Российскому НИИ развития общественных сетей (РосНИИРОС) была передана ответственность за домены .ru и .su. Рассказать о том, как это произошло, а также о конкретных людях, которые в РосНИИРОС и в Координационной группе приложили свои знания и силы для запуска регистрации доменов в зоне .ru, участвовали в формировании правил регистрации, внедрении новых технологий, разрабатывали принципы работы с пользователями, мы попросили **Алексея Дмитриевича Лесникова,** заместителя директора РосНИИРОС в 1992-2000 годах.

Сотрудники РосНИИРОС.

— Алексей Дмитриевич, расскажите, как получилось, что именно РосНИИРОС стал организацией, ответственной за домен .ru?

В 1992 году в международную организацию IANA, которая регистрирует домены разных стран, было направлено сразу три заявки на администрирование зоны .ru — от двух крупнейших на тот момент интернет-провайдеров — «Релкома» и «Демоса», а также от академической сети FREEnet (на базе Института органической химии РАН). IANA предложила заявителям договориться между собой и определить того, кому будет предоставлено право начать регистрацию в домене .ru.

Более года шло обсуждение, и 4 декабря 1993 года семь ведущих на тот момент интернет-провайдеров России подписали **Протокол собрания ведущих провайдеров о передаче полномочий по администрированию домена .ru РосНИИРОС,** где констатировалось, что ответственность за домен .ru передается РосНИИРОС как некоммерческой независимой организации, работающей в сфере компьютерных сетей. Также в протоколе было зафиксировано решение организовать консультативный орган, в который войдут все заинтересованные стороны, для координации административной деятельности домена .ru.

— Но все же — почему был выбран именно РосНИИРОС, молодая организация, которой на тот момент не исполнилось еще и двух лет от «рождения»?

К декабрю 1993 года РосНИИРОС как некоммерческая организация уже обеспечивал ведение реестра домена .su и выполнял функции регистратуры IP-адресов, выделяя IP-адреса по заявкам организаций России. Эта деятельность была очень близкой к регистрации доменов зоне .ru.

А также уже успешно работала Ассоциация RELARN, которую РосНИИРОС создал для выполнения задачи, поставленной **Государственным Комитетом РСФСР по делам науки и высшей школы,** по обеспечению возможности пользования услугами

PROTOCOL

of the meeting of IP service providers:
Demos Plus, Techno, GlasNet, SovAm Teleport,
EUnet/Relcom, X-Atom
with the participation of RosNIIROS/RELARN

The representatives of IP service providers - Demos Plus, Techno, GlasNet, SovAm Teleport, EUnet/Relcom, X-Atom discussed the questions concerning the administration of RU domain and decided that responsibility for this domain should be handled to RosNIIROS as the non-commercial independent organization working in the field of computer networking. Now RosNIIROS is responsible for SU domain and performs the role of IP Registry for xSU/RU zone.

The representatives of service providers mentioned above decided to organize the Consultative Commitee which will include all interested sides to coordinate the RU domain administrative activities.

On behalf of service providers:

Demos Plus — Vladimir Molchanov

Techno — Andrew Romanov

GlasNet — Pavel Prokopenko

SovAm Teleport — Andrew Kolesnikov

EUnet/Relcom — Oleg Tabarovsky

X-Atom — Andrew Bobyshev

04.12.93

On behalf of RosNIIROS: Alexei Platonov

FREEnet/SUNEARN/UNICOM-Russia Andrej Mendkovich

Протокол собрания ведущих провайдеров о передаче полномочий по администрированию домена .ru РосНИИРОС.

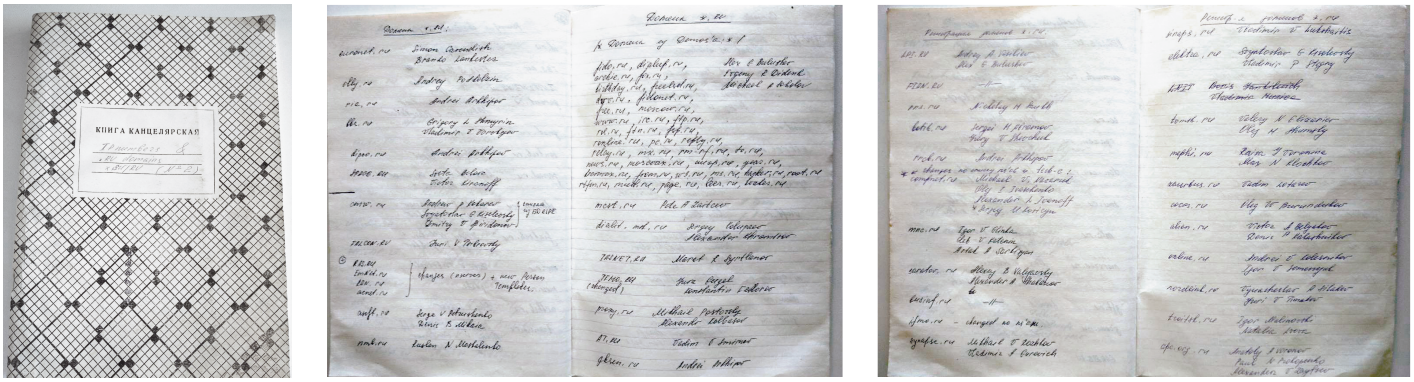
Российский научно-исследовательский институт развития общественных сетей (РосНИИРОС) был зарегистрирован 21 января 1992 года в качестве некоммерческой организации, его учредители: Государственный Комитет РСФСР по делам науки и высшей школы, Институт атомной энергии (ИАЭ) им. Курчатова и Информационно-вычислительный центр ИАЭ им. Курчатова.

электронной почты научным и учебным организациям России. Такие услуги в то время предоставляла только сеть RELCOM, оператором которой был ИВЦ ИАЭ им. Курчатова. В сентябре 1992 года была создана **Ассоциация RELARN**. Было организовано взаимодействие с коммерческими узлами сети RELCOM. Эти узлы предоставляли услуги электронной почты и осуществляли сбор статистики потребления почтовых услуг научными и учебными организациями (членами Ассоциации RELARN). Узлы сети RELCOM за оказанные услуги получали оплату через единый расчётный центр — из денег, выделяемых на эти цели Министерством науки и технической политики РФ, еще примерно 50% услуг сеть RELCOM предоставила бесплатно. Доступ к электронной почте получили более 800 научных и учебных организации России. Работали они через 80 коммерческих узлов сети RELCOM.

Благодаря проектам ведения реестра домена .su, выполнения функции регистратуры IP-адресов и деятельности Ассоциации RELARN мы получили опыт взаимодействия практически со всеми организациями России, которые на тот момент оказывали телекоммуникационные услуги. Кроме того, РосНИИРОС получил опыт, создав передовую для нашей страны базу данных с автоматической загрузкой входных данных, их обработкой, автоматическим формированием финансовых отчётов и отправкой их участникам проекта: членам ассоциации, узлам RELCOM, в центральный офис сети RELCOM и в Миннауки. И, наконец, было налажено взаимодействие с очень широким кругом научных и учебных организаций России (более 800 организаций). Этот опыт, а также неком-

Руководство РосНИИРОС.
Слева направо: **Алексей Платонов, Ирина Рассолова, Елена Воронина, Алексей Лесников.**

Сотрудники РосНИИРОС — сотрудники группы, занимавшейся выделением IP-адресов.
Слева направо, первый ряд: **Елена Лаухина, Елена Яснопольская;** второй ряд: **Лариса Юркина, Сергей Зимин.**



Знаменитая тетрадка Светланы Лобановой.

мерческий статус РосНИИРОС определили, что ответственность за домен .ru была возложена на РосНИИРОС.

— Да, опыт и в самом деле уникальный. И, конечно, он был использован и в дальнейших проектах РосНИИРОС, которых было немало?

Конечно. Так, с 1992 мы занимались созданием сети **RELARN-IP** для науки и образования. Было создано восемь узлов в городах России, подключено более 80 институтов и университетов с использованием скоростных каналов. Проект на полную мощность заработал уже в 1995 году. В дальнейшем сеть RELARN-IP вошла в сеть RBNET.

В 1993 году РосНИИРОС подготовил **проект создания высокоскоростной опорной сети** обмена данными и подключения к ней научных и учебных организаций Москвы, проложил все оптические кабели. Позднее единая сеть была разделена на северную (NMBB) и южную (ЮМОС) части. Оператором северной части сети (NMBB) стал РосНИИРОС. К 1996 году на севере Москвы было создано 14 узлов, соединённых высокоскоростными оптическими каналами связи и работающих по технологии FDDI, к ним были подключены организации науки и образования.

Ну а в 1995 году появилось на свет одно из продолжающих и сегодня развиваться детищ РосНИИРОС: сеть обмена трафиком между провайдерами **MSK-IX (Московский Internet Exchange)**. В 1995-1996 годах были созданы узлы в Москве и Санкт-Петербурге, подключены первые 15 российских интернет-провайдеров. Именно тогда были заложены основы современного MSK-IX: отлажена технология обмена трафиком, система подключения и обслуживания интернет-провайдеров. В дальнейшем проект MSK-IX был выделен из РосНИИРОС в отдельную некоммерческую организацию. Сейчас сеть состоит из 45 узлов, размещённых в 10 городах России.

Сотрудники РосНИИРОС, работавшие с клиентами RELARN, RBNET, NMBB, MSK-IX.
Слева направо, первый ряд: **Алла Мордовина, Ольга Самойлова, Мария Баранова;**
второй ряд: **Александр Славинский, Александр Греков.**

Конец 90-х также был ознаменован появлением сети для науки и образования **RBNET**. В 1995-1997 годах создано 30 узлов в разных регионах России, подключены научные и образовательные сети этих регионов. **В 1996 году трафик сети RBNET по объёму занимал третье место среди всех сетей России, включая коммерческие**.

Участие в этих некоммерческих проектах привело к тому, что все организации, оказывавшие в России услуги Интернета, взаимодействовали с РосНИИРОС при реализации тех или иных проектов, знали руководство РосНИИРОС, его технических специалистов и понимали значение его некоммерческого статуса. Всё в целом это определило их доверие к РосНИИРОС.

— Седьмого апреля 1994 года домен .ru был делегирован, и РосНИИРОС сразу же стал, по сути, его оператором. Что это означало для вас? Какие были сложности?

Сразу после делегирования появилась возможность регистрировать в .ru домены второго уровня, и, конечно, мы получили первые заявки. **В 1994-1995 годах** заявки на регистрацию доменов приходили только от провайдеров телекоммуникационных услуг. Заявок было мало, приходили они в простой текстовой форме, обрабатывала первые заявки и заносила в тетрадь Светлана Лобанова, делегировал домены тоже вручную сотрудник Techno Сергей Турчин.

В начале 1996 года началось быстрое развитие Интернета в России, и, разумеется, поток заявок увеличился до нескольких штук в день. Именно тогда появилась необходимость разработки публичных правил регистрации, а также формы заявки на регистрацию, в которой данные были бы структурированы, что позволяло заносить их в базу данных автоматически.

Для формирования правил регистрации доменов в зоне .ru была создана Координационная группа (КГ). На начальном этапе, в 1996-1997 годах, в неё входили представители провайдеров, подписавших 4 декабря1993 года Протокол собрания ведущих провайдеров о передаче полномочий по администрированию домена .ru РосНИИРОС, в основном, технические специалисты, и их помощь была очень ценна. И некоторых из них мне бы хотелось сейчас упомянуть.

Галина Коваленко работала системным инженером в Techno, а потом в Demos, хорошо разбиралась в технических вопросах, очень хорошо формулировала положения с технической информацией в документах для широкого круга пользователей, долгое время была секретарем КГ.

Владимир Молчанов (Demos, «РосНет») долгое время был председателем КГ, объединителем и искателем компромисса в решениях КГ.

Игорь Семенюк (SovamTeleport) отлично формулировал положения правил и прекрасно разбирался в технических вопросах.

Также запомнились самые активные члены КГ — **Олег Табаровский** (Relcom, Techno), **Сергей Турчин** (Relcom, Techno), **Александр Щербаков** (MSUNet), **Дмитрий Сидельников** (FreeNet), **Андрей Романов** (Techno, в дальнейшем директор Координационного центра национального домена сети Интернет с 2005 по 2009 годы, а теперь заместитель директора КЦ), **Сергей Мухин** («РосНет»), **Кирилл Аношин** («РосНет»), **Александр Зайцев** (GlasNet), **Михаил Коротаев** (Demos), **Мария Степанова** (Relcom, в дальнейшем директор КЦ с 2001 по 2005 годы).

— В 2021 году, когда отмечалось 20-летие Координационного центра доменов .RU/.РФ, вы говорили, что в основе правил регистрации лежали правила пользования метрополитеном. Неужели это правда?

В целом – да, правила пользования метрополитеном были по структуре очень логичны и понятны: права, обязанности и ответственность сторон, правила проезда, провоза, тарифы и пр. Взята за основу была структура правил пользования метрополитеном, а наполнение, конечно же, полностью было новым.

В начале 1996 года запросов на регистрацию доменов было немного (до 10 в день), принимались заявки только от юридических лиц. Заявителям рекомендовалось, чтобы имя домена соответствовало названию организации, а в случае явного несовпадения в заявке должно было содержаться обоснование на регистрацию запрашиваемого доменного имени. Срока действия регистрации доменного имени не существовало, и решение о прекращении делегирования домена принималось путём голосования членов КГ. Все заявки направлялись на всех членов Координационной группы. Заявки находились на рассмотрении КГ в течение пяти рабочих дней, если кто-либо из членов КГ был против регистрации какого-либо домена, то вопрос решался большинством голосов при голосовании по электронной почте. Если в течение пяти дней приходили две заявки на одно доменное имя, то заявителям предлагалось решить между собой, кому будет принадлежать домен. Регистрация домена иностранными организациями допускалась только при наличии резидентного в России администратора домена или технического специалиста, осуществляющего ведение регистрируемого домена.

Таким способом домены регистрировались примерно до августа 1996 года, до тех пор, пока количество заявок на регистрацию за день не превысило 100 штук. Такое количество заявок члены КГ уже не могли физически рассмотреть в течение одного дня, у каждого из них была ещё загрузка по их основному месту работы.

И, кстати, до 1997 года регистрация доменных имён в .ru была бесплатной.

— И тогда понадобилось пересмотреть правила регистрации?

Да, правила регистрации доменных имён изменялись и совершенствовались непрерывно. Так, в конце 1996 года в соответствии с изменениями в правила домен стал регистрироваться на первого, приславшего заявку, были созданы списки географических доменов и правила их ведения, сформирован стоп-лист доменов, которые нельзя регистрировать, изменена форма заявки. Заявка больше не поступала на членов КГ, а направлялась сразу на рассмотрение сотрудниками РосНИИРОС и далее на регистрацию и делегирование.

В 1997 году поток заявок на регистрацию значительно увеличился, и была введена плата за регистрацию доменов. Установили срок регистрации домена, определили процедуру снятия делегирования и аннулирования регистрации в случае неоплаты продления срока регистрации домена.

В начале 1998 года разрешили регистрировать домены на физических лиц, завершили формирование списка географических доменов и стоп-листа, разрешили регистрировать имена собственные. РосНИИРОС технически реализовал систему работы с партнёрами, оказывающими услуги по регистрации доменов конечным пользователям. Многие из партнёров в дальнейшем стали регистраторами.

— Вы говорите про появление института распределённой регистрации? А как вы считаете, это в принципе была правильная идея? Есть же достаточно крупные национальные домены, где никакой распределённой регистрации нет, и все доменные имена регистрируются через национальную регистратуру.

Безусловно, это была правильная идея. У сообщества было большое желание участвовать не только в написании правил, но и в процессе регистрации, и уже в 1999 году стало понятно, что надо переходить на схему распределённой регистрации доменов, которая позволяла развивать бизнес регистрации и другим провайдерам интернет-услуг.

Кроме того, Интернет стал заметен, и государство начало обсуждать необходимость и возможные формы регулирования Интернета. Толчком перехода к распределённой регистрации, к созданию Координационного центра и участию в его работе государства стало совещание тогдашнего премьер-министра Владимира Путина с российским интернет-сообществом, которое прошло 28 декабря 1999 года. После совещания было определено, что вопросы по управлению Интернетом должны согласовываться в рамках общественного обсуждения, определён список организаций, с участием которых проводятся обсуждения. Этими организациями стали РосНИИРОС, АДЭ, СОИ и РОЦИТ, а Министерство по связи и информатизации определено в качестве наблюдателя.

В 2000 году в соответствии с поручением после этого совещания РосНИИРОС, АДЭ, СОИ и РОЦИТ решили создать Коор-

динационный центр национального домена сети Интернет (КЦ, cctld.ru), став его учредителями, а представитель Министерства связи и информатизации РФ был приглашён в Совет КЦ в качестве наблюдателя с правом вето.

Система регистрации РосНИИРОС была преобразована и стала распределённой. Она, как и ранее, обеспечивала ведение реестра доменов .ru, их делегирование, но добавилась возможность работы множества регистраторов. Первым таким регистратором в январе 2001 года стала некоммерческая организация АНО RU-CENTER, созданная из числа сотрудников РосНИИРОС.

— И РосНИИРОС передал свои полномочия новой организации? Никто не возражал против такого развития событий?

РосНИИРОС перестал регистрировать новые домены, но оставил у себя функции поддержки ранее зарегистрированных через него доменов. Так было до тех пор, пока все домены не были переданы от него новым регистраторам. В 2001 году был зарегистрирован Координационный центр, и РосНИИРОС сразу передал ему функции формирования правил регистрации, а Координационная группа вошла в состав КЦ в качестве одной из рабочих групп. В 2006 году РосНИИРОС полностью передал в КЦ ответственность за домен .ru, оформив КЦ в международной базе данных IANA в качестве администратора домена.

В июне 2001 года заработала система распределённой регистрации, функции регистрации доменных имён второго уровня были переданы от РосНИИРОС к регистраторам — независимым компаниям, профессионально занимающимся регистрацией доменных имён в домене .ru, аккредитацией которых занимался КЦ. В настоящее время услуги по регистрации доменов оказывает 131 регистратор.

В 2009 году КЦ и «Фонд Развития Интернет» создали ЗАО «Технический центр Интернет» (ТЦИ). Специалистами РосНИИРОС для ТЦИ была разработана новая система регистрации и делегирования доменов, включая систему работы с регистраторами. На работу в ТЦИ перешли часть специалистов из РосНИИРОС, а первым директором ТЦИ стал тогдашний директор РосНИИРОС Алексей Платонов — для обеспечения преемственности и гарантий работоспособности системы.

В 2010 году Координационный центр национального домена сети Интернет заключил с ЗАО «Технический центр Интернет» договор на обслуживание главного реестра и системы регистрации доменов верхнего уровня. Таким образом, обслуживание реестра .ru было передано от РосНИИРОС в ТЦИ.

— Вы сказали, что часть специалистов РосНИИРОС перешли на работу в ТЦИ. Не жаль было расставаться с сотрудниками?

Сотрудники — это основная ценность компании. Силу компании составляют знания сотрудников, их творческий подход, интерес к делу, когда каждый работает на интересном для него месте, когда вектор желаемого развития сотрудника совпадает с направлением развития компании. Компания — это целостный живой взаимосвязанный организм, где каждый сотрудник — это его частичка. Отдавать сотрудников больно, но в случае с ТЦИ было необходимо, т.к. это позволило запустить работу системы регистрации плавно и надёжно для регистраторов.

Очень хочется рассказать о некоторых сотрудниках, которые в первые годы жизни РосНИИРОС жили на работе, своими силами и творчеством создавали РосНИИРОС.

Алексей Павлович Платонов — Душа, Сердце и Мозг РосНИИРОС, его бессменный директор. Безусловно, то, что нам дали возможность реализовывать такие большие проекты, — его заслуга. Все первые проекты середины 90-х годов, включая их техническую часть, он обосновывал и согласовывал за пределами РосНИИРОС сам. Он давал сотрудникам свободу для действий и право на ошибку, и благодаря этому они могли реализовать себя. Алексей Павлович имеет настолько большой внутренний потенциал, что легко идёт на уступки, и в итоге это приводит к позитивным результатам.

Первыми техническими специалистами РосНИИРОС были Владимир Добрецов, Андрей Доброцветов и Михаил Всеволодов. До прихода в РосНИИРОС они работали в Курчатовском институте и занимались физическими исследованиями. Эти сотрудники заложили не только техническую и технологическую базу работы в РосНИИРОС, но и сформировали многие принципы работы, основанной на самостоятельности, доведении начатого дела до результата, описания сделанного для более простого освоения накопленного опыта новыми сотрудниками.

Владимир Добрецов (1992-1994) готовил для Ассоциации RELARN базу данных на Oracle и систему автоматической загрузки в неё данных, получаемых по электронной почте. Создавал систему для обработки статистики, формы для автоматической рассылки данных для узлов сети RELCOM и членов RELARN, статистику для Министерства. Специалистов, которые делали такие проекты, в России в то время было очень мало, и в основном они работали в вычислительном центре Курчатовского института. Заместитель директора института математики им. Стеклова, будучи представителем института в ассоциации RELARN, увидев наши наработки, говорил, что это сделать просто невозможно... Владимир Добрецов проработал в РосНИИРОС не очень долго, но вклад его в культуру работы РосНИИРОС очень большой.

Андрей Доброцветов (1992-2001 работал в РосНИИРОС, далее и по настоящее время — в RU-CENTER) создавал внутреннюю сеть РосНИИРОС, заложил и реализовал принципы сетевой безопасности работы сотрудников, создавал внутренние почтовые сервисы с резервированием и распределением потоков приходящих и уходящих писем, позволяющим избежать последствий атак на серверы. В 2004 году появилась почта от Google, и, тестируя их инфраструктуру, мы увидели у них структуру серверов, аналогичную той, что мы использовали в РосНИИРОС. Андрей Доброцветов создавал сетевую инфраструктуру для сети RELARN-IP, инфраструктуру Московского, Санкт-Петербургского (MSK-IX, SPB-IX) и других узлов обмена трафиком, инфраструктуру сети RBNET, северную часть Московской опорной сети (NMBB) для науки и образования, систему защищённых и высоконагрузочных DNS-серверов для домена .ru.

Михаил Всеволодов (1992 — н.в.) начал с освоения только что появившихся веб-технологий и создал сайт РосНИИРОС (www.ripn.net), ставший одним из пяти первых веб-сайтов, созданных в России. В дальнейшем Михаил создавал инструменты для организации работы сотрудников: были созданы сервисы во внутренней сети РосНИИРОС для размещения служебной информации и ведения проектов. Сервисы имели систему поддержки версий, систему ограничения доступа и прочие технологические новшества. Сейчас это выглядит привычно, но 30 лет назад это были передовые решения. К 1998 году у нас было более 1500 текстовых документов (инструкций), фиксирующих договорённости о том, как мы работаем и как обрабатываем нестандартные ситуации!

Самые первые сотрудники: Светлана Лобанова, Юлия Демидова, Алла Мордовина. На их плечи легли первые контакты с членами Ассоциации RELARN, первые регистрации и делегирования доменов. Светлана Лобанова на начальном этапе занималась регистрацией доменов, занося новые домены в тетрадь.

В 1994-1996 годах начали работать в РосНИИРОС Елена Благовещенская, Мария Коротаева, Ольга Самойлова. В 1997-1998 годах в группу работы с клиентами пришли Ольга Вакуленко, Ольга Яковлева, Янина Зеегофер, Лариса Шевченко, Екатерина Дернова, Галина Козлова.

Сложная работа по проверке домена на ненормативную лексику досталась **Елене Благовещенской**, она добавляла слова в стоплист и говорила, что даже не представляла, что существует такое разнообразие ненормативных слов в русском языке.

Мария Коротаева по своей внутренней сущности — человек, который помогает другим людям, поэтому, когда появился

Сотрудники РосНИИРОС — группа поддержки клиентов, регистрирующих домены.

Слева направо, первый ряд: **Светлана Есина, Ольга Федченко, Ольга Иваненко, Юлия Лоткова, Валентина Фурукина, Наталия Платонова, Мария Кузнецова;**

второй ряд: **Дмитрий Зиханов, Марина Брик, Ольга Семенюк, Ольга Вакуленко, Янина Зеегофер, Александра Охрименко, Ольга Яковлева, Светлана Лобанова;**

третий ряд: **Алексей Ефимов, Алексей Градюшко, Виктория Жигальцова, Галина Козлова, Анна Суханова.**

внешний офис, она пошла работать туда, в непосредственном контакте с клиентами. Много клиентов приезжали в офис и хотели, чтобы с ними работала только Мария Коротаева, стояли к ней в очередь.

Ольга Самойлова работала с клиентами RELARN, NMBB, MSK-IX, RBNET, организовывала ежегодные конференции RELARN, была секретарём и директором Ассоциации RELARN.

Ольга Вакуленко — организатор службы работы с клиентами, в её подчинении было более 100 человек.

Ольга Яковлева сначала работала руководителем группы учёта оплаты за домены, потом руководителем отдела развития услуг в RU-CENTER, сейчас начальник проектного отдела в КЦ, руководитель проектов от Бога, вникающая и понимающая проект с технической стороны, со стороны клиента, со стороны бухгалтерии, юристов и пр.

Янина Зеегофер — руководитель службы работы с клиентами, несла тяжесть текущего руководства группами, работающими с клиентами.

Первую автоматическую систему регистрации РосНИИРОС начинал делать **Алексей Колисниченко**, а продолжил работы и запустил систему в эксплуатацию **Алексей Другов.** Система регистрации при его участии начала нормально работать, дала возможность девушкам из службы работы с клиентами выдерживать всё нарастающий поток заявок. Алексей Другов развивал систему один, а когда он в начале 2000-х ушел из РосНИИРОС, всю ответственность за развитие системы регистрации взяли на себя только что закончившие МФТИ Сергей Петров и Павел Ильичёв. С их приходом мы вздохнули свободно, система оказалась в надёжных руках.

Сергей Петров — уникальный человек и специалист, очень глубокий и вдумчивый. Может решить любую задачу, качественно, глубоко в неё вникнув и как минимум в два раза быстрее, чем другие. Как-то я спросил у него, каков алгоритм проверки правильности ИНН, он задумался и сказал: «Это скалярное произведение векторов в десятимерном пространстве...» Для меня это было очень неожиданно в применении к ИНН. Работал системным архитектором, сейчас работает в ТЦИ.

Павел Ильичёв — руководитель отдела разработки расчётных систем и функциональных её модулей, очень ответственный, доводящий начатые дела до завершения специалист. Сейчас продолжает работать в RU-CENTER.

Марина Цитович — начальник департамента разработки информационных систем в RU-CENTER. При ней все технические работы были формализованы, создана масштабируемая структура, позволяющая реализовывать технические проекты любой сложности.

Александр Ильин пришёл в РосНИИРОС в 1997 сразу после окончания МФТИ. Работал в группе построения сетей. После выделения из РосНИИРОС инфраструктуры RU-CENTER остался в РосНИИРОС и стал начальником отдела построения сетей,

Сотрудники РосНИИРОС — разработчики сервисов.
Слева направо, первый ряд: **Дмитрий Канаев, Михил Всеволодов, Павел Храмцов, Александр Щербаков;**
второй ряд: **Сергей Баукин, Сергей Зимин, Павел Ильичёв, Константин Вышегородцев;**
третий ряд: **Михаил Аронов, Екатерина Кирсанова, Станислав Брик, Марина Цитович, Сергей Петров.**

Сотрудники РосНИИРОС — бухгалтерия.
Слева направо, первый ряд: **Алина Гаврилова, Ирина Рассолова, Татьяна Потанина;**
второй ряд: **Татьяна Нестеренко, Елена Сычёва, Анна Дергунова, Светлана Сахарова.**

через его руки прошли все проекты РосНИИРОС, а потом и MSK-IX. Сейчас технический директор АО MSK-IX.

Антон Коротин также пришёл в РосНИИРОС в 1997 после окончания МФТИ. Занимался построением высоконагрузочных систем для DNS. Рано ушёл из жизни.

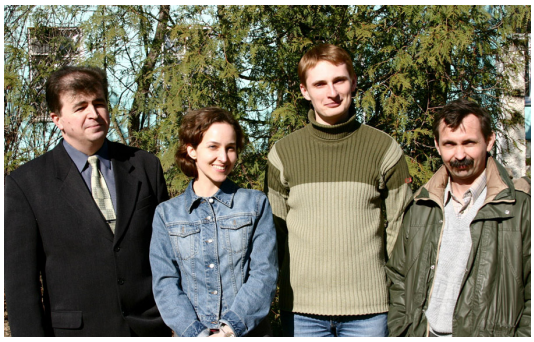
Дмитрий Кравчук в 1997-1999 годах создавал и развивал Личный кабинет для клиентов, регистрирующих домены. На первых порах он делал это один и при этом ещё успевал одновременно развивать свой ресурс stihi.ru. В дальнейшем развитие Личного кабинета для клиентов было передано в подразделение Марины Цитович.

Ирина Рассолова — главный бухгалтер РосНИИРОС со дня его создания, а после создания RU-CENTER стала его главным бухгалтером. С ней очень комфортно работать, всегда есть ощущение надёжности и опоры. Умеет организовать работу в подразделении так, что каждый сотрудник чувствует себя на своём месте, компетентным и с возможностью развития.

потом в RU-CENTER — директором департамента маркетинга, сейчас работает в MSK-IX руководителем проектов.

Андрей Воробьёв — руководитель отдела PR в РосНИИРОС, потом директор PR-департамента в RU-CENTER, с 2015 года директор КЦ. Очень творческий, энергичный, активный, очень хорошо понимающий людей и влияние внешних событий на ситуацию вокруг компании. Умеет находить нестандартные варианты решений в разных ситуациях, формировать позитивный внутренний и внешний имидж компании, объединять сотрудников компании и организовывать работу своих подчинённых.

Сотрудники РосНИИРОС — группа NOC – управление сетями.
Слева направо: **Евгений Кускевич, Александр Ильин, Антон Коротин, Андрей Стихеев.**



Сотрудники РосНИИРОС — группа по связям с общественностью и маркетингу.
Справа налево: **Павел Храмцов, Андрей Воробьев, Анастасия Чистякова.**

Елена Герцева — руководитель юридического отдела в РосНИИРОС, потом директор юридического департамента в RU-CENTER. В 1998 году благодаря её усилиям как консультанта были внесены очень непростые изменения в договор на регистрацию доменов — с этой задачей не могли справиться другие юристы. А с 1999 года уже в качестве штатного сотрудника Елена Герцева занялась начавшимися уже тогда судебными спорами по доменным именам.

Павел Храмцов — в нём объединены глубокие технические знания, умение писать и интересные книги, и грамотные документы, видение направлений развития, аналитический склад ума. В РосНИИРОС работал начальником отдела маркетинга,

Нам всем повезло, что мы работали в компании, статус которой как некоммерческой организации позволил нам, не задумываясь о прибыли, разумно с технической точки зрения, качественно и надёжно прокладывать оптику, строить сети, регистрировать домены, человечно выстраивать в коллективе отношения поддержки, творчества, постоянного развития и обновления.

После того как RU-CENTER преобразовался в коммерческую организацию, наши сотрудники просили меня дать им считаемую цель, лучше в деньгах, а я им отвечал, что не дам, и что наша цель — работать так, чтобы нам всем было интересно, а деньги тогда придут сами... Так работал РосНИИРОС.

Новости науки и техники

Министерство обороны Франции выделит до 500 миллионов евро на разработку квантовых компьютеров

Основными сферами применения квантовых вычислений в оборонной сфере названы коммуникации и криптография

Министерство обороны Франции объявило о заключении долгосрочных контрактов с пятью стартапами — Alice & Bob, C12, Pasqal, Quandela и Quobly. Эти компании признаны ключевыми игроками в области исследования и развития квантовых вычислений в стране. Сумма ассигнований, выделяемых на этот проект, составит до 500 миллионов евро. Решение в очередной раз подтверждает серьёзность намерений Франции выйти на лидирующие позиции в сфере квантовых вычислений.

Три года назад президент Эммануэль Макрон заявил о разработке национальной квантовой стратегии, необходимой для закрепления страны на передовом рубеже научных исследований. А год спустя стало известно о планах создания во Франции гибридной сети квантовых вычислений, которая объединит традиционные вычислительные системы и квантовые компьютеры. Предполагается, что доступ к ней получат научные учреждения, технологические стартапы и промышленные компании, которые станут партнерами проекта.

В сообщении Министерства обороны подчёркивается, что квантовые технологии имеют исключительно важное значение для вооружённых сил. Основными сферами их применения названы коммуникации и криптография. Координировать работу проекта будет агентство оборонных цифровых технологий AND. Его представители уверены, что компании, с которыми заключены контракты, имеют все возможности решить стоящую перед ними задачу. В то же время они понимают, что в процессе решения участникам проекта предстоит преодолеть немалые трудности. По этой причине проект является долгосрочным: через четыре года предполагается отобрать три наиболее перспективных технологии. А в 2032 году проект сосредоточится уже на двух наиболее успешных технологиях с целью их дальнейшего развития и практической реализации. Последняя подразумевает сначала создание прототипов квантовых компьютеров со 128 логическими кубитами, а затем и коммерческих систем с 2048 кубитами.

Источник: C4ISNET
https://www.c4isrnet.com/battlefield-tech/2024/03/07/french-defense-ministry-picks-startups-to-develop-quantum-computers/

Как квантовые вычисления повлияют на авторское право?

Неожиданный аспект развития квантовых технологий рассмотрели в своей работе британские юристы

Разговоры о квантовых вычислениях остаются по преимуществу прерогативой физиков, математиков и IT-специалистов. Однако считать, что квантовые компьютеры никого больше не интересуют, было бы огромной ошибкой. Их появление станет настоящей революцией во всех областях жизни, и последствия этой революции необходимо прогнозировать уже сейчас. Этим и занимаются многие учёные — в том числе в такой, казалось бы, сугубо гуманитарной отрасли, как юриспруденция. Группа специалистов Школы права Эксетерского университета (Великобритания) опубликовала статью, в которой размышляет о будущем влиянии квантовых вычислений на проблемы авторского права.

По мнению ведущего автора статьи, профессора Джеймса Гриффина (James Griffin), квантовые вычисления одновременно создают и предпосылки для более эффективной борьбы с нарушением авторских прав, и возможности для злоупотреблений. Экспоненциальный рост скорости вычислений, который принесут квантовые компьютеры, позволит быстрее и точнее определять авторство различных произведений и отслеживать случаи их полного или частичного несанкционированного использования третьими сторонами. Также вычислительные возможности квантовых компьютеров помогут юристам точнее устанавливать сам факт нарушения авторских прав, определяя, является ли нарушением та или иная форма использования.

С другой стороны, лавинообразный рост вычислительных возможностей создаст и предпосылки для более быстрого тиражирования и распространения произведений или их фрагментов. Следует также помнить и о возможности объединения функций квантовых вычислений и генеративных моделей искусственного интеллекта. Это позволит создавать новые тексты, музыкальные произведения, изображения или фильмы на основе уже существующих — и в этой ситуации вопрос о соблюдении авторских прав будет стоять очень остро.

Кроме того, в будущем наверняка возникнет и проблема авторских прав в отношении контента, создаваемого для самих квантовых компьютеров. В качестве примера Гриффин приводит сценарий компьютерной игры для квантового компьютера. С учётом вероятностной природы квантовых вычислений и действий игроков он может меняться произвольным образом, в том числе и выходя за рамки изначального авторского замысла.

Все эти вопросы требуют от юристов, работающих в области авторских и смежных прав, уже сейчас задуматься над новыми механизмами защиты и новыми формулировками законодательных актов.

Источник: The Quantum Insider
https://thequantuminsider.com/2024/03/07/study-quantum-computing-will-radically-alter-copyright-law-application/

Компания HP анонсировала выпуск компьютеров с защитой от квантовых кибератак

Квантовые компьютеры ещё не стали реальностью, но готовиться к их использованию в атаках необходимо уже сейчас

Компания Hewlett-Packard (HP) анонсировала выпуск партии «бизнес-компьютеров» с защитой аппаратного обеспечения от квантовых кибератак. Современные методы криптографической защиты основываются на асимметричном шифровании, взлом которого существующими вычислительными ресурсами не представляется возможным. Однако эпоха квантовых вычислений уже не за горами, а возможности квантовых вычислений многократно выше. Почти треть экспертов индустрии полагают, что уже в 2033 году с вероятностью 50% появятся квантовые компьютеры, чьи вычислительные возможности релевантны уровню современной криптографии — cryptographically relevant quantum computers (CRQC). Более того, научные прорывы в различных областях исследований могут и существенно повысить эту вероятность, и сократить этот срок.

Появление CRQC поставит под вопрос само понятие цифрового доверия, сделав уязвимыми цифровые подписи программного и аппаратного обеспечения. И многие страны уже на правительственном уровне работают над стратегиями защиты от квантовых кибератак. Так, власти Нидерландов настаивают на том, чтобы предприятия критической инфраструктуры незамедлительно начинали переход на постквантовую криптографию. Схожие указания разработаны и правительством США, они подразумевают, что для систем, имеющих дело с конфиденциальными данными, переход на постквантовую криптографию становится желательным уже в 2025 году и обязательным с 2030 года.

Перевод всей цифровой вселенной на новый стандарт криптографии — огромная задача, которую невозможно решить одномоментно. Но если программное обеспечение может получать обновления безопасности, с аппаратным обеспечением это невозможно. А ненадёжность его криптографической защиты потенциально позволяет злоумышленникам установить полный контроль над устройством и всеми хранящимися на нём данными.

Чтобы помочь решить эту проблему, компания HP начнёт выпуск серии «бизнес-компьютеров» с опцией защиты от квантовых кибератак. Её обеспечивает микрочип Endpoint Security Controller (ESC) — собственная разработка HP, уже давно используемая в продуктах компании. Пятое поколение этого чипа обладает новыми функциями. Изолированный от процессора и операционной системы ESC создаёт аппаратную платформу, обеспечивающую безопасность средствами криптографии, устойчивыми к квантовым кибератакам. По уверениям создателей, их разработка является уникальной, а использующие её компьютеры станут первыми в мире устройствами, защищёнными от квантовых кибератак на аппаратном уровне.

Источник: HP
https://press.hp.com/us/en/press-releases/2024/hp-unveils-largest-portfolio-ai-pc.html

Компания Kvantify представила коммерческий продукт для вычисления скорости высвобождения молекул действующего вещества в лекарственных препаратах

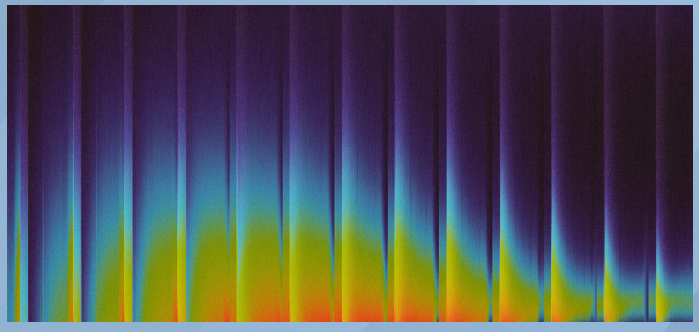
Kvantify Koffee обещает тратить несколько минут на то, на что требуются месяцы лабораторных исследований

Датская компания Kvantify объявила о выпуске своего первого коммерческого продукта. Компания специализируется в области квантовых вычислений и математического моделирования процессов в различных отраслях — от телекоммуникаций и логистики до фармакологии. Ранее специалисты Kvantify разработали квантовый алгоритм FAST-VQE, который уже успешно зарекомендовал себя в области квантовой химии.

Новинка от Kvantify адресована фармацевтическим компаниям. Kvantify Koffee осуществляет вычисление кинетики высвобождения молекул действующих веществ в составе лекарственных препаратов. Этот параметр является одним из ключевых при разработке новых лекарственных средств, и традиционно его значения устанавливаются в ходе длительных лабораторных исследований. Kvantify Koffee осуществляет расчёты кинетики высвобождения одной молекулы за несколько минут — время, достаточное для приготовления чашки кофе, что и дало продукту его несколько необычное название.

Появление Kvantify Koffee на рынке обещает фармацевтическим компаниям огромную экономию времени и средств, которые тратятся сегодня на лабораторные исследования кинетики высвобождения. Вычисления осуществляются традиционными методами, а также с использованием эмуляции квантовых вычислений. Но в компании заявляют, что продукт вполне готов и к переходу на квантовые вычисления, что повысит его эффективность и скорость расчетов. «Мы видим свою миссию в решении проблем и нацелены на создание прорывных инструментов, которые имеют реальную ценность для бизнеса непосредственно сейчас. И Kvantify Koffee в полной мере отвечает этому видению нашей миссии», — заявил один из основателей и руководитель Kvantify Ханс Хенрик Кнудсен (Hans Henrik Knudsen).

Источник: The Quantum Insider
https://thequantuminsider.com/2024/03/07/kvantify-launches-its-first-product-to-improve-drug-discovery/



ICANN79 Community Forum: краткий обзор

79-я конференция ICANN проходила 2-7 марта 2024 года в столице Пуэрто-Рико Сан-Хуане. Офлайн-участие в ICANN79 приняли около 1100 человек из 106 стран, ещё 526 человек зарегистрировались для участия онлайн – из них больше 300 человек посетили форум впервые. В течение шести дней работы форума прошло 199 секций.

Салли Костертон (Sally Costerton), врио президента и главный исполнительный директор ICANN, выступая на открытии форума 4 марта, подчеркнула важность миссии ICANN: ***«ICANN состоит из людей, представляющих разные сектора, поколения и мнения. У нас бывают разногласия по многим вопросам, но миссия – это та причина, по которой все члены нашего сообщества собрались здесь сегодня. Наша миссия — не просто заявления и декларации, это движущая сила, которая выходит за пределы разногласий и объединяет нас вокруг единой цели. Наша вера в общую миссию помогает нам преодолевать трудности и достигать консенсуса. И именно это позволяет нам поддерживать наше единство».***

Четвёртого марта на ICANN79 прошел традиционный **TechDay**, организатором которого является Организация поддержки национальных доменов (ccNSO). В ходе TechDay участники обсудили новые сервисы, инновационные подходы и масштабирование опыта работы регистратур, а также поделились последними новостями.

Модератором технического семинара в очередной раз выступил **Эберхард Лиссе** (Eberhard Lisse) – глава технической рабочей группы ccNSO и управляющий директор Namibian Network Information Centre, регистратуры домена верхнего уровня Намибии .na.

Первым докладчиком стал **Фред Невес** (Fred Neves), представитель LACTLD – региональной организации, объединяющей администраторов доменов верхнего уровня стран Латинской Америки и Карибского бассейна. Он представил облачный Anycast DNS-сервис – бесплатный проект, функционирующий с 2015 года и открытый для внешних организаций.

Представитель Hostmaster UA, регистратуры национального домена Украины .ua, **Дмитро Кохманюк** (Dmytro Kohmanyuk) рассказал о миграции DNS-инфраструктуры украинской регистратуры в части DNSSEC с open source-решения Bind на Knot от чешской регистратуры CZNIC. Предпосылкой к миграции послужили выявленные в ходе аудита текущего технического решения слабые места. Он также обозначил предпринятые в ходе миграции шаги, трудности и ошибки, возникающие в процессе, и поделился сделанными выводами по итогам пройденного пути.

Гэвин Броун (Gavin Brown), главный инженер технической службы GDS ICANN, представил новый сервис ICANN Registry System Testing 2.0, который должен заменить предшествующий ему Pre-Delegation Testing. Сервис предназначен для оценки готовности инфраструктуры оператора (или потенциального оператора) домена верхнего уровня и представляет собой набор автоматизированных тестов для каждой критической функции системы регистрации. Предыдущий сервис нуждался в переработке в преддверии грядущего нового раунда регистраций new gTLD, так как не содержал некоторых значимых аспектов, например, поддержки тестов RDAP.

На второй сессии TechDay **Тара Вален** (Tara Whalen), вице-председатель Консультативного комитета по вопросам безопасности и стабильности ICANN (SSAC), рассказала о деятельности Комитета и обновлённом составе. Она сообщила, что SSAC ищет новых членов – в частности, в Комитете нет участников из стран Африки, Латинской Америки и Карибского бассейна, а Азиатско-тихоокеанский регион представлен крайне немногочисленно.

Доктор **Сион Ллойд** (Dr. Sion Lloyd), главный специалист по безопасности, стабильности и отказоустойчивости технического офиса ICANN, представил эволюцию широко известного проекта Domain Abuse Activity Reporting (DAAR) – проект Domain Metrica. В сравнении с DAAR проект Domain Metrica имеет архитектуру, дающую возможность подключать новые модули по мере необходимости, объединяет в себе большее число измерительных методик, является более гибким и прозрачным инструментом и обладает всеми преимуществами облачного решения. Первый релиз ожидается в третьем квартале 2024 года.

Третья сессия TechDay прошла в формате круглого стола и была посвящена проблемам внедрения и использования единых электронных идентификаторов. Первая часть круглого стола была организована как Tour de Table, в ходе которого участники поделились опытом внедрения электронных идентификаторов и работы с ними в своих странах, а затем обсудили с аудиторией возможности масштабирования опыта на все интернет-сообщество и использование имеющихся в наличии у ICANN инструментов, таких как RDAP, DANE и других.

В заключительной четвёртой части технического дня выступил представитель принимающей стороны конференции – исполнительный вице-президент регистратуры национального домена Пуэрто-Рико доктор **Пабло Родригез** (Dr. Pablo Rodríguez). Он рассказал о домене .pr, способах его продвижения, ценообразовании, совместной работе с хостинг-провайдерами и используемом программном стеке.

Джефф Бедсер (Jeff Bedser), представитель CleanDNS, выступил с презентацией, посвящённой методикам измерения DNS Abuse. Он отметил, что необходимо уделять больше внимания не подсчёту случаев возникновения DNS Abuse, а попытаться измерить их влияние и оценить последствия каждого такого случая.

В завершении TechDay состоялось выступление руководителя подразделения DNS-сервисов Packet Clearing House **Эллисон Манкин** (Allison Mankin). Она рассказала об инновационном подходе использования технологии DANE для криптографической верификации цифровых эмблем, таких как, например, красный крест, с помощью которых могут быть промаркированы почтовые серверы медицинских организаций или электронное медицинское оборудование.

Участники **семинара по DNSSEC и безопасности**, который также состоялся 4 марта, обсудили вопросы цифрового доверия, как технического, так и человеческого, борьбу с дез-

информацией в Глобальной сети, экосистему доверенных реестров и возможности их применения для противодействия разного рода мошенничеству в Интернете. Кроме того, в ходе семинара были подняты вопросы взаимосвязанности классической иерархичной системы доменных имен DNS и децентрализованной системы имен BNS (blockchain name system). Участники обсудили, должны ли быть зависимости между этими двумя пространствами имён или они могут существовать независимо друг от друга, а также к каким техническим коллизиям и проблемам может привести подобное параллельное сосуществование.

Бари Лейба (Barry Leiba), представитель обновленной Leadership Team Консультативного комитета ICANN по вопросам безопасности и стабильности (SSAC), выступил с обзором отчёта SSAC №123, посвящённого эволюции разрешения доменных имён в пространстве Глобальной сети. Развитие децентрализованных альтернатив классической иерархической системы DNS, которая была разработана в 80-х годах, связано с рядом её недостатков в современных реалиях. Докладчик особенно подчеркнул, что основными рекомендациями комитета правлению ICANN являются необходимость постоянно отслеживать появление альтернативных протоколов, использующих пространство доменных имён, и усилия по смягчению последствий и снижению рисков, присущих сосуществованию нескольких пространств имён и протоколов.

Пятого марта в рамках 79-й конференции ICANN состоялась секция ccNSO, посвящённая фрагментации Интернета. Эксперты рассмотрели различные аспекты фрагментации Сети, а также внесли свои предложения по борьбе с ней. Также были затронуты проблемы, с которыми сталкиваются правительства и организации при обеспечении баланса между национальными интересами и глобальным взаимодействием. Участники уделили особое внимание важности продвижения подхода к управлению Интернетом с участием многих заинтересованных сторон и обеспечению защиты прав человека, конфиденциальности и безопасности в Интернете.

Модератором секции стала **Аннелиз Уильямс** (Annaliese Williams) (.au), председатель Комитета по вопросам управления Интернетом (Internet Governance Liaison Committee) ccNSO. В ходе секции участники обсудили работу Стратегической сети по фрагментации Интернета (Policy Network on Internet Fragmentation, PNIF) — межсессионного мероприятия IGF, основным направлением деятельности которого является обсуждение и повышение осведомленности о технических, политических, правовых и нормативных мерах и действиях, представляющих риск для открытого и взаимосвязанного Интернета. Целями PNIF на двухлетний период является следующее: предложение систематической и всеобъемлющей основы для определения фрагментации Сети, её преднамеренных и непреднамеренных причин, а также потенциальных последствий; сбор и анализ тематических исследований; установление общих принципов, рекомендаций или кодексов поведения, позволяющих предотвратить фрагментацию.

Бруна Мартинс дос Сантос (Bruna Martins dos Santos) (PNIF) в своем выступлении отметила, что не нужно создавать новые органы в сфере управления Интернетом, но необходимо улучшить координацию между существующими. Отсутствие взаимодействия между организациями, которые занимаются вопросами управления Интернетом, и органами, разрабатывающими стандарты, может привести к фрагментации Интернета, выражающейся в разрозненных и дублирующих друг друга правилах и требованиях.

«Фрагментация может создавать негативные последствия для всего глобального сообщества, как на техническом уровне, так на и уровне взаимодействия с конечными пользователями», — заключила Бруна Мартинс.

Она также представила меры, которые помогут предотвратить фрагментацию Интернета, среди которых:

- предотвращение дублирования мандатов организаций, занимающихся выработкой политики в области управления Интернетом;
- отказ от закрытых форумов с эксклюзивным участием;
- принятие необходимых мер на соответствующем уровне.

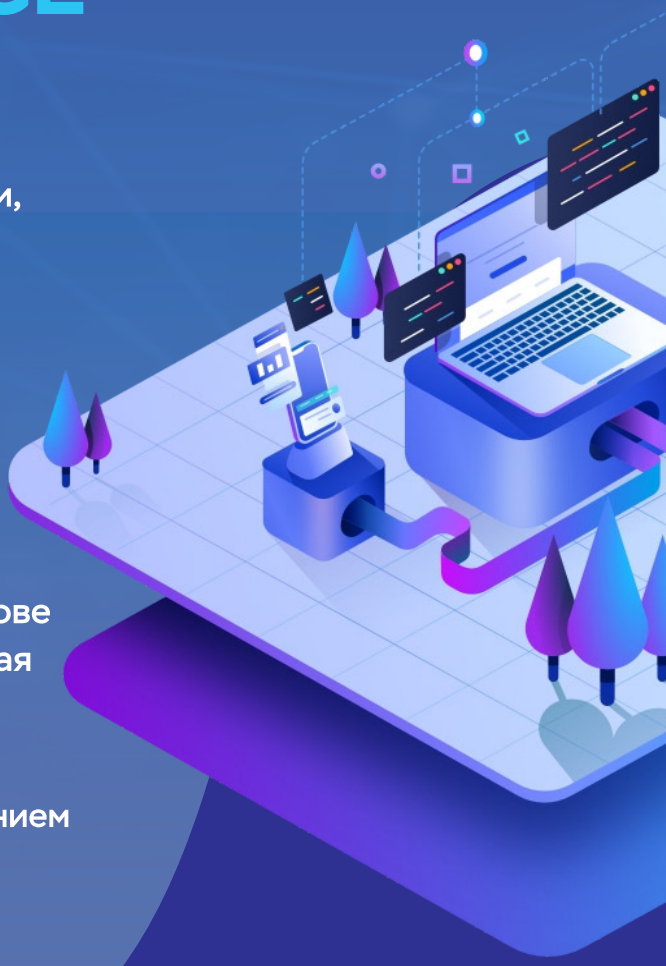
Деми Гечко (Demi Getschko) (.br) представил видение Руководящего комитета Бразилии по Интернету (CGI.br) касательно фрагментации Интернета. В частности, по мнению эксперта, не должны меняться принципы, лежащие в основе Глобальной сети, такие как свобода, сетевой нейтралитет, безопасность и стабильность, права человека, демократическое управление на основе сотрудничества и инклюзивность.

«Хотелось бы напомнить слова знаменитого писателя Гилберта Кита Честертона: “Мы учимся делать очень много умных вещей... Следующей великой задачей будет научиться их не делать”», — подытожил эксперт.

Следующая конференция, ICANN80, пройдёт 10-13 июня в Руанде, Кигали. Последняя открытая конференция ICANN, проводившаяся в Африке, состоялась в июне 2019 года, и в этом году ICANN вернётся в регион с ICANN Policy Forum.

MSK IX

СТАНЬТЕ ЧАСТЬЮ КРУПНЕЙШЕГО В РОССИИ СООБЩЕСТВА INTERNET EXCHANGE



- Прямой доступ к интернет-аудитории, контенту и сервисам Рунета
- Прямое подключение в 10 городах России или в любом городе через партнеров
- Многоуровневая архитектура на основе дублированных ядер, обеспечивающая полноценное резервирование
- Синхронизация времени с использованием NTP-сервера MSK-IX (Stratum I)

+7 495 737-92-95

msk-ix.ru

Реклама. Рекламодатель АО «ЦВКС «МСК-IX» ИНН: 7733661269

Интернет изнутри