№20
Апрель 2024

indata
ФОНД РАЗВИТИЯ СЕТЕВЫХ ТЕХНОЛОГИЙ «ИНДАТА»

Интернет изнутри

КВАНТОВЫЕ ТЕХНОЛОГИИ

Содержание:

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

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.

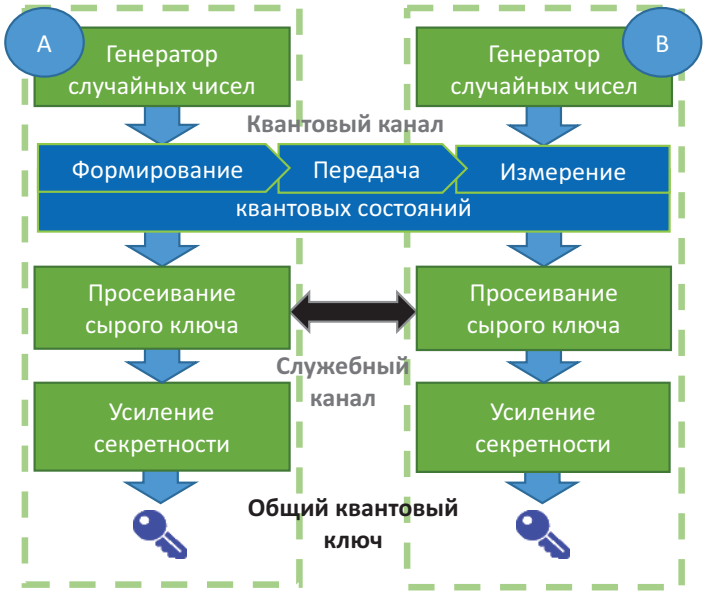


Рис. 1. Обобщённая схема реализации КРК.

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.

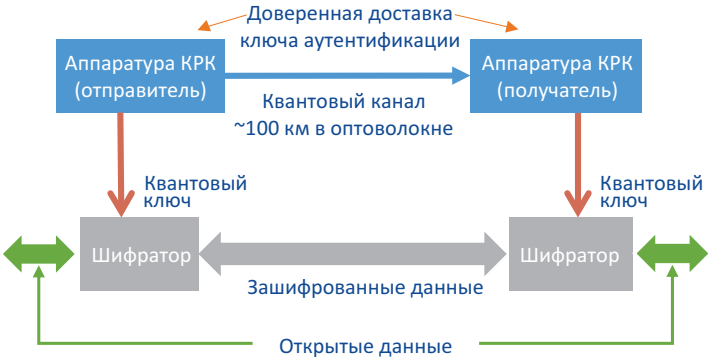


Рис. 2. Защита сетевого трафика в топологии «точка-точка» с помощью КРК.

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).

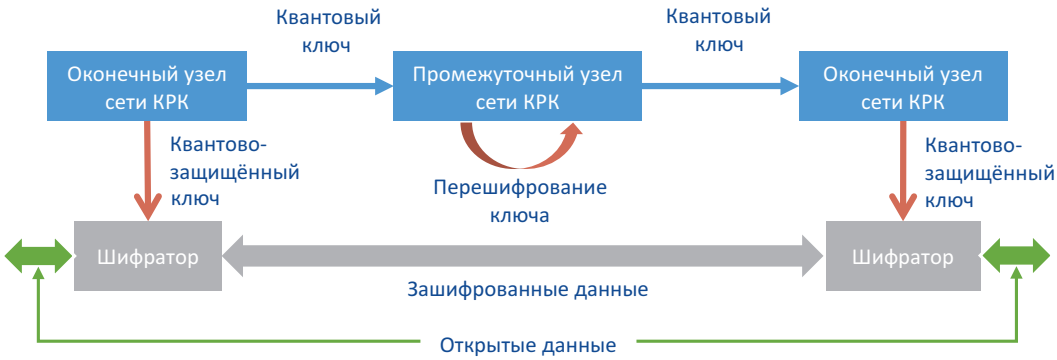


Рис. 3. Перешифрование ключа в магистральной сети КРК с ДПУ.

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)

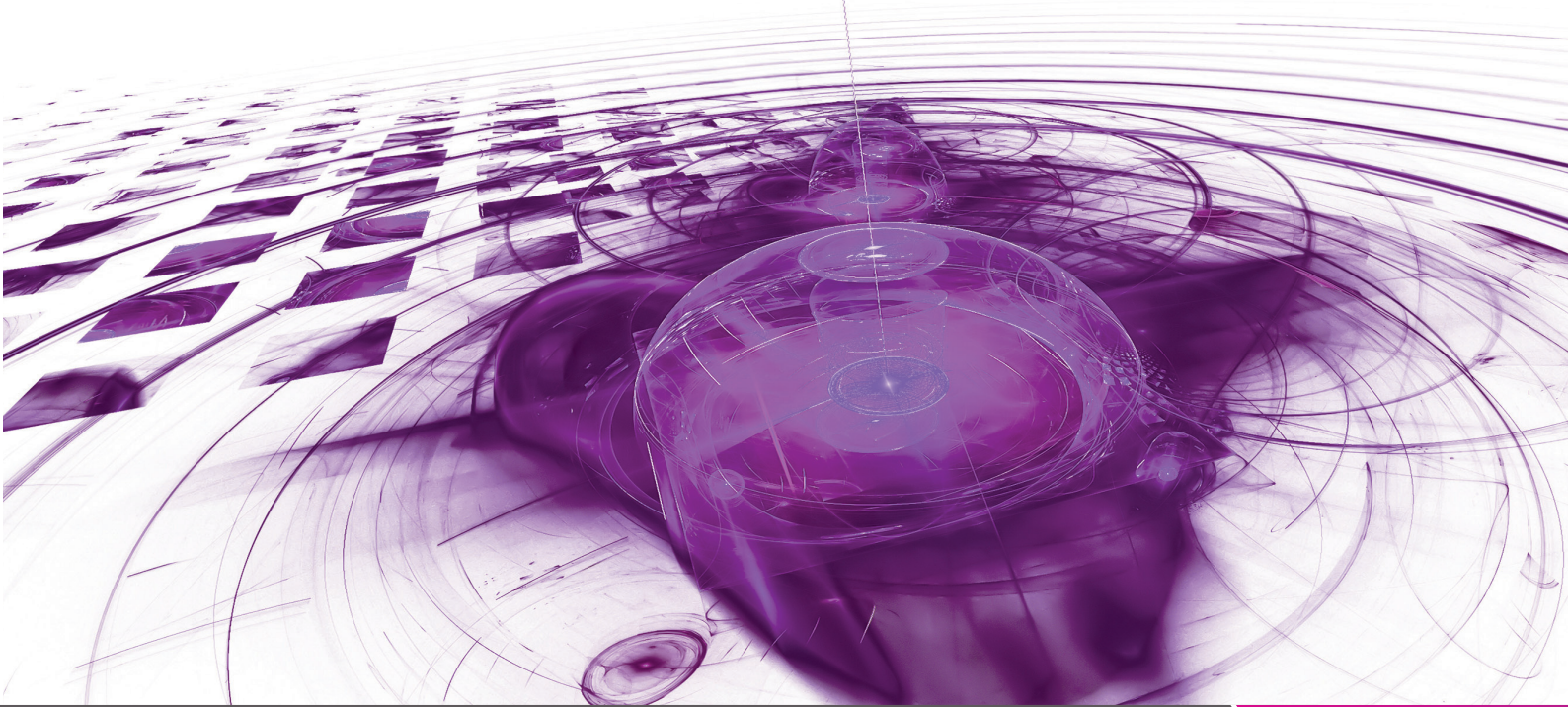
[13] ТУСУР планирует создать квантовую сеть для вузов Большого университета [Электронный ресурс] // РИА Томск 15.02.2024. URL: https://www.riatomsk.ru/article/20240215/69707 (дата обращения: 06.03.2006)

[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



Интернет изнутри