УДК 004.7
doi: 10.21685/2587-7704-2025-10-1-19

Open Access | RESEARCH ARTICLE

Национальные квантовые стандарты как основа квантовых коммуникаций в Российской Федерации

Светлана Евгеньевна Игошина
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
sigoshina@mail.ru.

Андрей Андреевич Карманов
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
starosta07km1@mail.ru

Аннотация. Рассмотрены задачи технического регулирования отрасли квантовых коммуникаций. Одной из ключевых задач является разработка рекомендаций функциональных требований к сетям квантовых криптографических систем выработки и распределения ключей и к техническим способам их достижения. Предполагается, что стандартизация квантовой отрасли послужит драйвером развития путем формирования точных требований к оборудованию в сфере квантовых коммуникаций.

Ключевые слова: квантовые коммуникации, распределение ключей, Международный союз электросвязи

Для цитирования: Игошина С. Е., Карманов А. А. Национальные квантовые стандарты как основа квантовых коммуникаций в Российской Федерации // Инжиниринг и технологии. 2025. Т. 10 (1). С. 1–3. doi: 10.21685/2587-7704-2025-10-1-19

National quantum standards as the basis of quantum communications in the Russian Federation

Svetlana E. Igoshina
Penza State University, 40 Krasnaya Street, Penza, Russia
sigoshina@mail.ru.

Andrey A. Karmanov
Penza State University, 40 Krasnaya Street, Penza, Russia
starosta07km1@mail.ru

Abstract. The paper considers the tasks of technical regulation of the quantum communications industry. One of the key tasks is to develop recommendations for functional requirements for networks of quantum cryptographic key generation and distribution systems (QCKDS) and technical methods for achieving them. It is assumed that standardization of the quantum industry will serve as a driver for development by forming precise requirements for equipment in the field of quantum communications.

Keywords: quantum communications, key distribution, International Telecommunication Union

For citation: Igoshina S.E., Karmanov A.A. National quantum standards as the basis of quantum communi-cations in the Russian Federation = *Engineering and Technology*. 2025;10(1):1–3. (In Russ.). doi: 10.21685/2587-7704-2025-10-1-19

Проблема распределения ключей между парами пользовательских устройств является актуальной научной проблемой, требующей решения в условиях появления новых угроз, связанных с созданием квантового компьютера.

В мире в настоящее время существует несколько десятков разработчиков систем ККС ВРК. В России известны три крупных центра, известных в области квантовых коммуникаций: МГУ имени М. В. Ломоносова совместно с АО «ИнфоТеКС» [1], Российский квантовый центр совместно с ООО «КуРейт» [2] и Национальный исследовательский университет ИТМО совместно с ООО «СМАРТС-Квантелеком» [3, 4]. При этом ККС ВРК разных производителей существенно различаются не только

используемым физическим оборудованием, но и реализуемыми квантовыми криптографическими протоколами выработки и распределения ключей (ККП ВРК). Все это приводит к возникновению принципиально новых задач при интеграции данных систем квантового распределения ключей (КРК) в единую квантовую криптографическую систему. Одной из ключевых задач является разработка рекомендаций функциональных требований к сетям ККС ВРК и к техническим способам их достижения. В связи с интенсивным развитием данного направления, ключевой задачей является разработка рекомендаций функциональных требований к сетям ККС ВРК и к техническим способам их достижения.

В настоящее время ведется работа по разработке документов национальной системы стандартизации в соответствии с планом дорожной карты развития высокотехнологичной области «Квантовые коммуникации» на период до 2030 г. Одним из таких документов будет документ «Рекомендации по стандартизации решений в области организации сетей ККС ВРК и определения функциональных требований к ним». В документе будут установлены требования к многоуровневой структуре и функциям сети КРК.

На основе разработанных требований будет формулироваться методика построения сетей КРК смешанной топологии, включая методику распределения общего секрета на произвольные пары узлов сети и с учетом Рекомендаций по уровням иерархии ККС ВРК с возможностью масштабирования ККС ВРК с учетом положений в ITU-T SG 13 Y.3801.

В направлении стандартизации технологии КРК наблюдается активная работа международных организаций, таких как группа стандартизации ETSI [5], известная результатами популярного известного проекта Secure Communication based on Quantum Cryptography (SECOQC) [6]. Разработанные документы устанавливают стандарты разных областей применения КРК. В настоящее время некоторые стандарты и спецификации, разработанные в 2010 г., требуют дополнения.

С 2019 г. ведутся активные работы по созданию рекомендаций в части управления квантовыми ключами в сетях КРК, в том числе вопросы хранения сгенерированных в сети КРК ключей, распределение ключей между узлами в сети КРК, передача ключей от аппаратуры КРК потребителям.

В 2020 г. Международный союз электросвязи принял рекомендацию «ITU-T SG 13 Y.3801 (ex Y.QKDN-req) Functional requirements for quantum key distribution networks». Согласно положениям ITU-T SG 13 Y.3801, сформированы функциональные требования к каждому квантовому уровню в иерархии ККС ВРК, а также функциональные требования к управлению квантовыми уровнями.

Данная рекомендация – первая принятая Международным союзом электросвязи в области квантовых технологий, для которой были определены функциональные требования к уровневой модели квантовой коммуникационной сети. Особенность построения такой сети заключается в том, что нижние уровни предоставляют ресурс, которым будут пользоваться вышестоящие уровни.

Важным изменением в структуре сети КРК, согласно документу ITU-T SG 13 Y.3801, является выделение специализированного уровня управления сетью КРК (QKD network management layer), реализуемое центром управления сетью, и уровнем контроля за сетью КРК (QKD control layer).

При построении сети КРК появляются новые задачи, направленные на взаимную идентификацию устройств, настройку и мониторинг параметров сети КРК, отвечающих за безопасное функционирование. Важным аспектом является обеспечение требуемых эксплуатационных свойств.

В России в настоящее время решаются задачи возможности построения децентрализованной сети КРК и необходимость решения проблемы распределения общего секрета на произвольные пары узлов сети с обеспечением не только конфиденциальности, но и целостности передаваемой ключевой информации [7], а также уточняются понятия доверия к промежуточным узлам.

Разнообразие проблем информационной безопасности в области глобальных квантовых коммуникационных сетей требует значительного расширения объема разработок и совершенствования как чисто квантовых криптографических устройств, так и комбинированных оптоэлектронных систем, для которых достижения квантовых технологий закрепляются рекомендациями к функциональным требованиям к сетям ККС ВРК и техническим способам их достижения.

Список литературы

1. Борисова А. В., Жиляев А. Е., Алферов С. В., Елисеев В. Л., Кармазиков Ю. В., Климов А. Н., Балыгин К. А. Испытание комплекса квантовой криптографической аппаратуры защиты информации на городских волоконно-оптических линиях связи // Вестник российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 4. С. 100–110.
2. Kiktenko E. O., Pozhar N. O., Duplinskiy A. V., Kanapin A. A., Sokolov A. S., Vorobey S. S., Miller A. V., Ustimchik V. E., Anufriev M. N., Trushechkin A. T., Yunusov R. R., Kurochkin V. L., Kurochkin Yu. V., Fedorov A. K. Demonstration

of a quantum key distribution network in urban fibre-optic communication lines // Quantum Electronics. 2017. Vol. 47, № 9. P. 798.
3. Егоров В. И., Глейм А. В., Рупасов А. В. Система квантового распределения ключа на поднесущих частотах модулированного излучения с компенсацией искажений сигнала // Ученые записки Казанского университета. Серия: Физико-математические науки. 2013. Т. 155, вып. 1. С. 59–65.
4. Глейм А. В., Чистяков В. В., Банник О. И., Егоров В. И., Булдаков Н. В., Васильев А. Б., Гайдаш А. А., Козубов А. В., Смирнов С. В., Кынев С. М., Хоружников С. Э., Козлов С. А., Васильев В. Н. Квантовая коммуникация на боковых частотах со скоростью 1 Мбит/св городской сети // Оптический журнал. 2017. Т. 84, № 6. С. 4–9.
5. Industry Specification Group (ISG) on Quantum Key Distribution for users (QKD) // ETSI. URL: https://www.etsi.org/committee/1430-qkd (дата обращения: 20.09.2020).
6. M. Peev [et al.]. The SECOQC quantum key distributin network in Vienna // New Jour. Of Phys. 2009. Vol. 11. P. 075001.
7. Патент РФ на изобретение RU 2792414 C1. Способ передачи информации между конечными узлами связи через промежуточные узлы без перешифрования / Филиппов А. В., Букин Е. Г., Карманов А. А. ; заявл. 22.03.2023 ; опубл. 11.04.2023.

References

1. Borisova A.V., Zhiljaev A.E., Alferov S.V., Eliseev V.L., Karmazikov Ju.V., Klimov A.N., Balygin K.A. Testing of a complex of quantum cryptographic information security equipment on urban fiber-optic communication lines. *Vestnik rossijskogo novogo universiteta. Serija: Slozhnye sistemy: modeli, analiz i upravlenie = Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* 2019;(4):100–110. (In Russ.)
2. Kiktenko E.O., Pozhar N.O., Duplinsky A.V., Kanapin A.A., Sokolov A.S., Vorobey S.S., Miller A.V., Ustimchik V.E., Anufriev M.N., Trushechkin A.T., Yunusov R.R., Kurochkin V.L., Kurochkin Yu.V., Fedorov A.K. Demonstration of a quantum key distribution network in urban fibre-optic communication lines. *Quantum Electronics*. 2017;47(9):798.
3. Egorov V.I., Glejm A.V., Rupasov A.V. A system of quantum key distribution at subcarrier frequencies of modulated radiation with compensation of signal distortion. *Uchenye zapiski Kazanskogo universiteta. Serija: Fiziko-matematicheskie nauki = Scientific notes of Kazan University. Series: Physical and mathematical sciences*. 2013;155(1):59–65. (In Russ.)
4. Glejm A.V., Chistjakov V.V., Bannik O.I., Egorov V.I., Buldakov N.V., Vasilev A.B., Gajdash A.A., Kozubov A.V., Smirnov S.V., Kynev S.M., Horuzhnikov S.E., Kozlov S.A., Vasilev V.N. Quantum side-band communication with a speed of 1 Mbit/sv of the urban network. *Opticheskij zhurnal = Optical magazine.* 2017;84(6):4–9. (In Russ.)
5. Industry Specification Group (ISG) on Quantum Key Distribution for users (QKD). *ETSI*. Available at: https://www.etsi.org/committee/1430-qkd (accessed 20.09.2020).
6. Peev M. et al. The SECOQC quantum key distributin network in Vienna. *New Jour. Of Phys*. 2009;11:075001.
7. Patent RU 2792414 C1. *A method of transferring information between end nodes of communication through intermediate nodes without re-encryption.* Filippov A.V., Bukin E.G., Karmanov A.A.; appl. 22.03.2023; publ. 11.04.2023. (In Russ.)

Поступила в редакцию / Received 18.03.2025

Принята к публикации / Accepted 07.04.2025