УДК 535.8

# МЕТОДЫ ОПТИМИЗАЦИИ ПРИ СОВМЕСТНОМ РАСПРОСТРАНЕНИИ КВАНТОВЫХ КАНАЛОВ КРКБЧ И ИНФОРМАЦИОННЫХ КАНАЛОВ В ОПТИЧЕСКИХ ТРАНСПОРТНЫХ СЕТЯХ

**Тарабрина А.Д.** (Университет ИТМО),
**Научный руководитель – к. ф.-м. н. Киселев Ф.Д.**
(Университет ИТМО)

**Введение.** В современном мире быстроразвивающихся цифровых технологий особенно остро встает вопрос безопасной передачи данных. Существующие алгоритмы шифрования основаны на вычислительной сложности и в теории могут быть взломаны. Перспективной технологией является квантовое распределение ключа (КРК), обеспечивающее безусловную безопасность обмена информацией. Основным препятствием для широкого внедрения КРК является дороговизна оборудования и необходимость выделения под квантовый сигнал отдельного волокна, поэтому в настоящее время разрабатываются возможные решения этой проблемы. Одно из них – распространение квантовых каналов в одном волокне с информационными при помощи плотного мультиплексирования по длине волны. Однако в таком случае снижается производительность системы КРК из-за того, что мощные информационные каналы порождают шумы (спонтанное комбинационное рассеяние – СКР, четырехволновое смешение – ЧВС), влияющие на квантовый сигнал [1]. Специальным образом выбранное расположение каналов на частотной сетке (конфигурация) минимизирует это влияние [2]. При этом, если рассматривать два узла городской оптической транспортной сети (OTN), между которыми необходимо осуществить КРК, но они не связаны напрямую отрезком оптического волокна, то нужно выбрать маршрут, соединяющий отправителя и получателя через последовательность других узлов сети, так, чтобы производительность системы КРК была как можно выше, а общее количество узлов было наименьшим. В данной работе рассматривается система квантового распределения ключа на боковых частотах (КРКБЧ).

**Основная часть.** Конфигурации каналов, минимизирующие мощность шумов, можно получить методом обоснованного предположения или применяя эвристики, например, алгоритм имитации отжига, в зависимости от параметров системы (количества каналов, шага частотной сетки).

Совместное распространение квантового и информационных каналов в одном волокне наиболее перспективно в городских OTN [3-6], поскольку расстояние между узлами составляет до десятков километров. Простейшая математическая модель городской OTN – граф, в котором вершины представляют собой узлы сети (корпуса университетов, офисы), а ребра есть соединяющие их оптоволоконные линии. Параметр, по которому оценивается производительность системы КРК, – скорость генерации секретного ключа. Участки оптического волокна, соединяющие соседние узлы сети, могут иметь различную длину, количество распространяющихся по ним информационных каналов, следовательно, свой уровень шума и соответствующее значение скорости генерации секретного ключа, которое и определяет вес ребра. Конечная скорость генерации секретного ключа будет ограничена самым медленным участком среди составляющих путь от отправителя к получателю. Чтобы найти оптимальный маршрут, необходимо максимизировать минимальную скорость генерации секретного ключа в пути. Это можно сделать, решив задачу об узком месте на графе. В этой работе задача решается методом полного перебора. Сначала находятся все пути, соединяющие два заданных узла сети. Затем для каждого пути вычисляется самый медленный участок. Оптимальным признается путь, самый медленный участок которого имеет самую высокую скорость генерации секретного ключа среди остальных и содержащий наименьшее количество узлов, если таких путей несколько.

**Выводы.** В итоге проведенной работы найдены оптимальные маршруты линии КРКБЧ между отправителем и получателем в сетях случайных топологий с различным количеством узлов. Применение метода полного перебора ограничивает размер сетей, с которыми можно работать. Для большого количества узлов и динамических сетей есть необходимость использования более эффективных алгоритмов. Результаты данного исследования могут быть использованы при проектировании сетей КРК, интегрированных в существующую инфраструктуру.

**Список использованных источников**:


1. Kiselev F. et al. A theoretical study of subcarrier-wave quantum key distribution system integration with an optical transport network utilizing dense wavelength division multiplexing //Journal of Physics B: Atomic, Molecular and Optical Physics. – 2021. – Т. 54. – №. 13. – С. 135502.Niu J. N. et al.
2. Optimized channel allocation scheme for jointly reducing four-wave mixing and Raman scattering in the DWDM-QKD system //Applied optics. – 2018. – Т. 57. – №. 27. – С. 7987-7996.
3. Perspectives and limitations of QKD integration in metropolitan area networks / Aleksic S. [et al.] // Optics Express. — 2015. — 4. — Vol. 23. — P. 10359.
4. Integration of Quantum Key Distribution in Metropolitan Area Networks / Poppe A. [et al.]. — OSA, 2014. — P. QW4A.6.
5. Quantum metropolitan optical network based on wavelength division multiplexing / Ciurana A. [et al.] // Optics Express. — 2014. — 1. — Vol. 22. — P. 1576.
6. Designing quantum networks using preexisting infrastructure / Rabbie J.[et al.] // npj Quantum Information. — 2022. — Vol. 8. — P. 5.