

УДК 535.012.2

## ОЦЕНКА ПАРАМЕТРОВ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В ОТКРЫТОМ ПРОСТРАНСТВЕ В ЗАВИСИМОСТИ ОТ ВНОСИМЫХ ПОТЕРЬ

Соломатин О.А. (Университет ИТМО), Баловнев Д.Ю. (Университет ИТМО)

Научный руководитель – Наседкин Б.А.  
(Университет ИТМО)

**Введение.** Квантовая криптография, в частности квантовое распределение ключей (КРК) в последнее время стала наиболее развитой отраслью квантовых информационных технологий. КРК позволяет осуществлять распределение ключей, не полагаясь на вычислительную сложность выполнения определенных математических функций, таких как односторонние функции, которые считаются краеугольным камнем классической криптографии с открытым ключом. Опираясь на физические принципы, КРК гарантирует безопасное распределение ключей, даже при условии атаки с использованием квантового компьютера.

Атмосферные оптические линии связи (АОЛС) и оптоволокно являются наиболее часто используемыми каналами передачи систем КРК. АОЛС при необходимости можно легко транспортировать в разные места, в отличие от оптоволоконных линий, которые обычно находятся под землей. Городские атмосферные линии КРК могут быть потенциально применимы для многих организаций, например финансовых, правительственных, расположенных в городских районах и которым требуется защищенный канал связи. Так же данные каналы возможно интегрировать в оптические городские сети и обеспечить более высокую пропускную способность в перегруженных местах, в которых наблюдается плохой уровень связи.

**Основная часть.** Для организации квантового канала используются телескопическая система, состоящая из двух модулей. Точность настройки этих модулей относительно друг друга обеспечивает уменьшение потерь в канале, поэтому важным этапом перед проведением следующих экспериментов является юстировка системы. На данный момент юстировка проводилась несколькими способами. Оба модуля системы установлены на подвижных опорах, которые позволяют модулям вращаться вокруг двух осей. Используя эти опоры, нам удалось снизить потери в атмосферном канале длиной 1 метр до 10 дБ при заведении излучения в многомодовое волокно. Для более точной настройки при использовании одномодового волокна телескопы были сняты с опор и установлены на оптический стол вплотную. Таким способом потери в канале удалось снизить до 7 дБ при заведении излучения в одномодовое волокно. Также, сейчас проводится настройка моторизированного зеркала из модуля фотоприёмника для более удобной последующей настройки системы.

**Выводы.** Настройка телескопических модулей позволит в будущем подключать к ним системы КРК. После этого будет возможно проводить испытания по передаче ключа по атмосферному каналу в городской черте, моделируя использование этого способа в будущем и оценивая потери для дальнейших исследований.

### Список использованных источников:

1. Quantum cryptography: Public key distribution and coin tossing / C. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. – 1984. – P.175-179.
2. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference / A. V. Gleim, V. I. Egorov, Yu. V. Nazarov,

- S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, G. S. Buller // Optics Express. – 2016. – Vol. 24, No. 3. - P. 2619- 2633.
3. Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres New J. Phys. 11 075003.
  4. The SECOQC quantum key distribution network in Vienna / M. Peev, C. Pacher, R. Alleaume, C. Barreiro et al. // New J. Phys. – 2009. – Vol. 11. – P.075001.