УДК 621.383.523

А.С. Задорин, Р.С. Круглов, С.И. Разгуляев, В.А. Краковский, А.Е. Мандель

Характеристики систем квантового распределения ключа по космическому каналу связи на основе однокубитовых протоколов

Отмечаются преимущества космических каналов оптической связи и возможности построения на их основе систем квантового распределения ключей (СКРК) космического базирования. Предложена программная модель такой системы КРК с однокубитовыми протоколом СКРК и линейным режимом детектирования одиночных фотонов. Исследована зависимость ошибок при генерации ключа от уровня затухания в квантовом канале системы и порога компаратора фотоприемника. Показано, что возможности рассмотренных систем КРК ограничены низкоорбитальными космическими аппаратами.

Ключевые слова: квантовое распределение ключей, космический квантовый канал.
doi: 10.21293/1818-0442-2019-22-4-39-43

Основой любой системы квантового распределение ключей (СКРК), как известно, является квантовый процессор, реализующий ряд логических операций над кубитами в квантовом канале (КК) системы и позволяющий удаленными пользователями ПА и ПБ формировать секретную ключевую последовательность (СКП) в режиме «одноразового блокнота» [1–5]. Обобщенная структурная схема такой системы приведена на рис. 1. Рассматриваемая система дает пользователям Alice и Bob возможность детектирования атак нелегитимного пользователя (Eve) на СКП. Данная возможность ограничена сверху максимально допустимым квантовым коэффициентом ошибок (QBER) в СКП $P_{f\_кр}$, определяемым используемым протоколом СКРК. Указанное ограничение на QBER определяет максимальную длину квантового канала L^* системы. Значение данного показателя определяется многими факторами – используемым протоколом КРК, механизмом ослабления оптического сигнала в квантовом канале и др. Так в канале, построенном на основе оптического волокна (ОВ), ослабление определяется диссипативными потерями энергии сигнала в сердцевине ОВ, ограничивающими L^* расстояниями ~200 км [10].

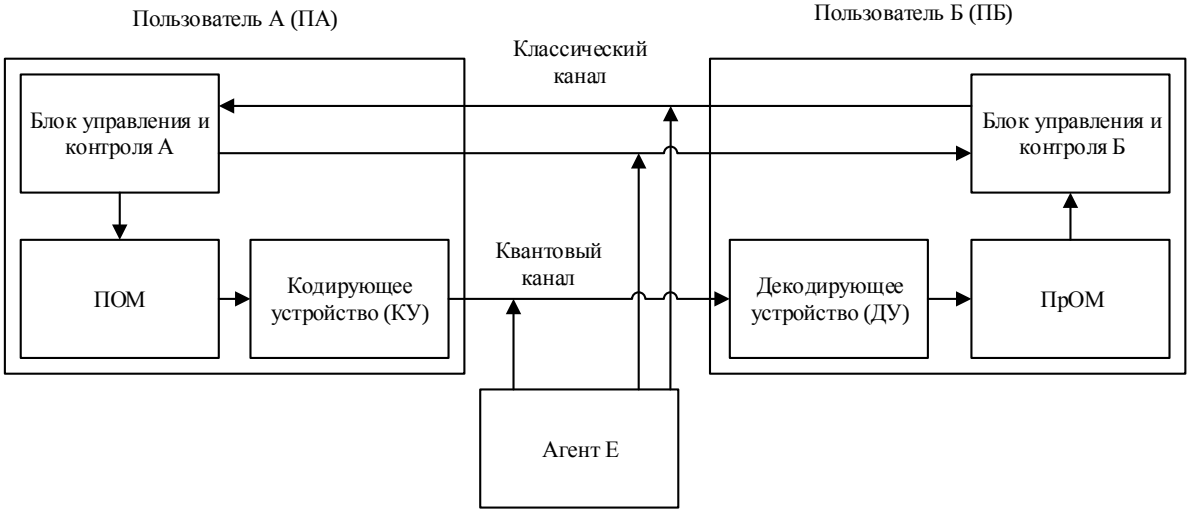

Рис. 1. Структурная схема СКРК

Радикальное снижение указанных потерь может быть достигнуто в космических каналах оптической связи, где ослабление сигнала, в основном, определяется расходимостью светового пучка. Влияние данного фактора на ослабление сигнала быстро снижается с увеличением длины канала. По этой причине в каналах космического масштаба потеря мощности сигнала может быть намного меньшей, чем в ОВ такой же длины [6–12]. Расчет показывает, что для длины световой волны 1,55 мкм по уровню оптического ослабления космический канал превосходит ВОЛС, начиная от $L^* \sim 100$ км. Приведенная оценка для L^* и представляет собой идейный стимул для исследования и разработки СКРК космического базирования [6–13].

Представленные в литературе результаты посвящены, главным образом, системам, построенным на основе использования в качестве носителей информации бифотонов, т.е. перепутанных фотонных пар (entangled photons pairs) [8–12]. При этом возможности применения в этих целях гораздо более простых и дешевых технологий приготовления оди-

ночных фотонов и использования их в рамках однокубитовых протоколов СКРК в литературе не обсуждались.

Целью данной работы является решение данной задачи, включающей в себя исследование ограничений на среднюю скорость генерации СКП (битрейт) B для СКРК космического базирования в линейном режиме детектирования кубитов.

Обозначим битовую скорость исходного ключа в схеме на рис. 1 как B_0. Снижение фактического битрейта B относительно B_0 в СКРК зависит от шумовых параметров лавинного фотодиода (ЛФД) в фотоприемном устройстве (ФПУ) системы, его порога срабатывания U_0, потерь в космическом пространстве КК и др. Все эти факторы объединяются в помехоустойчивости ФПУ, характеризующей вероятность генерации ложных символов P_f в СКП. Рассмотрим зависимость P_f от схемотехнических характеристик ФПУ.

Прежде всего отметим, что при формировании оптических кубитов за счет ослабления лазерных импульсов при среднем числе фотонов в каждом из них m~0,1, за счет 10-кратного уменьшения скорости генерации СКП имеет место рандомизация исходной последовательности.

Другие механизмы снижения битрейта в СКРК связаны с поглощением кубитов в КК, ограниченной квантовой эффективностью ЛФД η, а также особенностями протоколов КРК. Так, снижение k_p битрейта B в протоколе *BB*84 равно 0,5, а в *B*92 – 0,25 [1–5].

Зависимость B от помехоустойчивости линейного ФПУ рассмотрена в [14] и определяется вероятностью пропуска сигнальных посылок P_l в СКП, коэффициентом затухания γ сигнала на трассе КК длиной L_s, средним числом фотонов в сигнальной посылке n_c и априорной вероятностью символа $p(1) \approx 0{,}5$

$$B = B_0(1-P_l)\,p(1)k_p n_c \exp(\gamma L_s). \qquad (1)$$

Расчет P_l и P_f для линейного ФПУ, построенный на методике [14], приведен в [15]. При этом одним из источников рассматривались дробовые шумы темнового тока i_{tt}, которые складывались из собственного темнового тока ЛФД и тока фоновой засветки ЛФД. При этом среднее число n_{tt} темновых фотоэлектронов на измерительном интервале τ выражается через заряд электрона:

$$n_{tt} = (i_{tt} \cdot \tau)/e. \qquad (2)$$

Суммарный шум ФПУ считается гауссовым и представлен безразмерным параметром W, выражаемым через тепловые шумы сопротивления нагрузки и шумы усилителя ФПУ S_E, S_I на интервале τ [14]:

$$W = \frac{2kt\tau}{R\cdot e^2}\left(\frac{\tau}{T}\right) + \frac{S_I\tau}{e^2}\left(\frac{\tau}{T}\right) + \frac{S_E\tau}{2e^2R^2}\left(\frac{\tau}{T}\right), \qquad (3)$$

где t – температура в градусах Кельвина; k – постоянная Больцмана.

Параметр W определяет дисперсию шумового процесса $p_п(n)$ при отсутствии сигнала, а также распределения $p_c(n)$ в его присутствии. Искомые вероятности P_l и P_f выражаются через них как

$$P_l = \int_{-\infty}^{U_0} p_c(n)dn,\ P_f = \int_{-U_0}^{\infty} p_п(n)dn, \qquad (4)$$

где U_0 – порог срабатывания ФПУ, выраженный через n.

Далее воспользуемся результатами [4, 8] для оценки B космического канала. Прежде всего заметим, что в воздействиях атмосферных эффектов на квантовый битрейт в СКРК можно выделить следующие три основные составляющие: поглощение и рассеяние кубитов, а также турбулентность атмосферы в ее тропосферном слое. Общий коэффициент прохождения сигнала, связанный с его прохождением через атмосферу и безвоздушное пространство, может быть записан в виде

$$\gamma_{\text{uplink}} = \gamma^{\text{ext}}_{\text{uplink}} \cdot \gamma^{\text{atm}}_{\text{uplink}}, \qquad (5)$$

где $\gamma^{\text{ext}}_{\text{uplink}}$ – коэффициент прохождения, связанный с поглощением и рассеянием; $\gamma^{\text{atm}}_{\text{uplink}}$ – коэффициент прохождения, связанный с воздействием турбулентности.

Поглощение и рассеяние снижают амплитуду передаваемого оптического сигнала, так что потери в КК при вертикальном распространении оптического пучка через атмосферу толщиной h можно записать в виде

$$\gamma^{\text{ext}}_{\text{uplink}} = e^{(-\int_0^h \gamma(z')dz')}, \qquad (6)$$

где $\gamma(z')$ – коэффициент экстинкции, описывающий процессы поглощения и рассеяния светового сигнала.

Затем оценим влияние турбулентности атмосферы на B, т.е. ослабление оптического поля в условиях турбулентных вихрей, характерный масштаб которых лежит в диапазоне от миллиметров до сотен метров. Эти флуктуации приводят к случайным изменениям фазового фронта оптического пучка в КК СКРК. При этом влияние вихрей малого масштаба приводит к увеличению углового спектра пучка, тогда как вихри большого масштаба, значительно превышающего диаметр оптического пучка, приводят к флуктуации его направления, т.е. случайным блужданиям центра пучка по площадке ФПУ.

Основным параметром, описывающим турбулентность, является структурная постоянная C_n, а также радиус Фрида ρ_0, связанный с C_n, как [6–12].

$$\rho_0 = \left[0{,}423\cdot k^2 \cdot \int C_n^2(z')dz'\right]^{-(3/5)}. \qquad (7)$$

Здесь интегрирование ведется по трассе распространения, а $k = (2\cdot\pi)/\lambda$ – волновое число оптического сигнала. Угол расходимости светового пучка в турбулентной среде без учета флуктуаций центра пучка выражается через радиус Фрида [6–12]

$$\theta_{\text{turb}} = \sqrt{\theta_0^2 + (\lambda/\rho_0)^2}, \qquad (8)$$

где $\theta_0 \approx \lambda/(\pi\cdot D_t)$ – дифракционный угловой предел гауссова пучка; D_t – размер апертуры оптического пучка.

Действие крупномасштабных флуктуаций показателя преломления турбулентной атмосферы служит источником случайных отклонений (блуждания) пучка относительно его центра на расстоянии r с распределением [12]

$$p(r) = \frac{r}{\sigma_r^2} \cdot e^{(-r^2/\,2\cdot\sigma_r^2)}. \qquad (9)$$

Дисперсия распределения (9), которая выражается через апертуру приемного объектива D_r как

$$\sigma_r^2 = 2{,}87 \cdot L^2 \cdot D_r^{-(1/3)} \cdot \int_0^h C_n^2(z')dz'. \qquad (10)$$

Таким образом, угловое уширение светового пучка, вызванного турбулентностью, а также неидеальностью юстировки $\Delta\theta$ объектива на спутник [12]:

$$D = \sqrt{\Delta\theta^2 \cdot H^2 + D_{\text{beam}}^2 + \sigma_{\text{turb}}^2}\ . \qquad (11)$$

В качестве примера использования модели (5)–(11) на рис. 2 приведены расчетные зависимости затухания сигнала в нисходящем участке КК при апертуре передающего объектива 0,2 м для низкоорбитальных систем спутниковой связи.

Воспользуемся приведенными формулами для расчета основного показателя системы – квантового коэффициента ошибок Bit Error Rate (QBER) в квантовом канале связи спутниковой СКРК. Величину QBER определим как отношение битрейта шумовых отсчетов $B_n(s,\gamma,i_{tt},t)$ к общему битрейту декодированных сигнальных $B_c(s,\gamma,i_{tt},t)$ отсчетов

$$\text{QBER}(s,\gamma,i_{tt},t) = \frac{B_n(s,\gamma,i_{tt},t)}{B_c(s,\gamma,i_{tt},t) + B_n(s,\gamma,i_{tt},t)}. \qquad (12)$$

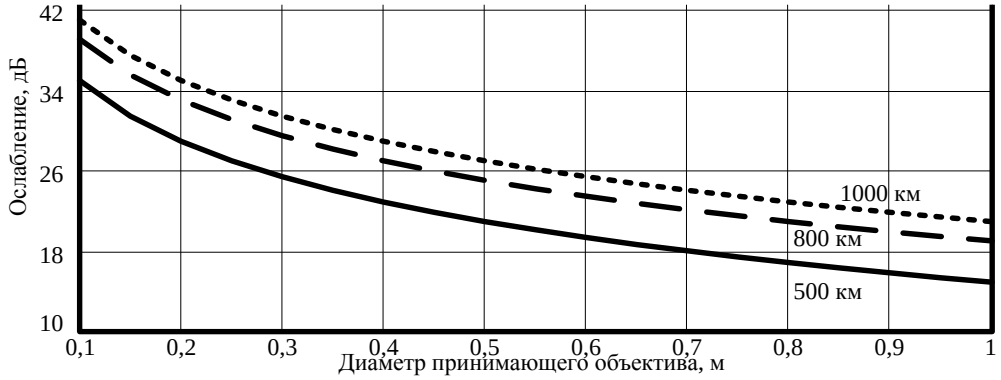

Рис. 2. Затухание оптического сигнала в КК при апертуре передающего объектива 0,2 м для низкоорбитальных систем спутниковой связи

Здесь s – пороговый уровень в дискриминаторе приемного оптического модуля (ПрОМ), γ – затухание сигнальной посылки на трассе длиной L_s, i_{tt} – темновой ток лавинного фотодиода, t – абсолютная температура ПрОМ.

Практический интерес представляет решение уравнения (12) относительно допустимого затухания КК при заданном уровне *BER*. Пример численного расчета такой зависимости для t = 80 К и QBER = 5% показан на рис. 3.

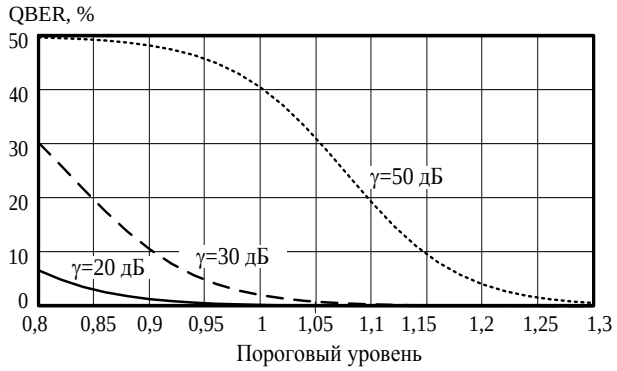

Рис. 3. Зависимость QBER от нормированного порогового уровня ФПУ и ослабления сигнала γ в КК при абсолютной температуре приемника 80 К

Из формул (1) и (12) можно заключить, что искомый уровень битрейта B рассматриваемого типа СКРК определится как

$$B = B_0\left\{\eta\left[1-P_f\right]p(1)n_c k_p \exp\left(-\gamma L_s\right) + p(1)P_f\right\}. \qquad (13)$$

Рассчитанные по формулам (12), (13) зависимости B от порогового уровня ФПУ, нормированного к отклику приемника на одиночный фотон, а также затухания в КК при температуре 80 К показаны на рис. 4.

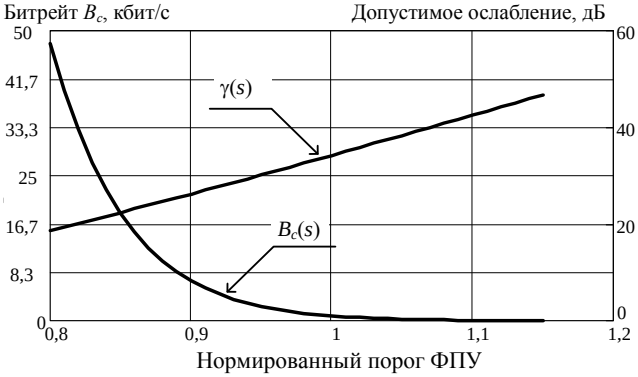

Рис. 4. Зависимости битрейта B и допустимого ослабления кубитов при QBER =5% в системе КРК от нормированного порогового уровня ФПУ при абсолютной температуре приемника 80 К

Заключение

Представленные на рис. 2–4 расчетные данные позволяют оценить возможности систем КРК космического базирования, построенных на основе однокубитового кодирования, и фотоприемников, работающих в линейном режиме регистрации одиночных фотонов. Из этих данных, в частности, следует, что в низкоорбитальных (LEO) системах спутниковой оптической связи рассматриваемые СКРК могут обеспечивать скорость формирования ключа в десятки бит в секунду даже при относительно небольших апертурах приемного и передающего объективов (~0,2 м).

Размещение таких систем на космических аппаратах, находящихся на геостационарных (GEO) или средневысотных (MEO) орбитах, приводит к дополнительному ослаблению оптического сигнала на несколько десятков децибел и соответствующему снижению квантового битрейта [6, 7]. Возможности повышения битрейта в данных условиях может быть основано на использовании в СКРК более сложных квантовых объектов, таких, например, как перепутанные фотонные пары [6–12].

Литература

1. Бауместер Д. Физика квантовой информации / Д. Бауместер, А. Экерт, А. Цайлингер. – М.: Постмаркет, 2002. – 376 с.

2. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М.: Мир, 2008. – 824 с.

3. Имре Ш. Квантовые вычисления и связь. Инженерный подход / Ш. Имре, Ф. Балаж. – М.: Физматлит, 2008. – 320 с.

4. Килин С.Я. Квантовая криптография: идеи и практика / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. – М.: Минск, 2007. – 392 с.

5. Молотков С.Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // Письма в ЖЭТФ. – 2004. – Т. 79. – С. 691–704.

6. Vasylyev D. Satellite-mediated quantum atmospheric links / D. Vasylyev, W. Vogel, F. Mol [Электронный ресурс]. – URL: https://www.researchgate.net/publication/330553517_Satellite-mediated_quantum_atmospheric_links, свободный (дата обращения: 01.12.2019).

7. Exploring the boundaries of quantum mechanics: advances in satellite quantum communications / A. Costantino, V. Francesco, S. Matteo, D. Daniele, C. Luca, T. Marco, M. Davide, S. Andrea, L. Vincenza, B. Giuseppe, V. Giuseppe, V. Paolo // Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018. – 6 p. [Электронный ресурс]. – URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5990660, свободный (дата обращения: 01.12.2019).

8. Comparison of free-space and fiber-based transmission systems in quantum cryptography / M. Toyoshima, Y. Shoji, C. Schaefer, Y. Takayama, H. Kunimori, M. Takeoka, M. Fujiwara, M. Sasaki // Phys. Rev. Lett. – 2009. – Vol. 7. – P. 26.

9. Long-distance quantum communication with entangled photons using satellites / M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, A. Zeilinger // Journal of Selected Topics in Quantum Electronics, 2003 [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/document/ 1263786, свободный (дата обращения: 01.12.2019).

10. Free-Space Optical Quantum Key Distribution Using Intersatellite Links / M. Pfennigbauer, W.R. Leeb, M. Aspelmeyer, T. Jennewein, A. Zeilinger // Phys. Rev. Lett. – 2003. – Vol. 9. – P. 34.

11. Bedington R. Progress in satellite quantum key distribution. / R. Bedington, JM. Arrazola, A. Ling // npj Quantum Inf. 3, 30 (10.1038/s41534-017-0031-5). – 2017 [Электронный ресурс]. – URL: https://www.nature.com/articles/s41534-017-0031-5, свободный (дата обращения: 01.12.2019).

12. Пат. 2566664 РФ, МПК H04L 9/00. Способ квантовой криптографии с использованием пассивных отражающих и перенаправляющих элементов, располагаемых на космических аппаратах / М.Ю. Сайгин, И.Е. Проценко, В.В. Фирсов, С.А. Магницкий. – № 2014113636/07; заяв. 08.04.2014, опубл. 27.10.2015. Бюл. № 30.

13. Томаси У. Электронные системы связи. – М.: Техносфера, 2007. – 1361 с.

14. Gerd Keiser. Optical fiber communications Second Edition. – McGraw-Hill, 2000. – 243 p.

15. Скорость генерации кода в системе квантового распределения ключей / А.С. Задорин, А.В. Максимов, Д.А. Махорин, С.О. Чечулин, А.А. Маликов // Доклады ТУСУР, 2011. – Р. 139–141.

Задорин Анатолий Семенович
Д-р физ.-мат. наук, профессор
каф. радиоэлектроники и систем связи (РСС)
Томского гос. ун-та систем управления
и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-913-820-65-43
Эл. почта: Anatoly.Zadorin@rzi.tusur.ru

Круглов Роман Сергеевич
Канд. техн. наук, науч. сотр. POF-Application Center
Polymer Optical Fiber Application Center (POF-AC)
Technische Hochschule Nürnberg Georg Simon Ohm
Wassertorstr. 10, Nürnberg, Germany, 90489
Тел.: +491-578-426-09-53
Эл. почта: roman.kruglov@pofac.th-nuernberg.de

Разгуляев Сергей Игоревич
Магистрант каф. РСС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-962-777-19-44
Эл. почта: Sergeant_96@mail.ru

Краковский Виктор Адольфович
Д-р техн. наук, профессор каф. телекоммуникаций
и основ радиотехники (ТОР) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-33-98
Эл. почта: office@tor.tusur.ru

Мандель Аркадий Евсеевич
Д-р физ.-мат. наук, профессор каф. сверхвысокочастотной
и квантовой радиотехники (СВЧиКР) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-18
Эл. почта: mandelae@svch.tusur.ru

Zadorin A.S., Kruglov R.S., Razgulyaev S.I.,
Krakowski V.A., Mandel A.E.

Capacity of the Quantum Key Distribution System with Single-Qubit Encoding via Satellite-Mediated Quantum Free-Space Link

The model of the quantum key distribution over free-space link has been developed and analyzed. The dependency of the quantum bit error rate on channel attenuation and decision threshold of the receiver has been investigated.

Keywords: quantum key distribution, free-space communication, satellite communication.
doi: 10.21293/1818-0442-2019-22-4-39-43

References

1. Baumester D., Eckert A., Zeilinger A. Physics of Quantum Information. *Postmarket*, 2002, 376 p.

2. Nielsen M., Chang I. Quantum Computing and Quantum Information. Translated from English. *World*, 2008, 824 p.

3. Imre S., Balazs F. Quantum computing and communication. Engineering approach. *Fizmatlit*, 2008, 392 p.

4. Kilin S.Y., Horoshko D.B., Nizovtsev A.P. Quatum cryptography: ideas and practice. 2008, 392 p.

5. Molotkov S.N. On the integration of quantum secret communication systems (quantum cryptography) into fiber optic telecommunication systems. *Letters in JETP*, 2004, pp. 691–704.

6. Vasylyev D., Vogel W., Mol F. Satellite-mediated quantum atmospheric links. Available at: https://www.researchgate.net/publication/330553517_Satellite-mediated_quantum_atmospheric_links (accessed: December 01, 2019).

7. Costantino A., Francesco V., Matteo S., Daniele D., Luca C., Marco T., Davide M., Andrea S., Vincenza L., Giuseppe B., Giuseppe V., Paolo V. Exploring the boundaries of quantum mechanics: advances in satellite quantum communications. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5990660 (accessed: December 01, 2019).

8. Toyoshima M., Shoji Y., Schaefer C., Takayama Y., Kunimori H., Takeoka M., Fujiwara M., Sasaki M. Comparison of free-space and fiber-based transmission systems in quantum cryptography. *Phys. Rev. Lett.*, 2009, p. 26.

9. Aspelmeyer M., Jennewein T., Pfennigbauer M., Leeb W., Zeilinger A. Long-distance quantum communication with entangled photons using satellites. *Journal of Selected Topics in Quantum Electronics.* 2003. Available at: https://ieeexplore.ieee.org/document/1263786 (accessed: December 01, 2019).

10. Pfennigbauer M., Leeb W.R., Aspelmeyer M., Jennewein T., Zeilinger A. Free-Space Optical Quantum Key Distribution Using Intersatellite Links. *Phys. Rev. Lett.*, 2003, p. 34.

11. Bedington R., Arrazola JM., Ling A. Progress in satellite quantum key distribution. *npj Quantum Inf. 3, 30 (10.1038/s41534-017-0031-5),* 2017. Available at: https://www.nature.com/articles/s41534-017-0031-5 (accessed: December 01, 2019).

12. Saigin M. Yu., Protsenko I.E., Firsov V.V., Magnitsky S.A. *Sposob kvantovoy kriptografii s ispol'zovaniyem passivnykh otrazhayushchikh i perenapravlyayushchikh elementov, raspolagayemykh na kosmicheskikh apparatakh* [A method of quantum cryptography using passive reflective and redirecting elements located on spacecraft]. Patent RF, no. 2014113636/07, 2014).

13. Tomasi W. Electronic Communications Systems. *Technosphere Moscow*, 2007, p. 1361.

14. Gerd Keiser. Optical fiber communications Second Edition. *Singapore, McGraw-Hill*, 2000, p. 243.

15. Zadorin A.S., Maximov A.V., Mahorin D.A., Chechulin S.O., Malikov A.A. Code generation rate in a quantum key distribution system. *Doklady TUSUR*, 2011, pp. 139–141.

Anatoly S. Zadorin
Doctor of Science in Physics and Mathematics, Professor,
Department of Radioelectronics and Communication Systems (RCS), Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-820 65-43
Email: Anatoly.Zadorin@rzi.tusur.ru

Roman S. Kruglov
Assistant Professor, Researcher,
Polymer Optical Fiber Application Center (POF-AC),
Technische Hochschule Nürnberg Georg Simon Ohm
10, Wassertorstr., Nürnberg, Germany, 90489
Phone: +491-578-426-09-53
Email: roman.kruglov@pofac.th-nuernberg.de

Sergey I. Razgulyaev
Undergraduate student
Department of RCS TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-820 65-43
Email: Sergeant_96@mail.ru

Victor A. Krakowski
Doctor of Engineering Sciences, Professor
Department of Telecommunications and Basic Principles of Radio Engineering (TFR), TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-820-65-43, +7 (382-2) 41-33-98
Email: office@tor.tusur.ru

Arkady E. Mandel
Doctor of Science in Physics and Mathematics, Professor,
Department of Microwave and Quantum Radio Engineering, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-18
Email: mandelae@svch.tusur.ru