

УДК 004.021

DOI: [10.26102/2310-6018/2025.50.3.011](https://doi.org/10.26102/2310-6018/2025.50.3.011)

Оптимизация сетей квантового распределения ключей с помощью алгоритмов кластеризации

Е.С. Раздьяконов¹✉, С.А. Корчагин¹, А.В. Тимошенко¹, М.Ф. Булатов²

¹Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

²Московский государственный университет имени М.В. Ломоносова, Москва, Российская Федерация

Резюме. Работа посвящена проблеме оптимизации сети квантового распределения ключей (КРК) путем объединения исходного набора конечных узлов на плоскости в небольшие сети доступа с топологией типа «звезда» с помощью алгоритмов кластеризации. В исследовании представлена модифицированная версия алгоритма k-medoids, учитывающая ограничение на максимальную длину соединения между парой узлов. Также была представлена новая неевклидова метрика оценки качества соединения на основе значения квантовой емкости, вычисляемая на основе физических свойств и длины оптоволоконного соединения. В статье проводилось сравнение работы данного алгоритма с использованием двух метрик: евклидовой нормы и представленной метрики оценки квантового соединения. Была проведена серия экспериментов по решению задачи кластеризации для множества наборов случайно распределенных на плоскости узлов. Оказалось, что применение неевклидовой метрики позволяет снизить количество кластеров на 11,7 % по сравнению с евклидовой нормой, а использование нескольких повторений на каждой итерации позволяет улучшить результат еще более чем на 20 %. Метод кластеризации и новая метрика, представленные в данной работе, позволяют уменьшить количество подсетей при разбиении, сократив затраты на организацию центральных узлов, а также позволяет в дальнейшем решать упрощенную задачу построения магистральной сети, объединяющую полученные подсети в одну сеть КРК.

Ключевые слова: квантовое распределение ключей, математическое моделирование, кластеризация, алгоритм k-medoids, программный комплекс.

Для цитирования: Раздьяконов Е.С., Корчагин С.А., Тимошенко А.В., Булатов М.Ф. Оптимизация сетей квантового распределения ключей с помощью алгоритмов кластеризации. *Моделирование, оптимизация и информационные технологии*. 2025;13(3). URL: <https://moitvvt.ru/ru/journal/pdf?id=1951> DOI: 10.26102/2310-6018/2025.50.3.011

Optimization of quantum key distribution networks using clustering algorithms

E.S. Razdyakonov¹✉, S.A. Korchagin¹, A.V. Timoshenko¹, M.F. Bulatov²

¹Financial University under the Government of the Russian Federation, Moscow, the Russian Federation

²Lomonosov Moscow State University, Moscow, the Russian Federation

Abstract. This paper is devoted to the problem of optimizing a quantum key distribution (QKD) network by combining an initial set of end nodes into small access networks with star-type topology using clustering algorithms. The study presents a modified version of the k-medoids algorithm that takes into account the constraint on the maximum quantum link length between a pair of nodes. A new non-Euclidean metric for link quality assessment based on the quantum capacitance value calculated based on the physical properties and length of the optical fiber link was also presented. The performance of the presented algorithm using two metrics, the Euclidean norm and the presented estimation metric, was

then compared. A series of experiments were conducted to solve the clustering problem for multiple sets of nodes randomly distributed on the plane. It is found that the application of the presented non-Euclidean metric reduces the number of clusters by 11.7% compared to the Euclidean norm, and using multiple attempts at each iteration can improve the result by even more than 20%. The clustering method and the new metric presented in this paper allow us to reduce the number of subnets, reducing the cost of organizing central nodes, and also allows us to further solve the simplified problem of building a backbone network, combining the obtained subnets into a single QKD network.

Keywords: quantum key distribution, mathematical modeling, clustering, k-medoids algorithm, software package.

For citation: Razdyakonov E.S., Korchagin S.A., Timoshenko A.V., Bulatov M.F. Optimization of quantum key distribution networks using clustering algorithms. *Modeling, Optimization and Information Technology*. 2025;13(3). (In Russ.). 2025;13(3). URL: <https://moitvvt.ru/ru/journal/pdf?id=1951> DOI: 10.26102/2310-6018/2025.50.3.011

Введение

Обеспечение безопасного обмена ключами через сети общего пользования является фундаментальной проблемой в области компьютерной безопасности с момента ее появления. На данный момент подавляющее большинство современных методов передачи ключей использует алгоритмы, требующие от злоумышленника больших временных и вычислительных ресурсов, то есть успешный взлом ключа слишком сложен с использованием современного технического обеспечения, но не является теоретически невозможным. Подобные методы называют вычислительно-безопасными. Таким образом, возможность прорыва в области криптографии, например, появления доступных квантовых компьютеров, ставит под угрозу все классические алгоритмы шифрования.

Процесс обмена ключами с помощью квантового распределения ключей (КРК) [1], использующего законы квантовой механики для защиты канала связи, является теоретически-безопасным, так как зашифрованный ключ невозможно перехватить через квантовый канал. Это делает сети квантового распределения ключей одним из самых перспективных направлений в области защиты информации [2].

Тем не менее, для сетей КРК существует ряд ограничений, наложенный законами квантовой механики и включающий в себя ограничения на длину соединения [3] и необходимость использования соединений точка-точка [4]. Это делает эффективность сетей квантового распределения зависимым от топологии, что, в свою очередь, требует тщательного анализа при проектировании таких сетей.

В работах, посвященных разработке аналитических методов оценки и оптимизации топологий сетей КРК, применяются различные подходы [5]. Так, например, оценка топологии путем решения задачи о максимальном потоке применяется в [6], а в работе [7] для построения оптимальной сети применяется алгоритм поиска пути. Однако подобные методы могут оказаться неэффективными в случае большого количества конечных узлов, так как в случаях, схожих с [7], построение оптимальной сети КРК сводится к задаче комбинаторной оптимизации.

Одним из способов решения данной проблемы является декомпозиция исходной задачи путем построения двуслойной сети КРК. На первом этапе будет производиться объединение исходного набора конечных узлов в небольшие сети доступа с топологией типа «звезда». Это позволит облегчить задачу построения магистральной подсети, связывающей только центральные узлы подсетей, количество которых значительно меньше исходных.

Целью данной работы является построение первого, «потребительского» слоя иерархической сети КРК путем выбора из исходного множества потребительских узлов минимального подмножества узлов в качестве центральных. Слой должен соответствовать следующим требованиям:

1. Каждый из исходных потребительских узлов должен находиться в одной из подсетей, то есть, быть соединенным с одним из центральных узлов.
2. Длина соединения между центральным и потребительским узлом не должна превышать заданной максимальной длины D_{max} .

Иерархическая топология также упростит маршрутизацию внутри сети, так как она будет проводиться между меньшим набором центральных узлов, а также улучшит масштабируемость. Более того, использование топологий типа «звезда» позволит сократить стоимость инфраструктуры благодаря использованию оптических коммутаторов на центральных узлах вместо соединений точка-точка.

Материалы и методы

Разбиение множества конечных узлов-потребителей сети квантового распределения ключей на подсети было продемонстрировано в [8], где для решения данной задачи применялся алгоритм кластеризации k-medoids. Задача в данном исследовании схожа с [8]. Тем не менее, главным отличием является использование в алгоритме неевклидовой метрики для оценки качества соединения между парами узлов.

Задача кластеризации на основе медоидов. Пусть задано множество конечных узлов $X = \{x_1, \dots, x_n\}$, и целью алгоритма является разделение его на k подсетей или кластеров c_j , где $C = \{c_1, \dots, c_k\}$ – множество кластеров.

В случае задачи кластеризации на основе поиска центроидов, чаще всего используют евклидово расстояние между элементами кластера и его центроидом v_j . Тогда целевая функция представляет собой сумму расстояний между центроидом и каждым элементом кластера [9]:

$$J = \sum_{x_i \in X} \min_{v_j \in C} \|x_i - v_j\|. \quad (1)$$

Координаты центроида v_j , в свою очередь, вычисляются как центр масс соответствующего кластера c_j :

$$v_j = \frac{1}{|c_j|} \sum_{x_i \in c_j} x_i.$$

Существует множество алгоритмов решения данной задачи, самым известным из которых является метод k-средних. Тем не менее, существует модификация данной задачи, в которой вместо центроида кластера используется медоид $m_j \in c_j$ – элемент, принадлежащий этому кластеру. Целевая функция (1) в этом случае принимает следующий вид:

$$J = \sum_{x_i \in X} \min_{m_j \in X | c_i \in C} d(x_i, m_j). \quad (2)$$

Для задач кластеризации на основе медоидов часто применяется алгоритм k-medoids [10]. В данном случае оптимизация состоит из выбора кластера и выбора репрезентативного элемента (медоида).

Использование репрезентативных элементов вместо точек позволяет повысить робастность кластеризации, поскольку медоиды менее подвержены влиянию выбросов, а также делает необязательным использование метрик: достаточно задания матрицы расстояний между всеми парами элементов из X , поскольку такой подход не требует вычисления координат в пространстве.

Метрика качества соединения. В данном исследовании вместо расстояния в евклидовом пространстве используется метрика, учитывающая параметр квантовой емкости соединения между двумя узлами, которая вычисляется на основе свойств оптического волокна:

$$q(x_u, x_v) = -\log_2[(1 - e^{-d(x_u, x_v)/\lambda_0})], \quad (1)$$

где $d(x_u, x_v)$ – длина соединения в км, а λ_0 – длина затухания, определяемая физическими свойствами соединения.

Критерий оптимальности квантового соединения, используемый в данной работе, вычисляется по формуле:

$$d_{QKD}(x_u, x_v) = \frac{d(x_u, x_v)}{q(x_u, x_v)}. \quad (2)$$

Таким образом, целевая функция (2) примет вид:

$$J = \sum_{x_i \in X} \min_{m_j \in X | c_i \in C} \frac{d(x_u, x_v)}{q(x_u, x_v)}. \quad (5)$$

Алгоритм кластеризации. Для кластеризации исходного набора узлов применяется алгоритм на основе k-medoids из [8], определяющий минимальное количество кластеров с учетом дополнительного ограничения максимальной длины соединения $d(x_u, x_v) < D_{max}$.

Процесс выглядит следующим образом:

- 1) задать максимальную длину соединения D_{max} , длину затухания соединения λ_0 и начальное количество кластеров k ;
- 2) вычислить квантовую емкость соединения $d_{QKD}(\cdot, \cdot)$ между всеми узлами;
- 3) задать начальное множество центральных узлов $m_1, \dots, m_k \in X$ случайным образом;
- 4) применить алгоритм k-medoids для поиска оптимального расположения центральных узлов m_j^* ;
- 5) оценить кластер для каждого центрального узла для проверки условия $d(x_i, m_j^*) < D_{max} \forall x_i \in c_j$;
- 6) если условие не выполнено, увеличить число кластеров k и вернуться к шагу 3.

Для улучшения качества кластеризации в условиях ограничения на длину соединения можно увеличить количество неудачных «попыток» кластеризации до перехода на увеличенное число кластеров, т. е. пункты 3–5 будут повторяться заданное количество раз в цикле. Это позволит уменьшить влияние неудачной случайной инициализации, тем самым уменьшив среднее количество кластеров.

Результаты

Алгоритмы были реализованы на языке программирования Python с использованием библиотек numpy и networkx. Реализация алгоритма k-medoids была взята из библиотеки scikitlearn-extra. Для визуализации использовалась библиотека matplotlib.

В данной работе была проведена серия экспериментов с использованием двух различных метрик: евклидовой нормы и метрики на основе квантовой емкости соединения. Для экспериментов были использованы наборы размерами от 50 до 250 узлов, равномерно распределенных внутри квадрата размером 100×100 км.

Для вычисления квантовой емкости было взято значение $\lambda_0 \approx 22$ км, что соответствует длине затухания для оптоволокна с затуханием 0,2 дБ/км. Максимальная

длина соединения для обоих экспериментов была взята несколько меньшей, чем длина затухания и равнялась $D_{max} = 20$ км.

Подсети и центральные узлы, а также количества кластеров для обоих методов, полученные в результате одного из экспериментов для 200 узлов, изображены на Рисунке 1.

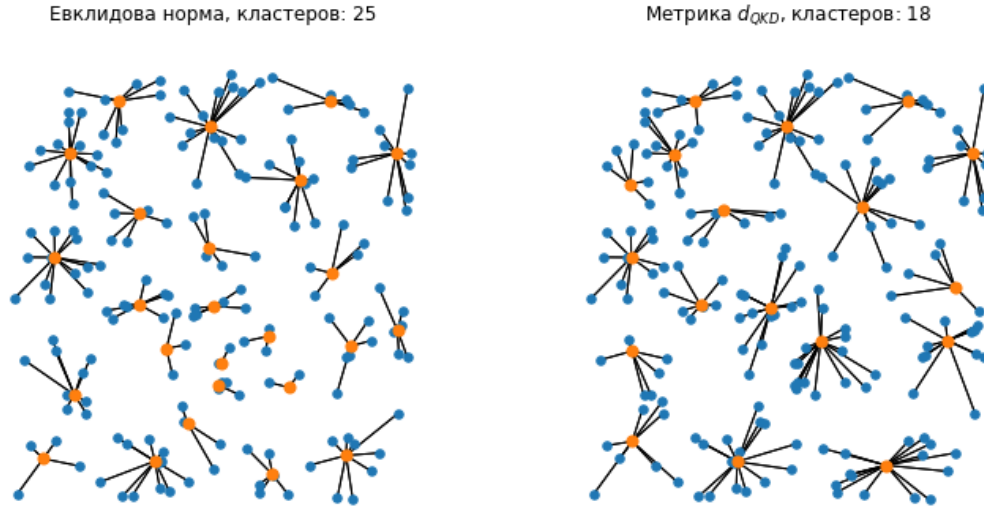


Рисунок 1 – Подсети и центральные узлы, полученные для набора из 200 узлов
Figure 1 – Sub-networks and central nodes for set of 200 nodes

Для сравнения методов кластеризации были проведены эксперименты для исходных наборов различных размеров N_{set} от 50 до 250 с шагом в 25 узлов. В обоих методах количество попыток кластеризации равнялось 1. Для каждого значения N_{set} было проведено 100 экспериментов, в результате которых были взяты усредненные значения количества кластеров и значений емкости квантовых соединений $q(d)$. Графы усредненных значений для обоих методов кластеризации, представлены на Рисунках 2 и 3.

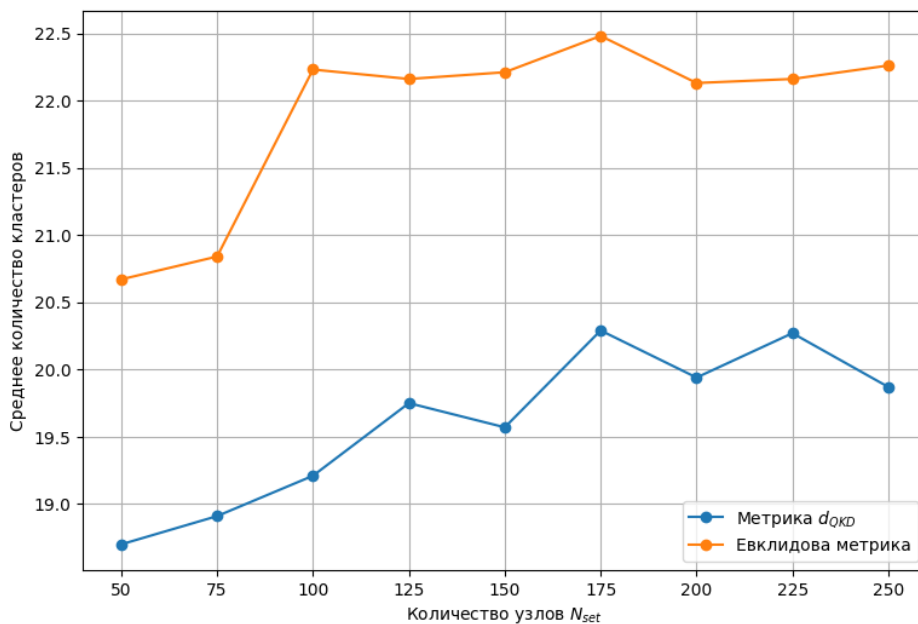


Рисунок 2 – Зависимость среднего количества кластеров от количества конечных узлов
Figure 2 – Dependence of the average number of clusters on the number of end nodes

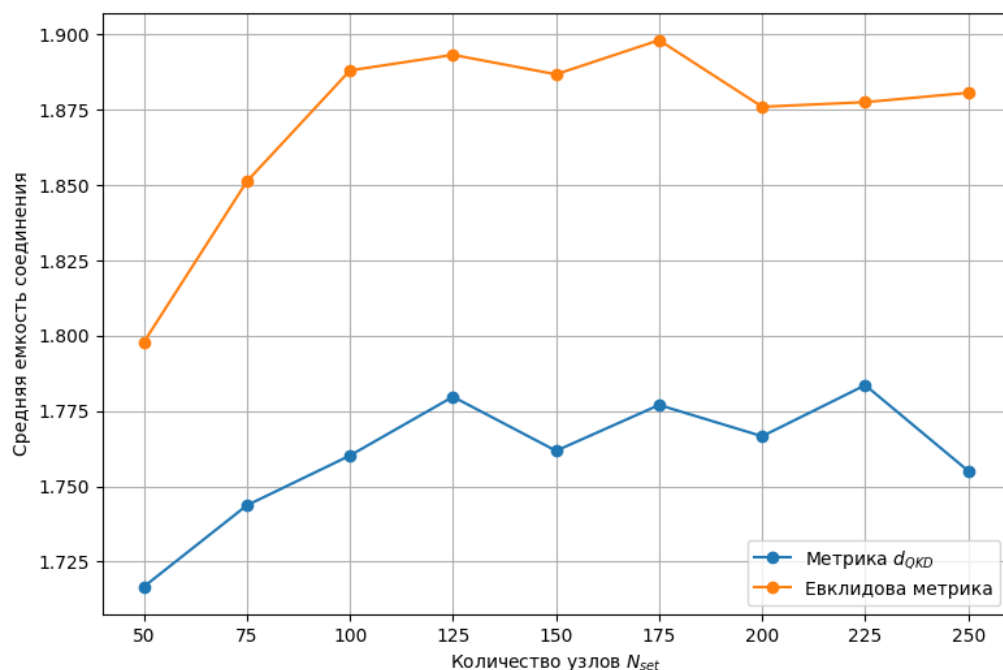


Рисунок 3 – Зависимость средней емкости соединения от количества конечных узлов
Figure 3 – Dependence of average link capacitance on the number of end nodes

Аналогичная серия экспериментов была проведена для сравнения влияния количества попыток на качество кластеризации. Был рассмотрен только метод на основе метрики d_{QKD} с 1, 5, 10 и 15 попытками. Значения N_{set} и количество повторений для каждого количества узлов аналогичны предыдущей серии экспериментов. Усредненные значения количества кластеров изображены на Рисунке 4.

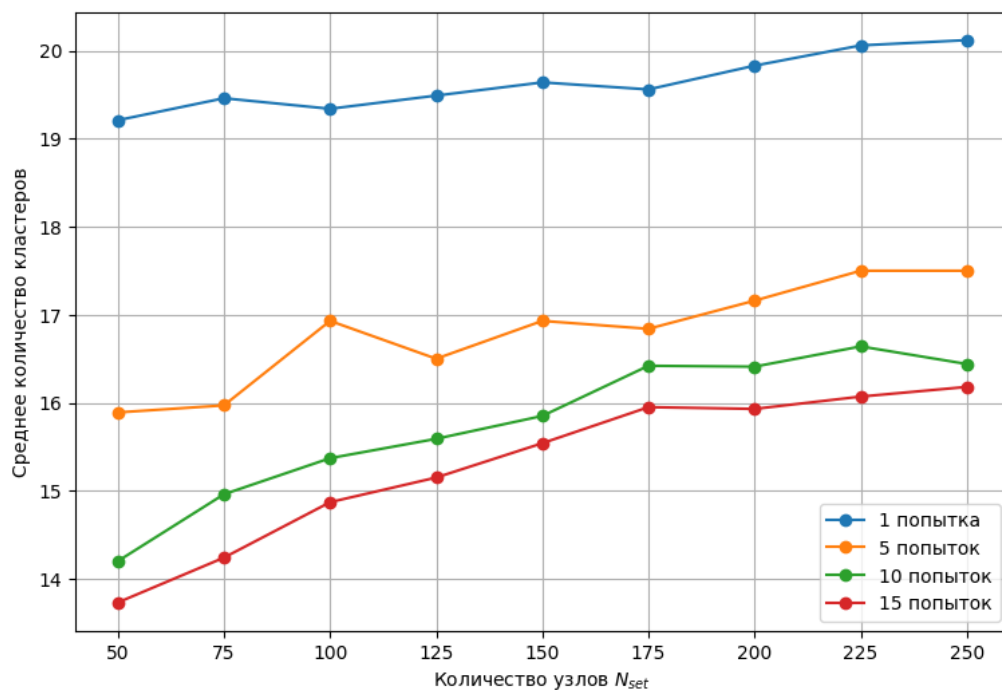


Рисунок 4 – Среднее количество кластеров для различного количества попыток
Figure 4 – Average number of clusters for different number of attempts

Обсуждение

Как видно из результатов экспериментов, метод кластеризации с применением метрики d_{QKD} позволяет получить меньшее количество кластеров, чем метод с применением евклидовой нормы, в среднем на 11,7 %. Более эффективное разбиение в условиях ограничения на максимальную длину соединения, скорее всего, достигается благодаря свойствам d_{QKD} , которая принимает значения, превосходящие евклидову норму при длинах соединения $d(x_u, x_v) > \lambda_0 \ln(2)$, то есть, $d(x_u, x_v) > 15,25$ км в данной серии экспериментов.

Среднее значение квантовой емкости соединения между узлами внутри подсетей является более высоким при использовании евклидовой нормы благодаря большему числу кластеров, и, следовательно, меньшему среднему расстоянию между конечными и центральными узлами.

Использование попыток для каждого количества кластеров позволило значительно улучшить качество кластеризации в условиях ограничения на максимальную длину соединения. Так, по сравнению с одной попыткой на каждую итерацию алгоритма, использование 5, 10 и 15 попыток позволяет получить в среднем на 14,4 %, 19,7 % и 22,1 % меньшее количество кластеров соответственно.

К недостаткам алгоритма и представленной метрики можно отнести его высокую вычислительную сложность, что особенно заметно при большом количестве узлов.

Возможные способы снизить вычислительные затраты в случае большого количества узлов включают в себя:

- использование приближенных алгоритмов (например, CLARA и CLARANS), которые работают с подвыборками данных;
- инициализацию начального расположения медоидов с использованием жадного алгоритма или эвристик вместо случайного выбора элементов.

Заключение

В работе было проведено исследование по объединению множества конечных узлов сети квантового распределения ключей в сети доступа с топологией типа «звезда» путем решения задачи кластеризации на основе медоидов с использованием неевклидовой метрики.

В ходе работы была предложена новая метрика оценки оптимальности соединения между парой узлов, основанная на значении квантовой емкости, которая была применена в алгоритме кластеризации. Результаты экспериментов на наборах случайно распределенных на плоскости узлов показали, что использование представленной метрики, а также добавление дополнительных попыток в итерации алгоритма позволяют получить более эффективное разбиение с меньшим количеством подсетей, что поможет снизить затраты на центральные узлы при организации сети квантового распределения ключей.

Центральные узлы, полученные в результате работы алгоритма, могут затем быть использованы для решения упрощенной задачи построения магистральной сети произвольной топологии, связывающей все подсети в одну сеть КРК.

В ходе данной работы были выделены следующие возможные направления для дальнейших исследований: применение приближенных алгоритмов кластеризации вместо k-medoids, изменение способа инициализации кластеров, модификация метрики квантового соединения путем использования величины уровня ошибок (QBER), а также решение задачи построения магистральной сети квантового распределения ключей, связывающей подсети, полученные в результате работы алгоритма кластеризации.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Bennett Ch.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science*. 2014;560:7–11. <https://doi.org/10.1016/j.tcs.2014.05.025>
2. Раздьяконов Е.С., Корчагин С.А. Применение математического моделирования для оценки топологии сетей квантового распределения ключей. В сборнике: *Цифровая трансформация управления: проблемы и решения: материалы VI Всероссийской научно-практической конференции, 18 апреля 2024 года, Москва, Россия*. Москва: Государственный университет управления; 2024. С. 137–140.
3. Mehic M., Niemiec M., Rass S., et al. Quantum Key Distribution: A Networking Perspective. *ACM Computing Surveys (CSUR)*. 2020;53(5). <https://doi.org/10.1145/3402192>
4. Peev M., Pacher Ch., Alléaume R., et al. The SECOQC Quantum Key Distribution Network in Vienna. *New Journal of Physics*. 2009;11. <https://doi.org/10.1088/1367-2630/11/7/075001>
5. Раздьяконов Е.С. Обзор методов оптимизации топологии сетей квантового распределения ключей. *Инженерный вестник Дона*. 2024;(7). URL: <http://www.ivdon.ru/ru/magazine/archive/n7y2024/9347>
Razdyakonov E.S. Survey of Topology Optimization Methods for Quantum Key Distribution Networks. *Engineering Journal of Don*. 2024;(7). (In Russ.). URL: <http://www.ivdon.ru/en/magazine/archive/n7y2024/9347>
6. Li Q., Wang Ya., Mao H., Yao J., Han Q. Mathematical Model and Topology Evaluation of Quantum Key Distribution Network. *Optics Express*. 2020;28(7):9419–9434. <https://doi.org/10.1364/OE.387697>
7. Cirigliano L., Brosco V., Castellano C., Conti C., Piloizzi L. Optimal Quantum Key Distribution Networks: Capacitance Versus Security. *npj Quantum Information*. 2024;10. <https://doi.org/10.1038/s41534-024-00828-7>
8. García-Cobo I., Menéndez H.D. Designing Large Quantum Key Distribution Networks Via Medoid-Based Algorithms. *Future Generation Computer Systems*. 2021;115:814–824. <https://doi.org/10.1016/j.future.2020.09.037>
9. MacQueen J. Some Methods for Classification and Analysis of Multivariate Observations. In: *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability: Volume 1: Statistics, 21 June – 18 July 1965, 27 December 1965, 07 January 1966, Berkeley, CA, USA*. Berkeley-Los Angeles: University of California Press; 1967. P. 281–297.
10. Kaufman L., Rousseeuw P.J. *Finding Groups in Data: An Introduction to Cluster Analysis*. John Wiley & Sons; 2009. 368 p.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Раздьяконов Егор Сергеевич, аспирант, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: esrazdyakonov@gmail.com

Egor S. Razdyakonov, Postgraduate, Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Корчагин Сергей Алексеевич, кандидат физико-математических наук, доцент, доцент кафедры искусственного интеллекта Финансового университета при Правительстве

Sergey A. Korchagin, Candidate of Physical and Mathematical Sciences, Docent, Associate Professor at the Artificial Intelligence Department, Financial University under the

Российской Федерации, Москва, Российская
Федерация.

e-mail: sakorchagin@fa.ru

ORCID: [0000-0001-8042-4089](https://orcid.org/0000-0001-8042-4089)

Government of the Russian Federation, Moscow,
the Russian Federation.

Тимошенко Александр Васильевич, доктор
технических наук, профессор, профессор
кафедры информационной безопасности
Финансового университета при
Правительстве Российской Федерации,
Москва, Российская Федерация.

e-mail: avtimoshenko@fa.ru

ORCID: [0000-0002-9791-142X](https://orcid.org/0000-0002-9791-142X)

Alexander V. Timoshenko, Doctor of Engineering
Sciences, Professor, Professor at the Information
Security Department, Financial University under
the Government of the Russian Federation,
Moscow, the Russian Federation.

Булатов Марат Фатыхович, доктор физико-
математических наук, профессор, профессор
кафедры математического моделирования в
космических исследованиях факультета
космических исследований Московского
государственного университета имени М.В.
Ломоносова, Москва, Российская Федерация.

ORCID: [0000-0001-7839-8416](https://orcid.org/0000-0001-7839-8416)

Marat F. Bulatov, Doctor of Physical and
Mathematical Sciences, Professor, Professor at
the Department of Mathematical Modeling in
Space Research, Faculty of Space Research,
Lomonosov Moscow State University, Moscow,
the Russian Federation.

*Статья поступила в редакцию 11.05.2025; одобрена после рецензирования 25.06.2025;
принята к публикации 04.07.2025.*

*The article was submitted 11.05.2025; approved after reviewing 25.06.2025;
accepted for publication 24.07.2025.*