RESEARCH AND ANALYSIS EFFICIENCY FIBER OPTICAL COMMUNICATION LINES USING QUANTUM TECHNOLOGY

DOI: 10.36724/2072-8735-2021-15-10-50-54

Bayram G. Ibrahimov,
Azerbaijan Technical University, Baku, Azerbaijan,
i.bayram@mail.ru

Allahverdi O. Orujov,
Azerbaijan Technical University, Baku, Azerbaijan,
allahverdi.oruc@aztu.edu.az

Arif H. Hasanov,
Military Academy of the Republic of Azerbaijan, Baku, Azerbaijan,
arifhasan2828@yandex.ru

Konul M. Tahirova,
Military Academy of the Republic of Azerbaijan, Baku, Azerbaijan

Manuscript received 27 August 2021;
Accepted 20 September 2021

Keywords: *Quantum key distribution, FOCL using quantum technology, efficiency, quantum cryptography protocols, information entropy, security threat, PNS-attack*

The analysis of the performance indicators fiber-optic communication lines (FOCL) using quantum technology based on the architectural concept of NGN (Next Generation Network) and future networks FN (Future Networks) for the construction highly efficient optical telecommunication networks supporting a wide range cryptographic resistance. Threats of unauthorized access, denial of service, loss information, cryptographic methods and algorithms for information protect?on are considered. Complex criteria of FOCL efficiency using such quantum technologies as network performance using WDM (Wavelength Division Multiplexing) technology, information security characteristics when using quantum cryptography protocols, taking into account resistance to various threats, informative characteristics photon sources are selected. A new approach is proposed for the study and assessment of complex indicators complex optical information protection systems and effective control of a set quantum key distribution systems for fiber-optic communication lines. The functioning of the investigated FOCL using quantum technology based on the principles "Point-to-point" network topology, which allows organizing a quantum information and service channel, is considered. On the basis of the proposed approach, the efficiency quantum key distribution, the capabilities quantum cryptography protocols under the influence of photon number splitting attack (PNS-Photon Number Splitting Attack) and the information entropy of the characteristics of sources of optical photon qubit fluxes are investigated. Analytical expressions are obtained for assessing the complex indicators of the information security system when using quantum key distribution (QKD) for FOCL. On the basis of the new approach, a numerical analysis was carried out and a graphical dependence of the information entropy of the packet on the packet length in qubits was constructed for the given transfer characteristics of the FOCL. It was found that an increase in the limited packet length in bits, which meets the requirements reliability and efficiency of the operation FOCL system, leads to an increase in the value information entropy as a fraction of the packet, at a given bit rate of the network.

Information about authors:

Bayram Ganimat Ibrahimov, *Doctor of Technical Sciences, Professor, Azerbaijan Technical University, Baku Azerbaijan*
Allahverdi Oruj Orujov, *Candidate of Technical Sciences, associate professor, Azerbaijan Technical University, Baku, Azerbaijan*
Arif Hasan Hasanov, *Candidate of Technical Sciences, associate professor, Military Academy of the Republic of Azerbaijan, Baku, Azerbaijan*
Konul Mobil Tahirova, *Adjunct of the Military Academy of the Republic of Azerbaijan, Baku, Azerbaijan*

Для цитирования:
Ибрагимов Б.Г., Оруджов А.О., Гасанов А.Г., Тахирова К.М. Исследования и анализ эффективности волоконно-оптических линий связи с использованием квантовой технологии // T-Comm: Телекоммуникации и транспорт. 2021. Том 15. №10. С. 50-54.

For citation:
Ibrahimov B.G., Orujov A.O., Hasanov A.H., Tahirova K.M. (2021) Research and analysis efficiency fiber optical communication lines using quantum technology. *T-Comm*, vol. 15, no.10, pp. 50-54. (*in Russian*)

Introduction

Currently, the problem information security and the problem protecting information in modern high-speed optical telecommunication systems using FOCL are very acute. Such systems can be connected to both multiservice networks, 5G / IMT-2020 networks and public access networks, as a result which they can be exposed to threats of unauthorized access, denial of service nodes, loss of information and other threats to information security.

The efficiency of optical networks, taking into account the indicators of the information security system, is characterized by the following complex criteria [1-3]:

– p rformance network based on FOCL when using spectral technologies;

– f ult tolerance FOCL functioning from the point view cryptographic methods information protection using quantum technologies;

– information security in the FOCL-based transmission system using the quantum cryptography protocol.

The problems of information protection in optical communication networks using FOCL with a wavelength λ_i occupy one of the leading places in solving the general problem of information security. These tasks include the following [3-6]:

– resear h of the cryptographic method and information security algorithms;

– threat on optical networks when protecting the outer perimeter of communication lines;

– unau horized access FOCL with a wavelength $\lambda_i = (0{,}85,...,1{,}55)$ μm, $i = \overline{1,n}$;

– s stem analysis promising methods and algorithms cryptography using a quantum key to encrypt network traffic;

– innovative methods of increasing the limiting range quantum key distribution.

The study of the principles quantum cryptography and the analysis problems of the efficiency QKD began in [2–5] and continued in the publications many other researchers [6–11].

This article is devoted to the study of the problem efficient control quantum key distribution for FOCL and the estimation informative indicators complex optical information security systems.

General problem statement

Based on the study, it was established [3, 11] that one of the unsolved problems in complex optical systems is the synthesis effective quantum control keys and the distribution quantum keys over arbitrarily large distances $L_{\max}(\lambda_i)$, that is:

$$F_{opt}(\lambda, K) = \max_i [K_{ef.}(\lambda_i), L_{\max}(\lambda_i)], \quad i = \overline{1,n} \qquad (1)$$

where $K_{ef.}(\lambda_i)$ – number of quantum key distribution with photon wavelength λ_i.

Expression (1) at the formal level is a general formulation of the research problem and can be described by the following restrictions:

$$K_{ef.}(\lambda_i) \le K_{ef.}^{all.}(\lambda_i), \; V_b(\lambda_i) \ge V_b^{all.}(\lambda_i),$$
$$L_{\max}(\lambda_i) \ge L_{\max.}^{all.}(\lambda_i), \; i = \overline{1,n}, \qquad (2)$$

where $V_b(\lambda_i)$ – bit rate transmission over spectral communication channels with WDM technology and with frequency division of channels at a wavelength λ_i, $i = \overline{1,n}$.

The last inequality (2) characterizes the required set of quantum key distribution, the bit rate of photon transmission $V_b^{all.}(\lambda_i)$ and the required transmission range $L_{\max}(\lambda_i)$ quantum key with wavelength λ_i, $i = \overline{1,n}$.

These sets of parameters define the required performance complex FOCL optical systems using efficient quantum technology protocols.

To formalize the problem, a new approach is proposed that will most accurately reflect the algorithms for the operation QKD systems using efficient quantum cryptography protocols.

Analysis of quantum cryptography protocols

Note that for practical reasons, photons are the most popular physical systems for implementing quantum key distribution. However, a significant limitation is the fact that most of the photons are scattered or absorbed before entering the receiving optical module or optical receiver-detector. Therefore, the solution to the above problem – research and analysis complex performance indicators of the FOCL functioning, using promising quantum technologies and quantum cryptography protocols is the most relevant.

In works [3, 7] the analysis of methods transfer characteristics fiber-optic communication lines based on WDM spectral technologies is carried out. Methods information protection in modern optical communication networks [4, 6, 12, 13] from unauthorized access and the quantum key distribution algorithm QKD are considered.

The authors of [6, 12-14] considered information-theoretic methods information security with quantum technologies and algorithms for the operation of the main single-photon protocols quantum cryptography BB84, B92, 4 + 2, with six states, EPR (E91 - Einstein-Podolsky-Rosen) Goldenberg-Vaidman, Koashi-Imoto, EPR-E91 and SARG04.

Considering the critical FOCL length, the average number of photons in a pulse, the secrecy of the QKD distribution, and the resistance to the PNS attack, modern quantum cryptography protocols BB84 & B92 & SARG04 were selected.

Descriptions and studies of the functioning FOCL

It is known [3, 11, 14] that the security of the transmission optical information transmitted over a quantum-cryptographic communication channel is due to the physical principles quantum mechanics. In [6, 10, 4], the problem crypto-protection transmitted FOCL optical signals using quantum technologies was investigated for a specific, specific scenario PNS attack - an attack with splitting by the number of photons.

In this case, QKD can be 128, 196 or 256-bit in length and varies with a frequency up to 100 Hz [13]. If the FOCL uses a 56-qubit key, with which you can encode 64 bits of information.

To organize confidential communication at the network level, the algorithms for the operation of the optical information transmission system are carried out using quantum states, secrecy is ensured by taking into account the level errors $Q_{BER} \le Q_{BER}^{all.}$ in the quantum channel, and the quantum key is distributed to the ends of the quantum channel.

From the description [3, 6, 14] it can be seen that FOCL is represented as a directed graph. In this case, the optical communication system and its point-to-point network topology are set in the form of a graph:

$$G=(V,E),\ V=[v_j,\ j=1,2,...,N_{y3}],\ E=(ke,kd), \quad (3)$$

wher V – many optical network nodes; E – many of its arcs-quantum communication channels.

Based on the network topology, consider formal setting of the problem and denote the set users and the set unauthorized access points:

$$\Lambda=\{1,...,k,...,n\},\ \Omega=\{1,...,j,...,m\},$$
$$\forall(k,j),\ k\in\Lambda\ ,\ j\in\Omega \quad (4)$$

Now, on the basis of (3) and (4), it is possible to determine the critical parameters of the FOCL, combining some criteria – the threat S_{kj}, threat probability P_j and distance L_{kj}:

$$L_{FOCL}^{\max}(\lambda_i)=\max_{k,j}[S_{kj},P_j,L_{k,j},\alpha_{kz}(\lambda_i)],$$
$$k=\overline{1,n},\ j=\overline{1,N} \quad (5)$$

where $\alpha_{kз}(\lambda_i)-$ kilometric attenuation coefficient in FOCL when implementing quantum key distribution with wavelength λ_i, dB/km.

Threat probability P_j, taking into account the risk category R, vulnerability probabilities P_y and the cost losing a message C_n is expressed as follows:

$$P_j=\frac{R}{P_y}\cdot C_n^{-1},\quad j=\overline{1,N} \quad (6)$$

Expressions (5) and (6) represent the formulation of the general problem in the case using the indicators single-mode FOCL with a single-photon protocol quantum cryptography, where $\lambda_i=(1.31,...,1.55)$ μm.

Analysis and estimation of the quantum channel length taking into account the PNS attack

Let us consider how the maximum quantum channel length is estimated in a PNS attack on FOCL using quantum cryptography protocols [6, 7].

Let us assume that the number photons in an optical pulse is distributed according to Poisson's law

$$P(m)=[\mu^m\cdot\exp(-\mu)]/m!,\ \ m=0,1,2,..., \quad (7)$$

where $\mu-$ average number of photons or mathematical expectation.

Taking into account (7), we can determine the probability of emission of a state with one photon and this is equal to: $P(m=1)=\mu\cdot\exp(-\mu)$. Suppose, $m\geq 2$, this means the probability generating a pulse with several photons and is equal to

$$P(m\geq 2)=1-\exp(-\mu)-\mu\cdot\exp(-\mu) \quad (8)$$

In the last expressions, the term characterizes the probability of the vacuum component, that is, the state of the system without photons. In this case, the fraction photons that will reach the FOCL receiver in the channel $L_{\max}(\lambda_i)$ with damping factor $\alpha_{kз}(\lambda_i)$ is equal to:

$$N(m)=[P(m=1)+P(m\geq 2)]\cdot 10^{-\alpha_{kz}(\lambda_i)\cdot L_{\max}(\lambda_i)/10} \quad (9)$$

From expressions (8) and (9) it follows that the goal countering a PNS attack on FOCL using the BB84 & B92 quantum cryptography protocols is to increase the maximum length communication lines: the greater it is $L_{\max}(\lambda_i)\geq L_{\max}^{all.}(\lambda_i)$ the more stable are optical systems using the quantum protocol. In addition, in the above formula, a conservative estimate in favor Eve was used under the effect PNS attack [12, 13]. Since the probability reaching the receiving side differs for states with different numbers photons, and the lower the probability reaching the FOCL receiver, the greater the Eve's ability to intercept.

The analysis showed that technical limitations with an unavoidable attenuation factor $\alpha_{kz}(\lambda_i)$ in real quantum channels, FOCL can lead to a loss of protocol secrecy due to the possibility using a PNS attack.

Informative characteristics of photon sources

Quantum cryptography as a science was born in 1984, when the first quantum key distribution protocol, called BB84 (Bennett & Brassard), was developed. The main advantage quantum cryptographic protocols over classical ones is the rigorous theoretical substantiation their resistance to various threats. However, on the basis research [6, 9, 10], it was found that one of the unsolved problems quantum key distribution is the question how to distribute a quantum key over arbitrarily large distances when used in fiber-optic communication lines, that is $L_{FOCL}(\lambda_i)\to L_{\max}(\lambda_i)$. In this case, the source photons is an infrared laser with a wavelength of 1.550 μm.

For practical reasons, photons are the most popular physical systems for implementing QKD. However, a significant limitation is the fact that most photons m are scattered and absorbed before reaching the receiver. In this case, the task for the analysis of informative characteristics is as follows:

$$\alpha_{kз}(\lambda_i)\leq\alpha_{kз}^{don.}(\lambda_i),\ \ H(m)\leq H_{\max}(m), \quad (10)$$

where $H(m)-$ informational entropy of photon sources m.

Suppose the transmission QKD via FOCL is realized in the form streams binary optical photons and the number photons in a message composed symbols N is determined by the formula [4]:

$$H(m,N)=-N\sum_{i=1}^{M}p_i(m)\ell og_2\ p_i(m), \quad (11)$$

Expression (11) is informational entropy that characterizes uncertainty. Based on quantum technology, the optical system is identified by a vector (wave function) $\psi(c_i,e_i)=\sum_{i=1}^{M}c_i|e_1\rangle$ carries a bit uncertainty

$$H[\psi(c_i,e_i)]=-N\sum_{i=1}^{M}|c_i|^2\ \ell og_2|c_i|^2, \quad (12)$$

Based on (12), a physical system can be described as a qubit identified with the vector $\psi(c_i,e_i)=c_1|e_1\rangle+c_2|e_2\rangle$, containing $H[\psi(c_1,e_1)]$.

Expression (12) is equal to the total number of photons contained in the packet of the quantum key if the transmission of their elements is independent.

Taking into account (12), we can take a photon as a qubit – as a quantum bit and is equal to

$$\psi(c_i, e_i) = c_1|0\rangle + c_2|1\rangle, \quad (13)$$

where c_1, c_2 – arbitrary complex coefficients, the sum squares of the moduli which is equal to 1: $|c_1|^2 + |c_2|^2 = 1$.

For a qubit, the state with the maximum informational entropy has the form:

$$H_{\max}[\psi(c_i, e_i)] = \frac{1}{\sqrt{2}}[(c_1|e_1\rangle + (c_2|e_2\rangle] = \frac{1}{\sqrt{2}}[(|0\rangle + (|1\rangle] \quad (14)$$

From (14) it follows that in this case, the task is reduced to ensuring the transfer of the maximum number photons $H_{\max}[\psi(c_i, e_i)]$ appropriate choice quantities N and $p_i(m) = |e_i|^2 = c_i$ – probability of state realization e_i when measuring photons in the basis:

$$T_m = N \cdot \sum_{i=1}^{M} |c_i|^2 \cdot t_i, \quad \sum_{i=1}^{M} |c_i|^2 = 1 \quad . \quad (15)$$

Based on (12), (13), (14) and (15), the proposed task is to establish in FOCL such a relationship between the durations photons and the probabilities their generation $\sum_{i=1}^{M} |c_i|^2$, at which the maximum range quantum key distribution is provided.

Numerical analysis of the quantum key distribution indicator

In figure 1, a graphical dependence of the information entropy is plotted as a fraction of the packet size on the packet length L_n in qubits taking into account the bit rate optical signals $V_b(\lambda_i)$ and attenuation coefficient $\alpha_{kz}(\lambda_i)$ FOCL.

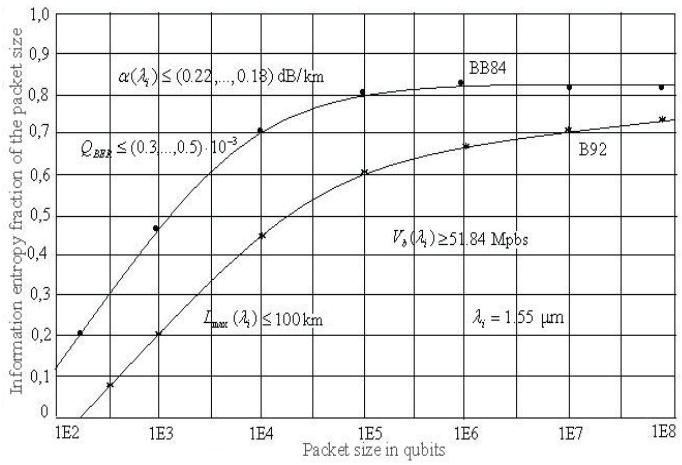

Figure 1. Graphical dependence information entropy as a fraction of the packet size on the packet length in qubits, taking into account the attenuation coefficient FOCL

Analysis of the graphical dependence $H(L_n, L_k) = F[V_b(\lambda_i), L_n, \alpha(\lambda_i)]$ shows that an increase in the limited packet length in bits that meet the requirements of reliability and robustness to PNS attacks leads to an increase in the entropy size as a fraction of the packet, for a given bit rate of the FOCL network $V_b(\lambda_i) \ge 25$ Mbps, error rate $Q_{BER} = (3.0,...,5.0)\%$ and attenuation coefficient $\alpha_{kz}(\lambda_i) \le (0.22,...,0.18)$ dB/km. Its noticeable change begins with the values $L_n \ge (1E4,...,1E5)$ of the qubits. In addition, the presented graphical dependence characterizes the network performance and estimates information entropy for various packet sizes.

Conclusions

The efficiency FOCL with the use quantum technology is investigated and complex criteria of the information security system and quantum cryptography protocols are selected, taking into account the resistance to various threats. The main tasks quantum cryptography and quantum key transfer are analyzed.

As a result of the study, a new approach was proposed for studying the efficiency quantum key distribution, informative characteristics sources optical photon fluxes and quantum cryptography protocols under the influence of a PNS attack.

On the basis of the new approach, analytical expressions are obtained for evaluating the characteristics of information entropy as a fraction of the packet size, the critical length quantum channel taking into account the PNS attack, and indicators complex optical information security system when using quantum key distribution systems.

References

1. Ryabko B.Ya., Fionov A.N. (2020). Fundamentals modern cryptography and steganography. Moscow: Hotline – Telecom. 232 p.

2. Korzhik V.I., Yakovlev V.A. (2016). Fundamentals of cryptography: SP .:NTs Intermedia, 296 p.

3. Ibrahimov B.G., Jafarova E.M. (2019). Analysis of information security methods in telecommunication systems using quantum cryptography. *Proceedings of the VIII International Conference "Technical Universities: Integration with European and World Education Systems"*. Izhevsk TU. Russia, Izhevsk. P. 404-410.

4. Gurevich I.M. (2011). Atoms, Molecules and Fundamental Restrictions on the Information Characteristics of Systems. *Information Technologies*, no9. P. 2-9.

5. Pozdnyakov A.M. (2019). Review of promising methods for overcoming the range threshold quantum key distribution. *Second Russian School of Quantum Technologies, Russia, Krasnaya Polyana*. P. 9-10.

6. Ibrahimov B.G., Mamedov R.M., Mamedov T.G. (2021). Research of the efficiency fiber-optic communication lines using quantum technology. *Proceedings of the XV – International Industrial Scientific and Technical Conference "Information Society Technologies"*. MTUCI, Moscow. Vol. 1. P. 37-39.

7. Kulik S.D. (2003). Quantum cryptography. Part 2. *Photonics*, no.3, P. 56-59.

8. Ribordy G., Gautier J. D., Gisin N. (1998). Automated 'plug & play' quantum key distribution. *Elec. Lett.*, 34. P. 2116-2117.

9. Bienfang J.C. (2004). Quantum key distribution with 1.25 Gbps clock synchronization. – *Optic Express*, Vol.12, Issue 9. pp.2011-2016.

10. Eliseev V.A. (2019). Distributed networks of quantum key distribution for information security. *2-nd Russian School of Quantum Technologies*, Russia, Krasnaya Polyana. P. 32-38.

11. Gorbunov A.V., Zachinyaev Yu.V., Plenkin A.P. (2019). Design of secure optical telecommunication systems. Rostov-on-Don: Southern Federal University. 126 p.

12. Bennett C. and Brassard G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing IEEE*. New York. P. 175-179.

13. Pearson D. (2004). High-speed QKD Reconciliation using Forward Error Correction. *Proc. 7th International Conference on Quantum Communication, Measurement and Computing*. P. 299-302.

14. Petrakov A.V., Lagutin V.S. (2007). Protection of subscriber teletraffic. Moscow: Energo-atomizdat. 528 p.

ИССЛЕДОВАНИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОЙ ТЕХНОЛОГИИ

Ибрагимов Байрам Ганимат оглы, *Азербайджанский Технический Университет, Баку, Азербайджан,* ***i.bayram@mail.ru***
Оруджов Аллахверди Орудж оглы, *Азербайджанский Технический Университет, Баку, Азербайджан*
Гасанов Ариф Гасан оглы, *Военная Академия Вооруженных Сил Азербайджанской Республики, Баку, Азербайджан*
Тахирова Конул Мобил кызы, *Адъюнкт Военная Академия Вооруженных Сил Азербайджанской Республики, Баку, Азербайджан*

Аннотация
Проведен анализ показателей эффективности волоконно-оптических линий связи (ВОЛС) с использованием квантовой технологии на базе архитектурной концепции NGN (Next Generation Network) и будущих сетей FN (Future Networks), для построения высокоэффективных оптических телекоммуникационных сетей, поддерживающих широкий спектр криптостойкости. Выбраны комплексные критерии эффективности ВОЛС с использованием таких квантовых технологии, как производительность сети при использовании WDM (Wavelength Division Multiplexing) технологии, характеристики информационной безопасности при использовании протоколов квантовой криптографии с учетом стойкости для различных угроз, информативные характеристики источников фотонов. Предложен новый подход для исследования и оценки комплексных показателей сложных оптических систем защиты информации и эффективного управления множества квантовых систем распределения ключей для ВОЛС. На базе предложенного подхода исследованы эффективности квантового распределения ключей, возможности протоколов квантовой криптографии при воздействии PNS-атаки (PNS – Photon Number Splitting Attack) и информационная энтропия характеристики источников потоков кубит оптических фотонов. Получены аналитические выражения для оценки комплексных показателей системы защиты информации при использовании квантового распределения ключей для ВОЛС.

Ключевые слова: *квантовое распределение ключа, ВОЛС с использованием квантовой технологии, эффективность, протоколы квантовой криптографии, информационная энтропия, угроза безопасности, PNS-атаки.*

Литература

1. *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии и стеганогрфии. М.: Горячая линия – Телеком, 2020. 232 с.
2. *Коржик В.И., Яковлев В.А.* Основы криптографии: СПб.: НЦ Интермедиа, 2016. 296 с.
3. *Ибрагимов Б.Г., Джафарова Э.М.* Анализ методов информационной безопасности в системах телекоммуникаций с использованием квантовой криптографии // Материалы VIII Международной конференции "Технические университеты: интеграция с европейскими и мировыми системами образования". Ижевский ТУ. Россия, Ижевск. 2019. С. 404-410.
4. *Гуревич И.М.* Атомы, молекулы и фундаментальные ограничения на информационные характеристики систем // Информационные технологии, 2011, №9. С. 2-9.
5. *Поздняков А. М.* Обзор перспективных способов для преодоления порога дальности квантового распределения ключей // Вторая Российская школа по квантовым технологиям, Россия, Красная Поляна, 2019. С. 9-10.
6. *Ибрагимов Б.Г., Мамедов Р.М., Мамедов Т.Г.* Исследования эффективности волоконно-оптических линий связи с использованием квантовой технологии// Сборник трудов XV - Международной отраслевой научно-технической конференции "Технологии Информационного Общества". Том 1. М.: МТУСИ. 2021. С. 37-39.
7. *Кулик С.Д.* Квантового криптография. Часть 2 // Фотоника, 2003, №3. С. 56-59.
8. *Ribordy G., Gautier J. D., Gisin N.* Automated 'plug & play' quantum key distribution // Elec. Lett., 1998. 34, pp. 2116-2117.
9. *Bienfang J.C.* Quantum key distribution with 1.25 Gbps clock synchronization // Optic Express, Vol.12, 2004. Issue 9, pp. 2011-2016.
10. *Елисеев В.А.* Распределенные сети квантового распределения ключа для защиты информации // 2-ая Российская школа по квантовым технологиям, Россия, Красная Поляна, 2019. С. 32-38.
11. *Горбунов А.В., Зачиняев Ю.В., Пленкин А.П.* Проектирование защищенных оптических телекоммуникационных систем. Ростов н/Д: ЮФУ, 2019. 126 с.
12. *Bennett C.and G. Brassard.* Quantum cryptography: Public key distribution and coin tossing in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing IEEE.* New York, 1984, pp. 175-179.
13. *Pearson D.* High-speed QKD Reconciliation using Forward Error Correction // Proc. 7th International Conference on Quantum Communication, Measurement and Computing, 2004, pp. 299-302.
14. *Петраков А.В, Лагутин В.С.* Защита абонентского телетрафика. М.: Энерго-атомиздат, 2007. 528 с.

Информация об авторах:
Ибрагимов Байрам Ганимат оглы, *д.т.н., профессор Азербайджанского Технического Университета, Баку, Азербайджан*
Орусов Аллахверди Орудж оглы, *к.т.н доцент Азербайджанского Технического Университета, Баку, Азербайджан*
Гасанов Ариф Гасан оглы, *к.т.н., доцент Военного Академия Вооруженных Сил Азербайджанской Республики, Баку, Азербайджан*
Тахирова Конул Мобил кызы, *Адъюнкт Военного Академия Вооруженных Сил Азербайджанской Республики, Баку, Азербайджан*