REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227 **https://doi.org/10.32014/2018. 2518-1483.1**
Volume 5, Number 321 (2018), 5 – 11

UDC 004.056.55:004.421.5

B. Akhmetov[1], S. Gnatyuk[2], T. Zhmurko[2], V. Kinzeryavyy[2], Kh. Yubuzova[3]

[1]Turan University, Almaty, Kazakhstan;
[2]National Aviation University, Kiev, Ukraine;
[3]Kazakh National Research Technical University named after K.I. Satpayev (Satbayev University), Almaty, Kazakhstan
E-mail: bakhytzhan.akhmetov.54@mail.ru, s.gnatyuk@nau.edu.ua, taniazhm@gmail.com, 0werl0rd@ukr.net, hali4a@mail.ru

EXPERIMENTAL RESEARCH OF THE SIMULATION MODEL FOR DETERMINISTIC SECURE COMMUNICATION PROTOCOL IN QUANTUM CHANNEL WITH NOISE

Abstract. Today there are many methods and approaches used to ensure the privacy of message transmission without encryption. The most advanced technology is quantum cryptography and quantum secure direct communication in particular. It allows information transmission using open channel without previous encryption. From this viewpoint, in this work there was carried out experimental research of the proposed simulation model for deterministic secure direct communication protocol in the quantum channel with noise for qutrit pairs in eavesdropping control mode. Given results can be used for quantum cryptography systems constructing and optimization from viewpoint of asymptotic security as well as its operation rate.

Key words: information security, quantum cryptography, deterministic protocol, quantum key distribution, quantum secure direct communication, qubit, qutrit.

Introduction

The theory of quantum mechanics, which is the basis of quantum cryptography, allows to improve all possible modern methods of ensuring the information transmission security, to solve the problems of encryption keys distribution that exist in classical (non-quantum) cryptography. Quantum secure direct communication protocol provide secrecy (this term in quantum cryptography denotes confidentiality and/or privacy) of the messages transmission without the use of any encryption methods, since this secrecy is guaranteed by the incomprehensibility of the postulates of quantum physics [1-2]. In deterministic quantum protocols [1,3] two-level, and more often multi-level quantum states of quantum systems groups are used to encode the source text of a secret message that are transmitted via a quantum communication channel. The laws of quantum physics guarantee the detection of eavesdropping in the communication channel, which allows legitimate users (e.g. subjects / users A and B) to detect the intruder (user E) during the communication session and to interrupt the communication session.

Related works

Nowadays, there have been carried out many researches of various types of deterministic quantum secure communication protocols, which can be implemented already on the basis of the available and used technical equipment for the information transmission [4]. This version of the protocol uses two Bell states of an entangled pair of qubits and allows one bit of classical information to be transmitted over one protocol cycle [1]. Using four states of a pair of Bell qubits, that is, using quantum superdense coding, it is possible to increase the number of transmitted bits per cycle by two times [2]. In order to build up the

information capacity, instead of the entangled pairs of qubits, there can used their triples, quarks, etc. The protocol with the entangled states of the Greenberger-Horn-Zeilinger (GHZ) triples and quadruples of qubits provides an information capacity equal to *n* bits per cycle, that is, the amount of qubits in the used states of GHZ. Also, in order to increase the information capacity of deterministic protocols, it is possible to use entangled states of multi-level quantum systems - for example, in works [6, 7] a protocol using Bell states of a pair of three-level systems (qutrits) and quantum superdense coding for qutrits. Various types of attacks, in particular a general incoherent attack on various versions of the protocol, including a protocol with pairs of qutrits, were considered in works [5-8]. During an attack, the intruder E can obtain some information before he is detected [8, 11-13]. The method of enhancing secrecy, based on the use of random invertible matrices [13], was investigated in work [14]. The model of the deterministic protocol proposed by the authors in work [15] with the use of an alternative method of enhancing secrecy [16] allows to conclude that there is no fact of eavesdropping.

Theoretical researches carried out in [15] confirm the occurrence of problems of synchronous fixation of the changes occurring in the states of transmitted photons, from collective effects in the channel of natural noise and from the intruder. The creation of a model simulating the operation of the protocol in the eavesdropping control mode will provide practical recommendations on the use of a quantum protocol in a channel with noise. Therefore, the purpose of this article is an experimental research of the simulation model of a deterministic protocol with pairs of qutrits in the eavesdropping control mode in a channel with noise.

Description of the method

As a result of the research of the deterministic protocol in a channel with noise, in the eavesdropping control mode there was revealed the problem of constructing a model allowing investigating a joint attack of the intruder and natural quantum noise in the channel. In the eavesdropping control mode there is considered the case of the impact on the transmitted quitrit of the noise operator.

The model simulates the operation of a deterministic protocol with pairs of quitrits in a depolarized channel at the presence of an intruder E. during the research and modeling of the deterministic protocol operation in the eavesdropping control mode there were obtained statistical data on error levels in the bases *x, z* and their average values [15]. In addition, the model used non-quantum method of enhancing the secrecy of the deterministic protocol, which is described in detail in works [9, 16].

In order to begin the process of message transmission, the user A converts his ternary message a $(a = (a_1, \dots, a_l), i = 1, \dots, l)$ of the length $r\cdot$, then for each block there is generated a random ternary sequence G $(G = (G_1, \dots, G_l),\ i = 1, \dots, l))$ of the size $r \times l$, each block of which is G_i bitwise summed according to the module 3 with the corresponding blocks of the message a_i:

$$b_i = a_i + G_i. \tag{1}$$

Further, with the help of the deterministic protocol, the message $b, (b = (b_1, \dots, b_l), i = 1, \dots, l)$, resulting according to (1), is transmitted to user B on the quantum channel. In case of message interception or its part by the intruder E, he cannot use it, because, without having randomly generated sequences G_i he cannot restore the original message a_i.

After completion of the transmission on the quantum channel, only if the users A and B are confident that the transmission session has not been overheard by the user E, the user B is transmitted sequences G_i along the classical open channel. In order to restore the original message, the user B must use the received random sequences by subtracting them from the corresponding message blocks according to (2):

$$a_i = b_i - G_i. \tag{2}$$

The length of the block *r* is chosen if a high level of stability can be achieved, and if the value of the probability of successful attack of the intruder of the user E after the transmission of one block s $(s(I, q, d) = \left(\frac{1-q}{1-q\cdot(1-d)}\right)^{I/I_0}$ was insignificant:

$$r = -kI_0 / \lg((1-q)/(1-q\cdot(1-d))), \quad (3)$$

where k - the exponent for calculating the probability of a non-detected attack of the intruder E; I_0 - the amount of information that the intruder E can receive in one cycle of the message transmission mode, q - the probability of switching to the eavesdropping control mode, d - the error level occurring from the actions of the intruder E. As a result of an experimental research of the simulation model of a deterministic protocol with pairs of quitrites in a depolarized channel with an attack of the intruder E, there were obtained statistical data on error levels in the bases x, z and their average values (see. table. 1 in [15]). In the above table, such designations and parameter values are accepted:

1) $length = 100000$ trit - length of the transmitted ternary data;

2) $k = 4$, that is $s(I, q, d,)10^{-k}$ - an exponent of ten, in order to calculate the probability of a non-detected attack of the intruder E;

3) $q = [0{,}1; 0{,}9]$ - probability of protocol switching between the eavesdropping control modes of and message transmission;

4) r - block length;

5) $d = 1/3$ - the error level occurring from the actions of the intruder E;

6) $d_x = 0 \ldots 2/3$ - the probability of attack detecting measured in the basis x;

7) $d_z = 2/3$ - the probability of attack detecting measured in the basis z;

8) $\rho = 0 \ldots 0{,}5$ - the probability of state depolarization;

9) $(1-\rho)$ - the probability of the qubit unchanged state;

10) $q_x = q_z = 0{,}5$ - the probability of switching of the users A and B between the basis x and z;

11) d_{Eva} - the average probability of attack detecting on two basis in an ideal channel;

12) l – the amount of blocks to which the transmitted data is divided;

13) Err_x, Err_z, Err_{mean} - the error probabilities for measurements in the basis x, z and the average value for the two basises;

14) $q, (1-q)$ - the probability of switching between the eavesdropping control modes and message transmission, respectively;

15) Err_x - the probability of modeling the error for the basis x;

16) Err_z - probability of modeling the error for the basis z;

17) $MinErrlvl_x, MinErrlvl_z, MinErrlvl$ - minimum values of error levels;

18) $MaxErrlvl_x, MaxErrlvl_z, MaxErrlvl$ - maximum values of error levels;

19) $MeanErrlvl_x, MeanErrlvl_z, MeanErrlvl$ - average values of error levels.

Experimental results

Analysis of the statistical data of the experimental research of the proposed simulation model. On Fig. 1-3 there are presented the diagrams of the dependencies of the *min* value of the error levels, $MinErrlvl$ at modeling the deterministic protocol operation for different values of d_x, d_z, d_{Eva}, which are constructed on the basis of Tables 1-3.

Table 1 - Modeling results for $d_x=0$, $d_z=0{,}667$, $d_{Eva}=0{,}333$

q	p1	p2	p3	p4
0,1	0,091	0,154	0,231	0,304
0,25	0,115	0,167	0,2	0,36
0,5	0,08	0,154	0,24	0,296

Table 2 - Modeling results for $d_x=0,333$, $d_z=0,667$, $d_{Eva}=0,5$

q	p1	p2	p3	p4
0,1	0,226	0,227	0,318	0,353
0,25	0,263	0,29	0,32	0,343
0,5	0,263	0,29	0,32	0,343

Table 3-Modeling results for $d_x=0,333$, $d_z=0,667$, $d_{Eva}=0,5$

q	p1	p2	p3	p4
0,1	0,382	0,367	0,423	0,419
0,25	0,385	0,333	0,381	0,375
0,5	0,381	0,37	0,353	0,32

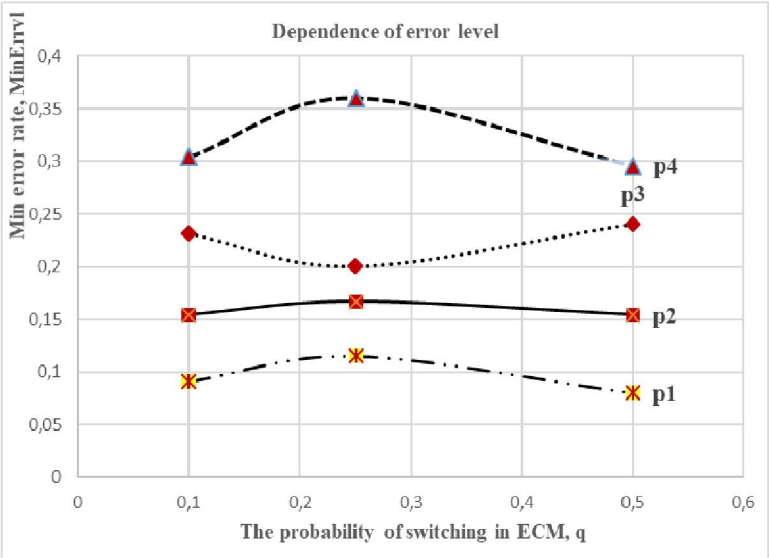

Figure 1 – Dependence of *min* error value levels, $MinErrlvl$ at modeling $d_x=0$, $d_z=0,667$, $d_{Eva}=0,333$ and the probability of depolarization of the state of quitrites from $\rho = 0,1$ to $\rho = 0,7$

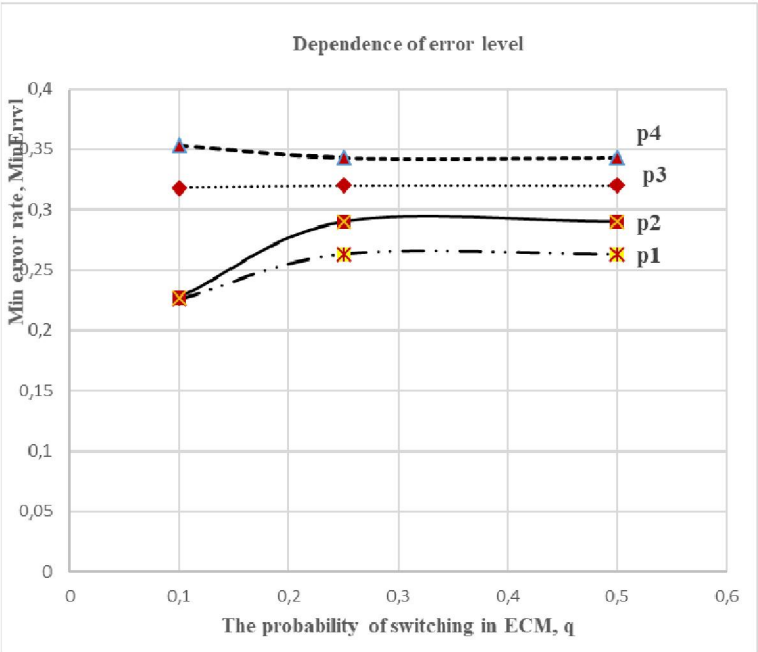

Figure 2 – Dependence of *min* error value levels, $MinErrlvl$ at modeling $d_x=0,333$, $d_z=0,667$, $d_{Eva}=0,5$ and the probability of depolarization of the state of quitrites from $\rho = 0,1$ to $\rho = 0,7$

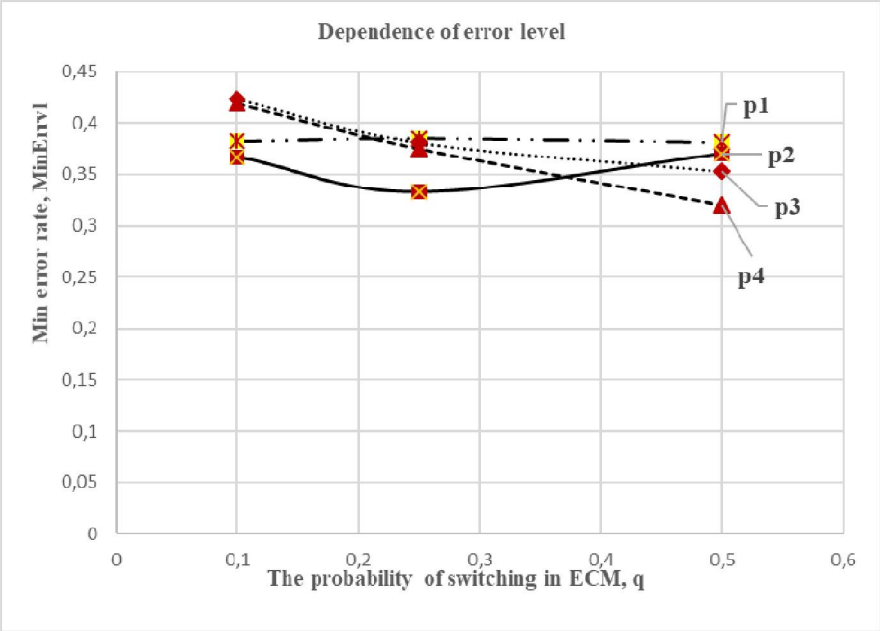

Figure 3 – Dependence of *min* error value levels, *MinErrlvl* at modeling d_x=0,333, d_z=0,667, d_{Eva}=0,5 and the probability of depolarization of the state of quitrites from $\rho = 0{,}1$ to $\rho = 0{,}7$

Analyzing Fig. 1-3, the following conclusions can be done:

1. The minimum error levels for both basises (*MinErrlvl*) are sufficiently small and in most cases less than the level of natural noise ρ (especially for $\rho \to 0{,}7$). This means that the users A and B can make an incorrect conclusion about the presence of the intruder E, therefore, at a sufficiently high level of natural noise the legitimate users must transmit a sufficiently large amount of blocks and only then decide whether there is the attack of the intruder E;

2. The probability q significantly influences the data transmission rate by a deterministic protocol - the smaller q is, the more often the data is transmitted and the higher the speed is. In addition, the length of the block r also depends on q - with the decreasing q according to the exponential law it increases;

3. At $\rho \to 0{,}7$ and at the attack of the intruder E with zero error level in one of the basis (for example, d_x=0, d_{Eva}=0,333 - figure 1), the average error level of *MeanErrlvl* almost does not exceed p, therefore legitimate users can accept incorrect decision about the absence of the attack - it is necessary to check the average level of errors in each of the basises x and z separately, in one of these basises the error level will be close to the value $2/3$;

4. For reliable detection of the attack the legitimate users should use a quantum channel with a natural noise level - in practice this means using a channel of the limited length.

Conclusion and future work

Therefore, in this work there were carried out experimental researches of the simulation model of the secure direct communication protocol in a quantum channel with noise for a pair of quitrites in the eavesdropping control mode proposed by the authors earlier. The obtained results allow legitimate users to choose the most effective strategy for secure data exchange, depending on the level of noise in the quantum communication channel. These results can be used for the construction and optimization of the quantum cryptography systems in terms of increasing the asymptotic stability of the system and the speed of its operation.

REFERENCES

[1] Bostrom K. Deterministic secure direct communication using entanglement. *Physical Review Letters*. **2002**. V. 89, issue18. doi = {10.1103/PhysRevLett.89.187902}

[2] Cai Q. Y. Improving the capacity of the Bostrom Felbinger protocol. *Physical Review A* **2004**. Vol. 69, issue 5. doi = {054301}

[3] Ostermeyer M On the implementation of a deterministic secure coding protocol using polarization entangled photons. *Optics Communications*. **2008**. Vol. 281, issue 17. P. 4540- 4544

[4] Wang Ch. Quantum secure direct communication with high dimension quantum superdense coding. *Physical Review A*. **2005**. Vol. 71, issue 4. doi = {10.1103/PhysRevA.71.044305}

[5] Vasiliu E. V. Analiz ataki passivnogo perekhvata na ping-pong protokol s polnostyu pereputannymi parami kutritov. *Vostochno evropejskij zhurnal peredovykh tekhnologij*. **2009**. № 4/ 2(40). S. 4 - 11. ISSN (print) 1729-3774, ISSN (on-line) 1729-4061 (In Russian)

[6] Zhang Zh. J. Improved Wojcik s eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. *Physics Letters A*. **2005**. Vol. 341, issue 5-6. P. 385-389. doi = {10.1016/j.physleta.2005.05.023}

[7] Deng F. G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical Review A*. **2003**. Vol. 68. Issue 4. 042317. doi ={10.1103/PhysRevA.68.042317}

[8] Korchenko O.G., Vasiliu E. V., Gnatyuk S. A., Kinzeryavyy V.M. Imitacionnaja model' ping-pong protokola s parami pereputannyh kutritiv v kvantovom kanale s shumom. *Zashhita informacii*. **2010.** №3 (48). P. 46-56. doi= {10.18372/2410-7840.12.1961}

[9] Gnatyuk S. A., Zhmurko T., Kinzeryavyy V., Yubuzova Kh. Jeksperimental'noe issledovanie metoda obespechenija stojkosti kutritovyh protokolov kvantovoj kriptografii. *Zashhita informacii*. **2016.** Vol. 18 №3. S. 218-228. doi={10.18372/2410-7840.18.10851}

[10] Gnatyuk S., Zhmurko T., Yubuzova Kh. Experimental studies of efficiency improving method for quantum cryptography. Mezhdunarodnaja nauchnaja konferencija UNITEH'16. Sbornik doklady. -Gabrovo.: **2016.** Vol. II. P. 425-430.

[11] Zhmurko T. O., Polishhuk Ju.Ja.,Yubuzova Kh. Jeksperimental'noe issledovanie metoda generirovanija tritovyh posledovatel'nostej. Aktual'nye voprosy obespechenija kiberbezopasnosti i zashhity informacii: tezisy dokladov uchastnikov i II Mezhdunarodnoj nauchno-prakticheskoj konferencii (Zakarpatskaja oblast', Mukachevskij rajon, selo Verhnee Studenoe, turisticheskij kompleks Jedel'vejs. 22-25 fevralja 2017). - M.: Izdatel'stvo Evropejskogo universiteta. **2017.** S. 76-80 (Tezisy).

[12] Pshelest M.,Gnatyuk S., Zhmurko T., Kinzeryavyy V., Yubuzova Kh. Jeksperimental'noe issledovanie metoda generirovanija tritovyh psevdosluchajnyh posledovatel'nostej dlja kriptograficheskih prilozhenij. *Zashhita informacii*. **2017.** Vol. 19. № 1. S. 67-76. doi={10.18372/2410-7840.19.11478}

[13] Vasiliu E. V. Ocenki vychislitel'noj slozhnosti ne kvantovogo sposoba usilenija bezopasnosti ping-pong protokola. *Prikladnaja radiojelektronika*. **2009**, №3. S.396–404. (In Russian)

[14] Vasiliu E. V. Sintez osnovannoj na ping-pong protokole kvantovoj svyazi bezopasnoj sistemy pryamoj peredachi soobshchenij. *Naukov prats ONAZ im. O. S. Popova*. **2009**. № 1. S. 83 -91. (In Russian)

[15] Akhmetov B., Gnatyuk S., Kinzeryavyy V., Yubuzova Kh. Model of simulation of operation of the deterministic protocol of safe communication in the quantum channel with noise. *Bulleten of national academy of sciences of the republic of Kazakhstan*. **2018.** V. 2, №372. P. 6-16. ISSN 2518-1467 (online), ISSN 1991-3494 (print)

[16] Gnatyuk S., Zhmurko T., Yubuzova K. Privacy amplification method for deterministic quantum cryptography protocols. Aktual'nye voprosy obespechenija kiberbezopasnosti i zashhity informacii: tezisy dokladov uchastnikov IV Mezhdunarodnoj nauchno-prakticheskoj konferencii Zakarpatskaja oblast', Mukachevskij rajon, selo Verhnee Studenoe. M.: Izdatel'stvo Evropejskogo universiteta, **2018.** S. 129-132.

Б. Ахметов[1], С. Гнатюк[2], Т. Жмурко[2], В. Кинзерявый[2], Х. Юбузова[3]

[1]«Тұран» университеті, Алматы, Қазақстан;
[2]Ұлттық авиациялық университеті, Киев, Украина;
[3]Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті
(Сәтбаев университеті), Алматы, Қазақстан

ШУЫ БАР КВАНТТЫҚ АРНАДА ҚАУІПСІЗДІК БАЙЛАНЫСТЫҢ ДЕТЕРМИНИСТИКАЛЫҚ ХАТТАМА ЖҰМЫСЫНЫҢ ИМИТАЦИЯЛЫҚ ҮЛГІСІНІҢ ЭКСПЕРИМЕНТТІК ЗЕРТТЕУЛЕР

Аннотация. Бүгінгі күнге шифрлауды қолданусыз хабарларды жіберудің құпиялығын қамтамасыз ету үшін көптеген әдістер мен көзқарастар бар. Ең дамыған технология кванттық криптография, соның ішінде кванттық түзу қауіпсіз байланыс. Ол ақпаратты ашық арнамен алдын ала шифрлаусыз жіберуге мүмкіндік береді. Осыған байланысты, берілген жұмыста тыңдауды бақылау режимінде кутриттер жұбы үшін шуы бар кванттық арнада авторлар ұсынған қауіпсіз байланыстың детерминистикалық хаттамасының имитациялық үлгісінің эксперименттік зерттеулері өткізілген. Алынған нәтижелер кванттық криптография жүйелерін жүйенің асимптотикалық беріктілігін және жылдамдығын жоғарлату көзқарасынан оңтайландыру және құру үшін қолдануға болады.

Түйін сөздер: ақпаратты қорғау, кванттық криптография, детерминистикалық хаттама, кванттық кілттерді тарату, кванттық түзу қауіпсіз байланыс, кубит, кутрит.

Б. Ахметов[1], С. Гнатюк[2], Т. Жмурко[2], В. Кинзерявый[2], Х. Юбузова[3]

[1]Университет «Туран», Алматы, Казахстан;
[2]Национальный авиационный университет, Киев, Украина;
[3]Казахский национальный исследовательский технический университет имени К.И. Сатпаева (Сатпаев университет), Алматы, Казахстан

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ИМИТАЦИОННОЙ МОДЕЛИ РАБОТЫ ДЕТЕРМИНИСТИЧЕСКОГО ПРОТОКОЛА БЕЗОПАСНОЙ СВЯЗИ В КВАНТОВОМ КАНАЛЕ С ШУМОМ

Аннотация. На сегодняшний день существует много методов и подходов, используемых для обеспечения секретности передачи сообщений без применения шифрования. Самая развитая технология это квантовая криптография, в частности квантовая прямая безопасная связь, позволяющая передавать информацию по открытому каналу без предварительного шифрования. В этой связи, в данной работе проведены экспериментальные исследования предложенной авторами имитационной модели детерминистического протокола безопасной связи в квантовом канале с шумом для пары кутритов в режиме контроля подслушивания. Полученные результаты могут быть использованы для построения и оптимизации систем квантовой криптографии с точки зрения повышения асимптотической стойкости системы и скорости ее работы.

Ключевые слова: защита информации, квантовая криптография, детерминистический протокол, квантовое распределение ключей, квантовая прямая безопасная связь, кубит, кутрит.

Information about the authors:

Bakhytzhan Akhmetov - Doctor of Technical Sciences, Professor, Turan University, https://orcid.org/0000-0001-5622-2233;

Sergey Gnatyuk - Doctor of Technical Sciences, Associate Professor, Leading Researcher in Cybersecurity R&D Lab, National Aviation University, https://orcid.org/0000-0003-4992-0564;

Tatyana Zhmurko - Ph.D., Senior Researcher in Cybersecurity R&D Lab, National Aviation University, https://orcid.org/0000-0001-9036-6556;

Vasily Kinzeryavy - Ph.D., Associate Professor, National Aviation University, https://orcid.org/0000-0002-7697-1503;

Khalicha Yubuzova - doctoral student, Satbayev University, hali4a@mail.ru, https://orcid.org/0000-0001-8892-6745