System of Cryptographic Protection of Information Based On Deterministic Chaos

Baimuhamedov M. F., Atanov S.K., Zhunusov K. M., Zhikeyev A.A., Bugubaeva A.U., Bulaev A.G.,

Abstract: ***In this paper we present a software system for cryptographic information protection based on deterministic chaos. The program system functionality includes encryption and decryption of text and graphic information on the basis of a random number generator, which is played by the Lorentz attractor. The use of an attractor in this program system guarantees randomness and absolute randomness when issuing numbers, limited only by the initial parameters. It is also necessary to transfer encryption parameters, excluding the possibility of its interception, because Encryption parameters are used in the program as decryption keys. After the process of text encryption, the program performs a frequency analysis of the input and output files. Accordingly, the frequency of a certain group of letters, which is vulnerable to frequency analysis, must be clearly expressed in the input file. In the output file, the frequency should be stable and uniform, thereby proving the effectiveness of encryption.***

Keywords: ***cryptographic protection, data encryption, deterministic chaos, information, Lorentz attractor, program system.***

I. INTRODUCTION

In recent decades, there has been great interest in the possibility of using deterministic chaos for data encryption. At a conceptual level between chaotic systems and cryptographic systems, there is a kind of interconnection. The known properties of chaotic systems (exponential divergence of trajectories, mixing) can be useful in the development of new encryption schemes [1].

As is known, the reason for the appearance of chaos is instability (sensitivity) with respect to initial conditions and parameters: a small change in the initial condition with time leads to arbitrarily large changes in the dynamics of the system.

The chaotic behavior observed in time arises not because of external noise sources (they are not in the Lorentz equations), not because of an infinite number of degrees of freedom (there are only 3 degrees of freedom in the Lorentz system) and not because of the uncertainty associated with quantum mechanics (The systems considered are purely classical).

The main reason for the irregularity is determined by the property of nonlinear systems to exponentially rapidly build up initially close trajectories in a limited region of the phase space (for example, three-dimensional in the Lorentz system) [2].

Thus, it becomes almost impossible to predict the long-term behavior of such systems, since real conditions can be set only with finite accuracy, and errors increase exponentially.

II. METHODOLOGY

We present a program for cryptographic information protection based on deterministic chaos. The program's functionality includes encryption (decryption) of text and graphic information on the basis of a random number generator, in which the Lorentz attractor appears. The use of an attractor guarantees randomness and absolute randomness when issuing numbers, limited only by the initial parameters. It is also necessary to transfer encryption parameters, excluding the possibility of its interception, because Encryption parameters and are decryption keys. After the text is encrypted, the program performs a frequency analysis of the input and output files. Accordingly, the frequency of a certain group of letters, vulnerable to frequency analysis, must be clearly expressed in the input file. In the output file, the frequency should be stable and uniform, thereby proving the effectiveness of encryption.

The Lorentz attractor is a compact invariant set L in the three-dimensional phase space of a smooth flow that has a certain complex topological structure and is asymptotically stable, it is Lyapunov stable, and all trajectories from some neighborhood L tend to L at $t \to \infty$ [3,4].

The Lorenz attractor was found in the numerical experiments of Lorentz, who investigated the behavior of trajectories of a nonlinear system (1).

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(r - z) - y \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Baimuhamedov M. F*., PhD in technical sciences, Z. Aldamzhar Kostanay Social and Technical University, Kostanay, Kazakhstan. Email: bmf45@mail.ru

Atanov S.K., PhD in technical sciences, professor, L. Gumilev ENU, Astana, Kazakhstan. Phone number: +77172709500

Zhunusov K.M., PhD in Technical Sciences, Associate Professor, Head of the Department of Information Technology and Automation M. Dulatov KEEU, Kostanay, Kazakhstan. Email: zunusov_k@mail.ru

Zhikeyev A.A., PhD in technical sciences, dean of the faculty of information technology A.Baitursynov Kostanay State University, Kostanay, Kazakhstan. Email*:* a_zhikeev@mail.ru

Bugubaeva A.U., PhD in Agricultural Sciences, Deputy Head of the Regional "Smart Center" of A.Baitursynov Kostanay State University, Kostanay, Kazakhstan. Email: alia-almaz@mail.ru

Bulaev A.G., PhD in biological sciences, Head of the Laboratory of Chemolithotrophic Microorganisms, Russian Federation. Email: bulaev.inmi@yandex.ru

With the following values of the parameters: σ = 10, r = 28, b = 8/3.

Consider changes in the behavior of the solution of the Lorentz system for various values of the parameter r:

- r <1 - the origin is the attractor, there are no other stable points.
- 1 <r <13,927 - the trajectories are spirally approaching (this corresponds to the presence of damped oscillations) to two points whose position is determined by the formulas:

$$\begin{cases} x = \pm\sqrt{b(r-1)} \\ y = \pm\sqrt{b(r-1)} \\ z = r-1 \end{cases}$$

These points determine the state of the steady-state convection mode when a structure is formed in the layer from the rotating fluid shafts.

- r≈13,927 - if the trajectory leaves the origin, then, after making a complete revolution around one of the stable points, it will return back to the starting point - two homoclinic loops arise. The concept of a homoclinic trajectory means that it leaves and comes to the same equilibrium position.
- r> 13,927 - depending on the direction, the trajectory comes to one of two stable points. Homoclinic loops degenerate into unstable limit cycles, and a family of complexly arranged trajectories that is not an attractor, but rather a repulsive trajectory from itself, also appears.
- r≈24,06 - trajectories now don't lead to stable points, but asymptotically approach unstable limit cycles - the Lorentz attractor itself arises. However, both stable points are preserved up to r≈24.74.

In the program, crypto-conversion is implemented as a combination of random number generation using dynamic chaos (keys) and using the Vernam method for text encryption.

Vernam's cipher is a system of symmetric encryption, is one of the simplest cryptosystems and the only encryption system for which absolute cryptographic stability has been proved [5].

To obtain ciphertext, the plaintext is combined by an exclusive-OR operation with the key. In this case, the key must have three critically important properties:

- have a randomly uniform distribution: $P_k(k) = 1/2^N$, k – key, N - The number of binary characters in the key;
- match in size with the given plain text;
- apply only once.

When encrypting the plain text, each character is represented in binary form. The encryption key is also represented in binary form. Encryption of the source text is carried out by modulo 2 addition of binary plaintext characters with binary symbols of the key Y = P□K. Decryption consists in adding modulo 2 characters of ciphertext with a key (Figure 1).

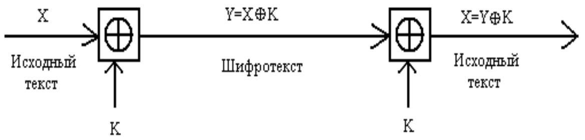


Fig. 1. Scheme of the Vernam encryption system.

Without knowledge of the key, such a message cannot be analyzed. Even if it were possible to go through all the keys, the result would be all possible messages of a given length, plus a huge number of meaningless decipherings (a messy combination of letters). But even among the meaningful decipherings, there would be no way to choose what was sought. When a random sequence (key) is combined with non-random (open text), the result of this (ciphertext) is completely random and, therefore, devoid of those statistical features that could be used to analyze the cipher.

In practice, you can physically transfer media with a long, truly random key once, and then forward messages as necessary. This is the basis for the idea of cryptographic codes: the cryptographer, through a diplomatic mail or in person, is provided with a notebook, each page of which contains keys. The same pad is also on the receiving side. The pages used are destroyed.

In addition, if there are two independent channels, in each of which the probability of interception is low but different from zero, the Vernam cipher is also useful: one channel can send an encrypted message, the other is a key. In order to decrypt the message, the interceptor should listen to both channels.

Vernam's code can be used if there is a one-way protected channel: the key is transmitted to one side under the protection of the channel, messages to the other side are protected by a key.

The main problem is the transfer of the encryption key. The symmetric Vernam encryption method is used. In our case, the encryption key is the encryption parameters (the initial values of the Lorenz attractor).

You can use a variety of encryption methods to hide the parameters. Then, through a special closed communication channel, transfer this key to the receiving party. This method is used quite often, and its implementation is quite simple. But this method requires strict control over the closed communication channel, the secrecy of the fact of the transfer of the key, ensuring the integrity of the data.

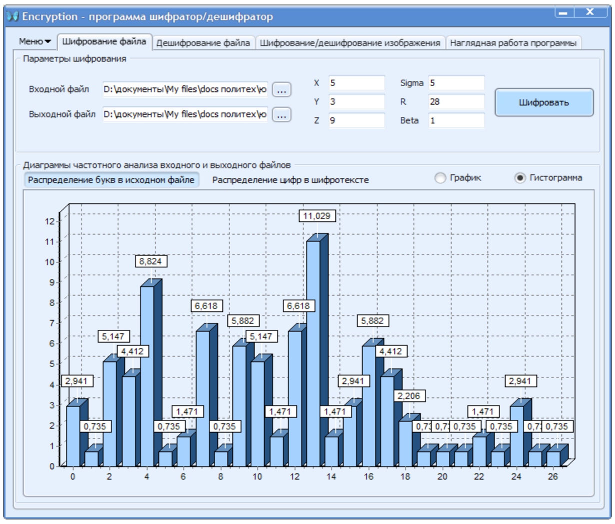
It was decided to use a different approach to this problem. The general principle is that encryption parameter are transmitted along with the ciphertext, but the very fact that the parameters are transmitted in this way is hidden, i. The element of steganography is used.

So, the program encrypts text from the input file and writes ciphertext to the output file. Then the encryption parameters are written in a certain order to the program created an alternative stream of the same output file.

The software product was created in the Delphi 7.0 integrated development environment. For each operation (encryption / decryption) a separate tab is highlighted. There is also a tab for a visual presentation of the algorithm of the program. It is possible to view the Lorenz attractor in two-dimensional space with given initial parameters.

After starting the program, the user will see the first tab "File Encryption". To start encryption, you must select an input text file for encryption. The choice of the output file (the file where ciphertext with encryption parameters will be recorded) is made similarly.

After selecting the files and filling in the parameters (X, Y, Z, Sigma, Beta, and R), you must click the Encrypt button. When the operation is successfully completed, the ciphertext is written to the output file, and an alternative stream is created in the file itself, in which encryption parameters are stored. Also in the current tab, there will be a histogram (graph) of the distribution of symbols in the source and output files (Figure 2).



Входной файл D:\документы\My files\docs политех\ю

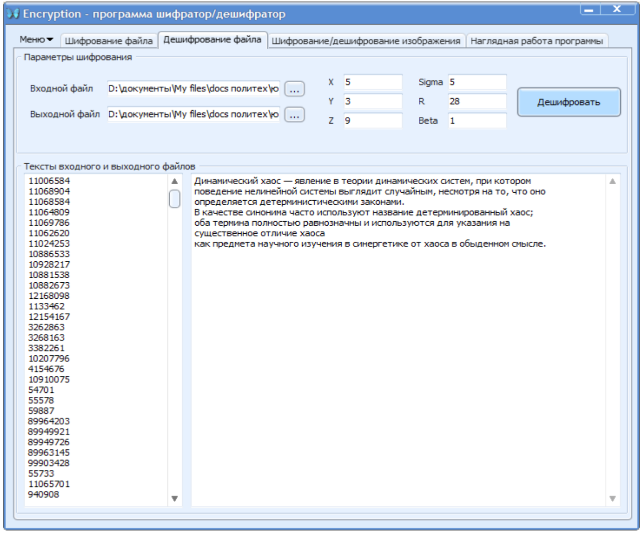
Выходной файл D:\документы\My files\docs политех\ю

X 5
Y 3
Z 9
Sigma 5
R 28
Beta 1

Fig. 2. The interface of the program.

The resulting ciphertext can be decrypted on the tab "Decrypting the file." In this case, the input file is the file with ciphertext obtained earlier, and as an output file, you need to select an empty text file. The parameters are filled in as follows: if the input file has an identical alternative stream, the program scans it and determines the contents as encryption parameters. If the thread is empty or not, the program simply continues to work, however, this means that the integrity of the ciphertext has been violated and without ciphertext parameters, it cannot be decrypted.

After receiving the parameters, the "Decrypt" button is pressed. If the ciphertext is successfully decrypted, the source text appears in the lower right field (Figure 3).


Encryption - программа шифратор/дешифратор
Меню
Шифрование файла
Дешифрование файла
Шифрование/дешифрование изображения
Наглядная работа программы
Параметры шифрования
Дешифровать
Тексты входного и выходного файлов

Входной файл D:\документы\My files\docs политех\ю

Выходной файл D:\документы\My files\docs политех\ю

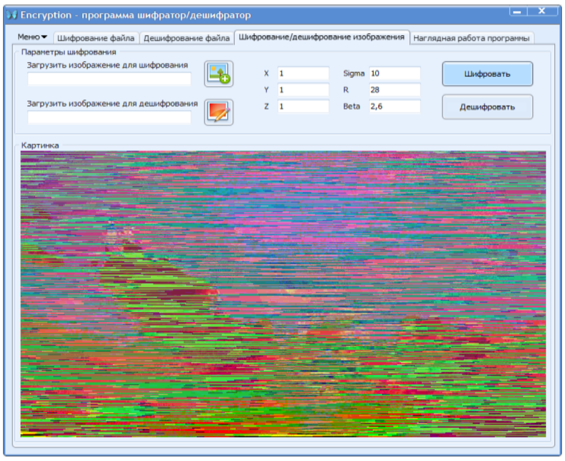
X 5
Y 3
Z 9
Sigma 5
R 28
Beta 1

```
11006584
11068904
11068584
11064809
11069786
11062620
11024253
10886533
10928217
10881538
10882673
12168098
1133462
12154167
3262863
3268163
3382261
10207796
4154676
10910075
54701
55578
59887
89964203
89949921
89949726
89963145
99903428
55733
11065701
940908
```

Динамический хаос — явление в теории динамических систем, при котором
поведение нелинейной системы выглядит случайным, несмотря на то, что оно
определяется детерминистическими законами.
В качестве синонима часто используют название детерминированный хаос;
оба термина полностью равнозначны и используются для указания на
существенное отличие хаоса
как предмета научного изучения в синергетике от хаоса в обыденном смысле.

Fig. 3. The tab «Decrypting the file».

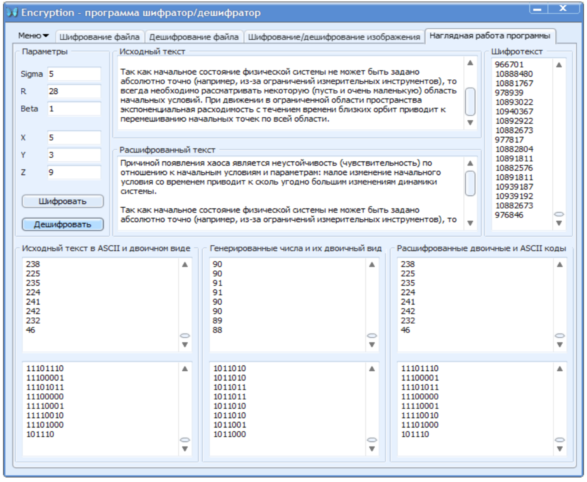
Decryption of the image occurs in the same way, except that you need to select the encrypted file (Figure 4). If there is a file in the file, the program considers the parameters and inserts them into the appropriate fields.


Encryption - программа шифратор/дешифратор
Меню
Шифрование файла
Дешифрование файла
Шифрование/дешифрование изображения
Наглядная работа программы
Параметры шифрования
Загрузить изображение для шифрования
Загрузить изображение для дешифрования
Шифровать
Дешифровать
Картинка

X 1
Y 1
Z 1
Sigma 10
R 28
Beta 2,6

Fig. 4. Image Encryption Tab.

On the «Visible work of the program» tab, you can manually type the text that you want to encrypt, you also need to fill in the encryption settings fields and click on the «Encrypt» button. After that intermediate data will appear in the corresponding fields, which were calculated during encoding, and the ciphertext itself will appear in the ciphertext field. When you click on the «Decryp» button, using the same parameters, the program decrypts the text (Figure 5).


Encryption - программа шифратор/дешифратор
Меню
Шифрование файла
Дешифрование файла
Шифрование/дешифрование изображения
Наглядная работа программы
Параметры
Шифровать
Дешифровать
Исходный текст
Расшифрованный текст
Шифротекст
Исходный текст в ASCII и двоичном виде
Генерированные числа и их двоичный вид
Расшифрованные двоичные и ASCII коды

Sigma 5
R 28
Beta 1
X 5
Y 3
Z 9

Исходный текст:

Так как начальное состояние физической системы не может быть задано
абсолютно точно (например, из-за ограничений измерительных инструментов), то
всегда необходимо рассматривать некоторую (пусть и очень маленькую) область
начальных условий. При движении в ограниченной области пространства
экспоненциальная расходимость с течением времени близких орбит приводит к
перемешиванию начальных точек по всей области.

Расшифрованный текст:

Причиной появления хаоса является неустойчивость (чувствительность) по
отношению к начальным условиям и параметрам: малое изменение начального
условия со временем приводит к сколь угодно большим изменениям динамики
системы.

Так как начальное состояние физической системы не может быть задано
абсолютно точно (например, из-за ограничений измерительных инструментов), то

Шифротекст:

```
966701
10888480
10881767
978939
10893022
10940367
10892922
10882673
977817
10882804
10891811
10882576
10891811
10939187
10939192
10882673
976846
```

Исходный текст в ASCII и двоичном виде	Генерированные числа и их двоичный вид	Расшифрованные двоичные и ASCII коды
238	90	238
225	90	225
235	91	235
224	91	224
241	90	241
242	90	242
232	89	232
46	88	46
11101110	1011010	11101110
11100001	1011010	11100001
11101011	1011011	11101011
11100000	1011011	11100000
11110001	1011010	11110001
11110010	1011010	11110010
11101000	1011001	11101000
101110	1011000	101110

Fig. 5. The program work tab.

III. RESULTS AND DISCUSSION

Thus, the use of the Lorenz attractor to generate random sequences in combination with Vernam's encryption method yields sufficiently crypto-resistant ciphertext that cannot be deciphered by standard methods. The peculiarity of the program is not only in the use of deterministic chaos but also in the fact that for decryption it is not necessary to transfer any key or a set of keys of a certain length. It is only necessary to transfer the initial parameters of the attractor.

REFERENCES

1. Ptitsyn N.S. The application of deterministic chaos in cryptography. //– M.: MGTU after name Bauman, 2002. - p. 154.

2. Dmitriyev A. S. Dynamical chaos and information //- Nizhny Novgorod, IAP RAS, 2003.- p. 231.
3. Andreyev V.V., SapozhnikovaYu.V. The study of the encryption method based on the use of the Lorenz attractor as a generator of deterministic chaos. //M . Information security: encryption methods. 2011. - pp.57-74.
4. Kuznetsov S. P. Dynamical chaos. //– M.: Fizmatlit, 2001.- p. 324.
5. Salii V. N. Cryptographic methods and means of information protection. // -Saratov, 2015.-p. 343.

AUTHORS PROFILE

Baimuhamedov Malik Fayzulovich, PhD in technical sciences, professor, vice-rector for science and international affairs, Z. Aldamzhar Kostanay Social and Technical University.

Email: bmf45@mail.ru

Scientific work: 5 monographs, 7 textbooks, as well as over 140 titles of scientific papers were published;

Academic title, specialty: professor of Higher Attestation Commission.

A current member of the Dissertation Council D.05.11.034 at the Institute of Physical and Technical Problems of the National Academy of Sciences of the Kyrgyz Republic, a member of the editorial board of the All-Russian scientific journal "Agrarian Bulletin of the Urals", an editor-in-chief of the International scientific journal "Problems of Law and Economics",

Academician of the International Academy of Informatization (MAI) and the International Economic Academy of Eurasia (IEAE).

List of significant works: “Intellectualization of computer technologies for teaching.” (Monograph RIC, Alma-Ata, 1993, 276 pp.); “Expert Systems” (textbook, Kostanay Printing House, 2007, 212 p.); “Information Systems”, (textbook. MASTER REPRINT Publishing House, 2012, p.370) "INFORMATION SYSTEMS" (textbook (in English), Bastau Publishing House, Almaty, 2013 - p. 288).

Awards, titles: Badge "Honorary Worker of Education of the Republic of Kazakhstan", Badge "Excellence in Education of the Republic of Kazakhstan", diplomas of the Ministry of Education and Science of the Republic of Kazakhstan, regional and city akimats, diploma of the International Academy of Informatization.

Atanov Sabyrzhan Kubeysinovich, PhD in technical sciences, professor, L. Gumilev Eurasian National University.

Phone number: +77172709500

Scientific work: over 80 scientific publications, including 24 of them in foreign countries and in journals with a non-zero IP factor, textbooks on microelectronics and a monograph on microcontroller systems, innovative patents and certificates of intellectual property for computer programs, more than 40 educational allowances and textbooks.

Head of a number of projects under a grant of the Ministry of Education and Science of the Republic of Kazakhstan, including "Designing robotic systems with artificial intelligence", the international scientific and technical project "Development of a neural network system for ensuring the stability of control of spacecraft."

Participant of the international seminars and conferences - Urumqi (China, 2008), Moscow (Russia, 2010), Paris (France, 2012), New York, Washington (USA, 2013), Hong Kong (Hong Kong, 2013), London (United Kingdom, 2014), etc.

In 2008, was awarded with the grant of the Ministry of Education and Science of the Republic of Kazakhstan “The Best University Teacher”.

Further training: certificates of the Republican Center for Education and Science of the Republic of Kazakhstan "Republican trainer to reduce information inequality", Almaty, 2006; National Accreditation Center of the Ministry of Education and Science of the Republic of Kazakhstan “Expertise of the quality of professional education”, Astana, 2009; “Administration of computer networks”, 2007; “Credit system of education”, 2007; "Information Technologies", Almaty, KazNU named after Al Farabi and others.

Zhunusov Kuat Muratovich, PhD in technical science, Head of the Department of Information Technology and Automation, academician of the Moscow Aviation Institute.

Email: zunusov_k@mail.ru

Awards: For achievements in the field of science, K. Zhunusov was awarded the Ministry of Education and Science of the Republic of Kazakhstan on 04/08/2010 with the breastplate "FOR SERVICE IN THE DEVELOPMENT OF SCIENCE OF THE REPUBLIC OF KAZAKHSTAN".

Work experience in the field of higher education and research - 22 years.

Scientific work: List of scientific papers:

• Economic - mathematical model of the rationale for investment projects based on information modeling. Almaty: Eurasian Community No. 2 (Kazakhstan Development Institute), ed. Bilik House, 1999 (co-authored)

• The main directions of improving the management systems of the FPA. // Economic stimulation of industrial and innovative growth of Kazakhstan: Proceedings of the II International Economic Congress of Karaganda, September 23-24, 2004 / Association of Economists of Kazakhstan, 2004

• Integrated management systems for financial and industrial groups. / Information-analytical magazine "Sayasat - Policy". Factors of Economics.-№7 (July 2005) - Almaty.

• Management of a machine-building cluster based on information technology of high-tech production. // Proceedings of the conference of the International scientific and practical conference "Science and Education" Czech Republic. December 27, 2011 - January 05, 2012

Classes are held at the proper professional level. For classes uses electronic textbooks, presentations, interactive learning systems, application packages.

Zhikeev Azamat Aitpayevich, PhD in technical sciences, dean of the faculty of information technology A.Baitursynov Kostanay State University.

Email: a_zhikeev@mail.ru

Scientific work: since 2005, about 49 works were published in domestic and foreign scientific journals, including those approved by the Ministry of Education and Science of the Republic of Kazakhstan, and international ones with a non-zero impact factor;

Since 2016 - work in a group of performers in research projects on grant financing of the Ministry of Education and Science of the Republic of Kazakhstan, Ministry of Agriculture of the Republic of Kazakhstan.

Public work: a member of the disciplinary commission of A. Baitursynov KSU, Conciliation Commission, Scientific Council, administration, developer of normative and reference documentation of A. Baitursynov KSU.

Chairman of the Kostanay City Parental Public Council of the Education Department of the Akimat of Kostanay, member of the commission on minors and the protection of their rights under the Akimat of Kostanay, member of the political party “Nur Otan”.

Awards: Diploma of the Minister of Education and Science of the Republic of Kazakhstan, 2017; letter of rector of the university, 2016; Certificate of Akim, 2019.

Bugubayeva Aliya Uzbekovna, PhD in Agricultural Sciences, Deputy Head of the Regional “Smart Center” of A.Baitursynov Kostanay State University.

Email: alia-almaz@mail.ru

Scientific work: number of publications - 43, of which: 1-monograph and 3 publications in a peer-reviewed foreign scientific publication indexed in the Web of Science or Scopus databases with non-zero impact factor;

Leading Researcher of Active Projects funded by the Ministry of Education and Science of the Republic of Kazakhstan;

Awards: Diploma for contribution to the development of agricultural science from KazAgroInnovation, 2011; Certificate for contribution to the development of Kostanay State University, 2018.

Further training: certificates "ISO / IEC 17025: 2017" General requirements for the competence of testing and calibration laboratories "; “Measurement and testing in shipbuilding and related industries”; "Office management at the enterprise"; "Systems of machine control software"; “Commercialization is a tool for integrating science and business”.

Bulaev Alexander Genrikhovich, PhD in biological sciences (Microbiology), Head of the Laboratory of Chemolithotrophic Microorganisms, Federal State Institution Federal Research Center "Fundamentals of Biotechnology" of the Russian Academy of Sciences (FIC Biotechnology RAS).

Email: bulaev.inmi@yandex.ru

Scientific work: over 20 scientific publications were published in domestic and international respected scientific magazines, for the part of the inventions patents were obtained etc.

The work of the laboratory is supported by programs of the Presidium of the Russian Academy of Sciences, grants from the Russian Federal Property Fund, the President of the Russian Federation, and subsidies from the Ministry of Education and Science (as part of event 1.2). In the laboratory, more than 10 economic agreements were concluded with enterprises of the Russian Federation and the CIS to optimize and develop biohydrometallurgical technologies.