Biometrics as a method of information security in the banking sector digitalization

Bakunova T.V.
Ural State University of Economics
Yekaterinburg, Russia
tatyana.bakunova@mail.ru

Trofimova E.A.
Ural Federal University
Yekaterinburg, Russia
Elena.Trofimova@urfu.ru

Lapteva E.V.
Ural Federal University
Yekaterinburg, Russia
laptevazhenya.00@mail.ru

***Abstract* — Today, biometrics as an integral component of the information technology market and an indicator of the digital economy as a whole is becoming a convenient tool for solving a wide range of tasks, but at the same time it has some drawbacks, the main of which is high exposure to fraudulent attacks. The main costs may be incurred by users of online banking, where there is the greatest vulnerability of personal data. In connection with these factors, the authors see the need for a detailed review of this tool. This paper analyzes the international and Russian experience of the active implementation of biometric technologies in the banking sector, sets out the possibilities of introducing biometric identification systems, considers aspects and risks of their use, and presents a forecast for this market development.**

Keywords* — biometric technologies, biometric identification, fraudulent attacks, information protection, online banking.

I. Introduction

The widespread development of digital technology has made the personal data of banking sector users more vulnerable to fraudulent attacks. The threat of loss of bank customers' confidential information necessitates the study and active use of new tools aimed at protecting it in the most vulnerable sector – online banking.

As a result of the unauthorized transactions analysis conducted by the The Financial Sector Computer Emergency Response Team (FinCERT) of the Central Bank of the Russian Federation, the data provided by financial institutions allow to record an increase in the number and volume of thefts for the period of 2015-2018. The general trend is presented in Figures 1, 2.

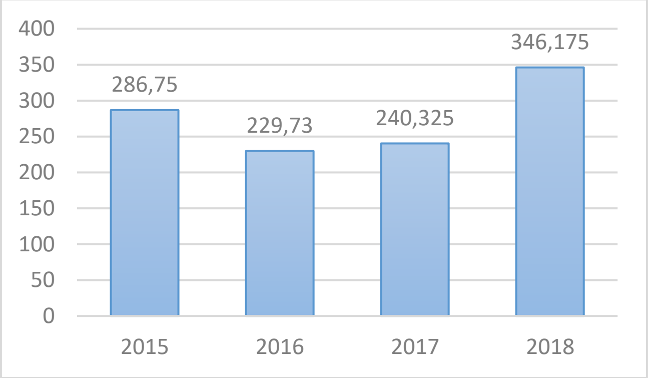

Fig. 1. Number of unauthorized transactions using payment cards of individuals on average per year, times

Compared with 2017, in which the number of unauthorized transactions amounted to 317178, in the reporting period of 2018 their number increased by 31.4%, reaching 416 933 times. Also, the average amount of one operation of this kind increased by 9.6% from 3.03 thousand rubles in 2017 to 3.32 thousand rubles in 2018 [1].

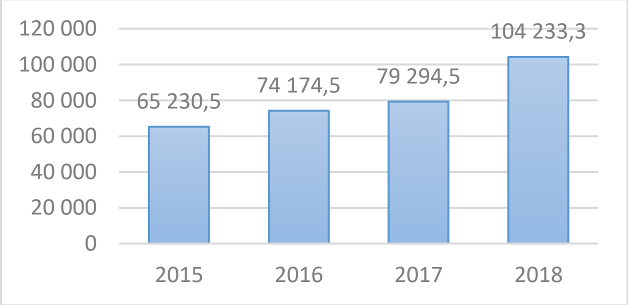

Fig. 2. Volume of unauthorized transactions using payment cards of individuals on average per year, million rubles.

The volume of all unauthorized transactions using payment cards, which amounted to 961.3 million rubles in 2017, increased by 44% over the next year to the level of 1384.7 million rubles.

The upward trend can be observed in the diagrams presented, which indicates the growing relevance of implementing measures to counter fraudulent attacks in relation to bank accounts access.

There is also an increase in the number of illegal actions with the legal entities accounts. Based on the results of 2018, the Central Bank provided data on 6151 unauthorized transactions with corporate accounts, the volume of which amounted to a total of 1.499 billion rubles, while in 2017 these indicators were: 841 transactions and 1.57 billion rubles, respectively. Thus, with an increase in the number of thefts and their attempts, the dynamics of a decrease in their volumes is observed.

The largest part of all unauthorized access to individuals accounts is made through the fraudsters access to electronic payment instruments (hereinafter - EPI). As for the accounts of legal entities, a number of reasons for fraudulent attacks include violation of the procedure for using EPIs and their use without a customer's consent. According to statistics, about 50% of thefts in 2018 were recorded as a result of fraudsters accessing a remote banking service system using malicious software (hereinafter – malware), the purpose of which is to hack software (hereinafter – software) on stationary computers.

Among the main factors countering unauthorized transactions should be the introduction of antivirus software in banking applications on customer devices, and more reliable ways to authenticate users. One of such measures is the system of a unified identification and authentication of customers (a single biometric system).

II. Research Methodology

In researching the trends of unauthorized attacks on the banking users information, as well as the nature and content of biometric technologies as a way to combat fraud, we used the information reflected in the Central Bank report on the development of the banking sector and banking supervision [2], a research of the main directions of financial technologies development [3], a review of the international market for biometric technologies in the financial sector [4], as well as research materials of K.K. Simonchik, D.O. Belevitin, Yu.N. Matveev, D.V. Darmovsky [5], N.M. Lynn, P. Kim, S. Yeom [6]. The relevance of the study and implementation of biometric systems was highlighted in an analytical research of J'son & Partners international consulting company [8], a joint research by MasterCard and Oxford University [9], the safety of storing biometric data was the focus of attention of such authors as S.I. Berlin, G.A. Bathory, D.V. Kopylova [7].

To process the obtained data, mathematical and statistical methods, as well as methods of analysis, synthesis and collection of facts were used.

The target vector of paper is the research of the biometric technology market as part of the actualization of the problem of fraudulent attacks in the banking sector.

To achieve the goal, the following tasks were set:

1. To assess the number and volume of unauthorized transactions in the banking sector;
2. To determine the volume and structure of the biometric market, to identify key consumer segments;
3. To study the Russian and foreign experience in biometric technologies participation in the banking services market;
4. To analyze competition in the Russian market of biometric systems;
5. To demonstrate the risks of introducing biometric identification technology.

III. Results

Technologies based on the person identification by unique biological characteristics are considered to be biometric.

According to the research [9], there is a need for biometric technologies from both banks and their customers: 93% of users prefer biometrics to traditional access to online banking (passwords, code words, etc.), 92% of banks intend to implement biometric identification in their security systems, 36% of respondents involved in the mobile biometrics implementation said they had positive experience in using data systems, which shows the need for refinement and development of this technology.

In the report of the J'son & Partners international consulting company [8], the volume of the global biometric technology market for 2016 was estimated at USD 14.45 billion. In the next 6 years, the compound annual growth rate (CAGR) of the biometric systems market will be 18.6%, and the market volume will grow to USD 40.2 billion by 2022 (Fig. 3)

Russia has a small share in the global market, but shows more active growth: CAGR for 2018-2022 will amount to 29.5% and will increase by 1.8 times.

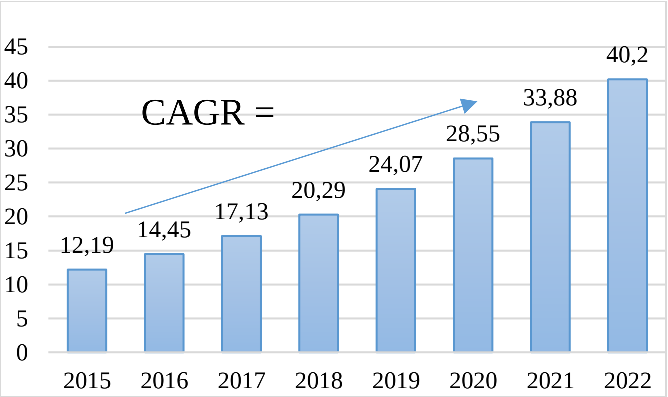

Fig. 3. Volume of the global market for biometric systems 2015-2022, USD billion

The following biometric data underlying the application of identification technology in the global market for biometric systems can be distinguished (the market size occupied is presented in brackets):

1. fingerprints (more than 50%);
2. face image (21.6%);
3. image of the iris (10.2%);
4. voice (4%);
5. vein pattern (3%).

6. palm geometry, DNA and other (about 7%).

At the same time, based on forecasts [8], the market for biometric authentication technologies using fingerprint recognition will grow more slowly than the average growth rate of the entire biometric technology market until 2022, as a result of which this sector will reduce its occupied share. Facial identification technologies will also show growth rates below the average market, however, the share of this technology in the global market for biometric systems will grow from 21% to almost 23%. The technology of identification by voice and image of the iris, as well as authentication by vein pattern of the palm will be the most promising in the next few years.

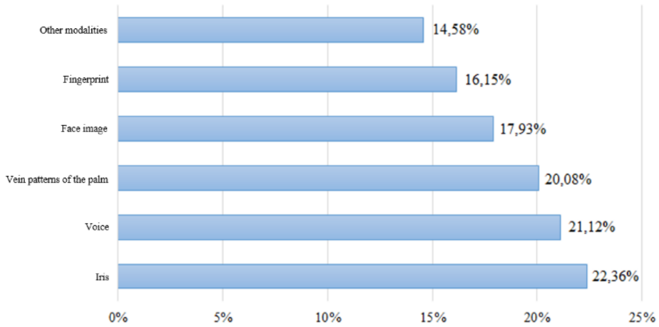

Fig. 4. Forecast of the average annual growth rate of the biometric systems market by technology up to 2022, %

Currently, the ways of applying biometrics are greatly transforming in the world. Within these changes, the most indicative is the transition of these technologies from the traditional sphere of state security to the implementation in commercial and user structures.

Moreover, in recent years, the financial sector, which is the third largest market for biometric systems with a share of 15%, shows the development of multi-factor authentication with the use of biometric technologies has been proceeding most rapidly. This identification system is common in critical areas, the most important of which are the banking sector, government services, defense and health care.

Among all multi-factor authentication models, two-factor (bimodal) authentication is traditional today, which is a combination of, for example, a password with biometric access control solutions. This technology is used in online banking, ATMs, access to safe deposit boxes.

The main consumer of bimodal biometrics, which is a generalization of the results obtained during voice and facial verification, and aimed at enhancing the protection of networks from threats of security breaches and ensuring safe access to systems for employees, is the banking services sector that accounts for 43% of the global market for such solutions. Many international banks and financial institutions integrate two-factor biometric authentication systems to ensure the security of user access to secure systems, in particular to Internet banking.

The authors of the research work [5] conducted test evaluating the reliability of the bimodal solution both separately for each authentication method and for both modules as a whole. To assess the voice modality, YOHO, RSR2015 speech bases were used, as well as the base of one of the US banks, the total volume of which reached 80 thousand records. The research of access reliability by facial modality was tested using FERET and MOBIO databases with a volume exceeding 2 thousand images. To test a joint solution that included both modalities, a database of 40 people was used for 50 access attempts under their own and other people's accounts.

Based on the collected data, the authors examined 2 access cases involving:

1) the attacker has no image of the customer and their voice recording;
2) the attacker has a customer passphrase and their image.

For each of the cases considered, errors of the 1st / 2nd kind were calculated:

1) error of fraudster false admission to the system;
2) error of false rejection of the customer by the system.

The probability of false access when applying each individual verification (by voice or by face) was about 40%. This value was reduced to 1% by introducing a bimodal solution (by voice and face at the same time). As for the false refusal, the probability of it in the case of verification by voice was 50%, by face - about 7%. Bimodal technology has reduced this probability to the level of 2-3%. Thus, two-factor identification does not allow fraudsters to access the bank’s information system on behalf of employees or agents, revealing information about their username and password.

The principles of combining modalities presented in the research, due to their high efficiency, are becoming increasingly relevant for implementation in information security systems. Banks are actively using biometric technologies to reduce attackers and increase customer convenience: many financial services are provided through online banking and eliminate the need for customers to directly contact banking centers. This fact today is increasingly becoming an important incentive for the active use of biometric technologies in Russia. The introduction of a remote identification mechanism in the financial market since 2018 makes banking operations more accessible for people with limited mobility and will help reduce the costs of banking sector, making its players more competitive in the future.

Let us turn to the international experience in introducing biometric technologies in the financial market in general and the banking sector in particular.

An important feature is the introduction of biometric technologies in payment systems. For example, PayPal, together with Synaptics, a biometric technologies developer, began to work with Lenovo and Intel electronic equipment manufacturers to provide personal computer users with the ability to authenticate when making payments using fingerprints.

In 2014, MasterCard together with Zwipe, a biometric technology used to create authentication solutions for banking services, access control and ID, developed a plastic card that allows contactless banking transactions using an integrated sensor for fingerprint recognition of cardholders.

In 2016 MasterCard has introduced MasterCard’s Identify Check Mobile, a payment application that uses biometric data to identify a customer’s identity and simplify online shopping. The technology involves the fingerprint scanner on a user's mobile device or face recognition. The company is also exploring the prospects of using the so-called "internal" biometric identification technologies (heartbeat, venous pattern), considering them to be quite progressive and more reliable [12].

In 2016 the French company Morpho entered into an agreement with Visa on the new payment systems creation using biometrics [13].

A significant event in the biometric technology market was the introduction of Apple Pay, Samsung Pay and Android Pay services, which account for more than 85% of transactions. A mobile phone with built-in biometric technologies is used to make a payment. According to Grand View Research forecasts, the global “mobile wallets” market will amount to USD 7.5 trillion by 2024 with an average annual growth rate of almost 33%.

Most global banks use pilot projects to test biometric technologies, some of which are already being actively implemented in business practice. In particular, the most important banks in Singapore (DBS and OCBC) use voice recognition systems in their call centers. Along with them, CityGroup has implemented voice biometrics in its systems in Central Asia: The bank plans to connect about 1 million regular and new customers to the service. Barclays in the UK uses finger vein reader technology (VeinID) and voice authentication to provide access to mobile applications and authorize payments.

A key trend in the banking sector is the growing interest of market players in other identification systems in online banking, in addition to fingerprint authentication, which is widespread in major banks (Bank of America, JPMorgan Chase, Wells Fargo). For example, Wells Fargo uses the solution of STC Russian biometric company as a form of a multifunctional biometric authentication platform for remote servicing of VoiceKey.OnePass, and Citigroup launches a project to introduce a system for identifying users by voice in the Asian region [14].

BBVA in Bolivia uses face recognition technology (Facephi) 6 to identify senior citizens, and a USAA group of financial services companies in banking, investment and insurance in the United States uses face, fingerprints and voice recognition technology.

The active introduction of biometric technologies in the financial sector extends not only to Europe and the USA, but also includes players such as China and Japan. For example, Alibaba announced the possibility of making biometric mobile payments, Alipay has launched of face identification, Merchants Bank has integrated face identification technologies into ATMs (plans are for 12 thousand ATMs), Union Pay has developed a biometric version (similar to Apple Pay).

Also in 2017, an ATM network was launched in India, created on the basis of the Aadhaar national biometric system (DCB Bank), where the customer is assigned a personal Aadhaar number instead of the traditional password.

In the same year, the Saudi bank Al Rajhi began a pilot project of a biometric ATM with the possibility of creating debit payment cards for customers. The user needs to be identified by fingerprint, choose the method of displaying the name and surname on a bank card, and immediately receive the card itself [15].

In some countries, the implementation of biometric systems is currently limited. In particular, in South Africa, such technologies are developed by each bank only in its own branches or only for its own services. For example, in May 2015, Standard Bank has offered its customers with smartphones the ability to use fingerprint scanners to enter mobile banking applications. An interoperable standard for receiving personal data on a biometric reader will allow this information to be recognized in other banking organizations and will enable various banks to exchange payment orders certified by biometric identifiers.

Tyme, a company specializing in high-tech banking services in South Africa, has been using biometric banking kiosks since mid-2016. Currently, there are 685 biometric kiosks in South Africa equipped with a fingerprint scanner, an identity document scanner, and a high-resolution camera. There are biometric kiosks running the Android operating system, and their sizes do not exceed the dimensions of kiosks at airports in which air passengers can independently pass pre-flight registration. Based on Tyme reports, in 2017 biometric kiosks provided an influx of 100 thousand new customers; the cost of attracting each of them did not exceed USD 4.

Key players in the biometric systems market see great potential in Brazil. In 2017, a Brazilian company focused on the banking sector, together with IBM launched the Smart Authentications product that uses face and voice identification systems [16].

In Mexico, the National Banking and Security Commission is working on a new bill requiring mandatory use of biometric equipment in banks to enhance the security of customers' personal data. After the adoption of this law, the commission expects to introduce fingerprint scanners to all banking institutions in Mexico over the next year. Future users of banking services will need to verify all fingerprints with samples from the National Electoral Institute information database.

Biometrics is also actively introduced into the banking sector of Japan. For example, Ogaki Kyoritsu Bank is the first bank in Japan which widely uses the biometric authentication system in a large number of services using palm vein scanners in 160 of its branches [17]. The introduction of this technology was a well-grounded response to the devastating earthquake and tsunami in March 2011 in eastern Japan. After the disaster, almost all residents lost their bank cards, documents and seals, which forced them to undergo tedious identification procedures to withdraw money from ATMs and bank branches.

Russia does not lag behind global trends in the biometrics implementation in the banking sector. TCS conducted a research in which it estimated that almost 70% of all biometric technologies in banks are used for customer services and 30% for corporate purposes [4].

In 2017, VTB24 Bank launched a test version of personal identification using photos of its customers and their voices. To do this, more than 1000 customers who use the bank's mobile application left their data with which selfies and voice recordings are compared when they are trying to identify themselves. This technology is used in the bank to confirm large amount mobile transfers. Upon subsequent requests from customers, the complex will initiate verification of voice recordings with the saved sample in the database and, based on the results of the verification, identify the customer or additionally request input data from them.

At the end of 2017, Otkritie Bank launched the Otkritie.Transfers mobile application and became the first bank in the world with such a service. The service is designed to use a neural network facial recognition systems, which is the most accurate when identifying a person by their biometric data.

In the same year, Pochta Bank introduced biometric technologies into the employee identification process. To enter the bank's operational CRM system, they need to enter not only a username and password, but also pass biometric authentication.

However, it should be noted that biometric data is sensitive information, the disclosure of which can lead to serious consequences. Based on this, when using them, uniform requirements for their transfer, storage, processing and protection should be applied.

In accordance with Federal Law No. 482-FZ [18], a federal executive body regulating the sphere of identification based on biometric personal data will appear in Russia. The tasks of the new body:

- to determine the procedure for processing biometric personal data for identification purposes, as well as the requirements for information technologies and technical means intended for processing biometric personal data for identification purposes;
- to determine the forms to demonstrate compliance with information technologies and technical means intended for processing biometric personal data in order to perform identification;
- to develop and approve methods for verifying the conformity of the provided biometric personal data of an individual with their biometric personal data stored in the Unified Biometric System, as well as to determine the degree of mutual correspondence of these biometric personal data sufficient for identification.

In general, it is worth noting that the growth rate in the segment of the Russian biometric market is ahead of world figures since 2014 by almost 7%. The gap between the studied data, according to J'son & Partners, will increase to 11.3% by 2022 (Fig. 5).

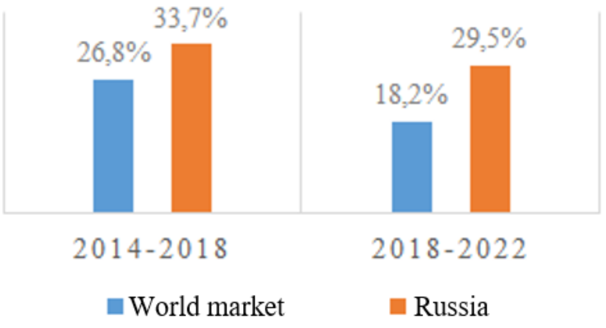

Fig. 5 Growth rates for biometric systems market

The following companies are among the key players in the biometric technology market: 3DiVi, BioLink Solutions, Fujitsu, HBS, IDEMIA, ITV / Axxonsoft, N-Tech lab, Tevian, Visionlabs, AAM Systems, Armo systems, Vokord, Vzor Technology, Technoserv Group, Papillon, Prosoft-Biometrics, Satro Paladin, Sonda Technology, STC Group.

The presence of a large number of key players indicates the attractiveness of this industry not only for direct users, but also for manufacturers of these systems. Together with the trend of increasing growth rates, this fact actualizes the study of this market.

IV. Conclusions

The current refraction of the downtrend of 2017 in terms of the number of information security violation incidents indicates the real need for increasing the transparency of the data provided by banks and confirms the correctness of the development and implementation of measures to minimize the risk of unauthorized transactions taken by market participants and the Bank of Russia, as well as the need for their further development. Such measures include:

- improvement of the legislation of the Russian Federation in ensuring information security of financial organizations;
- improvement of Bank of Russia regulations in information security of financial organizations;
- improving the financial literacy of the population in terms of ensuring the security of the applied information technologies and payment technologies;
- organization of information exchange on the basis of FinCERT for implementation of operational and continuous mutual information about threats to information security breaches;
- organization of information exchange on the basis of FinCERT for implementation of operational and continuous mutual reporting of operations without customers' consent
- introduction of promising financial technologies: Big Data and data analysis, artificial intelligence, robotics, biometrics, cloud technologies.

Application of these measures will significantly narrow the scope of activity accessible to attackers, which will positively affect the fight against fraud.

References

[1] Obzor nesanktsionirovannykh perevodov denezhnykh sredstv za 2018 god, provedennyy Tsentrom monitoringa i reagirovaniya na komp'yuternye ataki v kreditno-finansovoy sfere (FinTsERT Banka Rossii) Departamenta informatsionnoy bezopasnosti Banka Rossii // [Elektronnyy resurs]: URL: //ne-nature.ru/sibir/28-peshera-barsukovskaya Data obrashcheniya: 05.09.2019).

[2] Otchet Tsentral'nogo Banka o razvitii bankovskogo sektora i bankovskogo nadzora // [Elektronnyy resurs]: URL: //ne-nature.ru/sibir/28-peshera-barsukovskaya Data obrashcheniya: 05.09.2019).

[3] Osnovnye napravleniya razvitiya finansovykh tekhnologiy na period 2018-2020 godov // [Elektronnyy resurs]: URL: //ne-nature.ru/sibir/28-peshera-barsukovskaya Data obrashcheniya: 05.09.2019).

[4] Obzor mezhdunarodnogo rynka biometricheskikh tekhnologiy i ikh primenenie v finansovom sektore // [Elektronnyy resurs]: URL: https://www.cbr.ru/content/document/file/36012/rev_bio.pdf (data obrashcheniya: 05.09.2019).

[5] Simonchik K.K., Belevitin D.O., Matveev Yu.N., Darmovskiy D.V. Dostup k internet-bankingu na osnove bimodal'noy biometrii // Zhurnal Mir izmereniy. 2014. № 3.

[6] Lynn H.M., Kim P., Yeom S. Ecg-based biometric human identification based on backpropagation neural network // Proceedings of the 2018 research in adaptive and convergent systems, Racs 2018

[7] Berlin S.I., Batori G.A., Kopylova D.V. Biometriya v bankovskoy sfere. Issledovanie voprosa bezopasnosti khraneniya biometricheskikh dannykh // Vestnik Akademii znaniy. 2019. №32 (3).

[8] http://json.tv/ict_telecom_analytics_view/issledovanie-rossiyskogo-rynka-biometricheskih-tehnologiy-2018-2022-gg-20181130015609

[9] https://newsroom.mastercard.com/news-briefs/overcoming-mobile-biometric-challenges-mastercard-and-university-of-oxford-collaborate-on-new-research-initiative/

[10] Michael E. Schuckers. Test Sample and Size / Encyclopedia of Biometrics, Li, SZ and Elliot SJ (eds).

[11] Silant'yev D.A. Otsenka neobkhodimogo razmera svertki biometricheskogo obraztsa dlya obespecheniya zadannykh parametrov nadezhnosti biometricheskoy sistemy identifikatsii

[12] https://newsroom.mastercard.com/mastercardidentity-check-mobile/

[13] https://www.morpho.com/en/media/morpho-and-visajoin-forces-further-promote-contactless-paymentasia-pacific-eastern-europe-middle-east-andafrica-20150309

[14] https://www.speechpro.ru/product/sistemy-upravleniyakachestvom-i-avtomatizatsii/voicekey/specification

[15] https://findbiometrics.com/bank-biometric-selfservice-401171/

[16] https://www.cpqd.com.br/en/

[17] https://www.blacklistednews.com/Ogaki_Kyoritsu_Bank_To_Introduce_Japan’s_First_Biometric_ATM/18915/0/38/38/Y/M.html

[18] Federal'nyy zakon ot 31.12.2017 g. № 482-FZ // [Elektronnyy resurs]: URL: //ne-nature.ru/sibir/28-peshera-barsukovskaya Data obrashcheniya: 19.09.2019).