ORIGINAL PAPER

DOI: 10.26794/2587-5671-2021-25-6-212-226
UDC 336:004.056(045)
JEL G21, G32, L86

Phishing Schemes in the Banking Sector: Recommendations to Internet Users on Protection and Development of Regulatory Tasks

P.V. Revenkov[a] ✉, **K.R. Oshmankevich**[b], **A.A. Berdyugin**[c]
[a, c] Financial University, Moscow, Russia; [b] Moscow State Linguistic University, Moscow, Russia
[a] https://orcid.org/0000-0002-0354-0665; [b] https://orcid.org/0000-0003-3539-003X;
[c] https://orcid.org/0000-0003-2301-1776
✉ Corresponding author

ABSTRACT

The **aim and objectives** of the article are to analyze fraudulent phishing schemes and develop recommendations for Internet use and relevant regulatory tasks. The **relevance** of the article is due to the peculiarities of working in cyberspace with the emergence of new sources of banking risks, both for customers and organizations. The **scientific novelty** of the manuscript consists of a detailed analysis of phishing schemes, the development of recommendations and directions in relation to the Russian Federation. The **object** of the study is cyber fraud in the credit and financial sphere; the **subject** is social engineering and phishing schemes. The **methodology** of the paper includes a systematic analysis of the literature and sources on the research topic, general scientific methods (analysis, synthesis, deduction, analogy, classification), correlation analysis of data, graphical visualization of information. The authors **consider** the main methods of phishing and the most common techniques used by cybercriminals. Based on the critical analysis of the literature the authors determined a promising direction for the scientific and technical potential of Russia. A correlation analysis of the relationship between the number of cybercrimes and commercial banks is performed. The study offers **recommendations** to Internet users (how to recognize the signs of fraud), and to regulatory bodies on improving the system of supervision over the dissemination of information in cyberspace. The authors **concluded** that it is necessary to increase the level of cyber literacy and general literacy of the population, on the one hand, and to modernize the methods of supervision and control of the information posted on the Internet, on the other hand, to effectively counter financial and cybercrime. The research **results** can be used in the further development of remote banking services for the population to increase competitiveness in the banking services market. **Prospects** for further research on this topic lie in expanding its structure, developing the competencies of specialists in the field of remote banking technologies, as well as developing the scientific and technical potential of Russia.

Keywords: cyberspace; phishing; cybersecurity; cyber literacy; remote banking services; risks; attacker; user; fictitious organization

For citation: **Revenkov P.V., Oshmankevich K.R., Berdyugin A.A. Phishing schemes in the banking sector: Recommendations to Internet users on protection and development of regulatory tasks. *Finance: Theory and Practice.* 2021;25(6):212-226. DOI: 10.26794/2587-5671-2021-25-6-212-226**

INTRODUCTION

In today's world, the amount of time spent on the Internet is increasing. The Internet not only provides access to the required information, but also allows making online purchases, bank transfers and payments. The global amount of information generated by people, governments and businesses will more than fivefold to 175 zettabytes by 2025 (1 zettabyte requires 34.4 billion 32GB drives), up from 33 zettabytes today.[1]

The active development of information and communication technologies and their use in most spheres of human activity makes new cybersecurity issues and information protection in cyberspace relevant. There is a need to develop new algorithms and methods for assessing risks (examples of such developments can be found in [1]). Algorithms and methods should be associated with certain features of the functioning of corporate information systems of commercial banks, including various options for electronic banking (Internet banking, mobile banking, etc.).

The ISO/IEC 27032:2012 standard describes cyberspace as "a complex environment resulting from the interaction of users connected to the global Internet, hardware and software, and the services provided on this network. This environment exists in a virtual (constructed), and not in a material (physical) form". At the same time, cybersecurity is "maintaining the confidentiality, integrity and availability of information in cyberspace".[2]

Robert Metcalfe's Law can be applied to cyberspace, which determines the growth in value (utility) of a network with an increase in the number of devices connected to each other via the Internet:

$$V_n \approx n^2/2.$$

This is explained by the fact that the graph K_n contains $n\cdot(n-1)/2$ edges (links) at the n vertices (technologies). This value approaches $n^2/2$. asymptotically. It is worth adding that in economics, Metcalfe's law is a characteristic of a positive network effect. Today, more than half of the world's population (more than 4.6 billion people) uses the Internet (*Fig. 1*).

The use of "master keys" by a hacker not to the computer, but to the user's logic is informational and psychological impact (IPI, social engineering). In the book [2], the arsenal of basic tools and psychological techniques of a social hacker (transactional analysis, neuro-linguistic programming) is characterized by numerous examples, methods of protection against social hacking are considered. Despite some obsolescence of the book, the advice given are still relevant to this day. The peculiarities of the provision of financial services in cyberspace were analyzed in a collective work [3]. The book highlights the methodology of ensuring cybersecurity in electronic banking technologies and reducing the risks arising from the use of remote banking services.

In the monograph [4], the author (an employee of the Institute of the USA and Canada of the Russian Academy of Sciences) creates an extensive and fact-filled picture of the risks of information security breaches in the social, military, political and economic life of the USA, the growth of which entails a sharp increase in the impact of cyberspace objects on real life. The book is interdisciplinary in nature: it touches on issues related to various sciences (sociology, political science, economics), and convinces readers to apply a multidimensional approach to analyzing the problems of the information society.

In the human brain there are nerve cells that are activated not only when performing a certain action, but also when a person observes the performance of this action by others — these are mirror neurons [5]. Knowledge of mirror neurons helped Chinese researchers in the early 21st century, when they sent a delegation to the US corporations (Apple, Microsoft, Google) to ask inventors

[1] Expert: The volume of data in the world by 2025 will grow more than fivefold. URL: https://tass.ru/ekonomika/6209822 (accessed on 10.01.2021).

[2] ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. International Organization for Standardization. URL: http://www.iso.org/standard/44375.html (accessed on 05.01.2021).

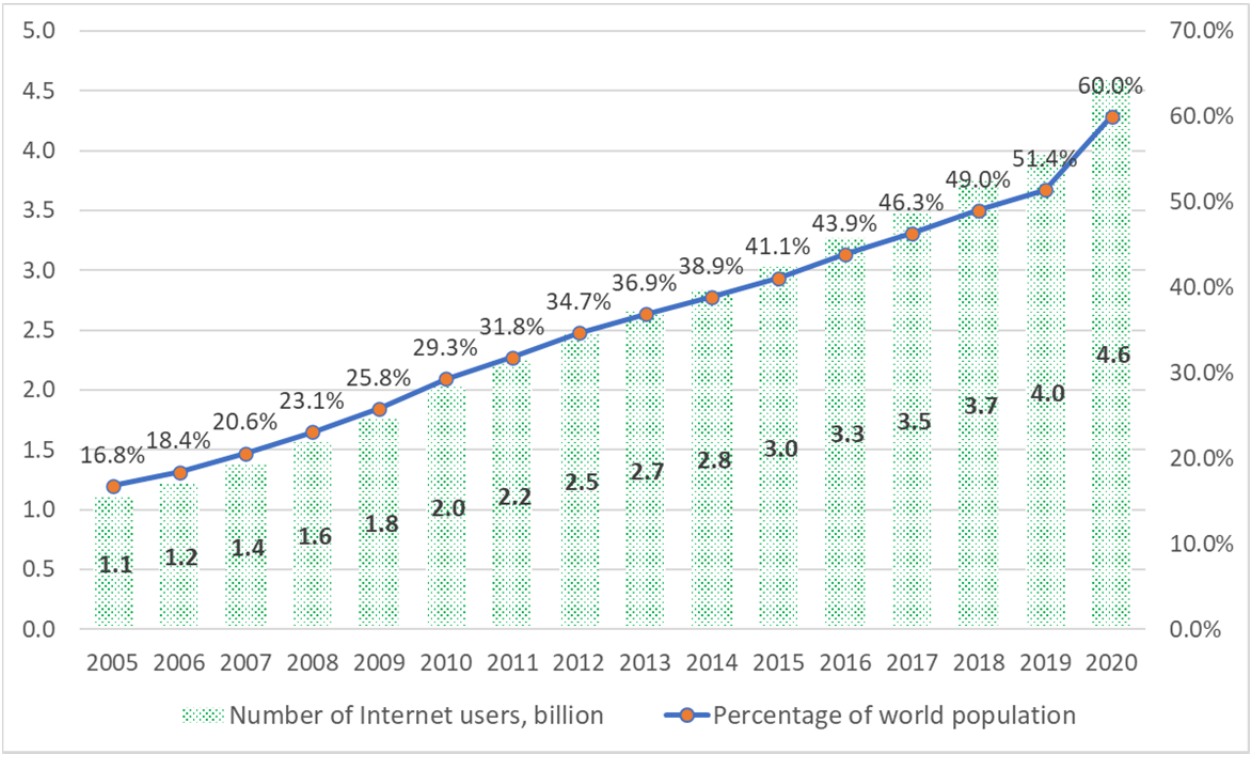

Fig. 1. **Dynamics of the number of Internet users and their share of the world population**

Source: Internet access (global market). URL: https://www.tadviser.ru/a/53635 (accessed on 10.01.2021).

about their lifestyle. After that, works of the favorite genre of literature of inventors (science fiction) were included in the educational program of China on literature, and today the developments of Alibaba, Xiaomi, Huawei are among the world leaders [6–7]. Human exposure of the works of Georgy Sytin and Dale Carnegie (bibliotherapy) is also associated with the effect of mirror neurons, which was first noted in this article.

The authors of the article propose to add the utopian HSF novel[3] by the Soviet scientist I.A. Efremov "Andromeda Nebula" to the list of "100 books for schoolchildren" from the Ministry of Education and Science of Russia. As in the case of China, attention to the HSF literature (in parallel with the development of fundamental and applied sciences) will lead to competitive import substitution in the field of digital technologies, and Russia will become famous not only for military equipment (which was mainly developed in the USSR [8]), but also peaceful electronics (computers, smartphones, household appliances). We emphasize that without observance of ***formal logic*** and ***financial literacy***, both science fiction and phishing remain just a set of sophisms.

Motivational and informative but by no means a fantastic book telling about the history of Russian startups in the Republic of Sakha (Yakutia) is [9]. The author (founder and CEO) characterizes the emergence and development of the Sinet Team IT company, the Ykt.Ru information portal and the international Internet aggregator of taxi services inDriver through the prism of historical events in Russia and his own life experience. Cybersecurity issues (chargeback — demanding a refund of a payment not authorized by the current cardholder) for the inDriver Yakut taxi arose only in New York.

Popular science book [10] characterizes risk factors in various areas: from financial systems and nuclear power plants to aircraft

[3] Hard science fiction (HSF) is a sub-genre of science fiction that focuses on scientific and technological progress.

and digital platforms. The authors use the concepts of the complexity of the system and the rigidity of the connectivity of its elements to determine the causes of failures and disruptions in the operation of systems. Developing the theory of "normal accidents" by Charles Perrow, the authors analyze the disasters that have occurred, offering specific tools and practical recommendations that can prevent unwanted consequences.

Thus, the analysis of information and cybersecurity is now considered quite widely, as cyberspace has become the fifth theater of warfare after land, sea, air and space.

CYBERCRIME IN BANKING: PHISHING

Along with the emergence of the conveniences provided by cyberspace, new methods of fraud have emerged. The most active fraudulent activity on the Internet is carried out in the credit and financial sector and in the retail sector. First of all, this is due to the fact that in these areas attackers can get the greatest material benefit.

Phishing is one of the most common methods of committing fraud in cyberspace, which is used to steal passwords and confidential information by misleading the client. Usually, a fraudster copies the source code of the official page (this function is available in any browser) and saves it in a text editor. Further, in the source code, the original URL for logging into the system is replaced with the address of the program (script), which specifies the conditions for substituting addresses, the algorithm of actions after entering the registration data, and the way the fraudster receives this data. The main work of creating a phishing page is now complete. With a domain and hosting, a hacker places his page on the Internet and redirects users to it [11].

In Q1 2020, phishing emails were linked to the COVID-19. At the same time, almost half of them (44%) were sent to individuals and every fifth — to government organizations.[4]

Let us determine the closeness of the relationship between the statistics of the Ministry of Internal Affairs of Russia on crimes in the field of computer information, the preliminary investigation of which is mandatory, and the data of the Central Bank of the Russian Federation on the number of credit institutions in Russia (*Table 1*).

Let us determine the standard deviation $\sigma_x \approx \sqrt{\frac{\sum_{i=1}^{n} x_i^2}{n} - \bar{x}^2}$ and $\sigma_y \approx \sqrt{\frac{\sum_{i=1}^{n} y_i^2}{n} - \bar{y}^2}$:

$$\sigma_x = \sqrt{\frac{17812989}{18} - 950,2^2} \approx 294,5$$

and $\sigma_y = \sqrt{\frac{712122038}{18} - 5354,2^2} \approx 3300,7.$

And find the covariance $C_{xy} \approx \frac{\sum_{i=1}^{n} x_i y_i}{n} - \bar{x} \cdot \bar{y}$:

$$C_{xy} = 5\,774\,002 - 950,2 \cdot 5354,2 \approx 686\,441,16.$$

The correlation coefficient $r_{xy} = \frac{C_{xy}}{\sigma_x \sigma_y}$ is

$$r_{xy} = \frac{686\,441,16}{294,5 \cdot 3300,7} \approx 0,71.$$

The correlation value $r_{xy} \approx 0,71$ confirms the progress and optimization results.[5] The elimination of financial "vacuum cleaners" that attract depositors with risky transactions to transfer their money abroad leads to the optimization of financial activities and an increase in the reliability of banking information protection means due to the development of telecommunication technologies and a gradual transition from traditional banking to online platforms.

These phenomena are constantly changing, which complicates the process of detecting and solving crimes committed in cyberspace. As information technology develops, special tools and programs appear to detect and prevent attacks on users on the Internet.

[4] Positive Technologies: About 13% of all phishing attacks are related to the COVID-19. URL: https://www.securitylab.ru/news/509238.php (accessed on 08.01.2021).

[5] Calculations can be carried out automatically in programs for processing statistical data [12], but for clarity, a manual calculation is given.

Table

Data of the Bank of Russia and the Ministry of Internal Affairs of Russia

Year	Banks (X)	Crimes (Y)	X^2	Y^2	$X \cdot Y$
2003	1,329	7,540	1,766,241	56,851,600	10,020,660
2004	1,329	8,739	1,766,241	76,370,121	11,614,131
2005	1,299	10,214	1,687,401	104,325,796	13,267,986
2006	1,253	8,889	1,570,009	79,014,321	11,137,917
2007	1,189	7,236	1,413,721	52,359,696	8,603,604
2008	1,136	9,010	1,290,496	81,180,100	10,235,360
2009	1,108	11,636	1,227,664	135,396,496	12,892,688
2010	1,058	7,398	1,119,364	54,730,404	7,827,084
2011	1,012	2,698	1,024,144	7,279,204	2,730,376
2012	978	2,820	956,484	7,952,400	2,757,960
2013	956	2,563	913,936	6,568,969	2,450,228
2014	923	1,739	851,929	3,024,121	1,605,097
2015	834	2,382	695,556	5,673,924	1,986,588
2016	733	1,748	537,289	3,055,504	1,281,284
2017	623	1,883	388,129	3,545,689	1,173,109
2018	490	2,500	240,100	6,250,000	1,225,000
2019	442	2,883	195,364	8,311,689	1,274,286
2020	411	4,498	168,921	20,232,004	1,848,678
Total	17,103	96,376	17,812,989	712,122,038	103,932,036
Average	950.2	5,354.2	989,610.5	39,562,335.4	5,774,002

Source: Information about the banking system of the Russian Federation. Central Bank of the Russian Federation (Bank of Russia). URL: https://www.cbr.ru/statistics/? PrtId=lic (accessed on 21.01.2021). The state of crime (archival data). Ministry of Internal Affairs of the Russian Federation. URL: https://mvd.ru/folder/101762 (accessed on 21.01.2021).

Information security specialists divide cyberattacks into the following main groups:

- phishing;
- social engineering (IPI);
- malware [13].

Phishing attacks combine social engineering and the use of malware, making them one of the main and most dangerous ways to carry out attacks on the Internet [14].

For the purposes of this article, phishing will mean an information system used to obtain confidential information from third parties (system users) by misleading them as to its authenticity due to the similarity

Fig. 2. **Example of a phishing website of a fictitious bank**

Source: [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (accessed on 27.05.2021).

of domain names, design, or content of information.[6] Based on this approach to phishing, we will consider the most common online scams.

FAKE BANKS

One of the most common categories of phishing resources is websites of fictitious (non-existent, fake) banks. An unscrupulous person creates a "bank" resource and begins to attract funds from citizens and legal entities for deposits. The user of the resource does not think about the legality of the activity of this person, since the interface of a non-existent "credit organization" is very similar to the interface of an operating bank [15]. Unfortunately, freedom of speech sometimes develops into the freedom of disinformation.

Fake documents presented on the resource (such as copies of licenses and powers of attorney) give the consumer the impression that this bank is legal (*Fig. 2*).

On behalf of the bank, the attackers are ready to provide all kinds of loans. When a consumer contacts such a bank (with a request to provide him, for example, a mortgage loan), his application is approved and he is asked to pay for the courier delivery of the contract and the sum insured. After the payment, the bank stops any communication with the client.

According to the official statistics of the Bank of Russia,[7] in Q3 2020, 375 sites of fake banks were identified, of which 95% of websites were blocked. It should be noted that the number of fake banks has tripled compared to the same period in 2019. Presumably, this is due to the expansion of people' need for money, as well as the expansion of the range of remote provision of financial services during the COVID-19 pandemic, which caused a reorientation of fraudsters in this area.

Also, cybercriminals actively use the names of operating banks and create clone sites or twin sites, which allows them to deceive the user [16].

Here is a list of the signs of phishing resources in this category:

1. Lack of information about the organization in the reference books (registers) of the Bank of Russia.

[6] Domain names registration rules in.RU and.РФ domain zones. URL: https://cctld.ru/ru/docs/project/algoritm/rules_draft.pdf (accessed on 17.01.2021).

[7] Review of the reporting of information security incidents during the transfer of funds. URL: https://www.cbr.ru/analytics/ib/review_3q_2020/ (accessed on 01.02.2021).

The official website of the Central Bank of the Russian Federation (URL: http://www.cbr.ru) contains:

- Book of state registration of credit institutions.
- Reference book on credit institutions.

2. Lack of information about the organization in the relevant registers of the Federal Tax Service of the Russian Federation and Roskomnadzor.

Information about the organization presented on the site can also be checked in the following registries:

- The Unified State Register of Legal Entities is posted on the official website of the Federal Tax Service (FTS) of the Russian Federation.
- The register of operators processing personal data is posted on the official website of Roskomnadzor of Russia.

Fake banks have become one of the most common methods of fraud in Russia, since attackers do not need to accurately copy the resources of real credit institutions, it is enough to place tabs with the name "Loan", "Deposits", etc. on the site. These names can mislead the user and give him a real idea that he is on the site of an operating bank.

Consumers need to pay attention to the design of the resource: fraudsters, as a rule, do not bother to post the relevant documentation on the "official website" (in some cases, they do not even indicate the license number for operations).

FAKE INSURANCE COMPANIES

The emergence of the possibility of issuing electronic compulsory motor third party liability insurance (OSAGO) using the Internet not only made life easier for drivers but also provoked an increase in fraud in this area.

Within this category, the attacker acts in various ways:

- creates a copy of the resource of an operating insurance company with proposals for issuing electronic OSAGO;
- offers for sale fake or unsecured insurance company forms.

The consumer either pays for a falsified OSAGO or pays for delivery and buys fake forms.[8]

According to the statistics of FinCERT of the Bank of Russia, in the period from 01.09.2018 to 31.08.2019, 22 resources were removed from the delegation, on which the activities of fake insurance organizations were carried out.[9]

The phishing site of an insurance company allows the consumer to create a false impression that the purchase of a form does not entail negative consequences for the consumer. However, when acquiring knowingly false, empty and invalid forms, the consumer loses the opportunity to claim insurance compensation in the event of an insured event.

Fake insurance companies are becoming quite common in Russia due to the fact that the consumer is trying to save time and money when drawing up an insurance certificate in the hope that an insured event will not occur [2].

Also, in practice, there are cases when an insurance company creates a resource and pretends to be an organization that provides insurance services. The consumer orders this or that insurance service, pays for it by transferring the money to the insurer's card or to his account. The insurer undertakes to deliver the insurance certificate or provide another service at a certain time but never provides the offered certificate or service to the consumer (*Fig. 3*).

In this regard, the consumer should not only pay attention to the design and content of the resource of the insurance company but also check this organization in the relevant directories and registers (in the Directory of financial market participants of the Bank of

[8] According to Art. 327 "Forgery, manufacture or circulation of forged documents, state awards, stamps, seals or letterheads" of the Criminal Code of the Russian Federation both sellers and buyers answer in law.

[9] For more details see "Report of the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia" posted on the official website of the Bank of Russia. URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (accessed on 02.02.2021).

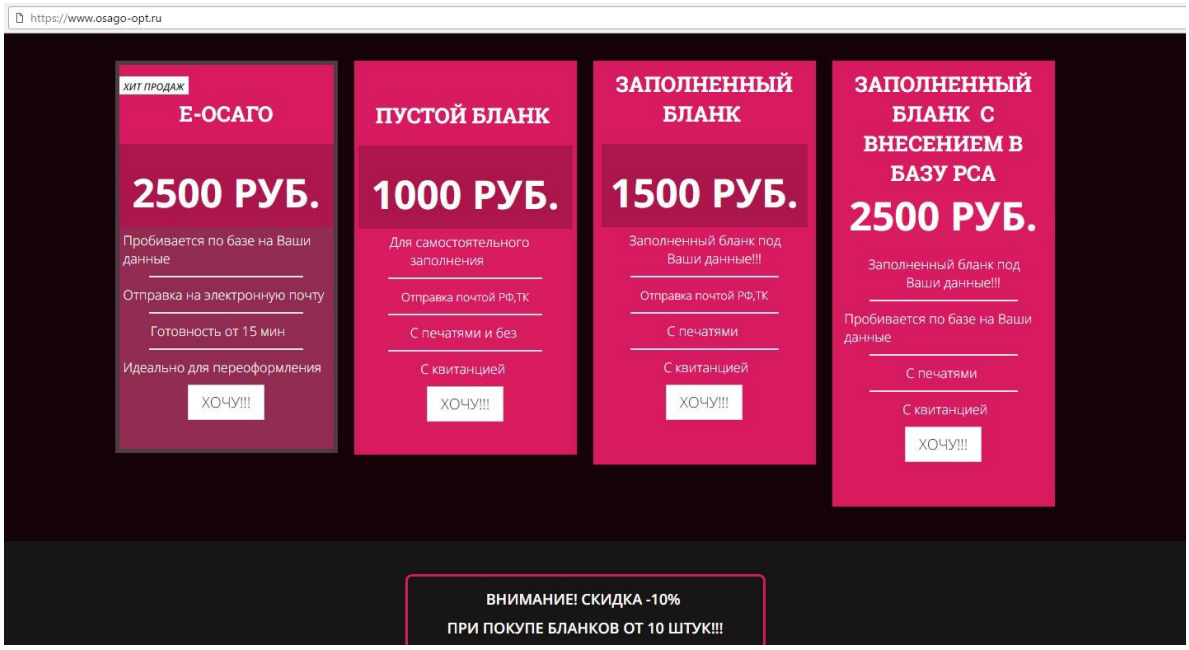

Fig. 3. **Example of a phishing website of a fictitious insurance company**

Source: [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (accessed on 28.05.2021).

Russia,[10] in the list of the Russian Union of Auto Insurers[11]).

FAKE P2P (PEER-TO-PEER)

This category is one of the most attractive for cybercrime, due to the simplicity of the design of an information resource for theft of funds. Attackers using this method get access to confidential information of both the payment card and the consumer himself. According to the statistics of FinCERT of the Bank of Russia, in the period from 01.09.2018 to 31.08.2019, 132 sites were removed from the delegation, which pretended to be resources that provide services for P2P transfers.[12]

The simplicity of the design of information resources that provide services for P2P transfers allows fraudsters to fake them easily: an image of plastic cards is drawn up, and the emblems and names of payment systems or a credit institution are indicated. These attributes allow the consumer to form a false idea that he is on the site of an operating organization (*Fig. 4*).

It should be noted that the user transfers to the attackers not only his personal data but also the number of the third party's payment card to which he makes a remote transfer.

Such resources are very attractive for consumers since they offer services for an interest-free transfer or a transfer with a low percentage of funds between payment cards of different banks or payment systems [17].

Avoiding the use of unscrupulous resources will help to check the presence of the organization in the Register of payment system operators of the Bank of Russia, as well as the use of a secure connection when making a transfer.

At the same time, if the resource indicates that the services are provided by any credit institution, then it is necessary to check the presence of this organization in the corresponding list of the Bank of Russia.

[10] Directory of participants in the financial market of the Bank of Russia. URL: http://www.cbr.ru (accessed on 02.02.2021).

[11] Is the organization's web address included in the list of the Russian Union of Auto Insurers? URL: https://www.autoins.ru/e-osago/chleny-rsa-osushchestvlyayushchie-oformlenie-elektronnykh-polisov/ (accessed on 02.02.2021).

[12] For more details see «Report of the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia». Official website of the Bank of Russia. URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (accessed on 02.02.2021).

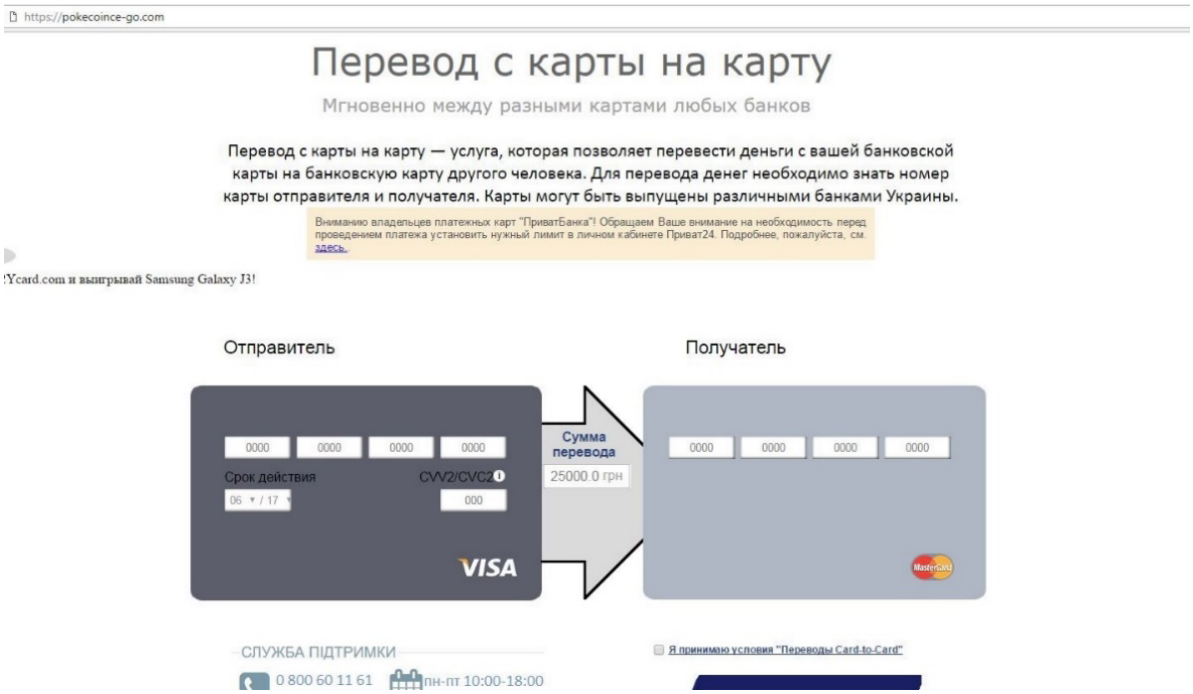

Fig. 4. **Example of a phishing website of a fictitious P2P system**

Source: [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (accessed on 29.05.2021).

FAKE ONLINE STORES

Online stores attract customers with their prices (due to savings on the rental of premises), as well as the possibility of convenient delivery.[13] Online stores attract customers with their prices (due to savings on the rental of premises), as well as the possibility of convenient delivery. The scheme of fraud, in this case, is the same: as soon as the buyer transfers his money to the seller's account, communication with him is ceased (the store's website stops working, there is no response by e-mail).

The design and content of the resources are also similar to the sites of the operating organizations (*Fig. 5*) [18].

To protect themselves and purchase the appropriate product, the consumers need to check the information about the organization that provides the goods or services indicated on the site,[14] as well as reviews and the domain name in the search engine.

FRAUD

This category is generalized. It contains fraud schemes that are carried out by organizations using the Internet. These schemes of fraudulent activities of fictitious organizations can be divided into the following subtypes:

- an organization conducting fake surveys under the pretext of paying a reward;
- an organization promising employment;
- an organization offering to formalize the payment of non-existent compensation (*Fig. 6*) [19];
- the organization issuing the "COVID-19 Vaccination Certificate".[15]

Attackers attract users by providing an opportunity to get money quickly. Users,

[13] In a number of cases, the seller justifies these prices, sometimes not at all hiding such facts as "stolen goods", "confiscated", etc. Therefore, if the victim decides to buy such a product, then it is unlikely that he will later go to complain, since, in fact, he is an accomplice in the crime (buying stolen goods).

[14] This information can be checked on the official website of the Unified State Register of Legal Entities of the Federal Tax Service of the Russian Federation. URL: https://egrul.nalog.ru (accessed on 26.10.2021).

[15] "The same as the original": How scammers sell COVID passports in Russia. URL: https://ria.ru/20210303/covid-1599609177.html (accessed on 14.03.2021).

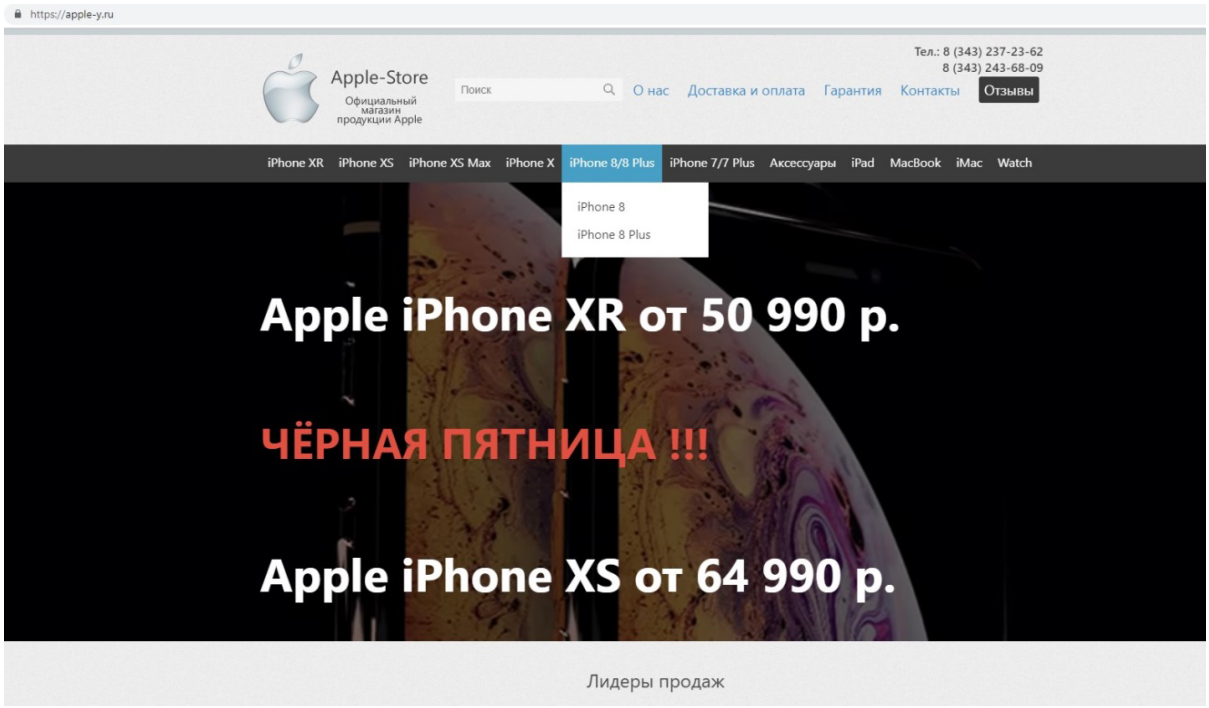

Fig. 5. **Example of a phishing website of a fictitious online store**

Source: [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (accessed on 01.06.2021).

counting on this, transfer personal data to cybercriminals, including bank card data, to transfer the promised salary.[16]

The interface of resources in this category is identical to the interfaces of official resources, which allows misleading the client about generating income.

A user on this resource takes a survey (test), which consists of 7–10 simple questions. Once the survey is complete, the resource generates a fictitious prize and invites the user to transfer funds to his payment card. To save money and arrange their withdrawal to the resource, it is proposed to post a deposit.[17] The user provides the attackers with the card details and personal data, which allows the scammers to write off funds from his payment card [20].

In addition to surveys, fraudsters offer various compensation (for example, for medical services). As a rule, the resource contains non-existent documentation of the Government of the Russian Federation, which makes it possible to return and pay compensation to the population.

Users (most often pensioners) are actively involved in this category of resources through calls and SMS-mailings, in which people are convinced that compensation is provided within the framework of one of the federal programs and does not lend itself to publicity, since there is a payment limit.

Attention should be paid to the fact that surveys and compensation can be carried out both by real organizations and by government services. In order not to become a victim of fraudsters, you need to pay attention to the following signs, which most often indicate the fraudulent nature of the resource in this category:

- transfer of funds to third parties as payment;
- the lack of an organization in the Unified State Register of Legal Entities of the Federal Tax Service of Russia;

[16] It is not uncommon for people to pay an insurance premium for the provision of orders or to fix payments to find a non-existent job, or it is proposed to pay for the delivery of an employment contract.

[17] The payment amount is insignificant and ranges from 250 to 1000 rubles.

Fig. 6. **Example of a phishing website with information about payments of non-existent compensation**

Source: [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (accessed on 02.06.2021).

- carrying out activities not provided for by the license (permit);
- reviews of real people about the organization, found online (Yandex, Google).

Counteraction to this type of fraud is carried out not only by law enforcement but also by regulatory authorities. In accordance with the regulations of the Bank of Russia, credit and non-credit financial institutions inform the Bank of Russia when information and financial security incidents are detected,[18] and also notify about identified phishing resources [21].

Supervisory measures by the Bank of Russia and Roskomnadzor are aimed primarily at ensuring the stability of the financial system and the protection of creditors and depositors. Such activities are based on an integrated approach: compliance with regulations, timely notification of the Bank of Russia and comprehensive analysis within the framework of supervisory measures allow credit and non-credit financial institutions to minimize the risks of adverse consequences both for themselves and their clients, as well as increase the level of information safety and security.

IMPROVING CYBERSPACE CONTROL

Given the active use of cyberspace in the provision of various types of banking services, it is necessary to understand that the regulatory authorities are faced with a rather difficult task — to build effective supervision over the reliability of information posted on Web-representations of financial institutions. Obviously, such work should be carried out with active interaction with law enforcement agencies to take timely measures to prevent fraudulent actions (close fraudulent resources as soon as possible and take measures to bring the perpetrators to justice) [3, 22].

An important role in reducing cybercrime is also assigned to increasing the overall level

[18] For more details see the regulation of the Bank of Russia dated 09.06.2012 No. 382-P "On the requirements for ensuring the protection of information when making money transfers and on the procedure for the Bank of Russia to monitor compliance with the requirements for ensuring the protection of information when making money transfers", Regulation of the Bank of Russia dated 17.04.2019 No. 683-P "On the establishment of mandatory requirements for credit institutions to ensure the protection of information in the implementation of banking activities in order to counteract the transfer of funds without the consent of the client", Regulation of the Bank of Russia dated 17.04.2019 No. 684-P "On the establishment of mandatory requirements for non-bank financial organizations to ensure the protection of information when carrying out activities in the field of financial markets in order to counter the implementation of illegal financial transactions".

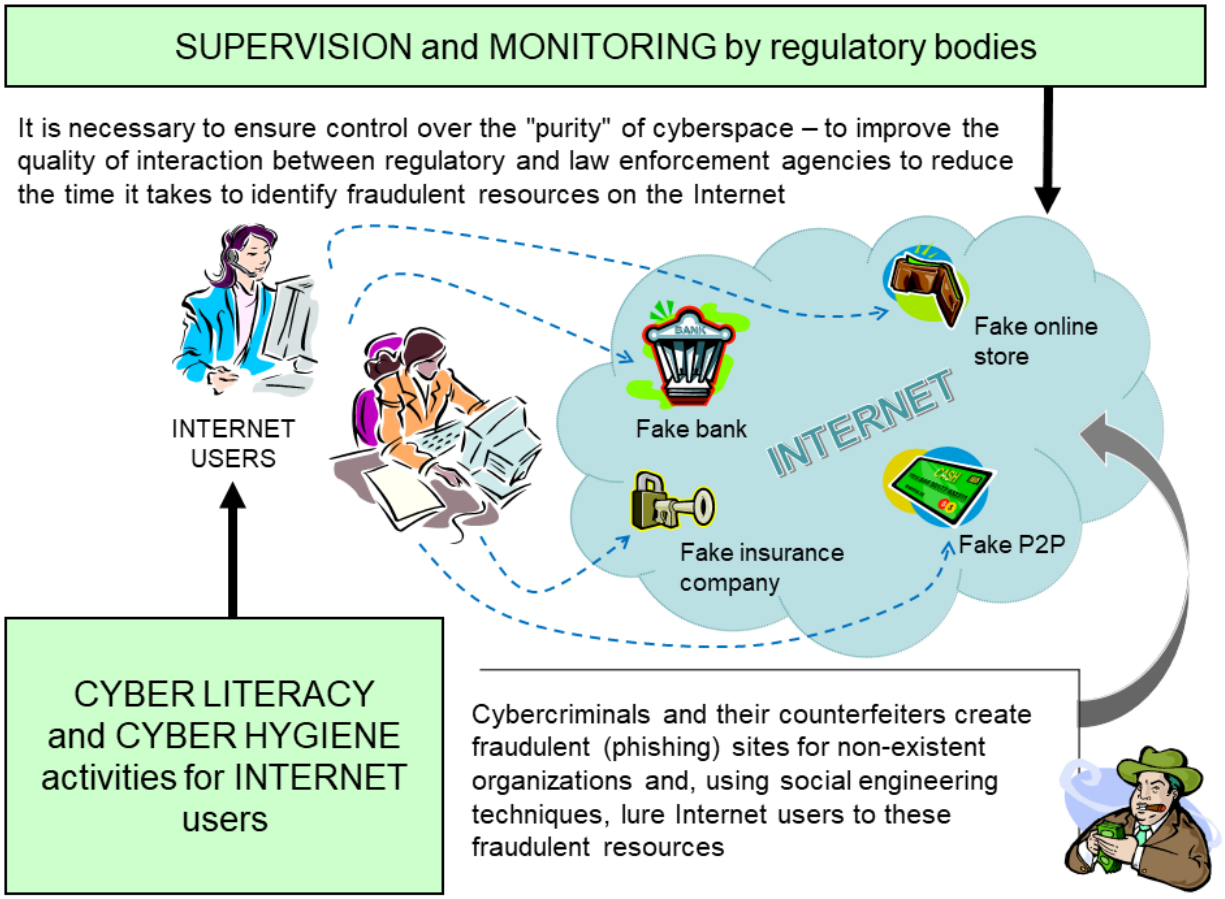

Fig. 7. **Measures to control cyberspace**

Source: complied by the authors.

of cyber literacy among all groups of the population (*Fig. 7*). One of the most effective ways is to include specialized disciplines (courses) in educational programs for students of secondary and higher educational institutions, according to which students will gain knowledge in the field of functioning of new financial technologies, as well as in basic methods ensuring cybersecurity (including specific topics on countering cyber fraud).

In addition, the literature discussed in the first part of the article "Introduction" will contribute to an increase in the level of cyber literacy and general literacy of the population. Since the beginning of June 2021, the Bank of Russia has published a list of companies with identified signs of illegal activity in the financial market (the so-called "black" list): https://cbr.ru/inside/warning-list/, which includes, among other things, and phishing companies. If the organization is on this list, then it is better to ignore its services and leave. If a client has encountered a fraudulent company, but it is not on the list, he can report it.[19]

Phishing prevention also includes watching TV programs such as "Eduard Petrov's Investigation. Internet pandemic, or COVID-19 Cult — Russia 24" (URL: https://youtu.be/0hklRanOSxI) and "Finiko Finale. Special Report — Russia 24" (URL: https://youtu.be/5OtEZtLw9bE), which illustrate the results of human belief in magic pills and financial pyramids.[20] Thus, a control system in cyberspace will be developed

[19] More details: "The Central Bank has published a blacklist of 1.8 thousand illegal companies". URL: https://www.rbc.ru/finances/01/06/2021/60b5fbdc9a79471a267396e1 (accessed on 25.07.2021).

[20] Only fakes about the miraculous effect of eating ... fly agarics, which are gaining popularity, can surpass the existing phishing methods. (see URL: https://smotrim.ru/article/2639202).

and the cultural behavior of all cyberspace participants will be enhanced.

CONCLUSIONS

The contribution to the development of theoretical and applied science consists in adapting solutions for the development of scientific and technological progress in Russia based on the positive experience of China, as well as in expanding the methodological apparatus of information security and cyber literacy.

The new reality and cybersecurity challenges that both financial institutions and their clients are forced to face when using remote banking technologies require modernization, and in some cases, a significant revision of risk management procedures, including new procedures for controlling information posted on the web-representations (sites) of organizations [15]. It is also necessary to increase the level of cyber literacy of various groups of the population.

The lag in cyber literacy is becoming the main reason for stealing money from clients of organizations in the credit and financial sector. In this regard, it is necessary to use various communication channels and media to alert customers to potential threats from cyber fraudsters, the most common types of cyberattacks and methods of social engineering.[21] Such activity will significantly reduce the level of cyber fraud and minimize it. Regulators should improve the way they oversee and control the information posted on the Internet. The result of such activities will not only increase the confidence of customers and Internet users in remote banking technologies but also increase confidence in the credit and financial sector as a whole.

[21] On this topic, the Bank of Russia issued recommendations for credit institutions dated February 19, 2021, No. 3-MP "Methodological Recommendations for Strengthening Information Work with Clients by Credit Institutions in order to counteract unauthorized transactions". URL: https://cbr.ru/StaticHtml/File/117596/20210219_3-mr.pdf (accessed on 02.02.2021).

REFERENCES

1. Berdyugin A.A., Revenkov P.V. Cyberattack Risk Assessment in Electronic banking Technologies (the Case of Software Implementation). *Finance: Theory and Practice*. 2020;24(6):51–60. (In Russ.). DOI: 10.26794/25875671–2020–24–6–51–60
2. Kuznetsov M.V., Simdyanov I.V. Social engineering and social hackers. St. Petersburg: BHV-Petersburg; 2007. 368 p. URL: https://www.koob.ru/kuznetsov_m/social_engineering (accessed on 27.07.2021). (In Russ.).
3. Konyavskaya S.V., Revenkov P.V., Rusin L.I. et al. Cybersecurity in the conditions of electronic banking: Practical guide. Moscow: Prometei; 2020. 522 p. (In Russ.).
4. Rogovsky E.A. Cyber-Washington: global ambitions. Moscow: International relations; 2014. 848 p. (In Russ.).
5. Bushov Y., Ushakov V., Svetlik M., Esipenko E., Kartashov S., Orlov V., Malakhov D. Activity of mirror neurons in man in the observation, pronunciation and mental pronunciation of words. *Procedia Computer Science*, 2020;169:100–109. DOI: 10.1016/j.procs.2020.02.121
6. Dolingo B.A. Science fiction is the most powerful tool for the development of imagination. *Nauka i zhizn' = Science and Life*. 2016;6:118–121. URL: https://www.nkj.ru/archive/articles/28924/ (accessed on 27.01.2021). (In Russ.).
7. Osmankevich K.R. Features of legal regulation of the banking system and banking supervision in the People's Republic of China. *Bulletin of the Moscow University. Series 26: State Audit*, 2020;1:50–59.
8. Sorokin D.E. Political economy of Russia's technological modernization. *Ekonomicheskoye vozrozhdeniye Rossii = Economic revival of Russia*. 2020;1(63):18–25. URL: https://www.elibrary.ru/item.asp?id=42543826 (accessed on 05.08.2021). (In Russ.).
9. Tomsky A.G. inDriver: From Yakutsk to Silicon Valley. The history of the creation of a global technology company. Moscow: Alpina Publisher; 2020. 256 p. (In Russ.).
10. Clearfield C., Tilcsik A. Meltdown: Why Our Systems Fail and What We Can Do About It. Penguin Press; 2018. 304 p.
11. Vincent A. Don't feed the phish: how to avoid phishing attacks. *Network Security*. 2019;2:11–14. DOI: 10.1016/S 1353–4858(19)30022–4

12. Kaganov V.I. Computer calculations in Excel and Mathcad environments. Moscow: Hotline — Telecom; 2015. 328 p. (In Russ.).
13. Dobryshin M.M, Zakalkin P.V. Model of a "Phishing" type of computer attack on a local computer network. *Cybersecurity issues = Voprosy kiberbezopasnosti*. 2021;2(42):17–25. (In Russ.). DOI: 10.21681/2311–3456–2021–2–17–25
14. Salihu A., Metin H., Hajrizi E., Ahmeti M. The Effect of Security and Ease of Use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine*. 2019;52(25):159–163. DOI: 10.1016/j.ifacol.2019.12.465
15. Eskindarov M.A., Solov'ev V.I., eds. Paradigms of the digital economy: Artificial intelligence technologies in finance and fintech. Moscow: Cogito-Center; 2019. 325 p. (In Russ.).
16. Grassegger T., Nedbal D. The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*. 2021;181:59–66. DOI: 10.1016/j.procs.2021.01.103
17. Derek S. Reveron, John E. Savage. Cybersecurity Convergence: Digital Human and National Security. *Orbis*. 2020;64(4):555–570. DOI: 10.1016/j.orbis.2020.08.005
18. Mitnick K., Vamosi R. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company; 2017. 320 p.
19. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley publ.; 2018. 320 p.
20. Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute evaluation on attack trees with incomplete information: a preprint. *Computers & Security*. 2020;88:1–21. URL: https://arxiv.org/abs/1812.10754 (accessed on 28.02.2021).
21. Frumina S.V. Developing the digital economy: Experience of Russia and Germany. *Finansy i kredit = Finance and credit*. 2019;25(2):263–276. (In Russ.). DOI: 10.24891/fc.25.2.263
22. Salloum S., Gaber T., Vadera S., Shaalan K. Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*. 2021;189:19–28. DOI: 10.1016/j.procs.2021.05.077

ABOUT THE AUTHORS

***Pavel V. Revenkov* —** Dr. Sci. (Econ.), Prof., Department of Information Security, Financial University, Moscow, Russia
pavel.revenkov@mail.ru

***Kseniya R. Oshmankevich* —** lecturer of the Information Sciences Institute, Moscow State Linguistic University, Moscow, Russia
osh-ksenia94@mail.ru

Aleksandr A. Berdyugin — junior researcher, Department of Information Security, Moscow, Russia
AABerdyugin@fa.ru

Authors' declared contribution:
Revenkov P. V.— the setting of the research task, development of the concept of the article, verification of the results and conclusions.
Oshmankevich K. R.— the results of the research, graphical representation of the material, formation of recommendations and conclusions.
Berdyugin A. A.— introduction and analysis of the literature, tabular data and correlation analysis, text proofreading.

The article was submitted on 24.02.2021; revised on 09.03.2021 and accepted for publication on 22.09.2021.
The authors read and approved the final version of the manuscript.