Alexander A. Berdyugin[1], Pavel V. Revenkov[2]
[1, 2] *Financial University under the Government of the Russian Federation,*
Scherbakovskaya Street, 38, Moscow, 105187, Russia
[1]*e-mail: a40546b@gmail.com, https://orcid.org/0000-0003-2301-1776*
[2]*e-mail: pavel.revenkov@mail.ru, https://orcid.org/0000-0002-0354-0665*

Approaches to measuring the risk of cyberattacks in remote banking services of Russia

DOI: http://dx.doi.org/10.26583/bit.2019.4.06

Abstract. Purpose. Due to the use of technology in banks their risks of information security breach are rising significantly. In the context of active introduction of remote banking services (RBS) in banking business of Russia, additional study of issues of assessing the risk of cyberattacks on banking automated systems was required. *Methods.* The methods of financial management, probability theory, system analysis of scientific literature on fundamental and applied research, and a method of graphical interpretation of analyzed phenomena are used. The paper gives a detailed analysis of the concepts of "cyberspace" and "cybersecurity". Remote banking is considered from the point of view of financial management. Attention is drawn to the factors of work in cyberspace that increase the levels of banking risks. The relationship of cyberattacks on banking automated systems and possible consequences for the bank is analyzed. *Novelty.* Given the wide spread of social engineering methods when committing fraudulent activities on the Internet the measures to increase the cyber literacy of population are needed. The method for assessing the risk of cyberattacks on RBS for use by risk department specialists and employees of internal control services is developed. As a result, considering innovative systems and technologies that await us in the future, the effectiveness of risk assessment for solving current challenges is increased. *Results.* Attempts are made to formulate the mathematical model of the probabilistic analysis of information security incidents to optimize the algorithm for responding to incidents. Calculations based on the proposed model made it possible to determine the duration of exploitation of vulnerability of RBS, when the probability of preventing an incident exceeds probability of its realization. The findings may be useful for scientific research on the risks of information security breach in RBS.

Keywords: cyberspace, risk of cyberattacks, remote banking services, cybersecurity, risk assessment, information security incident

For citation: BERDYUGIN, Alexander A.; REVENKOV, Pavel V. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. IT Security (Russia), [S.l.], v. 26, n. 4, p. 83-92, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1233>. Date accessed: 20 nov. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.06.

Introduction

The latest achievements in the field of information and telecommunication technologies have significantly changed the process of conducting the banking business and have become the basis for the active implementation of remote banking services (RBS)[1]. The process of interaction between the bank and the client in the conditions of application of RBS is carried out in a virtual environment or, in other words, in cyberspace.

The concepts of "cyberspace" and "cybersecurity" are currently absent in the legislation of the Russian Federation[2]. The concepts of "cyberspace" and "cybersecurity" can be found in a few international and national standards related to ensuring information security. Further on we will use these terms. If we combine different approaches to the definition of these concepts, then cyberspace is most often understood as an environment of information interaction and data

[1] The most common RBS options are: Internet banking (managing bank accounts and cards via the Internet and an on-line web browser) and mobile banking (managing bank accounts and cards from tablet computers, smartphones and other smart devices).

[2] The terms "information space" and "information security" are traditionally used.

exchange implemented in computer communication networks and networks, where the elements of cyberspace are servers, computers, telecommunication equipment, communication channels, information and telecommunication networks, and cybersecurity is maintaining the confidentiality, integrity and availability of information in cyberspace[3].

The banking business began to use cyberspace, first of all, due to significant cost savings for operating activities (there is no need to maintain banking offices, and the client himself performs the functions of the operator from his computer, tablet or smartphone) [6].

We add that the daily increase in the number of cellular subscribers and users of the global Internet network contributes to the spread of RBS in various parts of the world (including both developed and developing countries[4]) [8].

Additional income comes from the increase the value of cash flows due to the increase in commission fees and/or reducing expenses due to growth in operating efficiency. Consider the impact of scientific and technological progress on return on equity (ROE):

$$ROE = ROA \times EM = PM \times AU \times EM, \quad (1)$$

where PM is the profit margin; AU – asset turnover ratio (asset utilization); EM – the value of the equity multiplier. The main variable in the formula (1) is PM – net profit to total revenue ratio and AU – the ratio of total revenue to asset value. Return on equity ratio represents the amount of the bank's income per monetary unit of equity:

$$ROE = NP/E,$$

where NP is net profit (the difference between income and expenses), and E is the average equity.

Investments in RBS increasing PM by minimizing costs and AU by increasing the bank's commission income, therefore ROA and ROE will increase. If the expansion of market share and the increase in the asset base as a result of innovations exceed the growth of capital, then the resulting financial leverage (a higher EM value) will advance ROE. For the banks with excess capital relative to the minimum, which regulators require, it is necessary to invest in RBS and other innovations.

However, in addition to the obvious advantages, work in cyberspace is accompanied by a number of factors that can increase levels of banking risks:

- remote banking operations are mostly "virtual" in nature (in fact the client after the invoice and registration a contract for the provision of services using RBS has no direct contact with the bank). This type of interaction places increased demands on customer identification (including the implementation of the "Know your customer" principle). Otherwise, an attacker may initiate operations on behalf of the client;
- the availability of "open" telecommunication systems (the availability of the global Internet and cellular communications in the absence of proper control over these types of communications complicates the control over actual users of these types of communications);
- extremely high speed of transactions (the speed of banking operations performed using RBS is limited to seconds, which also imposes increased control requirements) [9];

[3] For the analysis of approaches to the definition of the concepts of "cyberspace" and "cybersecurity" we used [1, 2, 3], as well as [4, 5].

[4] For example, mobile payments play a key role on the African continent. Given the large distances, poor transport and insufficient number of banks in Africa, various money transfer systems allow hundreds of millions of Africans who have recently migrated to cities to send money to their families in villages [7].

- the global nature of inter-network operational interaction (since with RBS operations are performed not only in the country in which the client is located, but also beyond its borders, then additional sources of risks arise due to the peculiarities of the legislation in each individual country through which clients pay[5]) [10];

- the possibility of using RBS for illicit activities (due to insufficient control by regulators, speed of execution of the operations themselves and the ability to hide some of the data of the real perpetrators, etc.).

In this paper (applicable in practice in the credit and financial sphere), the authors use the term "risk of cyberattacks" (RCa), which is understood as a measure of the increase in typical banking risks (including financial losses) arising from realization of a cyberattacks on banking automated systems (BAS)[6].

Thus, the aim of the study is to analyze cause-effect relationships under the influence of computer attacks on typical banking risks and to develop new (applicable in practice in the credit and financial sphere) approaches to assessing RCa, due to which possible to improve significantly the quality of ensuring cybersecurity in organizations of the financial sector.

1. Expanding profiles of typical banking risks due to computer attacks

Consider the main types of cyberattacks on BAS noted in the annual reports of FinCERT of the Bank of Russia[7] and the company's Group-IB[8]: attacks on AWP CBR, AWP SWIFT, AWP RBS[9] and attacks on self-service devices (Automated Teller Machines – ATMs).

To implement all these attacks, first one needs to download malicious software (malware) into the local area network (LAN) of the credit institution. To do that, an attacker sends an e-mail to a credit institution containing malware, which is not detected by antivirus tools. After malware infection, using SMB requests, a scan of the LAN segment accessible to the infected machine is performed to infect new workstations.

Subsequently, additional malware loads onto infected machines, which acts as a botnet-client and has remote management capabilities (hiding the desktop, which allows remote management to be invisible to the user), as well as malware to steal passwords.

The main reason why the above attacks are "successful" is the human factor, which manifests itself in the form of a negligent attitude of bank employees to the established algorithm for preparing, storing, processing and transmitting electronic customer orders. According to the Group-IB's report for 2018 year, in Russia 1-2 banks were subjected to computer robberies every month. The damage from one theft on average is 132 million rubles ($2 million).

The development of the digital economy in Russia and the minimization of the level of RCa are associated with an increase in the level of cyberliteracy of the population of our country [13]. Particular attention should be paid to the understanding by all users of the global Internet that they work more often than not in a "trusted environment". Therefore, knowledge of the main

[5] It is necessary to take into account the features of a number of offshore zones, where in addition to tax benefits, there is a certain ban on the issuance of information about customers and their operations.

[6] The term has already been used by authors in scientific papers, for example, [11] and [12].

[7] FinCERT is a specialized unit of the Information Security Department of the Bank of Russia, whose functions include countering computer attacks on credit and financial institutions. The article uses the data of the annual reports of FinCERT for 2016, 2017 and 2018 years, available on the official website of the Bank of Russia (www.cbr.ru).

[8] Group-IB has been operating since 2003 year. One of the leading international companies for the prevention and investigation of cybercrime and fraud using high technology (www.group-ib.ru).

[9] AWP CBR is an automated workstation of a client of the Bank of Russia, AWP SWIFT is an automated workstation of a client of the Society for Worldwide Interbank Financial Telecommunications, AWP RBS is an automated workstation of a client of RBS.

types of cyber-fraud can significantly reduce the number of hacker attacks [14]. The development of computer discipline and the prevention of uncontrolled development of cyberspace [15] can be facilitated by the studying of "blind" typing with ten fingers.

The authors of this paper propose introducing the method of "blind" typing with ten fingers into the education system in Russia, as the development of fine motor skills of the hands contributes to the activation of the frontal lobes of the brain. Proper finger positioning on a keyboard is analogic to complying with traffic signs when traveling.

Work in cyberspace, first of all, increases role of the technical components of all typical banking risks (Fig. 1), among which operational, legal, strategic, reputational and liquidity risks can be highlighted[10] [11].

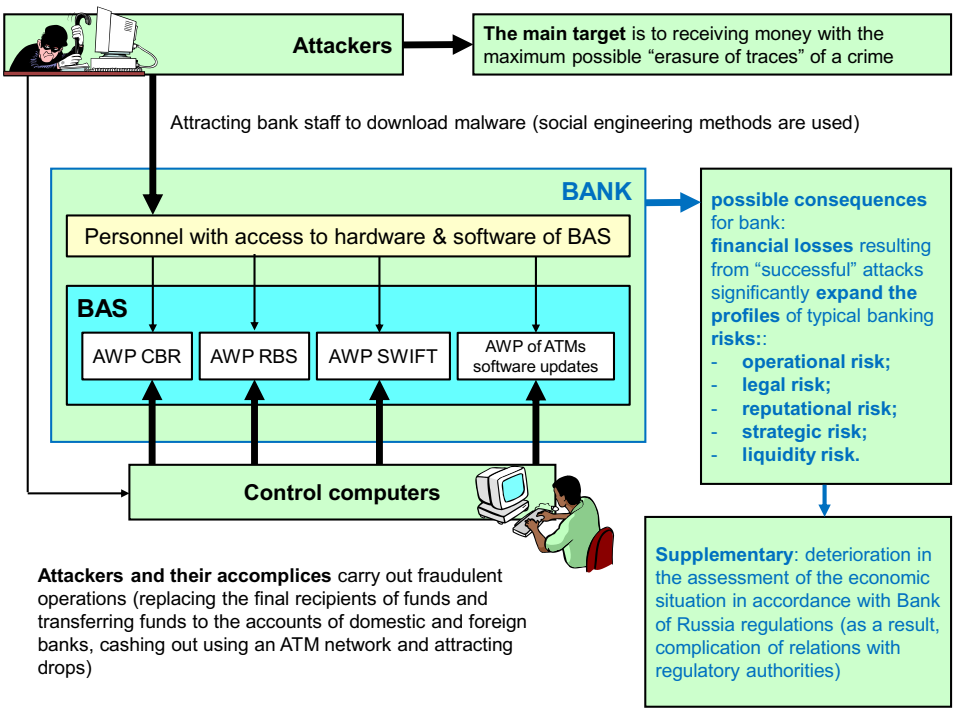

Fig. 1. Interconnection of cyberattacks on hardware and software (H&S) of BAS and possible consequences for the bank

Underestimation of the possible consequences of cyberattacks can seriously affect the stability of a commercial bank. In this regard, the assessment of RCa manifestations by specialists of risk divisions should be carried out in a timely manner, followed by notification to the management of the credit organization so that the management of the credit organization can take preventive measures in a timely manner.

In the risk-divisions of credit institutions the specially trained professionals should be able to assess the quality of the vulnerability of different areas of digital circuit technology bank, formed in each individual credit institution (including in terms of increasing RCa). In order to understand the features of the functioning of distributed computing systems and have a clear understanding of the construction of information circuits of banking electronic services via the

[10] Full list of typical banking risks is given in the Letter of the Bank of Russia dated June 23, 2004 "On Typical Banking Risks" No. 70-T.

Internet and mobile communications, risk department specialists must have a technical education in addition to humanitarian (economic or legal) education.

Modern cybersecurity systems must be well automated for timely response on emerging incidents. The immediate start-up of the response process should occur from virtually any signal from information security monitoring systems. The effectiveness of the selected response method can be checked by the formula:

$$RRL = \frac{RE_{before} - RE_{after}}{RRC}, \quad (2)$$

where RRL is the effect of reducing risk (the method is applicable when $RRL > 1$); RE_{before} and RE_{after} – exposure to RCa before and after application of the response method; RRC – costs associated with the application of a particular response method.

Of course, the calculation by the formula (2) of compensation costs can be ignored in the presence of minor consequences of the implementation of the RCa. There is enough reserve for RCa in the budget plan [16, 17], as described below.

The consequences of cyber-risks are one of the components of an organization's operational risk. The Basel Committee on Banking Supervision (BCBS) recommends using this approach to risk assessment. In accordance with the recommendations of the committee, commercial banks should create a reserve for operational risk (OpR), considering the active use of digital technologies. The assessment of capital, which is reserved for OpR, is carried out using the basic indicative method:

$$K_{\text{OpR}} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^{3} \text{GI}_i, \quad (3)$$

where K_{OpR} is amount of capital allocated to cover OpR, $\frac{1}{3} \cdot \sum_{i=1}^{3} \text{GI}_i$ is average gross income for 3 years with the condition that $\text{GI}_i > 0$, $\alpha = 15\%$ – factor established by the Basel Committee on the basis of empirical research and influenced by the banking community, which includes mainly commercial banks in Europe. The average gross income of a commercial bank for the past 3 years is calculated according to the financial statements of the bank[11].

However, European standards are not always the benchmark for Russian's conditions. This requires developing a method adapted to the characteristics of credit organizations of the Russian Federation.

2. Formalization of the RCa assessment model in the RBS

For the most objective assessment of the violation's results, the possible consequences of realization of the RCa for banks and their customers should be considered. Authors propose a method of quantitative account of the consequences, considering such parameters as:

1) an increase in the amount of damage incurred as a result of realization of the RCa in the RBS, – conventional monetary units (n);

2) an increase in the intelligence coefficient of cybercriminals (i.e., the smarter the hacker, the more damage and opportunities to go unnoticed), is a dimensionless quantity (IQ_{zlo});[12]

[11] See in detail in the articles [12, 18].

[12] Founding of a source of the threat is beyond the scope of the study. However, all activities on the Internet are monitored by web servers and are recorded in special logs. If the attack is conducted from a public institution, then the data is taken from the surveillance cameras installed there.

3) an increase in the period spent on restoring the continuity of banking activity after realization of the RCa, – hours (r);

4) reduction the time required for the manufacture and use of cyber-weapons for realization of the RCa (Hacking Services), – hours $(t \neq 0)$;

5) reduction in the cost of production (acquisition) of H&S for the implementation of cyberattacks, – conventional monetary units (d);

6) reduction in the amount of overhead costs for using H&S for cybersecurity breach (Hacking Services), – conventional monetary units (v).

Determining the effectiveness of cyber-weapons[13] (ef) is as follows:

$$ef = \frac{n \cdot IQ_{zlo} \cdot r}{(d+v) \cdot t}. \quad (4)$$

Thus, the ratio of formulas (3) and (4) allows us to determine the size of the reserve for cyber-risk in the composition of the OpR, that is $RCa = K_{\text{OpR}} / ef$.

The presented method of accounting for RCa can be used by both risk department specialists and employees of internal control services. The use of this relationship for the management of the continuity of credit institution activities may become the basis for estimates of reserved capital for the RCa in the RBS.

A significant part of the space-time continuum must be scientifically investigated if one wishes to obtain reliable results. In the opposite case, one might arrive to false conclusions [19, 20]. The mathematical representation of the RCa can be represented in the form of a model that underlies the classical "task of meeting" of probability theory (in our case, meet cybercriminals and anti-hacker in the network). Opponents act in cyberspace independently at any time period, their presence in the network is discrete due to the human factor. Let's say

S_1 – event 1 (the penetration of hacker into the LAN);

S_2 – event 2 (exploiting of RBS vulnerability);

S_3 – event 3 (the implementation of a computer incident and theft of money).

An event S_1 means a signal from cybersecurity system and the start of a response process. The time moments of the above persons in the network are denoted as a and b, respectively, and depicted on the axis aOb (Fig. 2).

From the conditions of the task, double inequalities follow:

$$0 \le a \le S_3 \text{ and } 0 \le b \le S_3$$

The coordinates of any point in the square $S_1 S_3 A S_3$ correspond to these inequalities.

Denote this square by a figure F. The points of the figure F have coordinates corresponding to the values of the stay of the cybercriminal and the anti-hacker online. This computer incident can be prevented if the difference between presence of the opponents on the network is less than S_2, i.e.

$$\begin{cases} b - a \le S_2 \text{ if } b > a \\ a - b \le S_2 \text{ if } a > b \end{cases}. \quad (5)$$

[13] The generalized term proposed by the authors includes a set of measures aimed at minimizing the possible consequences of the manifestation of the RCa.

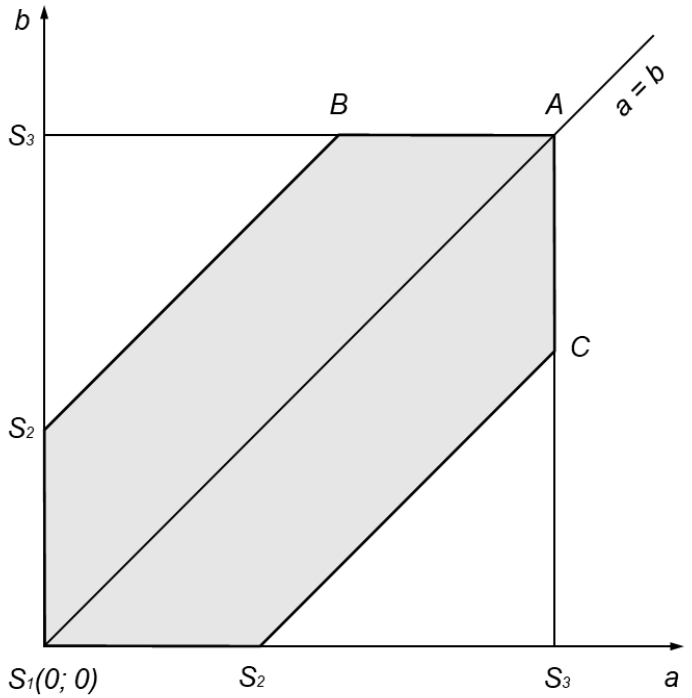

Fig. 2. Representation of the task in the Cartesian coordinate system

By the property of the absolute value of a number, the system (5) is equivalent to the inequality:

$$|a-b| \le S_2$$

The coordinates of the meeting points of the opponents fall into the figure $S_1S_2BACS_2$. Let's denote this hexagon by a figure f. Then the probability of realization of the RCa is equal to

$$P_{\text{RCa}} = \frac{\text{area of } f}{\text{area of } F} = \frac{S_3^2 - (S_3 - S_2)^2}{S_3^2} = \frac{S_2 \cdot (2S_3 - S_2)}{S_3^2}. \quad (6)$$

Accordingly, the probability of the opposite event (computer incident prevention – CIP) is equal to

$$P_{\text{CIP}} = 1 - P_{\text{RCa}}. \quad (7)$$

Let's consider, how this model acts "in numbers". For example, the bank determined by its information security (or cybersecurity) policy that the maximum response time to an information security incident is no more than 90 minutes. Based on this $S_3 = 90$. Let's compute the values of P_{RCa} and P_{CIP} by the formulas (6) and (7) for different values S_2 (Table 1):

Table 1. Determining the response to a computer attack

S_2	2	45	85
P_{RCa}	$\frac{2 \cdot (2 \cdot 90 - 2)}{90^2} \approx 0{,}044$	$\frac{45 \cdot (2 \cdot 90 - 45)}{90^2} \approx 0{,}75$	$\frac{85 \cdot (2 \cdot 90 - 85)}{90^2} \approx 0{,}997$

P_{CIP}	0.956	0.25	0.003

From this, we can determine the value S_2 when the implementation and prevention of the RCa are equally possible, i.e. $P_{\text{CIP}} = P_{\text{RCa}} = 0{,}5$:

$$\frac{x \cdot (2 \cdot 90 - x)}{90^2} = 0{,}5$$

$$180x - x^2 = 0{,}5 \cdot 90^2$$

$$x^2 - 180x + 4050 = 0. \quad (8)$$

The roots of this equation (8) are $x_1 \approx 153{,}6$ and $x_2 \approx 26{,}4$. But the value $x_1 \approx 153{,}6$ does not satisfy the condition of the task, because it exceeds $S_3 = 90$. Therefore, if the vulnerability of the RBS is exploited no longer than $S_2 \approx 26{,}4$ minutes, then the probability of the incident prevention exceeds the probability of its realization. In other words, the longer the vulnerability in BAS (including RBS) remains, the greater the chance for the theft of money through its use.

Thus, the RCa assessment methodology proposed by the authors makes it possible to analyze information security incidents that happened earlier to determine their relative frequency, with further forecasting of incident response and optimization of the response algorithm. Thank to its implementation in the risk assessment methodologies used by the cybersecurity units, it is possible to significantly increase the effectiveness of measures aimed at minimizing the possible consequences of realization of the RCa.

Conclusion

1. New challenges and cybersecurity issues, which arise due to credit and financial institution and their customers using RBS, require continuous improvement of solutions and often a substantial revision of the risk-management procedures, which include the internal control procedures in cyberspace. It also requires the mastering of measures to increase cyber-literacy and prevent the uncontrolled development of cyberspace (for example, financial literacy and method of "blind" typing with ten fingers);

2. Implementation of RBS allows credit organizations to significantly reduce the cost of operating expenses, but the work of the bank in cyberspace is associated with additional sources of typical banking risks, which include: operational and legal risk, strategically and liquidity risk, as well as the risk of loss of business reputation;

3. Accounting and evaluation of RCa on a risk-based approach should imply that each reason for the implementation of RCa has a potential impact on the bank (associated with disruption in the continuity of banking activities, reduced quality of RBS, financial losses, etc.) [21, 22]. Nevertheless, for a bank the size of the consequences of the destructive nature of the losses is more important, rather than the reasons for the loss of money (non-repayment of the loan, hacker attempt on the security system, etc.).

4. The risk divisions of credit and financial organizations should include specialists who are able to assess cyberrisks, and the methodological support used to audit and resolve issues of leveling the possible consequences of realization of the RCa on the H&S BAS must be updated in a timely manner;

5. The scientific research and developments should be one of the "pillars" of the RCa's management structure at the RBS. The models proposed in this paper (assessing the capital reserved for RCa and the task of meeting a cybercriminal and an antihacker in the network) are aimed at increasing the effectiveness of RCa management in the RBS.

REFERENCES:

[1] Interstate council for standardization, metrology and certification (2016) GOST 34009-2016 Mezhgosudarstvennyy standart: Sredstva i sistemy upravleniya zheleznodorozhnym tyagovym podvizhnym sostavom. Trebovaniya k programmnomu obespecheniyu [GOST 34009-2016 Interstate standard: Control devices and systems for railway traction rolling stock. Software requirements], Standardinform, Moscow, Russia (in Russian).

[2] The official site of the Federation Council of the Federal Assembly of the Russian Federation (2014) Kontseptsiya strategii kiberbezopasnosti Rossiyskoy Federatsii [Concept of Cybersecurity Strategy of the Russian Federation]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed: 14.07.2019) (in Russian).

[3] Federal Agency for Technical Regulation and Metrology (2014) GOST R 56205-2014 IEC/TS 62443-1-1:2009: Seti kommunikatsionnyye promyshlennyye. Zashchishchennost' (kiberbezopasnost') seti i sistemy. Chast' 1-1. Terminologiya, kontseptual'nyye polozheniya i modeli [GOST R 56205-2014 IEC/TS 62443-1-1:2009: Industrial communication networks. Security (cybersecurity) network and system. Part 1-1. Terminology, conceptual positions and models], Standardinform, Moscow, Russia (in Russian).

[4] Kasperskaya, Natalya I. et al. To the problem of assessing and ensuring the correctness of business processes. IT Security (Russia), [S.l.], v. 26, n. 3. P. 8–21, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1213 (accessed: 11.09.2019). DOI: http://dx.doi.org/10.26583/bit.2019.3.01 (in Russian).

[5] Yun Zhang, Qingxiong Weng and Nan Zhu (2018) The relationships between electronic banking adoption and its antecedents: A meta-analytic study of the role of national culture. International Journal of Information Management, vol. 40. P. 76–87. DOI: https://doi.org/10.1016/j.ijinfomgt.2018.01.015.

[6] Berdyugin A.A. (2018) Risk of cyber attacks impact on remote banking services. Proceedings of the Informatsionnaya bezopasnost' v bankovsko-finansovoy sfere [Information security in banking and financial industry], International youth scientific-practical conference within the framework of the V International Forum “How to get into the top five?”. Moscow, Russia, November 29, 2018. P. 149–154 (in Russian).

[7] Skinner C. (2018) Digital Human: The Fourth Revolution of Humanity Includes Everyone, Singapore: Marshall Cavendish International (Asia).

[8] Slavin B.B. (2019) Tsifrovyye platformy – novyy trend v korporativnoy avtomatizatsii [Digital platforms is new trend in corporate automation]. BIT. Biznes & Informatsionnyye tekhnologii = BIT. Business & Information Technology, no. 2 (85). P. 12–15 (in Russian).

[9] Revenkov P.V., Pimenov P.A. and Ozhered I.V. (2019) Protivodeystviye komp'yuternym atakam v usloviyakh primeneniya sistem elektronnogo bankinga: Uchebnoye posobiye [Countering Computer Attacks Using Electronic Banking Systems: A Training Manual], Moscow: Prometheus publisher (in Russian).

[10] Lyamin L.V. (2018) Elektronnyy banking i riski yego kliyentov [Electronic banking and the risks of its customers]. Banknoty stran mira = Banknotes of the World, no. 7. P. 26–28 (in Russian).

[11] Revenkov P.V. (2018) Rasshireniye profiley bankovskikh riskov v usloviyakh raboty v kiberprostranstve [Extending the profile of bank risk under conditions of work in cyberspace]. Finansy i kredit = Finance and Credit, vol. 24, no. 11 (779). P. 2471–2485. DOI: 10.24891/fc.24.11.2471 (in Russian).

[12] Berdyugin, Alexander A. Development of algorithm for assessment risk of cyber attacks in electronic banking. IT Security (Russia), [S.l.], v. 26, n. 2. P. 86–94, 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1201> (accessed: 31.05.2019). DOI: http://dx.doi.org/10.26583/bit.2019.2.06 (in Russian).

[13] Summanen K. (2019) IT-importozameshcheniye v Rossii [IT import substitution in Russia]. BIS Journal − Informatsionnaya bezopasnost' bankov (electronic journal), №2 (33). URL: https://ib-bank.ru/bisjournal/post/888 (accessed 03 September 2019) (in Russian).

[14] Revenkov P.V. and Krupenko D.S. (2019) Otsenka riskov informatsionnoy bezopasnosti v usloviyakh primeneniya sistem mobil'nogo bankinga [Risk assessment of information security in the context of the use of mobile banking systems]. Voprosy kiberbezopasnosti = Cybersecurity issues, no. 2 (30). S. 21–28. DOI: 10.21681 / 2311-3456-2019-2-21-28 (in Russian).

[15] Clearfield Chris and Tilchsik Andrásh (2018) Neuyazvimost'. Otchego sistemy dayut sboy i kak s etim borot'sya [Meltdown. Why our systems fail and we can do about]. Moscow: Azbuka-Attikus, KoLibri Publisher (in Russian).

[16] Avdoshin S.M. and Pesotskaya E.Yu. (2011) Informatizatsiya biznesa. Upravleniye riskami [Informatization of business. Management of risks], Moscow: DMK-Press (in Russian).

[17] Koz'minykh S.I. (2018) Modelirovaniye obespecheniya informatsionnoy bezopasnosti ob"yekta kreditno-finansovoy sfery [Modelling the Provision of Information Security of the Object of the Credit and Financial Sphere]. Finansy: teoriya i praktika = Finance: theory and practice, vol. 22, no. 5 (107). S. 105–121. DOI: 10.26794/2587-5671-2018-22-5-105-121 (in Russian).
[18] Yarygina I.Z., Gisin V.B. (2019) Metodologicheskiye podkhody k otsenke stoimosti bankovskikh aktivov kak metodu upravleniya finansovymi riskami [Evaluation of Bank Assets and Financial Risk Management: Methodological Approach]. Bankovskiye uslugi = Banking services, no. 2. P. 20–26.
[19] Turing A.M., Neumann J.v. and Yanovskaya S.A. (2018) Mozhet li mashina myslit'? Obshchaya i logicheskaya teoriya avtomatov. Per. s angl. 3-e izd. [Can the machine think? General and logical theory of automata. Trans. from Eng. 3rd ed.], Moscow: Lenand Publisher (in Russian).
[20] Barabanov, Alexander V.; Markov, Alexey S.; Tsirlov, Valentin L. Information security systematics of software supply chains. IT Security (Russia), [S.l.], v. 26, n. 3. P. 68–79, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1218 (accessed: 11.09.2019). DOI: http://dx.doi.org/10.26583/bit.2019.3.06 (in Russian).
[21] Dolganova O.I. and Deeva E.A. (2019) Gotovnost' kompanii k tsifrovym preobrazovaniyam: problemy i diagnostika [Company readiness for digital transformations: problems and diagnosis], Biznes-informatika = Business Informatics, vol. 13, no. 2. P. 59–72. DOI: 10.17323/1998-0663.2019.2.59.72 (in Russian).
[22] Ross A.J. (2016) The Industries of the Future, New York: Simon & Schuster.

Поступила в редакцию – 05 ноября 2019 г. Окончательный вариант – 23 ноября 2019 г.
Received – November 05, 2019. The final version – November 23, 2019.