ORIGINAL PAPER

DOI: 10.26794/2587-5671-2025-29-6-148-163
UDC 336.717.061(045)
JEL G21

Cyber Resilience of Credit Institutions in the Context of Digital Banking Business Development

M.F. Gumerov[a], I.A. Rizvanova[b], M.T. Belova[c]
[a] Central Economic and Mathematical Institute of the Russian Academy of Sciences, Moscow, Russian Federation;
[b, c] Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ABSTRACT

The development of the digital banking business and the transition from offline interaction to an online format in modern conditions encourage us to pay more attention to the generation of cyber risks in the banking sector. The **purpose** of the study is to develop the theoretical and practical foundations for ensuring the cyber stability of credit institutions in the context of the development of digital banking business. The **objectives** of the study were to study the conceptual apparatus of the cybersphere of credit institutions; to substantiate management decisions for building a cybersecurity system in a commercial bank; and to access the parameters of ensuring the security of client transactions in the process of cooperation between a commercial bank and an IT company. The **scientific novelty** of the research lies in the substantiation of management decisions in an economic system with a high level of turbulence and insufficient information about the mechanisms of their functioning using specific tools in the form of a phenomenological type model. The study aimed to describe the system's response to various impacts. In the course of the research, a dialectical method was used, revealing the possibilities of studying cyber risks in conditions of geopolitical instability, interconnection and interdependence, as well as such general scientific methods and techniques as scientific abstraction, analysis and synthesis, methods of grouping and comparison. The process of researching cyber risks in the context of the development of digital banking was considered through the prism of general patterns of banking activity, interconnection and unity of theory and practice, and a number of empirical research **methods** were also used. The paper presents a critical review of domestic and foreign scientific literature on cyber risks and cybersecurity and proposes a new concept of "cyber ecosystem". A model of interaction between a commercial bank and an IT-company specializing in the provision of anti-cyber risk services was developed, and an algorithm for justifying the bank's management decisions on allocating funds for cyber protection was proposed. The bank's cyber resilience map has been built, which made it possible to visualize the modern landscape of cyber threats to credit institutions. The conducted research can be useful both for specialists in this field and for regulatory and supervisory authorities of the financial market.

Keywords: cyber risk; cyber risk management; phenomenological modeling; digital economy; cyber stability of a commercial bank; digital banking business

For citation: **Gumerov M.F., Rizvanova I.A., Belova M.T. Cyber resilience of credit institutions in the context of digital banking business development.** ***Finance: Theory and Practice.*** **2025;29(6):148-163. DOI: 10.26794/2587-5671-2025-29-6-148-163**

INTRODUCTION

Digitalization, the main aspects of which were officially announced by the Government of the Russian Federation in 2011,[1] is associated not only with a positive effect on the economy in the medium and long term, but also with risks of various natures. By increasing the accessibility and convenience of digital financial services and products and reducing their costs, digitalization creates new and exacerbates existing challenges — cyber risks emerge and spread, leading to customer distrust of new technologies and digitalization in general. In this regard, in the context of the new reality, the goal of regulation and supervision in the financial market is trust: "achieving long-term trust in digital technologies is a key factor for the success of the digital transformation of the Russian economy".[2] However, long-term trust in digital technologies is impossible to achieve without a comprehensive analysis of cyber risks, which is what makes this research *relevant*.

Digital banking business is inherently derived from the traditional form of banking operation and is characterized by specific types of risks, particularly cyber risks. In turn, these risks are not fundamentally new in nature. They are a modification of the risk landscape, which is also relevant for traditional banking. Nevertheless, the digitalization of the banking sector in some cases increases the relevance of cyber risks and leads to the emergence of fundamentally new types of threats.

It should be noted that in today's reality, issues of cyber risks, cybersecurity, personal data protection, and information ethics are becoming increasingly interconnected. This is also evidenced by the review of domestic and foreign literature that was conducted.

In the paper [1], categories of cyber risks are identified, with significant importance given to the protection of personal data. The presented category is expanded in studies [2–6], which examine the classification of cyber risks based on various criteria in the new digital realities. In study [7], the necessity of cyber exercises, in other words, information ethics, is examined in detail and justified, and a simulation model of a cyber-threat realization scenario is proposed. When considering the development of new financial technologies, the authors of the study [8–10] highlight new types of operational risks. In the paper [11], the problems of cyber threats and cybersecurity are discussed in detail, and a classification of the most relevant cyber threats to the Russian financial system is presented. Key indicators of cyberattacks on institutions of the Russian national financial system are analyzed, and the main scenarios for the development of cyber threats and cyberattacks against the national financial system are identified. The work [12] is practical in nature, as it examines trends in cybercrime and measures to counter cybercrime, but it does not provide clear terminology. In contrast, the authors of the study [13] deeply analyzed the relationship between concepts such as "digitalization", "the challenge of digitalization", "threat", and "cyber risk", defining cyber risk as "the risk of digital information security breach". In turn, the study [14] presents a

[1] Statement of the Government of the Russian Federation and the Central Bank of the Russian Federation dated April 5, 2011, No. 1472-p-P13, 01–001/1280 "On the Strategy for the Development of the Banking Sector of the Russian Federation for the Period up to 2015". URL: http://base.garant.ru/591345/ (accessed on 21.05.2024); "Digital Economy of the Russian Federation" program. URL: http://static.government.ru/media/files/9gFM4FHj4PsB 79I5v7yLVuPgu4bvR 7M0.pdf (accessed on 21.05.2024); Key directions for the development of financial technologies for the period 2018–2020. URL: http://cbr.ru/Content/Document/File/35816/on_2018_2020.pdf (accessed on 21.05.2024); Main directions for the development of the financial market of the Russian Federation for 2023 and the period of 2024 and 2025. URL: onfr_2023–2025.pdf (cbr.ru) (accessed on 21.05.2024).

[2] Main directions for the development of the financial market of the Russian Federation for 2023 and the Period of 2024 and 2025. URL: onfr_2023–2025.pdf (cbr.ru) (accessed on 21.05.2024).

comparative analysis of the organization of the cybersecurity system in Russia and abroad. The authors of the paper [15] presented an analysis of cyber risks, as well as their main types: data leakage, network attacks, and financial fraud.

Summarizing the above, it is important to note that most studies focus on clarifying the conceptual framework. In doing so, the authors aim to take into account as many factors and threats as possible to which banks may be exposed, arguing that cyber risks primarily cause losses for the risk subject. A small number of studies contrast this statement, making the conclusions of the authors of papers [16–18] interesting, as they concluded that cybersecurity (as one of the functions of cyber risk management) is a stimulus for further economic development.

Within the framework of this study, we adhere to the concept formulated by the Bank of Russia, where cyber-risk is included in the group of information security risks, which, in turn, are classified as operational risks. The Regulation of the Bank of Russia No. 716 from 8 April 2020 defines the concept of "cyber risk" as "the risk of intentional actions by credit institution employees and/or third parties using software and/or software and hardware tools aimed at the objects of the credit institution's information infrastructure (the parent credit institution of a banking group) for the purpose of disrupting and/or terminating their functioning and/or creating a threat to the security of information prepared, processed, and stored by such objects, as well as for the purpose of unauthorized appropriation, theft, alteration, deletion of data and other information (data structures, system parameters and characteristics, program code) and violation of access control".[3]

We define cyber resilience as the ability to ensure the functioning of a credit institution during cyberattacks and to successfully counter them.

Let's define the relationship between existing concepts in the field of cybersecurity and present a possible structure for a commercial bank's "cyber ecosystem" in *Fig. 1*. An optimally functioning cyber ecosystem will help identify unsafe areas across the key and target activities of the credit institution, thereby informing management and employees about the possibility of an unacceptable event occurring at the hands of real attackers. Organizations that regularly conduct penetration and other activities within the framework of the entire cyber ecosystem, and take appropriate security measures based on their results, ultimately have more opportunities to reach a higher level of cybersecurity and detect cyberattacks at an early stage — before unacceptable consequences occur.

A crucial factor in the effectiveness of monitoring and responding to cyber incidents is IT infrastructure. Skills in identifying cyberattacks and responding to cyber incidents are honed during cyber exercises, while penetration testing involves external or internal attackers attempting to breach an organization's information systems. Infrastructure hardening is a way to modernize an existing IT landscape to increase the security level of key and target systems without using established information security tools. Cybersecurity encompasses the protection of computer systems, networks, software, and data from cyber threats, including hacking attacks, viruses, and malware, while cyber resilience, in turn, characterizes the ability to ensure the continuity of business processes and IT infrastructure functioning in the event of a real cyberattack.

As the number of internet users grows, cybercriminals have more and more

[3] Regulation of the Bank of Russia from 8 April 2020. No. 716-P "On the Requirements for the Operational Risk Management System in a Credit Institution and a Banking Group". URL: https://base.garant.ru/74279372/ (accessed on 21.05.2024).

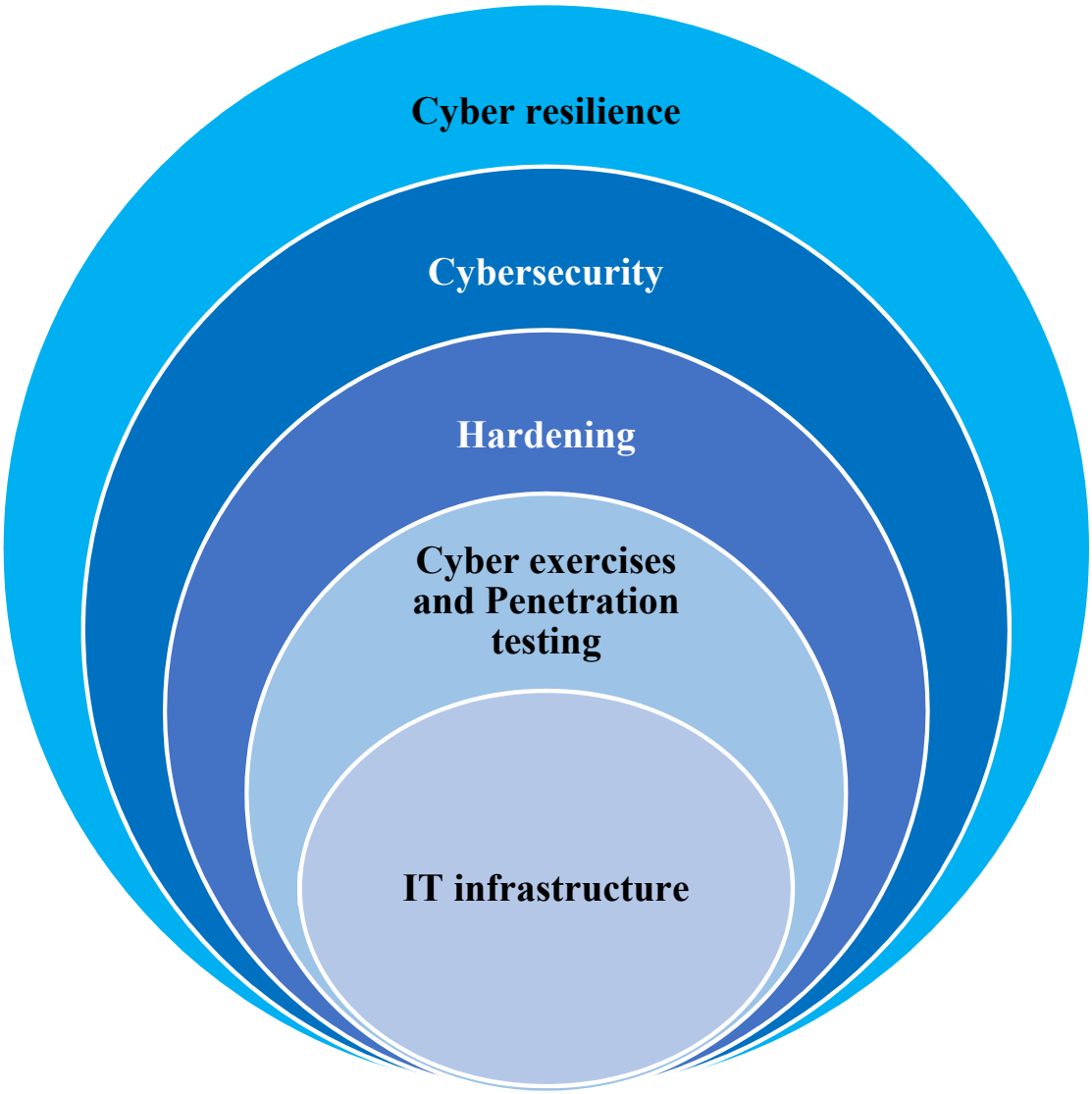

Fig. 1. **Cyber Ecosystem of a Credit Organization**

Source: Compiled by the authors.

opportunities to commit crimes. Financial losses related to cybercrime are expected to rise sharply in the coming years, from $ 9.2 trillion in 2024 to $ 3.8 trillion by 2028.[4] Attackers' methods are becoming increasingly sophisticated, and they have more and more tools at their disposal [19, 20]. A significant surge in cyberattacks occurred during the coronavirus pandemic, when many organizations faced more frequent cyberattacks due to the insecurity of remote work and the shift towards virtualized IT environments.

JUSTIFICATION OF MANAGEMENT DECISIONS IN BUILDING A CYBER ECOSYSTEM IN A COMMERCIAL BANK

The current practice of countering cyber risks is characterized by commercial banks diversifying their investments in resources allocated to building a unified cybersecurity system. Some of the work in this direction is carried out by the bank's own IT services, mainly those related to ensuring its own cybersecurity. As for minimizing cyber threats to customer operations, banks are increasingly outsourcing these services to specialized IT companies. Banks typically enter into contracts with outsourcers for one year, and a key task for bank management here is to correctly calculate and justify the amount

[4] Consumer opinion survey data. URL: https://kolgota.ru/ (accessed on 21.06.2024).

Table 1

Indicators of Resource Exchange and Changes in Resource Exchange Included in the Phenomenological Model of Making a Decision on Cooperation Between a Bank and a Cybersecurity Company

Type of resource exchange Subsystem	P	A	E	I
Object (δ) — the commercial bank under consideration	P_δ: the bank's total cybersecurity costs (TC_{cb}) in the short term (1 year)	A_δ: short-term return on cybersecurity investment ($SR_c = \frac{L_{s.}}{TC_{CB}}$), where L_s — is the sum of losses prevented due to short-term (1 year) investments in cybersecurity	E_δ: weighted average investment period in cybersecurity measures ($\frac{\sum_{i=1}^{k} CM_i * PM}{TC_{CB}}$), where k — is the number of cybersecurity measures in the long term (5 years), CM_i — are the costs of implementing the i-th measure, PM_i — is the implementation period of the i-th measure	I_δ: long-term return on cybersecurity costs ($\frac{LI_c}{TC_{CB}}$), where LI_c — is the long-term income (over a 5-year period) additionally earned by the bank due to investments in cybersecurity
Environmental (α) — a group of banks with relevant financial standing	P_α: total cybersecurity spending in the relevant group of banks in the short term (TC_{RG})	A_α: the average short-term return on cybersecurity spending within the relevant group of banks (SC_{RG})	E_α: weighted average term of cybersecurity contracts within the relevant group of banks (WC_{RG})	I_α: long-term return on investment in cybersecurity costs within a relevant group of banks (LC_{RG})
The connection between the object and environment subsystems	***P_δ / P_α: the share of the bank under consideration's spending on cybersecurity as a percentage of similar spending by a relevant group of banks***	***A_δ / A_α: the relative return on investment in cybersecurity for the bank in question within the relevant group***	***E_δ / E_α: the position of the bank in question within the relevant group in terms of the timing of investments in cybersecurity measures***	***I_δ / I_α: the bank's position in the relevant group regarding the long-term return on cybersecurity costs***
Project (γ) — IT outsourcing company	P_γ: the currency of the outsourcing company's balance sheet (CC_O)	A_γ: the costs incurred by the outsourcing company to create technologies to counter cyber threats (C_O)	E_γ: the average term of the outsourcing company's contracts with counterparties supplying resources to support operations over the past 5 years (AC_O)	I_γ: the average total currency of the outsourcing company's client balance over 5 years (ACC_O)

Table 1 (continued)

Type of resource exchange Subsystem	P	A	E	I
Process (β) — the outsourcing company's business in other areas	P_β: the total value of the outsourcing company's contracts with all clients in the short term (TV_S)	A_β: the sum of prevented losses from cyber threats to the outsourcing company's clients in the short term (PL_S)	E_β: the weighted average term of the outsourcing company's contracts with clients ($\frac{\sum_{i=1}^{m} CA_i * CT_i}{TC_S}$), where m — is the number of the outsourcing company's contracts with clients in the long term (5 years), CA_i — is the contract amount with the i-th client, CT_i — is the contract term with the i-th client	I_β: average additional income earned by the outsourcing company's clients over the past 5 years through the use of its services. (AI_{OC})
The connection between the project and process subsystems	***P_γ / P_β: the efficiency of using the funds received by the outsourcing company under contracts from clients***	***A_γ / A_β: return on investment for the outsourcing company's expenditure on creating cybersecurity technologies***	***E_γ / E_β: alignment of the outsourcing company's contract terms with clients and suppliers***	***I_γ / I_β: the share of the company's customer revenue from using services in their total value***
Resource exchange change indicator	$P_{ed.}$: the contract amount of the bank in question with the outsourcing company (***CA***)	$A_{ed.}$: the expected amount of losses prevented thanks to the contract with the outsourcing company (***ELP***)	$E_{ed.}$: contract term (***CT***)	$I_{ed.}$: the expected long-term revenue earned by the bank through the contract with the outsourcing company (***LR***)

Source: Compiled by the authors.

of services fixed in the contract for the next year. Because, on the one hand, this amount should be adequate to the volume and nature of the work performed by the outsourcer, considering the current situation in the market for cybersecurity services, and at the same time, unreasonably large amounts of financial resources that could generate a greater economic effect if used in other areas of banking business should not be spent within this direction. But a management decision of this kind is made in conditions of high turbulence: the fight against cyber risks is developing very rapidly, both in terms of the technologies offered by IT companies and in relation to customer needs in the face of new types of cyber threats.

Justifying managerial decisions in economic systems with a high level of turbulence and insufficient information about their functioning mechanisms requires specific tools.

Table 2

The Values of Resource Exchange Indicators in the Simulated Economic System in the Periods Preceding the Preparation of a New Contract

Indicator	Dimension	Sources of information for the calculation	Evaluation period	Meaning
The bank's total cybersecurity costs (TC_{CB}) in the short term (1 year)	Billion rubles	Bank reporting	2023	59.19
Short-term return on cybersecurity spending (SR_C)	%		2023	17.61
Weighted average investment period in cybersecurity measures	Month		2019–2023	30
Long-term return on cybersecurity investment ($\frac{LI_C}{TC_{CB}}$)	%		2019–2023	120.52
Total cybersecurity spending in the relevant group of banks in the short term (TC_{RG})	Billion rubles	External publicly available information resources about banks and their relevant group	2023	24700. 20
The average short-term return on cybersecurity spending within the relevant group of banks (SC_{RG})	%		2023	7.70
Weighted average term of cybersecurity contracts within the relevant group of banks (WC_{RG})	Month		2019–2023	41
Long-term return on cybersecurity costs within a relevant group of banks (LC_{RG})	%		2019–2023	103.12

Table 2 (continued)

Indicator	Dimension	Sources of information for the calculation	Evaluation period	Meaning
The balance sheet currency of the outsourcing company (CC_0)	Billion rubles	Reporting from the outsourcing company, external publicly available information resources about the current corporate clients of the outsourcing company in question	2023	3.34
The costs incurred by the outsourcing company for creating cybersecurity technologies (C_0)	Billion rubles		2023	0.10
The average term of contracts between the outsourcing company and its counterparties supplying resources to support its operations over the past 5 years (AC_0)	Month		2019–2023	18
The average total currency of the outsourcing company's client balance over 5 years (ACC_0)	Billion rubles		2019–2023	0.94
The total value of the outsourcing company's contracts with all clients in the short term (TC_S)	Billion rubles		2023	1.52
The sum of prevented losses from cyber threats to the outsourcing company's clients in the short term (PL_S)	Billion rubles		2023	0.07
Weighted average term of the outsourcing company's contracts with clients	Month		2019–2023	12
The average additional income earned by the outsourcing company's clients over the past 5 years through the use of its services (AI_{OC})	Billion rubles		2019–2023	0.59

Source: Compiled by the authors according to SPARK. URL: http: www.spark-interfax.ru (accessed on 23.05.2024).

Table 3

The Values of Resource Exchange Indicators in the Simulated Economic System, Projected for 2023, Provided that There is no New Concluded Contract Between Delta Bank and Gamma IT Company

Type of resource exchange Subsystem	P	A	E	I
Environment (α)	TC_{RG} = 30053 billion rubles	SC_{RG} = 15%	WC_{RG} = 42 month	LC_{RG} = 70
Object (δ)	TC_{CB} = 52 billion rubles	$SR_C = \frac{L_S}{TC_{CB}} = \frac{4*2\ billion\,rub.}{52\ billion\,rub.}$	$\frac{\sum_{i=1}^{k} CM_i * PM_i}{TC_{CB}} = \frac{1734(billion\,rub.*month)}{52(billion\,rub.)}$	$\frac{LI_C}{TC_{CB}} = \frac{56.16}{52}$
Project (y)	Ao = 4 billion rubles	i = 0.1 billion rubles	AC_O = 15 month	ACC_O = 0.91 billion rubles
Process (β)	TS_S = 1.3 billion rubles	PL_S = 0.06 billion rubles	$\frac{\sum_{i=1}^{m} CA_i * CT_i}{TC_S} = \frac{6.9(billion\,rub.*month)}{1.3\,billion\,rub.}$	AI_{OC} = 0.47 billion rubles

Source: Compiled by the authors.

In the paper [21], phenomenological models are proposed to justify decisions in the management process in economic systems of this type, and their construction methodology, initially developed within the natural and technical disciplines, is adapted to the specific features of the functioning of economic systems.

A phenomenological model of the system shows how changes in some indicators affect others. It describes how the system responds to various impacts. In this model, it's not necessary to explain the reaction mechanisms in detail. It task is to show the quantitative characteristics of these reactions. This helps the manager make decisions about how to influence the system to achieve goals.

In the papers [22–28], phenomenological models are proposed for making managerial decisions in individual areas of economic activity. In study [21], a generalized

approach to the phenomenological modelling of economic systems as control objects is developed, within which their elements are grouped based on two characteristics.

The first characteristic is the influence of the initial information about them on the new knowledge synthesized by the thinking of decision-makers. In this case, the peculiarities of how these individuals perceive different types of information are considered within the framework of D. Kahneman and A. Tversky's behavioral management theory [29], and the result here is the grouping of elements of the modelled economic system into 4 subsystems, as identified in systems management theory [30, 31]. Only within the framework of the proposed approach are subsystems distinguished by boundaries not in physical space and time, but in information space. The object subsystem (δ) includes elements whose information is used for and directly influences a series of management decisions. Information about the environmental subsystem (α) is also used in a series of management decisions, but it influences them indirectly through information about the object subsystem. The project subsystem (γ) is the set of elements whose information is used only for the current decision and directly influences it. The process subsystem (β) is related to information that only affects the current decision, but indirectly through the design subsystem.

The second characteristic is the changes that the management decision causes in the processes of resource exchange between the elements of the four identified subsystems. Resource exchange processes within subsystems are also divided into 4 types from the perspective of which basic organizational management functions initiate them, according to I. Adizes [32]. Specifically, within the proposed approach, the Adizes function "Producing" (P) is considered as initiating the primary transfer of resources between elements in the short term, while "Administering" (A) is seen as their reciprocal return of resources to each other, also in the short term. The "Entrepreneurship" (E) and "Integration" (I) functions ensure the system elements' ability to maintain their capacity for these actions in the long term.

Thus, the phenomenological model for managerial decision-making in an economic system establishes a connection between the values of 16 resource exchange indicators within it before the decision is made (4 resource exchanges in 4 subsystems) and their values, which change as a result of the decision. The economic content of these indicators in relation to the decision-making situation regarding the parameters of the bank's interaction with the cybersecurity company is presented in *Table 1*.

Let's consider an algorithm for the practical application of the resource exchange indicators discussed. Let's assume that commercial bank "Delta" plans to sign a contract with IT company "Gamma" at the beginning of 2025, under which the latter, as an outsourcer, will ensure the protection of the bank's customers' transactions from potential cyber threats. The purchasing department has been given tasks:

1. Determine the two main contract parameters — the total amount (CA) and the term (CT) — in such a way that they take into account four groups of factors: the current state of the cyber threat countermeasure system within Delta Bank itself, the state of similar systems in banks with a similar financial and economic condition to the one under consideration (the relevant group), the financial and economic condition of the outsourcing company, and its performance indicators with existing clients;

2. Assess the potential benefits a bank could gain from collaborating with this IT-company: the size of expected losses prevented (ELP) and the additional revenue

the bank could generate from entering into a contract with the IT company by increasing the resilience of customer transactions to cyber threats.

To build a phenomenological model of the described situation, the values of the indicators from *Table 1* were calculated for the period preceding the preparation of the new contract. The obtained values are summarized in *Table 2*, which also indicates the time intervals for assessing the indicators and the sources of information for their calculation.

Using special forecasting methods (extrapolation), the projected values for the indicators from *Table 2* for 2025 were obtained (assuming no new contract is concluded between Delta Bank and Gamma IT company). Forecast values for 2025 are summarised in *Table 3*.

In the paper [20], a general view of a phenomenological model of an economic system is presented, designed to generate a management decision within it under conditions of high system development turbulence and incomplete knowledge of the patterns of this development. Based on this general model, this paper proposes a specific form of this model for making a decision on the parameters of cooperation between a commercial bank and an IT company, ensuring the cybersecurity of customer banking operations.

$$\left(\begin{array}{c} \left[\frac{TC_{CB} + \boxed{CA}}{TC_{RG}} + \frac{CC_O}{TC_S + \boxed{CA}} \right] = \\ = \left[\frac{TC_{CB}}{TC_{RG}} + \frac{CC_0}{TC_S} \right] \\ \left[\frac{L_S + \boxed{ELP}}{\frac{TC_{CB} + \boxed{CA}}{SC_{RG}}} + \frac{PL_S + \boxed{ELP}}{C_O} \right] = \\ = \frac{\left[\frac{\sum CM * PM + \boxed{CA} * \boxed{CT}}{TC_{CB} + \boxed{CA}} \right]}{WC_{RG}} + \frac{\left[\frac{\sum CA * CT + \boxed{CA} * \boxed{CT}}{TC_S + \boxed{CA}} \right]}{AC_O} = \\ = \frac{\left[\frac{\sum CM * PM}{TC_{CB}} \right]}{WC_{RG}} + \frac{\left[\frac{\sum CA * CT}{TC_S} \right]}{AC_O} \\ \left[\frac{LI_C + \boxed{AI}}{\frac{TC_{CB} + \boxed{CA}}{LC_{RG}}} + \frac{AI_{OC} + \boxed{AI}}{ACC_O} \right] = \\ = \left[\frac{\frac{LI_C}{TC_{CB}}}{LC_{RG}} + \frac{AI_{OC}}{ACC_O} \right] \end{array} \right)$$

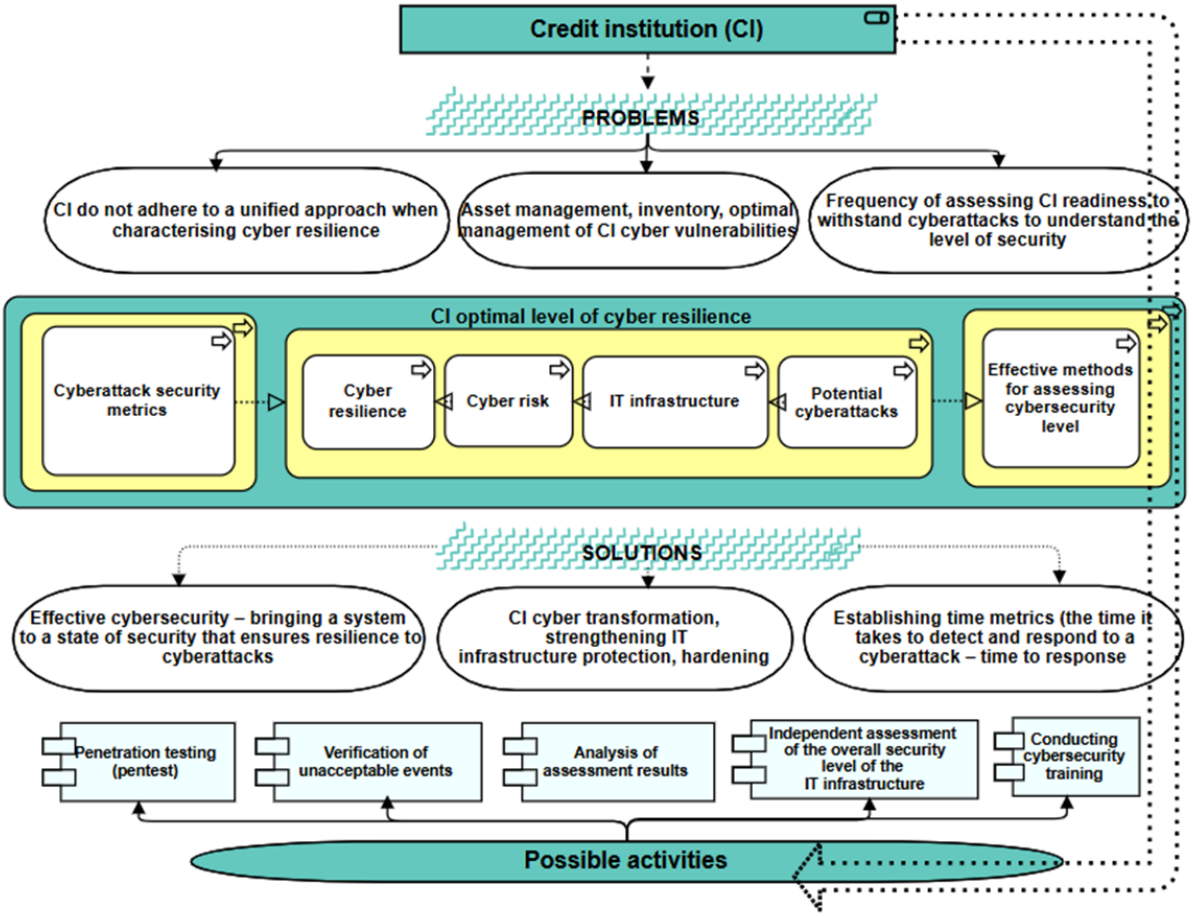

Fig. 2. **A Commercial Bank's Cyberstability Map**

Source: Compiled by the authors.

In this model, the left sides of the equations include the values of resource exchange indicators in the simulated economic system for the period in which the management decision is made (index pr), while the right sides include the values of these same indicators for the preceding period (index p.p.). Substituting the values from *Table 3* into the left sides of the equations and the values from *Table 2* into the right sides, we get:

$$\begin{cases} \left[\frac{52+\boxed{CA}}{30\,053}+\frac{4}{1.3+\boxed{CA}}\right]=\left[\frac{59.19}{24\,700.20}+\frac{3.34}{1.52}\right] \\ \left[\frac{\frac{4*2+\boxed{ELP}}{52+\boxed{CA}}}{15}+\frac{0.06+\boxed{ELP}}{0.10}\right]=\left[\frac{17.61}{7.70}+\frac{0.07}{0.10}\right]= \\ =\frac{\left[\frac{1734\ +\boxed{CA}*\boxed{CT}}{52+\boxed{CA}}\right]}{42}+\frac{\left[\frac{6.9+\boxed{CA}*\boxed{CT}}{1.3+\boxed{CA}}\right]}{15}=\frac{30}{41}+\frac{12}{18} \\ \left[\frac{\frac{56.16+\boxed{LR}}{52+\boxed{CA}}}{70}+\frac{0.47+\boxed{LR}}{0.91}\right]=\left[\frac{120.52}{103.12}+\frac{0.59}{0.94}\right] \end{cases}$$

Solving this system of equations, we get:

$$\boxed{CA} \approx 0.5,\ \boxed{ELP} \approx 0.1,\ \boxed{CT} \approx 13,\ \boxed{LR} \approx 0.2.$$

Thus, based on the calculations performed, it can be stated that if Delta Bank signs a contract with Gamma IT company for cybersecurity services for customer transactions worth 500 million rubles for a period of 1 year, the amount of prevented losses should be 100 million rubles within the next year after the contract is signed, and the additional income within 5 years after the start of cooperation should be 200 million rubles.

The use of phenomenological modelling allowed for the calculation of specific parameters for ensuring the security of client operations during the commercial bank's collaboration with an IT company, as well as the development of a cyber-resilience map (*Fig. 2*), which will help optimize monitoring, timely detection of potential cyberattacks, response to cyber incidents, and priorities tasks for strengthening the credit institution's IT infrastructure.

Further research in this area could focus on considering more complex cases to develop solutions and parameters for collaboration between a commercial bank and several IT companies simultaneously.

CONCLUSION

The paper presents a critical review of domestic and foreign scientific literature on the issues of cyber risks and cybersecurity in the context of the development of digital banking business. The theoretical significance of the study lies in the fact that theoretical pluralism regarding the analyzed concept is considered, and a conceptual apparatus is justified that allows for the study of the functioning, development, and justification of managerial decisions in building a cybersecurity system in a commercial bank: the concept of a "cyber ecosystem" is proposed, the construction of which at the level of a credit institution will help to more optimally identify and minimize the possibility of cyber risk realization in key and target areas of the commercial bank's activities, as well as contribute to the organization's cyber resilience in the context of the development of digital banking. The practical significance of the study lies in the development of applied aspects of systems analysis and practical problem-solving: a model of interaction between a commercial bank and an IT company specializing in providing cybersecurity services has been developed. Based on this model, an algorithm is proposed for justifying the bank's management decisions regarding the allocation of funds for cybersecurity. The use of phenomenological modelling within this study allowed for the formal calculation of specific parameters of cooperation between a commercial bank and an IT company that ensures the security of customer transactions. Building a cyber-resilience map for a commercial bank allowed for the visualization of the cyber threat landscape and justified the need for continuous improvement of forms and methods for ensuring cybersecurity at the level of credit institutions.

REFERENCES

1. Shvyrov V.V., Hvozdiukova S.N. Cyberspace risk categories: Nature of loss and business sectors. *Vestnik Luganskogo gosudarstvennogo pedagogicheskogo universiteta. Seriya 5. Gumanitarnye nauki. Tekhnicheskie nauki*. 2022;(2):96–104. (In Russ.).
2. Larina O.I., Moryzhenkova N.V. On the development of the cyber risk identification methodology. *Bankovskoe delo = Banking*. 2023;(1):66–71. (In Russ.).
3. Amosova N.A., Rudakova O.S. Financial stability in financial markets: Identification of leadership and sources of risk generation. Moscow: KnoRus; 2025. 240 p. (In Russ.).

4. Larionova I. V. Competition in the financial services market of Bigtech companies and Big Banks. Regulatory issues, risks, and financial stability. *Bankovskie uslugi = Banking services*. 2025;(3):12–18. (In Russ.). DOI: 10.36992/2075–1915_2025_3_12
5. Larionova I. V. New approaches to financial market regulation in conditions of increasing risks of uncertainty of economic development with the introduction of sanctions restrictions. Moscow: KnoRus; 2024. 190 p. (In Russ.).
6. Larionova I. V., Ustinov D. A. Implementation of the borrower's internal credit ratings into the credit risk assessment system. *Finansy, den'gi, investitsii = Finances, Money, Investments*. 2024;(4):30–37. DOI: 10.36992/2222–0917_2024_4_30
7. Metel'kov A. N. Cyber exercises: foreign experience in protecting critical infrastructure. *Pravovaya informatika = Legal Informatics*. 2022;(1):51–60. (In Russ.). DOI: 10.21681/1994–1404–2022–1–51–60
8. Vasiliev S. A., Nikonova I. A., Miroshnichenko O. S. Banks, information platforms and big data: Development trends and regulatory directions. *Finansovyi zhurnal = Financial Journal*. 2022;14(5):105–119. (In Russ.). DOI: 10.31107/2075–1990–2022–5–105–119
9. Dyudikova E. I., Rizvanova I. A. DeFi risk profile as an indicator of a crisis of confidence. *Innovatsii i investitsii = Innovation & Investment*. 2025;(5):632–637. (In Russ.).
10. Rizvanova I. A. Identification and control of risks in the payment system: Russian and foreign experience. *Vestnik universiteta (Gosudarstvennyi universitet upravleniya)*. 2024;(9):203–212. (In Russ.). DOI: 10.26425/1816–4277–2024–9–203–212
11. Shkodinsky S. V., Dudin M. N., Usmanov D. I. Analysis and assessment of cyberthreats to the national financial system of Russia in the digital economy. *Finansovyi zhurnal = Financial Journal*. 2021;13(3):38–53. (In Russ.). DOI: 10.31107/2075–1990–2021–3–38–53
12. Antonian E. A., Kleshchina E. N. Cybercrime at the present stage: Trends and directions of counteraction. *Vestnik ekonomicheskoi bezopasnosti = Vestnik of Economic Security*. 2022;(5):11–15. (In Russ.). DOI: 10.24412/2414–3995–2022–5–11–15
13. Khalin V. G., Chernova G. V. Digitalization and cyber risks. *Upravlencheskoe konsul'tirovanie = Administrative Consulting*. 2023;(7):28–41. (In Russ.). DOI: 10.22394/1726–1139–2023–7–28–41
14. Dudin M. N., Shkodinsky S. V. Challenges and threats of the digital economy to the sustainability of the national banking system. *Finance: Theory and Practice*. 2022;26(6):52–71. DOI: 10.26794/2587–5671–2022–26–6–52–71
15. Cheng S., Li J., Luo, L., Zhu Y. Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters*. 2024;65:105533. DOI: 10.1016/j.frl.2024.105533
16. AlGhamdi S., Than W. K., Vlahu-Gjorgievska E. Information security governance challenges and critical success factors: Systematic review. *Computers & Security*. 2020;99:102030. DOI: 10.1016/j.cose.2020.102030
17. Norbekov J. Ensuring information security as an ideological problem. *Mental Enlightenment: Scientific-Methodological Journal*. 2020;(1):56–65. URL: https://mentaljournal-jspu.uz/index.php/mesmj/article/view/9/8
18. Belova M. T. Practical issues of improving the policy of the bank of Russia in the field of protecting the rights of consumers of financial services. *Innovatsionnoe razvitie ekonomiki = Innovative Development of Economy*. 2022;(3–4):197–204. (In Russ.). DOI: 10.51832/2223798420223–4197
19. Belova M. T., Shilov I. S. Prospects of banking business development in the context of digital transformation of the financial system. *Finansovye rynki i banki = Financial Markets and Banks*. 2023;(12):79–87. (In Russ.).
20. Gumerov M., Salutina T., Platunina G., Sharavova O., Boychenko I. Emergent decision-making in business-processes management. In: Managerial sciences in the modern world: Proc. 9th Int. sci.-pract. conf. Geneva: Eurasian Scientific Editions SA; 2022:103–108. URL: https://scispace.com/pdf/ix-international-scientific-practical-conference-managerial-3ejt5k3s.pdf

21. Priven A., Kynin A. A phenomenological model of parameter growth in engineering systems. *International Journal of Systematic Innovation*. 2012;2(2):9–23. DOI: 10.6977/IJoSI.201209_2(2).0002
22. Ianenko M. B., Badalov L. A., Rovensky Y. A., Bunich G. A., Gerasimova E. B. Essence, risks and control of uncertainties in the process of making investment decisions. *Espacios*. 2018;39(31). DOI: 10.12816/0002259
23. Maergoiz L. S., Khlebopros R. G. The indicator of "happiness" in the resource-based economy: An extreme approach. *Journal of Siberian Federal University. Humanities and Social Sciences*. 2016;9(8):1739–1745. DOI: 10.17516/1997–1370–2016–9–8–1739–1745
24. Semenychev V. K., Kurkin E. I., Semenychev E. V., Danilova A. A. Multi-model forecasting of non-renewable resources production. *Energy*. 2017;130:448–460. DOI: 10.1016/j.energy.2017.04.098
25. Brovkina N. E., Rizvanova I. A. Transactional banking business. Moscow: KnoRus; 2022. 212 p. (In Russ.).
26. Gumerov M. F., Rizvanova I. A. Credit risks of Russian commercial banks: New approaches to management. *Finance: Theory and Practice*. 2023;27(2):64–75. DOI: 10.26794/2587–5671–2023–27–2–64–75
27. Tyukin I. Y., Gorban A. N., Sofeykov K. I., Romanenko I. Knowledge transfer between artificial intelligence systems. *Frontiers in Neurorobotics*. 2018;12:1–16. DOI: 10.3389/fnbot.2018.00049
28. Kahneman D., Tversky A. Conflict resolution: A cognitive perspective. In: Choices, values, and frames. Cambridge: Cambridge University Press; 2000:473–488.
29. Kleiner G. B., Karpinskaya V. A. Transition of firms from the traditional to ecosystem form of business: The factor of transaction costs. In: Inshakova A., Inshakova E., eds. Competitive Russia: Foresight model of economic and legal development in the digital age (CRFMELD 2019). Cham: Springer; 2020:3–14. (Lecture Notes in Networks and Systems. Vol. 110). DOI: 10.1007/978–3–030–45913–0_1
30. Kornai J. The system paradigm revisited: Clarification and additions in the light of experiences in the post-socialist region. *Revue d'Etudes Comparatives Est-Ouest*. 2017;48(1–2):239–296.
31. Adizes I., Čudanov M., Rodic D. Timing of proactive organizational consulting: Difference between organizational perception and behavior. *Amfiteatru Economic*. 2017;19(44):232–248.

ABOUT THE AUTHORS

Marat F. Gumerov — Dr. Sci. (Econ.), Senior Researcher at the Laboratory of Macroeconomic Analysis and Modeling, Central Economic and Mathematical Institute of the Russian Academy of Sciences, Moscow, Russian Federation
https://orcid.org/0000-0002-6886-0192
m.f.gumerov.kki@mail.ru

Irina A. Rizvanova — Cand. Sci. (Econ.), Assoc. Prof., Department of Banking and Monetary Regulation of the Faculty of Finance, Senior Researcher at the Institute of Financial Studies of the Faculty of Finance, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0000-0001-9238-0247
Corresponding author:
iarizvanova@ya.ru

Marianna N. Belova — Cand. Sci. (Econ.), Assoc. Prof., Department of Banking and Monetary Regulation of the Faculty of Finance, Researcher at the Institute of Financial Studies of the Faculty of Finance, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0000-0001-6505-8607
mtbelova@fa.ru

Authors' declared contribution:
M. F. Gumerov — scientific guidance; collecting data and evidence; conducting critical analysis of materials; drawing conclusions; writing the text of the article.
I. A. Rizvanova — development of methodology; collection of data and evidence; writing the text of the article.
M. T. Belova — methodology development; collection of data and evidence; writing the text of the article.

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

The article was submitted on 30.09.2024; revised on 29.10.2024 and accepted for publication on 22.02.2025.
The authors read and approved the final version of the manuscript.

Translated by V.I. Timonina