ОРИГИНАЛЬНАЯ СТАТЬЯ

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

Киберустойчивость кредитных организаций в условиях развития цифрового банковского бизнеса

М.Ф. Гумеров[a], И.А. Ризванова[b], М.Т. Белова[c]
[a] Центральный экономико-математический институт Российской академии наук, Москва, Российская Федерация;
[b, c] Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

АННОТАЦИЯ

Развитие цифрового банковского бизнеса и переход от офлайн-взаимодействия к онлайн-формату в современных условиях побуждает более внимательно относиться к генерации киберрисков в банковской сфере. **Цель** исследования состоит в развитии теоретических и практических основ обеспечения киберустойчивости кредитных организаций в условиях развития цифрового банковского бизнеса**. Задачами** исследования явились: изучение понятийного аппарата киберсферы кредитных организаций; обоснование управленческих решений для построения системы кибербезопасности в коммерческом банке; оценка параметров обеспечения безопасности клиентских операций в процессе сотрудничества коммерческого банка и IT-компании. **Научная новизна** исследования заключается в обосновании управленческих решений в экономической системе с высоким уровнем турбулентности и недостаточным объемом информации о механизмах их функционирования с применением специфического инструментария в виде модели феноменологического типа, описывающей меры реагирования системы на различные воздействия. В процессе исследования использован диалектический **метод**, раскрывающий возможности исследования вопросов киберрисков в условиях геополитической нестабильности, взаимосвязи и взаимообусловленности, а также такие общенаучные методы и приемы, как научная абстракция, анализ и синтез, методы группировки и сравнения. Процесс исследования киберрисков в условиях развития цифрового банковского бизнеса рассмотрен через призму общих закономерностей банковской деятельности, взаимосвязи и единства теории и практики, также авторы применили ряд эмпирических методов исследования. Представлен критический обзор отечественной и зарубежной научной литературы по вопросам киберрисков и кибербезопасности и предложено новое понятие «киберэкосистема». Разработана модель взаимодействия коммерческого банка с ИТ-компанией, специализирующейся на оказании услуг по противодействию киберрискам, а также предложен алгоритм обоснования управленческих решений банком по выделению средств на киберзащиту. Построена карта киберустойчивости банка, позволившая визуализировать современный ландшафт киберугроз кредитных организаций. Результаты исследования могут быть полезными как для специалистов в данной области, так и для органов регулирования и надзора финансового рынка.

Ключевые слова: киберриск; управление киберриском; феноменологическое моделирование; цифровая экономика; киберустойчивость коммерческого банка; цифровой банковский бизнес

Для цитирования: **Гумеров М.Ф., Ризванова И.А., Белова М.Т. Киберустойчивость кредитных организаций в условиях развития цифрового банковского бизнеса.** ***Финансы: теория и практика.*** **2025;29(6):148-163. DOI: 10.26794/2587-5671-2025-29-6-148-163**

ORIGINAL PAPER

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**

ВВЕДЕНИЕ

Цифровизация, основные аспекты которой официально были заявлены Правительством Российской Федерации в 2011 г.,[1] связана не только с положительным эффектом для экономики в средне- и долгосрочной перспективе, но и с рисками различной природы. Повышая доступность, удобство пользования цифровыми финансовыми услугами и продуктами и уменьшая ее издержки, цифровизация создает новые и усложняет текущие вызовы — появляются и распространяются киберриски, что приводит к недоверию клиентов к новым технологиям и в целом к отдельным аспектам цифровизации. В связи с этим, в условиях новой реальности, целью регулирования и надзора на финансовом рынке является доверие: «достижение долгосрочного доверия к цифровым технологиям является ключевым фактором успеха цифровой трансформации российской экономики»[2]. Однако долгосрочного доверия к цифровым технологиям невозможно достичь без комплексного анализа киберрисков, что и обуславливает *актуальность* данного исследования.

Цифровой банковский бизнес по своей природе является производным от традиционной формы функционирования банков и для него характерны специфические виды рисков, в частности — киберриски. В свою очередь, эти риски не имеют в своей основе принципиально новой природы. Они являются модификацией риск-ландшафта, который актуален и для традиционного банковского дела. Тем не менее цифровизация банковского сектора в ряде случаев повышает актуальность киберрисков и приводит к появлению принципиально новых видов угроз.

Необходимо отметить, что в современной реальности вопросы киберрисков, кибербезопасности, защиты персональных данных и информационной этики становятся все более взаимосвязанными. Об этом свидетельствует и проведенный обзор отечественной и зарубежной литературы.

В работе [1] выделены категории киберрисков, где важное значение отведено защите персональных данных. Представленная категория расширена в исследованиях [2–6], где рассмотрена классификация киберрисков в зависимости от различных критериев в новых цифровых реалиях. В исследовании [7] подробно рассматривается и обосновывается необходимость киберучений, другими словами, информационной этики, предлагается имитационная модель сценария реализации киберугроз. При рассмотрении вопроса о развитии новых финансовых технологий авторы исследования [8–10] выделяют новые виды операционных рисков. В работе [11] подробно рассмотрены проблемы киберугроз и кибербезопасности и представлена классификация наиболее актуальных киберугроз для финансовой системы России, про-

[1] Заявление Правительства РФ и ЦБР от 05.04.2011 № 1472-п-П13, 01–001/1280 «О Стратегии развития банковского сектора Российской Федерации на период до 2015 года». URL: http://base.garant.ru/591345/ (дата обращения: 21.05.2024); Программа «Цифровая экономика Российской Федерации». URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 21.05.2024); Основные направления развития финансовых технологии на период 2018–2020 гг. URL: http://cbr.ru/Content/Document/File/35816/on_2018_2020.pdf (дата обращения: 21.05.2024); Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов. URL: onfr_2023–2025.pdf (cbr.ru) (дата обращения: 21.05.2024).

[2] Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов. URL: onfr_2023–2025.pdf (cbr.ru) (дата обращения: 21.05.2024).

анализированы ключевые показатели кибератак на институты национальной финансовой системы России и определены основные сценарии развития киберугроз и кибератак для национальной финансовой системы. Практический характер носит работа [12], где рассмотрены тенденции киберпреступности и меры противодействия киберпреступлениям, однако не приведена четкая терминология. В противоположность этому авторы работы [13] глубоко проанализировали взаимосвязь таких понятий, как «цифровизация», «вызов цифровизации», «угроза», «киберриск», раскрывая киберриск как «риск нарушения безопасности цифровой информации». В свою очередь, в исследовании [14] представлен компаративный анализ организации системы обеспечения кибербезопасности в России и за рубежом. Авторы работы [15] представили анализ киберрисков, а также их основные виды: утечка данных, сетевые атаки и финансовое мошенничество.

Обобщая вышеизложенное, важно отметить, что в большинстве исследований акцент делается на раскрытие понятийного аппарата. При этом авторы стремятся учесть как можно больше факторов и угроз, которым могут быть подвержены банки, аргументируя это тем, что киберриски в основном несут убытки для субъекта риска. Небольшое количество работ контрастирует с данным утверждением, поэтому интересным представляются выводы авторов работ [16, 17], которые пришли к выводу, что кибербезопасность (как одна из функций управления киберрисками) является стимулом для дальнейшего экономического развития.

В рамках данного исследования мы придерживаемся понятия, сформулированного Банком России, где *кибериск* включается в состав группы рисков информационной безопасности, которые, в свою очередь, отнесены к операционным рискам. В Положении Банка России от 08.04.2020 № 716-П дается определение понятию «кибериск» — «риск преднамеренных действий со стороны работников кредитной организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа»[3]. Киберустойчивость мы определяем как способность к обеспечению функционирования кредитной организации в процессе кибератак и успешному противодействию им.

Определим соотношение существующих понятий в сфере кибербезопасности и представим на *рис. 1* возможный вариант построения «киберэкосистемы» коммерческого банка. Оптимально функционирующая киберэкосистема поможет выявлять небезопасные места по ключевым и целевым направлениям деятельности кредитной организации, тем самым информируя руководство и сотрудников о возможности реализации недопустимого события со стороны реальных злоумышленников. Организации, которые будут регулярно проводить пентесты и другие мероприятия в рамках работы всей киберэкосистемы, принимают соответствующие меры по обеспечению безопасности по их результатам, в итоге имеют больше возможностей по выходу на более высокий уровень киберзащищенности и выявления кибератак на ранних этапах — до наступления недопустимых последствий.

Важным фактором эффективности мониторинга и реагирования на киберинциденты является ИТ-инфраструктура. Отработка навыков по выявлению кибератак и реагированию на киберинциденты происходит в рамках киберучений, а пентест представляет собой тестирование на проникновение внешних или внутренних злоумышленников в информационные системы организации. Усиление защиты инфраструктуры (hardening) — способ модернизации существующего ИТ-ландшафта для повышения уровня защищенности ключевых и целевых систем без использования налаженных средств зашиты информации. Кибербезопасность аккумулирует защиту компьютерных систем, сетей, программ и данных от киберугроз, включая хакерские атаки, вирусы, вредоносное программное обеспечение, а киберустойчивость, таким образом, характеризует способность обеспечить непрерывность бизнес-процессов и функционирование ИТ-инфраструктуры в условиях реальной кибератаки.

По мере роста числа пользователей интернета у киберпреступников появляется все больше возможностей для совершения преступлений. Так, в ближайшие несколько лет ожидается резкий рост финансовых потерь, связанных с киберпреступностью: с 9,2 трлн долл. США в 2024 г. до 13,8 трлн долл. к 2028 г.[4] Методы злоумышленников становятся все более продвинутыми, и в их распоряжении появляется все больше инструментов [18, 19]. Особый скачок в развитии кибератак произошел во время пандемии коронавируса, когда

[3] Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе». URL: https://base.garant.ru/74279372/ (дата обращения: 21.05.2024).

[4] Данные Исследования потребительских мнений. URL: https://kolgota.ru/ (дата обращения: 21.06.2024).

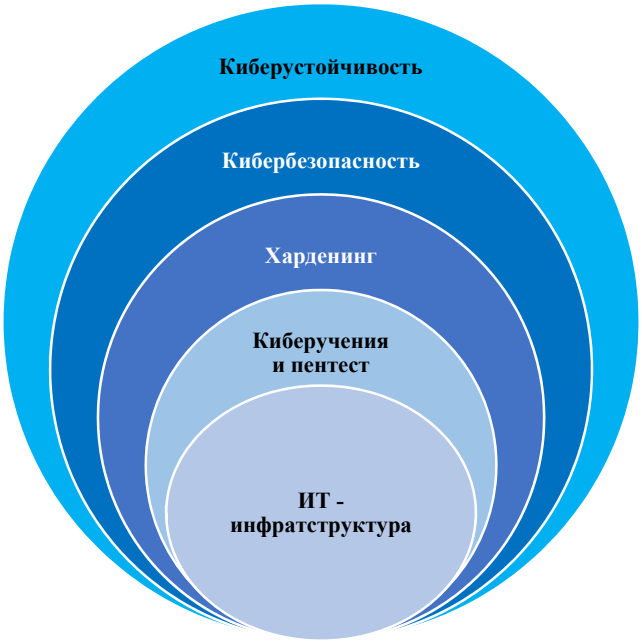

Рис. 1 / Fig. 1. **Киберэкосистема кредитной организации / Cyber Ecosystem of a Credit Organization**

Источник / Source: составлено авторами / Compiled by the authors.

многие организации стали чаще сталкиваться с кибератаками из-за незащищенности удаленной работы, а также перехода к виртуализированным ИТ-средам.

ОБОСНОВАНИЕ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ПРИ ПОСТРОЕНИИ КИБЕРЭКОСИСТЕМЫ В КОММЕРЧЕСКОМ БАНКЕ

Существующая практика противодействия киберрискам-характеризуется тем, что коммерческие банки диверсифицируют вложения своих ресурсов, направляемых на выстраивание единой системы кибербезопасности. Часть работ в данном направлении реализуют IT-службы самого банка, в основном те, что связаны с обеспечением его собственной кибербезопасности. Что же касается минимизации киберугроз для клиентских операций, то эти услуги банки чаще отдают на аутсорсинг специализированным IT-компаниям. Договоры с аутсорсерами банки заключают, как правило, на один год, и здесь важной задачей для менеджмента банка является правильный расчет и обоснование суммы услуг, фиксируемой в договоре на очередной год. Потому что, с одной стороны, эта сумма должна быть адекватной объему и характеру работ, реализуемых аутсорсером с учетом актуальной ситуации на рынке услуг по обеспечению кибербезопасности, и в то же время в рамках данного направления не должны расходоваться необоснованно завышенные объемы денежных ресурсов, которые способны сгенерировать больший экономический эффект при использовании их по другим направлениям банковского бизнеса. Но управленческое решение подобного рода вырабатывается в условиях высокой турбулентности: противодействие киберрискам развивается очень интенсивно как в плане технологий, предлагаемых IT-компаниями, так и относительно потребностей клиентов в условиях возникновения новых видов киберугроз.

Для обоснования управленческих решений в экономических системах с высоким уровнем турбулентности и недостаточным объемом информации о механизмах их функционирования требуется специфический инструментарий.

В работе [20] для обоснования решений в процессе управления в экономических системах подобного рода предложены модели феноменологического типа, а их методика построения, изначально развивавшаяся в рамках естественных и технических дисциплин, адаптирована к особенностям функционирования экономических систем.

Феноменологическая модель системы показывает, как изменения одних показателей влияют на другие. Она описывает, как система реагирует на различные воздействия. В этой модели не нужно детально объяснять механизмы реакций. Ее задача — показать количественные характеристики этих реакций. Это помогает управляющему принимать решения о том, как воздействовать на систему для достижения целей.

В работах [21–27] предлагаются феноменологические модели для выработки управленческих решений в отдельных сферах экономической деятельности. В исследовании [20] разработан обобщенный поход к феноменологическому моделированию экономических систем как объектов управления, в рамках которого их элементы группируются с учетом двух характеристик.

Первая характеристика — влияние исходной информации о них на новое знание, синтезируемое мышлением лиц, принимающих решения. В данном случае учитываются особенности восприятия данными лицами разных видов информации в рамках теории поведенческого менеджмента Д. Канемана и А. Тверски [28], а результатом здесь является группировка элементов моделируемой экономической системы на 4 подсистемы, выделяемые в теории системного менеджмента [29, 30]. Только в рамках предлагаемого подхода подсистемы выделяются границами не в физическом пространстве и времени, а в информационном. Объектная подсистема (δ) включает элементы, информация о которых используется для серии управленческих решений и влияет на них напрямую. Информация о средовой подсистеме (α) также используется в серии управленческих решений, но влияет на них опосредованно через информацию об объектной подсистеме. Проектная подсистема (γ) —

Таблица 1 / Table 1

Показатели ресурсообмена и изменения ресурсообмена, включаемые в состав феноменологической модели выработки решения о сотрудничестве банка с компанией, обеспечивающей кибербезопасность / 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

Вид ресурсообмена / Type of resource exchange Подсистема / Subsystem	P	A	E	I
Объектная (δ) — рассматриваемый коммерческий банк	Pδ: общие затраты банка на обеспечение кибербезопасности (ОЗКБ) в краткосрочном периоде (1 год)	Aδ: краткосрочная отдача от затрат на обеспечение кибербезопасности $(КО_{ОЗ} = \frac{ПП_{Кр.}}{ОЗ_{КБ}})$, где ППКр — сумма потерь, предотвращенных благодаря вложениям в кибербезопасность в краткосрочном периоде (1 год)	Eδ: средневзвешенный срок вложений в мероприятия по обеспечению кибербезопасности $(\frac{\sum_{i=1}^{k} ЗМ_i * СрМ_i}{ОЗ_{КБ}})$, где k — количество мероприятий по обеспечению кибербезопасности в долгосрочном периоде (5 лет), ЗМi — затраты на реализацию i-го мероприятия, СрМi — срок реализации i-го мероприятия	Iδ: долгосрочная рентабельность затрат на кибербезопасность $(\frac{ДД_{ОЗ}}{ОЗ_{КБ}})$, где ДДОЗ — долгосрочный доход (в 5-летнем периоде), дополнительно заработанный банком благодаря вложениям в кибербезопасность
Средовая (α) — группа банков с релевантным финансовым состоянием	Pα: суммарные затраты на обеспечение кибербезопасности в релевантной группе банков в краткосрочном периоде (ОЗРГ)	Aα: средняя в краткосрочном периоде отдача от затрат на обеспечение кибербезопасности в релевантной группе банков (КОРГ)	Eα: средневзвешенный срок контрактов по обеспечению кибербезопасности в релевантной группе банков (ССКРГ)	Iα: долгосрочная рентабельность затрат на кибербезопасность в релевантной группе банков (ДДРГ)
Связь объектной и средовой подсистем	Pδ / Pα: доля затрат рассматриваемого банка на обеспечение кибербезопасности в объеме аналогичных затрат релевантной группы банков	Aδ / Aα: относительная отдача от затрат на обеспечение кибербезопасности рассматриваемого банка в релевантной группе	Eδ / Eα: позиция рассматриваемого банка в релевантной группе по срокам вложений в мероприятия по обеспечению кибербезопасности	Iδ / Iα: позиция рассматриваемого банка в релевантной группе по долгосрочной рентабельности затрат на кибербезопасность

Окончание таблицы 1 / Table 1 (continued)

Вид ресурсообмена / Type of resource exchange Подсистема / Subsystem	P	A	E	I
Проектная (γ) — IT-компания-аутсорсер	Pγ: валюта баланса компании-аутсорсера (ВБКА)	Aγ: затраты компании-аутсорсера на создание технологий противодействия киберугрозам (ЗТКА)	Eγ: средний за 5 лет срок договоров компании-аутсорсера с контрагентами, поставляющими ресурсы для обеспечения деятельности (СДКА)	Iγ: средняя за 5 лет суммарная валюта баланса клиентов компании-аутсорсера (ВБККА)
Процессная (β) — бизнес компании-аутсорсера на других направлениях	Pβ: общая сумма контрактов компании-аутсорсера со всеми клиентами в краткосрочном периоде (СККА)	Aβ: сумма предотвращенных потерь от киберугроз клиентов компании-аутсорсера в краткосрочном периоде (ППКА)	Eβ: средневзвешенный срок контрактов компании-аутсорсера с клиентами $(\frac{\sum_{i=1}^{m} СумК_i * СрК_i}{СК_{КА}})$, где m — количество контрактов компании-аутсорсера с клиентами в долгосрочном периоде (5 лет), СумКi — сумма контракта с i-м клиентом, СрКi — срок контракта с i-м клиентом	Iβ: средний за 5 лет дополнительный доход, заработанный клиентами компании-аутсорсера за счет использования его услуг (ДДККА)
Связь проектной и процессной подсистем	Pγ / Pβ: производительность использования средств, получаемых компанией-аутсорсером по контрактам от клиентов	Aγ / Aβ: отдача от затрат компании-аутсорсера на создание технологий противодействия киберугрозам	Eγ / Eβ: согласованность по срокам договоров компании-аутсорсера с клиентами и с поставщиками	Iγ / Iβ: доля доходов клиентов компании от использования услуг в общем объеме их стоимости
Показатель изменения ресурсообмена	PИзм: сумма контракта рассматриваемого банка с компанией-аутсорсером (СумК)	AИзм: ожидаемая сумма потерь, предотвращенных благодаря контракту с компанией-аутсорсером (ОПП)	EИзм: срок контракта (СрК)	IИзм: ожидаемый долгосрочный доход, дополнительно заработанный банком благодаря контракту с компанией-аутсорсером (ДДК)

Источник / Source: составлено авторами / Compiled by the authors.

это совокупность элементов, информация о которых используется только для текущего решения и влияет на него напрямую. Процессная подсистема (β) связана с информацией, которая влияет только на текущее решение, но опосредовано через проектную подсистему.

Вторая характеристика — это изменения, которые вызывает принимаемое управленческое решение в процессах обмена ресурсами между элементами 4-х выделенных подсистем. Ресурсообменные процессы в подсистемах делятся также на 4 вида с позиции того, какими базовыми функциями организационного управления они инициируются по И. Адизесу [31]. А именно, в рамках предлагаемого подхода адизесовская функция «Производство» (Producing, P) рассматривается

Таблица 2 / Table 2

Значения показателей ресурсообмена в моделируемой экономической системе в периоды, предшествующие моменту подготовки нового контракта / The Values of Resource Exchange Indicators in the Simulated Economic System in the Periods Preceding the Preparation of a New Contract

Показатель / Indicator	Размерность / Dimension	Источники информации для расчета / Sources of information for the calculation	Период оценивания, годы / Evaluation period	Значение / Meaning
Общие затраты банка на обеспечение кибербезопасности (ОЗКБ) в краткосрочном периоде (1 год)	Млрд руб.	Отчетность банка	2023	59,19
Краткосрочная отдача от затрат на обеспечение кибербезопасности ($КО_{ОЗ}$)	%		2023	17,61
Средневзвешенный срок вложений в мероприятия по обеспечению кибербезопасности	Месяцы		2019–2023	30
Долгосрочная рентабельность затрат на кибербезопасность $(\frac{ДД_{ОЗ}}{ОЗ_{КБ}})$,	%		2019–2023	120,52
Суммарные затраты на обеспечение кибербезопасности в релевантной группе банков в краткосрочном периоде (ОЗРГ)	Млрд руб.	Внешние доступные информационные ресурсы о банках их релевантной группы	2023	24 700, 20
Средняя в краткосрочном периоде отдача от затрат на обеспечение кибербезопасности в релевантной группе банков (КОРГ)	%		2023	7,70
Средневзвешенный срок контрактов по обеспечению кибербезопасности в релевантной группе банков (ССКРГ)	Месяцы		2019–2023	41
Долгосрочная рентабельность затрат на кибербезопасность в релевантной группе банков (ДДРГ)	%		2019–2023	103,12

Окончание таблицы 2 / Table 2 (continued)

Показатель / Indicator	Размерность / Dimension	Источники информации для расчета / Sources of information for the calculation	Период оценивания, годы / Evaluation period	Значение / Meaning
Валюта баланса компании-аутсорсера (ВБКА)	Млрд руб.	Отчетность компании-аутсорсера, внешние доступные информационные ресурсы о действующих корпоративных клиентах рассматриваемого аутсорсера	2023	3,34
Затраты компании-аутсорсера на создание технологий противодействия киберугрозам (ЗТКА)	Млрд руб.		2023	0,10
Средний за 5 лет срок договоров компании-аутсорсера с контрагентами, поставляющими ресурсы для обеспечения деятельности (СДКА)	Месяцы		2019–2023	18
Средняя за 5 лет суммарная валюта баланса клиентов компании-аутсорсера (ВБККА)	Млрд руб.		2019–2023	0,94
Общая сумма контрактов компании-аутсорсера со всеми клиентами в краткосрочном периоде (СККА)	Млрд руб.		2023	1,52
Сумма предотвращенных потерь от киберугроз клиентов компании-аутсорсера в краткосрочном периоде (ППКА)	Млрд руб.		2023	0,07
Средневзвешенный срок контрактов компании-аутсорсера с клиентами	Месяцы		2019–2023	12
Средний за 5 лет дополнительный доход, заработанный клиентами компании-аутсорсера за счет использования его услуг (ДДККА)	Млрд руб.		2019–2023	0,59

Источник / Source: составлено авторами по данным СПАРК / Compiled by the authors according to SPARK. URL: http: www.spark-interfax.ru (дата обращения: 23.05.2024) / (accessed on 23.05.2024).

Таблица 3 / Table 3

Значения показателей ресурсообмена в моделируемой экономической системе, спрогнозированные на 2024 г. при условии отсутствия нового заключенного контракта между банком «Дельта» и IT-компанией «Гамма» / 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

Вид ресурсо обмена / Type of resource exchange Подсистема / Subsystem	P	A	E	I
Среда (α) / Environment (α)	$ОЗ_{РГ}$ (пр) = 30 053 млрд руб.	$КО_{РГ}$ (пр) = 15%	$ССК_{РГ}$ (пр) = 42 мес.	$ДД_{РГ}$ (пр) = 70
Объект (δ) / Object (δ)	$ОЗ_{КБ}$ (пр) = = 52 млрд руб.	$КО_{ОЗ} = \frac{ПП_{Кр.}}{ОЗ_{КБ}} = \frac{4*2\,млрд\,руб.}{52\,млрд\,руб.}$	$\frac{\sum_{i=1}^{k} ЗМ_i * СрМ_i}{ОЗ_{КБ}} = \frac{1734(млрд\,руб.*мес.)}{52(млрд\,руб.)}$	$\frac{ДД_{ОЗ}}{ОЗ_{КБ}}$ (пр) = $\frac{56,16}{52}$
Проектная (γ) / Design (γ)	$ВБ_{КА}$ (пр) = = 4 млрд руб.	$ЗТ_{КА}$ (пр) = = 0,1 млрд руб.	$СД_{КА}$ (пр) = 15 мес.	$ВБК_{КА}$ (пр) = = 0,91 млрд руб.
Процессная (β) / Process (β)	$СК_{КА}$ (пр) = 1,3 млрд руб.	$ПП_{КА}$ (пр) = = 0,06 млрд руб.	$\frac{\sum_{i=1}^{m} СумК_i * СрК_i}{СК_{КА}} = \frac{6,9(млрд\,руб.*мес.)}{1,3\,млрд\,руб.}$	$ДДК_{КА}$ (пр) = = 0,47 млрд руб.

Источник / Source: составлено авторами / Compiled by the authors.

как инициирующая первичную передачу элементами ресурсов друг другу на краткосрочном интервале времени, «Администрирование» (A) — ответную отдачу ими ресурсов друг другу также в краткосрочном периоде. Функции «Предпринимательство» (Entrepreneur, E) и «Интеграция» (I) обеспечивают способности элементов системы сохранять способности к этим же действиям в долгосрочной перспективе.

Таким образом феноменологическая модель для принятия управленческого решения в экономической системе устанавливает связь между значениями 16 показателей ресурсообмена в ней до принятия решения (4 ресурсообмена в 4-х подсистемах) и их же значениями, изменяющимися в результате решения. Экономическое содержание этих показателей применительно к ситуации с выработкой решения о параметрах взаимодействия банка с компанией, обеспечивающей кибербезопасность, представлено в *табл. 1*.

Рассмотрим алгоритм практического применения рассмотренных показателей ресурсообмена. Допустим, что коммерческий банк «Дельта» в начале 2025 г. планирует заключить контракт с IT-компанией «Гамма», в рамках которого она в качестве аутсорсера будет обеспечивать защиту операций клиентов банка от возможных киберугроз. Перед отделом закупок поставлены задачи:

1. Определить два основных параметра контракта — общую сумму (СумК) и срок (СрК) таким образом, чтобы они учитывали четыре группы факторов: текущее состояние системы противодействия киберугрозам в самом банке «Дельта», состояние аналогичных систем в банках, схожих по финансово-экономическому состоянию с рассматриваемым (релевантная группа), финансово-экономическое состояние компании-аутсорсера и показатели его работы с действующими клиентами.

2. Оценить потенциальную возможность получения выгоды банком от сотрудничества с данной IT-компанией: размер ожидаемых предотвращенных потерь (ОПП) и дополнительный доход, который банк может получить от заключения контракта с IT-компанией за счет повышения сопротивления киберугрозам клиентских операций.

Для построения феноменологической модели описанной ситуации были рассчитаны значения показателей из *табл. 1* для периода, предшествующего моменту подготовки нового контракта. Полученные значения сведены в *табл. 2*, где также указаны временные интервалы оценки показателей и источники информации для их расчета.

С помощью специальных прогностических методов (экстраполяции) получены прогнозные значения показателей из *табл. 2* на 2025 г. (при условии отсутствия нового заключенного контракта между банком «Дельта» и IT-компанией «Гамма»). Прогнозные значения на 2025 г. сведены в *табл. 3*.

В работе [20] представлен общий вид феноменологической модели экономической системы, предназначенной для выработки в ней управленческого решения в условиях высокой турбулентности развития системы и неполноты знаний о закономерностях этого развития. На основе этой модели общего вида в настоящей работе предлагается частный вид этой модели для выработки решения о параметрах сотрудничества коммерческого банка с IT-компанией, обеспечивающий кибербезопасность банковских операций клиентов.

$$
\left\{
\begin{array}{c}
\left[\dfrac{\text{ОЗ}_{\text{КБ}}(\text{пр})+\boxed{\text{СумК}}}{\text{ОЗ}_{\text{РГ}}(\text{пр})}+\dfrac{\text{ВБ}_{\text{КА}}(\text{пр})}{\text{СК}_{\text{КА}}(\text{пр})+\boxed{\text{СумК}}}\right]=
\left[\dfrac{\text{ОЗ}_{\text{КБ}}(\text{п.п.})}{\text{ОЗ}_{\text{РГ}}(\text{п.п.})}+\dfrac{\text{ВБ}_{\text{КА}}(\text{п.п.})}{\text{СК}_{\text{КА}}(\text{п.п.})}\right]
\\
\left[\dfrac{\dfrac{\text{ПП}_{\text{Кр}}(\text{пр})+\boxed{\text{ОПП}}}{\text{ОЗ}_{\text{БК}}(\text{пр})+\boxed{\text{СумК}}}}{\text{КО}_{\text{РГ}}(\text{пр})}+\dfrac{\text{ПП}_{\text{КА}}(\text{пр})+\boxed{\text{ОПП}}}{\text{ЗТ}_{\text{КА}}(\text{пр})}\right]=
\left[\dfrac{\dfrac{\text{ПП}_{\text{Кр}}(\text{п.п.})}{\text{ОЗ}_{\text{БК}}(\text{п.п.})}}{\text{КО}_{\text{РГ}}(\text{п.п.})}+\dfrac{\text{ПП}_{\text{КА}}(\text{п.п.})}{\text{ЗТ}_{\text{КА}}(\text{п.п.})}\right]=
\\
\dfrac{\left[\dfrac{\sum \text{ЗМ*СрМ}\ (\text{пр})+\boxed{\text{СумК}}*\boxed{\text{СрК}}}{\text{ОЗ}_{\text{БК}}(\text{пр})+\boxed{\text{СумК}}}\right]}{\text{ССК}_{\text{РГ}}(\text{пр})}+\dfrac{\left[\dfrac{\sum \text{СумК*СрК}+\boxed{\text{СумК}}*\boxed{\text{СрК}}}{\text{СК}_{\text{КА}}(\text{пр})+\boxed{\text{СумК}}}\right]}{\text{СД}_{\text{КА}}(\text{пр})}=
\dfrac{\left[\dfrac{\sum \text{ЗМ*СрМ}\ (\text{п.п.})}{\text{ОЗ}_{\text{БК}}(\text{п.п.})}\right]}{\text{ССК}_{\text{РГ}}(\text{п.п.})}+\dfrac{\left[\dfrac{\sum \text{СумК*СрК}}{\text{СК}_{\text{КА}}(\text{п.п.})}\right]}{\text{СД}_{\text{КА}}(\text{п.п.})}
\\
\left[\dfrac{\text{ДД}_{\text{ОЗ}}(\text{пр})+\boxed{\text{ДДК}}}{\dfrac{\text{ОЗ}_{\text{КБ}}(\text{пр})+\boxed{\text{СумК}}}{\text{ДД}_{\text{РГ}}(\text{пр})}}+\dfrac{\text{ДДК}_{\text{КА}}(\text{пр})+\boxed{\text{ДДК}}}{\text{ВБК}_{\text{КА}}(\text{пр})}\right]=
\left[\dfrac{\dfrac{\text{ДД}_{\text{ОЗ}}(\text{п.п.})}{\text{ОЗ}_{\text{КБ}}(\text{п.п.})}}{\text{ДД}_{\text{РГ}}(\text{п.п.})}+\dfrac{\text{ДДК}_{\text{КА}}(\text{п.п.})}{\text{ВБК}_{\text{КА}}(\text{п.п.})}\right]
\end{array}
\right\}
$$

В данной модели левые части уравнений включают значения показателей ресурсообмена в моделируемой экономической системе на период, в котором принимается управленческое решение (индекс пр), а правые части — значения этих же показателей в предшествующий период (индекс п.п.).

Подставляем в левые части уравнений значения из *табл. 3*, в правые — значения из *табл. 2*, и получаем:

$$\begin{cases} \left[\dfrac{52+\boxed{\text{СумК}}}{30\,053}+\dfrac{4}{1{,}3+\boxed{\text{СумК}}}\right]=\left[\dfrac{59{,}19}{24\,700{,}20}+\dfrac{3{,}34}{1{,}52}\right] \\ \left[\dfrac{\dfrac{4*2+\boxed{\text{ОПП}}}{52+\boxed{\text{СумК}}}}{15}+\dfrac{0{,}06+\boxed{\text{ОПП}}}{0{,}10}\right]=\left[\dfrac{17{,}61}{7{,}70}+\dfrac{0{,}07}{0{,}10}\right] \\ \dfrac{\left[\dfrac{1734+\boxed{\text{СумК}}*\boxed{\text{СрК}}}{52+\boxed{\text{СумК}}}\right]}{42}+\dfrac{\left[\dfrac{6{,}9+\boxed{\text{СумК}}*\boxed{\text{СрК}}}{1{,}3+\boxed{\text{СумК}}}\right]}{15}=\dfrac{30}{41}+\dfrac{12}{18} \\ \left[\dfrac{\dfrac{56{,}16+\boxed{\text{ДДК}}}{52+\boxed{\text{СумК}}}}{70}+\dfrac{0{,}47+\boxed{\text{ДДК}}}{0{,}91}\right]=\left[\dfrac{120{,}52}{103{,}12}+\dfrac{0{,}59}{0{,}94}\right] \end{cases}$$

Решив данную систему уравнений, получаем:

$$\boxed{\text{СумК}} \approx 0{,}5,\ \boxed{\text{ОПП}} \approx 0{,}1,\ \boxed{\text{СрК}} \approx 13,\ \boxed{\text{ДДК}} \approx 0{,}2.$$

Таким образом, на основе проведенных расчетов можно сформулировать: если банк «Дельта» заключит контракт с IT-компанией «Гамма» на услуги по обеспечению кибербезопасности клиентских операций на сумму 500 млн руб. на срок 1 год, то в течение ближайшего года после заключения контракта сумма предотвращенных потерь должна составить 100 млн руб., а дополнительный доход в течение 5 лет после начала сотрудничества — 200 млн руб.

Использование феноменологического моделирования позволило рассчитать конкретные параметры обеспечения безопасности клиентских операций в процессе сотрудничества коммерческого банка с IT-компанией, а также разработать карту киберустойчивости (*рис. 2*), которая позволит оптимизировать мониторинг, своевременное выявление возможных кибератак, реагирование на киберинциденты и приоритизировать задачи по укреплению ИТ-инфраструктуры кредитной организации.

Дальнейшие исследования в этой области могут быть направлены на рассмотрение более сложных кейсов для разработки решений и параметров сотрудничества коммерческого банка одновременно с несколькими IT-компаниями.

ВЫВОДЫ

В работе представлен критический обзор отечественной и зарубежной научной литературы по вопросам киберрисков и кибербезопасности в условиях развития цифрового банковского бизнеса. Теоретическая значимость исследования заключается в том, что рассмотрен теоретический плюрализм в отношении анализируемого понятия и обоснован понятийный аппарат, позволяющий исследовать функционирование, развитие и обоснование управленческих решений при построении системы киберустойчивости в коммерческом банке: предложено понятие «киберэкосистема», построение которой на уровне кредитной организации поможет более оптимально выявлять и минимизировать возможность реализации киберриска по ключевым и целевым направлениям деятельности коммерческого банка, а также способ-

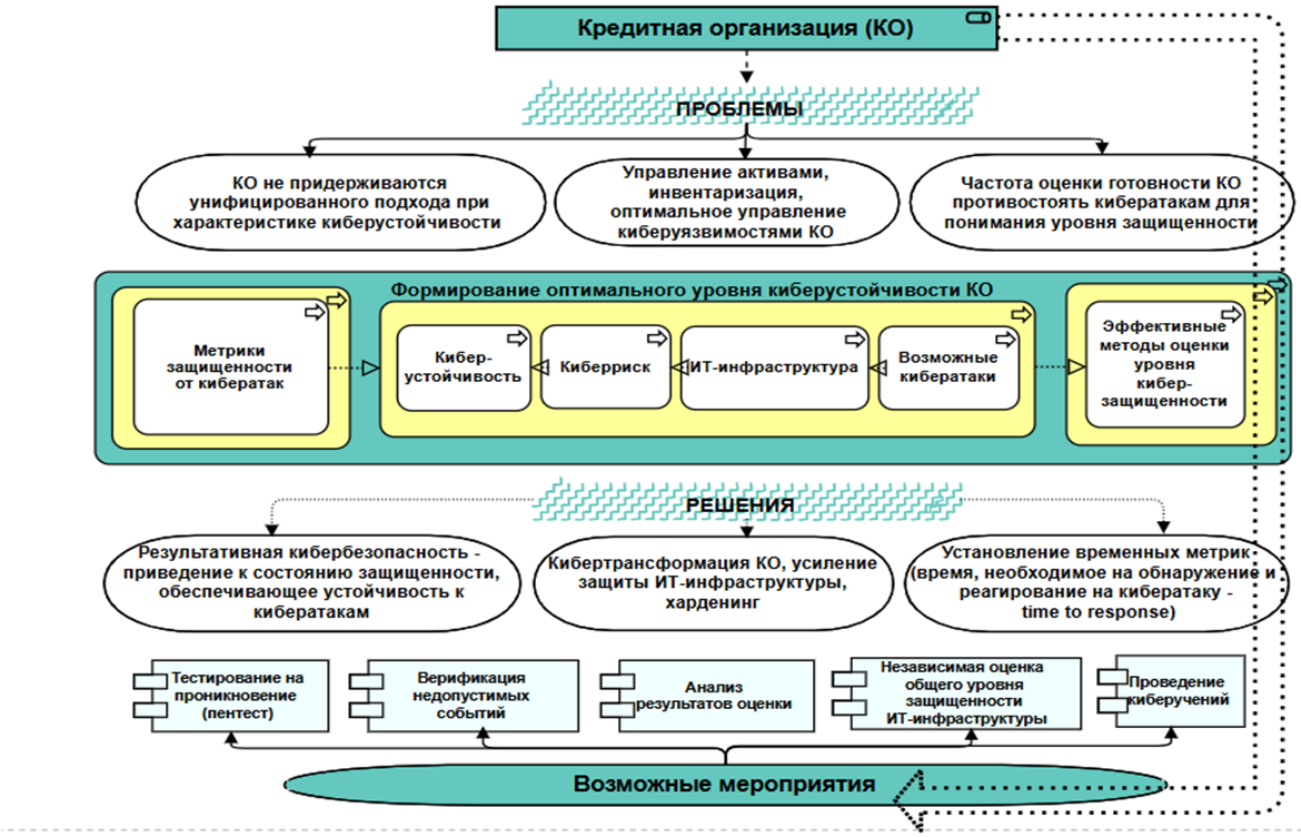

Рис. 2 / Fig. 2. **Карта киберустойчивости коммерческого банка / A Commercial Bank's Cyberstability Map**
Источник / Source: составлено авторами / Compiled by the authors.

ствовать киберустойчивости организации в условиях развития цифрового банковского бизнеса. Практическая значимость исследования заключается в развитии прикладных аспектов системного анализа и решения практических проблем: разработана модель взаимодействия коммерческого банка с ИТ-компанией, специализирующейся на оказании услуг по противодействию киберрискам. На основе данной модели предложен алгоритм обоснования управленческих решений банка по выделению средств на киберзащиту. Использование феноменологического моделирования в рамках данного исследования позволило формализованным путем рассчитать конкретные параметры сотрудничества коммерческого банка и IT-компании, обеспечивающей безопасность клиентских операций. Построение карты киберустойчивости коммерческого банка позволило визуализировать ландшафт киберугроз и обосновать необходимость постоянного совершенствования форм и методов обеспечения кибербезопасности на уровне кредитных организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Швыров В.В., Гвоздюкова С.Н. Категории рисков, связанных с киберпространством: характер убытков и бизнес-сектора. *Вестник Луганского государственного педагогического университета. Серия 5. Гуманитарные науки. Технические науки.* 2022;(2):96–104.
2. Ларина О.И., Морыженкова Н.В. К вопросу о развитии методологии идентификации киберриска. *Банковское дело*. 2023;(1):66–71.
3. Амосова Н.А., Рудакова О.С. Финансовая стабильность на финансовых рынках: идентификация лидерства и источников генерации рисков. М.: КноРус; 2025. 240 с.
4. Ларионова И.В. Конкуренция на рынке финансовых услуг Бигтех-компаний и БигБанков. Проблемы регулирования, риски и финансовая стабильность. *Банковские услуги*. 2025;(3):12–18. DOI: 10.36992/2075–1915_2025_3_12
5. Ларионова И.В. Новые подходы к регулированию финансового рынка в условиях возрастающих рисков неопределенности экономического развития при введении санкционных ограничений. М.: КноРус; 2024. 190 с.

6. Ларионова И.В., Устинов Д.А. Имплементация внутренних кредитных рейтингов заемщика в систему оценки кредитного риска. *Финансы, деньги, инвестиции*. 2024;(4):30–37. DOI: 10.36992/2222–0917_2024_4_30
7. Метельков А.Н. Киберучения: зарубежный опыт защиты критической инфраструктуры. *Правовая информатика*. 2022;(1):51–60. DOI: 10.21681/1994–1404–2022–1–51–60
8. Васильев С.А., Никонова И.А., Мирошниченко О.С. Банки, финансовые платформы и Big Data: тенденции развития и направления регулирования. *Финансовый журнал*. 2022;14(5):105–119. DOI: 10.31107/2075–1990–2022–5–105–119
9. Дюдикова Е.И., Ризванова И.А. Риск-профиль DeFi как индикатор кризиса доверия. *Инновации и инвестиции*. 2025;(5):632–637.
10. Ризванова И.А. Идентификация рисков и контроль за ними в платежной системе: российский и зарубежный опыт. *Вестник университета (Государственный университет управления)*. 2024;(9):203–212. DOI: 10.26425/1816–4277–2024–9–203–212
11. Шкодинский С.В., Дудин М.Н., Усманов Д.И. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике. *Финансовый журнал*. 2021;13(3):38–53. DOI: 10.31107/2075–1990–2021–3–38–53
12. Антонян Е.А., Клещина Е.Н. Киберпреступность на современном этапе: тенденции и направления противодействия. *Вестник экономической безопасности*. 2022;(5):11–15. DOI: 10.24412/2414–3995–2022–5–11–15
13. Халин В.Г., Чернова Г.В. Цифровизация и киберриски. *Управленческое консультирование*. 2023;(7):28–41. DOI: 10.22394/1726–1139–2023–7–28–41
14. Дудин М.Н., Шкодинский С.В. Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы. *Финансы: теория и практика*. 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. Белова М.Т. Практические вопросы совершенствования политики Банка России в области защиты прав потребителей финансовых услуг. *Инновационное развитие экономики*. 2022;(3–4):197–204. DOI: 10.51832/2223798420223–4197
19. Белова М.Т., Шилов И.С. Перспективы развития банковского бизнеса в условиях цифровой трансформации финансовой системы. *Финансовые рынки и банки*. 2023;(12):79–87.
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. Бровкина Н.Е., Ризванова И.А. Транзакционный банковский бизнес. М.: КноРус; 2022. 212 с.
26. Гумеров М.Ф., Ризванова И.А. Кредитные риски российских коммерческих банков: новые подходы к управлению. *Финансы: теория и практика*. 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.

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.

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Марат Фаридович Гумеров — доктор экономических наук, ведущий научный сотрудник лаборатории микроэкономического анализа и моделирования, Центральный экономико-математический институт Российской академии наук, Москва, Российская Федерация
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

Ирина Азатовна Ризванова — кандидат экономических наук, доцент кафедры банковского дела и монетарного регулирования Финансового факультета, старший научный сотрудник института финансовых исследований Финансового факультета, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
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
Автор для корреспонденции / Corresponding author:
iarizvanova@ya.ru

Марианна Толевна Белова — кандидат экономических наук, доцент кафедры банковского дела и монетарного регулирования Финансового факультета, научный сотрудник института финансовых исследований Финансового факультета, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
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

Заявленный вклад авторов:
М.Ф. Гумеров — научное руководство; сбор данных и доказательств; проведение критического анализа материалов; формирование выводов; написание текста статьи.
И.А. Ризванова — развитие методологии; сбор данных и доказательств; написание текста статьи.
М.Т. Белова — развитие методологии; сбор данных и доказательств; написание текста статьи.

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.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила в редакцию 30.09.2024; после рецензирования 29.10.2024; принята к публикации 22.02.2025.
Авторы прочитали и одобрили окончательный вариант рукописи.
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.

Переводчик В.И. Тимонина