УДК 658.15:005.342
DOI: 10.34020/1993-4386-2023-2-79-83

РАЗВИТИЕ БАНКОВСКОГО РИСК-МЕНЕДЖМЕНТА КАК СПОСОБ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Е. А. Фомина
Уфимский филиал Финансового университета при Правительстве Российской Федерации,
Уфа, Россия

Ю. В. Ходковская
Уфимский государственный нефтяной технический университет» (УГНТУ),
Уфа, Россия

Авторами научной статьи представлено исследование по развитию банковского риск-менеджмента в условиях цифровой трансформации бизнес-процессов и бизнес-операций. Проанализированы условия формирования стратегий риск-менеджмента крупнейших банков России. Исследованы аспекты регуляторных требований в России и за рубежом к управлению рисками, включая киберриски. Предложена интегрированная модель управления банковскими киберрисками, дополненная положениями стандартов COSO ERM и FERMA, и даны рекомендации по ее использованию.

Ключевые слова: банк, риск-менеджмент, цифровая трансформация, киберриск, стандарты COSO ERM, экономическая безопасность.

Приоритеты устойчивого развития, направленность национальных экономик на опережающее развитие, трансформация социально-экономических отношений, цифровизация бизнес-процессов, высокая геополитическая нестабильность способствовали усилению неопределенности и рисков в финансово-кредитном секторе экономики России. На фоне санкционного давления недружественных стран, обвала рынка ценных бумаг, временного закрытия Московской биржи, оттока вкладов из банков, отключения российской платежной системы от SWIFT, угрозы потери ликвидности, платежеспособности, доходности отечественных банков стали очевидными, что обострило актуальность поиска решения проблемы обеспечения экономической безопасности российских банков.

Уровень банковских рисков в современной российской практике регулируется нормативными актами, стандартами Банка России с учетом международных принципов Базельского комитета, а также международными и национальными стандартами (серия ISO 20000[1, 2]; серия ISO 27000[3];

[1] ISO 20000: принципы использования и область применения международного стандарта / Сайт Системы добровольной сертификации «Единый центр сертификации». URL: https://isorus.ru/blog/ sertifikaciya/ standart-iso-20000-opredelenie-trebovaniya-printsipyi-oblast-primeneniya/ (дата обращения: 20.05.2023).

[2] Основой для создания ISO 20000 послужила последняя версия британского стандарта BS 15000, разработанного BSI и содержащего описание универсальных критериев для оценки системы управления IT-сервисами организации, в том числе оценки систем ее информационной безопасности. ISO 20000 состоит из двух частей: первая часть содержит подробное описание требований к системе управления IT-сервисами, а также ответственность за них; вторая часть стандарта является практической и содержит рекомендации по процессам и требованиям, описанным в первой части. В 2011 г. международный стандарт ISO 20000 получил обновление – вышла новая редакция ISO/IEC 20000:2011. В 2013 г. Федеральное агентство по техническому регулированию и метрологии (Росстандарт) утвердило ГОСТ Р ИСО/МЭК 20000-1-2013 (он был введен в действие 01.01.2015), идентичный международному стандарту ISO/IEC 20000-1:2011 «Информационные технологии. Управление услугами». Этот документ является стандартом Системы управления услугами (СУУ) и содержит требования к поставщику услуг по планированию, созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию Системы управления услугами для обеспечения соответствия требованиям к услугам. 7 декабря 2021 г. взамен стандарта ГОСТ Р ИСО/МЭК 20000-1-2013 приказом Росстандарта № 1718-ст был утвержден национальный стандарт РФ ГОСТ Р ИСО/МЭК 20000-1-2021 «Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов», с датой введения в действие 30 апреля 2022 г.

[3] В России стандарт серии ISO 27000, а именно Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология», был утвержден приказом Росстандарта от 15 ноября 2012 г. № 813-ст, а введен в действие с 1 января 2013 г. С 30 ноября 2021 г. в связи с изданием Приказа Росстандарта от 19 мая 2021 г. № 392-ст стандарт ГОСТ Р ИСО/МЭК 27000-2012 утратил силу, взамен его был введен в действие (с 30 ноября 2021 г.) ГОСТ Р ИСО/МЭК 27000-2021, который содержит общий обзор систем менеджмента информационной безопасности (СМИБ). В нем приведены термины и определения, используемые в семействе стандартов СМИБ. Стандарт применим для коммерческих и некоммерческих организаций, в органов государственной власти, органов местного самоуправления и их учреждений.

серия ГОСТ Р53647[4]; серия ISO 31000[5]), регламентирующими вопросы организации менеджмента риска, оценки системы управления IT-сервисами организации, в том числе оценки систем ее информационной безопасности, вопросы организации систем менеджмента информационной безопасности, планирования и разработки стратегии и политики управления человеческими ресурсами и др. В условиях цифровой трансформации банковского бизнеса кредитные организации особое внимание уделяют внутреннему аудиту, мониторингу рисков, формированию системы лимитирования наиболее сомнительных операций, обеспечению информационной и экономической безопасности и др.

Поскольку классификация банковских рисков весьма обширна и отсутствует унифицированный алгоритм группировки, большинство банков России для обеспечения экономической безопасности сосредоточивают внимание на управлении рисками концентрации, оценивая:

– наличие наиболее существенного объема требований к одному или нескольким контрагентам;

– выбор в качестве инвестиций продуктов одного вида, ценность которых связана с воздействием различных факторов;

– наличие существенной численности кредитных требований к контрагентам, функционирующим на одном участке территории, производящих одинаковую продукцию, либо обязательства которых номинированы в одной валюте;

– хеджирование рисков и связанные с этим операции залога или поручительств и т.д.

Анализ деятельности крупнейших банков России за последние 5 лет позволил установить, что реализуемые стратегии риск-менеджмента сформировались в следующих условиях:

– нацеленность банка на увеличение клиентской базы, объема депозитов и кредитов, операций с ценными бумагами, т.е. масштабирование деятельности (в 2022 г. по сравнению с 2021 г. кредитный портфель банков РФ вырос на 14,3 %, объем вложений в долговые ценные бумаги – на 2,3 трлн руб.)[6];

– ориентация на операции как с юридическими, так и с физическими лицами, что обеспечило в 2022 году рост объема кредитования, несмотря на снижение процентных ставок по вкладам и депозитам и реализации программы государственного субсидирования субъектов малого и среднего предпринимательства (МСП), программы государственной поддержки ипотечных заемщиков (чистые процентные доходы банков РФ увеличились на 2,9 %, комиссионные доходы – на 5,7 % в 2022 г. к уровню 2021 г.);

– высокодинамичное распространение современных финансовых технологий при отставании разработок по обеспечению их безопасного использования: уровень затрат кредитных организаций России на цифровые решения и технологии ежегодно возрастает на 12–14 %[7];

– использование типовых методик управления банковскими рисками, предложенных Банком России, без необходимой адаптации к условиям конкретного банка, что снижает ценность их применения вследствие слишком формального подхода.

Несмотря на быстрое обновление банковских технологий с учетом требований цифровой бизнес-среды, обеспечение экономической безопасности в отечественных банках остается проблемным. Эксперты утверждают, что применяемые инструменты управления банковскими рисками не в полной мере обладают требуемой функциональностью и отвечают требованиям качества и безопасности[8].

В условиях цифровой экономики наибольшая угроза современного банковского сектора связана с киберрисками. Сложность управления киберрисками объясняется тем, что пруденциальные требования в отечественном банковском праве не предусматривают формирование резервов под убытки, связанные с киберрисками, что свидетельствует о неадекватности существующих подходов и методологий банковского риск-менеджмента. Кроме того, под влиянием происходящих процессов цифровизации обширный перечень киберрисков постоянно трансформируется, появляются их новые модифицированные подвиды, следова-

[4] ГОСТ Р 53647.8-2013. Национальный стандарт РФ «Менеджмент непрерывности бизнеса. Управление человеческими ресурсами» утвержден приказом Росстандарта от 22 ноября 2013 г. № 1667-ст, а введен в действие с 1 января 2014 г. Стандарт представляет собой «руководство по планированию и разработке стратегии и политики управления человеческими ресурсами (ЧР) при возникновении инцидента, предусматривающее: меры реагирования при непосредственном воздействии инцидента; организационные действия на этапе восстановления после воздействия инцидента (обеспечения непрерывности деятельности); поддержку персонала при восстановлении деятельности организации. В нем определены дополнительные требования к обеспечению непрерывности деятельности соответствующие требованиям, установленным в стандартах серии ГОСТ Р 53647. Стандарт предназначен для высшего руководства, ответственного за управление ЧР организации, и применим к организациям любых форм собственности и видов деятельности вне зависимости от численности персонала».

[5] Одним из основных стандартов серии ISO 31000 является стандарт ГОСТ Р ИСО 31000-2019. Национальный стандарт РФ «Менеджмент риска. Принципы и руководство», утвержденный приказом Росстандарта от 10 декабря 2019 г. № 1379-ст и введенный в действие с 1 марта 2020 г. Стандарт предназначен для лиц, чья деятельность направлена на создание и защиту ценностей организаций путем менеджмента риска (МР), принятия решений, постановки и достижения целей, повышения эффективности деятельности. Согласно стандарту, МР является итеративным процессом и помогает организациям в определении стратегии, достижении целей и принятии обоснованных решений; являясь частью корпоративного управления организации, МР имеет фундаментальное значение для управления на всех уровнях, способствует совершенствованию системы управления организацией, затрагивает любые виды деятельности, осуществляемые в рамках организации, и включает взаимодействие с причастными сторонами; учитывает внешнюю и внутреннюю среду организации, включая поведение людей и культурные факторы. В стандарте определены принципы, структура МР и подробно описан его процесс.

[6] 2022 год. Банковский сектор. Аналитический обзор / Сайт Банка России. URL: https://cbr.ru/Collection/Collection/File/43816/analytical_review_bs-2022.pdf (дата обращения: 22.05.2023).

[7] Цифровизация банков 2022: Обзор TAdviser (публикация от 20.01.2023). URL: https://www.tadviser.ru/index.php/Статья:Обзор_TAdviser:_Цифровизация_банков_2022 (дата обращения: 22.05.2023).

[8] Там же.

тельно, становится необходимым развитие новых подходов к управлению киберрисками [1-3].

Актуальность решения проблемы обеспечения экономической безопасности кредитных организаций России в условиях киберрисков усиливается в связи с увеличением ассортимента банковских продуктов и услуг, предоставление которых связано с финансово-информационными технологиями [4-6]. На это обращается особое внимание в Докладе для общественных консультаций Банка России «Регулирование рисков участия банков в экосистемах и вложений в иммобилизованные активы»[9], опубликованном в 2021 г.

В международной практике банковского риск-менеджмента наиболее известны стандарты COSO ERM[10] и FERMA[11]. Стандарт COSO ERM основывается на повышении достоверности отчетности организации и применяется в публичных компаниях США. Стандарт FERMA строится на положениях международного стандарта ISO 31000, который содержит наиболее полное описание рисков, что объясняет его широкое применение в банковской сфере.

В современных условиях преимуществом применения на практике стандартов COSO ERM и FERMA выступают возможности их распространения на процессы управления киберрисками. Положения стандартов COSO ERM и FERMA легко адаптируются к любому типу бизнес-операций и интегрируются с другими стандартами и руководствами, используемыми в банковской сфере.

Для построения наиболее эффективного механизма управления банковскими рисками в России целесообразно применяемую в отечественной практике модель риск-менеджмента дополнить положениями стандартов COSO ERM и FERMA, сформировав интегрированную модель управления банковскими киберрисками, что обеспечит учет влияния киберрисков и, соответственно, более высокий уровень экономической безопасности кредитной организации (рисунок 1).

В предложенной модели управления банковскими киберрисками целевые установки в части экономической безопасности интегрированы в общую стратегию риск-менеджмента кредитной организации с учетом системы локальных оценочных индикаторов, устанавливаемых службой риск-менджмента. Целевые установки обеспечения экономической безопасности кредитной организации должны учитывать приоритеты ее устойчивого развития.

Оценку банковских киберрисков следует проводить на систематической основе, поскольку долгосрочные последствия сегодняшних нововведений в части цифровой трансформации банковского бизнеса безусловно проявятся, но их прогнозирование и оценка представляют весьма сложную задачу. Поэтому применение комплексного подхода к оценке банковских киберрисков позволит уделить особое внимание управляемым/неуправляемым рискам упущенных возможностей, исследовав их влияние на отдельные банковские операции и финансовую устойчивость банка в целом.

При реализации этапа оценки банковских киберрисков важным является разработка лимитов открытых позиций по рисковым активам. Экономически обоснованные лимиты могут быть установлены только при отслеживании движения конъюнктурных факторов финансового рынка, постоянно генерирующего новые подвиды банковских рисков. Лимиты открытых позиций по рисковым активам целесообразно устанавливать по субъектам риска, по уровню диверсификации, по степени релевантности и др. На основе полученных оценок банковских киберрисков уместна количественная и качественная оценка сложившихся индикаторов экономической безопасности кредитной организации, их соответствие стратегическим целевым установкам.

Элиминирование киберрисков по стандартам COSO ERM включает выбор направлений и способов минимизации киберрисков. В условиях цифровой трансформации банковского бизнеса кредитные организации формируют прогнозные показатели эффективности отдельных бизнес-процессов путем стресс-тестирования, в связи с этим важной задачей становится имплементация оценки киберриска в систему банковского стресс-тестирования, что позволит выявить влияние киберрисков при различных сценариях развития банка, адаптировать способы минимизации киберрисков под его конкретные бизнес-задачи.

Этап координации деятельности служб информационных технологий и экономической безопасности со стороны службы риск-менеджмента банка включает обмен информацией и консультирование на протяжении всего процесса управления киберрисками кредитной организации. Согласованность во взаимодействии служб информационных технологий и экономической безопасности кредитной организации со службой управления банковскими рисками обеспечит более высокое качество системы внутреннего контроля и эффективное проведение последующего контроля реализации банковских операций. Продуктом такого взаимодействия может быть, к примеру, создание значительного по объему списка сервисов, технологий, систем хранения данных, важным для которых является идентификация критически важных киберрисков. Координация деятельности служб безопасности банка также предполагает и взаимодействие со стейкхолдерами, заинтересованными в устранении киберугроз в банковской сфере.

Традиционный гэп-анализ, касающийся соответствия чувствительных к изменению процентной ставки активов и пассивов банка, не учитывает влияние киберрисков, поэтому на этапе 4 (рис. 1) настоятельно рекомендуется корректировка состава и структуры рисковых активов банка на основе оценки киберрисков по требованиям стандарта FERMA. С учетом долгосрочных последствий влияния киберрисков данная корректировка должна проводиться на постоянной основе.

---

[9] URL: https://cbr.ru/Content/Document/ File/123688/Consultation_Paper_23062021.pdf

[10] Compliance Risk Management: Applying the COSO ERM Framework. URL: https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

[11] Мария Шантаренкова. Управление ИТ-рисками. Часть 2. URL: https://upr.ru/article/sistema-upravleniia-it-riskami/ (дата обращения: 22.05.2023).

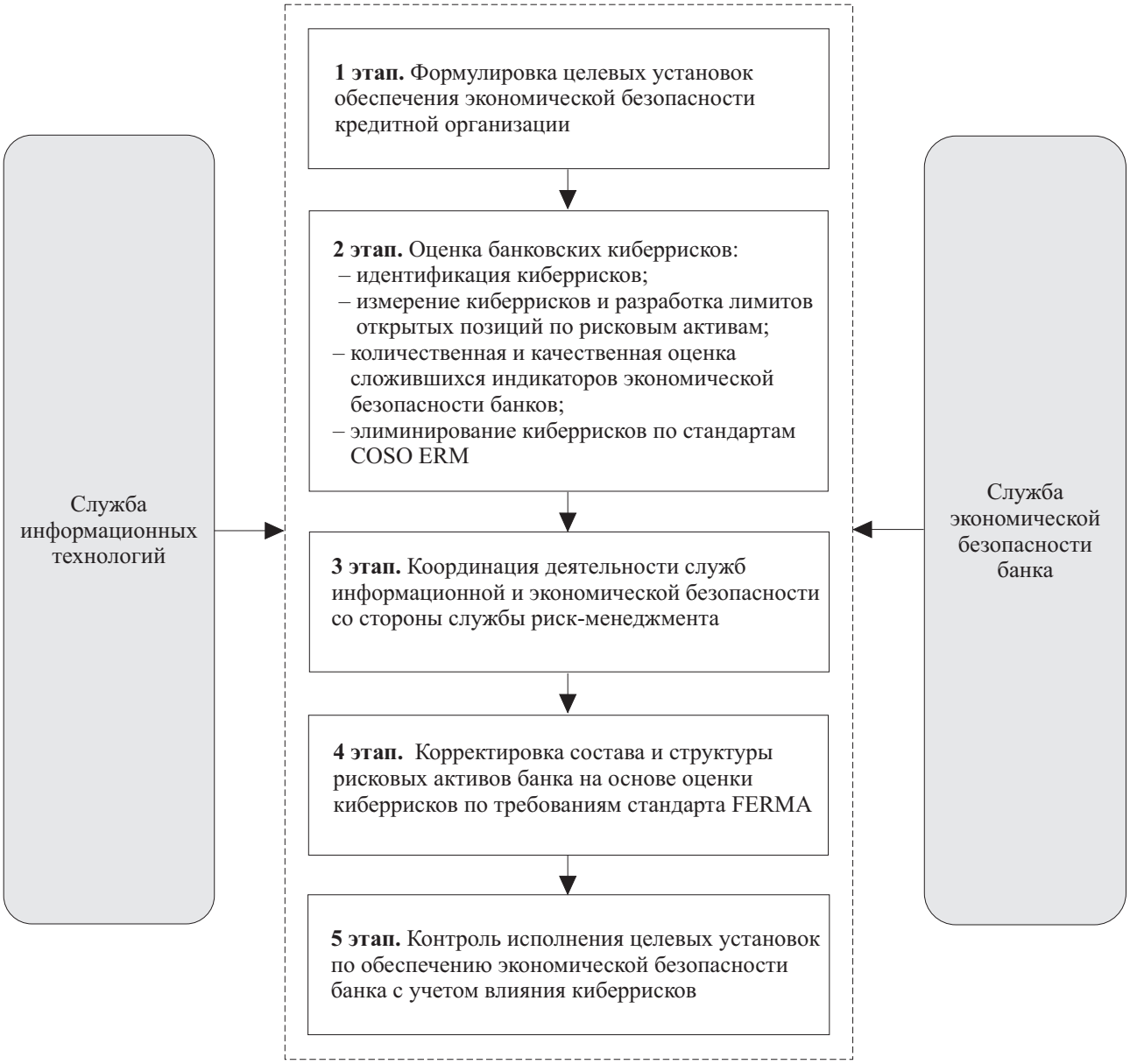

Рис. 1. Интегрированная модель управления киберрисками в системе банковского риск-менеджмента

Данная модель управления киберрисками не является автономной, а составляет неотъемлемую часть риск-менеджмента, являющегося существенным элементом системы менеджмента банка, поэтому контроль исполнения целевых установок по обеспечению его экономической безопасности с учетом влияния киберрисков должен быть нацелен на достижение результативных показателей деятельности банка, определенных в его стратегии развития.

Литература

1. *Tarek A., Kokh I. A.* Bank risk management tools and techniques / В сборнике: Экономика в меняющемся мире. IV Всероссийский экономический форум (Казань, 29 апреля 2020 г.) // Сборник научных трудов. – Казань: Издательство Казанского университета, 2020. С. 511–515. URL: https://dspace.kpfu.ru/xmlui/viewer?file=159726;EMM_2020_511_515.pdf&sequence=1&isAllowed=y.

2. *Piao G., Xiao B.* Risk Management Analysis of Modern Commercial Banks Using Behavioral Finance Theory and Artificial Neural Networks // Wireless Communications and Mobile Computing. 2022. Vol. 8. PP. 1-8. DOI: https://doi.org/10.1155/2022/1161784.

3. *Солонина С. В., Лабов А. А.* Риск-менеджмент в коммерческом банке // Научный вестник Южного института менеджмента. 2020. № 2 (30). С. 75–82. DOI: 10.31775/2305-3100-2020-2-75-82.

4. *Tursoy T.* Risk management process in banking industry / Munich Personal RePEc Archive, Paper No. 86427, posted 02 May 2018. URL: https://mpra.ub.uni-muenchen.de/86427/1/MPRA_paper_86427.pdf

5. *Ikramova N. B.* Risk management in Banks / International Conference of Scientific and Social Studies. 2022. PP. 28-39. URL: https://nextscientists.com/index.php/science-conf/article/view/82/74/ (дата обращения: 19.06.2023).

6. *Team R.* Proactive IT Risk Management in Banking Sector. – Risk Management Studio. 2021. URL: https://www.riskmanagementstudio.com/proactive-it-risk-management-in-banking-sector/ (дата обращения: 19.06.2023).

Сведения об авторах

Фомина Елена Александровна – канд. экон. наук, доцент кафедры «Финансы и кредит», Уфимский филиал ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Уфа, Россия.
E-mail: kaffda@list.ru

Ходковская Юлия Викторовна – канд. экон. наук, доцент кафедры «Экономика и стратегическое развитие», ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Уфа, Россия.
E-mail: khodkovskiy@bk.ru

DEVELOPMENT OF BANK RISK MANAGEMENT AS A WAY TO ENSURE ECONOMIC SECURITY

E. Fomina
Ufa Branch of the Financial University under the Government of the Russian Federation (Financial University), Ufa, Russia
Yu. Khodkovskaya
Ufa State Petroleum Technical University (USNTU), Ufa, Russia

The authors of the scientific article present a study on the development of banking risk management in the context of digital transformation of business processes and business operations. The conditions for the formation of risk management strategies of the largest banks in Russia are analyzed. Aspects of regulatory requirements in Russia and abroad for risk management, including cyber risks, are investigated. An integrated model of banking cyber risk management is proposed, supplemented by the provisions of the COSO ERM and FERMA standards, and recommendations for its use are given.

*Key word*s: bank, risk management, digital transformation, cyber risk, COSO ERM standards, economic security.

References

1. Tarek A., Kokh I. A. Bank risk management tools and techniques, *Ekonomika v menyayushchemsya mire* [Economy in a changing world], Collection of scientific papers of the IV All-Russian Economic Forum, Kazan, April 29, 2020, Kazan: Izdatel'stvo Kazanskogo universiteta, 2020. pp. 511–515. Available at: https://www.researchgate.net/publication/344357186_Bank_risk_management_tools_and_techniques.

2. Piao G., Xiao B. Risk Management Analysis of Modern Commercial Banks Using Behavioral Finance Theory and Artificial Neural Networks. Wireless Communications and Mobile Computing. 2022. Vol. 8. PP. 1-8. DOI: https://doi.org/10.1155/2022/1161784.

3. Solonina S. V., Labov A. A. Risk management in a commercial bank, *Nauchnyi vestnik Yuzhnogo instituta menedzhmenta,* 2020, No. 2, pp. 75-82. DOI: https://doi.org/10.31775/2305-3100-2020-2-75-82.

4. Tursoy T. Risk management process in banking industry. MPRA Paper No. 86427, posted 02 May 2018 14:20 UTC. https://mpra.ub.uni-muenchen.de/86427/1/MPRA_paper_86427.pdf

5. Ikramova N., Burkhon Q. Risk management in Banks. International Conferenceof Scientificand Social Studies. 2022. pp. 28-39. Available at: https://nextscientists.com/index.php/science-conf/article/view/82/74/.

6. Team R., Proactive IT Risk Management in Banking Sector. Risk Management Studio. 2021. https://www.riskmanagementstudio.com/proactive-it-risk-management-in-banking-sector/ (accessed: 06/19/2023).

About the authors

Elena A. Fomina – Candidate of Economic Sciences, Associate Professor of the Department of Finance and Credit Ufa Branch of the Financial University under the Government of the Russian Federation (Financial University), Ufa, Russia.
E-mail: kaffda@list.ru

Yulia V. Khodkovskaya – Candidate of Economic Sciences, Associate Professor of the Department of Economics and Strategic Development Ufa State Petroleum Technical University (USNTU), Ufa, Russia.
E-mail: khodkovskiy@bk.ru