Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»

На правах рукописи

Одинцов Владислав Олегович

РАЗВИТИЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ ЦИФРОВИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ ПРИ ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

5.2.3. Региональная и отраслевая экономика: экономическая безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата экономических наук

Научный руководитель — Орлова Любовь Николаевна,
доктор экономических наук, профессор

Москва – 2024

Оглавление

Введение

Актуальность темы исследования. Обеспечение достаточности уровня экономической безопасности в организациях каждой из отраслей экономики связано с развитием системы управления рисками, повышением финансовой устойчивости и готовностью к различным негативным сценариям. Рост технологической конкуренции – одна из главных характеристик современной экономической среды, в условиях борьбы за технологическое превосходство границы между рисками, доходами и безопасностью организаций становятся все более размытыми, воздействие рисков на ликвидность, формируемую во многом за счет эффективности бизнес-процессов, становится все ощутимее. Риски, связанные с применением цифровых технологий, в настоящее время находятся в стадии активного роста и характеризуются большим влиянием на безопасность, нежели ранее, угрозы кибербезопасности при этом выходят на первый план. Подобные риски, если ими не управлять должным образом, могут поставить под угрозу и конкурентоспособность, и финансовую устойчивость организации, являющуюся одной из главных составляющих ее экономической безопасности.

Цифровизация напрямую влияет и на финансовую систему Российской Федерации – особенно на банковский сектор, который переживает трансформацию, связанную с реализацией цифровых технологических и операционных инноваций. Сложившаяся тенденция повсеместной цифровизации определяет возможности для развития кредитных организаций, но также и влечет за собой появление новых видов рисков, которые оказывают влияние на уровень экономической безопасности в данных организациях. Научная проблема необходимости развития системы управления рисками цифровизации бизнес-процессов при обеспечении экономической безопасности связана, во-первых, с тем, что цифровая трансформация организаций приводит к дифференциации цифровых рисков по различным

бизнес-процессам; во-вторых, с низким уровнем оснащенности инструментами (в особенности аналитическими) для оценки рисков; в-третьих, с недостаточностью изученности природы цифровых рисков, методов их оценки и митигации.

В рамках исследования рассматриваются кредитные организации, а в частности банки, составляющие 93% от общего количества кредитных организаций в России [36], так как они наиболее подвержены угрозам атак в цифровом контуре, поскольку хранят большие объемы финансовой информации о клиентах, обладают их персональными данными, ежесекундно обрабатывают многочисленные денежные потоки – в совокупности со сложной технической инфраструктурой, которая содержит уязвимые места, а также с фактом отключения российских кредитных организаций от передовых решений в области кибербезопасности из-за сложной геополитической ситуации, именно кредитные организации (особенно российские) являются одной из главных целей для преступного сообщества.

Степень разработанности темы исследования. Исследованию широкого круга вопросов обеспечения экономической безопасности, формирования системы управления рисками организаций и развития теоретических и практических аспектов элементной структуры данной системы посвящены работы зарубежных и отечественных ученых.

Вопросам обеспечения экономической безопасности, а также становления и развития системы управления рисками организаций (в том числе кредитных) посвящены труды таких ученых, как В.И. Авдийский, В.М. Безденежных, Г.Н. Белоглазова, Н.И. Валенцева, В.Н. Вяткин, В.А. Гамза, В.В. Земсков, С.Н. Кабушкин, Е.В. Каранина, Л.Н. Красавин, Н.Ф. Кузовлева, О.И. Лаврушин, В.И. Лобанов, Е.П. Рамзаева, М.В. Сигова, С.Н. Сильвестров, Н.Г. Синявский, В.М. Смирнов, В.Г. Старовойтов, А.М. Тавасиев, Г.А. Тосунян и других. Однако изменение внешней экономической конъюнктуры требует актуализации научных положений в части формирования новых подходов к управлению рисками при обеспечении

экономической безопасности организаций в условиях повсеместной цифровизации их бизнес-процессов.

Влияние цифровой трансформации на бизнес-процессы организаций (в том числе кредитных) рассматривалось в трудах многих исследователей: в контексте утраты организациями ряда конкурентных позиций (Д.Н. Бажановой, О.М. Марковой); в контексте взаимообусловленного влияния процессов цифровизации и применяемых цифровых технологий на показатели эффективности деятельности, рыночной стоимости организаций, стоимости цифровых активов (Л.В. Волкова, Е.А. Исаевой, Л.Н. Орловой, К.А. Санниковой, А.С. Преображенской, Т.Н. Резвяковой, М.М. Сорокиной); в контексте возникновения новых видов риска организаций различных отраслей, неоднородности их влияния и проявления (В.Ф. Гапоненко, Н.В. Капустиной, И.П. Хоминич). Однако необходимость определения степени влияния рисков, связанных с цифровизацией, на экономическую безопасность организаций оставляет место для проведения научного исследования.

Методические рекомендации по оценке рисков организации в условиях цифровизации нашли отражение в трудах зарубежных и российских авторов О.У. Ависа, Д.А. Курмановой, К.Д. Мартемьяновой, Дж. С. Паради, Д.Р. Султангареева, Ф.К. Там, Л.Р. Хабибуллиной, Х.Д. Шермана, Н.В. Щербаковой и других. Использование анализа среды функционирования в качестве метода сравнительной эффективности применительно к различным субъектам экономики представлено в работах Е.А. Вечкинзовой, О.С. Гасановой, В.А. Ефименко, М.И. Ильиной, Е.В. Медюхи, А.А. Мицеля, Е.Д. Шумской, С.В. Юровой и других. Однако многогранность рисков, связанных с цифровизацией, и широкий спектр сопутствующих ей опасностей и угроз обуславливают необходимость дальнейшего изучения и развития инструментов митигации и оценки данной категории рисков.

Существующие исследования в основном сосредоточены на отдельных аспектах цифровой трансформации бизнеса, вопросы влияния цифровизации

на экономическую безопасность как финансового, так и нефинансового сектора носят фрагментарный характер. Недостаточной степенью изученности проблем использования цифровых технологий в контексте возникающих в связи с этим рисков, а также воздействия данных рисков на бизнес-процессы организации и обеспечение ее экономической безопасности обусловлены цель и задачи диссертационного исследования.

Целью исследования является формирование теоретико-методических положений по развитию системы управления рисками цифровизации бизнес-процессов при обеспечении экономической безопасности организации, а также разработка практических рекомендаций по оценке и митигации данных рисков.

Достижение цели основывается на решении следующих **задач**:

а) исследовать теоретический аспект взаимосвязи между экономической безопасностью и управлением рисками организации в условиях цифровизации для последующего определения направлений реагирования организации на опасности и угрозы, возникающие в связи с цифровизацией бизнес-процессов;

б) выявить особенности регулирования бизнес-процессов кредитной организации в рамках их протекания в цифровом пространстве, определить взаимосвязь между рисками, связанными с цифровизацией, и бизнес-процессами кредитной организации;

в) уточнить понятийно-категориальный аппарат риска, связанного с цифровизацией, осуществить идентификацию и классификацию рисков данного вида, а также определить причины их возникновения;

г) разработать методические рекомендации по оценке и минимизации рисков, связанных с цифровизацией бизнес-процессов организации;

д) разработать практические рекомендации, направленные на минимизацию рисков, связанных с цифровизацией, а также на обеспечение экономической безопасности организации (на примере кредитной организации).

Объектом исследования является система управления рисками как инструмент обеспечения экономической безопасности организаций в условиях роста влияния цифрового пространства на бизнес-процессы.

Предметом исследования являются экономико-управленческие отношения, возникающие в процессе становления и развития системы управления цифровыми рисками и обеспечения экономической безопасности организаций (в том числе кредитных).

Область исследования диссертации соответствует п. 13.14. «Управление рисками при обеспечении экономической безопасности» Паспорта научной специальности 5.2.3. Региональная и отраслевая экономика: экономическая безопасность (экономические науки).

Теоретическая значимость работы заключается в расширении теоретико-методических основ оценки и управления цифровыми рисками в организациях, а также в решении научной задачи по формированию перечня инструментов, повышающих уровень экономической безопасности кредитных организаций в условиях цифровизации бизнес-процессов.

Практическая значимость работы заключается в возможности использования предложений и рекомендаций исследования в деятельности организаций при решении задач по управлению рисками и обеспечению экономической безопасности, ориентированных на проблематику функционирования организаций в цифровом контуре. Предложенный методический подход к идентификации цифровых рисков, сформулированная взаимосвязь между цифровыми рисками и бизнес-процессами, а также предложенный метод оценки цифровых рисков позволят организациям модернизировать текущую, во многом традиционную систему управления рисками. Предложенные направления использования метода анализа среды функционирования для количественной оценки цифровых рисков и определения эффективности мер кибербезопасности организаций могут быть использованы в рамках совершенствования системы управления рисками при обеспечении экономической безопасности.

Методология и методы исследования. Методологическую основу исследования составляют научные труды российских и зарубежных ученых по теории управления рисками и теории обеспечения экономической безопасности, в том числе безопасности кредитных организаций, по вопросам цифровизации экономики и банковского сектора, включая теоретические и практические аспекты цифровой трансформации бизнес-моделей кредитных организаций, а также нормативные документы, регулирующие деятельность банковской системы Российской Федерации. В рамках проведения исследования применялись метод системного анализа, сравнительного анализа, метод анализа и синтеза, методы структурного и факторного анализа, а также специальные методы экономико-математического анализа, включая непараметрический метод сравнительной оценки эффективности – метод анализа среды функционирования в качестве инструмента оценки, прогнозирования и митигации цифровых рисков.

Информационную базу исследования составили законодательные нормы регулирования деятельности кредитных организаций, в том числе нормативные и рекомендательные документы Банка России, аналитические отчеты, обзоры Банка России, системно значимых кредитных организаций, данные Федеральной службы государственной статистики. Также использованы данные зарубежных источников, в том числе документы рекомендательного характера Базельского комитета по банковскому надзору, аналитические отчеты консалтинговых и рейтинговых агентств, проводящих исследования в области банковского сектора.

Научная гипотеза исследования. Цифровизация бизнес-процессов организации определяет появление цифровых рисков, влияющих на экономическую безопасность организации, а также формирует потребность в разработке новых инструментов ее обеспечения.

Научная новизна исследования состоит в разработке теоретико-методических положений по идентификации, оценке и митигации цифровых рисков при обеспечении экономической безопасности организации.

Положения, выносимые на защиту:

1) Для условий цифровизации экономики определена взаимосвязь между экономической безопасностью организации и системой управления рисками как инструментом ее обеспечения. Эта взаимосвязь определяется включением в контур экономической безопасности организации опасностей и угроз, возникающих в связи с трансформацией бизнес-моделей под воздействием цифровых технологий, что позволяет формировать релевантные направления реагирования, включающие комбинацию традиционных и новых методов и способов митигации рисков (С. 38–41; 50–51).

2) Определены особенности регулирования бизнес-процессов кредитной организации в условиях их осуществления в цифровом пространстве, а также предложено распределение рисков, связанных с цифровизацией, по основным и вспомогательным бизнес-процессам, в том числе рассмотрен риск передачи бизнес-процессов на аутсорсинг. В отличие от существующих, представленные положения направлены на расширение институциональных норм, связанных с управлением операционными рисками в кредитных организациях. Это позволяет кредитной организации определить виды рисков, митигация которых должна проводиться в приоритетном порядке (С. 57–70).

3) Предложена расширенная трактовка категории «цифровой риск», включающая в себя определение понятий «цифровой риск» и «митигация цифрового риска», выявление причин возникновения цифровых рисков, определение видов и подвидов цифровых рисков, идентификацию цифровых рисков согласно выделенному перечню бизнес-процессов, определение риск-статуса цифровых рисков, а также структуризацию методов оценки цифровых рисков в зависимости от вида риска, что позволяет сформировать теоретическую основу для разработки практического инструментария управления цифровыми рисками при обеспечении экономической безопасности организации (С. 99–100; 102–113).

4) Разработаны методические рекомендации по оценке и минимизации цифровых рисков организации, включающие алгоритм оценки цифровых

рисков организации и оценку эффективности мер обеспечения экономической безопасности на основе метода анализа среды функционирования. Предложенные рекомендации позволяют интегрировать двойную природу традиционных и цифровых рисков в процесс оценки рисков и принятия решений за счет идентификации любого количества входных и выходных переменных бизнес-процессов организации в формате дополнительных нежелательных факторов, а также определить эффективность системы управления рисками цифрового контура организации (С. 114–115; 118–146).

5) Разработаны практические рекомендации по минимизации цифровых рисков и развитию системы обеспечения экономической безопасности кредитной организации: предложен трехступенчатый алгоритм управления цифровыми рисками кредитной организации, предполагающий использование метода анализа среды функционирования; разработан комплексный подход к организации процесса митигации цифровых рисков и последующего обеспечения экономической безопасности кредитной организации на основе построения цифровой линии защиты и применения инновационных решений для управления цифровыми рисками. Разработанные рекомендации позволяют в трехмерной системе объект-риск-средство защиты («куб безопасности») осуществлять идентификацию, оценку и митигацию цифровых рисков при реализации практических действий по обеспечению экономической безопасности кредитной организаций (С. 149–175).

Степень достоверности, апробация и внедрение результатов исследования. Достоверность исследования обеспечивается использованием методов научного познания в исследовании, достоверных статистических данных, научных трудов отечественных и зарубежных ученых, полнотой анализа и практической проверкой результатов исследования.

Результаты исследования представлялись и обсуждались на следующих научно-практических мероприятиях: на Научно-практическом семинаре «Современные формы устойчивого развития социально-экономических систем» (Москва, Государственный университет управления,

17 февраля 2022 г.), на IV Всероссийской научно-практической конференции «Финансы и корпоративное управление в меняющемся мире» (Москва, Финансовый университет, 29 сентября 2022 г.), на 9-ой Международной студенческой научно-практической конференции «Анализ социально-экономического состояния и перспектив развития Российской Федерации» (Москва, Государственный университет управления, 6 декабря 2022 г.), на XXX Международной конференции студентов, аспирантов и молодых ученых «Ломоносов» (Москва, Московский государственный университет имени М.В. Ломоносова, 14–20 апреля 2023 г.), на IV Международной научно-практической конференции «Теоретические и прикладные вопросы экономики, управления и образования» (г. Пенза, Пензенский государственный аграрный университет, 13–14 июня 2023 г.), на X Всероссийской научно-практической конференции «Проблемы управления, экономики и права в общегосударственном и региональном масштабах» (г. Пенза, Пензенский государственный аграрный университет, 13–14 сентября 2023 г.), на XVIII Международной научно-практической конференции молодых ученых, студентов и магистрантов, посвященной памяти выдающегося экономиста В.Д. Новодворского «Стратегия устойчивого развития и экономическая безопасность страны, региона, хозяйствующих субъектов» (г. Барнаул, Финансовый университет, Алтайский филиал, 14 декабря 2023 г.), на IV Международной научно-практической конференции «Управление, экономика и общество: проблемы и пути развития» (г. Челябинск, Челябинский государственный университет, 11 апреля 2024 г.).

Результаты исследования используются в практической деятельности «Банк ВТБ» (ПАО), в частности предложенные методические рекомендации по идентификации цифровых рисков согласно бизнес-процессам и определению риск-статуса цифровых рисков, структуризация методов оценки цифровых рисков в зависимости от типа риска, выявленные особенности трансформации бизнес-модели кредитной организации под воздействием

цифровых технологий. Используются описанные в исследовании рекомендации по оценке и минимизации цифровых рисков на основе математико-экономического метода анализа среды функционирования, позволяющие определить тип цифрового риска и выработать возможное управленческое решение по его минимизации. Сформулированные направления по улучшению бизнес-процессов в целях минимизации цифровых рисков, а также предложенный трехступенчатый алгоритм управления цифровыми рисками способствуют системному и эффективному противодействию рискам, связанным с использованием в «Банк ВТБ» (ПАО) передовых цифровых технологий, а также повышению общего уровня экономической безопасности организации.

Материалы диссертации используются Кафедрой экономической безопасности и управления рисками Факультета экономики и бизнеса Финансового университета в преподавании учебной дисциплины «Экономическая безопасность и риски» для студентов, обучающихся по направлению подготовки 38.03.01 «Экономика», образовательная программа «Экономика и бизнес».

Апробация и внедрение результатов исследования подтверждены соответствующими документами.

Публикации. Основные положения и результаты исследования отражены в 16 публикациях общим объемом 9,99 п.л. (авторский объем – 8,27 п.л.), в том числе 10 работ общим объемом 7,93 п.л. (авторский объем – 6,36 п.л.) опубликованы в рецензируемых научных изданиях, определенных ВАК при Минобрнауки России.

Структура и объем диссертации обусловлены поставленными целью, задачами и логикой исследования. Диссертация состоит из введения, трех глав, заключения, словаря терминов, списка литературы, состоящего из 204 наименований, и четырех приложений. Текст диссертации изложен на 228 страницах, содержит 34 таблицы, 36 рисунков и одну формулу.

Глава 1
Теоретические основы построения системы управления рисками как инструмента обеспечения экономической безопасности организации

1.1 Экономическая безопасность и управление рисками организации: генезис понятий и теорий

Быстрые темпы цифровизации значительно изменили ландшафт банковских услуг, использование новых технологий привело к повышению операционной эффективности, а также к возможности создания инновационных банковских продуктов в соответствии с развивающимися рыночными тенденциями и растущими потребностями клиентов. Технологические разработки также поспособствовали расширению спектра предоставляемых кредитной организацией услуг, тем самым повысив уровень инклюзивности и гибкости цифровой экосистемы. По мере того, как технологические инновации все глубже укореняются в бизнес-моделях кредитных организаций, инфраструктуре и каналах продаж банковских продуктов, растут и связанные с этим риски, влияющие, в том числе, и на уровень экономической безопасности.

Растущая тенденция к использованию технологий инициировала рост зависимости кредитных организаций от динамичной операционной среды и среды киберугроз [162], усложнились процессы управления рисками и обеспечения кибербезопасности. Цифровые технологии привели к формированию единого пространства, объединяющего приложения, платформы и ИТ-инфраструктуру. Кредитные организации активно применяют нововведения при осуществлении бизнес-операций, продвигают открытое цифровое сотрудничество, интегрируют Интернет вещей, аналитику больших данных и облачные вычисления в системы поддержки синхронного

поиска, анализа и хранения информации на одной платформе. Однако в условиях быстрого развития цифровых технологий (основные тенденции развития цифровизации рассмотрены в соавторстве с Л.В. Волковым [136]) и увеличения объема онлайн-транзакций растет и необходимость повышения экономической безопасности для обеспечения защиты финансовых данных и безопасности совершаемых сделок. В современном понимании экономическая безопасность кредитной организации представляет собой организованную систему защиты информации, счетов и средств клиентов от несанкционированного доступа или использования, то есть защиту от всевозможных рисков [82]. Стоит отметить, что традиционно обеспечение безопасности в кредитной организации включает в себя обеспечение защиты корпоративных интересов, защиту объектов кредитной организации, которая включает в себя обеспечение информационной безопасности, обеспечение безопасности участников банковской экосистемы (для крупных кредитных организаций), обеспечение экономической безопасности (мониторинг бизнес-подразделений, например, по расчетно-кассовому обслуживанию).

С учетом обозначенной выше тенденции к повсеместному росту цифровых технологий организация безопасности на каждом из представленных уровней связана с обеспечением защиты информации, передаваемой цифровым путем [156], именно от этого в наибольшей степени зависит уровень экономической безопасности в современной кредитной организации. С ростом цифровых технологий значительно сократился период воздействия рискового события на доходы кредитной организации. Так, например, мошенники, используя фишинговые сайты, все быстрее обходят протоколы защиты данных, и системы информационной безопасности кредитных организаций зачастую не успевают обнаружить их до перевода средств на счета злоумышленников. Существует следующий ряд мер и рекомендаций для обеспечения и поддержания высокого уровня экономической безопасности в кредитной организации с учетом перевода большей части процессов в цифровой контур:

а) «Многофакторная аутентификация подтверждения личности клиентов, подразумевающая использование сложных паролей, кодов подтверждения, биометрических данных (например, сканера отпечатков пальцев) и других способов подтверждения личности» [141].

б) «Шифрование данных для защиты информации о клиентах и транзакциях, на основе которого может быть предотвращен несанкционированный доступ к конфиденциальным данным» [141].

в) «Методы мониторинга и обнаружения аномалий, за счет которых можно выявлять подозрительную активность на ранних стадиях взаимодействия какой-либо части структуры кредитной организации (как внутренней, так и внешней) с программным обеспечением, людьми (клиентами, контрагентами) и всевозможными цифровыми каналами. Использование данных методов позволяет кредитным организациям оперативно реагировать на потенциальные угрозы безопасности» [141].

г) «Регулярные тренинги и обучение персонала кредитной организации в области безопасности, которые повышают осведомленность сотрудников о возможных рисках и угрозах, возникающих вследствие их невнимательности, либо неосведомленности в результате осуществления рабочей деятельности. При проведении обучения необходимо делать упор на соблюдение требований, касающихся информационной безопасности» [141]. Важность обеспечения информационной безопасности затрагивает, к примеру, Н.В. Щербакова, отмечающая, что «нарушения информационной безопасности влекут финансовые и репутационные потери кредитной организации» [171].

д) «Обновление программного обеспечения и операционных систем в целях устранения выявленных уязвимостей и предотвращения возможных атак на технологическую среду кредитной организации» [141].

е) «Сотрудничество с внешними партнерами кредитной организации в части обеспечения безопасности, в первую очередь специализирующимися на обеспечении бесперебойной работы информационных систем кредитной

организации, так как в данных системах содержится конфиденциальная информация о контрагентах, клиентах, договорных и первичных документах (доступ к такой информации со стороны злоумышленников приведет к большим финансовым и репутационным потерям)» [141].

Кроме того, регулярное обновление и аудит безопасности систем также являются важными мерами для повышения экономической безопасности в банковской сфере [109]. Кредитные организации должны постоянно следить за новыми тенденциями в области кибербезопасности и применять соответствующие меры для защиты своих клиентов и собственных активов от потенциальных угроз [138].

Влияние рисков, которые являются неизбежным сопутствующим фактором деятельности любого хозяйствующего субъекта, стало более значимым с развитием науки и технологий, ужесточения и ускорения действия негативных факторов внешней среды. В экономической литературе известны различные подходы к определению сущности риска кредитной организации, которую можно описать и как опасность, и как вынужденный образ действий в условиях неопределенности, ведущий в конечном результате к преобладанию успеха над неудачей. Исследователи также отмечают особую важность системы управления рисками в кредитных организациях [94]. В классических концепциях понимания рисков, в том числе в контексте обеспечения безопасности, экономисты оперируют понятием «ожидаемой ценности», которое включают сумму всех возможных положительных или отрицательных результатов, умноженную на их соответствующие вероятности. Основой таких концепций является исследование, проведенное Фрэнком Найтом в 1920-е годы, разделившим риск, который можно измерить и которым можно управлять, и неопределенность, которую невозможно измерить и которой невозможно управлять [194]. В дальнейшем исследования по управлению рисками в финансах провел Гарри Марковиц, в 1950-х годах разработавший концепцию современной портфельной теории и определивший эффективную границу, которая является графическим представлением

компромисса между риском и доходностью для набора инвестиционных инструментов [196]. Для исследования систем безопасности кредитной организации интересны и результаты исследования Дональда Кресси, в 1950-х годах разработавшем теорию «треугольника мошенничества» [184]. Д. Кресси утверждает, что мошенничество происходит, когда у человека есть мотив, возможность и схема его совершения. Таким образом, в экономической литературе создан достаточно сильный базис для оценки цифровых рисков, как с точки зрения психологии мошенников, так и с позиций определения вероятности убытков.

Теоретически банковский бизнес включает в себя несколько различных видов деятельности, но общая классификация рисков основана на традиционной банковской деятельности и традиционных операциях кредитной организации. На практике банковская деятельность создает множество уникальных рисков, естественным образом возникающих в результате ее осуществления. Эти риски связаны и с некорректным определением платежеспособности клиента, и возникающим вследствие такой операции кредитования риском утраты ликвидности, платежеспособности, а также риском недополучения доходов. Уникальность природы рисков для каждой кредитной организации будет обосновываться выбранными направлениями стратегии развития кредитной организации, общей концепцией достижения конкурентоспособности на рынке, а также согласованностью системы управления рисками [120]. Классификация рисков кредитной организации достаточно широко представлена в научной литературе и нормативных актах [3; 12; 21; 150], однако остаются не до конца раскрытыми специфичные виды рисков кредитных организаций, связанные с цифровизацией, являющиеся наиболее актуальными в современных условиях.

Информационные технологии (в частности искусственный интеллект [76; 136]) проникают в банковский сектор, делая его более мобильным и гибким. Меняются потребности и предпочтения клиентов, способы предоставления услуг. На рынок финансовых услуг выходят ИТ-компании,

предлагающие традиционные банковские продукты в новом, современном формате, с которыми кредитным организациям приходится конкурировать в достаточно агрессивной внешней среде. Кредитным организациям приходится вкладывать огромные средства в разработку инноваций, чтобы оставаться востребованными. Все это требует изменения как способов предоставления своих услуг и общения с клиентами, так и формирования новой корпоративной культуры, качественной перестройки операционных процессов, методов и подходов к их управлению, включая процессы обеспечения экономической безопасности [122; 131]. Согласно Доктрине информационной безопасности Российской Федерации, «организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка» [16] являются важными участниками системы обеспечения информационной безопасности России. Кредитным организациям важно трансформировать бизнес-модель с учетом всевозможных многогранных рисков. Необходимость такой трансформации также подтверждается и усилением вероятности возникновения рисковых событий именно в современных российских реалиях.

Риски кредитной организации в цифровом пространстве зачастую разделяются исследователями на две категории: риск безопасности данных и риск кибербезопасности [153]. Кибербезопасность и безопасность данных тесно связаны между собой, поскольку направлены на обеспечение защиты информационного контура кредитной организации от утечки информации. Эксперты следят за активностью в цифровом пространстве, чтобы при необходимости принять меры против постоянных активных угроз, а также угроз повышенной сложности. Стоит отметить, что под цифровым пространством автор понимает «виртуальную среду, созданную взаимосвязанными цифровыми устройствами, сетями и Интернетом. Это нематериальная область, в которой накапливается цифровая информация, контент, история взаимодействия и операций» [141]. Безопасность данных в цифровом пространстве предполагает защиту информации, предоставленной клиентом (личные данные, данные доступа, данные подтверждения,

авторизации и аутентификации личности). Меры безопасности направлены на обеспечение конфиденциальности и целостности банковских операций, они формируются в том числе за счет управления рисками, связанными с цифровизацией, особую актуальность приобретают вопросы обеспечения кибербезопасности [114].

Основные типы рисков, с которыми сталкиваются кредитные организации в цифровом пространстве, идентичны традиционным банковским рискам за некоторым исключением. Во-первых, растут *риски, связанные с платежными онлайн-системами*. По типу оплаты платежные системы онлайн делятся на:

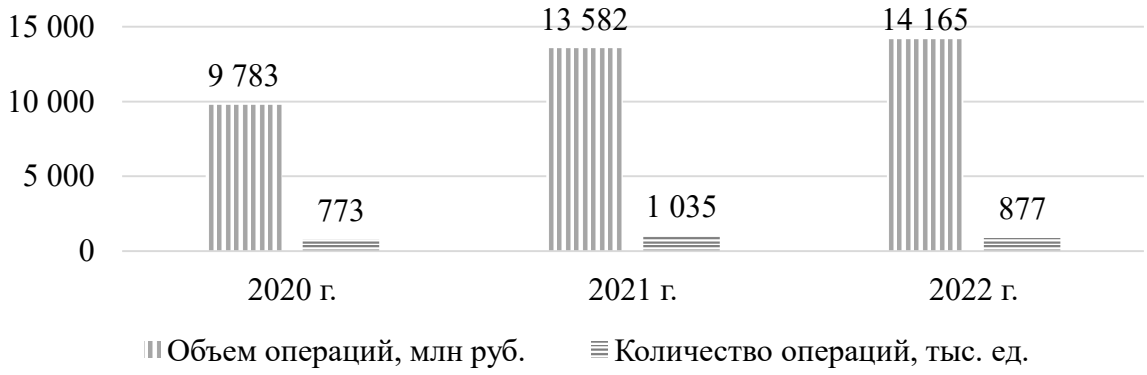
а) Карточные платежные системы — оплата производится банковскими картами в сети Интернет на сайте продавца товаров или услуг [63].

б) «Операторы цифровой наличности — оплата в сети Интернет производится так называемой цифровой наличностью или электронными деньгами, разновидностью внутренней валюты, которую можно обналичить у соответствующих участников электронной платежной системы (например, Яндекс.Деньги)» [63], что отмечено на интернет-портале «TAdviser.ru».

в) «Платежные шлюзы представляют собой синергию карточных систем и операторов цифровой наличности, предоставляя широкие возможности для взаимной конвертации и способов оплаты товаров и услуг в сети Интернет» [63], что также отмечают исследователи «TAdviser.ru».

Стремительный рост поставщиков платежных услуг увеличивает риск преступлений, связанных с цифровыми платежами. Недостаточная защищенность операций по проведению платежей на многих электронных платформах инициирует рост риска мошенничества. Кроме того, в России действует система санкций на финансовые услуги. В 2022 году ключевые западные поставщики финансовых услуг, включая Mastercard, Visa, Apple Pay, Samsung Pay и PayPal [26], приостановили свою деятельность на территории страны, в связи с чем высокую актуальность приобрело развитие отечественных платежных систем. Система Быстрых Платежей (далее – СБП)

относится к наиболее защищенным системам платежей онлайн в России, поскольку валовые расчеты в реальном времени контролируются Банком России. Они относятся к операциям с низким риском мгновенного платежа, а также возможностью осуществления крупных транзакций с минимальной вероятностью сбоя. Кроме того, в России действует внутренняя платежная система банковских карт «Мир», управляемая Национальной системой платежных карт. По данным обзора Банка России, опубликованном в феврале 2023 года, «в 2022 году в России зафиксировано около 877 тыс. случаев хищения средств с банковских счетов, что на 15,3% меньше, чем годом ранее. Количество хищений средств с российских банковских счетов сократилось впервые за 7 лет, при этом размер ущерба от действий мошенников в 2022 году увеличился на 4,3%, до 14,2 млрд рублей» [37], что показано на рисунке 1. «Большая часть ущерба связана с дистанционным банковским обслуживанием, он составил 9,3 млрд рублей в 2022 году» [37] (исследователи также подчеркивают необходимость тщательного контроля за процессами дистанционного банковского обслуживания в контексте обеспечения безопасности кредитных организаций [170]).

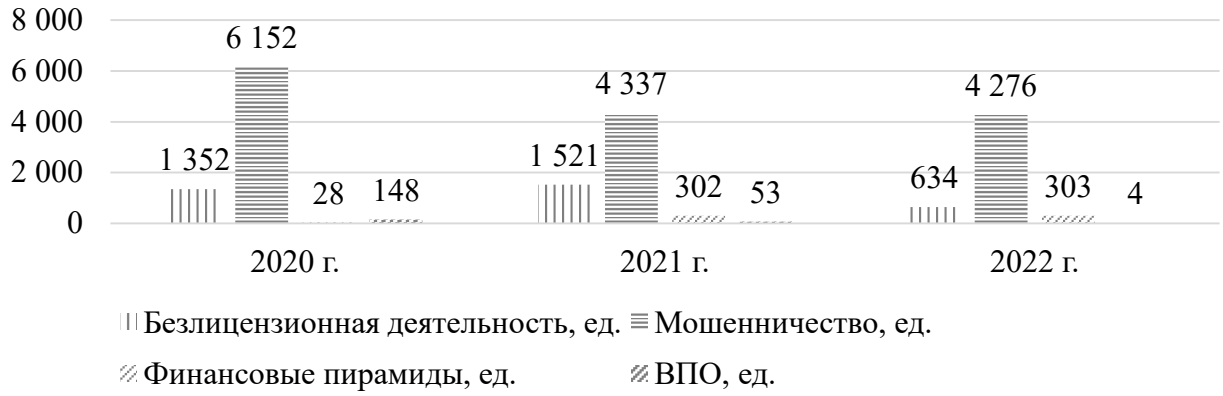


Источник: составлено автором по материалам [38; 39].
Рисунок 1 – Динамика операций без согласия клиентов в 2020–2022 гг.

Во-вторых, растет *кредитный риск*. Включение в цифровую кредитную платформу множества компаний дало толчок цифровому кредитованию от нефинансовых организаций, нерегулируемых центральными банками, тем самым повышая риск невыплат по кредитам.

Операционный риск связан с людьми, процессами, системами и процедурами, а также с внутренним мошенничеством и мошенничеством извне. Электронные банковские системы разных уровней и типов уязвимы с точки зрения безопасности, системы, дизайна, внедрения и обслуживания.

Риск необеспечения безопасности возникает, когда фишинговые сайты получают доступ к банковскому контуру, извлекают и используют конфиденциальную информацию клиентов, средства управления критически важными системами учета и управления рисками кредитной организации при этом находятся под угрозой. Третьи лица, получающие доступ к информационным системам кредитной организации, с помощью вредоносных программ завладевают всевозможной информацией о кредитной организации и его клиентах. Р.Г. Нафиков в работе по анализу процессов цифровизации банковской системы отмечает, что «поскольку цифровизация развивается очень быстро, велики риски появления в программе ошибок, связанных с автоматизацией различных процессов внутри банков. С целью быстрого устранения возможных проблем цифровые системы необходимо регулярно мониторить» [128]. Объем распространения фишинговых сайтов в России также находится на высоком уровне, что нашло свое отражение на рисунке 2. Как отмечает Н.В. Алексеева в работе по анализу киберпреступлений в банковской сфере России, в 2022 году Банк России выявил информацию о «5 217 ресурсах с целью последующего снятия их с делегирования, что на 16% меньше, чем в 2021 году (6 213 ресурсов)» [70]. Также исследователь отмечает, что «с февраля 2022 года Банк России начал заниматься деятельностью по блокировке страниц (групп) в социальных сетях и компьютерных (мобильных) программах, размещенных в цифровых магазинах приложений, которые злоумышленники использовали для распространения аналогичной (вредоносной) информации. В период с 28 февраля по 31 декабря 2022 года Банк России инициировал ограничение доступа к 1 942 страницам (группам) в социальных сетях и к 23 приложениям» [70].



Источник: составлено автором по материалам [38; 39].
Рисунок 2 – Мошеннические Интернет-ресурсы, направленные регистраторам доменных имен (в единицах) в 2020–2022 гг.

Также Н.В. Алексеева пишет, что «в 2022 году количество ресурсов, к которым был ограничен доступ на основании сведений Банка России, составило 10 716 единиц, что более чем в три раза превышает показатель 2021 года (3 100 ресурсов). Как и в 2021 году, основная часть ресурсов (34%), по которым было инициировано принятие мер со стороны Банка России, использовалась злоумышленниками для осуществления безлицензионной деятельности в сфере рынка ценных бумаг, а также для рекламирования деятельности несуществующих кредитных, микрофинансовых и страховых организаций» [70]. «12% составили ресурсы из категории «Фишинг», которые маскировались злоумышленниками под сайты действующих организаций финансовой сферы. Менее 1% пришлось на ресурсы, распространяющие вредоносное программное обеспечение» [70].

Следующий тип риска связан *с мошенничеством со стороны сотрудников*. Сотрудники могут получить различную информацию о клиентах или украсть данные по осуществлению входа в банковские системы [99]. Стоит заметить, что кредитные организации, сталкивающиеся с перебоями или замедлением работы существующих систем из-за отсутствия совместимых требований, нуждаются во внешних поставщиках услуг. Наемные специалисты поддерживают часть деятельности, то есть кредитные организации допускают аутсорсинг операций, которые они не могут

обеспечить самостоятельно, подвергая себя дополнительным операционным рискам и возможной утечке информации.

Риск низкой квалификации кадров связан с тем, что быстро меняющиеся технологии представляют собой проблему для банковских служащих, поскольку сотруднику может потребоваться время, чтобы разобраться в основах функционирования технологии, в связи с чем возникает рост возможности операционных ошибок.

Клиентский риск возникает, когда клиенты не следуют банковским инструкциям. Например, они вводят личную информацию на фишинговых сайтах, что позволяет преступникам получить доступ к их счетам.

Репутационный риск возникает в результате низкого уровня обслуживания кредитной организацией клиентов, выявления фактов мошенничества и коррупции. Потеря доверия клиентов к кредитной организации может привести к потере сегментов бизнеса, увеличению проблем с ликвидностью, а также может привести к клиентскому оттоку. В некоторых случаях репутационный риск можно связать и с развитием экосистемы кредитной организации. Под экосистемой (цифровой экосистемой) кредитной организации автор понимает коммерческий альянс (соглашение или иные законные и юридические формы сотрудничества) между кредитной организацией и ее коммерческими партнерами, не относящимися к банковскому сектору. Так, в случае с наиболее динамично развивающейся российской экосистемой ПАО «Сбербанк России» [85] был открыт Сбермегамаркет. Утрата конкурентных позиций (например, в сравнении с Озон или Яндекс.Маркет) по продажам в этом сервисе может нанести кредитной организации непоправимый репутационный ущерб, поскольку в экосистеме сохраняется единое имя бренда.

Следующий тип риска, повышение уровня которого связано с внедрением цифровых технологий – *юридический риск*. Несоблюдение нормативных руководящих принципов (политик), а также законодательных требований, к примеру, при внедрении нового технологического продукта

(процесса) без надлежащего тестирования, при отсутствии плана по снижению рисков на случай неуспешной реализации технологического изменения или плана контролируемых действий для новейших продуктов может привести к соответствующим юридическим рискам.

Значимой проблемой также является *недостаточно разработанная стратегия*, направленная зачастую именно на предотвращение рисков (при наихудших вариантах формирования стратегии ожидаемые риски практически не учитываются). Особое внимание к стратегическим рискам наблюдается в таких областях, как разработка продуктов, продажи и банковская культура, в связи с чем проходят регулярные внутренние аудиты для последующего выявления недочетов в управлении.

Ориентация банковского менеджмента на современные технологии и выявленные новые виды рисков, отраженные на рисунке 3, позволят кредитной организации успешно трансформировать бизнес-модель.

Источник: составлено автором.
Рисунок 3 – Риски кредитной организации в цифровом пространстве

Цифровой банкинг несомненно открывает множество привлекательных возможностей как для кредитной организации, так и для клиентов [149]. Необходимость выстраивания процессов управления рисками в цифровом банкинге также возрастает (в том числе и в контексте обеспечения экономической безопасности [89]). Управление рисками позволяет уменьшить как вероятность возникновения риска, так и его потенциальное воздействие. Оно включает в себя идентификацию, анализ и реагирование на факторы-триггеры риска. Эффективное управление рисками означает, что

организация процессов управления направлена на то, чтобы максимально полно контролировать будущие результаты, при этом действуя упреждающе.

Под системой управления рисками в кредитной организации автор понимает процессы выявления, оценки и принятия кредитной организацией мер по снижению вероятности негативных последствий принятия операционных и / или инвестиционных решений. Риск-ориентированный подход предполагает, что кредитная организация осуществляет выявление и оценку рисков, после чего применяет соответствующие меры для их минимизации в зависимости от уровня риска. Этот подход играет особенно важную роль в противодействии рискам, связанным с отмыванием денег, финансированием терроризма, коррупцией и взяточничеством [167]. Формирование системы управления рисками в кредитной организации может проходить в шесть этапов:

а) *Идентификация*: определение характера рисков, в том числе источника их происхождения, и причин, по которым они представляют угрозу для кредитной организации.

б) *Оценка и анализ*: определение вероятности того, что риск может стать угрозой для кредитной организации, а также оценка потенциальной серьезности этой угрозы. На этом этапе организация проводит ранжирование рисков по приоритетности.

в) *Смягчение последствий:* создание и реализация банковских политик и процедур, направленных на снижение вероятности возникновения рисков и минимизацию ущерба, который могут причинить потенциальные угрозы.

г) *Мониторинг*: сбор данных о предотвращении угроз и реагировании на инциденты для определения того, насколько хорошо работает стратегия управления рисками. Деятельность на данном этапе также включает в себя исследование новых тенденций в области рисков для определения того, нуждается ли (или потребуется) в обновлении система управления рисками кредитной организации [8; 9; 10].

д) *Сотрудничество*: установление взаимосвязей между рисками и стратегиями их снижения в различных областях деятельности кредитной организации для создания более централизованной и скоординированной системы реагирования на угрозы.

е) *Отчетность*: документирование и проверка информации, связанной с деятельностью кредитной организации по управлению рисками, для оценки их эффективности. Также используется для отслеживания изменения общего профиля рисков кредитной организации с течением времени.

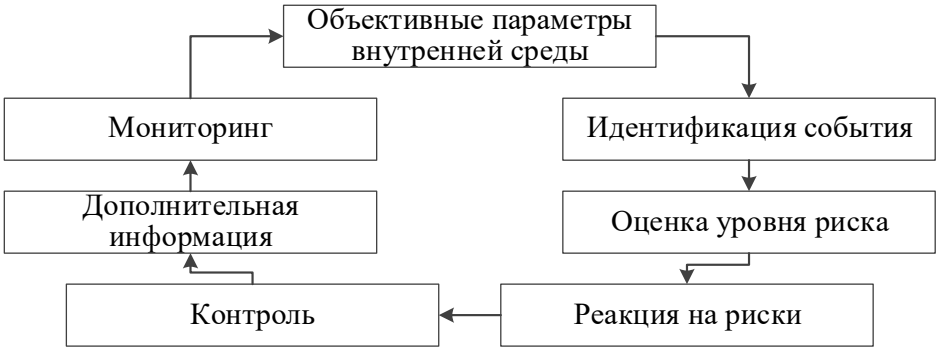
В научной литературе теоретические аспекты управления рисками кредитной организации рассматривались в трудах В.И. Авдийского, В.Н. Алферова, В.М. Безденежных, Е.В. Караниной, В.И. Лобанова, Н.Г. Синявского, В.Г. Старовойтова, Н.В. Старовойтова, К.Н. Тутовой, Е.Б. Чернобровкиной и других. Исследования ученых можно сгруппировать по следующим признакам:

а) Подходы к формированию этапов управления рисками формулируется и описывается в трудах В.И. Авдийского, В.М. Безденежных, Н.Г. Синявского [1; 65; 78; 79; 80; 155].

б) Формирование стратегий, подходов и методов к управлению рисками, в том числе в банковском секторе отражено в трудах В.Н. Алферова, Е.В. Караниной, В.И. Лобанова; К.И. Тутовой [72; 116].

в) Формирование рекомендаций для регулятора – Банка России в концепте выявленных рисков банковского сектора и мероприятий по повышению экономической безопасности банковского сектора страны отражено в трудах В.Г. Старовойтова, Н.В. Старовойтова, Е.Б. Чернобровкиной [158; 165].

В работах исследователей прослеживается мысль о том, что одним из ключевых аспектов управления рисками является цикличность описанного процесса — этапы связаны друг с другом как организационно, так и функционально, что отражено на рисунке 4.



Источник: составлено автором по материалам [5].

Рисунок 4 – Взаимосвязь элементов системы управления рисками организации

Стоит заметить, что каждый из обозначенных этапов управления рисками, связанный с оценкой, сбором информации, проведением мониторинга и анализом, может быть улучшен с использованием современного технологического банковского и FinTech-инструментария.

В.М. Безденежных отмечает, что «система управления рисками организации пронизывает всю управленческую структуру. Это позволяет комплексно регулировать риски, в том числе проводить идентификацию и оценку, риск-мониторинг, а также постоянную модернизацию и улучшение методической основы управления рисками. Риск-ориентированный подход в управлении определяет ответственность (и полномочия) владельцев риска одним из ключевых условий эффективного управления» [78]. Также исследователь отмечает, что «по существу нет кроме системы управления рисками других механизмов, с необходимой эффективностью обеспечивающих экономическую безопасность организаций» [80]. Ученый также делает вывод «об ограниченной рациональности принимаемых решений в политике и экономике на всех уровнях сложной социально-экономической системы от мега- до микроуровня. Это порождает повышение рискогенности принимаемых стратегий и тактик развития, соответственно, важность активного развития риск-ориентированного подхода. Это требует широкого профессионального освоения и применения риск-ориентированного подхода в построении моделей анализа современной экономики, методов оценки, снижающих субъективность при принятии и реализации управляющих воздействий» [79].

В.И. Лобанов и Е.В. Каранина отмечают, что «риск-ориентированный подход, учитывающий на федеральном и региональном уровне, а также на уровне хозяйствующих субъектов критерии и индикаторы, выявляющие факторы экономических рисков в государстве, является важным направлением внедрения, использования и развития цифровых технологий и инструментов управления социально-экономической безопасностью» [116]. Также исследователи делают вывод, что «индустрия 4.0, или четвертая промышленная революция, отличительными чертами которой являются слияние цифровых технологий и технологий физического мира, образование из киберфизических комплексов цифровых экосистем, характеризуется быстрым развитием» [116]. Отмечают, что «помимо возникновения огромного количества возможностей экспоненциальный темп четвертой промышленной революции создает большое количество рисков. В таких условиях система управления ими на всех уровнях активно развивается» [116].

Структура управления рисками, сформированная на данных динамики статей баланса, движения денежных потоков и финансовых результатов по типам операций кредитной организации может быть использована для оценки неопределенности и ее влияния на банковские операции. Эффективное управление балансом можно осуществлять с помощью современных аналитических систем по планированию бюджета, а также прогнозных моделей изменения показателей ликвидности активов, определения источников риска и отслеживания временных границ долговых обязательств.

Управление денежными потоками возможно за счет применения прогностических аналитических моделей и современных методов начисления заработной платы, погашения долговых обязательств клиентами, а также отслеживания их платежей. Инвестиционные денежные потоки можно регулировать путем принятия решений на основе автоматизированных аналитических исследований. Архитектуру построения банковской отчетности о рисках можно переложить на современное программное обеспечение. Для того чтобы кредитная организация была готова к

чрезвычайным ситуациям, следует также использовать прогнозные модели, которые помогут определить те вводные, при которых риск потери ликвидности наиболее высок. Также для эффективного управления ликвидностью кредитной организации необходимо модернизировать системы управления денежными средствами, инвестиционными потоками, а также авансами и ссудами. Потенциальные риски могут возникать из различных источников [126], инструментарий, используемый в рамках управления рисками, должен быть максимально широким.

Прочие типы рисков, в частности комплаенс-риск, налоговый риск и регуляторный риск также могут быть подвержены контролю со стороны кредитной организации путем применения современных технологий, так как данные типы риска можно отслеживать с помощью расчета аналитических показателей. В части контекста верификации комплаенс-риска стоит отметить, что комплаенс-контроль и внутренний контроль кредитной организации – это разные понятия [176]. Ю.В. Каприян и И.В. Толмачева в статье о корреляции комплаенс и внутреннего контроля на уровне коммерческих и кредитных учреждений отмечают, что «в соответствии с рекомендациями Базельского комитета по банковскому надзору комплаенс-контроль и внутренний контроль должны быть отдельными функциями, выполняемыми разными подразделениями. Внутренний контроль по своим функциям шире, чем комплаенс-контроль. Комплаенс-контроль – это проверка на соответствие требованиям, а внутренний контроль – проверка всех направлений деятельности организации на предмет эффективности, дальнейшего развития, выработки различных концепций и политик» [102]. Также авторы делают вывод, что «комплаенс-контроль реализуется с целью предупреждения комплаенс-рисков, а внутренний контроль проверяет уже завершенное, фактически реализованное событие» [102].

В.Н. Алферов и К.Н. Тутова в своей работе по управлению рисками как инструмента обеспечения устойчивости кредитной организации обозначают, что «кризисные явления в кредитных организациях накладывают ограничения

на их возможности в сфере кредитования и оказывают значительное влияние на выполнение ими своих обязательств и осуществление банковских операций. В таких экономических условиях вопросы формирования эффективной системы управления рисками в кредитных организациях становятся все более значимыми и актуальными» [72]. Также исследователи выделяют определенные методики управления рисками. Например, правило четырех глаз, при котором любое решение в рамках операционной деятельности подвержено нескольким уровням контроля (минимум — двум), и исполнительный орган не может единолично принимать какое-либо решение, что позволяет избежать финансовых рисков (растрата, нецелевое использование средств), а также злоупотребления служебным положением со стороны исполнительного органа [72]. В том случае, когда ни один процесс в рамках осуществления управления рисками не зависит от одного человека, риск возникновения ошибок уменьшается.

Также В.Н. Алферов и К.Н. Тутова рассматривают формирование системы управления рисками кредитной организации в формате четырех линий защиты [72]. Большинство российских кредитных организаций имеют несколько линий защиты, чаще всего три: операционные подразделения, чья деятельность непосредственно связана с рисками; подразделение по управлению рисками; подразделение внутреннего аудита. Исследователи предлагают внедрить четвертую линию защиты, которую будут представлять внешние независимые аудиторы, либо представители мегарегулятора — Центрального банка [72]. В.Н. Алферов и К.Н. Тутова отмечают, что «появление четвертого элемента (линии) защиты будет способствовать подтверждению эффективности системы внутреннего контроля со стороны внешнего аудитора и стимулировать ее постоянные улучшения. Включение регулятора в четвертую линию защиты позволит сформировать представление о недостатках в системах внутреннего контроля и управления рисками и их влияния на стабильность банка в целом» [72]. В.Н. Алферов и К.Н. Тутова также делают вывод, что четвертая линия защиты может быть использована в

рамках оценки кредитного риска — внешний аудитор будет осуществлять проверку оценки кредитных рисков и давать комментарии при необходимости их перерасчета [72]. Помимо внутренних систем фрод-мониторинга предлагается внедрить также внешние независимые системы, которые с помощью собственных технологий будут предупреждать финансовые преступления, а также проводить оценку операционных, кредитных и корпоративных рисков [72].

Как правило четырех глаз, так и линии защиты, и фрод-мониторинг в современном мире новейших технологий могут быть автоматизированы, что повысит точность функционала, так как данные методики основаны на анализе, а методы и инструменты проведения такого анализа совершенствуются с каждым днем, их внедрение в процессы управления рисками повысит защиту данных всех структур кредитной организации. Также стоит отметить, что, если при формировании плана и стратегии трансформации бизнес-модели кредитной организации учитывать возможные угрозы, а также предусмотреть инструменты для устранения вероятных рисков, бизнес-модель будет устойчивой, а также эффективной.

Согласно трудам Н.Г. Синявского, выбор подходящих бизнес-моделей может привести к устойчивым конкурентным преимуществам и более высоким финансовым показателям для компаний, которые их используют [155]. Следовательно, если подходящая бизнес-модель будет устойчивой к рискам, эффективной банковской деятельности как в период стабильности, так и в кризисный период не помешают ни внешние, ни внутренние риск-факторы (триггеры).

В.Г. Старовойтов и Н.В. Старовойтов в своей работе по рассмотрению системы управления рисками и мониторинга экономической безопасности Российской Федерации обосновывают «необходимость создания системы управления рисками, которая позволяет в оперативном режиме на федеральном, региональном и отраслевом уровне выявлять вызовы и угрозы экономической безопасности, а также организационные, технологические,

логистические, правовые и иные факторы их возникновения» [158]. Показывают, что «федеральная система управления рисками позволяет развивать методы и инструменты системного анализа, имитационного моделирования динамики сложных организационно-технических и социально-экономических объектов в условиях высокой неопределенности, а также принимать решения по своевременному реагированию органов государственного и корпоративного управления на внезапно возникающие риски в экономической сфере» [158].

Анализ подходов к определению термина «риск» (в том числе проведенный в соавторстве с Л.Н. Орловой и К.А. Санниковой [143]) позволяет сделать вывод о том, что риск неразрывно связан с достижением целей организации:

– согласно национальному стандарту Российской Федерации «Менеджмент риска. Термины и определения» (аналогичен международному стандарту ISO 31000), риск представляет собой возможность негативного влияния неопределенности на достижение целей [23];

– риск как влияние неопределенности на достижение целей рассматривается и в национальном стандарте Российской Федерации «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (аналогичен международному стандарту ISO/IEC 27000) [24];

– риск как неопределенность происходящего события, которое может повлиять на достижение целей, рассматривается международной профессиональной ассоциацией «Институт внутренних аудиторов», разрабатывающей стандарты в области внутреннего аудита [193];

– Банк России определяет риск как возможность негативного влияния неопределенности на достижение целей деятельности и выполнение функций организации [53];

– Пол Хопкин – сертифицированный член Института управления

рисками (ведущая международная организация по профессиональному управлению рисками), а также бывший технический директор Института, описывает риск как событие, которое способно повлиять на цели организации [193];

– В.И. Авдийский и В.М. Безденежных отмечают связь риска с вероятностью достижения желаемого результата организации, а также отклонения от цели [1].

По данным изучения определений и элементного состава систем управления рисками кредитной организации, представленного в работах различных ученых, стоит отметить, что современное состояние цифрового пространства кредитной организации таково, что применение существующих подходов может привести к дефрагментации и утрате экономической безопасности кредитной организации, «поскольку отсутствует комплексное представление и достоверная идентификация рисков как первоначального элемента выстраивания системы управления рисками» [139] именно в контексте цифровизации.

С усиливающейся тенденцией распространения цифровых технологий темпы развития российского банковского сектора постепенно ускоряются, но увеличивается и волатильность рынка. Подходы и инструменты управления рисками трансформируются, так как традиционные модели больше не отвечают требованиям современной системы управления рисками [160]. Появляется и специфический вид риска – модельный риск. Под модельным риском можно понимать риска, который возникает, когда бизнес-модель используется для измерения количественной информации, например, стоимостных операций, и модель дает сбой или работает неадекватно и приводит к неблагоприятным результатам для организации. С точки зрения окружающего организацию цифрового пространства этот риск описывает потенциальные события, возникающие в результате использования ошибочной модели для принятия решений по цифровизации. Как отмечают эксперты McKinsey, кредитным организациям необходимо пересмотреть свои

модельные стратегии: «Им необходимо разработать и применить как эффективные краткосрочные действия, так и долгосрочный план по повышению устойчивости модели. В течение двух приоритетных временных горизонтов кредитные организации могут осуществлять скоординированные корректировки моделей, чтобы обеспечить непрерывность бизнеса в краткосрочной перспективе, одновременно анализируя потребности в разработке и переработке своих моделей и модернизируя свои системы управления модельными рисками в долгосрочной перспективе» [177].

В настоящее время кредитные организации испытывают сильное давление, пытаясь решить проблемы цифровой трансформации, связанные с автоматизацией банковских операций, с помощью инициатив, ориентированных на цифровые технологии [6; 71]. Традиционные кредитные организации построены на надежном управлении (такая надежность, по мнению автора, во многом обусловлена достаточно развитым пруденциальным регулированием), которое помогает им пройти беспрепятственный путь цифровой трансформации. Но необходимо отметить, что из-за огромного потока данных о транзакциях, продажах, маркетинге и прочих аспектах риск неосуществления безопасности будет возрастать.

Управление рисками в банковской сфере тесно связано с соблюдением нормативных требований [69], которое включает бесчисленные ресурсоемкие и подверженные ошибкам проверки документов. Технологии машинного обучения и искусственного интеллекта могут способствовать автоматизации данного процесса. Потребности кредитных организаций (в том числе в части необходимости соблюдения законодательных требований) наилучшим образом оцениваются с помощью бизнес-аналитики, данные технологии полагаются на самообучение для выполнения различных задач – они заменяют человеческий интеллект [111]. Стоит заметить, что актуальность применения подобных технологий обусловлена также возможностью разработки новых принципов определения аппетита к риску. Повышение квалификации внутри компании с помощью внешних профильных экспертов поможет кредитным

организациям соответствовать утвержденным банковским стандартам. Тестирование продуктов на основе технологических моделей на этапах их проектирования, реализации, эксплуатации и процесса проверки, а также на протяжении всего их жизненного цикла также должно быть неотъемлемой частью управления рисками.

Если говорить об определении самого понятия «риск» в контексте цифровизации, российские и зарубежные авторы в основном отмечают связь такого типа риска с технологиями, не формулируя дополнительной связи подобных рисков с достижениями определенных целей, а также не выделяя их влияния на бизнес-процессы. Например, Е.В. Янченко определяет цифровой риск как «термин, охватывающий все цифровые возможности, обусловливаемый ИКТ, автоматизацией обработки данных, автоматизацией решений» [174]. Также автор отмечает, что «к цифровым рискам приводит использование цифровых технологий» [174].

М.С. Марамыгин, Г.В. Чернова и Л.Г. Решетникова определяют группы цифровых рисков, разъясняя каждую из них (риски новых цифровых финансовых инструментов – криптоактивов, риски цифровой финансовой инфраструктуры, риски дистанционного взаимодействия, киберугрозы, риски нарушения прав человека, риски неадекватного государственного регулирования) [121], не раскрывая общего понятия термина «цифровой риск».

И.А. Аренков И.А., Я.Ю. Салихова и А.А. Сайфутдинов в работе, в которой систематизированы научные публикации по цифровой трансформации в контексте управления рисками, замечают, что в области исследования цифровых рисков делается упор именно на их категоризацию, например, на киберриски, риски утечки данных [74]. Исследователи «отмечают необходимость выявления количественной оценки рисков, характерных для цифровой экономики. Данная оценка позволит наиболее точно закладывать величину цифровых рисков в ставке дисконтирования или

денежном потоке в моделях при анализе привлекательности цифрового проекта» [74].

Е.Н. Карпова, Е.А. Чумаченко, А.А. Коновалов также отмечают процессы цифровизации, связанные с рисками: «Возрастает доля безналичных платежей, традиционные финансовые институты и инструменты трансформируются и переходят в плоскость мобильных приложений и онлайн-сервисов, стремительно развивается сфера финансовых технологий» [104]. Указывают на то, что «цифровизация несет в себе новые угрозы, в особенности в сфере противодействия отмыванию преступных доходов и финансированию терроризма» [104]. Большинство российских авторов, изучающих цифровые риски, делают упор именно на их категоризацию и классификацию, не приводя определения термина как такового [106; 123; 149; 161].

Похожая ситуация наблюдается и в исследованиях зарубежных авторов. Исследователи из Иллинойсского университета отмечают, что термин «цифровой риск» «охватывает проблемы, связанные с постоянными изменениями и возрастающей сложностью операций системы, технологий и сред угроз, связанных с кибербезопасностью, конфиденциальностью, соблюдением нормативных требований, непрерывностью бизнеса, доступностью ИКТ и управлением рисками» [190].

Э. Кост (автор многочисленных статей по кибербезопасности, эксперт компании UpGuard, занимающейся кибербезопасностью) отмечает, что «цифровой риск относится ко всем неожиданным последствиям, которые возникают в результате цифровой трансформации» [203], в своих исследованиях делает упор на типизацию цифровых рисков.

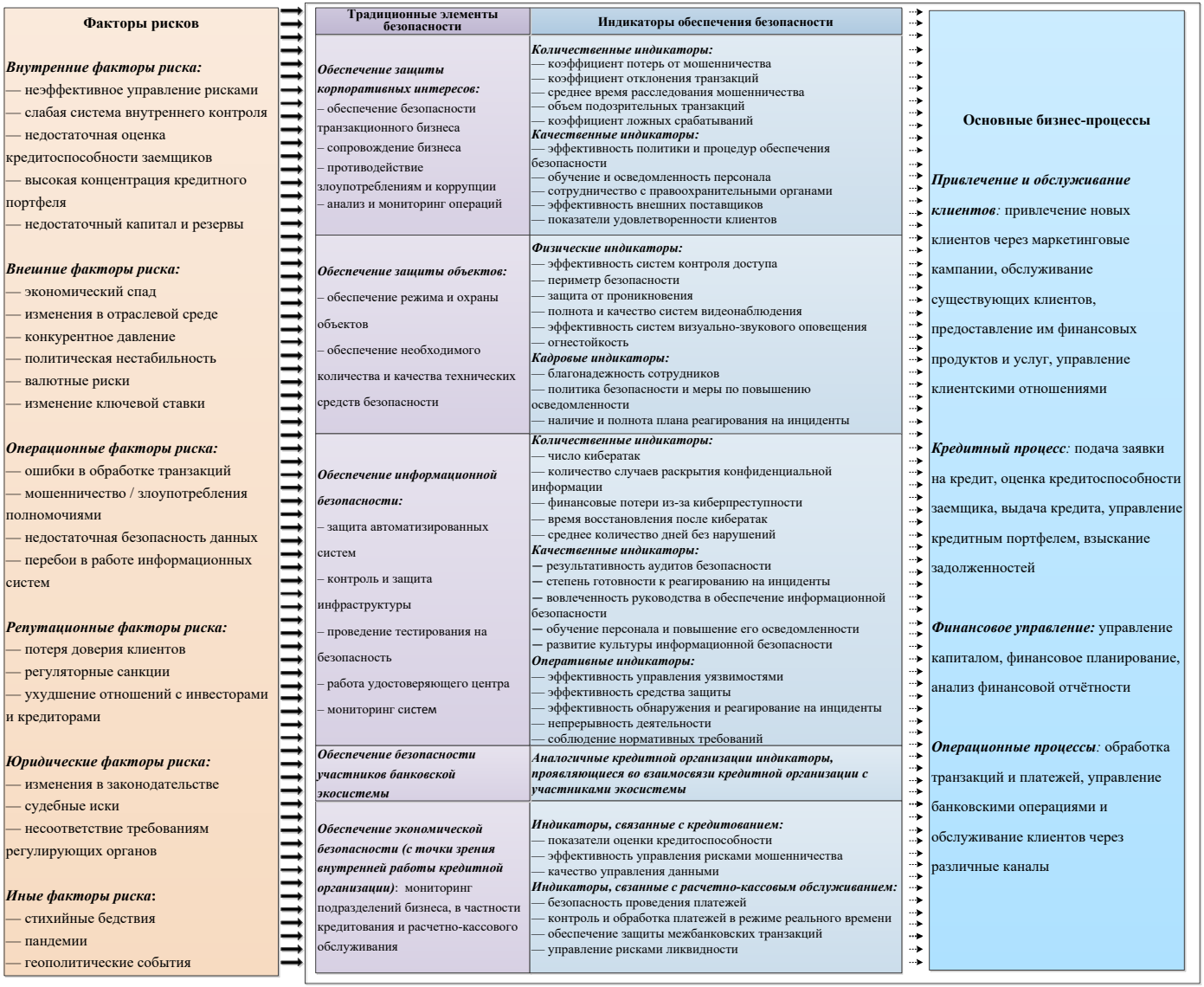
Исследователи компании Proofpoint делают вывод, что «цифровой риск в широком смысле относится к потенциальным угрозам и уязвимостям, возникающим в результате использования цифровых инструментов, платформ и технологий» [202]. Отмечают, что «оценка цифрового риска на

организационном уровне рассматривает все негативные последствия, которые могут возникнуть в результате цифровой трансформации» [202].

Авторы из консалтинговой компании McKinsey формулируют понятие «цифровой риск» как «термин, охватывающий все цифровые возможности, которые повышают эффективность управления рисками, особенно автоматизацию процессов, автоматизацию принятия решений, а также оцифрованный мониторинг и раннее предупреждение» [191], что соответствует определению, отраженному Е.В. Янченко. Таким образом, можно сделать вывод, что российские и зарубежные авторы прежде всего отождествляют «цифровой риск» именно с термином «цифровизация», а не с термином «риск», существующие подходы к формулированию понятия «цифровой риск» требуют уточнения и дополнения.

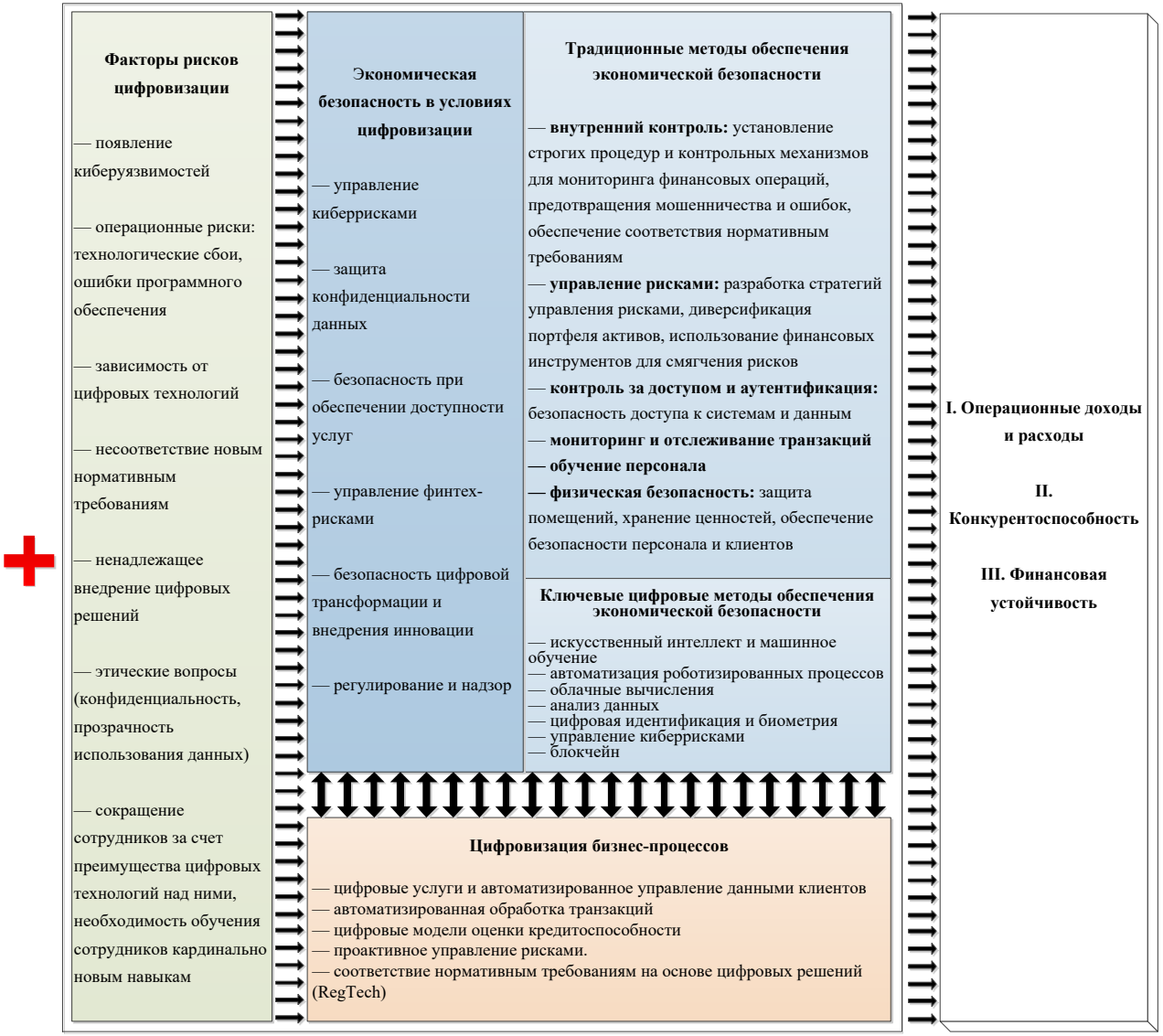
Столкнувшись с проблемами ограничения доступа к мировому финансовому рынку, организации России должны использовать новые инструменты и средства управления рисками, чтобы нивелировать дальнейшее возможное ухудшение внешней обстановки, и в максимальной степени стремиться к повышению безопасности на основе контроля уровня банковских рисков. Традиционные подходы к обеспечению экономической безопасности в организации, которые обсуждаются авторами, исследующими данную тему, в основном поверхностно охватывают стандартные элементы, составляющие деятельность по обеспечению безопасности, в том числе информационной.

С учетом возникновения новых технологий, а также сопутствующих им рисков, данная развертка может быть дополнена, как минимум, отражением новоявленных элементов, которые прочно закрепились в деятельности организаций, но несмотря на это могут быть отнесены к категории инструментов, предшествующих новейшим цифровым технологиям, и могут быть улучшены с помощью них [7], тем самым влияя на повышение кибербезопасности и снижение влияния соответствующих рисков, что нашло отражение на рисунке 5 и рисунке 6.



Источник: составлено автором.

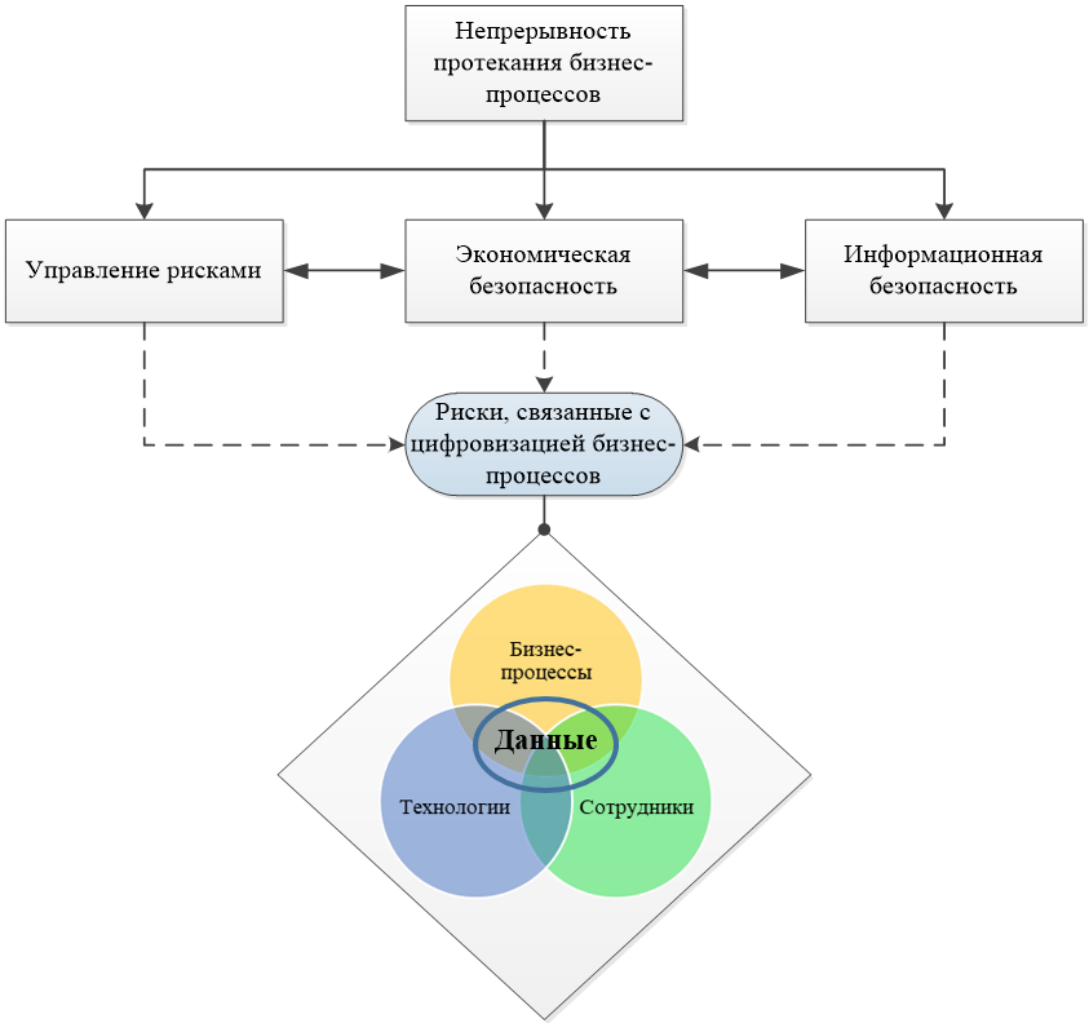
Рисунок 5 – Экономическая безопасность и риски организации в условиях цифровизации



Источник: составлено автором.

Рисунок 6 – Экономическая безопасность и риски организации в условиях цифровизации

Таким образом, по итогам проведенного теоретического анализа, изучения статистических данных, связанных с цифровым мошенничеством, установлено, что «несмотря на преимущества, получаемые от интеграции цифровых технологий, цифровые уязвимости и угрозы стали серьезной проблемой как для пользователей, так и для кредитных организаций: перевод большей части деятельности в цифровой контур влечет за собой рост количества рисков и вероятности утраты кредитной организацией финансовой стабильности и операционной устойчивости. Информационная безопасность становится определяющим элементом в контексте обеспечения экономической безопасности кредитной организации» [141], что продемонстрировано на рисунке 7.



Источник: составлено автором.

Рисунок 7 – Взаимосвязь экономической безопасности организации с информационной безопасностью и управлением рисками в условиях цифровизации бизнес-процессов

Для того, чтобы эффективно управлять рисками, связанными с цифровизацией, необходима соответствующая теоретическая основа, раскрывающая понятие «цифрового риска», описывающая виды такого риска и его связь с бизнес-процессами, что особенно актуально в контексте возрастающего значения информационной безопасности в рамках обеспечения экономической безопасности современной организации.

1.2 Научные подходы к трансформации бизнес-моделей организации на основе цифровизации бизнес-процессов

Под научным подходом применительно к предмету диссертационного исследования автор понимает процесс объективного установления фактов посредством изучения существующих тенденций в банковской сфере, формирование гипотезы, анализа результатов и прогнозирования будущих событий. Цифровая трансформация бизнес-моделей организации в настоящее время не получила универсального определения среди исследователей. Существующие исследования довольно разрозненны, исследователи имеют тенденцию сосредотачиваться на конкретных элементах, а не на целом объекте.

В современных экономических условиях деятельность каждого хозяйствующего субъекта связана с цифровой средой и цифровыми технологиями. Поскольку в рамках данной работы исследуется кредитные организации (коммерческие банки), необходимо рассмотреть сущность коммерческого банка как особого вида кредитной организации. Под кредитной организацией согласно статье 1 федерального закона «О банках и банковской деятельности» понимается «юридическое лицо, которое для извлечения прибыли как основной цели своей деятельности на основании специального разрешения Центрального банка Российской Федерации имеет право осуществлять банковские операции» [15]. Существует несколько типов кредитных организаций: банки, микрофинансовые и факторинговые

компании, инкассаторские службы, а также организации, занимающиеся оборотом электронных денежных средств. Е.П. Рамзаева замечает, что «основной задачей коммерческих банков было и остается поддержание непрерывного процесса циркуляции временно свободных финансовых ресурсов от одних участников рынка к другим, на принципах платности и возвратности» [147], а также указывает на то, что «основной источник дохода коммерческого банка – это операции по кредитованию физических и юридических лиц [147]».

В современных условиях трансформация большинства бизнес-процессов в крупных организациях (в том числе кредитных), а также в организациях, которые хотят быть конкурентоспособными, связана с использованием цифровых технологий. Согласно исследованиям международной консалтинговой компании Deloitte, индекс цифровизации российских кредитных организаций выше, чем в среднем по миру [64]. Кредитные организации в своей деятельности используют наиболее эффективные современные технологии, такие как искусственный интеллект, машинное обучение, большие данные и роботы.

Эволюция развития организаций связана с появлением новых форм операций и проникновением цифровых технологий во все отрасли экономики. Термин «цифровая экономика» введен в оборот в 1995 году Николасом Негропонте для обозначения нового типа экономики, при котором товары и услуги переходят в цифровую среду, что обуславливает появление новых типов рисков. «В банковской сфере цифровая трансформация привела к появлению таких инноваций, как мобильные приложения для интернет-банкинга, электронные платежные системы и цифровые кошельки. Данные технологии предлагают клиентам удобство и доступность в управлении своими финансами, а также снижают банковские затраты и повышают банковскую эффективность» [141]. Кроме того, цифровизация привела к появлению новых способов анализа данных и прогнозирования, что помогает организациям лучше понимать потребности клиентов и предлагать

более персонализированные услуги (это и привело к трансформации традиционной банковской бизнес-модели). Например, с помощью анализа больших данных и искусственного интеллекта кредитные организации могут предлагать клиентам рекомендации по инвестициям, кредитным продуктам и другим услугам, основываясь на их финансовых потребностях и предпочтениях, следовательно, актуализируется и усовершенствуется система поддержки клиентов.

Трансформация традиционной бизнес-модели кредитной организации, представленной на рисунке 8, рассматривается далее в тексте работы, на рисунке 9 показано как именно (в какую форму) трансформируется бизнес-модель.

Источник: составлено автором по материалам [77; 87; 119; 121; 164].
Рисунок 8 – Традиционная бизнес-модель кредитной организации

В результате исследования научных подходов к пониманию цифровой трансформации кредитных организаций в зарубежной и российской литературе установлено, что они достаточно сильно различаются. Некоторые авторы подчеркивают необходимость активизации внедрения цифровых

технологий [145], в том числе и на уровне стратегии развития кредитной организации, то есть основное внимание уделяется технической и стратегической стороне цифровой трансформации. Вторая группа авторов больше сосредотачивается на потребностях клиентов как на основе цифровой трансформации банковских услуг и операций [172].

Цифровые технологии позволяют кредитным организациям снизить операционные издержки и повысить уровень безопасности. Например, автоматизация процессов и использование роботизированного процесса автоматизации способствует сокращению времени на обработку заявок на кредит и другие операции [159], а блокчейн-технология обеспечивает безопасность и прозрачность при совершении финансовых транзакций [134]. Однако необходимо отметить, что переход к концепции «цифрового общества» (при которой новые технологии постоянно сопровождают человека на его жизненном пути, что уже является реальностью) также представляет некоторые вызовы и риски. Например, повышается уровень киберугроз и необходимость обеспечения безопасности данных клиентов. В целом, инновационный формат цифровых технологий, конечно, обеспечивает кредитным организациям приток клиентов (онлайн обслуживание становится все более востребованным, кроме того обеспечивает рост кросс-продаж или сопутствующих услуг), оптимизируются тарифы комиссионных операций (комиссия за расчетно-кассовое обслуживание становится все меньше по мере развития цифровых технологий), а значит растут и доходы кредитных организаций. Однако кредитные организации должны быть готовы к постоянным изменениям окружающей их экономической действительности и инвестировать в цифровую трансформацию, чтобы оставаться конкурентоспособными.

Согласно исследованиям К. Мэтта, «цифровая трансформация – это сложный процесс, который включает: изменения в создании стоимости, структурные изменения и использование технологий и финансовых аспектов, он призван решить проблемы, с которыми в настоящее время сталкиваются

кредитные организации. Цифровая трансформация блокируется рядом барьеров, которые могут препятствовать или даже разрушать данный процесс» [197]. К ключевым инструментам цифровой трансформации в научной литературе относят стратегические направления обеспечения конкурентного лидерства организации с учетом цифровых тенденций, а также внедрение цифровых технологий на основе клиентоориентированного подхода.

Цифровая трансформация требует:

– Активного участия и поддержки руководства организации. Лидеры должны обладать цифровым мышлением, быть готовыми к инновациям и принимать стратегические решения, способствующие цифровой трансформации. Они также должны создать в организации культуру, которая поощряет эксперименты и новаторство.

– Понимания последних цифровых тенденций и их влияния на банковский бизнес.

– Необходимости инвестирования в обучение и развитие своих сотрудников, чтобы они могли обеспечить успешное внедрение цифровых технологий.

– Разработки стратегии, определяющей цели и направления развития организации в цифровой среде.

– Внедрения цифровых технологий и инструментов в бизнес-процессы организации: облачные вычисления [151], интернет вещей, искусственный интеллект [100], автоматизация процессов, а также специально разработанные технические устройства (лазерная разведка данных [115]). Организации должны выбирать и внедрять технологии, которые наилучшим образом соответствуют их бизнес-потребностям, стратегии и размеру активов;

– тщательной переориентации на клиента и его потребности (клиентоориентированный подход). Организации должны использовать преимущества инструментов по работе с данными и аналитикой для лучшего

понимания своих клиентов, предлагать персонализированные услуги и улучшать клиентский опыт.

Появление цифровых технологий в банковском секторе привело к возникновению нового типа кредитных учреждений, таких как цифровые банки и необанки. Цифровые банки или онлайн-банки (виртуальные банки) предлагают банковские услуги и операции исключительно через цифровые каналы – мобильные приложения или интернет-банкинг [157]. Подобные банки не имеют физических отделений, их работа основываются на технологиях для обслуживания клиентов. Цифровые банки обеспечивают легкие и удобные процедуры открытия счетов, переводов, оплаты услуг и других банковских операций. Необанки — это компании, предоставляющие банковские услуги и продукты, однако не обладающие банковской лицензией [124]. Необанки обычно сотрудничают с лицензированными банками или используют их инфраструктуру для обработки транзакций. Они часто предлагают более гибкие и инновационные услуги, чем традиционные банки, и могут быть особенно популярны у молодых поколений и цифровых аборигенов [124].

Оба типа кредитных учреждений (цифровые банки и необанки) предлагают клиентам удобство, доступность и инновационные функции. Они меняют традиционную модель банковского обслуживания и стимулируют конкуренцию в отрасли, что в итоге приводит к улучшению услуг и более выгодным условиям для клиентов. Стоит отметить, что безопасность и защита данных являются важными аспектами деятельности для цифровых банков и необанков, и они (аналогично коммерческим банкам [67]) должны следовать требованиям по защите данных, а также бороться с мошенничеством.

Эксперты отмечают, что в условиях цифровой трансформации для кредитной организации «мобильное приложение уже не дань трендам, а продукт-локомотив, который становится главным средством удержания, а иногда и привлечения клиентов» [34]. Мобильные приложения включают инновационные функции, такие как автоматизированный анализ расходов или

персонализированные финансовые рекомендации. Эффективность мобильного приложения кредитной организации как инструмента маркетинга оценивается несколькими показателями. К базовым показателям относятся: «количество скачиваний, регистраций, активность в приложении, вовлеченность пользователей, или «липкость», средняя продолжительность сессии, коэффициент удержания клиентов, виральность, показатель оттока клиентов, показатели монетизации, включая стоимость привлечения клиента. Для оценки и отслеживания показателей эффективности мобильного приложения существуют платформы, например, AppMetrica (сервис от Яндекса), Firebase Analytics, Flurry (для сбора и анализа статистики мобильного приложения, отслеживания монетизации) [27].

Также можно отметить, что появилась и специфическая подотрасль банковского маркетинга – цифровая. Цифровой маркетинг определяется учеными как вторая после интернет маркетинга фаза развития маркетинга в условиях информационной экономики, когда процессы информатизации общества достигли уровня его тотальной цифровизации [146]. В результате цифровой трансформации банковского сектора произошли следующие фундаментальные изменения в банковских системах и процедурах: снизилась скорость обслуживания клиентов, в том числе посредством автоматизации процедур андеррайтинга; удобные для клиента и ориентированные на маркетинг процессы привели к росту уникальности продукта; рабочий процесс стал больше ориентирован на клиента, а система отчетности начала демонстрировать снижение нагрузки на персонал. К отрицательным последствиям развития банковского цифрового маркетинга относится тот факт, что такое развитие требует значимых инвестиций и в систему безопасности кредитной организации.

Расширение спектра услуг каждой конкретной кредитной организации во многом зависит от применяемых финансовых технологий. *Финансовые технологии (Financial technology, FinTech)* включают в себя программные

продукты, которые используются для улучшения и автоматизации финансовых операций корпоративного и частного сектора.

В банковской сфере финансовые технологии объединяют:

а) Цифровые платежи. Финтех-компании предлагают различные способы онлайн-платежей, такие как мобильные кошельки, электронные деньги и переводы через мессенджеры. Они делают платежи более удобными, быстрыми и безопасными.

б) Кредитование и финансирование. Финтех-платформы предоставляют альтернативные и инновационные способы кредитования и финансирования для малого и среднего бизнеса, стартапов и частных лиц, например, пиринговое кредитование, краудфандинг и онлайн-кредиты [95].

в) Личное финансовое планирование. Мобильные приложения и платформы кредитных организаций помогают клиентам управлять своими финансами, создавать бюджеты, отслеживать расходы (планировать кредитные платежи), инвестировать и получать персонализированные финансовые рекомендации [107]. Они помогают клиенту улучшать финансовую грамотность и принимать осознанные финансовые решения.

г) Краудинвестинг и инвестиции. Финтех-платформы предлагают возможности для инвестирования в стартапы, недвижимость, цифровые активы и другие активы через краудинвестинговые платформы. Они делают инвестиции доступными для широкой аудитории и снижают порог для участия в рынке капитала.

д) Блокчейн и криптовалюты. Технология блокчейн используется для создания безопасных и децентрализованных систем платежей, учета, смарт-контрактов и других финансовых операций. Криптовалюты, такие как биткоин, эфириум (и другие) основаны на блокчейне, они предоставляют новые возможности для хранения, передачи и использования цифровых активов.

Финансовые технологии меняют способы, с помощью которых люди управляют своими денежными средствами, получают кредиты и инвестируют.

Однако важно отметить, что обеспечение безопасности и защиты данных это критически важные аспекты в рамках внедрения и использования финансовых технологий. В банковском секторе финтехнологии применяются и в сфере регулирования деятельности кредитных организаций, например, в установленных нормативных стандартах («Базель III» [176]), что отражает трансформацию бизнес-модели кредитной организации не только в части оказания базовых банковских услуг или управления бизнес-процессами, но и в части пруденциального надзора, то есть бизнес-процессы нацелены еще и на обеспечение безопасности кредитной организации по требованиям регулятора (что, например, раскрыто в статье В.И. Авдийского [65]).

Бизнес-модель кредитной организации в современных реалиях должна быть основана на проработанной ИТ-инфраструктуре – соответствующей текущим и будущим бизнес-планам, масштабируемой и мобильной. В рамках трансформации кредитной организации изменяются как цели, задачи и функции кредитной организации, так и архитектура баз данных и программного обеспечения, сопровождающих банковскую деятельность (некоторыми авторами определяется как базовая составляющая экономической безопасности кредитной организации [154]). Применение цифровых технологий при трансформации бизнес-модели позволяет сделать кредитную организацию более гибкой, готовым к изменениям, отступить от традиционной модели бизнеса.

Исследователи по-разному интерпретируют схемы трансформации банковских бизнес-моделей под влиянием цифровых технологий. К примеру, Ю.Б. Бубнова выделяет следующую форму бизнес-модели кредитной организации [87], отраженную на рисунке 9, подтверждающую основные тенденции в банковской цифровизации. Модель Ю.Б. Бубновой дополнена, показано, что с переходом на новые продукты кредитная организация наращивает и количество рисков, одновременно растет и вероятность убытков из-за снижения информационной и экономической безопасности кредитной организации. Помимо технологий, таких как искусственный интеллект, работа

с распределенными реестрами и квантовые вычисления, исследователь выделяет также роль сотрудника, который в новой парадигме должен иметь обособленную от остальных сотрудников роль, то есть в отличие от традиционной модели обладать ключевой особенностью, обособляющей его от других.

Источник: составлено автором по материалам [87].

Рисунок 9 – Трансформация бизнес-модели кредитной организации под воздействием цифровых технологий

По мнению исследователей компании CDO Partners [59] цифровая трансформация, которая помимо бизнес-модели затрагивает сотрудников, бизнес-процессы, технологии и продукты, работу с целевой аудиторией, организационную структуру и культуру, может происходить по двум направлениям: «Создание новых бизнес-моделей; оптимизация и

цифровизация существующих бизнес-процессов. Оптимизация существующей бизнес-модели занимает немногим меньше времени по сравнению с созданием новой бизнес-модели» [59], однако требует намного меньше расходов. Создание новой бизнес-модели предполагает использование кардинально новых методов ведения деятельности (к примеру, избавление от посредников, экономика совместного потребления, дематериализация), в то время как трансформация текущей бизнес-модели позволяет использовать существующие бизнес-процессы с внедрением новшеств, что особо актуально для кредитных организаций, так как у них нет возможности рисковать текущей парадигмой для создания новой здесь и сейчас – от кредитной организации зависит огромное количество клиентов, создание новой бизнес-модели влечет за собой риск нарушений в работе банковских процессов, что критично для кредитной организации как для основополагающей организации в жизни общества. Трансформация бизнес-модели организации может быть выполнена по нескольким сценариям, которые во многом схожи между собой [77]. Основные этапы, которые должны быть пройдены в рамках цифровой трансформации для успешной ее реализации, включают в себя:

а) *Проведение обучения сотрудников*. Ответственные за трансформацию сотрудники (от уровня специалиста до уровня топ-менеджера) должны понимать, для чего нужна трансформация и каким образом ее необходимо осуществить. Обучение необходимо начать со введения в само понятие цифровизации, затронув основные аспекты, связанные с организацией, объяснив, какое место организация должна занимать в структуре цифровой экономики, и насколько данная трансформация сможет ускорить бизнес-процессы, сократить издержки, а также сформировать защиту от рисков разного рода. Особое внимание в ходе обучения стоит уделить анализу статистических данных, на основе которых строятся все алгоритмы работы новейших технологий. Сотрудникам необходимо также объяснить, что цифровизация в подавляющем большинстве случаев требует декомпозиции

существующих бизнес-процессов для выявления «узких» мест, которые требуют модернизации.

б) *Аудит для оценки текущей возможности проведения трансформации и подготовки стратегии*. Оценка готовности организации к трансформации бизнес-модели представляет собой выявление наличия актуальных карт бизнес-процессов организации, а также подготовку таких карт в случае их отсутствия. Карты бизнес-процессов необходимы для того, чтобы были видны этапы осуществления процесса, которые могут быть подвергнуты изменению (некоторые этапы не могут быть изменены, например, по причине необходимости использования исключительно человеческого мышления, либо релевантность изменения данных этапов может быть сомнительна), а также с помощью них возможно выделить ключевые этапы, изменения которых будут наиболее выгодны организации, либо ускорят бизнес-процесс. Также аудит подразумевает под собой предоставление экспертной оценки со стороны ответственных за бизнес-процессы сотрудников на предмет выявления характерных особенностей процессов, которые должны быть изменены. Важным этапом аудита является проведение опроса сотрудников-операционистов, которые являются исполнителями по процессам с технической точки зрения.

в) *Разработку и реализацию стратегии трансформации бизнес-модели*. Разработка стратегии является одним из важнейших этапов осуществления трансформации, как и в случае с любыми крупными проектами, либо изменениями в организации. Подготовка стратегии зачастую реализуется в рамках стратегических сессий, проведения GAP-анализа, разработки проектов и составления карты рисков. Реализация стратегии может быть осуществлена как самой организацией, так и отдана на аутсорсинг – в данном случае все зависит от бюджета, заложенного на проведение трансформации, а также от наличия соответствующих компетенций внутри организации. Стратегия имеет определенную структуру, включающую следующие пункты:

– определение целей и задач трансформации;

– определение набора проектов с указанием их приоритизации и проведением оценки наличия необходимых ресурсов и бюджета, а также возможных рисков;

– подготовку финансовой модели перечня проектов с выявлением ключевых прогнозных показателей;

– подготовку плана осуществления трансформации (проведение пилотов, возможность полноценного внедрения проектов, анализ итогов, оценка с помощью использования показателей эффективности);

– подготовку плана по работе с возможными рисками как по итогам реализации трансформации, так и в случае ее неполноценного осуществления.

Исполнение стратегии согласно детально проработанному плану повлечет за собой успешное завершение трансформации, чему должен способствовать эффективный проектный менеджмент. Трансформация бизнес-модели (в том числе на основе риск-ориентированного подхода) осуществляется с помощью определенных навыков и методик, используемых сотрудниками. С организационной точки зрения цифровая трансформация предполагает применение различных апробированных методологий совершенствования бизнес-структуры и бизнес-процессов организации, например, Agile и Scrum, дополненных аналитикой больших данных и виртуализацией банковских продуктов. Методология Agile в частности активно применяется в рамках борьбы с модельным риском. Т.В. Никитина и М.А. Гальпер в своей работе по трансформации банковских стратегий в соответствии с методологией Agile в условиях глобальной неустойчивой среды замечают, что в рамках перехода к инновационному развитию именно методология Agile является незаменимой как при создании инноваций, так и при проведении диджитализации в кредитной организации [129]. Банковские процессы зачастую не могут быть изменены в силу специфики строгого регулирования со стороны служб безопасности и государства. Однако если говорить про внедрение цифровых технологий — это именно тот процесс, в котором Agile-методология будет эффективной [110]. Гибкие

бизнес-процессы способствуют ускорению внедрения технологий, а также позволяют избежать больших издержек. Кросс-функциональные команды, которые формируются в рамках методологии, способны за счет быстрого взаимодействия между участниками, в том числе, выявлять риски на ранних этапах, а также предотвращать их до дальнейшего возрастающего влияния.

Использование больших данных нельзя отнести к новейшим технологиям, так как работа в направлении внедрения аналитики больших данных ведется в России с 2013 года, однако важность этой технологии возрастает с каждым днем, о чем свидетельствует постоянное появление новых разработок в данной сфере, например, современные облачные хранилища (хранение данных с использованием виртуальных [облачных] пространств), Deeplearning (глубокая аналитика обработки большого объема данных разной структурной составляющей) и другие. В России в 2021 году был утвержден первый национальный стандарт в области больших данных [30]. Термин «большие данные» относится к огромным наборам данных, содержащим информацию о различных областях бизнеса, поведении людей, отраслях и многом другом. Применение больших данных в рамках трансформации бизнес-модели организации особенно актуально в рамках формирования новой парадигмы управления рисками:

а) Описательная аналитика позволяет выявить причины процессного, либо иного сбоя на основе анализа данных за текущий и прошедший периоды. По итогам рассмотрения результатов проведенного анализа процессный и проектный менеджмент организации определит слабые места процесса, что послужит первым шагом к его модернизации и устранению возможных рисковых ситуаций.

б) Прогнозная (предикативная) аналитика, используя имеющиеся данные, прогнозирует последующее развитие событий в рамках бизнес-процесса. Данная технология в рамках работы организации может быть одной из важнейших, так как с помощью нее (в случае кредитных организаций) можно спрогнозировать изменение уровня платежеспособности

заемщика, а также уровень цен на рынке ценных бумаг, что актуально для инвестиционных подразделений кредитной организации. Таким образом, прогнозная аналитика может сыграть ключевую роль в предупреждении рисковых ситуаций.

в) Предписательная аналитика является усовершенствованной версией предикативной – помимо выявления возможных отклонений в бизнес-процессе, она также предлагает сценарий осуществления данного процесса, при котором этого отклонения не произойдет. При правильном внедрении данной технологии в банковскую ИТ-архитектуру возможна практически полная автоматизация процесса проведения анализа рисков [75].

г) Диагностическая аналитика отчасти похожа на описательную с той только разницей, что она позволяет не просто выявить причины банковского сбоя, но и показывает определенные события, которые не должны были произойти в рамках бизнес-процесса, однако произошли и повлияли на итоговый (более глобальный) сбой. Данный вид больших данных может быть актуален для выявления неочевидных связей между объектами процесса, которые при детальном изучении могут быть использованы для предотвращения, либо предупреждения рисков.

Исследователи также отмечают важность использования больших данных в банковской сфере, в том числе, для повышения информационной безопасности. М.К. Беляев и А.Д. Дорохова, исследуя большие данные, приходят к выводу, что они могут быть использованы «для отслеживания поведения клиентов с целью выявления подозрительной активности, а также для повышения точности данных, сокращения ошибок, своевременного реагирования на претензии клиентов и предотвращения мошенничества» [81].

Исследования трансформации бизнес-моделей кредитной организации на основе цифровизации бизнес-процессов в основном затрагивают вопросы своевременного пересмотра положений стратегий развития кредитных организаций (в силу частого обновления технических аспектов осуществления банковских операций), совершенствования цифрового банковского

маркетинга, более полного анализа и учета потребностей клиентов как основы цифровой трансформации банковских услуг и операций. Аспекты экономической безопасности и управления рисками также должны быть рассмотрены в качестве связующих элементов стратегической (долгосрочной) цифровой трансформации. Эффективность осуществления данного процесса напрямую связана с управлением сопутствующими цифровыми рисками, которые нуждаются в идентификации и последующем анализе.

1.3 Особенности регулирования бизнес-процессов и возникновения рисков кредитной организации в условиях цифровизации

Анализ, проведенный в предыдущих параграфах, показал, что деятельность современных кредитных организаций сопряжена с появлением новых видов рисков (в том числе связанных с активным внедрением цифровых технологий), при этом элементный состав ранее существовавших традиционных рисков банковской деятельности множится и усложняется. Эффективно функционирующая кредитная организация не только ведет оценку и учет рисков, но и постоянно оптимизирует процесс принятия решений по рассмотрению компромисса между риском, доходностью бизнес-процессов и целями заинтересованных сторон, собственников банковского бизнеса, что продемонстрировано в таблице 1.

Таблица 1 – Функции управления, реализуемые в рамках осуществления бизнес-процессов

Функция управления	Содержание функции, воздействие на бизнес-процессы	Улучшение / изменение / развитие функции в цифровом пространстве	Среда регулирования
1	2	3	4
Планирование	Деятельность, посредством которой кредитная организация определяет свой будущий курс действий. Разработка стратегии использования ресурсов бизнеса в пределах прогнозируемой среды для достижения общих целей	Улучшение процесса координации текущих планов деятельности различных подразделений кредитной организации	Внутренняя

Продолжение таблицы 1

1	2	3	4
Организация	Определение масштабов работ для достижения цели и описание процедуры их исполнения	Улучшение / развитие человеческого капитала кредитной организации	Внутренняя
Мотивация	Постановка целей, вознаграждение за их выполнение, применение санкций за не достижение	Улучшение процесса учета достижений и неудач	Внутренняя
Контроль	Оценка качества работы, оценка недостатков работы	Совершенствование системы контроля рисков	Внешняя
Мониторинг	Проверка операций по определенным признакам	Улучшение функции разработки альтернатив развития кредитной организации	Внутренняя, внешняя
Диспетчеризация	Оптимизация процессов, а также подходов к управлению и мониторингу производительности	Улучшение систем загрузки данных, качества управления рисками, устранение сбоев в процессе жизнедеятельности кредитной организации при помощи цифровых технологий	Внутренняя

Источник: составлено автором.

Цифровая трансформация бизнес-процессов кредитной организации, появление новых банковских продуктов и услуг, нормативные изменения, изменения в конкурентной среде и рыночных условиях функционирования кредитной организации являются важными факторами, влияющими на стратегию управления кредитной организацией. Предоставляя кредитные средства, кредитные организации по сути наполняют экономику страны ликвидностью, и значение их деятельности отождествляется с инструментом – катализатором экономического роста любой страны. Банковский сектор и экономика в целом оказывают взаимное влияние друг на друга, стабильность финансовой системы во многом зависит от эффективности банковского сектора. Именно поэтому банковский сектор является одной из наиболее регулируемых отраслей в мире.

Макропруденциальное регулирование — это подход к финансовому регулированию, направленный на снижение риска для всей финансовой системы и, таким образом, на предотвращение и снижение

макроэкономических издержек финансовой нестабильности. В макропруденциальном регулировании, осуществляемом центральными банками и регулирующими органами, используются различные инструменты, в том числе введение ограничения на соотношение долга к доходу, ограничение на кредитное плечо (которое ограничивает рост активов путем привязки активов кредитных организаций к их собственному капиталу). В соответствии с типом денежно-кредитной политики различаются не только инструменты, но и подходы к макропруденциальному регулированию в стране / регионе. Подход может быть как мягким (ограничения носят рекомендательный характер), так и жестким (вплоть до отзыва лицензии у кредитной организации). Эффективные макропруденциальные структуры важны по многим причинам. Одной из них является взаимодействие макропруденциальной и денежно-кредитной политики. Оптимальное сочетание данных сущностей в контексте сохранения финансовой и экономической стабильности зависит от множества факторов, в том числе от того, откуда исходят риски и насколько далека экономика от ценовой стабильности и полной занятости. Чем грамотнее выстроена макропруденциальная политика, тем меньше вероятность того, что центральному банку придется рассматривать вопрос о повышении процентных ставок выше среднесрочного прогноза занятости и инфляции. Среди различных мер макропруденциального регулирования следует выделить мониторинг размера и уровня достаточности банковского капитала (показатель имеет важное значение в контексте формирования устойчивости кредитной организации [91; 113]).

Основным нормативным документом, отражающим пруденциальные требования к внедрению системы оценки и учета рисков в кредитной организации и являющимся основой значительного ускорения и ужесточения регулирования данного процесса, является Базель III – пакет реформ по банковскому регулированию Базельского комитета по банковскому надзору. Базель III был разработан и введен в ответ на финансовый кризис, который

начался в 2007–2008 гг. По итогам кризиса стало очевидно, что существующие подходы к регулированию и нормативы (Базель II) не обеспечивают достаточного уровня финансовой стабильности и контроля рисков в банковской системе. С появлением Базеля III ужесточились требования к уровню капитала для обеспечения кредитных организаций достаточными финансовыми ресурсами (возможность к покрытию потенциальных убытков и рисков), были повышены требования к ликвидности кредитных организаций (снижение вероятности проблем с обеспечением платежеспособности в кризисные периоды), введены новые нормы по управлению операционными рисками (снижение вероятности возникновения сбоев банковской деятельности), а также дополнительные требования по оценке рисков и управлению ими.

Стоит отметить, что ключевой причиной изменений в имеющихся на тот момент стандартах являлось снижение доверия широкого круга заинтересованных сторон к величине коэффициентов капитала, взвешенных с учетом риска. Поскольку банковская система России включена в мировые процессы стандартизации банковских процессов, то стандарты Базель III вводятся и для российских кредитных организаций. Центральный банк в большинстве стран в соответствии с Базельскими стандартами разрабатывает и внедряет собственные нормативно-правовые акты. В России для кредитных организаций разработан ряд документов, определяющих целый набор подходов к управлению банковскими рисками и представляющих стандарт оформления развитых практик управления рисками.

Отправной точкой регулирования уровня достаточности капитала в Базель III по большей части является операционный риск. Это обусловлено тем, что передовые технологии, повышенная доступность данных, новые бизнес-модели и цепочки создания стоимости меняют способы обслуживания клиентов, взаимодействия с третьими сторонами и внутреннюю работу кредитных организаций. Операционный риск впервые упомянут Базельским комитетом в серии документов, опубликованных в период с 1999 года по

2001 год, уже тогда он был определен в качестве отдельной и контролируемой категории риска, требующей собственных инструментов оценки и идентификации. Современные кредитные организации несомненно добились значительного прогресса в управлении рисками в рамках макропруденциальных требований, однако стоит отметить, что управление операционным риском *усложняется по ряду причин*: в сравнении, например, с кредитным или рыночным риском, операционный риск имеет большее количество подвидов (риск человеческого фактора [117], системный риск, процессуальный риск и так далее); управление операционным риском требует непрерывного мониторинга всех бизнес-процессов кредитной организации, а также обеспечения их прозрачности; различия в определениях функций служб управления операционными рисками и других надзорных групп (особенно в области соблюдения нормативных требований, отслеживания финансовых преступлений и рисков, связанных с цифровизацией) нечеткие и неоднозначные; операционный риск в целом сложнее поддается управлению и измерению именно с точки зрения макропруденциальных лимитов.

Рост возможностей по хранению и использованию данных, а также потенциала применения сквозной аналитики создали возможность к трансформации процессов обнаружения и оценки операционных рисков – традиционные контрольные мероприятия сменились мониторингом на основе данных в режиме реального времени. Однако подобная трансформация привела и к возникновению новых типов операционных рисков: процессы цифровизации и автоматизации банковской деятельности поспособствовали минимизации количества традиционных человеческих ошибок, при этом сопутствуя появлению рисков, связанных с *управлением изменениями* (практика в сфере ИТ, позволяющая свести к минимуму нарушения в предоставлении ИТ-услуг при внесении изменений в критически важные системы и сервисы [204]); партнерство с компаниями сферы финансовых технологий влечет за собой появление киберрисков (киберриски в сравнении с рисками, связанными с цифровизацией, более узкоспециализированное

понятие, относящееся к угрозам использования информационных технологий и сетей); применение машинного обучения и искусственного интеллекта поднимает вопросы субъективных суждений / предвзятости при принятии управленческих решений; границы между функциями управления операционными рисками и другими группами рисков (например, комплаенс-рисками) продолжают меняться – кредитные организации стремятся «гармонизировать» таксономии и подходы к оценке рисков, но все же сохраняется их значительное пересечение.

Банк России, реализуя совокупность целенаправленных действий с использованием финансовых инструментов, рычагов и стимулов, создает макропруденциальные требования, базируясь на требованиях Базеля III. В 2022 году «Банк ВТБ» (ПАО)» стала первой кредитной организацией, которая прошла проверку системы управления операционным риском (далее – СУОР) на соответствие Положению № 716-П [20] и получила разрешение перейти на расчет требований к капиталу под операционный риск согласно Положению № 744-П [18]. Стоит отметить, что ранее в соответствии с Положением № 652-П расчет размера операционного риска для определения нормативов достаточности формировался, исходя из величины среднего дохода кредитной организации за последние три года.

Новый подход по стандартам Базеля III [19] обязывает кредитные организации рассчитывать объем капитала для покрытия операционного риска, основываясь на фактическом уровне прямых убытков от рисковых событий. Это позволяет существенно сократить резервирование капитала (на 10–30%) по сравнению с предыдущим порядком. В абсолютных величинах экономия может достигать от 50 млрд руб. для ВТБ до 100 млрд руб. для Сбербанка. Так, по данным ВТБ [50] введение специального порядка информирования топ-менеджмента о событиях свыше 1 млн руб. оправдало себя – в кредитной организации отметили резкое улучшение дисциплины в части выявления и регистрации событий на стороне первой линии защиты. В результате применения нового подхода нагрузка на капитал кредитной

организации снизилась более чем на 40 млрд руб. (или 10 базисных пунктов в терминах достаточности капитала). Также в ходе внедрения данного подхода в ВТБ было выявлено, что важным инструментом обеспечения полноты и корректности баз данных событий операционного риска является *реконсиляция* (процесс сопоставления и согласования данных или транзакций из разных источников с целью установления соответствия и выявления расхождений или ошибок) базы потерь с бухгалтерским учетом [50].

Необходимо отметить, что внедрение положений Базеля III на практике имеет и отрицательные стороны: строгое соответствие требованиям Базельского комитета влечет за собой уменьшение объемов кредитования, так как доступность кредитов для некоторых категорий заемщиков снижается; также подобные регуляторные нововведения знаменуют не только улучшение системы оценки и учета операционных рисков, но и рост расходов на операционную деятельность, что нашло отражение на рисунке 10.

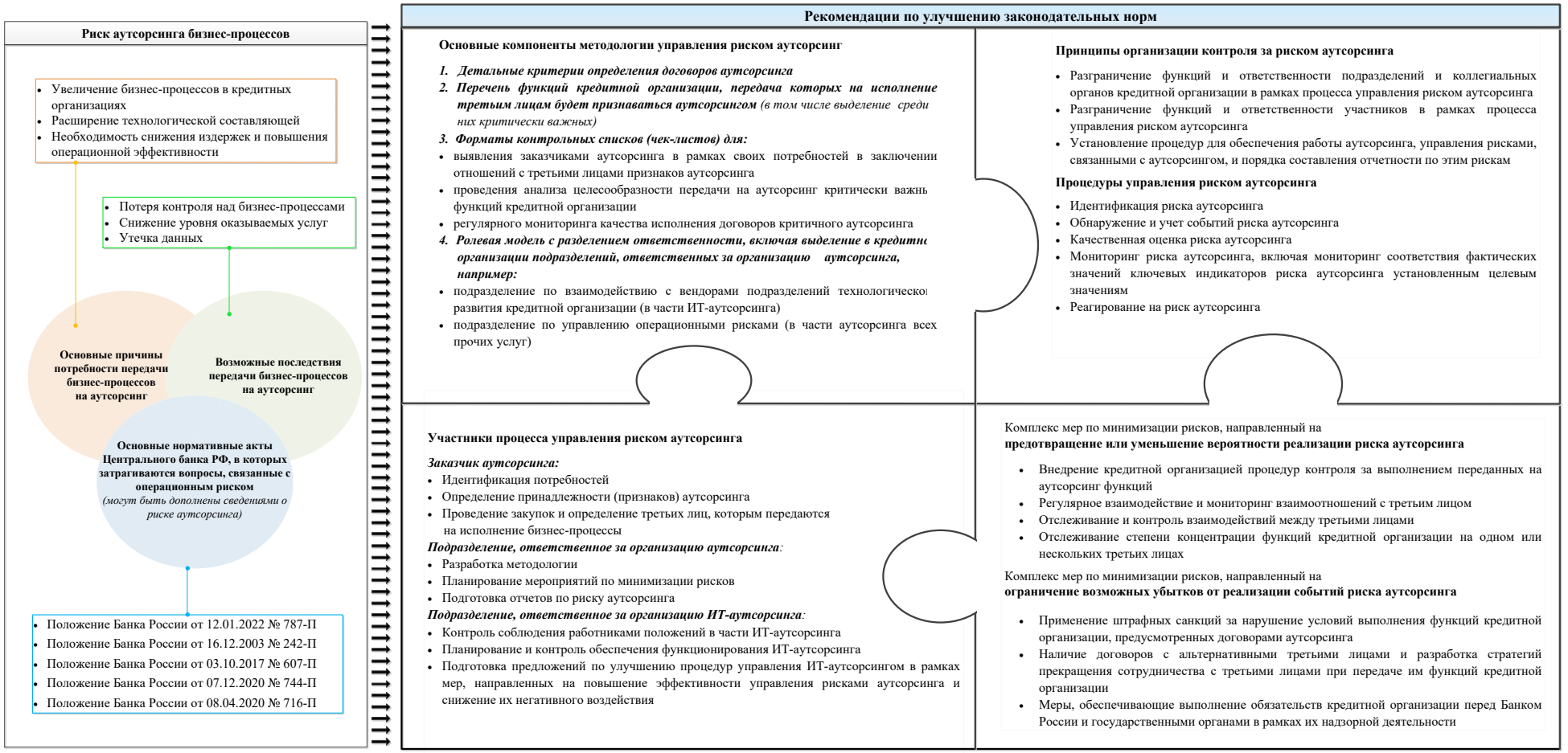
Источник: составлено автором по материалам [20].

Рисунок 10 – Изменения в управлении операционными рисками, введенные Положением Банка России № 716-П

В условиях роста числа бизнес-процессов в кредитных организациях, увеличения роли технологий в их работе, а также необходимости сокращения затрат и повышения операционной эффективности, кредитные организации активно передают свои функции на аутсорсинг, под которым можно понимать передачу определенных функций, задач, бизнес-процессов, связанных с деятельностью организации, сторонним организациям для их выполнения на основании заключенных договоров, которая позволяет организации сосредоточиться на основных бизнес-процессах и снизить затраты на содержание собственных подразделений. Передача ключевых функций кредитной организации на аутсорсинг может привести к появлению определенных рисков, например, связанных с потерей контроля над бизнес-процессами и снижением уровня оказываемых услуг. Также существует риск утечки данных, что является особенно важной проблемой для банковской сферы, где большая часть данных носит конфиденциальный характер, что отмечается, к примеру, А.И. Карасовым: «В связи с быстрым развитием технологий защита конфиденциальности становится все более сложной задачей. Поэтому государство должно регулярно обновлять правила и нормативы, связанные с защитой конфиденциальности, и осуществлять контроль за их соблюдением» [103].

Для того чтобы кредитные организации успешно справлялись с рисками, связанными с аутсорсингом своих функций, услуг и бизнес-процессов, необходимо выстроить процесс регулирования риска аутсорсинга со стороны законодательства. В целях развития практики управления операционными рисками со стороны государства может быть дополнено Положение Банка России от 8 апреля 2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

Рекомендации по улучшению законодательных норм в части дополнения существующих нормативных документов, касающихся операционного риска, определением особенностей регулирования и управления риском аутсорсинга, отражены на рисунке 11.



Источник: составлено автором.

Рисунок 11 – Риск аутсорсинга: особенности регулирования и управления

Кредитным организациям также необходимо определить перечень функций, операций, услуг и бизнес-процессов, передача которых на исполнение третьему лицу признается аутсорсингом – рекомендации по наполнению данного перечня отражены в таблице 2.

Таблица 2 – Перечень функций, операций, услуг и бизнес-процессов, передача которых на исполнение третьему лицу может признаваться аутсорсингом

Функции	Критичная функция
Услуги, связанные с обеспечением осуществления кредитной организацией операций / сделок с клиентами	да / нет
Услуги, связанные с размещением привлеченных средств от имени и за счет кредитной организации (включая кредитование)	да
Услуги, касающиеся привлечения денежных средств физических и юридических лиц на депозитные счета	да
Услуги по открытию и ведению счетов физических и юридических лиц	да
Услуги, связанные с переводами денежных средств для физических и юридических лиц	да
Услуги расчетно-кассового обслуживания физических и юридических лиц	да
Эквайринговые услуги	да
Услуги по купле-продаже иностранной валюты в наличной и безналичной форме	нет
Услуги, связанные с обеспечением выполнения операций на финансовых рынках	да
Услуги по информационно-справочной поддержке клиентов	нет
Услуги по работе с обращениями клиентов	нет
Услуги по поддержанию внутренних процессов кредитной организации	да / нет
Услуги инкассации	нет
Услуги по поддержанию собственной ликвидности	да
Услуги процессингового центра	да
Услуги по внедрению бухгалтерского учета	да
Услуги по формированию и предоставлению регуляторной отчетности	да
Услуги по сопровождению кредитного процесса (андеррайтинг, скоринг)	нет
Услуги по работе с проблемной задолженностью	нет
Услуги по работе с залоговым имуществом	нет
Услуги хранения ценностей кредитной организации	да
Услуги по идентификации в сфере ПОД/ФТ, включая биометрическую	да
Услуги по техническому обслуживанию специализированного оборудования, используемого для осуществления банковских операций	нет
Услуги по персонализации банковских карт	нет
Услуги хранения документации	нет
Услуги по подбору и управлению персоналом	нет
Услуги по обеспечению информационной безопасности	да
ИТ (включая облачные)	да / нет
Услуги по технической поддержке, сопровождению и обслуживанию ИТ-систем и связанных сервисов, включая те, которые обеспечивают функционирование онлайн-сервисов дистанционного обслуживания и предоставляют доступ к операциям в этих сервисах	нет
Обслуживание и эксплуатация оборудования, используемого для ИТ-систем кредитной организации	да
Услуги по предоставлению облачных платформ или облачной инфраструктуры	нет

Источник: составлено автором.

Недостаточное внимание к управлению риском аутсорсинга может привести к негативным последствиям, таким как утечка конфиденциальной информации, нарушение обязательств перед клиентами и контрагентами, а также снижение доверия к самой организации. Такой подход позволит не только минимизировать возможные угрозы, но и создать надежные механизмы для своевременного обнаружения и устранения событий риска аутсорсинга. Внедрение стандартов и практик управления риском аутсорсинга – один из ключевых факторов поддержания стабильности и безопасности кредитных организаций в условиях динамично меняющегося под воздействием новых технологий экономического ландшафта. Предложенный подход к управлению риском аутсорсинга (с выделением ИТ-аутсорсинга в отдельную категорию) может быть использован в рамках урегулирования данного вопроса в банковском законодательстве.

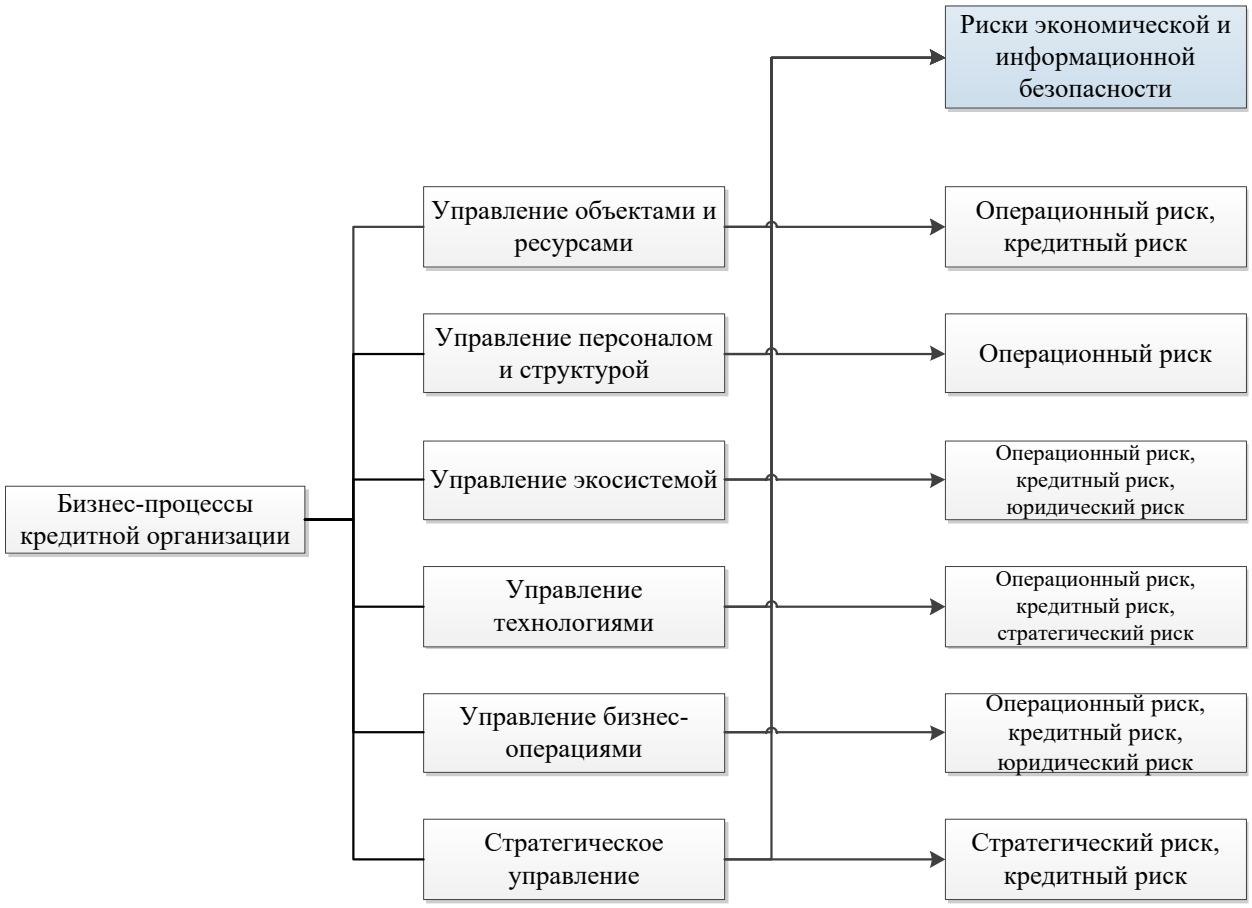
В последние несколько лет российская экономика и банковский сектор пережили достаточно серьезные потрясения, которые было сложно предсказать заранее. Банком России в связи с этим вводятся дополнительные меры поддержки финансовой устойчивости кредитных организаций, направленные на повышение их самостоятельности в вопросах выбора инструментов и методов стресс-тестирования. Центральный банк в докладе «Перспективные направления развития банковского регулирования и надзора» предлагает сделать обязательным для крупнейших кредитных организаций участие в надзорном стресс-тестировании (далее – НСТ), а также закрепить в законодательстве полномочия Банка России к проведению стресс-тестирования и использования их результатов для оценки банковских рисков [51]. Надзорное стресс-тестирование – основной аналитический инструмент оценки запаса прочности кредитных организаций в стрессовых условиях, позволяющий оценить качество внутренних стресс-тестов кредитных организаций, используемых во внутренних процедурах оценки достаточности капитала и планах восстановления финансовой устойчивости. Банком России также используется автоматизированная платформа «Знай

своего клиента» – сервис, с помощью которого «кредитные организации получают от Центрального банка информацию об уровне риска совершения их клиентами-юридическими лицами и индивидуальными предпринимателями подозрительных операций. Банк России относит каждое юридическое лицо (каждого индивидуального предпринимателя) к одной из трех групп риска совершения подозрительных операций: низкой, средней и высокой степени риска («зеленая», «желтая», «красная» группы соответственно)» [52]. Решение о том, к какой группе риска относится клиент, Банк России принимает «на основании совокупности критериев, основанных на информации о видах и характере деятельности юридических лиц (индивидуальных предпринимателей), об операциях по их счетам в кредитных организациях, их учредителях (участниках) и руководителях, аффилированности с иными юридическими лицами (индивидуальными предпринимателями), совершающими подозрительные операции, о количестве банковских счетов (вкладов, депозитов), а также на данных, поступающих от государственных органов» [52]. «Информация платформы является для кредитных организаций вспомогательной, окончательную оценку добросовестности бизнеса своих клиентов с точки зрения антиотмывочного законодательства они присваивают самостоятельно» [52].

Итак, макропруденциальное регулирование в условиях цифровизации банковского сектора направлено на противодействие киберрисками, оценку влияния новых технологий на финансовую устойчивость кредитной организации, контроль за соблюдением регуляторных стандартов (в том числе в области кибербезопасности) и оценку применения кредитными организациями финансовых технологий (взаимодействия с финтех-компаниями). Операционный риск, приобретающий новые формы в рамках осуществления цифровизации бизнес-процессов, требует особого внимания и применения широкого спектра подходов к его регулированию.

Таким образом, на основе рассмотренных существующих в научной литературе представлений о цифровых рисках и причинах их возникновения

сформировано распределение видов рисков, связанных с цифровизацией (в рамках традиционного подхода к определению рисков), по ключевым бизнес-процессам кредитной организации, что отражено на рисунке 12.



Источник: составлено автором.

Рисунок 12 – Уточненный перечень основных бизнес-процессов кредитной организации и распределение по ним рисков, связанных с цифровизацией

Также в рамках изучения теоретических аспектов построения системы управления рисками кредитной организации определено ключевое значение информационной безопасности при обеспечении экономической безопасности, что подтверждено установленным в ходе анализа возрастающим влиянием цифровых технологий на безопасность банковского сектора.

Выявлена необходимость формирования теоретических подходов к определению «цифрового риска» кредитной организации, его видов и связи этих видов с бизнес-процессами, что обусловлено отсутствием в научной литературе систематизированного описания методов оценки и управления

данной категорией рисков. Отмечено, что существующие исследования направлены на оценку негативных событий постфактум, превентивные методы управления рисками практически не рассматриваются. Бизнес-процессы кредитных организаций в условиях цифровизации в основном анализируются с позиций повышения скорости деятельности и наращивания удобств для клиентов. Управление рисками цифровизации бизнес-процессов также должно осуществляться с помощью внедрения инноваций в деятельность по обеспечению экономической безопасности кредитной организации, которая, как было отмечено ранее, напрямую сопряжена с безопасностью информационной, на что в том числе указывает увеличение количества атак на банковскую инфраструктуру в цифровом контуре.

Глава 2

Методические аспекты оценки рисков организации в условиях цифровизации при обеспечении экономической безопасности

2.1 Анализ уровня рисков и экономической безопасности кредитной организации

Исследователи Банка России отмечают, что в мировой экономике нарастают риски, которые способны привести к глобальной рецессии, «заражению» банковской системы, а также снижению безопасности банковского сектора России [33]. «Мировая экономика переживает один из наиболее синхронных в международном масштабе эпизодов ужесточения денежно-кредитной политики за последние пять десятилетий» [33]. Рост инфляции и процентных ставок в совокупности с высокой волатильностью депозитных счетов приводят к снижению ликвидности кредитных организаций и их финансовой устойчивости [83], в связи с чем функция управления рисками обретает особую актуальность.

Логическая взаимосвязь между управлением рисками и экономической безопасностью кредитной организации определяется тем, что выявление потенциальных рисков и оценка их потенциального воздействия на кредитную организацию имеют основополагающее значение для определения вектора развития кредитной организации. С теоретической точки зрения управление рисками в банковском секторе представляет собой логическую разработку и реализацию плана по предотвращению потенциальных убытков. На практике управление рисками реализуется в алгоритмах управления подверженностью кредитной организации убыткам или рискам, а также защите стоимости ее активов с помощью различных инструментов. Банковская деятельность (как и любая предпринимательская деятельность) всегда считалась рискованной. Однако с точки зрения трансформации бизнеса кредитные организации сталкиваются с куда более разнообразными и сложными к управлению видами

рисков (они не могут контролироваться в рамках одной операции, одного подхода – например, только процедурой андеррайтинга при кредитовании не может быть установлен уровень и способность клиента противостоять мошенническим действиям в будущем).

Угрозами (факторами, влияющими на возникновение угроз) здесь выступают достаточность уровня надежности существующих систем информационной безопасности кредитной организации, изменчивые ожидания клиентов, растущие случаи цифрового мошенничества, непредсказуемые изменения рынка. Многие риски трансформации сложно предвидеть, идентифицировать и устранить. Более того, клиенты кредитных организаций зачастую не отдают себе отчет в том, что их действия (под влиянием мошенников) могут привести не только к потере их личных сбережений, но и к штрафным санкциям и репутационному ущербу, который впоследствии понесет именно кредитная организация.

Базовая детерминанта управления рисками кредитной организации может рассматриваться как оценка или взвешивание возможности того, что отрицательный (не достижение показателей деятельности / невыполнение цели) результат может возникнуть из-за определенного действия, осуществления определенной деятельности или принятия определенного решения. Кредитная организация любого охвата и масштаба деятельности, будь она системообразующей государственной, крупной частной, либо мелкой региональной – не будет развиваться и не будет приносить достаточную прибыль, если не будет *приминать* риски, а также *противостоять* им. Из этого «правила» следует, что ни одна кредитная организация не может сделать исключение: управление рисками является фундаментальной частью банковской деятельности. Научная истина, сформулированная В.М. Безденежных, заключающаяся в том, что «по существу нет кроме системы управления рисками других механизмов, с необходимой эффективностью обеспечивающих экономическую безопасность организаций» [80], применима и к кредитным организациям. Е.А. Касюк

отмечает, что «успешное управление рисками резко оптимизирует текущие расходы учреждений, тем самым увеличивая общую финансовую эффективность, а также стабильность финансовых институтов» [105].

На практике в кредитной организации создается стратегия управления рисками, которая определяет все вероятные риски (с выделением наиболее вероятных к возникновению на данном этапе), а также методы управления ими, направленная на то, чтобы они не материализовались в будущем. Например, кредитная организация может использовать расширенный анализ и автоматизированный сбор данных для постоянного мониторинга своих операций – такой непрерывный, технологически поддерживаемый надзор за рисками помогает кредитным организациям разрабатывать и адаптировать ключевые индикаторы риска к изменяющейся среде, заранее *предупреждая* его возникновение.

Как было отмечено в первой главе работы, в рамках управления рисками (в том числе при проведении трансформации бизнес-процессов) кредитные организации проводят идентификацию рисков, их анализ и оценку, осуществляют мероприятия по смягчению последствий реализации рисков, проводят их мониторинг, выстраивают взаимосвязи между связующими элементами, связанными с управлением рисками, а также формируют соответствующую отчетность. Практическое применение подходов к управлению рисками в современной кредитной организации характеризуется следующими *недостатками*:

– недостаточность проработки возможных новых рисков – изменения, связанные с цифровой трансформацией, влекут за собой появление новых рисков, которые раскрыты в данном исследовании;

– отсутствие гибкости – традиционные модели управления рисками зачастую характеризуются сложной адаптивностью к изменениям, из-за чего в том числе замедляется реакция банковских структур на возникающие риски;

– проблемы обеспечения кибербезопасности – проблемы, связанные с тем, что во время проведения трансформации системы обеспечения

кибербезопасности проходят процедуры калибровки, либо глобального изменения, зачастую в период прохождения данных адаптивных процедур кредитные организации наиболее подвержены атакам извне [138];

– аналогично проблемам обеспечения кибербезопасности калибровке и обновлению подвергаются и процессы мониторинга, в связи с чем возникают сопутствующие риски;

– необходимость обновления нормативных политик и процедур – трансформация (особенно в настолько регулируемой банковской среде) сопряжена с большим количеством бюрократических процессов, кредитные организации корректируют текущие положения, вносят изменения в нормативные документы – процессы являются крайне трудоемкими и требуют прохождения большого количества этапов согласования на самых разных уровнях.

Банком России разработан ряд нормативно-правовых документов [21], направленных на установление процедур по управлению рисками и их анализу, в них описываются внутренние процедуры контроля за рисками. При анализе рисков конкретной кредитной организации мегарегулятор оценивает соблюдение кредитной организацией нормативов по достаточности капитала, включая оценку уровня рисков по крупным кредитам и финансовым операциям, таким как торговля ценными бумагами или кредитование частных лиц. Шкала рисков для кредитной организации реализована Банком России в формате рекомендуемого диапазона значений для каждого норматива достаточности собственных средств [22]. Если кредитная организация не выполняет установленные требования по достаточности собственных средств, она может быть признана финансово неустойчивой и лишена лицензии. Если показатели достаточности капитала кредитной организации длительное время соответствуют значениям критического уровня, она будет квалифицирована как рискованная.

Реализация макропруденциальной и денежно-кредитной политики осложняется ограничениями в виде роста бюджетных рисков и рисков

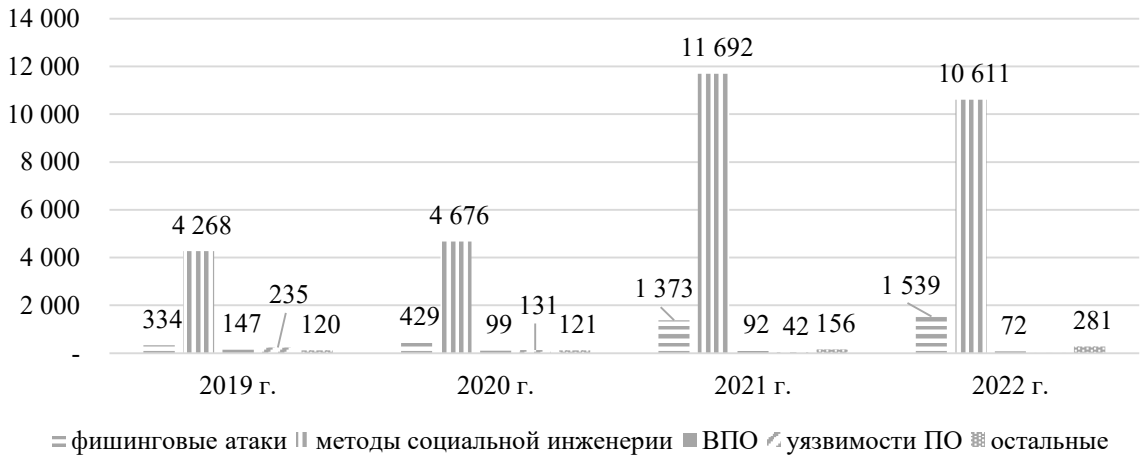
финансовой стабильности. В современных условиях нестабильной внешнеэкономической и внешнеполитической ситуации [90] банковская система Российской Федерации сталкивается с определенными трудностями. В приложении А представлены макроэкономические показатели, отражающие динамику развития экономики Российской Федерации и афтершоки (дополнительные негативные последствия или волнения, которые возникают после преодоления кризиса) российской экономики. Адаптация к перестройке хозяйственных связей и смягчение ее последствий для банковской системы Российской Федерации (корпоративный сектор и домохозяйства указаны справочно) представлены на рисунке 13.

Источник: составлено автором по материалам [29; 48].

Рисунок 13 – Адаптация к перестройке хозяйственных связей и смягчение ее последствий

Стоит отметить, что самые первые (и самые массированные) санкции были введены именно против финансового сектора [73]. Рынки отреагировали очень высокой волатильностью, курс рубля и фондовые индексы начали стремительно падать. Использование Банком России апробированных инструментов антикризисного управления (актуальность и важность которого подчеркивается, в том числе, в контексте деятельности кредитных организаций [133; 140]) нивелировало влияние негативных факторов, в результате чего показатели банковский сектора показали небольшой рост по

данным за 2022 год, что отражено в приложении Б. Влияние санкций на банковский сектор крайне велико [163] и «чувствуется» и по сей день, например, нарушения системы поставок для предприятий отражаются на банковской системе с отсроченным временным эффектом, что влияет на величину совокупного рыночного риска банковского сектора, что отражено в приложении В. Банковский сектор России также характеризуется недостаточным уровнем инвестиций в кибербезопасность и ИТ-обучение. Растущий риск кибератак, продемонстрированный в таблице 3 и на рисунке 14, и их существующее (в виде возмещения средств клиентам) и потенциальное воздействие на кредитные организации вызывают серьезную озабоченность Банка России.



Источник: составлено автором по материалам [40; 41; 42; 43; 44; 45; 46; 47].
Рисунок 14 – Динамика среднегодового значения инцидентов по типам и векторам кибератак (в единицах) в 2019–2022 гг.

Российские кредитные организации в основном сталкиваются с кибератаками с применением методов социальной инженерии, доля таких атак резко возросла в 2021 году. Социальная инженерия в контексте обеспечения экономической безопасности кредитной организации является значимой угрозой, поскольку ее применение основано на человеческих ошибках, а не на уязвимостях в программном обеспечении и операционных системах кредитной организации. Ошибки, совершаемые клиентами, гораздо менее предсказуемы, поэтому в сравнении атаками с использованием вредоносного программного обеспечения их сложнее выявить и предотвратить.

Таблица 3 – Динамика инцидентов по типам и векторам кибератак, направленных на клиентов финансовых организаций и финансовые организации в 2019–2022 гг.

В единицах

Типы и векторы кибератак	2019 г.			2020 г.			2021 г.			2022 г.			Темп прироста к пред. году (по среднеквартальным), в процентах		
	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	2020 г. / 2019 г.	2021 г. / 2020 г.	2022 г. / 2021 г.
Атаки, направленные на клиентов финансовых организаций (фишинговые атаки)	554	340	108	432	583	273	963	1 160	1 995	705	682	3 230	28,54	219,72	12,12
Атаки, направленные на клиентов финансовых организаций (с использованием методов социальной инженерии*)	6 466	4 462	1 876	4 806	4 589	4 634	10 136	11 173	12 211	9 691	8 781	13 360	9,57	150,02	-9,25
Атаки, направленные на финансовые организации (с использованием ВПО**)	172	251	17	102	103	93	56	112	107	50	34	132	-32,27	-7,72	-21,45
Атаки, направленные на клиентов финансовых организаций (с использованием уязвимостей ПО)	223	430	53	165	186	42	47	56	22	-	1	-	-44,33	-68,19	-99,20
Остальные инциденты	224	113	23	131	113	119	137	251	79	284	428	132	0,83	28,65	80,73
*Психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. ** Вредоносное программное обеспечение.															

Источник: составлено автором по материалам [40; 41; 42; 43; 44; 45; 46; 47].

Согласно оценке Банка России [40; 41; 42; 43; 44; 45; 46; 47], а также описанию, приведенному Н.В. Алексеевой, в 2021–2022 гг. «наблюдался стабильный рост средней суммы одного хищения, совершенного с использованием приемов и методов социальной инженерии, что в том числе привело к увеличению общего размера ущерба по операциям без согласия клиентов» [70]. В 2021–2022 гг. также значительно вырос риск побочных эффектов от кибератак, во многом это связано с развитием платежных систем.

Клиенты российских кредитных организаций имеют право на возврат средств – законодательство определяет, что кредитные организации должны возвращать деньги, снятые со счетов клиентов без их разрешения. Н.В. Алексеева также отмечает, что «в 2022 году клиентам кредитных организаций возвратили 4,4% (618,4 млн руб.) от всего объема операций по переводу денежных средств, совершенных без согласия клиентов (в 2021 году данный показатель составил 6,8%, или 920,5 млн руб.)» [70]. В 2020 году данный показатель составил 11,3%, или 1 105,3 млн руб., что продемонстрировано в таблицах 4 и 5 [40; 41; 42; 43; 44; 45; 46; 47]. Согласно проведенным расчетам, наибольшим объемом возмещения характеризуются выплаты по категории «Оплата товаров и услуг в Интернете», сумма за 3 квартала 2022 года составила 357,59 млн руб., что отражено в таблице 6 [40; 41; 42; 43; 44; 45; 46; 47].

Таким образом, с каждым годом в период с 2019 по 2022 год совокупный объем операций, осуществленных без согласия клиентов российских кредитных организаций, возрастал, при этом объем средств, которые удалось возместить, в это же период сокращалось. Усложнившаяся геополитическая ситуация привела к тому, что российские кредитные организации и их клиенты стали одной из приоритетных целей для мошенников со всего мира. Статистические данные указывают на то, что российские кредитные организации не всегда могут эффективно противостоять преступникам.

Таблица 4 – Динамика объема операций, осуществленных без согласия клиентов в 2019–2022 гг.

В миллионах рублей

ОБС по типу операций	2019 г.			2020 г.			2021 г.			2022 г.		
	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.
Банкоматы, терминалы, импринтеры	157,0	111,0	134,8	112,0	127,0	200,5	304,9	435,6	462,9	532,1	296,0	390,0
Оплата товаров и услуг в Интернете	669,0	603,0	838,7	926,0	1 122,0	1 182,4	879,2	857,0	900,6	953,5	582,0	592,4
Система дистанционного банковского обслуживания физлиц	397,0	460,0	742,9	559,0	728,0	944,6	1 126,8	1 239,2	1 688,0	1 660,9	1 807,5	2 722,8
Система дистанционного банковского обслуживания юрлиц	105,0	194,0	185,3	231,0	193,0	179,1	562,4	481,9	155,0	147,6	163,2	268,3

Источник: составлено автором по материалам [40; 41; 42; 43; 44; 45; 46; 47].

Таблица 5 – Динамика доли возмещенных средств в 2019–2022 гг.

В процентах

Доля возмещенных средств по типу операций	2019 г.			2020 г.			2021 г.			2022 г.		
	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.	I кв.	II кв.	III кв.
Банкоматы, терминалы, импринтеры	9,00	22,00	9,00	9,00	18,00	6,00	6,80	3,90	2,90	2,50	6,10	3,40
Оплата товаров и услуг в Интернете	22,00	24,00	19,00	17,00	16,00	19,00	18,90	22,10	22,90	17,70	18,50	13,70
Система дистанционного банковского обслуживания физлиц	9,00	13,00	7,00	3,00	6,00	5,00	1,50	1,30	1,90	1,10	0,90	1,00
Система дистанционного банковского обслуживания юрлиц	17,00	7,00	8,00	5,00	14,00	17,00	1,20	0,20	0,40	2,50	1,10	4,60

Источник: составлено автором по материалам [40; 41; 42; 43; 44; 45; 46; 47].

Таблица 6 – Расчет потерь банковской системы из-за возмещения средств клиентам в 2019–2022 гг.

В миллионах рублей

Потери по типу операций	2019 г.	2020 г.	2021 г.	2022 г.
Банкоматы, терминалы, импринтеры	50,68	44,97	51,15	44,62
Оплата товаров и услуг в Интернете	451,25	561,60	561,81	357,59
Система дистанционного банковского обслуживания физлиц	147,53	107,68	65,08	61,77
Система дистанционного банковского обслуживания юрлиц	46,25	69,02	8,33	17,83
Итого	695,72	783,26	686,37	481,81

Источник: составлено автором по материалам [40; 41; 42; 43; 44; 45; 46; 47].

Согласно оценке «РТК-Солар», «основной угрозой для финансовой отрасли являются высококвалифицированные хакерские группировки, так как периметр кредитных организаций и других крупных финансовых организаций обычно хорошо защищен и для его взлома нужны определенные технические знания и крупные финансовые вложения. Атаки злоумышленников средней и низкой квалификации в основном направлены на клиентов кредитных организации – в этих атаках используется социальная инженерия для прямой кражи денег со счетов» [49]. Наибольшие потери несут кредитные организации, которые не выделяют достаточно средств на обеспечение информационную безопасности и безопасности ИТ-систем.

Аналитики отмечают, что «в октябре – декабре 2022 года была зафиксирована 281 тыс. событий ИБ – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на треть превышает аналогичный показатель III квартала 2021 года (214 тыс. инцидентов), и это самый высокий квартальный показатель за весь 2022 год. При этом число подтвержденных инцидентов в IV квартале характеризовалось падением – почти на 20% (речь о сложных инцидентах, которые подтвердила кредитная организация)» [49].

Также исследователи «РТК-Солар» отмечают продуманность действий мошенников: «В целом картина типична для конца года: четвертый квартал, особенно декабрь, характеризовался резким всплеском событий ИБ. С одной стороны, предновогодняя суета и распродажи, с другой – поспешное закрытие финансового года, подготовка отчетов, финальные поставки. Все это активно используют злоумышленники в надежде на то, что в ворохе задач их действия останутся незамеченными. В 2022 году многие кредитные организации усилили защиту ИТ-периметра, и реализовывать несложные атаки хакерам стало сложнее» [49]. С момента начала политического обострения в 2022 году российский бизнес серьезно озаботился вопросами собственной киберзащиты, что продемонстрировано на рисунке 15.

Источник: составлено автором по материалам [49].

Рисунок 15 – Распределение инцидентов атак по степени критичности в 2022 году

В частности, была осуществлена «кастомизация сценариев детектирования инцидентов и реагирования на них, что в итоге и ознаменовало положительную динамику на общем фоне. Чтобы не допустить роста числа критических инцидентов, кредитным организациям важно своевременно выстраивать эффективные процессы выявления угроз и реагирования на них» [49]. Защиты периметра безопасности банка «держится» на двух ключевых факторах – экспертная команда и выстроенные бизнес-процессы. Кибератаки затрагивают банки по-разному. В дополнение к денежным потерям, которые возникают в результате кражи денег у кредитных организаций хакерами, кредитные организации несут дополнительные расходы на внедрение систем кибербезопасности для защиты цифровых (и не только) активов. Кроме того, кибератаки (эффективность реагирования на них банков) влияют на уровень доверия клиентов к кредитным учреждениям, а также на осуществление банковской операционной деятельности, зачастую нарушая (либо затормаживая) самые разные процессы, связанные с обеспечением бесперебойной работы кредитной организации. Можно сделать вывод, что кибератаки тем или иным образом относятся к разным типам риска – операционному, кредитному, репутационному и другим.

Таким образом, в рамках изучения специфики предметной области исследования установлено, что процессы управления рискам при осуществлении экономической безопасности как ключевого фактора, от которого зависит финансовая устойчивость кредитной организации,

претерпевают значимые изменения в ходе цифровой трансформации банковского сектора. Зачастую в кредитных организациях отсутствует системный подход в управлении рисками, скорее происходит точечная проработка наиболее подверженных опасности процессов (что подтверждается статистическими данными) – в контексте появления рисков, связанных с цифровизацией, которые способны повлиять на всю операционную систему кредитной организации, подобный подход может повлечь за собой серьезные проблемы, в том числе необеспечения экономической безопасности.

В целом текущие системы обеспечения безопасности на разных уровнях неэффективны с технической точки зрения (что опять же подтверждается статистикой): используется программное обеспечение, не позволяющее в реальном времени определить начало совершения атак (особенно их новых типов), оборудование не обладает нужными системными требованиями для внедрения более продвинутого программного обеспечения (что в том числе связано с изоляцией России от западных технологий), внутренние процедуры контроля характеризуются недостаточной гибкостью именно в контексте управления рисками цифрового контура.

Российские кредитные организации выстраивают алгоритмы оценки рисков в соответствии с методическими указаниями Банка России, однако в них (на момент написания диссертационного исследования) не прописаны подходы к управлению цифровыми рисками – как с методологической, так и с практической точки зрения. Общие рекомендации по обеспечению информационной безопасности не покрывают всего масштаба и изощренности угроз, на которые российским кредитным организациям предстоит отвечать. Природа рисков в современных условиях использования новых технологий (как кредитными организациями, так и преступниками, как гражданами, так и государством) является высокоизменчивой, методы управления рисками также должны характеризоваться достаточным уровнем гибкости. Статистически опасности и угрозы, относящиеся по специфике к цифровому

контуру, связаны в большей мере с операционной деятельностью кредитных организаций. Таким образом, необходимо исследовать существующие методы оценки подобных рисков, а также рассмотреть возможности их применения (и адаптации) относительно цифрового пространства.

2.2 Возможности применения методов оценки цифровых рисков организацией

В общем виде под таким определением как «банковский риск» предлагается понимать вероятность того, что события, как ожидаемые, так и непредвиденные, могут оказать неблагоприятное воздействие на капитал или прибыль кредитной организации (в том числе в рамках процессов цифровизации [97]). Риски оправданы, если они понятны, измеримы, контролируемы и находятся в пределах способности кредитной организации легко противостоять неблагоприятным обстоятельствам.

Рассмотрим методы оценки и учета рисков, применяемые кредитными организациями и ведущими рейтинговыми агентствами. Эксперты McKinsey применительно к кредитным организация предлагают оценивают девять видов рисков: «Кредитный, ликвидный, процентный, ценовой, валютный, транзакционный, стратегический, репутационный и комплаенс-риск» [177]. По их мнению, значения и динамика именно этих девяти рисков дают исчерпывающую картину системы управления рисками в кредитной организации в том виде, в каком она существует сегодня, а также позволяют обнаружить проблемы, стоящие перед кредитной организацией в обозримом будущем. Влияние каждого из рисков на прибыль и капитал зависит от специфики работы конкретной кредитной организации и может меняться с течением времени. Кроме того, некоторые из этих рисков являются подвидами других, основных с точки зрения теории категорий рисков. Например, процентный, ценовой и валютный риски исследователи часто обозначают

«рыночным» риском. Российскими авторами также выделяются риски инкорпорирования цифровой валюты в экономику страны [127].

Риски различных видов взаимосвязаны. Любой банковский продукт или услуга, как правило, подвергают кредитную организацию одновременно ряду рисков, и эти риски часто влияют друг на друга. Например, трудно напрямую определить точный уровень кредитного риска как такового по сравнению с процентным риском по кредиту. Существующий контекст взаимосвязи различных рисков (особенно значимым является операционный риск, приобретающий новые формы в условиях цифровизации) требует определенного комплексного подхода к управлению ими, что особенно актуально в условиях динамично изменяющейся среды российского банковского сектора.

В зарубежных методиках [178] подчеркивается, что нет необходимости в определении точной суммы каждого риска в конкретном продукте или услуге. Новейшие зарубежные методики оценки рисков для кредитных организаций включают модули определения рисков на основе рейтинговых показателей в областях: мобильный банкинг, удаленное открытие вклада, электронный банкинг, использование социальных сетей клиентами. После выявления конкретных видов рисков осуществляется разработка общей основы для документирования решений по управлению ими. Некоторые аспекты системы оценки рисков различаются в зависимости от того, является ли кредитная организация крупной или системно значимой.

В системе оценки рисков для крупных организаций обычно в основу документации по принятию решений о рисках включаются такие аспекты, как уровень риска, эффективность управления рисками, общая и составная оценка риска, а также направление его воздействия:

а) *Количество риска* – это уровень или объем существующего риска. Количество подразумевает измерение. Но «измерение» не всегда означает количественную оценку этих рисков в прямом денежном или процентном

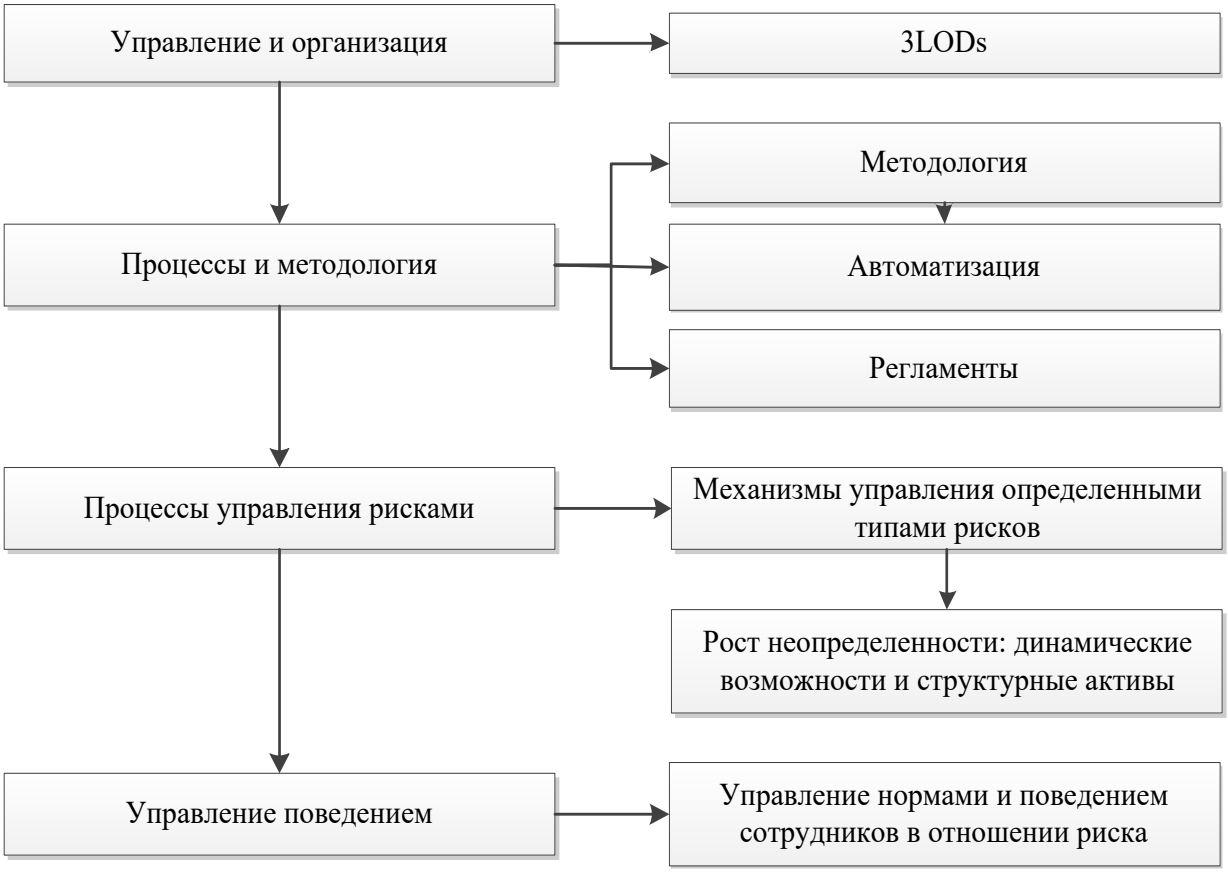
выражении. Например, количественную оценку транзакционного или комплаенс-риска трудно выполнить в денежном выражении.

б) *Качество управления рисками* оценивается как слабое, приемлемое или сильное. Управление рисками – это внутренний процесс организации, который не просто измеряет количество рисков. Это перспективный и активный процесс. Эффективный процесс управления рисками должен выявлять, измерять, отслеживать и контролировать риски. Процесс должен повышать рыночную стоимость организации, обеспечивая последовательность, проактивную культуру, эффективную коммуникацию и координацию всех подразделений организации (с особым выделением подразделения по внутреннему мониторингу рисков [68]).

в) *Совокупный и составной риск*. Совокупный риск отражает уровень количества рисков организации, сопоставленных с качеством управления рисками. Совокупный риск классифицируется как низкий, умеренный или высокий. Составной риск включает динамику двух рисков – стратегического и репутационного риска, и он классифицируется как низкий, умеренный или высокий. Составной риск похож на совокупный риск, за исключением того, что он более одномерный.

г) *Направление риска* отражает вероятные изменения совокупного или составного профиля риска в течение определенного срока (например, следующих 12 месяцев), оно описывается с точки зрения возрастания, стабильности или убывания и означает, что совокупный риск имеет восходящий либо нисходящий тренд, или остается неизменным. Для системно значимых кредитных организаций, которые характеризуются более сложными и разнообразными банковскими операциями, а также присутствием во всех регионах страны, существуют области повышенного риска.

Система оценки и учета рисков в организации (включающая применяемые методики оценки риска) состоит из четырех основных уровней, отраженных на рисунке 16.



Источник: составлено автором.
Рисунок 16 – Система оценки и учета рисков организации

а) *Управление и организация.* Данный уровень охватывает структуру подотчетности (*три линии защиты* [176]), определяя распределение и источники возникновения рисков, уровень контроля за рисками и подотчетность по гарантиям, которые осуществляются через комитеты по рискам и формализуются в рамках соответствующих политик организации. Этот уровень также включает базовую таксономию рисков для распределения ответственности руководства / подразделений организации.

б) *Процессы и методология.* На данном уровне определяются общий подход к управлению рисками в организации и процессы, сопутствующие подходу. Как правило, они сосредоточены на структурах лимитов. Профиль риска «управляется» с помощью многочисленных методов: управление инцидентами, оценка и контроль, риск-аппетит, процессы мониторинга и отчетности.

в) *Процессы управления рисками*. Этот уровень охватывает все механизмы, направленные на управление конкретными видами и категориями рисков. Важно отметить, что обычно объем данных, используемых для поддержки этих процессов, не способен полностью учитывать внезапные технологические изменения, кризисы в сферах здравоохранения и климата, а также быстро меняющиеся тенденции в социальных сетях, связанные с поведением клиентов. Стресс-тестирование банковских процессов / процедур / продуктов в современных реалиях должно проходить регулярно, а возможные сценарии должны учитывать широкий набор потенциальных результатов.

г) *Динамические возможности* (динамическое управление риском). Способность организации адаптироваться и реагировать на изменяющиеся условия и угрозы в реальном времени, в современных условиях может реализовываться с помощью использования больших данных, аналитики для мониторинга рисков, принятия оперативных решений, а также корректировки стратегий управления рисками в соответствии с высоковолатильной изменяющейся средой.

д) *Структурные активы*. Хотя капитал и наличие денежных резервов играют важную роль в процессах по минимизации рисков, для успешного преодоления сбоев в работе организациям также требуется акцентировать внимание на других аспектах поддержания устойчивости, например, развитии организационных компетенций, укреплении цепочек поставок (в рамках проектов, в которых организация принимает участие), расширении технологических возможностей, поддержке позиций на рынке, поддержании стабильного уровня репутации, реализации устойчивого развития и соответствии социальным ожиданиям.

е) *Управление поведением*. Под управлением поведением подразумевается регулярное проведение мероприятий, направленных на формирование и поддержание сознательного и ответственного отношения сотрудников к взаимодействию с рисками, а также на создание подходящей

организационной культуры в данной сфере: обучение и обратная связь; установление стандартов и нормативов по управлению рисками; поощрение сотрудничества подразделений в части противостояния рискам и обмена знаниями); мотивация и стимулирование сотрудников.

В связи с тем, что управление рисками в банковской отрасли строго контролируется Банком России, в системно значимых кредитных организациях до 10% сотрудников могут быть вовлечены в процессы, связанные с управлением рисками. Кредитные организации создают серьезные централизованные структуры управления рисками, чтобы соответствовать все более строгим нормативным требованиям, более эффективно и на постоянной основе выявлять причины возникновения рисковых ситуаций. Методы оценки и учета рисков, применяемые кредитными организациями, включают широкий спектр показателей оценки рисков. На практике они незначительно отличаются друг от друга и реализуются разными способами, поэтому первая задача при составлении методических рекомендаций состоит в том, чтобы убедиться, что все оценки рисков согласованы, а также используется общий язык «транскрипции» показателей.

Кредитные организации внедряют в методологии оценки рисков следующие основополагающие элементы: *таксономия рисков* – категоризация общих категорий рисков, специфичных для банковского бизнеса, в целях определения того, какие именно риск-сущности следует измерять; *терминология и показатели оценки рисков* – определение терминов и ключевых показателей, используемых для измерения и оценки рисков, в целях согласованности в понимании рисков внутри организации и соблюдения единых стандартов оценки; непосредственно *процесс оценки рисков* – определение основных правил для оценки воздействия рисков на деятельность кредитной организации, а также формирование подходов к приоритизации рисков.

Используемые на практике методы оценки рисков подразделяются в

соответствии с исходной и результирующей информацией на количественные и качественные. Их описание кратко приведено в таблице 7.

Таблица 7 – Качественные и количественные методы анализа рисков

Подвид метода	Метод	Сущность метода
Качественный	Метод аналогий	Предусматривает сравнение объектов на основе различных характеристик, связанных с риском
	Идентификация рисков	Включает сбор и детальный анализ информации о бизнес-процессе и связанных с ним рисках
	Причинно-следственный анализ	Включает выделение рисковых событий на основе эвристики, анализ их причин с использованием формальной логики и разработку мер по снижению риска
	Метод «События – последствия»	Предполагает разбиение бизнес-процесса на составляющие для выявления рисков на каждом этапе
Количественный	Корректировка нормы дисконтирования	Включает увеличение ставки дисконтирования в зависимости от общего уровня рисков, влияющих на бизнес-процесс
	Метод достоверных эквивалентов	Предполагает корректировку денежных потоков экспертами на основе субъективной оценки уровня рисков, связанных с их получением
	Анализ показателей эффективности и динамики денежного потока	Включает анализ устойчивости бизнес-процесса с использованием относительных показателей
	Анализ чувствительности	Посредством поочередных изменений в отдельных технико-экономических параметрах бизнес-процесса определяются наиболее значимые риски
	Метод сценариев	Путем одновременных изменений в нескольких технико-экономических параметрах создаются альтернативные сценарии развития процесса
	Имитационное моделирование	Включает создание финансовой модели и многократный расчет возможных сценариев бизнес-процесса с учетом взаимосвязи его параметров
Количественно-качественный	Метод экспертных оценок	Основной фигурой метода является эксперт, который использует логические и математико-статистические методы для оценки рисков
	Создание профиля рисков или карты рисков	Включает оценку рисков проекта по различным параметрам с их последующим отображением на соответствующих шкалах, для сравнения полученного профиля с эталонным

Источник: составлено автором по материалам [125].

Также достаточно эффективным качественным методом является *матрица оценки риска* (также известная как матрица оценки вероятности риска). Она представляет собой визуальный инструмент, который отображает потенциальные риски, влияющие на бизнес. Матрица оценки вероятности риска основана на двух пересекающихся факторах: вероятность того, что событие риска произойдет, и потенциальное влияние, которое событие риска окажет на бизнес. Другими словами, это инструмент, который помогает визуализировать вероятность потенциального риска и его влияние на экономическую безопасность организации. В данной матрице выставляется значение влияния риска в зависимости от уровня безопасности, на котором этот риск может проявить себя.

Например, отключение России от межбанковской системы передачи информации и совершения платежей (далее – SWIFT), примененное западными странами в качестве одной из самых жестких санкционных мер, можно классифицировать как риск высокого уровня – событие, которое имело высокую вероятность наступления после политических обострений и оказало значительное влияние на банковский сектор России, так переход на альтернативные системы потребовал значительного количества времени, а также затрат.

Базовая матрица оценки рисков может быть представлена путем визуализации различных рисков в виде таблицы, где каждый риск классифицируется исходя из его степени серьезности и обозначается соответствующим цветом. Высокие риски, которые могут нанести значительный ущерб организации, помечаются красным цветом, умеренные риски, которые также могут повлиять на работу организации, но не требуют срочных мер, обозначаются желтым цветом, низкие риски, которые не представляют существенной угрозы, отмечаются зеленым цветом. Например, матрица рисков условной организации может быть представлена в формате, отраженном на рисунке 17.

Уровни формирования политики и механизмов обеспечения экономической безопасности / Риск	Кредитный	Операционный	Рыночный
Уровень 1: собственники и акционеры			
Уровень 2: руководство			
Уровень 3: оргструктура, персонал			
Уровень 4: построение бизнес-процессов			
Уровень 5: клиенты			
Уровень 6: техническое обеспечение операций			

Источник: составлено автором.

Рисунок 17 – Шаблон матрицы рисков условной организации

Качественный анализ и количественный анализ – две ключевых совокупности методов, используемых в процессе принятия решений по управлению рисками. Качественный анализ основан на оценке вероятности возникновения рисков и их потенциальных последствий, способствует идентификации основных рисков и проблем, влияющих на принятие решений, а также является основой для последующего количественного анализа. Количественный анализ предполагает использование конкретных числовых данных для оценки вероятности и величины рисков, может включать статистические модели, математические расчеты и сценарные прогнозы. Эффективное сочетание качественного и количественного анализа позволяет организациям более точно и комплексно оценивать риски, управлять ими, а также принимать обоснованные стратегические решения в рамках динамичной, сложной и технологичной банковской среды.

Количественные методы анализа рисков многогранны, с технико-технологическим развитием экономики, статистики (и других совокупных отраслей знаний, исследующих явления в числовой форме) они расширяются и развиваются. Можно выделить следующие группы количественных методов анализа (расширенный перечень относительно тех методов, что были рассмотрены ранее):

– *статистические методы* (основаны на анализе и интерпретации данных);

– *логико-вероятностные методы* (используют различные модели для оценки рисков и принятия решений, они могут применяться для моделирования различных сценариев и оценки вероятностей реализации

каких-либо событий);

– *аналитические методы* (включают в себя различные подходы к оценке рисков, основанные на проведении анализа, которые, опять же, позволяют выявлять ключевые факторы, влияющие на риски, зачастую на основе числовых показателей).

Каждый из этих методов имеет свои преимущества и ограничения, и выбор конкретного метода зависит от целей организации, доступных данных, сложности ситуации и других факторов. Количественные методы современного типа требуют применения системного подхода. Кредитные организации оценивают риски с помощью совокупности различных количественных методов, отраженных на рисунке 18, применяя более централизованный подход в силу усиленного пруденциального надзора (в отличие от сугубо традиционного подхода, основанного на бизнес стороне рисков).

Источник: составлено автором по материалам [88; 125; 166].

Рисунок 18 – Количественные методы оценки рисков кредитных организаций

Наибольшую популярность в аналитической деятельности организаций разных отраслей экономики при оценке рисков получили следующие методы: дерево событий, анализ чувствительности, сценарный анализ, имитационное моделирование. Описание методов приведено в таблице 8.

Таблица 8 – Методы оценки риска организаций

Метод	Описание метода	Применяемые показатели оценки
Дерево событий	Составление схемы проблем и возможных рисков, служащей основанием для ранжирования рисков	Балльная шкала
Анализ чувствительности	Исследование изменений значений критических параметров финансовой модели организации и показателей, связанных с операциями / бизнес-процессами	Показатели эффективности, достаточности капитала
Сценарный анализ	Определение ключевых факторов, подлежащих одновременным изменениям, и разработка стандартов для оценки значимости риска	2–4 фактора, которые оказывают наибольшее влияние на результаты деятельности организации
Имитационное моделирование	Аналогично анализу чувствительности, каждому сценарию развития событий на основе экспертных оценок присваивается вероятность его реализации с использованием моделей, имитирующих поведение реальных систем	2–4 фактора, которые оказывают наибольшее влияние на результаты деятельности организации

Источник: составлено автором по материалам [11; 88; 125].

Дерево событий представляет собой графическое изображение последовательности событий, начиная с исходного события (например, изменение рыночных условий или финансовый кризис), и далее отображает возможные последствия или варианты развития событий. Перед составлением схемы потенциальных проблем и возможных рисков производится: анализ бизнес-среды и экономики в целом; анализ отрасли / отраслей, в которой находится большая часть кредитного портфеля организации [96; 152]; анализ («понимание») сущности управленческой команды, а также структуры собственности организации. Дерево событий подразумевает ранжирование вероятности событий, при которых, например, может произойти дефолт или организация понесет убытки в результате внедрения нового продукта. Цифровые технологии могут применяться в данном случае для

прогнозирования событий, в том числе моделирования изменений параметров внешней среды.

Анализ чувствительности, сценарный анализ, имитационное моделирование. Эти методы предполагают каскадирование общей методики количественного анализа до управленческих алгоритмов. Алгоритмы в данном случае включают следующие элементы: четкий задокументированный процесс оценки рисков и определения того, должен ли риск привести к определенной сумме убытка; политика и процедуры, разработанные для обеспечения того, чтобы организация выявляла, измеряла и сообщала обо всех существенных рисках, в том числе требующих инвестиционных вложений в рамках борьбы с ними; процесс, который связывает капитал с текущими и ожидаемыми будущими уровнями риска в соответствии с аппетитом организации к риску; процесс, в котором устанавливаются цели достаточности капитала с учетом рисков, стратегической направленности организации и применяемой бизнес-модели; процесс внутреннего контроля (необходимость усиления которого отмечается и в научных работах [66]), регуляторных обзоров и аудитов для обеспечения целостности общего процесса управления рисками.

Стоит отметить, что при соотнесении капитала с уровнем риска кредитным организациям необходимо учитывать ряд факторов: сравнение собственного уровня капитала с нормативными стандартами и с показателями других кредитных организаций; рассмотрение выявленных «концентраций» рисков в кредитной и прочей деятельности; оценка текущих рейтингов аналитических агентств (для оценки уровня цифровой трансформации применимо, например, в отношении рейтинга мобильных приложений кредитных организаций); оценка потенциальных серьезных неблагоприятных событий, основанных на историческом опыте либо самой организации, либо рынков, на которых организация ведет бизнес, а также оценка неисторических сценариев; анализ осуществленных запланированных изменений в

бизнес-планах или стратегических планах кредитной организации, а также изменений ее операционной среды, инициированных цифровизацией.

При оценке достаточности капитала по отношению к риску и при принятии решений о надлежащем уровне и структуре капитала кредитные организации могут продолжать в значительной степени полагаться на задокументированные качественные оценки рисков. Качественные описания рисков могут включать неявные или явные нормативные и рыночные ожидания, анализ сопоставимых групп, а также результаты перспективных стресс-тестов и анализов чувствительности компонентов рисков, которые должны покрываться капиталом (что в свою очередь может быть также использовано и в отношении рисков, которые не поддаются прямой количественной оценке, например, репутационного риска).

Проведенный анализ существующих методов оценки риска позволил выделить: преимущества каждого метода в отношении оценки рисков, связанных с цифровизацией; возможность их применения и адаптации к подобным рискам; виды рисков, в отношении которых данный метод по мнению автора сможет дать лучший результат, что отражено в таблице 9. Результаты анализа позволяют констатировать, что существующие методы в той иной степени пригодны для описания вероятностей и событий, связанных с возможными рисками, например, при помощи методов имитационного моделирования могут быть обработаны большие объемы данных.

Таблица 9 – Результаты анализа существующих методов оценки риска с точки зрения их применения в рамках функционирования организации в цифровом контуре

Метод оценки риска	Преимущества и недостатки методов с точки зрения их использования для оценки рисков, связанных с цифровизацией	Возможности применения методов и их адаптация	Направления применения / риск, в отношении которого применение метода даст наилучший результат
1	2	3	4
Дерево событий	Позволит качественно описать вероятные события, связанные с рисками цифровизации	Позволит проранжировать риски, связанные с цифровизацией, по степени их влияния на безопасность	Возможность описания вероятных событий для операционного риска (например, недостаточность инвестиций в обеспечение безопасности мобильного приложения может повлечь за собой его сбой)

Продолжение таблицы 9

1	2	3	4
Анализ чувствительности	Позволит оценить чувствительность бизнес-процесса организации к рискам, связанным с цифровизацией	Позволит оценить критические значения реализации рисков, связанных с цифровизацией	Целесообразно использовать в качестве инструмента управления операционным риском (например, насколько сильно повлияет операционный сбой в системе платежей на операционную прибыль организации)
Сценарный анализ	Установление перечня критических факторов, которые будут изменяться одновременно при реализации риска, связанного с цифровизацией	Позволит оценить критические значения реализации рисков, связанных с цифровизацией	Целесообразно использовать в качестве инструмента управления рыночным риском (например, насколько актуален вопрос доработки мобильного приложения, добавления новых функций)
Имитационное моделирование	Аналогично анализу чувствительности (например, на основе данных о количестве мошеннических инцидентов в приложении) возможно оценить влияние цифровизации на потери организации	Позволит оценить критические значения реализации рисков, связанных с цифровизацией	Аналогично анализу чувствительности целесообразно использовать в качестве инструмента управления операционным риском

Источник: составлено автором и опубликовано [139].

Для построения эффективной системы учета и оценки рисков в организации возможно использовать теорию стратегирования В.Л. Квинта. По состоянию на начало 2023 года в научной литературе представлено несколько вариантов практической адаптации стратегирования применительно к различным отраслям народного хозяйства. В монографии В.Л. Квинта и С.Д. Бодрунова [4] приводятся оценки и взгляды авторов на глобальные тренды трансформации общества в современную эпоху, на предопределяемые этими трендами стратегические приоритеты и цели общественного развития, обозначаются возможные пути их достижения для реализации национальных интересов (стоит отметить, что в исследованиях, посвященных национальной безопасности России, различные авторы выделяют банковский сектор как одну из главных составляющих ее обеспечения [112; 165; 168]). На основе этих взглядов применительно к формированию стратегии оценки и учета рисков можно выделить три ключевых компонента стратегирования:

а) При внедрении новых технологий в организацию необходимо определить приемлемые уровни риска, разработать набор мер по его

снижению и объединить все эти элементы в стратегию изменений для последующей мобилизации сотрудников. После того как стратегия будет сформулирована, она может быть каскадирована внутри подразделений организации по тактическим планам, каждый из которых подразумевает ведение регулярной риск-отчетности с помощью средств автоматизации.

б) Для трансформации кредитных организаций в полноценные технологические компании финансовой индустрии требуется значительное расширение знаний о технологиях и связанных с ними рисках на уровне совета директоров (или иного главного управляющего органа), а также в масштабах всей кредитной организации. Данный процесс может быть осуществлен с помощью проведения регулярных встреч ИТ-лидеров кредитной организации с топ-менеджерами, а также с помощью проведения обучения для руководителей разных уровней. Изменение мышления на уровне совета директоров должно сопровождаться соответствующей поддержкой на операционном уровне. Процесс внедрения технологий должен быть подкреплен концепцией совместного подхода к работе. На практике работа по управлению изменениями возглавляется бизнес-подразделениями, реализовывается ИТ-подразделениями и контролируется службами поддержки – целесообразно же эту деятельность осуществлять в формате кросс-функциональных команд, в которых есть специалисты разных сфер (и ИТ, и бизнеса, и поддержки), за счет чего будет происходить обмен опытом, а также увеличатся шансы успешного завершения проекта по интеграции технологии в деятельность, так как специалисты смогут органично дополнять друг друга и превентивно выявлять потенциальные опасности и риски.

в) Перенос акцента с организационного мышления на управленческое. Безусловно, кредитные организации должны соблюдать регуляторные требования и следовать принципам, описанным во внутренних документах. Однако зачастую кредитные организации слишком «жестко» интерпретируют подобные правила и требования, в некотором смысле «сковывая» сотрудников в процессах реализации технологических изменений. Руководство кредитной

организации, а также подразделения контроля и аудита должны осознавать всю сложность внедрения технологий – от процессов поиска наилучшего решения до бесчисленного количества этапов согласования изменений. Процесс внедрения не должен отягощать ИТ-команды «нормативным бременем», должен соблюдаться баланс между важностью и необходимость соблюдения требований и их излишней строгостью.

Стоит отметить, что риски, возникающие в рамках деятельности кредитной организации в цифровом контуре, не проявляются в «чистом» виде, как скажем, например, кредитный риск. Действие подобных рисков (зачастую, не во всех случаях) является промежуточным, и ведет к возникновению определенного традиционного риска. Возникающие угрозы, например, связанные с действиями киберпреступников, не содержат достаточного объема ретроспективных данных, в силу чего сопутствующие риски являются более неопределенными, чем традиционные. Таким образом, и методы оценки для подобных «цифровых» рисков должны быть соответствующими – учитывать их двойственную природу (могут быть идентифицированы как в качестве полноценных рисков, так и в качестве факторов для возникновения традиционных рисков), а также необходимость проведения всестороннего многофакторного анализа, в том числе и с использованием новых неочевидных аналитических методов (именно в контексте анализа кредитной организации) [101], основанных на принципах математической экономики и системного анализа, являющихся прикладным решением задачи по оценке сложных экономических и технических систем.

2.3 Разработка методических рекомендаций по оценке цифровых рисков организации при обеспечении экономической безопасности

Проведенное исследование трансформации бизнес-моделей развития кредитных организаций на основе риск-ориентированного подхода показало, что «риски кредитных организаций активно эволюционируют под влиянием

различных факторов развития общества, науки и технологий, изменяются под воздействием мер и инструментов противорискового характера, инициируемых центральными банками и надзорными органами» [139]. Результаты исследования, отраженные в предыдущих параграфах, свидетельствуют о том, что цифровые риски, присутствующие в практике деятельности кредитных организаций, необходимо *идентифицировать* (так как вопрос определения и идентификации цифровых рисков недостаточно изучен), и на основе проведенной идентификации следует разработать методические рекомендации по оценке подобных рисков.

Изучение теоретических подходов к определению «риска», приведенное в первой главе исследования, позволяет сделать вывод, что цифровой риск должен быть связан с достижением целей организации при внедрении организацией цифровых технологий. Цифровые технологии, в свою очередь, помимо очевидных преимуществ несут в себе и угрозы в рамках достижения целей организации (цели определяют как задачу получения прибыли [108], так и операционные задачи, например, по развитию технологий). В контексте цифровизации главной угрозой является недостижение цели по внедрению цифровых технологий.

Таким образом, по итогам изучения теоретических и регуляторных подходов к определению «риска», определению «цифрового риска», а также рассмотрения риска в контексте цифровизации можно сделать вывод, что наиболее полное определение «цифрового риска» должно:

– отражать риск во взаимосвязи с достижением целей организации;

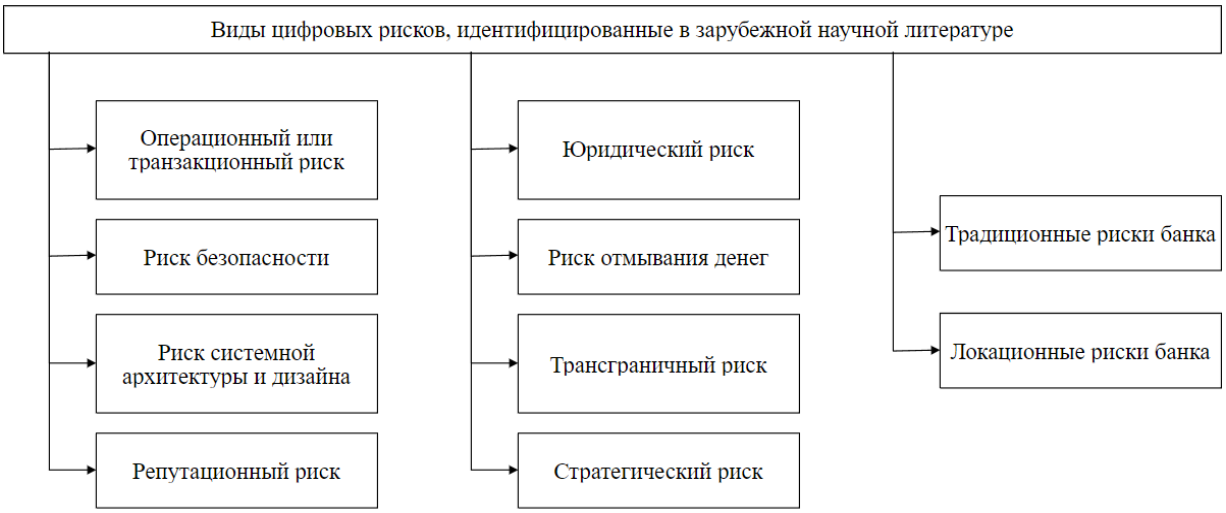
– отражать отличие угрозы (определяет причины и условия возникновения риска) и риска (оценка и ранжирование последствий возможной реализации рискового события в рамках принятия решений по достижению цели).

Данный подход позволяет установить причинно-следственную связь по принципу «галстук-бабочка», то есть сначала угроза может привести к реализации рискового события, далее рисковое событие может привести к

рисковому (или нескольким) исходу, препятствующему достижению цели. Этот принцип дает возможность подсчета вероятностей и рискового события и далее его последствий. После количественных оценок идет выбор решений по более надежному достижению целей.

Под «*цифровым риском* автор предлагает понимать вероятность недостижения (частичного достижения) установленных целей организации при использовании организацией передовых цифровых технологий» [139]. Под *митигацией цифрового риска* автор предлагает понимать скоординированную корректировку аналитики, данных, передовых цифровых технологий и бизнес-процессов, направленную на реализацию установленных целей организации (доведение отклонений до допустимого уровня). Данные определения сформулированы с целью уточнения текущих подходов к понятию «цифрового риска», отраженных в первом параграфе первой главы.

Стоит отметить, что цифровые риски рассматриваются в основном в зарубежной научной литературе [175; 186; 200] – виды цифровых рисков, предложенные зарубежными авторами, продемонстрированы на рисунке 19.



Источник: составлено автором.

Рисунок 19 – Виды цифровых рисков, идентифицированные в зарубежной научной литературе

Во многом подходы к определению рисков, связанных с цифровизацией, предложенные зарубежными авторами, идентичны предложениям российских авторов (аналогично выделяется операционный риск, риск безопасности,

репутационный риск, юридический риск, стратегический риск и другие), однако зарубежные исследователи в том числе делают акцент на прикладном характере рисков, выделяя некоторые специфические виды (этим обусловлено обозначение подхода зарубежных авторов именно в текущей «практической» главе, так как прикладной подход имеют и предложенные в дальнейшем методические рекомендации, которые во многом связаны с данными рисками), например, *риск системной архитектуры и дизайна*. В контексте деятельности по проектированию систем безопасности техническими специалистами под *дизайном* понимается макет или структура такой системы, подразумевающая некую план-схему технологий по обеспечению безопасности организации (системы контроля доступа, камеры наблюдения, датчики и сигналы тревоги, которые интегрируются друг с другом). Безопасность бизнес-операций в онлайн-формате формируется системной архитектурой и соответствующими средствами контроля, внедренными организацией. Выбор «конструкции» построения системы, выбор технологических инструментов, определение членов ИТ-команды / подрядчика – все это сопряжено с рисками возможного нарушения информационной безопасности, а также неэффективности системы и, соответственно, зависящих от нее бизнес-процессов.

Стоит отметить, что зарубежными исследователями также выделяется *трансграничные риски* (связанные с трансграничными переводами и подверженностью экосистемы трансграничных платежей кибератакам) и цифровые риски, *связанные со страной местоположения кредитной организации,* например, в случае с российской банковской системой наибольшие проблемы в настоящее время возникают у кредитных организаций, чья деятельность, так или иначе, ранее была международной, поскольку в результате ограничительных санкций отменена (или осложнилась) возможность осуществления международного расчетно-кассового обслуживания для кредитных организаций в таких отраслях как торговля (особенно в сфере поставки сырья, комплектующих, оборудования), логистика, добыча ископаемых (нефтегазовый сектор),

строительство, а также сфера информационных и телекоммуникационных технологий.

В контексте формирования подхода к оценке цифровых рисков необходимо сделать акцент на такой сущности как «экосистема». Поскольку цифровизацией охвачено большинство бизнес-процессов кредитных организаций, можно констатировать, что они присущи каждой кредитной организации (как активно осуществляющей внедрение цифровых технологий, так и просто использующей «блага цивилизации» для «облегчения» работы), однако степень влияния цифровых рисков на эффективность деятельности кредитной организации варьируется и напрямую зависит от уровня ее цифрового развития. Многие современные российские кредитные организации развиваются как *экосистема*. Соответственно появление цифровых рисков также можно рассматривать через «призму» экосистемы. Для определения рисков, связанных с участием кредитных организаций в экосистемах, Банк России предлагает использовать три модели [32], учитывающие разную роль, степень участия и делегирования полномочий кредитной организации в них. Центральный банк выделяет три типа функционирования кредитной организации в рамках экосистемы: во-первых, кредитная организация может быть дочерней структурой, во-вторых, кредитная организация, являясь центральным элементом экосистемы, может объединять участников в ней на партнерской основе (например, АО «Тинькофф Банк»), и в-третьих, кредитная организация может быть и центральным звеном, и учредителем компаний, входящих в экосистему (например, ПАО «Сбербанк») [32]. Стоит отметить, что рыночные риски в данном случае растут от первой модели к третьей, поскольку кредитная организация «входит» в экосистему всем своим капиталом.

Изучение теоретических аспектов построения системы управления рисками кредитной организации как инструмента обеспечения экономической безопасности, классификаций рисков, сформулированных авторами научных трудов, аналитическими агентствами, а также отраженными законодательно,

рассмотрение научных подходов к трансформации бизнес-моделей кредитной организации на основе цифровизации бизнес-процессов, включая исследование непосредственно применяемых цифровых технологий, изучение особенностей регулирования бизнес-процессов и возникновения рисков кредитной организации в условиях цифровизации, выделение типов рисков, связанных с цифровизацией, отраженных в научных трудах, а также изучение соответствующей статистической информации позволили идентифицировать цифровые риски, а именно:

а) Установить внешние и внутренние причины возникновения цифровых рисков кредитных организаций, отраженные на рисунке 20, каждая из которых в большей или меньшей мере влияет на появление каждого из видов цифрового риска (важно отметить именно совокупное влияние каждой причины, конкретная причина не влечет за собой конкретный риск);

б) Идентифицировать бизнес-процессы, на которых проявляются определенные виды цифровых рисков, что отражено в таблице 10.

Источник: составлено автором.

Рисунок 20 – Внутренние и внешние причины возникновения цифровых рисков кредитных организаций

В таблице 10 каждый цифровой риск оценен исходя из того, с какой силой данный риск может себя проявить на конкретном бизнес-процессе. С позиции общенаучных подходов в менеджменте [169] предлагается оценивать степень влияния в диапазоне от 0 до 1 баллов, где 0 означает отсутствие или незначительное влияние, 0,5 – умеренное влияние, а 1 – сильное влияние. Представленные ниже данные основаны на опросе пяти экспертов, занимающихся управлением рисками в крупнейших российских кредитных организациях

Слабое влияние (0) – последствия отсутствуют либо возникают в рамках одного подразделения, не влияют на деятельность кредитной организации в целом и могут привести к:

– судебным актам, актам исполнительных органов власти, Банка России, не приводящим к приостановке деятельности или уплате штрафов;

– неисполнению обязательств по сделке или неоказанию услуги;

– замедлению работы информационных систем, оказывающему незначительное влияние на качество и скорость обслуживания клиентов;

– снижению качества предоставления услуг, выполнения операций;

– увеличению сроков проекта не более чем на две недели;

– незначительному влиянию на вторичные функции в рамках проектной деятельности.

Умеренное влияние (0,5) – последствия, которые могут привести к:

– частичной приостановке деятельности одного или нескольких подразделений кредитной организации в результате, например, технологического сбоя систем низкого или среднего уровня критичности;

– частичной утечке или искажению защищаемой информации, не приводящей к существенным последствиям для кредитной организации;

– возникновению уязвимостей в объектах информационной инфраструктуры, программном обеспечении и приложениях, процессах;

– ограничениям, приводящим к выполнению невыгодных действий, накладываемым со стороны суда, органов власти, Банка России;

– оттоку клиентов (меньше одного процента от всей клиентской базы);

– увеличению сроков проекта на две недели – один месяц;

– незначительному влиянию на задачи и сроки достижения целей.

Сильное влияние – последствия, которые могут привести к:

– частичной приостановке деятельности Банка в результате, например, технологического сбоя систем высокого уровня критичности;

– частичной утечке или искажению защищаемой информации;

– снижению лимитов на межбанковское кредитование;

– нарушению целостности (искажение) или частичной потере данных;

– оттоку клиентов (1–5% от общего числа);

– увеличению сроков проекта на 1–4 месяца;

– реализации проекта с контролируемыми отклонениями от изначальных целей.

Таблица 10 – Идентификация цифровых рисков кредитной организации согласно бизнес-процессам

В баллах

Перечень оцениваемых рисков, сформированных на этапе качественного анализа	Бизнес-процессы						Итого
	Стратегическое управление	Осуществление бизнес-операций	Управление персоналом и структурой	Технологическое обеспечение деятельности	Развитие кредитной организации в модели экосистемы	Управление бизнес-процессами	
1	2	3	4	5	6	7	8
Цифровые бизнес-риски	-						
Низкое качество / недостаточность маркетинговых исследований рынка (некорректная прогнозная оценка и выбор партнеров)	1	1	0,5	1	1	1	-
Низкое качество / недостаточность маркетинговых исследований рынка (ошибочный выбор объектов инвестирования)	1	1	0,5	1	1	1	

Продолжение таблицы 10

В баллах

1	2	3	4	5	6	7	8
Низкое качество / недостаточность маркетинговых исследований рынка (ошибочная приоритизация продуктов и сервисов)	1	1	0,5	1	1	1	
Низкое качество управления ресурсной базой для развития / недостаточность или неточность данных, используемых в управлении ресурсами для инвестирования	1	1	0,5	1	1	1	-
ИТОГО	4	4	2	4	4	4	22
Цифровые операционные риски	-						
Недостаточная квалификация / подготовка и переподготовка / мотивация сотрудников	1	0	1	1	0,5	0,5	
Высокая вероятность отказа информационных систем, технических сбоев (в том числе и из-за отсутствия обновлений)	1	1	0	1	1	0,5	-
Неэффективный (излишняя простота / усложненность) дизайн архитектуры систем безопасности	0,5	1	0	1	1	0,5	
Высокая вероятность нарушений системы информационной безопасности, в том числе потерь данных	0,5	0,5	1	1	0	1	
ИТОГО	3	2,5	2	4	2,5	2,5	16,5
Риски вынужденной поддержки участников цифрового контура	-						-

Продолжение таблицы 10

В баллах

1	2	3	4	5	6	7	8
Вероятность роста объема финансовых ресурсов, направляемых в экосистему из-за некорректного расчета показателей инвестпроектирования, в том числе срока окупаемости деятельности участников экосистемы	0,5	0	0	0	1	1	-
Вероятность возникновения дополнительных расходов по инвестициям в цифровой контур (в том числе из-за форс-мажорных обстоятельств) вплоть до банкротства участников экосистемы и стратегических партнеров	1	0	0	0	1	1	
ИТОГО	1,5	0	0	0	2	2	5,5
ИТОГО	8,5	6,5	4	8	8,5	8,5	-

Источник: составлено автором.

Цифровые бизнес-риски связаны со всевозможными бизнес-активностями кредитной организации – взаимодействие с партнерами; инвестиционные проекты; развитие технологичных продуктов и сервисов и сопутствующие этому проблемы, связанные со сбоями в работе, непроработанным защитным контуром, либо неуспехом в реализации и последующими финансовыми и репутационными проблемами. Эффективная борьба с данными рисками напрямую влияет на достаточность обеспечения экономической безопасности кредитной организации, а также на поддержание защиты корпоративных интересов и информационную безопасность.

Цифровые операционные риски представляют собой *проблемы, связанные с работой сотрудников* с технологиями (например, ошибки при работе со сложными технологиями, нежелание вникать в рабочие процессы

при новом технологическом укладе), *риски всевозможных сбоев* в работе и приостановок функционирования новых технологических систем, *риски сложной архитектуры данных и ИТ-инфраструктуры, риски информационной безопасности,* которые являются самыми опасными с учетом того, что кредитные организации из-за специфики работы владеют практически полной конфиденциальной информацией о физических и юридических лицах, утечка которой может нанести значимый урон экономической безопасности, а также репутации кредитной организации.

Крупные системообразующие кредитные организации (особенно в России) зачастую имеют развитые экосистемы, в связи с чем возникает риск *вынужденной поддержки участников цифрового контура*, подразумевающий продуктовые и сервисные проблемы участников банковской экосистемы. То есть какой-либо сервис, связанный с кредитной организацией (например, у Сбера есть сервис по продаже товаров – Мегамаркет), не может достичь поставленных финансовых целей, либо требует больше вложений в связи с непроработанностью, либо непривлекательностью своих продуктов (приложения, цифровые решения по ипотеке, электронная коммерция, медиасервисы, B2B-сервисы и так далее).

Обеспечение безопасности участников банковской экосистемы имеет важное значение в контексте обеспечения экономической безопасности кредитной организации [93], так как активы участников экосистемы, а также издержки, формируемые за счет обеспечения кредитной организацией участников, напрямую влияют на экономические интересы кредитной организации и их защищенность.

Цифровые риски оказывают прямое влияние на *бизнес-процессы кредитной организации* – осуществление бизнес-операций, стратегическое управление, управление персоналом и структурой, технологическое обеспечение деятельности, развитие экосистемы, управление объектами деятельности и ресурсами.

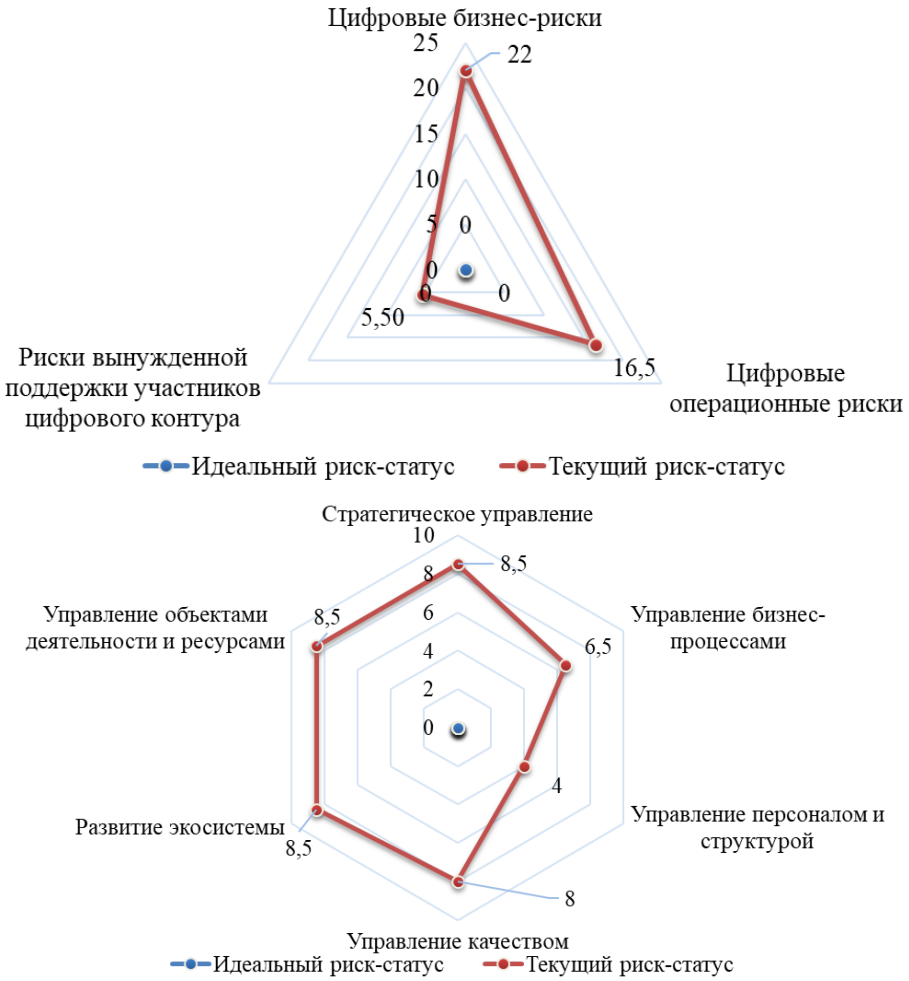
В части *цифровых бизнес-рисков* значимому влиянию подвержены все бизнес-процессы, исключением могут быть лишь процессы по управлению персоналом и структурой, *цифровые операционные риски* напрямую влияют на технологическое обеспечение деятельности и стратегическое управление, а также значительно затрагивают экосистему кредитной организации, *риски вынужденной поддержки участников цифрового контура* наибольшее влияние оказывают на экосистему и управление объектами деятельности и ресурсами.

«Сильное влияние цифрового риска (1,0) на бизнес-процесс предполагает существенное снижение не только операционных результатов кредитной организации, но и годовой прибыли» [141]. Причем чем дольше воздействие риска, тем значительнее будут убытки. Например, с позиции стратегического управления неправильный выбор партнеров (причем как в экосистеме, так и вне ее) может привести к серьезным последствиям для финансовой устойчивости кредитной организации.

Умеренное (0,5) влияние предполагает временное влияние риска на финансовые результаты, вызванное зачастую недостаточной «компенсацией» инвестиционных затрат кредитной организации в выбранные цифровые технологии.

Отсутствие влияния (0) цифрового риска означает, что текущая цифровая трансформация проведена успешно, все внешние факторы учтены и серьезного влияния на устойчивость кредитной организации не оказывает. Каждой ситуации присваивается степень критичности и определяется плановое время устранения. Действия по устранению сбоя зависят от его природы: проблема на стороне партнера, либо причина в нарушении внутренних процессов кредитной организации.

Иллюстративно значимость определенных видов цифрового риска в контексте их влияния на кредитную организацию, а также подверженность бизнес-процессов цифровым рискам отражены на рисунке 21.



Источник: составлено автором и опубликовано [139].
Рисунок 21 – Риск-статус цифровых рисков

Для каждого вида цифрового риска могут быть использованы различные методы оценки. Так, «в отношении цифровых рисков сложной архитектуры информационных технологий, которые характеризуются множеством данных с высоким уровнем неопределенности и отсутствием статистически корректной базы внедрения аналогов по другим кредитным организациям, имеется крайне низкая целесообразность применения сложных аналитических моделей» [141]. Для данного вида риска целесообразно использовать методы аналогий или стандартные сравнительные методы. А определение величины корректировки вложенных средств (изменений пропорций между соответствующими статьями бюджета) целесообразно проводить на основе существующих практик осуществления инвестиционной деятельности в кредитной организации. На рисунке 22 предложена структуризация методов оценки цифровых рисков в зависимости от вида риска.

Источник: составлено автором и опубликовано [141].

Рисунок 22 – Структуризация методов оценки цифровых рисков в зависимости от вида риска

По итогам исследования, проведенного в данном параграфе, можно составить профиль цифрового риска, представленный в таблице 11.

Таблица 11 – Профиль цифрового риска

Составляющая профиля	Описание
1	2
Факторы риска	*Внутренние факторы:* — недостаточность мер кибербезопасности — сбои в работе информационных систем и ошибки программного обеспечения — человеческий фактор — ошибки в управлении данными — недостаточная осведомленность сотрудников о рисках, недостаточная обученность сотрудников *Внешние факторы:* — кибератаки — технологические сбои у поставщиков и партнеров — изменения в нормативно-правовой базе — конкурентное давление и необходимость быстрого внедрения новых технологий — геополитические события и стихийные бедствия
Объект риска	Материальные и нематериальные активы, процессы или системы, подверженные риску потерь или возникновения нарушений при осуществлении деятельности в результате использования цифровых технологий. Объектами цифрового риска могут быть данные, информационные системы и сети, процессы, репутация, финансовые активы, сотрудники
Виды риска	-
а) цифровые бизнес-риски	— низкое качество / недостаточность маркетинговых исследований рынка: некорректная прогнозная оценка и выбор партнеров, ошибочный выбор объектов инвестирования, ошибочная приоритизация продуктов и сервисов — низкое качество управления ресурсной базой для развития / недостаточность или неточность данных, используемых в управлении ресурсами для инвестирования
б) цифровые операционные риски	— недостаточная квалификация / подготовка и переподготовка /мотивация сотрудников — высокая вероятность отказа информационных систем, технических сбоев (в том числе и из-за отсутствия обновлений) — неэффективный (излишняя простота / усложненность) дизайн архитектуры систем безопасности — высокая вероятность нарушений системы информационной безопасности, в том числе потерь данных
в) риски вынужденной поддержки участников цифрового контура	— вероятность роста объема финансовых ресурсов, направляемых в экосистему из-за некорректного расчета показателей инвестпроектирования, в том числе срока окупаемости деятельности участников экосистемы — вероятность возникновения дополнительных расходов по инвестициям в цифровой контур (в том числе из-за форс-мажорных обстоятельств) вплоть до банкротства участников экосистемы и стратегических партнеров
Оценка риска	-
а) параметры модели оценки риска	— уровень доступности данных — степень защищенности информации от несанкционированного доступа — уровень шифрования — эффективность систем управления доступом к данным — способность к обнаружению и реагированию на инциденты — частота обновлений программного обеспечения — наличие функциональных возможностей к анализу угроз

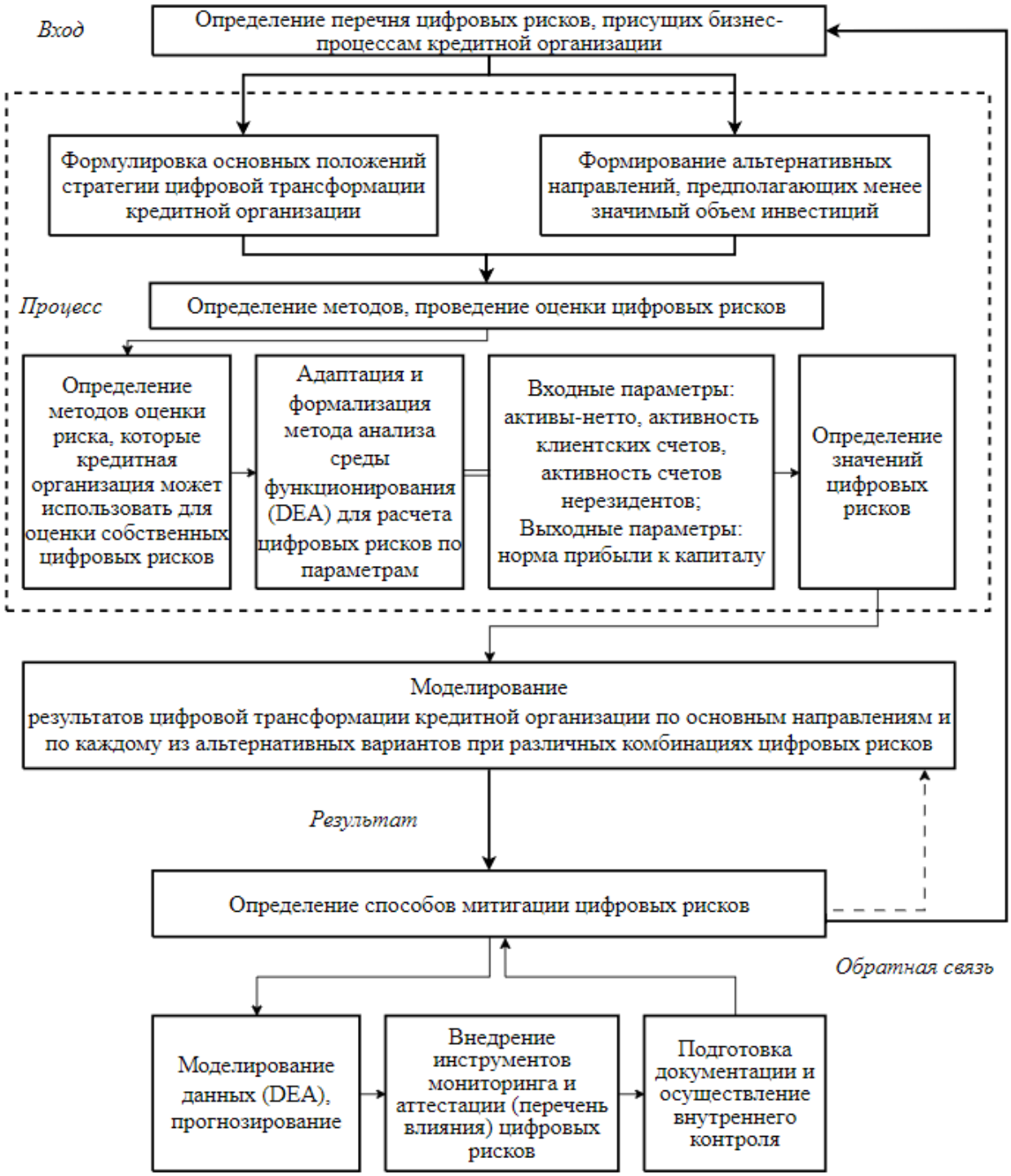
Продолжение таблицы 11

1	2
б) функциональная зависимость объекта риска от факторов риска	Взаимосвязь между объектом риска и факторами, которые могут повлиять на его уязвимость. Уравнение функциональной зависимости может иметь следующий вид: *уязвимость объекта риска = f (Фактор риска 1, фактор риска 2, ..., фактор риска n).* Под уязвимостью объекта риска можно понимать вероятность и уровень потенциального воздействия риска на объект, а под факторами риска – внутренние и внешние факторы, которые могут увеличить или уменьшить уязвимость объекта риска
в) построение прогноза факторов риска	— анализ исторических данных — моделирование рисков на основе алгоритмов машинного обучения — выявление и оценка уязвимостей для прогнозирования потенциальных объектов атаки — экспертная оценка (специалисты в области управления рисками и кибербезопасности) — анализ сценариев — мониторинг тенденций
Сопряженные бизнес-процессы	— стратегическое управление — осуществление бизнес-операций — управление персоналом и структурой — технологическое обеспечение деятельности — развитие организации в модели экосистемы — управление бизнес-процессами

Источник: составлено автором.

Оценка цифровых рисков подразумевает применение различных методов и подходов для обеспечения точности и надежности полученных результатов. Сочетание этих методов с учетом контекста возникновения риска, текущего уровня его влияния на организацию и доступных инструментов управления рисками позволяет провести максимально полную оценку рисков. Например, можно комбинировать аналитический подход в части выявления ключевых риск-индикаторов и логико-вероятностный подход в части сопоставления выявленных индикаторов в разрезе временных рамок, либо в сравнении аналогичных данных с индикаторами других бизнес-процессов / подразделений / проектов, или, к примеру, статистический анализ на основе исторических данных в совокупности с аналитическим сценарным анализом позволяют высокоточно спрогнозировать появление различных видов рисков.

Рассмотренные методы оценки цифровых рисков могут быть реализованы в форме алгоритма, представленного на рисунке 23.



Источник: составлено автором и опубликовано [139].
Рисунок 23 – Алгоритм оценки цифровых рисков кредитной организации

Последствия реализации цифровых рисков могут заключаться как в прямых финансовых потерях, так и иметь «пролонгированный» негативный эффект. Например, разовый сбой системы информационной безопасности, не рассматриваемый в дальнейшем как полноценная значимая ошибка функционирования операционной деятельности, а отнесенный, например, на «типичные» ошибочные действия сотрудников, может оказаться полноценной

брешью системы, и привести впоследствии к утечке данных. Принятие неизбежности возникновения цифровых рисков приводит к последующему полноценному изменению стратегии организации (не только в части изменения подходов к обеспечению экономической безопасности и управления рисками), слишком велико их влияние. Приведенный выше алгоритм отражает необходимость адаптации и формализации метода анализа среды функционирования применительно к оценке цифровых рисков, а также выбора направлений митигации цифровых рисков (подробно рассмотрено в третьей главе исследования). Стоит отметить, что для создания «синергии» между различными методами оценки (именно в случае кредитной организации) необходимо учитывать размер кредитной организации. Для бюджета системно значимой кредитной организации инвестиции в цифровые технологии менее ощутимы, чем для бюджета небольшой кредитной организации. Однако неизменным остается факт, что кредитным организациям жизненно важно внедрять новые технологии. К интересному выводу пришли исследователи Калифорнийского университета, США – они отмечают, что уровень цифрового разрыва между финансовыми организациями в будущем будет формироваться не столько из-за наличия доступа кредитных организаций к новым технологиям, сколько из-за возможности обеспечивать безопасность банковских систем, конфиденциальность данных и их автономию с помощью использования таких технологий [195].

Итак, «современные цифровые риски банковского сектора характеризуются как сложные, многофакторные и очень динамичные явления, проявляющиеся практически во всех аспектах деятельности» [141] и протекания бизнес-процессов кредитных организаций, необходимо искать новые пути к управлению данными рисками, основанные на их оценке и анализе с помощью математико-статистических методов, обеспечивающих высокую точность искомых результатов.

Таким образом, в рамках исследования методологических аспектов оценки рисков кредитной организации в условиях цифровизации с учетом специфики изученных подходов к трансформации бизнес-моделей данных организаций в условиях цифровизации:

– выявлена тенденция изменчивости процессов управления рисками при обеспечении экономической безопасности в кредитной организации под влиянием цифровой трансформации банковского сектора;

– определено несовершенство системного подхода современных кредитных организаций к управлению рисками, связанными с цифровизацией, что проявляется в неэффективности использования кредитными организациями современного технологического инструментария (как в процессах по обеспечению безопасности, так и в рамках осуществления бизнес-процессов), недостаточности проработки внутренних процедур контроля и их гибкости относительно изменяющейся цифровой среды, отсутствии прописанных подходов к управлению цифровыми рисками со стороны Банка России;

– определены возможности адаптации традиционных методов управления рисками кредитных организаций к управлению рисками, связанными с цифровизацией;

– предложены определения «цифрового риска» и «митигации цифрового риска»;

– установлены внешние и внутренние причины возникновения цифровых рисков;

– сформулированы и описаны виды цифровых рисков (*цифровые бизнес-риски, цифровые операционные риски, риски вынужденной поддержки участников цифрового контура*);

– идентифицированы бизнес-процессы кредитной организации (*стратегическое управление, осуществление бизнес-операций, управление персоналом и структурой, технологическое обеспечение деятельности,*

развитие кредитной организации в модели экосистемы, управление бизнес-процессами) и обозначено влияние на них цифровых рисков;

– проведена структуризация методов оценки цифровых рисков (*логико-вероятностные, аналитические и статистические методы*) в зависимости от их видов, а также предложен алгоритм оценки цифровых рисков, подразумевающий использование методических рекомендаций по митигации цифровых рисков, которые будет рассмотрены в третьей главе исследования.

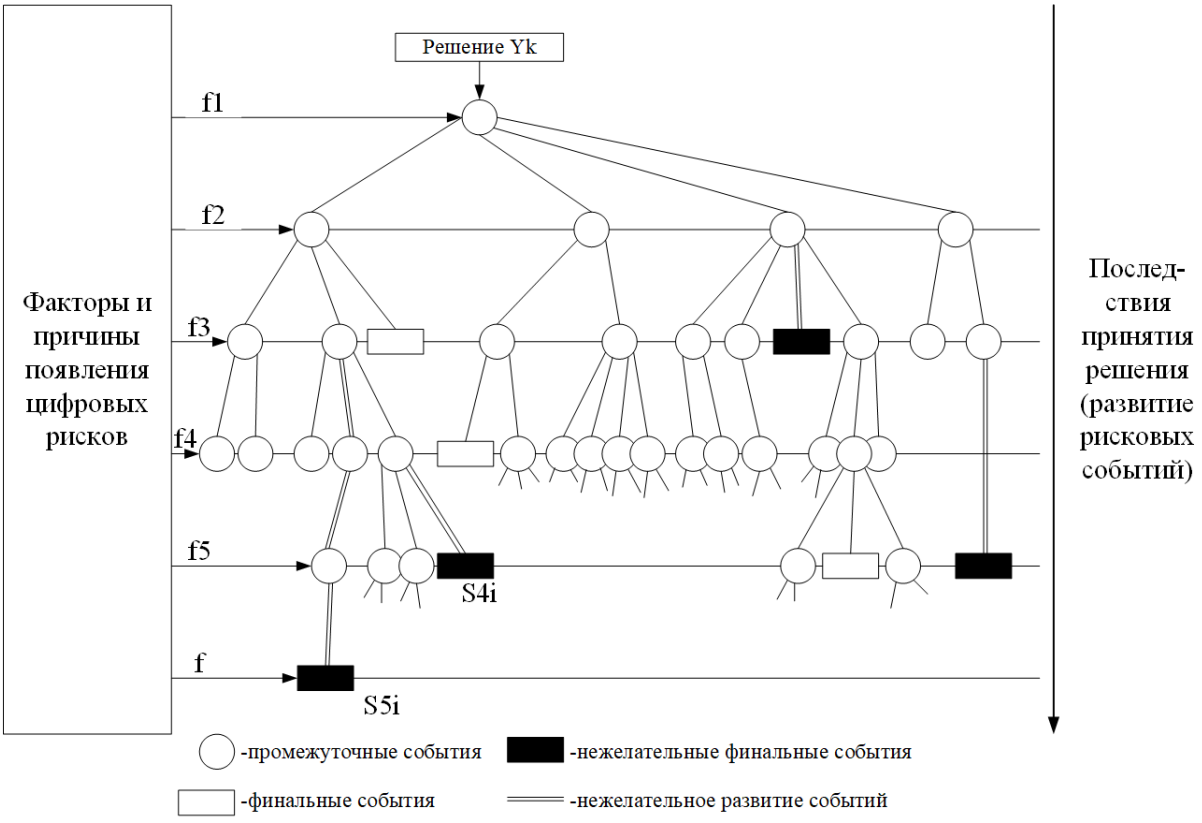
Глава 3
Направления митигации цифровых рисков и повышения уровня экономической безопасности организации

3.1 Формализация методических рекомендаций по митигации цифровых рисков

По итогам исследования, проведенного в первой и второй главах работы, установлено, что риски, связанные с цифровизацией, являются неотъемлемой частью деятельности современной кредитной организации, и существующие методы оценки традиционных банковских рисков могут быть использованы и для цифровых рисков при условии проведения соответствующих адаптивных мероприятий данных методов к условиям функционирования кредитных организаций в цифровой среде. При формализации методических рекомендаций по митигации цифровых рисков необходимо учесть общетеоретические основы моделирования рисков. Под «моделью риска» можно понимать математический метод, систему методов или прогнозную модель, которая отражает элементы риска осуществления бизнес-процессов в кредитной организации. Модель риска позволяет получить функциональные данные, а также сформировать количественные оценки (расчет вероятностей разного вида, определение математического ожидания), которые поспособствуют кредитным организациям в принятии финансовых, стратегических и операционных решений. В качестве основного метода оценки цифровых рисков организации предлагается использовать метод анализа среды функционирования (далее — DEA [Data envelopment analysis]), который позволяет учитывать двойственность природы цифровых рисков (когда одно событие может инициировать возникновение нескольких видов цифровых рисков или возникновение сочетания цифровых и традиционных рисков) и подразумевает использование любого количества входных

(издержки) и выходных (результаты) переменных, связанных с бизнес-процессами организации (использование метода DEA рассмотрено в соавторстве с Е.А. Вечкинзовой [132; 137]). «Метод DEA – непараметрический метод измерения эффективности или качества набора равнозначных объектов. К основным преимуществам данного метода относится его способность нивелировать проблему гетероскедастичности, возникающую при параметрическом моделировании. Он позволяет рассматривать показатели, представленные различными шкалами и единицами измерения. Метод анализа среды функционирования разработан в исследованиях А. Чарнса, В. Купера [182], Е. Роудса [181], М. Фаррелла [192] и достаточно обширно представлен в западной практике научно-теоретических и практических исследований. Суть метода состоит в отыскании в конкретной совокупности наиболее эффективных объектов по параметрам наибольшей отдачи (выходы) на вложенный ресурс (входы), а также в определении модельных (эталонных) объектов и параметров для неэффективных» [132; 137]. «Если с увеличением количества ресурса отдача его в эталонных объектах не снижается, а пропорционально увеличивается, то эталонные объекты будут находиться на прямой линии – границе производственных возможностей с постоянным эффектом масштаба – модель Constant Returns to Scale (далее – CRS). Если с ростом количества ресурса его отдача меняется, то граница производственных возможностей эталонных объектов будет представлена кривой, описывающей переменный эффект масштаба – модель Variable Returns to Scale (далее – VRS). Эффективность объектов, лежащих на границе производственных возможностей, равна единице. Метод позволяет построить модель не только постоянного или переменного эффекта масштаба, но и ориентировать ее на входы (ресурсы) или выходы (результаты) деятельности рассматриваемых объектов. В моделях, ориентированных на вход, основная цель заключается в минимизации входных параметров, при этом выходные параметры остаются на первоначальном уровне, или увеличиваются. Обратные зависимости характерны для моделей, ориентированных на выход» [132; 137].

Предположим, что исходная информация, необходимая для математической постановки задачи оценки цифровых рисков, может быть представлена в виде причинно-следственной сети, отражающей результат макропруденциального регулирования рисков кредитных организаций и факторов, выявленных в ходе анализа уровня рисков и экономической безопасности кредитных организаций банковского сектора России. В случае разработки методов минимизации цифровых рисков узлы этой сети отражают события или факторы (триггеры) риска (начальные узлы сети) и последствия их проявления, а дуги – возможные пути развития событий, отраженные на рисунке 24. Неопределенность и неоднозначность развития внешней «цифровой» среды находят свое отражение в причинно-следственной связи – каждый узел причинно-следственной связи подразумевает реализацию не одного, а нескольких событий.



Источник: составлено автором по материалам [57].

Рисунок 24 – Схема причинно-следственной связи для оценки цифровых рисков

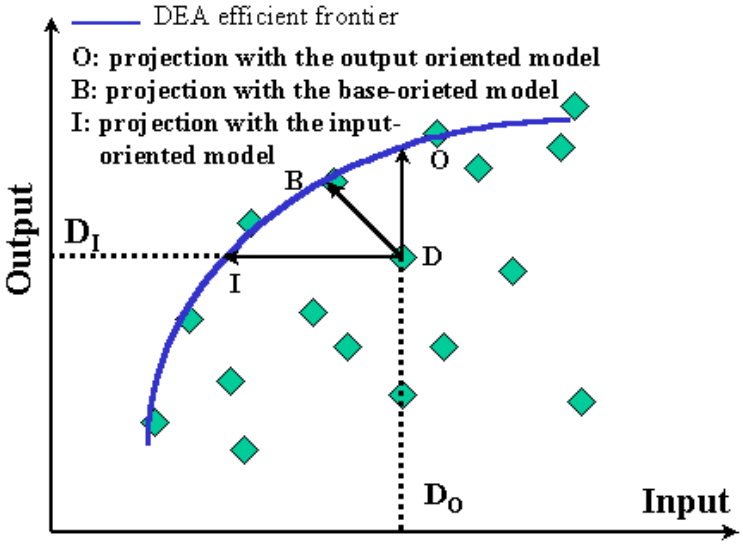
Ранее выделенная в работе классификация цифровых рисков организации (с учетом особенности проанализированных методов оценки

рисков) позволяет систематизировать входные и выходные финансовые показатели, определяющие уровень банковских рисков и эффективность кредитных организаций, реализующих цифровую трансформацию бизнес-процессов. Применение метода DEA обеспечивает всестороннее понимание эффективности (с точки зрения количественных показателей) и помогает определить области митигации рисков, что было доказано, например, в статье Д. Трайпа [201] (аналогичных исследований российскими учеными не проводилось). В классическом варианте метода DEA «входными данными являются объемы затраченных ресурсов, выходными данными – объемы выпускаемой или реализованной продукции, поэтому связь между выходными и входными данными всегда прямо пропорциональна» [141]. Применение данного метода в области митигации цифровых рисков позволяет определить пути к снижению *модельных рисков*. Под модельными рисками организации, в том числе, понимаются потенциальные убытки, которые организация может понести в результате решений, основанных на результатах использования внутренних моделей, а также возникших в результате ошибок при разработке, внедрении или использовании моделей (любых, не обязательно связанных с цифровыми рисками). Из этого определения следует, что основными типами модельных рисков являются риск спецификации (разработка), риск реализации (внедрение) и риск применения (использование) модели. Управление модельными рисками (далее – MRM [Model Risk Management]) направлено на осуществление контроля рисков, на которые указывают возможные неблагоприятные последствия выбора, сделанного с использованием ошибочных или неподходящих в конкретных случаях моделей.

В рамках исследования экономический объект выражается «не объемами затраченных ресурсов и выпускаемой продукции, а финансовыми показателями, в том числе специфическими (например, анализ активности по счетам, соотношение наличных к активам-нетто – описание дано ниже). В качестве исследуемых объектов рассматриваются крупнейшие российские

кредитные организации. Метод DEA подразумевает измерение входов и выходов с использованием различных шкал, что позволяет оценивать ключевой конечный показатель с учетом разного набора входных переменных, а также ранжировать объекты по уровням цифровых рисков» [141]. «Результаты расчетов позволят выявить кредитные организации с высоким уровнем цифровых рисков и определить направления рекомендаций по минимизации этих рисков» [141].

На рисунке 25 изображено наглядное представление модели – на плоскости, отражающей вход и выход, изображен исследуемый объект D, который находится внутри границы эффективности. В зависимости от типа ориентации модели объекту будут соответствовать различные эффективные виртуальные образы – объекты, которыми мог бы стать исследуемый объект D при сокращении входных параметров, смещаясь в точку I (input), либо при увеличении выходных параметров, смещаясь в точку O (output). Точка B (base) при этом является эффективным образом базовой модели, то есть корректировке может быть подвержен как входной, так и выходной параметр.



Источник: составлено автором по материалам [179].
Рисунок 25 – Ориентация метода анализа среды функционирования

Ситуация, при которой исследуется один входной и один выходной параметр, реализуется в двумерном пространстве. Чем большее количество параметров будет взято за основу расчета модели, тем большей будет

размерность пространства, то есть метод анализа среды функционирования благодаря алгоритмам линейного программирования позволяет построить границу эффективности рассматриваемых объектов в многомерном пространстве, с помощью чего можно проводить сравнительный анализ разных объектов во множестве разрезов.

В качестве входных и выходных параметров предлагается использовать финансовые показатели кредитной организации, представленные в таблице 12.

Таблица 12 – Входные и выходные показатели метода оценки цифровых рисков кредитной организации

Наименование группы	Наименование показателя	Экономическое содержание показателя
Входные показатели	Активы-нетто	Активы-нетто (чистые активы) – стоимость капитала по рыночной цене минус долговые обязательства. Другими словами, чистые активы представляют собой оценочную сумму имущества, которая могла бы остаться в распоряжении организации после погашения обязательств
	Кредитный портфель	Совокупность активов, переданных в кредит физическим или юридическим лицам или остаток задолженности на определенную дату по всем выданным кредитной организацией кредитам
	Привлеченные средства физических лиц	Средства, внесенные в кредитную организацию клиентами – физическими лицами, то есть населением, на определенные счета или путем продажи собственных долговых обязательств
	Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	Резкая активизация при проведении клиентских расчетов можем являться признаком смены бизнес-модели развития кредитной организации, прихода новых акционеров, новых активно работающих клиентов (активизация по проведению в том числе так называемых «сомнительных» операций)
	Доля наличности в составе активов-нетто, в процентах	Резкое повышение часто означает возможный «выход в кэш», когда все активы кредитной организации аккумулируются в виде наличности с последующей возможностью выноса ее «в чемодане». Доля наличности в составе активов у «нормально работающей» кредитной организации редко превышает 5-6% (среднее по отрасли)
	Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	Внутримесячные обороты по текущим клиентским счетам компаний и физлиц-нерезидентов (с учетом их размера активов). Наличие высокой платежной активности клиентов при отсутствии понимания, что именно они делают, является возможным признаком участия банка в проведении сомнительных операций
	Активность лоро-счетов, относительные единицы (соотношение оборотов и активов-нетто)	Высокие внутримесячные обороты по лоро-счетам являются признаком участия кредитной организации в проведении сомнительных операций
Выходные показатели	Собственный капитал	Общая стоимость средств кредитной организации, принадлежащих ей на правах собственности и применяемых ей для создания определенной части ее активов
	Прибыль (норма прибыли к капиталу, в процентах)	При прочих равных критериях – чем больше кредитная организация заработала средств в текущем отчетном периоде, тем более успешен ее бизнес на текущий момент

Источник: составлено автором и опубликовано [141].

Представленные в таблице 12 показатели способствуют определению уровня рисков и эффективности процессов по обеспечению экономической безопасности кредитной организации, поскольку кредитные организации, которые обеспечивают большую доходность при заданном объеме издержек / инвестиций, характеризуются как эффективные и безопасные. Предлагается разделять «рыночное окружение» определенной кредитной организации на два типа: системно значимые кредитные организации и прямые конкуренты. В России (на дату проведения исследования) действует 13 системно значимых кредитных организаций [36]. На их долю приходится около 78% совокупных активов российского банковского сектора, они являются своего рода монополистами. Системно значимая кредитная организация обладает превосходящим (по сравнению с оставшейся большей долей кредитных организаций, а системно значимых кредитных организаций всего 4% от всех кредитных организаций в России) уровнем внедрения и развития цифровых технологий, а также творческим позиционированием своих услуг и цифровых банковских продуктов.

Для проведения анализа, направленного на оценку модельных рисков, целесообразно сравнивать между собой кредитные организации, относящиеся к системно значимым, а показатели должны быть сформированы с учетом выявленного соотношения конкурентных сил в банковском секторе России. Для проведения расчетов используются показатели, представленные в таблице выше, поскольку практически все операции современных кредитных организаций связаны с цифровой средой. Это обусловлено тем, что, во-первых, большинство денежных операций осуществляются в безналичной форме (по данным Банка России объем безналичного оборота составил в 2023 году 81% [35]). Такие операции осуществляются либо с применением карт и приложений, либо по каналам цифровой связи – поскольку тенденция отказа от наличных будет сохраняться, безналичный денежный оборот будет расти. Частично активы кредитной организации не имеют овеществленную форму – они являются цифровыми, подверженными цифровым рискам.

Во-вторых, даже если кредитная организация не является крупной (предположим, у нее нет мобильного приложения, нет внедренных цифровых технологий, нет сайта), ее операции и денежные средства все равно будут проходить через каналы цифровой связи, поскольку кредитная организация определенно будет взаимодействовать с юридическими лицами.

Логика разработанной модели заключается в том, что, меняя исходные значения входных параметров банковских операций (активов-нетто, на которые в том числе влияет объем инвестиций кредитной организации в цифровые технологии и обеспечение безопасности, доля наличности, которая уменьшается, если кредитная организация наращивает онлайн-платежи своих клиентов) можно рассчитать изменение нормы прибыли на капитал**.** Такое изменение может быть положительным (приведет к росту нормы прибыли на капитал) и отрицательным (приведет к снижению доходов кредитной организации), что в свою очередь согласуется с портфельной теорией Марковица – «риск, доходность, ликвидность – при росте риска растет доходность» [84]. Результатом такого исследования должно быть «выявление компонентов совокупного цифрового риска кредитной организации (или той входной переменной, которая сильнее всего на возникновение риска) и определение по каждой компоненте соответствующих характеристик» [141]. *Выбор объектов* должен основываться на оценке трансформации бизнес-моделей российских кредитных организаций, а также на их ранжировании по степени развития экосистем. Для определения уровня развития кредитной организации в контексте функционирования в экосистеме можно использовать шкалу, предложенную М.А. Мамедовым в его исследовании деятельности кредитных организаций в условиях формирования экосистем, как показано в таблице 13:

а) 1 – сервис полностью и хорошо развит;

б) 0,5 – сервис развит не полностью;

в) 0 – сервис отсутствует.

Таблица 13 – Ранжирование кредитных организаций по уровню развитии сервисов в бизнес-моделях цифровых экосистем

В баллах

Наименование кредитной организации	Сервисы цифровой экосистемы				Индекс (итого баллов)	Присвоенный ранг
	Финансы	Развлечения	ИТ услуги	Life-style услуги		
ПАО «Сбербанк»	1	1	1	1	4	1
АО «Тинькофф Банк»	1	1	1	1	4	1
«Банк ВТБ» (ПАО)	1	0,5	1	1	3,5	1
АО «Банк ГПБ»	1	0	0,5	0,5	2	2
АО «Альфа-Банк»	1	0	0,5	0,5	2	2
АО «ЮниКредит Банк»	1	0	0	0,5	1,5	3
ПАО «Совкомбанк»	1	0	0	0,5	1,5	3
ПАО «Московский Кредитный Банк»	1	0	0	0,5	1,5	3
ПАО Банк «ФК Открытие»	1	0	0	0,5	1,5	3
ПАО «РОСБАНК»	1	0	0	0,5	1,5	3

Источник: составлено автором по материалам [25].

Итоговые данные ранжирования кредитных организаций по развитию сервисов в бизнес-моделях цифровых экосистем, приведенные в таблице 13, подтверждают ранее сформулированную гипотезу о «неравномерности цифрового развития системно значимых кредитных организаций и других кредитных организаций» [119] банковского сектора России. В то время как системно значимые кредитные организации развивают все элементы экосистемы (включая, например, развлекательные сервисы, такие как подписки на кино или рестораны), большинство российских кредитных организаций предпочитают инвестировать только в цифровые проекты. Во-первых, это проекты с относительно быстрым сроком окупаемости, такие как развитие финансовых сервисов, например, подача онлайн-заявок на кредит. Во-вторых, эти проекты тесно связаны с их основной деятельностью. Специфика данной ситуации определяется и нехваткой ресурсов, и недостаточностью понимания достоинств универсальной экосистемы (грамотно выстроенная экосистема в перспективе обеспечит кредитную организацию большей доходностью, чем сервисы и услуги, предоставляемые в отрыве, без концепции общего позиционирования). Согласно результатам,

отраженным в таблице 13, «к полностью универсальным экосистемам следует отнести экосистемы ПАО «Сбербанк», «Банк ВТБ» (ПАО)», АО «Тинькофф Банк» [119]. М.А. Мамедов отмечает, что кредитные организации с рангом 2 «расширяют свои продуктовые предложения и сферу деятельности соответственно только в определенных секторах экономики, соответственно консервативны в рисковой политике. Кредитные организации с рангом 3 не трансформируют свою бизнес-модель в экосистему, однако это не означает, что эти кредитные организации не работают над цифровизацией продуктов и услуг и развитием цифровой инфраструктуры в целом» [119].

Характеристика экосистем исследуемых кредитных организаций приведена М.А. Мамедовым в работе по изучению трансформации деятельности крупнейших российских кредитных организаций в цифровые экосистемы. Исследователь отмечает, что «экосистема ПАО «Сбербанк» формируется в виде *гибридной модели* (компания активно работает над объединением структурных подразделений в единую цифровую систему в рамках единого бесшовного интегрированного процесса)» [119]; «стратегией «Банк ВТБ» (ПАО) является *создание экосистемы путем партнерских платформ*, в которые, помимо банковских услуг, входят сервисы мобильного оператора, цифровой бухгалтерии, жилищный маркетплейс для аренды и покупки жилья, проект велопроката и другие проекты в том числе с зарубежными партнерами и правительством Москвы (модель «Банк ВТБ» (ПАО) также относится к *гибридным, но строится постепенно*)» [119]; «АО «Тинькофф Банк» позиционирует себя не только как банковская организация, но и как *финансовая компания, внедряющая инновации в свои процессы*, то есть финтех-компания, которая развивала в первую очередь мобильное приложение (в данном случае *экосистема строится по принципам открытой модели*, где головной компанией является сама кредитная организация)» [119].

М.А. Мамедов также замечает, что «крупнейшие кредитные организации будут создавать цифровые банковские экосистемы, что требует

значительных финансовых вложений*, а значит и роста активов*, в сложившихся условиях российские кредитные организации, формирующие цифровые экосистемы, будут конкурировать как с другими кредитными организациями, так и российскими цифровыми экосистемами, формирующихся на базе технологических компаний» [119], следовательно, кредитные организации уже сейчас подвержены цифровым рискам, и в дальнейшем масштаб их влияния будет только увеличиваться.

В рамках проведенного исследования были проанализированы показатели входных и выходных переменных кредитных организаций за период январь 2017 г. – январь 2022 г. Динамика данных показателей для ПАО «Сбербанк», «Банк ВТБ» (ПАО) и АО «Тинькофф Банк» представлена в приложении Г, в сводном виде в таблице 14.

Таблица 14 – Результаты анализа входных и выходных переменных ПАО «Сбербанк», «Банк ВТБ» (ПАО) и АО «Тинькофф Банк»

Наименование показателя	ПАО «Сбербанк»	«Банк ВТБ» (ПАО)	АО «Тинькофф Банк»
1	2	3	4
Активы-нетто, млрд руб.	-	-	-
изменение с 01.01.2017 по 01.01.2022	15 876	9 939	1 096
среднемесячное значение	29 082	14 246	560
среднемесячное отклонение	4 031	2 506	258
Собственный капитал, млрд руб.	-	-	-
изменение с 01.01.2017 по 01.01.2022	1 739	645	175
среднемесячное значение	4 326	1 537	97
среднемесячное отклонение	424	191	32
Кредитный портфель, млрд руб.	-	-	-
изменение с 01.01.2017 по 01.01.2022	12 146	6 408	566
среднемесячное значение	20 049	9 310	330
среднемесячное отклонение	2 873	1 884	142
Привлеченные средства физлиц, млрд руб.	-	-	-
изменение с 01.01.2017 по 01.01.2022	3 829	4 508	563
среднемесячное значение	12 470	3 349	293
среднемесячное отклонение	1 438	1 289	139
Активность клиентских счетов, относительные единицы	-	-	-
изменение с 01.01.2017 по 01.01.2022	0,01	-0,06	7,22
среднемесячное значение	1,42	1,53	4,83
среднемесячное отклонение	0,17	0,19	3,05
Доля наличности в составе активов-нетто, в процентах	-	-	-

Продолжение таблицы 14

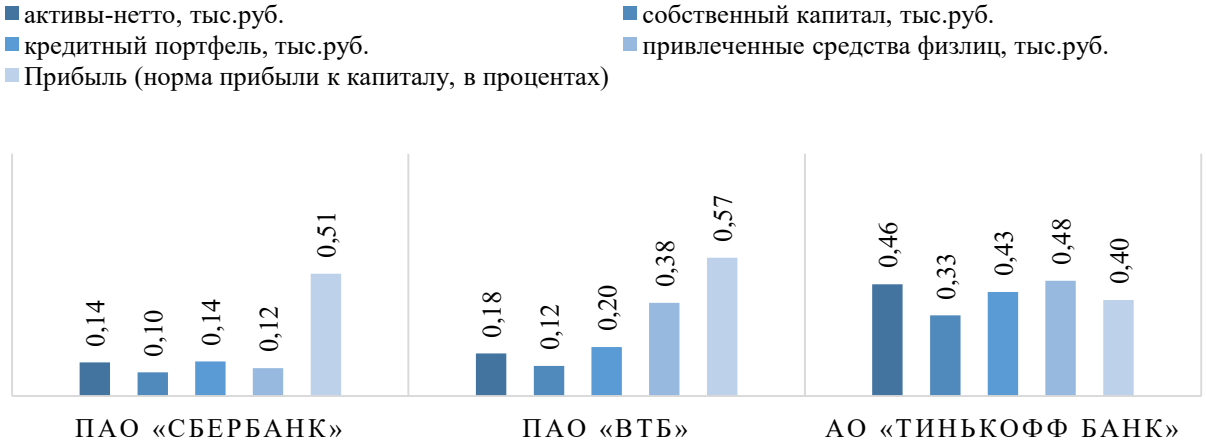
1	2	3	4
изменение с 01.01.2017 по 01.01.2022	-	-	2,00
среднемесячное значение	2,00	2,00	1,02
среднемесячное отклонение	-	-	0,47
Активность счетов нерезидентов, относительные единицы	-	-	-
изменение с 01.01.2017 по 01.01.2022	-0,02	-0,09	-0,06
среднемесячное значение	0,04	0,02	0,02
среднемесячное отклонение	0,02	0,01	0,01
Активность лоро-счетов, относительные единицы	-	-	-
изменение с 01.01.2017 по 01.01.2022	-0,03	-0,38	-
среднемесячное значение	0,47	0,33	-
среднемесячное отклонение	0,05	0,07	-
Прибыль (норма прибыли на капитал), в процентах	-	-	-
изменение с 01.01.2017 по 01.01.2022	-14,00	-7,00	-32,00
среднемесячное значение	10,64	5,95	17,28
среднемесячное отклонение	5,37	3,40	6,84

Источник: составлено автором и опубликовано [141].

По данным таблицы 14 установлено, что «наибольшим приростом активов-нетто, собственного капитала и кредитного портфеля характеризуется ПАО «Сбербанк», наибольшим приростом привлеченных средств физических лиц – «Банк ВТБ» (ПАО)» [141]. «Сильные изменения активности клиентских счетов, нормы прибыли к капиталу фиксируются за исследуемый период у АО «Тинькофф Банк». Оценка волатильности этих показателей, рассчитанная как отношение среднемесячного отклонения к среднемесячному значению, показала, что наибольшая волатильность нормы прибыли на капитал наблюдается у ПАО «Сбербанк» (0,51) и «Банк ВТБ» (ПАО) (0,57)» [141], что отражено на рисунке 26.

По данным таблицы 14 установлено, что «наибольшим приростом активов-нетто, собственного капитала и кредитного портфеля характеризуется ПАО «Сбербанк», наибольшим приростом привлеченных средств физических лиц – «Банк ВТБ» (ПАО)» [141]. «Сильные изменения активности клиентских счетов, нормы прибыли к капиталу фиксируются за исследуемый период у АО «Тинькофф Банк». Оценка волатильности этих показателей, рассчитанная как отношение среднемесячного отклонения к среднемесячному значению,

показала, что наибольшая волатильность нормы прибыли на капитал наблюдается у ПАО «Сбербанк» (0,51) и «Банк ВТБ» (ПАО) (0,57)» [141], что отражено на рисунке 26.



Источник: составлено автором и опубликовано [141].
Рисунок 26 – Волатильность входных и выходных переменных ПАО «Сбербанк», «Банк ВТБ» (ПАО) и АО «Тинькофф Банк»

«Установленные значения волатильности входных и выходных переменных ПАО «Сбербанк», «Банк ВТБ» (ПАО) и АО «Тинькофф Банк» являются, во-первых, признаками влияния внешней среды и конкуренции в отрасли, во-вторых, определяются влиянием цифровых рисков, поскольку у АО «Тинькофф Банк» (0,40) все бизнес-операции осуществляются в онлайн-формате. Следовательно, наращивание таких бизнес-операций оказало влияние на норму прибыли к капиталу. Таким образом, согласно данным, отраженным на рисунке 26, установлено, что, изменяя объемы операций с клиентами, АО «Тинькофф Банк» (цифровая кредитная организация) смог добиться максимального отношения прибыли к капиталу. На 01.01.2022 показать равен 26%, у ПАО «Сбербанк» – 24%, у «Банк ВТБ» (ПАО) – 13%, при этом наращивая объемы операций без существенного увеличения имущества (активов-нетто)» [141].

Оценка рисков. «Для оценки цифровых рисков исходный метод DEA был модифицирована в соответствии с полученными данными анализа кредитных организаций. Поскольку в реальности ресурсы кредитных организаций ограничены, а входные и выходные переменные не могут изменяться

иррационально, то за основу расчетов взята базовая (радиальная и направленная) модель DEA (как подвид). Эта модель была предложена Seiford и Zhu [199], она применяется для анализа нежелательных входов / выходов и ненаправленной ориентации (то есть ориентированной на вход или выход) при постоянной отдаче от масштаба. Модель позволяет проводить относительные сравнения между бизнес-объектами с небольшим количеством выборок, то есть используется подход, отличный от анализа производственной функции. В качестве *входных переменных* выбраны: активы-нетто, активность клиентских счетов, активность счетов нерезидентов» [141].

«*Выходная переменная* определена как норма прибыли к капиталу (в качестве совокупного показателя влияния цифровых рисков на бизнес кредитной организации). В результате ввода показателей в программное обеспечение по предоставлению расчетов на основе метода анализа среды функционирования получены решения, именуемые Decision Making Unit (далее – DMU) или модуль принятия решения. DMU отражает преобразование определенных ресурсов в продукцию (входы в выходы)» [141]. Расчетная база отражена ранее в таблице 14, результаты расчетов представлены в таблице 15 – «установлена положительная корреляция по всем показателям входным параметров» [141].

Таблица 15 – Данные расчетов показателей по ПАО «Сбербанк»

Наименование показателя	Minimum	Maximum	Mean	Standard Derivation	Корреляция с выходным параметром
Активы-нетто, тыс. руб.	23 135	39 012	29 392	5 046,4678	0,3389
Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	1,31	2,11	1,6009	0,2541	0,7659
Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	0	0,08	0,0509	0,0231	0,5432
Прибыль (норма прибыли к капиталу, в процентах)	7	24	14,8182	4,8583	1

Источник: составлено автором по материалам [54].

В таблице 16 представлены размеры Slacks или дополнительного «усовершенствования» (увеличения выпуска продукции и / или уменьшения затрат), необходимого для того, чтобы бизнес-единица стала эффективной.

Таблица 16 – Данные расчетов Slacks по ПАО «Сбербанк»

Slacks	Активы-нетто, тыс. руб.	Активность клиентских счетов, относительные единицы	Активность счетов нерезидентов, относительные единицы
DMU1	0	0	0,011
DMU2	0	0	0
DMU3	0	0	0
DMU4	911,705	0	0,009
DMU5	0	0	0
DMU6	1565,927	0	0,008
DMU7	0	0,219	0
DMU8	1695,777	0	0,009
DMU9	0	0,013	0
DMU10	2333,254	0	0,016
DMU11	0	0	0,029

Источник: составлено автором по материалам [54].

Результаты, отраженные в таблице 16, позволяют сделать вывод, что наиболее эффективное управленческое решение может быть достигнуто на DMU 2, DMU 3, DMU 5 (дополнительные улучшения по ним равны нулю по всей строке).

По данным таблицы 17 возможно установить цели минимизации рисков (строка *targets*), следуя которым ПАО «Сбербанк» сможет повысить норму прибыли на капитал, минимизировав при этом цифровые риски.

Таблица 17 – Данные расчетов DMU2, DMU3, DMU5 по ПАО «Сбербанк»

Наименование решения / показателя	Активы-нетто, тыс. руб.	Активность клиентских счетов, относительные единицы	Активность счетов нерезидентов, относительные единицы	Норма прибыли к капиталу, в процентах
DMU2	-	-	-	-
Slacks	0	0	0,01	0
Weights	0	0,32	0	0,06
Values	23 135	1,47	0,08	16
Targets	22 087,62	1,4	0,07	16
DMU3	-	-	-	-
Slacks	0	0	0,011	0
Weights	0	0,325	0	0,06
Values	23 135	1,47	0,08	16
Targets	22 087,621	1,403	0,065	16
DMU5	-	-	-	-
Slacks	0	0	0,01098	0
Weights	0,00002	0,32473	0	0,05967
Values	23135	1,47	0,08	16
Targets	22 087,62147	1,40345	0,0654	16

Источник: составлено автором по материалам [54].

Аналогичные расчеты, выполненные для «Банк ВТБ» (ПАО) и АО «Тинькофф Банк», представлены следующим образом: результаты для ПАО «Банк ВТБ» отображены в таблицах 18; 19; и 20, а для АО «Тинькофф Банк» – в таблицах 21; 22 и 23.

Таблица 18 – Данные расчетов показателей по «Банк ВТБ» (ПАО)

Наименование показателя	Minimum	Maximum	Mean	Standard Derivation	Корреляция с выходным параметром
Активы-нетто, тыс. руб.	9 433	19 412	14 210	3 302,0694	0,1671
Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	1,32	2,36	1,6973	0,3017	0,2883
Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	0	0,1	0,0273	0,0245	-0,0087
Прибыль (норма прибыли к капиталу, в процентах)	3	16	8	4,264	1

Источник: составлено автором по материалам [28].

По данным таблицы 18 установлена отрицательная корреляция по активности счетов нерезидентов, что означает отрицательное влияние фактора на норму прибыли на капитал, вероятно из-за специфики работы в рамках «особой» бизнес-модели кредитной организации. Исходя из результатов, отраженных в таблице 19, можно сделать вывод, что наиболее эффективное управленческое решение для «Банк ВТБ» (ПАО) может быть достигнуто на DMU 2 и DMU 5.

Таблица 19 – Данные расчетов Slacks по «Банк ВТБ» (ПАО)

Slacks	Активы-нетто, тыс. руб.	Активность клиентских счетов, относительные единицы	Активность счетов нерезидентов, относительные единицы
DMU1	0	0,562	0,086
DMU2	0	0	0
DMU3	0	0,307	0,016
DMU4	1 410,017	0	0,004
DMU5	0	0	0
DMU6	2 625,924	0	0
DMU7	1 123,006	0	0,001
DMU8	3 002,557	0	0,003
DMU9	0	0,098	0,006
DMU10	4 250,908	0	0,01
DMU11	618,348	0	0

Источник: составлено автором по материалам [28].

Данные, представленные в таблице 20, позволяют сделать вывод, что «Банк ВТБ» (ПАО) следует снижать активность счетов нерезидентов.

Таблица 20 – Данные расчетов DMU2, DMU5 по «Банк ВТБ» (ПАО)

Наименование решения / показателя	Активы-нетто, тыс. руб.	Активность клиентских счетов, относительные единицы	Активность счетов нерезидентов, относительные единицы	Норма прибыли к капиталу, в процентах
DMU2	-	-	-	-
Slacks	0	0,56	0,09	0
Weights	0	0	0	0,14
Values	9 727	1,74	0,1	7
Targets	9 727	1,18	0,01	10,84
DMU5	-	-	-	-
Slacks	0	0,56163	0,08646	0
Weights	0,00016	0	0	0,14286
Values	9 727	1,74	0,1	7
Targets	9 727	1,17837	0,01354	10,83562

Источник: составлено автором по материалам [28].

«Расчет по АО «Тинькофф Банк» показал, что существует отрицательная корреляция по показателям активов-нетто и активности клиентских счетов, данные факторы отрицательно влияют на показатель нормы прибыли на капитал (аналогично «Банк ВТБ» (ПАО) это связано со спецификой бизнес-модели кредитной организации, однако в случае АО «Тинькофф Банк» причина заключается именно с осуществлением бизнес-операций и операционной деятельности исключительно в цифровом контуре)» [141], что продемонстрировано в таблице 21.

Таблица 21 – Данные расчетов показателей по АО «Тинькофф Банк»

Наименование показателя	Minimum	Maximum	Mean	Standard Derivation	Корреляция с выходным параметром
Активы-нетто, тыс. руб.	194	1 307	587,6364	332,9939	-0,0929
Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	2,05	12,93	5,3382	3,8675	-0,0398
Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	0	0,1	0,0364	0,0296	0,5816
Прибыль (норма прибыли к капиталу, в процентах)	13	34	23,2727	6,8635	1

Источник: составлено автором по материалам [58].

По данным таблицы 22, в которой отражены размеры Slacks (смысл показателя описан ранее), можно сделать вывод, что «наиболее эффективное управленческое решение для АО «Тинькофф Банк» может быть достигнуто на DMU 1 и DMU 2» [141].

Таблица 22 – Данные расчетов Slacks по АО «Тинькофф Банк»

Slacks	Активы-нетто, тыс. руб.	Активность клиентских счетов, относительные единицы	Активность счетов нерезидентов, относительные единицы
DMU1	0	0	0
DMU2	0	0	0
DMU3	100,381	0	0,018
DMU4	122,81	0	0
DMU5	167,709	0	0
DMU6	174,896	0	0
DMU7	199,924	0	0
DMU8	82,704	0	0
DMU9	0	2,126	0
DMU10	0	3,422	0
DMU11	284,539	0	0

Источник: составлено автором по материалам [58].

Исходя из результатов, отраженных в таблице 23, можно сделать вывод, что «АО «Тинькофф Банк» следует снижать активность счетов нерезидентов (аналогично «Банк ВТБ» (ПАО))» [141].

Таблица 23 – Данные расчетов DMU1, DMU2 по АО «Тинькофф Банк»

Наименование решения / показателя	Активы-нетто, тыс. руб.	Активность клиентских счетов, относительные единицы	Активность счетов нерезидентов, относительные единицы	Норма прибыли к капиталу, в процентах
DMU1	-	-	-	-
Slacks	0	0	0	0
Weights	0	0	4,9	0
Values	194	2,1	0,1	34
Targets	194	2,1	0,1	34
DMU2	-	-	-	-
Slacks	0	0	0	0
Weights	0	0	4,9	0,03
Values	194	2,1	0,08	34
Targets	194	2,1	0,08	34

Источник: составлено автором по материалам [58].

«Сводные результаты оценки показателей, связанных с определением уровня цифровых рисков, и предлагаемые параметры минимизации для ПАО «Сбербанк», «Банк ВТБ» (ПАО) и АО «Тинькофф Банк» [141] представлены в таблице 24.

Таблица 24 – Сводные данные расчетов оценки цифровых рисков по ПАО «Сбербанк», «Банк ВТБ» (ПАО), АО «Тинькофф Банк»

Наименование решения / показателя	ПАО «Сбербанк»	«Банк ВТБ» (ПАО)	АО «Тинькофф Банк»
Номер решения	DMU2	DMU2	DMU1
Активы-нетто, тыс. руб.	22 087,62	9 727	194
Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	1,4	1,18	2,1
Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	0,07	0,01	0,1
Прибыль (норма прибыли к капиталу, в процентах)	16	10,84	34
Вид цифрового риска, который необходимо минимизировать	Цифровые операционные риски	Цифровые бизнес-риски	Цифровые бизнес-риски
Возможные варианты действий	Усиление процедур внутреннего контроля	Снижение объемов операций по нерезидентам	Снижение объемов операций по нерезидентам

Источник: составлено автором и опубликовано [141].

Результаты проведенных расчетов позволили установить, что ПАО «Сбербанк» наиболее подвержен влиянию цифровых операционных рисков, «Банк ВТБ» (ПАО) и АО «Тинькофф Банк» – влиянию цифровых бизнес-рисков. В качестве рекомендации по митигации данных рисков предложено усиление процедур внутреннего контроля для ПАО «Сбербанк» и снижение объемов операций по нерезидентам для «Банк ВТБ» (ПАО) и АО «Тинькофф Банк».

Использование модели анализа среды функционирования также может иметь прикладной характер в части отслеживания дополнительной метрики уровня обеспечения безопасности. Как было описано ранее, одной из ключевых проблем в современных условиях для организаций является выстраивание устойчивых систем кибербезопасности (что также актуально в контексте борьбы с цифровыми рисками). Например, специалисты из ведущей консалтинговой компании Ernst & Young замечают, что кибербезопасность является риском номер один для крупнейших мировых организаций [188].

Используя анализ среды функционирования, организация может оценить эффективность существующих мер цифровой защиты от кибератак в сравнении с другими организациями. Можно выделить следующие

показатели, связанные с кибербезопасностью в кредитных организациях (и других видах организаций): количество обнаруженных инцидентов безопасности (совершенных кибератак) за определенный период; количество устраненных инцидентов безопасности (совершенных кибератак) за определенный период; процент предотвращенных с помощью проактивных мер (предиктивный анализ угроз, выявление нарушений системами обнаружения) инцидентов безопасности; количество ложноположительных результатов, полученных в рамках работы средств мониторинга безопасности; количество ложноотрицательных результатов, полученных в рамках работы средств мониторинга безопасности; частота имитации фишинговых атак для проверки восприимчивости систем к фишингу; среднее время обнаружения инцидента безопасности; среднее время реагирования на инцидент безопасности (до полного устранения сбоя); среднее время локализации (время от обнаружения инцидента до полного предотвращения); количество сотрудников оперативной службы реагирования (центра мониторинга информационной безопасности).

Для поведения расчетов необходимо определить входные и выходные показатели модели. Учитывая контекст развития систем киберзащиты в российских кредитных организациях (недостаточное развитие, что подтверждается количеством утечек данных, описанных ранее), а также низкую осведомленность топ-менеджеров кредитных организаций об основах функционирования систем защиты (что подтверждается мнениями экспертов [180]), модель не должна быть перегружена глубоко прикладной информацией, но при этом должна обладать достаточными характеристиками для принятия последующего управленческого решения, влияющего на уровень обеспечения экономической безопасности организации.

Предлагается использовать следующие показатели модели анализа среды функционирования для определения эффективности существующих мер кибербезопасности, отраженные в таблице 25.

Таблица 25 – Входные и выходные показатели метода оценки эффективности мер кибербезопасности организации

Наименование группы	Наименование показателя
Входные показатели	расходы на технологии и инструменты кибербезопасности (расходы на облачную безопасность, безопасность данных, защиту инфраструктуры, управление доступом к идентификационным данным, интегрированное управление рисками)
	расходы на обучение и развитие кадров в области кибербезопасности
	расходы на аудит и тестирование информационных систем
	количество сотрудников оперативной службы реагирования на инциденты безопасности (кибератаки)
Выходные показатели	количество устраненных инцидентов безопасности низкого уровня критичности
	количество устраненных инцидентов безопасности среднего уровня критичности
	количество устраненных инцидентов безопасности высокого уровня критичности

Источник: составлено автором.

Логика выбора данных показателей заключается в необходимости оценки количества успешно отраженных кибератак при трате определенного количества средств и найме определенного количества сотрудников. На выходе получается «коэффициент эффективности» в части обеспечения кибербезопасности организации относительно организаций-конкурентов (может рассматриваться как компонент бенчмаркинга). При текущих вводных данный показатель обладает прозрачностью для топ-менеджмента организации, а также может быть использован в качестве дополнительной риск-метрики при выстраивании системы управления цифровыми рисками и при определении общего уровня экономической безопасности, которая во многом зависит от безопасности информационной.

Количественные данные, связанные с кибербезопасностью, по большей части засекречены, однако организация может запросить данные у других организаций путем направления соответствующих писем и организации референс-встреч. Подобная активность особенно важна в контексте исполнения Указа Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года», в которой обозначена «необходимость обеспечения противодействия вызовам и угрозам экономической безопасности в финансовой сфере, внедрения новых перспективных технологий (в том числе технологий цифровой экономики)» [17], а также подчеркивается «уязвимость информационной инфраструктуры

финансово-банковской системы» [17]. Для апробации модели используется ориентировочная информация за годовой период по 5 коммерческим американским кредитным организациям, сформированная на основе опубликованных в средствах массовой информации данных за 2021-2023 годы и отчетов аналитических агентств [185; 187; 189], отраженная в таблице 26.

Таблица 26 – Значения входных и выходных показателей метода оценки эффективности мер кибербезопасности организации по 5 исследуемым объектам

Наименование группы	Наименование показателя	Данные по организации				
		Банк А	Банк Б	Банк В	Банк Г	Банк Д
Входные показатели	Расходы на технологии и инструменты кибербезопасности, млрд долл.	15	5,6	5,1	1,9	0,4
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	0,008	0,004	0,006	0,0012	0,0023
	Расходы на аудит и тестирование информационных систем, млрд долл.	0,07	0,05	0,06	0,02	0,03
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	7,5	4,8	5	2,8	0,8
Выходные показатели	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	1,8	0,5	0,1	0,1	0,2
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	1,9	0,1	0,2	0,3	0,7
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	0,1	0,09	0,02	0,08	0,09

Источник: составлено автором по материалам [185; 187; 189].

В качестве расчетного метода выбран DEA с переменным эффектом масштаба (VRS). В отличие от представленной ранее модели CRS (постоянная отдача от масштаба), предполагавшей пропорциональное изменение выходных и выходных параметров (например, утроение ресурсов приведет к утроению результатов), модель VRS обладает большей вариативностью – она предполагает возможность возрастающей, постоянной и уменьшающейся отдачи от масштаба.

То есть несмотря на возможную эквивалентность входных и выходных параметров при постоянной отдаче от масштаба, например, количество затраченных на киберзащиту средств прямо пропорционально количеству внедренных протоколов защиты, есть априорные основания предполагать

возможность переменной отдачи от масштаба, так как увеличение затраченных средств и количества сотрудников не обязательно ведет к увеличению количества устраненных инцидентов – существуют факторы, которые нельзя предусмотреть наверняка (например, киберпреступники успешно использовали совершенно новую технологию, которую системы кибербезопасности организации сдержать не способны).

В данном случае линейная функция CRS дополняется, так как VRS является кусочно-линейной. Вычисления проведены с помощью программы Microsoft Excel:

а) для ориентации «на выход», подразумевающей способность организации к максимизации результатов при текущем уровне затрат;

б) для ориентации «на вход», которая подразумевает способность организации к минимизации затрат при сохранении результатов;

в) на основе подхода к расчету модели, предложенного Банкером, Чарнсом и Купером и называемого BCC. Эта модель была впервые представлена в 1984 году в целях ввода *переменной* отдачи от масштаба (модель CCR предполагала только постоянную отдачу от масштаба) [183];

г) с расчетом показателя «Прогнозируемые значения переменных», при которых можно достичь желаемого результата;

д) с расчетом показателя «группа аналогов», подразумевающего набор объектов, на которые следует ориентироваться исследуемому объекту для достижения необходимых результатов;

е) с расчетом показателя «Slacks», подразумевающего ресурсы, которые можно дополнительно использовать / результаты, которых можно дополнительно достичь без ущерба для текущей эффективности;

ж) с расчетом «Весового коэффициента», который присваивается входным переменным для поиска максимального уровня снижения ресурсов и присваивается выходным переменным для поиска максимального уровня повышения результатов.

Результаты проведенных расчетов отражены на рисунках 27 и 28.

Имя исследуемого объекта	Переменная	Ориентация переменной	Значения переменных	Значение рассчитанного показателя эффективности	Заключение об эффективности	Прогнозные значения переменных	Группа аналогов	Slacks	Весовой коэффициент
Банк А	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	15	1	Эффективен	15	Банк А	0	0,045083422
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,008			0,008		0	40,4685836
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,07			0,07		0	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	7,5			7,5		0	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	1,8			1,8		0	0,555555556
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	1,9			1,9		0	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,1			0,1		0	0
Банк Б	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	5,6	0,805	Неэффективен	3,62	Банк А, Банк Д, Банк Е	0,888	0
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,004			0,00322		0	250
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,05			0,036		0,00425	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	4,8			2,54		1,324	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,5			0,5		0	0,766666667
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,1			0,86		0,76	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,09			0,09		0	19,83333333
Банк В	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	5,1	0,4	Неэффективен	1,3	Банк Д, Банк Е	0,74	0
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,006			0,00164		0,00076	0
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,06			0,024		0	11,76470588
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	5			2		0	0,058823529
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,1			0,14		0,04	0
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,2			0,46		0,26	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,02			0,084		0,064	0
Банк Г	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	1,9	1	Эффективен	1,9	Банк Г	0	0
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,0012			0,0012		0	0
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,02			0,02		0	34,86486486
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	2,8			2,8		0	0,108108108
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,1			0,1		0	1,324324324
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,3			0,3		0	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,08			0,08		0	0
Банк Д	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	0,4	1	Эффективен	0,4	Банк Д	0	0
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,0023			0,0023		0	0
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,03			0,03		0	30,7875895
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	0,8			0,8		0	0,095465394
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,2			0,2		0	1,169451074
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,7			0,7		0	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,09			0,09		0	0

Источник: составлено автором.

Рисунок 27 – Показатели эффективности мер кибербезопасности организации, рассчитанные уточненным методом DEA (ориентация на вход)

Имя исследуемого объекта	Переменная	Ориентация переменной	Значения переменных	Значение рассчитанного показателя эффективности	Заключение об эффективности	Прогнозные значения переменных	Группа аналогов	Slacks	Весовой коэффициент
Банк А	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	15	1	Эффективен	15	Банк А	0	0,060882801
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,008			0,008		0	0
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,07			0,07		0	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	7,5			7,5		0	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	1,8			1,8		0	0,555555556
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	1,9			1,9		0	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,1			0,1		0	0
Банк Б	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	5,6	0,967924528	Неэффективен	4,754385965	Банк А, Банк Д	0,845614	0
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,004			0,004		0	19,49317739
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,05			0,041929825		0,0080702	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	4,8			2,798245614		2,0017544	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,5			0,677192982		0,1606238	0
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,1			1,057894737		0,9545809	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,09			0,092982456		0	11,11111111
Банк В	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	5,1	0,214548126	Неэффективен	5,1	Банк А, Банк Д	0	0,034246575
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,006			0,004134932		0,0018651	0
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,06			0,042876712		0,0171233	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	5			2,956849315		2,0431507	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,1			0,715068493		0,2489726	0
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,2			1,08630137		0,1541096	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,02			0,093219178		0	50
Банк Г	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	1,9	1	Эффективен	1,9	Банк Г	0	0
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,0012			0,0012		0	113,6363636
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,02			0,02		0	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	2,8			2,8		0	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,1			0,1		0	0
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,3			0,3		0	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,08			0,08		0	12,5
Банк Д	Расходы на технологии и инструменты кибербезопасности, млрд долл.	Входная	0,4	1	Эффективен	0,4	Банк Д	0	0,00761035
	Расходы на обучение и развитие кадров в области кибербезопасности, млрд долл.	Входная	0,0023			0,0023		0	0
	Расходы на аудит и тестирование информационных систем, млрд долл.	Входная	0,03			0,03		0	0
	Количество сотрудников оперативной службы реагирования на инциденты безопасности, тыс. чел.	Входная	0,8			0,8		0	0
	Количество устраненных инцидентов безопасности (кибератак) низкого уровня критичности, тыс. шт.	Выходная	0,2			0,2		0	0
	Количество устраненных инцидентов безопасности (кибератак) среднего уровня критичности, тыс. шт.	Выходная	0,7			0,7		0	0
	Количество устраненных инцидентов безопасности (кибератак) высокого уровня критичности, тыс. шт.	Выходная	0,09			0,09		0	11,11111111

Источник: составлено автором.

Рисунок 28 – Показатели эффективности мер кибербезопасности организации, рассчитанные уточненным методом DEA (ориентация на выход)

По итогам расчета можно сформировать развернутую цепочку выводов, позволяющую принять управленческое решение и тем самым повысить уровень кибербезопасности организации:

а) *Рассчитанный показатель эффективности (ключевая метрика)*. Данный показатель отражает относительную эффективность использования объектом ресурсов по сравнению с другими объектами исследования на основе используемого набора данных. В случае, если значение показателя по объекту равняется 1, объект характеризуется эффективностью осуществления деятельности (оптимальное использование ресурсов). Если показатель меньше 1, объект работает неэффективно и имеет потенциал к улучшению показателей. Проведенный анализ демонстрирует неэффективность Банка Б и Банка В как в модели, ориентированной на вход, так и в модели, ориентированной на выход. Таким образом, этим организациям требуется скорректировать подход к распределению ресурсов для достижения наилучших результатов.

б) *Прогнозные значения переменных*. Модель позволяет определить целевые значения показателей, при которых организации смогут добиться необходимых результатов – минимизировать затраты либо максимизировать результаты. По результатам анализа модели, ориентированной на вход, можно сделать вывод, что Банку Б следует сократить расходы по каждой из трех выходных переменных, связанных с затратами на киберзащиту, а также уменьшить количество сотрудников службы реагирования, за счет чего он сможет не только добиться аналогичных результатов, но и увеличить количество устраненных кибератак среднего уровня критичности на 0,76 тыс. шт. Банку В аналогично следует скорректировать каждый из входных показателей, при этом на выходе будут получены куда более высокие результаты по отражению атак – 0,14 тыс. шт. против 0,1 тыс. шт. по атакам низкого уровня критичности, 0,46 тыс. шт. против 0,2 тыс. шт. по атакам среднего уровня критичности, 0,084 тыс. шт. против 0,02 тыс. шт. по атакам высокого уровня критичности. Модель, ориентированная на выход, отражает

похожую картину – грамотное распределение ресурсов (даже с сокращением расходов и уменьшением штата сотрудников) позволит Банкам Б и В значительно улучшить результаты. Банк Б, к примеру, сможет в 10 раз улучшить показатель отражения кибератак среднего уровня сложности, а Банк В улучшит результат по противодействию кибератакам разного уровня в 5–6 раз.

в) *Определение группы аналогов*. Модель позволяет «отстающим» организациям определить организации, на принципы осуществления деятельности которых следует ориентироваться для достижения результата. В части сокращения затрат при сохранении успешного результата Банк Б может использовать распределения Банков А, Д и Е. Банку В подойдут подходы Банков Д и Е. В части максимизации результата при тех же ресурсах обе организации могут ориентироваться на Банки А и Д. Детально проанализировав причины распределения ресурсов в банках лидерах (например, использование иных технологий, либо подходов к выстраиванию защиты), менеджмент неэффективной организации может принять решения, которые в дальнейшем приведут к желаемым результатам по достижению эффективности.

г) *Slacks* в данном случае отражают не только дополнительные ресурсы, необходимые для достижения результата (как в случае с предыдущим анализом на основе метода DEA), но и показывают количество кибератак, которые могут быть дополнительно отражены без привлечения большего количества сотрудников и дополнительных затрат (например, Банк Б может сократить расходы на технологии на 0,888 млрд долларов, при этом преодолеть даже большее количество атак), а также отражают возможность сокращения затрат при увеличении количества отраженных атак (не в последнюю очередь это связано с крайней текущей неэффективностью Банка В, который согласно расчетам может сократить штат на 2 тыс. сотрудников без ущерба для эффективности).

Весовой коэффициент определяет важность и неоднородность каждой из входных и выходных переменных для расчета показателя эффективности и может быть дополнительно использован при определении оптимального решения по достижению эффективности при модернизации расчетов на основе линейного программирования.

Таким образом, предлагаемый подход на основе результатов расчетов, а именно эффективности организации относительно конкурентов, числовых значений ресурсно-результативных показателей, представленных к корректировке, предлагаемых вариантов развития на основе результатов других организаций, а также выявленных возможностей по достижению дополнительных результатов позволяет повысить уровень кибербезопасности, что достигается за счет оптимального распределения ресурсов, направленных на развитие технологий и инструментов, обучение и развитие кадров, аудит и тестирование информационных систем, а также подбор необходимого числа сотрудников для оперативного реагирования на инциденты безопасности. В результате данный подход напрямую улучшает управление цифровыми операционными рисками, что способствует обеспечению экономической и информационной безопасности.

Использование же входных и выходные параметров метода DEA в формате финансовых показателей (первый метод, описанный в данном параграфе) для последующего получения уточненной оценки влияния цифровых рисков на кредитные организации на их основе (модель расчета, основанная на консолидированных результирующих параметрах банковской деятельности) позволяет оценить эффективность использования капитала и определить значение показателя нормы прибыли к капиталу, при котором финансовая устойчивость кредитной организации не будет нарушена (экономическая безопасность кредитной организации обеспечивается на достаточном уровне, выстроена система управления рисками, при которой кредитная организация успешно противостоит цифровым рискам), то есть искомая эффективность будет достигнута. Стоит отметить, что приведенные

методы могут быть применимы к использованию организациями любых отраслей экономики. Рассмотренные в параграфе методы являются аналитической составляющей методических рекомендаций по митигации цифровых рисков.

3.2 Внедрение методических рекомендаций: возможные направления минимизации цифровых рисков

Процесс цифровой трансформации современной кредитной организации затрагивает большую часть банковских бизнес-процессов и косвенно влияет на процессы, которые нельзя «оцифровать». Импульс для внедрения новых технологий продолжает нарастать. Цифровые преобразования формируют реальную ценность для банковского бизнеса, многократно повышая эффективность банковской деятельности. Осуществление управления рисками на основе использования новых технологий позволяет кредитным организациям повысить точность и скорость процессов мониторинга, оценки и контроля рисков, а также способствует повышению качества работы в области соблюдения регуляторных требований. Полномасштабные и структурные изменения, направленные на снижение цифровых рисков кредитной организации, могут быть осуществлены с использованием тех же процедур и инструментов, что и для управления изменениями в других процессах. Однако управление цифровыми рисками имеет свои специфические особенности. В российской банковской системе вопросы цифровых рисков в основном касаются технологического обеспечения и информационной безопасности.

Проблема обеспечения информационной безопасности особенно актуальна в контексте возросшего количества кибератак на российские кредитные организации. Стоит отметить, что важность обеспечения цифровой защищенности кредитных организаций отражена в Доктрине информационной безопасности Российской Федерации, утвержденной

в 2016 году: «Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее» [16]. Е.И. Бричка, Ю.С. Жаркова и Е.С. Захарченко отмечают, что «кредитные организации, в частности, обеспечивают сохранность средств и персональных данных своих клиентов, последнее в период цифровизации всех сфер жизни общества является приоритетным» [86].

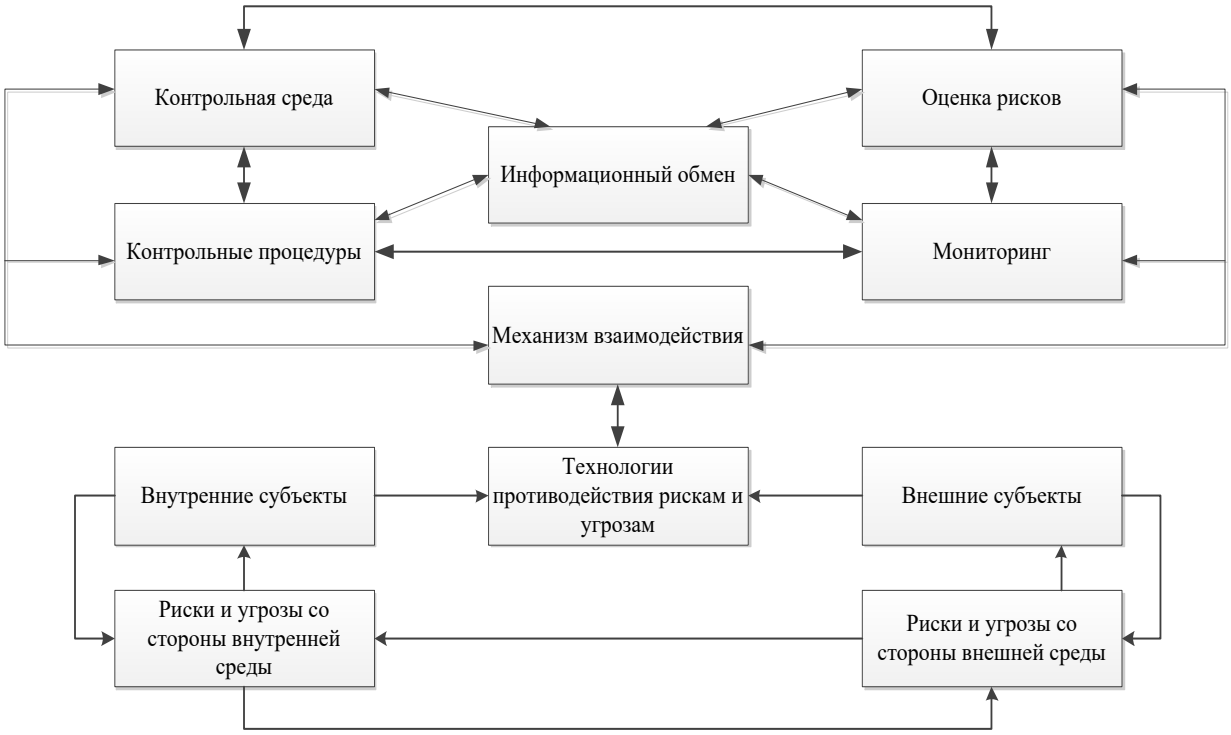
Специалисты по управлению рисками с осторожностью относятся к новым подходам ведения деятельности, характерным для цифровой трансформации, поскольку цена ошибок в области цифрового риска может быть неприемлемо высокой, в результате чего цифровизация бизнес-процессов российских кредитных организаций протекает куда медленнее, чем могла бы (что также является причиной необходимости разработки подходов к управлению цифровыми рисками). Лидеры цифровизации российского банковского сектора начинают осознавать, что так называемая ценность банковской деятельности может быть повышена с помощью использования цифровых автоматизированных подходов к управлению рисками.

Одним из таких подходов, например, может являться обеспечение постоянной эффективности функционирования рисковой контрольной среды и всесторонняя помощь ИТ-подразделений функции управления рисками в применении технологий в том числе для соответствия ожиданиям регулирующих органов в областях измерения рисков, агрегирования данных о рисках и ведения соответствующей отчетности. Чтобы реализовать все преимущества автоматизации бизнес-процессов, операционных процессов и процессов принятия управленческих решений, кредитным организациям

необходимо обеспечить соответствие системы управления рисками общей стратегии цифрового развития кредитной организации. Приоритетные варианты использования цифровых подходов к управлению рисками сосредоточены в таких областях как андеррайтинг, стресс-тестирование, управление операционным риском, соблюдение нормативных требований и осуществление контроля.

Работа с данными, проведение анализа и уровень развития ИТ-архитектуры являются ключевыми факторами управления цифровыми рисками. Сильно фрагментированные ИТ-архитектуры (в частности архитектуры данных) не могут обеспечить эффективную или, по крайней мере, действенную основу для управления цифровыми рисками (так как элементы систем разрознены, децентрализованы ими сложнее управлять) – современные аналитические методы (которые могут быть настроены на работу в том числе на алгоритмах метода DEA) и технологии хранения и обработки информации (платформы больших данных, облачные технологии, машинное обучение, искусственный интеллект, блокчейн, генеративные сети, интернет вещей, графовые базы данных) могут быть использованы в качестве инструментов, на основе которых будет возможно нивелировать недостатки таких систем.

Потенциальные преимущества модернизации процессов по управлению цифровыми рискам включают в себя повышение эффективности деятельности организации и увеличение доходов как от профильной, так и от непрофильной деятельности. Эффективность в управлении рисками может быть повышена за счет повышения прозрачности процессов, достигнутой за счет составления документации внутреннего контроля, в том числе модернизации традиционных алгоритмов информационного обмена в системе внутреннего контроля, описанного В.В. Земсковым и отраженного на рисунке 29, а также автоматизации систем сбора данных.



Источник: составлено автором по материалам [98].

Рисунок 29 – Алгоритм информационного обмена в системе внутреннего контроля

Анализ, проведенный в том числе в предыдущем параграфе исследования, показал, что возможные варианты действий в части управления цифровыми рисками крупнейших кредитных организаций России определяются в сфере:

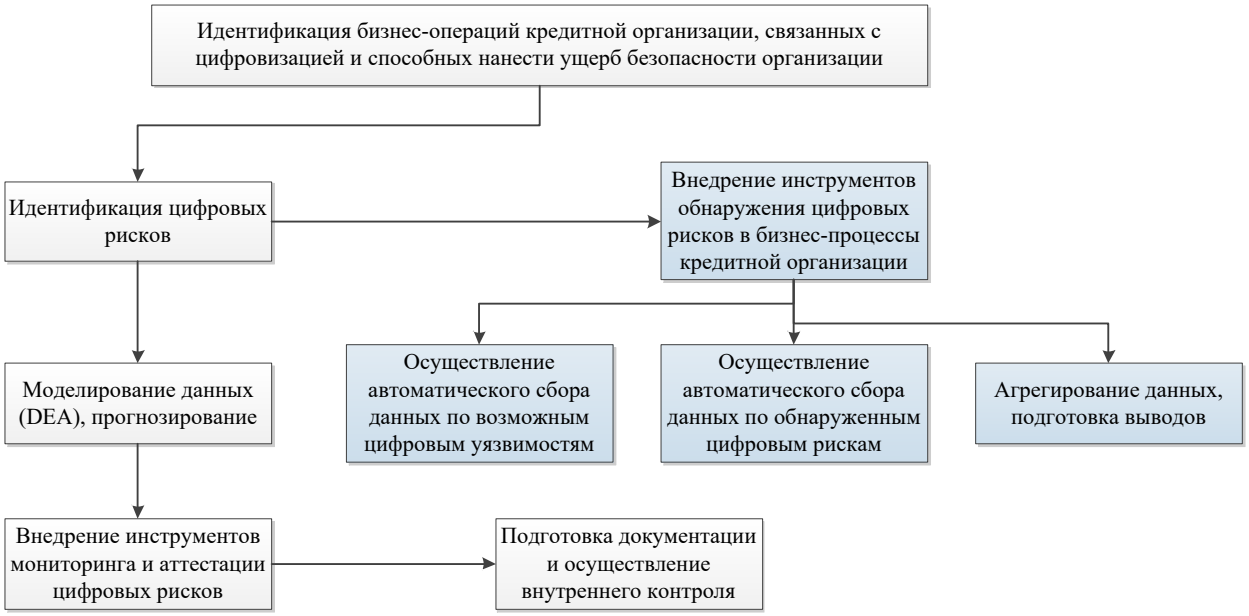
а) митигации кредитного риска;

б) проведения стресс-тестирования;

в) автоматизации операционной деятельности;

г) необходимости применения новых подходов к соблюдению внутренних нормативных требований (а также, возможно, и к содержанию внутренней нормативной документации кредитной организации с целью упросить процессы по внедрению цифровых технологий в банковскую деятельность).

Предлагаемые направления совершенствования бизнес-процессов кредитной организации в целях минимизации цифровых рисков представлены на рисунке 30.



Источник: составлено автором.

Рисунок 30 – Предлагаемые направления совершенствования бизнес-процессов кредитной организации в целях минимизации цифровых рисков

Стоит отметить, что из-за чувствительности среды, в которой формируются цифровые риски, идентификация подобных рисков может проходить в течение более длительного периода времени, чем при выявлении традиционных рисков (в частности рисков операционной деятельности). Конкретные мероприятия по минимизации рисков зачастую осуществляются дискретно (с перерывами), в связи с чем управление рисками в масштабе всей кредитной организации реализуется поэтапно и характеризуется краткосрочным целеполаганием.

Алгоритм управления цифровыми рисками в масштабе всей организации может происходить в три этапа:

а) приоритетные инициативы по управлению рисками определяются в соответствии с их выявленной «ценностью» и возможностью реализации в краткосрочной перспективе;

б) для реализации инициатив выбираются / разрабатываются цифровые решения, которые тестируются и при необходимости пересматриваются с учетом мнения заинтересованных сторон (в том числе участников банковской экосистемы);

в) принятые к реализации цифровые решения (в совокупности с дополнительными ресурсами, необходимыми для достижения результата, которые определяются на основе расчета Slacks метода DEA) внедряются в деятельность организации с учетом концепции «управления изменениями», при которой цифровое решение направлено на трансформацию определенного процесса с целью обеспечить его долгосрочное функционирование до того момента, пока цифровая среда в силу своей частой изменчивости не вынудит скорректировать бизнес-процесс / поменять подобранное цифровое решение, а также с учетом концепции «управления качеством данных» которая предполагает обеспечение достоверности и полноты данных через их регулярный мониторинг на наличие ошибок и проверку соответствия установленным стандартам и нормативным требованиям.

Возможности, выявленные на первом этапе, на втором этапе сопоставляются с цифровыми и основанными на технологических паттернах решениями, которые направлены на сокращение количества затрат и оптимизацию уже используемых ресурсов организации при одновременном повышении стандартов управления данными и их качества. Данные решения предлагается дополнить автоматизацией рабочих процессов, внедрением цифровых интерфейсов, а также использованием расширенной аналитики и машинного обучения. Также может быть использована «двухскоростная» ИТ-архитектура, под которой исследователи из компании Диасофт понимают ИТ-архитектуру «где все процессы сосредоточены во фронте (процессы взаимодействия с клиентом), доступ к ним осуществляется через различные каналы, а бэк-офисные учетные функции (внутренние процессы в случае кредитной организации) поддерживаются независимыми компонентами, доступ к которым осуществляется через процессы» [31], при этом основная ИТ-инфраструктура может продолжать работать в обычном режиме. На третьем этапе внедрения инновации в деятельность организации она сосредотачивается на процессах управления изменениями. Основное внимание уделяется настраиванию дизайна ИТ-архитектуры под новую

операционную модель, предполагающую использование современных методов анализа и оценки управления цифровыми рисками.

Стоит отметить, что организациям необходимо своевременно инвестировать в разработку цифровых продуктов, ИТ-решений и меры по обеспечению безопасности в цифровой среде для поиска новых возможностей, которые впоследствии могут быть применены как для модернизации процессов управления рисками и обеспечения экономической безопасности, так и для повышения эффективности бизнес-процессов.

Ключевым элементом успешной реализации данного подхода является подбор сотрудников, готовых работать над проектами высокой значимости. Особенно это актуально для сферы информационной безопасности, которая считается наиболее уязвимой, так как найти квалифицированных специалистов в этой области в России крайне сложно, что подтверждается мнением экспертов [62]. Важным аспектом является наличие у сотрудников кросс-функциональных навыков — знаний и опыта в разных областях, связанных с проектом. Например, ИТ-разработчик, участвующий в создании систем защиты от цифровых рисков, должен не только владеть навыками программирования, но и понимать основы управления рисками в банковской сфере. Это значительно увеличит шансы на успешную реализацию поставленных задач.

Эффективность процесса работы с цифровыми рисками зависит, в том числе, от удобства и скорости процесса работы с мероприятиями по митигации риска для сотрудников. Рассмотрим на примере цифровых операционных рисков. В целях минимизации риска в процессах / продуктах создаются *контрольные процедуры*. Под контрольными процедурами предлагается понимать действия, направленные на минимизацию операционного риска, они:

– встроены в процесс, сервис, продукт для снижения риска;

– подразделяются на автоматизированные, ручные, комбинированные;

– являются инструментами превентивного и детектирующего («обнаруживающего») контроля;

– совершаются как на регулярной, так и на разовой основе.

В случае неэффективности предусмотренных контрольных процедур или их отсутствия недостатки контрольной среды могут быть доработаны в виде реализации *мероприятий*. Мероприятия по минимизации цифрового операционного риска – это действия, направленные на:

– совершенствование существующих контрольных процедур для уменьшения цифровых рисков, например, обновление политик безопасности или усиление мониторинга операций, связанных с цифровыми активами;

– разработку новых контрольных механизмов для минимизации цифровых рисков, таких как создание автоматизированных систем реагирования на инциденты;

– минимизации последствий реализации цифрового риска (например, исправление дефектов систем или программного обеспечения, восстановление утраченных данных).

Основания для проведения мероприятий по митигации цифрового операционного риска включают:

– результаты самооценки операционных рисков, включая анализ бизнес-процессов;

– превышение допустимых уровней риск-аппетита в области операционных рисков;

– превышение пороговых значений ключевых индикаторов риска;

– рекомендации уполномоченных органов, лиц организации и подразделений, ответственных за управление операционными рисками;

– по итогам реализации событий операционного риска с потерями свыше установленной нормативной суммы.

Примеры мероприятий по минимизации цифрового операционного риска представлены в таблице 27.

Таблица 27 – Примеры мероприятий по минимизации цифрового операционного риска

Мероприятие	Какие риски минимизирует мероприятие?
Доработка сервиса проверки нотариальных доверенностей (автоматизация процесса проверки)	Проведение операций по поддельным доверенностям, отмененным доверенностям
Исправление дефекта систем оплаты в части дублирования платежей с помощью автоматизированных средств проверки	Излишнее / ошибочное перечисление средств получателям
Настройка проверки неблагонадежных партнеров при приеме на обслуживание в рамках «небанковских сервисов» с помощью алгоритмов искусственного интеллекта	Подключение неблагонадежных партнеров и возмещение убытков в результате их деятельности
Реализация на уровне автоматизированных систем контроля подтверждения вторым сотрудником расходных операций со счета клиента	Несанкционированные списания со счета клиента сотрудниками, третьими лицами, ошибочные списания со счета
Реализация автоматизированного информирования клиента о закрытии счета, подключении сервиса во всех каналах связи	Несанкционированное, ошибочное подключение сервиса клиенту
Реализация автоматизированного контроля поступления документов в архив	Утрата оригиналов документов и оспаривание клиентами операций
Реализация процедуры проверки клиента на предмет банкротства с помощью алгоритмов искусственного интеллекта	Неправомерное проведение операций по счетам банкротов
Изменение системы мотивации сотрудников для снижения случаев фиктивного выполнения бизнес-плана	Совершение фиктивных операций сотрудниками в целях выполнения бизнес-плана
Реализация кумулятивного лимита на клиента при совершении расходных операций в системах дистанционного банковского обслуживания	Несанкционированные списания средств со счета клиента в результате доступа третьих лиц в каналы дистанционного банковского обслуживания клиента
Переход на безбумажный документооборот по операции для минимизации риска утраты документа	Утрата оригиналов документов и оспаривание клиентами операций
Ограничение видимости критичной информации в автоматизированных системах	Проведение несанкционированных операций по счетам клиента сотрудниками
Реализация выборочного автоматизированного контроля начисления процентов на уровне бэк-офиса	Излишнее начисление и выплата процентов по счетам клиента

Источник: составлено автором.

Создание а*втоматизированной системы по управлению цифровыми рисками*, где подразделения могут регистрировать мероприятия и отслеживать процесс их осуществления, поспособствует повышению эффективности работы с данными рисками. Порядок работы с мероприятиями по митигации цифрового операционного риска представлен на рисунке 31.

Источник: составлено автором.

Рисунок 31 – Порядок работы с мероприятиями по митигации цифрового операционного риска

Функции участников процесса по реализации мероприятий по митигации цифрового риска могут быть описаны следующим образом:

а) Владелец мероприятия:

– разработка плана действий по управлению цифровыми операционными рисками, включая определение основных этапов и ресурсов, необходимых для минимизации потенциальных угроз;

– определение ответственного исполнителя, который будет заниматься непосредственной реализацией мероприятий по снижению операционного риска;

– первичная классификация и детальное описание мероприятий;

– регулярное внесение информации об исполнении мероприятия на каждом его этапе, а также обновление статуса и мониторинг прогресса;

– согласование исполнения мероприятия по итогам внесения факта исполнения исполнителем.

б) Исполнитель мероприятия:

– оперативное согласование или отклонение предложенного мероприятия, созданного владельцем, в зависимости от его актуальности, реальности выполнения, а также ресурсов, которые необходимы для его реализации;

– исполнение мероприятия и своевременное отражение фактических данных по каждому этапу исполнения для обеспечения прозрачности и контролируемости процесса.

в) Риск-менеджер операционного риска:

– согласование первичной информации по мероприятию, включая проверку его актуальности, адекватности предлагаемых мер, а также оценку рисков;

– согласование исполнения мероприятия.

Жизненный цикл мероприятий по митигации цифрового операционного риска представлен на рисунке 32.

Источник: составлено автором.

Рисунок 32 – Жизненный цикл мероприятий по митигации цифровых операционных рисков

Предложенный подход к организации процесса по проведению мероприятий по митигации цифровых рисков способствует повышению гибкости функции управления цифровыми рисками, улучшению адаптивности организации к изменяющимся условиям внешней и внутренней среды, увеличению эффективности работы сотрудников при выявлении рисков (внедрение четко структурированной процедуры упрощает процессы по идентификации, оценке и анализу рисков), повышению прозрачности процесса работы с рисками (каждый из участников процесса при необходимости может получить актуальные данные, касающиеся цифровых рисков), благодаря чему происходит развитие системы управления рисками.

Ландшафт цифровых рисков в сравнении с традиционными рисками более динамичный, изменчивый и сложный, поэтому минимизация цифровых рисков организации является перманентным (непрерывным) процессом управления рисками. По мере того, как функция управления цифровыми рисками будет автоматизирована, цель по повышению эффективности, результативности и точности анализа, оценки и последующей митигации цифровых рисков будет реализована на уровне, достаточном для того, чтобы цифровые риски не оказывали значимого влияния на финансовую устойчивость организации.

В будущем процессы управления цифровыми рисками, вероятно, станут характеризоваться совей гибкостью – умением подстраиваться под любые изменения внешней и внутренней цифровой среды при значительном снижении издержек (относительно текущего положения дел в банковском секторе, когда затраты на ИТ-инфраструктуру и обеспечение ее безопасности являются одной из основных расходных статей современной кредитной организации), однако современное состояние функции управления цифровыми рисками в организации требует поиска новых подходов и инструментов, способствующих ее эффективной реализации в целях обеспечения экономической безопасности.

3.3. Развитие системы управления рисками в кредитной организации в условиях цифровизации для обеспечения экономической безопасности

Современный этап развития российского банковского сектора характеризуется рядом ключевых особенностей: кредитные организации активно оцифровывают бизнес-процессы и внедряют инновации в операционную деятельность; совершенствуются способы проведения онлайн-платежей (также практически все современные цифровые площадки оказания услуг и предоставления сервисов позволяют совершать онлайн-оплаты); особое внимание уделяется обеспечению кибербезопасности; формируются экосистемы финансовых услуг (процессы предоставления банковских, инвестиционных, страховых и иных услуг осуществляются с помощью единых технологических каналов); кредитные организации конкурируют между собой путем выпуска новых цифровых продуктов, которые могут заинтересовать клиентов за счет их удобства, а также высокой скорости проведения операций; появляются новые регуляторные требования, направленные на обеспечение непрерывности банковской деятельности в условиях существования кредитных организаций в цифровой среде. При этом стоит отметить, что все обозначенные выше аспекты цифровизации банковского сектора так или иначе оказывают влияние на систему управления рисками кредитной организации, требуют ее совершенствования и адаптации к новым условиям, характеризующимся появлением особого вида рисков – цифровых.

Большая часть мошеннических действий, затрагивающих банковский сектор, связана с операционными и кредитными рисками. Так, криминологический анализ современного состояния мошенничеств в банковской сфере, выполненный А.Л. Репецкой и Л.А. Петряковой показал, что «в общей структуре мошенничеств, зарегистрированных в Российской Федерации, каждое десятое было совершено в банковской сфере,

где наибольшую долю (80%) составляют мошенничества с использованием электронных средств платежа. При их совершении в последние годы доминирует использование подлинных карт или их реквизитов, похищенных у владельцев путем обмана методами социальной инженерии» [148]. Очевидно, что кредитные организации с большим размеров активов (и клиентов, соответственно) будут больше подвержены цифровым рискам. В рамках проведения цифровизации бизнес-процессов в целях митигации цифровых рисков «основной акцент необходимо делать именно на бизнес-процессы, связанные с кредитованием, поскольку: кредитование продолжается оставаться ключевым источником доходов российских кредитных организаций и значимая доля мошеннических действий связана с психологическим давлением и принуждением клиентов к осуществлению кредитных операций (у людей зачастую не бывает накоплений, и мошенники требуют оформить кредиты под разными предлогами, чтобы в дальнейшем заполучить средства, взятые обманутым клиентом в кредит)» [141].

В качестве мер, направленных на митигацию цифровых рисков, обеспечивающих развитие системы управления банковскими рисками в контексте существования кредитных организаций в цифровой среде, предлагается использовать следующие:

а) «*Бизнес-модель: ожидания клиентов в отношении цифровых технологий, в том числе процедур одобрения дебетовых и кредитных карт*. Улучшение систем анализа данных клиентов как в части скорости принятия решений, так и в части отслеживания возможной подделки документов на основе современного технологического инструментария (в частности, машинного обучения) – ключевой фактор процесса митигации цифровых бизнес-рисков и цифровых операционных рисков» [141]. Согласно расчетам с помощью метода, описанного в параграфе 3.1, где приведенные риски оцениваются по параметру «активность клиентских счетов», данная мера может быть эффективна для АО «Тинькофф Банк».

б) Управление функциями подразделений и персоналом кредитной организации. В целях развития функций различных подразделений кредитной организации в области управления рисками возможна реализация направлений, распределенных по подразделениям, которые отражены в таблице 28. Процесс по работе по данным направлениям подразумевает проведение соответствующих мероприятий с помощью подхода, отраженного в предыдущем параграфе.

Таблица 28 – Направления митигации цифровых рисков в разрезе подразделений кредитной организации

Рекомендуемый стоимостной ориентир	Предлагаемые направления	Подразделение, ответственное за реализацию	Форма мотивации персонала
Доходы кредитной организации от совершения бизнес-операций (ограничение по размеру возможных потерь 5-10 процентов)	Удовлетворение спроса клиентов на цифровые услуги (решения в реальном времени, заявки на кредит)	Клиентские офисы, точки продаж, бэк-офисы (внутренние подразделения), технические службы	Премии, проценты от успешного осуществления сделок
	Минимизация риска потерь клиентов в результате замедления процессов утверждения и сопровождения кредитной сделки		
	Интеграция в деятельность третьих лиц (осуществляющих контроль) в рамках проведения кредитных сделках для повышения качества андеррайтинга		
	Концепция динамического ценообразования с поправкой на риск с установкой лимитов по сегментам клиентов		
Сокращение затрат по митигации рисков (повышение доходов на 10-15 процентов)	Анализ данных на основе машинного обучения с повышением точности оценки рисков за счет использования метода DEA (обработка статистических данных различного рода, мониторинг, моделирование)	Операционные подразделения	Премии
	Интеграция баз данных нового поколения в системы управления рисками кредитной организации		
	Повсеместное внедрение процессов обработки данных в реальном времени с возможностью оперативного получения отчетности для мониторинга и прогнозирования цифровых рисков		
Снижение текущих затрат (на 15-20 процентов)	Оцифровка процессов для обеспечения оптимального использования времени и ресурсов (рост добавленной стоимости)	Технические службы	Премии
	Стандартизация подходов к управлению цифровыми рисками с точки зрения технической реализации этапов анализа и оценки рисков		

Источник: составлено автором.

в) «*Требования регулирующих органов в отношении функции управления рисками*» [141]. Вопросы, связанные с цифровыми рисками, автоматизацией их контроля и агрегированием данных о рисках, становятся приоритетными в процессе разработки мегарегулятором новых правил по управлению банковскими рисками. Предположительно, Банк России примет новые нормативные акты и инструкции, касающиеся всестороннего анализа цифровых рисков, ограничения цифровых активов по отношению к капиталу кредитных организаций, оценки «качества цифровых активов, новых требований к управлению данными, а также к точности и корректности информации, используемой при проведении стресс-тестирования цифровых рисков» [141]. Предложенные подходы к использованию метода DEA, описанные ранее в работе, позволят кредитным организациям сформировать *модельный аппарат*, позволяющий краткосрочно и среднесрочно спрогнозировать достаточность количества ресурсов различного рода, необходимых для борьбы с цифровыми рисками, тем самым приблизить к максимуму вероятность достижения (выполнения) нормативов, установленных со стороны мегарегулятора.

г) «*Растущие требования к качеству управления данными и расширенной аналитики.* Цифровое пространство оказывает влияние на риски всех сегментов банковского бизнеса. Давление внешней среды на рыночную стоимость и прибыль кредитной организации с течением времени будет только нарастать. Финтех-компании, оказывающие конкурентные кредитным организациям услуги в платежных системах, работают без необходимости использования традиционных банковских операций, филиальных сетей и устаревших ИТ-систем, при этом они характеризуются гораздо более низким соотношением затрат к доходам. Для того чтобы не допустить ухудшения финансовых показателей, кредитные организации могут перенять цифровые подходы ведения деятельности у известных интернет-магазинов: например, можно разработать мобильные приложения, позволяющие мгновенно выдавать индивидуальные потребительские кредиты. В качестве способа

защиты может быть использована оцифровка ключевых этапов кредитных процессов, в частности автоматизация механизма принятия решений по выдаче кредита, за счет чего будет наблюдаться повышение эффективности деятельности, например, в сегментах малого и среднего бизнеса» [141]. Для успешной реализации процесса цифровизации кредитным организациям необходимо: обеспечивать высокую точность данных через эффективное управление, направленное на поддержание их доступности, целостности, конфиденциальности и актуальности для оптимизации бизнес-процессов и принятия решений; совершенствовать методы интеграции данных, объединяя информацию из различных источников для создания комплексных и надежных наборов данных; защищать данные от несанкционированного доступа с помощью шифрования, аутентификации, резервного копирования, восстановления данных, а также постоянного мониторинга и аудита; применять методы расширенной аналитики, такие как кластеризация и прогностический анализ с использованием алгоритмов машинного обучения и визуализации данных (создание дашбордов, под которыми, к примеру, И.Г. Рзун понимает «инструменты управления информацией, которые визуально отслеживают, анализируют и отображают ключевые показатели эффективности, метрики, позволяя отслеживать текущее состояние бизнеса, отдела, команды или конкретный процесс» [13]).

д) «Необходимость осуществления дальнейшей цифровой трансформации управления рисками» [141]. Отслеживание изменений, касающихся выхода новых технологий, связанных с процессами обеспечения экономической безопасности и управления рисками, а также мониторинг активностей, происходящих во внешней среде на предмет появления у злоумышленников новых средств для нанесения ущерба кредитным организациям – важнейшие аспекты функции управления цифровыми рисками. Грамотно выстроенные системы идентификации рисков и обеспечения безопасности на разных уровнях с течением времени утратят свою эффективность. Со временем будут выявляться малозаметные

неисправности, «дыры», через которые впоследствии могут быть нанесены атаки со стороны преступников. Новые вирусы различного рода имеют тенденцию к самораспространению, злоумышленникам зачастую нужно только запустить их в банковскую сеть. Киберпреступность развивается крайне стремительно, и кредитные организации не могут достойно ей противостоять в силу сильной бюрократизации процессов и тяжелого процесса внедрения технологий в банковскую деятельность. В этой связи кредитным организациям следует быть особо внимательными в контексте обновления ИТ-систем – делать это необходимо регулярно и своевременно, иначе уязвимость ИТ-архитектуры кредитной организации будет возрастать. Постоянное развитие технологических продуктов и инструментов защиты в части их функциональности позволит превентивно ответить на угрозы извне. Стоит отметить, что банковские технологии любого вида образуют технологическую экосистему – развивать и своевременно обновлять следует все ее элементы. Также кредитным организациям стоит акцентировать внимание клиентов на необходимости обновления всевозможного программного обеспечения, предоставляемого кредитными организациями (зачастую это делается с помощью информирования в мобильных приложениях, чего недостаточно). Рекомендуется формировать отдельные подразделения, ответственные за контроль технологического развития кредитной организации. В то же время необходимо понимать, что многие процессы, связанные с цифровыми рисками, остаются за пределами цифровых возможностей большинства российских кредитных организаций. Значительные финансовые усилия за последние годы были направлены на создание оригинальных интерфейсов мобильных приложений и разработку удобных порталов для предоставления клиентам услуг и сервисов – вопросы обеспечения защищенности банковского цифрового контура (в том числе и в рамках работы с приложениями и сайтами) были отодвинуты на второй план, о чем говорит статистика, представленная во второй главе исследования.

Каждый из приведенных в работе цифровых рисков должен быть управляем, каждая из обозначенных выше мер должна быть осуществлена – для этого предлагается использовать инновационные решения, не каждое из которых широко применяется в банковской среде, однако потенциально может иметь значимый эффект, в том числе при обеспечении безопасности кредитной организации:

а) Цифровой двойник для сценарного прогнозирования и стресс-тестирования. Цифровой двойник — это цифровая (виртуальная) модель любых объектов, систем, процессов или людей. Она точно воспроизводит форму и действия оригинала и синхронизирована с ним. Цифровой двойник нужен, чтобы смоделировать, что будет происходить с оригиналом в тех или иных условиях. Использовать данную технологию в кредитной организации можно по-разному. Например, создать цифрового двойника клиента кредитной организации (с учетом информации о его сбережениях, кредитной истории) и воспроизвести банковский процесс, к примеру, получение кредита, благодаря чему для клиента могут быть сформированы условия предоставления кредита, что поможет нивелировать кредитные риски как для кредитной организации, так и для клиента. Исследователи применения цифровых двойников в банковской сфере отмечают, что данная технология повышает эффективность банковского контроллинга и клиентского сервиса, обеспечивает снижение стоимости бизнес-процессов, способствует замещению ряда физических процессов виртуальными, что влияет на стоимость операций и формирует прямой экономический эффект для кредитных организаций [118]. Также отмечается, что создание в кредитной организации системы управления на базе технологии цифровых двойников позволяет сформировать действенный инструментарий, например, в области управления залоговым портфелем в условиях прогнозируемого на ближайшие годы роста кредитования кредитными организациями [142]. Таким образом, цифровой двойник может

быть эффективным инструментом в управлении цифровыми бизнес-рисками, в том числе при обеспечении безопасности процедур кредитования.

б) Учет в аналитических моделях показателя Risk-adjusted return on capital, или скорректированная риском доходность на капитал (далее – RAROC) для поддержания высокой эффективности использования капитала. Доходность капитала с поправкой на риск – это финансовая метрика, используемая для измерения доходности с поправкой на риск и определения оптимального распределения капитала. Показатель соотносит величину экономического капитала, подверженного риску, с получаемым доходом. RAROC позволяет кредитной организации оценить, приносит ли ее деятельность адекватную прибыль с учетом профиля риска. Использование метрики в передовых моделях предиктивного анализа позволит повысить точность количественной оценки риска, поспособствует принятию эффективных бизнес-решений и оптимизации использования капитала.

RAROC рассчитывается следующим образом (1) [144]

$$RAROC = \frac{\text{Чистый доход} - \text{Ожидаемые потери}}{K * EAD}, \quad (1)$$

где K – требование к экономическому капиталу, резервируемому против совокупного риска (чаще всего определяется как неожиданные потери в соответствии с формулой, установленной Базельским комитетом по банковскому надзору [176]);

EAD – стоимость под риском дефолта.

Основные преимущества использования RAROC:

– возможность оценки эффективности деятельности кредитной организации с учетом риска и эффективности использования капитала;

– возможность сравнения доходности различных бизнес-подразделений и продуктовых линий;

– возможность принятия высокоточных решений о распределении капитала;

– возможность установления лимитов риска.

В контексте использования новейших аналитических инструментов модели RAROC имеют особую актуальность в части:

– повышения качества данных – обеспечение наличия точных данных о рисках и доходности в различных разрезах осуществления деятельности;

– разработки моделей анализа риска – построение моделей, отражающих уникальный профиль риска, а также стратегию кредитной организации;

– калибровки моделей – проверка моделей на предмет сбоев для точной настройки измерения показателей риска;

– тестирования и валидации – обязательная проверка моделей до и после внедрения для подтверждения точности расчетов.

Эффективность использования данной метрики также подчеркивается исследователями ее применения в работе кредитных организаций, в частности некоторые авторы обозначают, что показатель является сопоставимым и, следовательно, может служить критерием размещения капитала между различными по величине и структуре портфелями, подразделениями и направлениями деятельности [173], а также может применяться при автоматизации бизнес-процесса принятия решения по размещению активов в банковском секторе [14], то есть использование данной метрики при формировании моделей продвинутой аналитики расчета финансовых показателей позволит кредитным организациям управлять цифровыми бизнес-рисками.

Высокая эффективность капитала может быть достигнута также и при помощи фиксирования и отслеживания соглашений об уровне сервисов по процедурам расчетов риск-метрик в соответствии с потребностями владельцев риска и внедрения автоматизированных инструментов риск-оценок и лимитных контролей на этапе анализа будущих сделок (в том числе под обработку запросов от платформенных деривативных решений для клиентов),

что позволит кредитным организациям спрогнозировать возможный уровень финансовой устойчивости при определенных вариантах развития событий и тем самым повысить уровень экономической безопасности за счет вариативности принятия решений.

в) Формирование персонализированных кредитных продуктов для розничного бизнеса с учетом концепции проактивного кредитного предложения в момент формирования потребности. Процесс обработки кредитных заявок, обеспечения их точности и соответствия внутрибанковским требованиям является достаточно проблемным и требует особого внимания в контексте управления рисками. Автоматизация выдачи кредитов – это инструмент, позволяющий оптимизировать и ускорять каждый этап кредитного цикла, начиная с кредитной отчетности и контроля за погашением кредита и заканчивая оценкой рисков и принятием решений.

Данная технология особенно актуальна в том случае, если клиент, к примеру, использует приложение кредитной организации для перевода денежных средств – в это время ему поступает уведомление о предварительном одобрении кредита, то есть клиент уже может подразумевать, что у него есть возможность взять кредит. Так формируется проактивное кредитное предложение, позволяющее кредитной организации обозначить для клиента возможность использования еще одной услуги. Искусственный интеллект, роботизированная автоматизация процессов, оптическое распознавание символов и другие передовые технологии используются в программном обеспечении для автоматизации выдачи кредитов, благодаря чему нивелируется риск, связанный с трудоемкими ручными процессами кредитования.

Преимущества современных автоматизированных систем обработки кредитов:

– более качественные банковские данные – отсутствие ручных операций по вводу данных и рассмотрению кредитных заявок снижает (если не полностью устраняет) вероятность человеческой ошибки;

– ускоренный прием клиентов;

– сокращение сроков рассмотрения заявок – с использованием автоматизации банковские процессы, часто связанные с работой с множеством неструктурированных разрозненных документов, могут быть оптимизированы нажатием одной кнопки;

– повышение соответствия нормативным требованиям;

– автоматизация общих запросов клиентов.

Особую актуальность также обретают кредитные конвейеры. Х.И. Аминов в работе, связанной с исследованием преимуществ кредитного конвейера, отмечает, что «кредитный конвейер – это комплексное решение для автоматизации и построения сквозного процесса обработки кредитных заявок и принятия решения по ним. Кредитные конвейеры позволяют автоматически определять сегмент заемщика, выбирать подходящий продукт кредитования, проверять заемщика на стоп-факторы, запрашивать данные по заемщику из внешних источников, рассчитывать сумму кредита в соответствии с запрашиваемыми параметрами, оценивать кредитоспособность заемщика на основе скоринговых моделей, формировать решение по кредитной заявке» [2].

С учетом использования технологий машинного обучения и обработки данных при помощи искусственного интеллекта эффективность и точность работы кредитных конвейеров может быть значительно повышена. Таким образом, данные технологии могут помочь кредитным организациям в борьбе как с операционными цифровыми рисками, так и с цифровыми бизнес-рисками.

г) Точность и скорость принятия решений по сделкам с корпоративными клиентами за счет аналитических инструментов в едином рабочем месте андеррайтера. Н.Н. Никулина замечает, что «андеррайтер в банковском секторе — это специалист кредитной организации, который проводит независимую экспертизу рисков кредитования, анализ и проверку информации клиента, данных из открытых источников. Он формирует

профессиональное суждение с идентификацией рисков, способов их минимизации, используя в работе общие подходы к управлению рисками, соответствующие требованиям единого мегарегулятора» [130]. Для повышения качества работы андеррайтера предлагается разработка рабочего места андеррайтера-аналитика с доступом ко всем параметрам кредитных заявок, лимитов и сделок, результатов мониторинга по клиенту, а также к его финансовым показателям с гибким интерфейсом для построения отчетности и с использованием «подсказок» на основании моделей для вынесения заключения (принятия решения).

Также кредитным организациям следует внедрять процесс автоматизированного распределения кредитных заявок между андеррайтерами на основе профиля риска задачи, нагрузки андеррайтера, уровня его компетенции и специфики сделки. Предложенные инструменты могут иметь решающее значение при управлении цифровыми операционными рисками.

д) Промышленное управление цифровыми операционными рисками, включая выявление аномалий с помощью продвинутой аналитики, а также контроль на этапе дизайна продуктов и сервисов. В части работы с операционными рисками кредитным организациям следует применять новые инструментарии для стресс-тестирования, например, программы для выявления чувствительностей и уязвимостей текущей бизнес-модели к изменению внешних факторов (в том числе с использованием обратного стресс-тестирования). Построение процесса промышленного управления операционными рисками может происходить за счет создания аналитических витрин и установления индикаторов операционных характеристик по направлениям деятельности, внедрения процесса учета операционных рисков на этапе проектирования процессов и продуктов, создания инструментов по выявлению аномалий (что напрямую повлияет на повышение информационной и экономической безопасности кредитной организации), а

также внедрения системы управления модельным риском на основе инструментов количественной оценки [135].

е) Продажи и планирование. Создание цифрового рабочего места для менеджеров по работе с клиентами. Отсутствие у персонала большинства российских кредитных организаций (в том числе, например, в ПАО «Сбербанк») систематических навыков по созданию цифровых взаимоотношений с клиентами с фрагментированным обзором данных (процесс анализа данных, который проводится на основе разрозненной информации о клиентах, то есть когда полного объема информации о клиенте еще нет, либо сбор продолжается) приводит к трудностям в части консолидации клиентской информации. Процессы адаптации, кредитования и послепродажного обслуживания требуют создания специальных цифровых рабочих мест (возможно, удаленно, как, например, реализовано в АО «Тинькофф Банк»). Подобная инновация увеличит качество взаимодействия с клиентами, сократив административные затраты.

ж) Более высокое качество данных может быть получено благодаря улучшению систем обмена данными и инструментов рабочего процесса. Автоматизация и интеграция автоматизированной системы управления цифровыми рисками (рассмотрена в предыдущем параграфе) в банковскую деятельность позволит повысить прозрачность процессов благодаря высокоточной обработке данных и мониторингу. Автоматизация экономит кредитной организации время и средства при принятии кредитных решений (от новых аналитических технологий по проверке кредитной истории, финансового состояния клиента и уровня его долговой нагрузки, а также технологий андеррайтинга до новых аналитических методов расчета и распределения капитала).

и) Идентификация и анализ. Сделав машинное обучение частью инструментария по оцифровке процессов управления риском, кредитные организации могут получить выгоду в среднесрочной перспективе

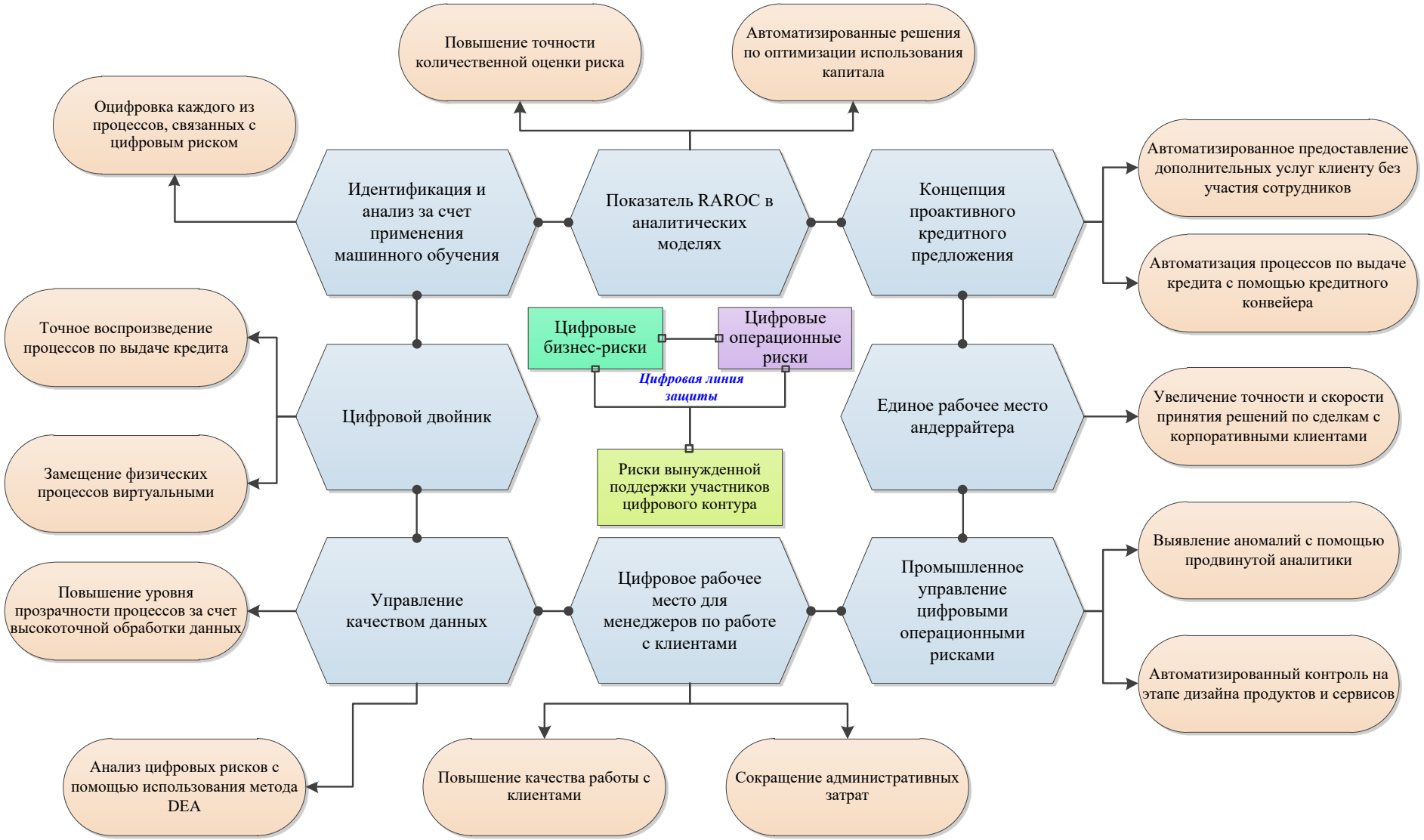
(оптимизация времени и операционных издержек), одновременно масштабируя потенциал для общей трансформации.

Машинное обучение может применяться, например, в системах раннего предупреждения для получения более глубокого понимания больших и сложных наборов данных без фиксированных ограничений стандартизированного статистического анализа. С помощью машинного обучения возможно автоматизировать отчетность, процедуры мониторинга кредитного портфеля (стоит отметить, что в сегменте малого и среднего бизнеса использование метода DEA, описанного в работе ранее, по параметру «активность клиентских счетов» поспособствует проведению качественного анализа с целью снижения просроченных платежей), повысить качество и скорость анализа данных, а также формировать мгновенные оптимальные рекомендации по действиям, связанным с возникновением инцидентов цифрового риска.

Приведенные инструменты формируют *новую линию защиты кредитной организации – цифровую*, ориентированную на события и риски, связанные с деятельностью, происходящей в цифровом контуре и окружающей кредитную организацию, начиная от внутренних операций и заканчивая взаимодействием с клиентами и партнерами в онлайн-пространстве.

Разработанные в ходе проведенного исследования положения были применены в практической деятельности «Банк ВТБ» (ПАО) – одной из крупнейших кредитных организаций России. В качестве управленческого инструмента был составлен «куб безопасности», который объединяет в себе предложенные положения в части идентификации, оценки и митигации цифровых рисков.

Цифровая линия защиты организации представлена на рисунке 33, «куб безопасности», сформированный для применения в кредитной организации «Банк ВТБ» (ПАО), отражен на рисунке 34 и рисунке 35.



Источник: составлено автором.

Рисунок 33 – Цифровая линия защиты организации

Y-объекты										
обеспечение защиты корпоративных интересов										
обеспечение защиты объектов										
обеспечение информационной безопасности										
обеспечение безопасности участников экосистемы										
обеспечение экономической безопасности										
X-риски	неправильный выбор партнеров	неправильный выбор объектов для инвестиций	неправильный фокус на развитие определенных продуктов и сервисов экосистемы	неправильное определение и неправильная оценка необходимых ресурсов и рисков	риски недобросовестной работы сотрудников	риски отказа информационных систем, сбоев в процедурах управления	риски сложной архитектуры информационных технологий	риски информационной безопасности, утечки и несанкционированного использования персональных данных клиентов	риск возникновения потребностей дополнительного финансирования у одного из участников экосистемы	риск возникновения хронической убыточности отдельных участников экосистемы или реализации рисков, приводящих к крупным финансовым потерям
Z-средства										
инструменты обнаружения цифровых рисков (искусственный интеллект, машинное обучение)										
инструменты автоматического сбора и агрегирования данных (большие данные)										
инструменты моделирования данных (в том числе метод DEA)										
инструменты защиты от кибератак (сетевая защита, блокчейн)										
инструменты мониторинга и аттестации цифровых рисков (предписательная аналитика, диагностическая аналитика)										
осуществление внутреннего контроля										
X-риски	неправильный выбор партнеров	неправильный выбор объектов для инвестиций	неправильный фокус на развитие определенных продуктов и сервисов экосистемы	неправильное определение и неправильная оценка необходимых ресурсов и рисков	риски недобросовестной работы сотрудников	риски отказа информационных систем, сбоев в процедурах управления	риски сложной архитектуры информационных технологий	риски информационной безопасности, утечки и несанкционированного использования персональных данных клиентов	риск возникновения потребностей дополнительного финансирования у одного из участников экосистемы	риск возникновения хронической убыточности отдельных участников экосистемы или реализации рисков, приводящих к крупным финансовым потерям

Источник: составлено автором.

Рисунок 34 – «Куб безопасности» для «Банк ВТБ» (ПАО)

Y-объекты										
обеспечение защиты корпоративных интересов										
обеспечение защиты объектов										
обеспечение информационной безопасности										
обеспечение безопасности участников экосистемы										
обеспечение экономической безопасности										
Z-средства	инструменты обнаружения цифровых рисков (искусственный интеллект, машинное обучение)	инструменты автоматического сбора и агрегирования данных (большие данные)	инструменты моделирования данных (в том числе метод DEA)	инструменты защиты от кибератак (сетевая защита, блокчейн)	инструменты мониторинга и аттестации цифровых рисков (предписательная аналитика, диагностическая аналитика)	осуществление внутреннего контроля				

Источник: составлено автором.

Рисунок 35 – «Куб безопасности» для «Банк ВТБ» (ПАО)

Таким образом, в рамках проведенного в данной главе исследования, посвященного формализации методических рекомендаций по митигации цифровых рисков, предложениям по внедрению данных рекомендаций, а также направлениям развития системы управления рисками кредитной организации в условиях цифровизации:

– предложен авторский подход к использованию метода анализа среды функционирования на основе финансовых показателей кредитной организации, позволяющий оценить эффективность использования кредитной организацией капитала, а также определить значение показателя нормы прибыли к капиталу, соответствующее достаточному уровню финансовой устойчивости кредитной организации (одна из главных метрик, определяющих уровень экономической безопасности кредитной организации), для последующей оценки влияния цифровых рисков на организацию;

– предложен авторский подход к определению уровня обеспечения кибербезопасности организации относительно других организаций, основанный на методе анализа среды функционирования, позволяющий в том числе сформировать значения метрик, на основе которых может быть принято управленческое решение, направленное на повышение уровня кибербезопасности в организации: *рассчитанный показатель эффективности* (коэффициент эффективности организации в области обеспечения кибербезопасности относительно конкурентов), *прогнозные значения переменных* (целевые значения показателей, при которых организация сможет достичь желаемых результатов в области обеспечения кибербезопасности), *определение группы аналогов* (определение организаций, на которые исследуемой организации стоит ориентироваться для достижения достаточности уровня обеспечения кибербезопасности), а также *slacks* (показатель, отражающий количественные значения дополнительных ресурсов, необходимых организации для получения желаемого результата,

либо улучшения текущего результата в области обеспечения кибербезопасности);

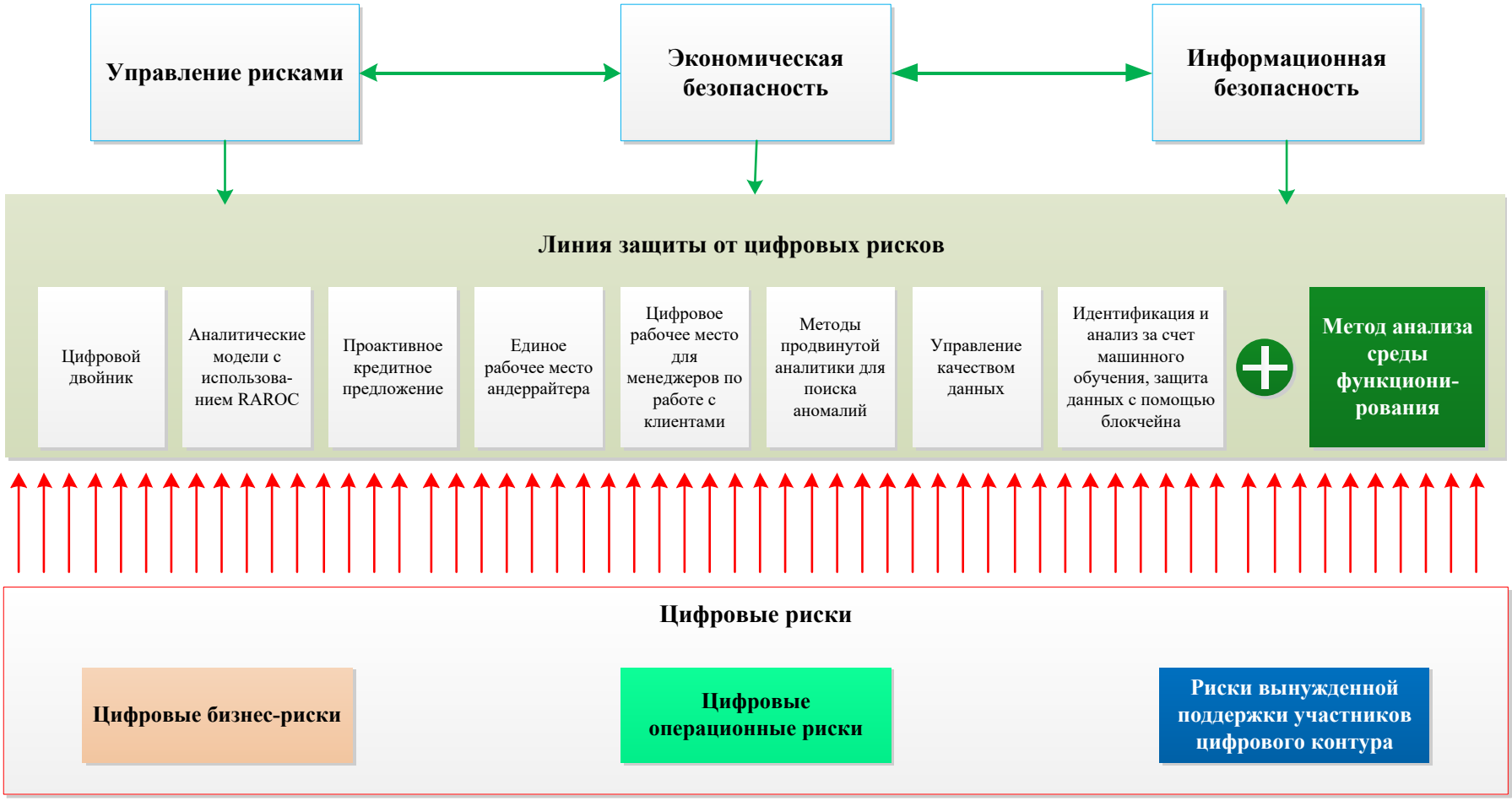
– предложен трехступенчатый алгоритм управления цифровыми рисками в организации, включающий в себя определение приоритетных инициатив по управлению рисками, выбор соответствующих инициативам цифровых решений, а также подход к внедрению данных решений с учетом концепции «управления изменениями»;

– предложен авторский подход к организации процесса проведения мероприятий по митигации цифровых рисков: рассмотрены понятия *«контрольных процедур»* и *«мероприятий»*, направленных на митигацию цифровых рисков; сформулированы основания для осуществления, а также приведены примеры данных мероприятий; представлены *порядок работы* с мероприятиями по митигации цифровых рисков, *функционал участников* данного процесса, а также *жизненный цикл* осуществления мероприятий;

– предложены меры, направленные на митигацию цифровых рисков, а также инструменты осуществления данных мер, формирующие *цифровую линию защиты* организации от цифровых рисков;

– сформирован *«куб безопасности»*, отражающий объекты обеспечения безопасности, риски, которым данные объекты подвержены, а также инструменты, с помощью которых следует управлять данными рисками, внедренный автором работы в деятельность Финансового департамента одной из крупнейших кредитных организаций России – «Банк ВТБ» (ПАО).

Развитие системы управления рисками цифровизации бизнес-процессов при обеспечении экономической безопасности организации заключается в выделении категории «цифровых» рисков, определении их видов и взаимосвязи с бизнес-процессами, предложении мероприятий и инструментов по борьбе с данной категорией рисков с использованием метода анализа среды функционирования в контексте сформулированной взаимозависимости экономической безопасности, информационной безопасности и управления рисками, что наглядно продемонстрировано на рисунке 36.



Источник: составлено автором.

Рисунок 36 – Развитие системы управления рисками цифровизации бизнес-процессов при обеспечении экономической безопасности

Заключение

Итогом проведенного исследования является достижение обозначенной цели по формированию теоретико-методических положений по развитию системы управления рисками цифровизации бизнес-процессов при обеспечении экономической безопасности организации, а также разработке практических рекомендаций по оценке и митигации данных рисков.

Решены поставленные задачи, а именно: исследован теоретический аспект взаимосвязи между экономической безопасностью и управлением рисками организации в условиях цифровизации, определены направления реагирования организации на опасности и угрозы, возникающие в связи с цифровизацией бизнес-процессов; выявлены особенности регулирования бизнес-процессов кредитной организации в рамках их протекания в цифровом пространстве, определена взаимосвязь между рисками, связанными с цифровизацией, и бизнес-процессами кредитной организации; уточнен понятийно-категориальный аппарат риска, связанного с цифровизацией, осуществлена идентификация и классификация рисков данного вида, а также определены причины их возникновения; разработаны методические рекомендации по оценке и минимизации рисков, связанных с цифровизацией бизнес-процессов организации; предложены практические рекомендации, направленные на минимизацию рисков, связанных с цифровизацией, а также на обеспечение экономической безопасности кредитной организации.

Определена основополагающая взаимозависимость экономической безопасности, управления рисками и информационной безопасности в контексте функционирования организации в цифровом контуре с выделением информационной безопасности как ключевого элемента при обеспечении экономической безопасности организации. Также выявлена необходимость совершенствования традиционных подходов к управлению рисками в кредитной организации, связанная с низкой адаптивностью текущих подходов к современным условиям повсеместного внедрения и использования новых

технологий как кредитными организациями, так и остальными субъектами экономики, а также недостаточной проработанностью проблемы управления рисками цифровизации бизнес-процессов при обеспечении экономической безопасности организации в научной литературе. Сформулированы особенности регулирования и управления риском аутсорсинга.

По итогам изучения вопросов, связанных с осуществлением трансформации бизнес-моделей организаций, а также исследования существующих методологических аспектов оценки рисков организаций в условиях цифровизации: введено понятие цифрового риска как вероятности недостижения (частичного достижения) установленных целей организации при использовании организацией передовых цифровых технологий; введено понятие митигации цифрового риска как скоординированной корректировки аналитики, данных, передовых цифровых технологий и бизнес-процессов, направленных на реализацию установленных целей организации (доведение отклонений до допустимого уровня); определены внешние и внутренние причины возникновения цифровых рисков; выделены и описаны виды цифровых рисков, а именно цифровые бизнес-риски, цифровые операционные риски и риски вынужденной поддержки участников цифрового контура; определены бизнес-процессы современной кредитной организации с выделением бизнес-процессов, наиболее подверженных рискам, связанным с цифровизацией, а также установлен уровень влияния каждого из видов цифровых рисков на данные бизнес-процессы; классифицированы методы оценки цифровых рисков применительно к каждому из видов цифрового риска; составлен развернутый алгоритм оценки цифровых рисков.

В рамках определения современных подходов к митигации цифровых рисков организации при обеспечении экономической безопасности, а также по итогам формирования методических рекомендаций по митигации данных рисков с целью развития системы управления рисками организации: сформулированы и обоснованы направления использования математико-экономического метода анализа среды функционирования для

проведения оценки влияния цифровых рисков на кредитную организацию и определения уровня обеспечения экономической безопасности организации на основе финансовых показателей ее деятельности, а также для определения уровня обеспечения кибербезопасности организации на основе значений ключевых показателей, которые позволяет определить данный метод, а именно коэффициента эффективности организации относительно конкурентов, оптимальных и потенциально достижимых показателей деятельности по обеспечению кибербезопасности, показателей количества ресурсов, требуемых для достижения цели по достаточности обеспечения кибербезопасности с определением групп аналогов – организаций, обладающих высоким уровнем кибербезопасности, являющихся ориентиром для исследуемой организации; предложен алгоритм управления цифровыми рисками в организации, состоящий из этапов по определению приоритетных инициатив, поиску цифровых решений и их внедрению с учетом концепции «управления изменениями»; сформулирован подход к организационной составляющей процесса по митигации цифровых рисков – рассмотрена сущность мероприятий по митигации, предложены порядок работы с данными мероприятиями, определены функционал участников процесса, а также его жизненный цикл; предложена цифровая линия защиты кредитной организации, состоящая из мер по митигации цифровых рисков, а также инструментов их осуществления, а именно идентификации и анализа за счет технологии машинного обучения, технологии цифрового двойника, концепции «управления качеством» данных, цифрового рабочего места для менеджеров по работе с клиентами, промышленного подхода к управлению цифровыми операционными рисками, единого рабочего места андеррайтера, концепции проактивного кредитного предложения и использования показателя скорректированной риском доходности на капитал в современных аналитических методах оценки рисков.

Практическая ценность предложенных в работе методов, мероприятий и современных инструментов управления рисками при обеспечении

экономической безопасности в организациях обусловлена их апробацией в системно значимой российской кредитной организации «Банк ВТБ» (ПАО).

Для достижения масштабных целевых амбиций организации, стремящейся к максимизации результатов деятельности по любым направлениям (в случае кредитных организаций данное стремление обусловлено высококонкурентной банковской средой), может потребоваться полная цифровая трансформация, которая потребует создания новых сквозных процессов между всеми блоками организации (подразделениями малого и среднего бизнеса, подразделениями розничного бизнеса, подразделениями корпоративно-инвестиционного бизнеса, подразделениями поддержки и контроля и топ-менеджментом), а также тесного сотрудничества между подразделениями по управлению рисками, операционными подразделениями и клиентами. Организациям, которые решатся на проведение трансформации, следует расставить соответствующие приоритеты – ориентироваться на области бизнеса и модернизации операционных процессов, где цифровизация потенциально может принести максимальную выгоду за разумный промежуток времени с учетом специфики соответствующих цифровых рисков и необходимости проработки подходов к обеспечению экономической безопасности в условиях глобальных изменений. Данный вопрос может быть рассмотрен в ходе дальнейшего изучения и развития темы текущего диссертационного исследования.

Словарь терминов

Базельский комитет по банковскому надзору: «Основной мировой разработчик стандартов пруденциального регулирования банков и форум для регулярного сотрудничества по вопросам банковского надзора» [176].

блокчейн: «Технология, организующая базу данных, состоящую из цепочки блоков, оформленных по определенным правилам. Каждая ячейка блока несет в себе информацию о предыдущей ячейке. Эта технология базируется на принципе децентрализации, то есть база находится не в одном месте, а во всех компьютерах участников системы, которые образуют сеть. Таким образом блоки не могут быть заменены или взломаны, так как для этого придется взломать все компьютеры» [61].

большие данные (или Big Data): «Структурированные или неструктурированные массивы данных большого объема. Их обрабатывают при помощи специальных автоматизированных инструментов, чтобы использовать для статистики, анализа, прогнозов и принятия решений» [60].

интернет вещей: Система, которая объединяет устройства в компьютерную сеть и позволяет им собирать, анализировать, обрабатывать и передавать данные другим объектам через программное обеспечение, приложения или технические устройства.

искусственный интеллект (ИИ): «Технология, которая имитирует человеческое поведение, чтобы выполнять задачи и постепенно обучаться, используя собираемую информацию» [198].

машинное обучение: «Один из подразделов науки, посвященной разработке и изучению искусственного интеллекта. Он фокусируется на создании систем автоматизации, которые обучаются посредством обработки данных. Такие системы используются для ускорения принятия решений и сокращения сроков окупаемости» [198].

цифровые аборигены (от англ. digital natives): «Отдельная и заметная группа молодых людей, которые рождены в цифровую эпоху и взрослеют,

используя информационно-коммуникационные технологии в своей повседневной жизни» [92].

Список литературы

Книги

1. Авдийский, В.И. Риски хозяйствующих субъектов: теоретические основы, методология анализа, прогнозирования и управления : учебное пособие / В.И. Авдийский, В.М. Безденежных. – Москва : АльфаМ : ИНФРА-М, 2018. – 368 с. – ISBN 978-5-16-006493-2.

2. Аминов, Х.И. Преимущества внедрения кредитного конвейера для малого и среднего бизнеса в коммерческих банках / Х.И. Аминов, П.С. Соловей // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. – Санкт-Петербург : Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. – С. 228-229. – ISBN 978-5-00182-047-5.

3. Банковское дело в 2 частях. Часть 1 : учебник / Н.Н. Мартыненко, О.М. Маркова, Н.В. Сергеева [и др.]. – Москва : Издательство Юрайт, 2019. – 217 с. – ISBN 978-5-534-08398-9.

4. Квинт, В.Л. Стратегирование трансформации общества: знание, технологии, ноономика : монография / В.Л. Квинт, С.Д. Бодрунов. – Санкт-Петербург : Ассоциация «Некоммерческое партнерство по содействию в проведении научных исследований «Институт нового индустриального развития им. С.Ю. Витте», 2021. – 351 с. – 1000 экз. – ISBN 978-5-00020-083-4.

5. Конягина, М.Н. Управление кредитным риском как элемент системы корпоративного управления коммерческого банка / М.Н. Конягина // Россия и Санкт-Петербург: экономика и образование в XXI веке : XXXVIII научная конференция профессорско-преподавательского состава, научных сотрудников и аспирантов по итогам научно-исследовательской деятельности

университета за 2015 год. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2017. – С. 96-100. – ISBN 978-5-7310-3807-2.

6. Одинцов, В.О. Развитие коммерческих банков в условиях цифровой трансформации экономики / В.О. Одинцов // Современные формы устойчивого развития социально-экономических систем : сборник научных трудов по материалам научно-практического семинара ; под редакцией В.В. Борисова [и др.]. – Москва : ГУУ, 2022. – С. 81-85. – 159 с. – ISBN 978-5-215-03520-7.

7. Одинцов, В.О. Современные инструменты обеспечения экономической безопасности коммерческого банка / В.О. Одинцов // Теоретические и прикладные вопросы экономики, управления и образования : сборник статей IV Международной научно-практической конференции ; под научной редакцией Б.Н. Герасимова. – Пенза : Пензенский государственный аграрный университет, 2023. – С. 267-271. – 467 с. – ISBN 978-5-00196-168-0. – Текст : электронный. – DOI отсутствует. – URL: https://www.elibrary.ru/download/elibrary_54273641_18917825.pdf (дата обращения: 12.07.2024).

8. Одинцов, В.О. Тенденции управления рисками и обеспечения экономической безопасности кредитных организаций / В.О. Одинцов // Анализ социально-экономического состояния и перспектив развития Российской Федерации : материалы 9-й Международной студенческой научно-практической конференции ; под редакцией С.Б. Чернова. – Москва : ГУУ, 2023. – С. 322-326. – 369 с. – ISBN 978-5-215-03711-9.

9. Одинцов, В.О. Управление рисками в коммерческих банках России в условиях цифровизации банковского сектора / В.О. Одинцов // Проблемы управления, экономики и права в общегосударственном и региональном масштабах : сборник статей X Всероссийской научно-практической конференции ; под редакцией О.А. Столяровой, Р.Р. Юняевой. – Пенза : Пензенский государственный аграрный университет,

2023. – С. 166-170. – 267 с. – ISBN 978-5-00196-184-0. – Текст : электронный. – DOI отсутствует. – URL: https://www.elibrary.ru/download/elibrary_54790052_26370675.pdf (дата обращения: 12.07.2024).

10. Одинцов, В.О. Управление рисками в современных кредитных организациях / В.О. Одинцов // Стратегия устойчивого развития и экономическая безопасность страны, региона, хозяйствующих субъектов : материалы XVIII Международной научно-практической конференции молодых ученых, студентов и магистрантов, посвященной памяти выдающегося экономиста В.Д. Новодворского ; под редакцией М.М. Богдановой, П.А. Косенковой. – Москва : Издательство «Перо», 2023. – С. 378-383. – 449 с. – ISBN 978-5-00244-114-3. – DOI отсутствует. – URL: https://elibrary.ru/download/elibrary_63493692_73952462.pdf (дата обращения: 12.07.2024).

11. Пеганова, О.М. Банковское дело : учебник / О.М. Пеганова. – Москва : Издательство Юрайт, 2023. – 538 с. – ISBN 978-5-534-18112-8.

12. Помазанов, М.В. Управление кредитным риском в банке: подход внутренних рейтингов (ПВР) : учебное пособие / М.В. Помазанов, Г.И. Пеникас. – Москва : Издательство Юрайт, 2024. – 292 с. — ISBN 978-5-534-17892-0.

13. Рзун, И.Г. Дашборд как эффективный инструмент бизнес-аналитики для финансовых показателей компании / И.Г. Рзун // Актуальные проблемы и перспективы развития экономики : труды XXI Международной научно-практической конференции. – Симферополь : Крымский федеральный университет им. В.И. Вернадского, 2022. – С. 72-76. – ISBN 978-5-6047625-5-4.

14. Щаникова, К.Е. Исследование методов и инструментов автоматизации процесса принятия решения по размещению активов банка на примере методики RAROC / К.Е. Щаникова // Альманах научных работ молодых ученых Университета ИТМО : материалы Пятьдесят первой (LI)

научной и учебно-методической конференции Университета ИТМО. – Санкт-Петербург : Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО», 2022. – С. 252-256. – ISBN 978-5-7577-0673-3.

Нормативные правовые акты

15. Российская Федерация. Законы. О банках и банковской деятельности : федеральный закон [принят Государственной Думой 02 декабря 1990 года № 395-1]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 10.09.2023).

16. Об утверждении Доктрины информационной безопасности Российской Федерации [Указ Президента Российской Федерации от 05 декабря 2016 года № 646]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 12.10.2023).

17. О Стратегии экономической безопасности Российской Федерации на период до 2030 года [Указ Президента Российской Федерации от 13 мая 2017 года № 208]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_216629/ (дата обращения: 12.10.2023).

18. О порядке расчета размера операционного риска («Базель III») и осуществления Банком России надзора за его соблюдением [Положение Банка России от 07 декабря 2020 года № 744-П (редакция от 10.01.2023)]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. –

URL: https://www.consultant.ru/document/cons_doc_LAW_375817/ (дата обращения: 15.11.2023).

19. О порядке расчета размера операционного риска [Положение Банка России от 03 сентября 2018 года № 652-П (редакция от 15.11.2023)]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_311859/ (дата обращения: 15.11.2023).

20. О требованиях к системе управления операционным риском в кредитной организации и банковской группе [Положение Банка России от 08 апреля 2020 года № 716-П (редакция от 25.03.2022)]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_355380/ (дата обращения: 15.11.2023).

21. О порядке получения разрешения на применение банковских методик управления кредитным риском и моделей количественной оценки кредитного риска, а также порядке оценки их качества [Указание Банка России от 13 июня 2023 года № 6445-У]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_462310/ (дата обращения: 14.12.2023).

22. Об обязательных нормативах и надбавках к нормативам достаточности капитала банков с универсальной лицензией [Инструкция Банка России от 29 ноября 2019 года № 199-И (редакция от 06.06.2023)]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_342089/ (дата обращения: 15.11.2023).

Стандарты

23. ГОСТ Р 51897–2021/Руководство ИСО 73:2009. Менеджмент риска. Термины и определения = Risk management. Terms and definitions: национальный стандарт Российской Федерации: издание официальное: утвержден и веден в действие Приказом Федерального агентства по техническому регулированию и метрологии от 11 ноября 2021 г. № 1489-ст : взамен ГОСТ Р 51897-2011 / Руководство ИСО 73:2009 : дата введения 2022-03-01 / разработан – ассоциацией риск-менеджмента «Русское Общество Управления Рисками» (АРМ «РусРиск») — Москва : Российский институт стандартизации, 2021.

24. ISO/IEC 27000:2018 – все права защищены. Международный Стандарт ISO/IEC 27000. Пятая редакция 2018-02. Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь. – Текст : электронный. - URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2018.pdf (дата обращения: 18.07.2023).

Диссертации

25. Мамедов, М.А. Деятельность коммерческих банков в условиях формирования экосистем в Российской Федерации : специальность 5.2.4 «Финансы» : диссертация на соискание ученой степени кандидата экономических наук / Мамедов Мурад Азер оглы ; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации. – Москва, 2023. – 205 с. – Библиогр.: с. 74-95.

Электронные ресурсы

26. Актуальное: PayPal и Samsung приостановили работу в РФ, в торговых сетях вводят ограничения на продажу товаров / Банки.ру : официальный сайт российской финансовой платформы онлайн-сервисов. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.banki.ru/news/daytheme/?id=10962261 (дата обращения: 22.04.2024).

27. Аналитика мобильных приложений: показатели эффективности и сервисы аналитики / Sendpluse.com : официальный сайт многоканальной маркетинговой платформы. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://sendpulse.com/ru/blog/mobile-app-effectivity (дата обращения: 22.04.2024).

28. Банк ВТБ – отчетность / BankoDrom.ru: аналитический портал. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.bankodrom.ru/bank/vtb/otchetnost/ (дата обращения: 23.01.2023).

29. Вестник Банка России № 63: нормативные акты и оперативная информация / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/Queries/XsltBlock/File/131643/-1/2395 (дата обращения: 21.01.2023).

30. В России утвержден первый национальный стандарт в области больших данных / Ведомости : официальный сайт российской ежедневной деловой газеты. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.vedomosti.ru/technology/articles/2021/07/15/878242-utverzhden-pervii-standart-v-oblasti-bolshih-dannih (дата обращения: 22.04.2024).

31. Диасофт: путь перемен, «осознанный Agile» и культура согласия / Компания «Диасофт» : официальный сайт российского поставщика программного обеспечения для банков. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.diasoft.ru/about/publications/19963/ (дата обращения: 22.04.2024).

32. Доклад для общественных консультаций «Регулирование рисков участия банков в экосистемах и вложений в иммобилизованные активы. Июнь 2021 года» / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/Content/Document/File/123688/Consultation_Paper_23062021.pdf (дата обращения: 25.03.2022).

33. Информационно – аналитический материал «Обзор финансовой стабильности. II – III кварталы 2022 года» / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/Collection/Collection/File/43512/2q_3q_2022.pdf (дата обращения: 21.01.2023).

34. Исследование приложений мобильного банкинга в России. – Текст : электронный. – DOI отсутствует. – URL: https://media.rbcdn.ru/media/reports/go_banki.pdf (дата обращения: 18.08.2023).

35. Карман не тянут: возможен ли в России отказ от наличных / Известия : официальный сайт российской деловой газеты. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://iz.ru/1556521/oksana-belkina/karman-ne-tianut-vozmozhen-li-v-rossii-otkaz-ot-nalichnykh (дата обращения: 22.04.2024).

36. Количественные характеристики банковского сектора Российской Федерации / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/statistics/bank_sector/lic/ (дата обращения: 13.09.2022).

37. Мошенничество с банковскими картами и платежами / TAdviser.ru : российский интернет-портал и аналитическое агентство. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Статья:Мошенничество_с_банковскими_картами_и_платежами (дата обращения: 22.04.2024).

38. Обзор операций, совершенных без согласия клиентов финансовых организаций: 2020 и 2021 годы / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/analytics/ib/operations_survey/2021/ (дата обращения: 16.09.2022).

39. Обзор операций, совершенных без согласия клиентов финансовых организаций: 2021 и 2022 годы / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 16.09.2022).

40. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: I и II кварталы 2019/2020 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_1q_2q_2020/ (дата обращения: 16.09.2022).

41. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: I квартал 2021 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_1q_2021/ (дата обращения: 16.09.2022).

42. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: I квартал 2022 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_4q_2022/ (дата обращения: 16.09.2022).

43. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: II квартал 2021 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_2q_2021/ (дата обращения: 16.09.2022).

44. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: II квартал 2022 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_2q_2022/ (дата обращения: 16.09.2022).

45. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: III квартал 2019/2020 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_3q_2020/ (дата обращения: 16.09.2022).

46. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: III квартал 2021 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_3q_2021/ (дата обращения: 16.09.2022).

47. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: III квартал 2022 года / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/statistics/ib/review_3q_2022/ (дата обращения: 16.09.2022).

48. Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2023 год и на плановый период 2024 и 2025 годов / Министерство финансов Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://minfin.gov.ru/common/upload/library/2022/11/main/2023-2025.pdf (дата обращения: 23.03.2024).

49. Отчет «Кибератаки на российские компании в 2022 году». – Текст : электронный. – DOI отсутствует. – URL: https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-

kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf (дата обращения: 19.08.2023).

50. Переход на Базель III в управлении операционным риском: опыт ВТБ / TAdviser.ru : российский интернет-портал и аналитическое агентство. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.reglament.net/bank/r/2021_2/get_article.htm?id=7145 (дата обращения: 22.04.2024).

51. Перспективные направления развития банковского регулирования и надзора / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/content/document/file/143838/dbra_20221227.pdf (дата обращения: 21.10.2022).

52. Платформа «Знай своего клиента» / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/counteraction_m_ter/platform_zsk/ (дата обращения: 21.02.2023).

53. Политика управления рисками Банка России / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://cbr.ru/content/document/file/36486/policy.pdf (дата обращения: 21.09.2022).

54. Сбербанк – отчетность / BankoDrom.ru: аналитический портал. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.bankodrom.ru/bank/sberbank/otchetnost/ (дата обращения: 23.01.2023).

55. Социально-экономическое положение России. Январь-сентябрь 2022 года / Федеральная служба государственной статистики : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://rosstat.gov.ru/storage/mediabank/soc_pol_RF_2022.rar (дата обращения: 13.09.2022).

56. Статистические показатели банковского сектора Российской Федерации / Центральный банк Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.cbr.ru/collection/collection/file/45113/obs_247.xlsx (дата обращения: 14.01.2023).

57. Стратегии бизнеса : Аналитический справочник / Kleiner.ru : официальный сайт советского и российского экономиста Георгия Борисовича Клейнера. – Москва. – Текст : электронный. – URL: https://kleiner.ru/wp-content/uploads/2014/10/str-biz.pdf (дата обращения: 14.04.2022).

58. Тинькофф Банк – отчетность / BankoDrom.ru: аналитический портал. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.bankodrom.ru/bank/tinkoff-bank/otchetnost/ (дата обращения: 23.01.2023).

59. Цифровая трансформация: определения, роли, дорожная карта. – Текст : электронный. – DOI отсутствует. – URL: http://cloud-digital.ru/sites/default/files/12.30-13.30_cdo_partners_kutuzov.pdf (дата обращения: 18.08.2023).

60. Что такое Big Data и почему их называют «новой нефтью» / РБК : деловой портал. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://trends.rbc.ru/trends/innovation/5d6c020b9a7947a740fea65c (дата обращения: 22.04.2024).

61. Что такое блокчейн? / РБК : деловой портал. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.rbc.ru/crypto/news/5a1691c39a79478ac778e13b (дата обращения: 22.04.2024).

62. Эксперты предсказали дефицит специалистов по кибербезопасности в России / Forbes : официальный сайт финансово-экономического журнала. – Москва. – Обновляется в течение

суток. – Текст : электронный. – URL: https://www.forbes.ru/tekhnologii/465619-eksperty-predskazali-deficit-specialistov-po-kiberbezopasnosti-v-rossii (дата обращения: 22.04.2024).

63. Электронные платежные системы в России / TAdviser.ru : российский интернет-портал и аналитическое агентство. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://www.tadviser.ru/index.php/Статья:Электронные_платежные_системы_в_России (дата обращения: 22.04.2024).

64. Deloitte оценила уровень цифровизации банков / Deloitte : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – URL: https://frankmedia.ru/25912 (дата обращения: 22.04.2024).

Статьи

65. Авдийский, В.И. Совершенствование механизма борьбы в сфере ПОД/ФТ, незаконного вывоза капитала в целях обеспечения национальной и экономической безопасности России / В.И. Авдийский // Экономические науки. – 2022. – № 212. – С. 35-41. – ISSN 2072-0858.

66. Автушенко, О.М. Оценка экономической безопасности коммерческого банка: сравнительный анализ подходов и вопросы совершенствования / О.М. Автушенко, Н.А. Кулагина, О.С. Надежина // Вестник Алтайской академии экономики и права. – 2020. – № 12-3. – С. 457-462. – ISSN 1818-4057.

67. Азаркова, А.А. Проблемы информационной безопасности финансовых систем / А.А. Азаркова // Вестник Академии знаний. – 2023. – № 2 (55). – С. 292-294. – ISSN 2304-6139.

68. Акопян, А.О. Мониторинг банковских рисков при обеспечении финансовой безопасности РФ / А.О. Акопян, О.Н. Афанасьева // Столыпинский вестник. – 2022. – № 2. Том 4. – ISSN 2713-1424. – Текст : электронный. – DOI 10.55186/27131424_2022_4_2_13. – URL:

https://cyberleninka.ru/article/n/monitoring-bankovskih-riskov-pri-obespechenii-finansovoy-bezopasnosti-rf (дата обращения: 11.04.2024).

69. Акопян, А.О. Система минимизации банковских рисков в процессе обеспечения финансовой безопасности страны / А.О. Акопян // Вектор экономики. – 2022. – № 3 (69). – ISSN 2500-3666. – Текст : электронный. – DOI 10.51691/2500-3666_2022_3_11. – URL: http://www.vectoreconomy.ru/images/publications/2022/3/financeandcredit/Akopyan.pdf (дата обращения: 11.04.2024).

70. Алексеева, Н.В. Киберпреступления в банковской сфере России: аналитика и методы противодействия / Н.В. Алексеева, А.С. Дуракова, Д.В. Горденко [и др.] // Вестник Института дружбы народов Кавказа (Теория экономики и управления народным хозяйством). Экономические науки. – 2023. – № 1 (65). – С. 54-64. – ISSN 2071-3819.

71. Алешина, А.В. Воздействие финансовых технологий и децентрализованных финансов (DeFi) на угрозы инфраструктуре национальной экономики / А.В. Алешина, А.Л. Булгаков // Финансовые рынки и банки. – 2023. – № 1. – С. 121-125. – ISSN 2658-3917.

72. Алферов, В.Н. Управление рисками как инструмент обеспечения устойчивости кредитной организации / В.Н. Алферов, К.И. Тутова // Проблемы современной экономики. – 2018. – № 4 (68). – С. 143-146. – ISSN 1818-3395.

73. Андрущук, В.В. Финансовая безопасность российских банков в условиях санкций / В.В. Андрущук // Экономика и предпринимательство. – 2022. – № 9 (146). – С. 1183-1185. – ISSN 1999-2300.

74. Аренков, И.А. Цифровая трансформация: направления исследований и цифровые риски / И.А. Аренков, Я.Ю. Салихова, А.А. Сайфутдинов // Креативная экономика. – 2021. – № 7. Том 15. – С. 2757-2776. – ISSN 1994-6929.

75. Афанасьева, Л.В. Изучение опыта применения цифровых технологий в финансовой сфере в целях обеспечения экономической

безопасности в России и за рубежом / Л.В. Афанасьева, А.Б. Евлоева // Национальная безопасность / Nota Bene. – 2023. – № 2. – С. 36-47. – ISSN 2073-8560.

76. Бабукин, Г.М. Цифровизация и искусственный интеллект в банках: шаг в будущее / Г.М. Бабукин // Chronos: экономические науки. – 2021. – № 1 (29). Том 6. – С. 6-9. – ISSN 2712-9713.

77. Бажанова, Д.Н. Трансформация бизнес-моделей коммерческих банков в условиях цифровизации / Д.Н. Бажанова, О.М. Маркова // Финансовая экономика. – 2022. – № 2. – С. 178-182. – ISSN 2075-7786.

78. Безденежных, В.М. Оценка зрелости систем управления рисками организаций / В.М. Безденежных // Экономика и управление: проблемы, решения. – 2023. – № 1 (133). Том 1. – С. 81-88. – ISSN 2227-3891.

79. Безденежных, В.М. Проблемы развития управления сложными социально-экономическими системами с учетом риск-ориентированного подхода - пути преодоления мифов / В.М. Безденежных // Экономическая безопасность. – 2022. – № 3. Том 5. – С. 819-834. – ISSN 2658-7548.

80. Безденежных, В.М. Формирование научной школы Департамента Экономической безопасности и управления рисками Финансового университета при Правительстве Российской Федерации / В.М. Безденежных // Экономика и управление: проблемы, решения. – 2023. – № 12 (141). Том 5. – С. 57-63. – ISSN 2227-3891.

81. Беляев, М.К. Большие базы данных как ресурс банка будущего / М.К. Беляев, А.Д. Ерохова // Банковское дело. – 2019. – № 5. – С. 44-47. – ISSN 2071-4904.

82. Бикметова, З.М. Обеспечение экономической безопасности кредитной организации / З.М. Бикметова // Инновационное развитие экономики. – 2019. – № 4-2 (52). – С. 30-42. – ISSN 2223-7984.

83. Бирюков, А.Н. Методики анализа финансовой устойчивости банка в оценке экономической стабильности / А.Н. Бирюков // Научное обозрение: теория и практика. – 2023. – № 2 (96). Том 13. – С. 226-244. – ISSN 2226-0226.

84. Боброва, Е.А. Портфельная теория Марковица в условиях современности / Е.А. Боброва, Л.В. Мазур, В.В. Малащенко // Экономическая среда. – 2021. – № 2 (36). – С. 78-83. – ISSN 2306-1758.

85. Болотнова, Е.А. Экосистемы в банковской системе РФ: проблемы и перспективы / Е.А. Болотнова, А.А. Храмченко, Т.В. Журавлева [и др.] // Естественно-гуманитарные исследования. – 2022. – № 39 (1). – С. 75-82. – ISSN 2309-4788.

86. Бричка, Е.И. Роль коммерческих банков в системе финансовой безопасности государства / Е.И. Бричка, Ю.С. Жаркова, Е.С. Захарченко // Финансовые исследования. – 2023. – № 3 (80). Том 24. – С. 23-34. – ISSN 1991-0525.

87. Бубнова, Ю.Б. Трансформация бизнес-модели банка в условиях цифровой экономики / Ю.Б. Бубнова // Известия Байкальского государственного университета. – 2019. – № 3. Том 29. – С. 425-433. – ISSN 2500-2759.

88. Булатов, А.Е. Методологические подходы к управлению предпринимательскими рисками / А.Е. Булатов, П.А. Фомин // Инженерный вестник Дона. – 2015. – № 2-2 (36). – С. 43. – ISSN 2073-8633. – Текст : электронный. – DOI отсутствует. – URL: https://cyberleninka.ru/article/n/metodologicheskie-podhody-k-upravleniyu-predprinimatelskimi-riskami (дата обращения: 11.04.2024).

89. Васильева, М.В. Теоретические характеристики экономической безопасности коммерческого банка / М.В. Васильева // Экономические и гуманитарные науки. – 2022. – № 11 (370). – С. 64-73. – ISSN 2073-7424.

90. Воробьева, Е.И. Направления развития банковской деятельности в Российской Федерации / Е.И. Воробьева // Научный вестник: финансы, банки, инвестиции. – 2022. – № 2 (59). – С. 62-70. – ISSN отсутствует.

91. Григорьева, К.В. Совершенствование методики анализа финансовой устойчивости банка в целях повышения экономической

безопасности / К.В. Григорьева // Национальная безопасность / Nota Bene. – 2022. – № 3. – С. 7-13. – ISSN 2073-8560.

92. Дегтярев, А.В. Работа в «облаке» как трансформация социально-трудовых отношений в цифровой экономике / А.В. Дегтярев // Креативная экономика. – 2017. – № 2. Том 11. – С. 241-248. – ISSN 1994-6929.

93. Дорохова, М.В. Подходы к регулированию рисков экономической безопасности государства, возникающие в результате распространения цифровых экосистем / М.В. Дорохова // Экономическая безопасность. – 2022. – № 2. Том 5. – С. 695-710. – ISSN 2658-7548.

94. Дрозд, О.В. Система управления рисками в банках / О.В. Дрозд, К. Кирилюк // Инновации. Наука. Образование. – 2022. – № 51. – С. 1768-1776. – ISSN отсутствует.

95. Ештокин, С.В. Российский финтех в национальной финансовой системе: защитник интересов или скрытая угроза? / С.В. Ештокин // Экономика, предпринимательство и право. – 2021. – № 8. Том 11. – С. 1915-1944. – ISSN 2222-534X. – Текст : электронный. – DOI 10.18334/epp.11.8.112709. – URL: https://1economic.ru/lib/112709 (дата обращения: 11.04.2024).

96. Запорожская, К.А. Мероприятия по обеспечению экономической безопасности коммерческого банка / К.А. Запорожская // Научный альманах Центрального Черноземья. – 2022. – № 1-3. – С. 97-100. – ISSN 2313-5581.

97. Зверев, А.В. Влияние цифровизации банковской деятельности на процесс формирования прибыли коммерческого банка / А.В. Зверев, А.В. Новиков, М.Ю. Мишина // Управленческий учет. – 2022. – № 5-1. – С. 41-47. – ISSN 1814-8476.

98. Земсков, В.В. Особенности регулирования рисков информационного обмена в системе внутреннего контроля / В.В. Земсков // Аудитор. – 2020. – № 10. Том 6. – С. 33-37. – ISSN 1998-0701.

99. Илюхина, Л.А. Кадровая безопасность в системе управления персоналом / Л.А. Илюхина, И.В. Богатырева // Экономика и предпринимательство. – 2022. – № 8 (145). – С. 1134-1138. – ISSN 1999-2300.

100. Исаева, Е.А. Актуальные вопросы цифровизации кредитных операций банка в современных условиях / Е.А. Исаева, Т.Н. Резвякова // Проблемы теории и практики управления. – 2022. – № 5-6. – С. 39-52. – ISSN 0234-4505.

101. Капишонова, В.С. Факторный анализ рисков в единой корпоративной автоматизированной система управления инфраструктурой / В.С. Капишонова, Т.Н. Асалханова // Молодая наука Сибири. – 2022. – № 1 (15). – С. 35-42. – ISSN отсутствует.

102. Каприян, Ю.В. Корреляция комплаенс и внутреннего контроля на уровне коммерческих и кредитных учреждений / Ю.В. Каприян, И.В. Толмачева // Теория и практика общественного развития. – 2021. – № 7 (161). – С. 68-72. – ISSN 1815-4964.

103. Карасов, А.И. Исследование методических основ процесса функционирования банковского надзора и контроля / А.И. Карасов // Отходы и ресурсы. – 2023. – № 1. Том 10. – ISSN 2500-0659.

104. Карпова, Е.Н. Новые риски отмывания денег и финансирования терроризма в условиях цифровизации экономики / Е.Н. Карпова, Е.А. Чумаченко, А.А. Коновалов // Управленческий учет. – 2022. – № 3-2. – С. 271-278. – ISSN 1814-8476.

105. Касюк, Е.А. Новые тенденции управления и контроля операционного риска в финансовых институтах / Е.А. Касюк // Вестник Сибирского института бизнеса и информационных технологий. – 2023. – № 1. Том 12. – С. 71-78. – ISSN 2225-8264.

106. Киюцевская, А.М. Финтех: современные тенденции и вызовы для денежно-кредитной политики / А.М. Киюцевская // Вопросы экономики. – 2019. – № 4. – С. 137-151. – ISSN 0042-8736.

107. Козленко, Э.И. Банк в смартфоне: финансовые сервисы в эпоху цифровизации / Э.И. Козленко, О.С. Зиниша, А.А. Мкртумян // Инновации. Наука. Образование. – 2022. – № 50. – С. 685-692. – ISSN отсутствует.

108. Кравцов, В.В. Риски как производная финансовой устойчивости банковской системы / В.В. Кравцов // Вестник Московского финансово-юридического университета МФЮА. – 2020. – № 4. – С. 40-44. – ISSN 2224-669X.

109. Кряжков, А.С. Анализ действующей системы внутреннего аудита и формирование рекомендаций по ее усовершенствованию на примере ПАО Банк «ФК Открытие» / А.С. Кряжков // Вестник евразийской науки. – 2023. – № S1. Том 15. – ISSN 2588-0101. – Текст : электронный. – DOI отсутствует. – URL: https://esj.today/PDF/10FAVN123.pdf (дата обращения: 11.04.2024).

110. Кузовлева, Н.Ф. Цифровизация банковской сферы: тенденции развития и экономическая безопасность / Н.Ф. Кузовлева, Н.В. Тарасова // Экономика и управление: проблемы, решения. – 2021. – № 9 (117). Том 1. – С. 93-98. – ISSN 2227-3891.

111. Кулагина, Н.А. Актуальные аспекты методического подхода к оценке уровня экономической безопасности банка в условиях цифровизации / Н.А. Кулагина, О.М. Автушенко, О.С. Надежина // Вестник Алтайской академии экономики и права. – 2021. – № 1-1. – С. 66-71. – ISSN 1818-4057.

112. Кульбашевский, В.О. Степень развития банковской системы государства в контексте обеспечения национальной безопасности / В.О. Кульбашевский // Финансовая экономика. – 2023. – № 4. – С. 222-227. – ISSN 2075-7786.

113. Курникова, И.В. К вопросу об эффективности и устойчивости деятельности российских коммерческих банков / И.В. Курникова, Т.М. Маленкина, А.Н. Ольховец // Современные наукоемкие технологии. Региональное приложение. – 2023. – № 3 (75). – С. 20-25. – ISSN 2413-5399.

114. Лебедь, С.В. Инновационные технологии в сфере кибербезопасности / С.В. Лебедь // Современные информационные технологии и ИТ-образование. – 2022. – № 2. Том 18. – С. 383-390. – ISSN 2411-1473.

115. Литвяков, А.А. Оценка риска нарушения конфиденциальности информации с использованием лазерных систем разведки / А.А. Литвяков, И.Н. Карманов // Интерэкспо Гео-Сибирь. – 2023. – Том 6. – С. 153-159. – ISSN 2618-981X.

116. Лобанов, В.И. Цифровой инструментарий управления социально-экономической безопасностью на основе риск-ориентированного подхода / В.И. Лобанов, Е.В. Каранина // Экономика и управление: проблемы, решения. – 2022. – № 11 (131). Том 3. – С. 72-83. – ISSN 2227-3891.

117. Логвинова, И.В. Роль человеческого фактора в обеспечении экономической безопасности коммерческого банка в прогнозировании рисков / И.В. Логвинова // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2023. – № 10 (161). – С. 30-33. – ISSN 2219-0279.

118. Лыткин, А.Н. Цифровые двойники в банковской деятельности: проблемы и перспективы / А.Н. Лыткин // Экономика и управление. – 2023. – № 6. Том 29. – С. 718-729. – ISSN 1998-1627.

119. Мамедов, М.А. Трансформация деятельности крупнейших российских коммерческих банков в цифровые экосистемы / М.А. Мамедов // Теоретическая и прикладная экономика. – 2022. – № 3. – С. 1-23. – ISSN 2409-8647. – Текст : электронный. – DOI 10.25136/2409-8647.2022.3.38598. – URL: https://cyberleninka.ru/article/n/transformatsiya-deyatelnosti-krupneyshih-rossiyskih-kommercheskih-bankov-v-tsifrovye-ekosistemy (дата обращения: 11.04.2024).

120. Мамедова, Э.Ф. Аппетит к риску и безопасность банковских услуг в современной России / Э.Ф. Мамедова, И.А. Янкина // Бизнес. Образование. Право. – 2022. – № 2 (59). – С. 110-116. – ISSN 1990-536X.

121. Марамыгин, М.С. Цифровая трансформация российского рынка финансовых услуг: тенденции и особенности / М.С. Марамыгин, Г.В. Чернова, Л.Г. Решетникова // Управленец. – 2019. – № 3. Том 10. – С. 70-82. – ISSN 2218-5003.

122. Марков, А.Д. Эффективность систем управления рисками в банковской (кредитно-финансовой) сфере / А.Д. Марков // Вестник евразийской науки. – 2023. – № S1. Том 15. – ISSN 2588-0101. – Текст : электронный. – DOI отсутствует. – URL: https://esj.today/PDF/08FAVN123.pdf (дата обращения: 11.04.2024).

123. Маркова, О.М. Реализация операционного риска коммерческого банка в цифровой среде / О.М. Маркова // Финансовые рынки и банки. – 2020. – № 2. – С. 63-68. – ISSN 2658-3917.

124. Маркова, О.М. Трансформация деятельности банков в парадигме экосистем: риски и возможности финансовых технологий / О.М. Маркова // Банковские услуги. – 2023. – № 6. – С. 21-28. – ISSN 2075-1915.

125. Машков, Д.М. Научные подходы к управлению рисками промышленных предприятий / Д.М. Машков // Инженерный вестник Дона. – 2014. – № 4-1 (31). – С. 65. – eISSN 2073-8633.

126. Муковникова, А.И. Финансовые риски коммерческого банка как угроза его финансовой безопасности / А.И. Муковникова // Интернаука. – 2023. – № 22-4 (292). – С. 65-67. – ISSN 2687-0142.

127. Мустафин, Т.А. Риски инкорпорирования цифровой валюты в экономику страны / Т.А. Мустафин // Экономика и предпринимательство. – 2023. – № 7 (156). – С. 260-267. – ISSN 1999-2300.

128. Нафиков, Р.Г. Цифровизация банковской системы: риски и возможности управления финансовыми активами / Р.Г. Нафиков // Управленческие науки. – 2022. – № 3. Том 12. – С. 39-52. – ISSN 2304-022X.

129. Никитина, Т.В. Трансформация банковских стратегий в соответствии с методологией Agile в условиях глобальной неустойчивой

среды / Т.В. Никитина, М.А. Гальпер // Ученые записки Международного банковского института. – 2018. – № 2 (24). – С. 58-66. – ISSN 2413-3345.

130. Никулина, Н.Н. Андеррайтинг в банковском секторе / Н.Н. Никулина, С.В. Березина, М.Е. Шашкина // Вестник экономической безопасности. – 2017. – № 1. – С. 176-182. – ISSN 2414-3995.

131. Носова, Т.П. Классификация банковских рисков и мероприятия по их снижению с целью оптимизации банковской деятельности / Т.П. Носова, А.Б. Паршин, К.И. Терпицкая // Вестник Академии знаний. – 2022. – № 53 (6). – С. 349-353. – ISSN 2304-6139.

132. Одинцов, В.О. Анализ эффективности функционирования крупнейших банков России с использованием метода непараметрической оптимизации / В.О. Одинцов, Е.А. Вечкинзова // Друкеровский вестник. – 2021. – № 2. – С. 153-163. – ISSN 2312-6469.

133. Одинцов, В.О. Антикризисное управление в коммерческом банке: вызовы и решения / В.О. Одинцов // Экономика и предпринимательство. – 2021. – № 2 (127). – С. 1044-1048. – ISSN 1999-2300.

134. Одинцов, В.О. Блокчейн как инновационный метод обеспечения экономической и информационной безопасности коммерческого банка / В.О. Одинцов // Modern Economy Success / Успехи современной экономики. – 2023. – № 1. – С. 275-278. – ISSN 2500-3747. – Текст : электронный. – DOI отсутствует. – URL: https://www.elibrary.ru/download/elibrary_50168906_35150124.pdf (дата обращения: 12.07.2024).

135. Одинцов, В.О. Инструменты управления рисками цифровизации бизнес-процессов кредитной организации при обеспечении экономической безопасности / В.О. Одинцов // Экономика, предпринимательство и право. – 2024. – № 4. Том 14. – С. 1597-1606. – eISSN 2222-534X. – Текст : электронный. – DOI 10.18334/epp.14.4.120686. – URL: https://www.elibrary.ru/download/elibrary_65667626_99152352.pdf (дата обращения: 12.07.2024).

136. Одинцов, В.О. Основные тенденции развития цифровизации / В.О. Одинцов, Л.В. Волков // Стратегии бизнеса. – 2021. – № 5. Том 9. – С. 142-144. – ISSN 2311-7184. – Текст : электронный. – DOI 10.17747/2311-7184-2021-5-142-144. – URL: https://www.elibrary.ru/download/elibrary_45691279_62945535.pdf (дата обращения: 12.07.2024).

137. Одинцов, В.О. Оценка эффективности функционирования коммерческих банков России на основе анализа среды функционирования / В.О. Одинцов, Е.А. Вечкинзова // Креативная экономика. – 2021. – № 5. Том 15. – С. 2017-2032. – ISSN 1994-6929.

138. Одинцов, В.О. Проблемы обеспечения кибербезопасности в коммерческих банках России в современных условиях / В.О. Одинцов // Горизонты экономики. – 2023. – № 3 (76). – С. 103-107. – ISSN 2219-3650.

139. Одинцов, В.О. Развитие теории управления рисками в условиях расширения присутствия кредитных организаций в цифровом пространстве / В.О. Одинцов // Общество: политика, экономика, право. – 2024. – № 1. – С. 115-121. – ISSN 2071-9701.

140. Одинцов, В.О. Устойчивость банковского сектора России в периоды кризисов / В.О. Одинцов // Экономика и предпринимательство. – 2021. – № 3 (128). – С. 248-251. – ISSN 1999-2300.

141. Одинцов, В.О. Экономическая безопасность кредитных организаций в условиях роста цифровых рисков / В.О. Одинцов // Вестник евразийской науки. – 2023. – № 6. Том 15. – ISSN 2588-0101. – Текст : электронный. – DOI 10.15862/64ECVN623. – URL: https://www.elibrary.ru/download/elibrary_65006544_64472634.pdf (дата обращения: 12.07.2024).

142. Орлов, С.Н. Применение технологии Digital Twin для управления залоговым портфелем коммерческого банка / С.Н. Орлов, А.А. Тищенко // Финансы и кредит. – 2023. – № 3 (831). Том 29. – С. 575-600. – ISSN 2071-4688.

143. Орлова, Л.Н. Анализ существующих систем управления рисками в финансовых и нефинансовых организациях / Л.Н. Орлова, В.О. Одинцов, К.А. Санникова // Креативная экономика. – 2022. – № 4. Том 16. – С. 1341-1358. – ISSN 1994-6929.

144. Поддуева, И.С. Управление эффективностью кредитной организации с учетом риска RAROC / И.С. Поддуева, С.А. Шелковников // Международный научно-исследовательский журнал. – 2015. – № 3-3 (34). – С. 82-83. – ISSN 2303-9868.

145. Потапенко, А.В. Информационная безопасность операционной банковской деятельности: подходы, методы и практические рекомендации для повышения эффективности решения основных функциональных задач / А.В. Потапенко // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 7-2. – С. 99-104. – ISSN 2223-2966.

146. Прокопова, Л.Г. Феноменологический подход: новые возможности для маркетинга (на примере рынка банковских услуг) / Л.Г. Прокопова // Вестник Российского экономического университета им. Г.В. Плеханова. Вступление. Путь в науку. – 2022. – № 2 (38). Том 12. – С. 34-46. – ISSN 2226-6860.

147. Рамзаева, Е.П. Экономическая безопасность как фактор стабильности сферы потребительского кредитования коммерческого банка / Е.П. Рамзаева // Вестник Международного института рынка. – 2022. – № 2. – С. 48-52. – ISSN 1998-9520.

148. Репецкая, А.Л. Криминологический анализ современного состояния мошенничеств в банковской сфере России / А.Л. Репецкая, Л.А. Петрякова // Вестник Омского университета. Серия: Право. – 2022. – № 1. Том 19. – С. 62-72. – ISSN 1990-5173.

149. Рудакова, О.С. Цифровой банкинг в России: научная интерпретация, организационная структура и векторы развития (вопросы

теории и практики) / О.С. Рудакова, О.М. Маркова // Банковские услуги. – 2021. – № 3. – С. 2-14. – ISSN 2075-1915.

150. Русанов, Ю.Ю. Виды, классификация и группировки рисков банковского менеджмента / Ю.Ю. Русанов // Финансы и кредит. – 2005. – № 4 (172). – С. 35-39. – ISSN 2071-4688.

151. Рыжов, Д.И. Оценка информационных рисков при использовании облачных сервисов по критериям существующих стандартов / Д.И. Рыжов, П.Б. Хорев // Информационные системы и технологии. – 2022. – № 6 (134). – С. 124-132. – ISSN 2072-8964.

152. Рязанова, О.А. Формирование системы экономической безопасности коммерческого банка на примере банка ВТБ (ПАО) / О.А. Рязанова, Н.В. Лакирева // Вектор экономики. – 2022. – № 12 (78). – ISSN 2500-3666. – Текст : электронный. – DOI отсутствует. – URL: http://www.vectoreconomy.ru/images/publications/2022/12/financeandcredit/Ryazanova_Lakireva2.pdf (дата обращения: 11.04.2024).

153. Саенко, Е.В. Кибербезопасность в банковском секторе: общая характеристика, российский подход, зарубежная практика / Е.В. Саенко, А.С. Дайнеко, Ю.С. Субботина // Актуальные проблемы гуманитарных и социально-экономических наук. – 2022. – № 89. Том 3. – С. 19-22. – ISSN 2712-8911.

154. Самышева, Е.Ю. Анализ базовых понятий современной теории экономической безопасности / Е.Ю. Самышева, А.С. Усов // Вестник экономики, права и социологии. – 2023. – № 3. – С. 45-49. – ISSN 1998-5533.

155. Синявский, Н.Г. Анализ моделей развития бизнеса в условиях рисков / Н.Г. Синявский // Финансовая экономика. – 2019. – № 2. – С. 767-770. – ISSN 2075-7786.

156. Соловьев, С.В. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах / С.В. Соловьев, М.А. Тарелкин, В.В. Текунов [и др.] // Вопросы кибербезопасности. – 2023. – № 1 (53). – С. 41-57. – ISSN 2311-3456.

157. Соловьева, Н.Е. Интернет-банкинг как инновационная форма обслуживания в экономических системах / Н.Е. Соловьева, А.М. Кулик, М.В. Гуменюк // Организатор производства. – 2023. – № 3. Том 31. – С. 78-85. – ISSN 1810-4894.

158. Старовойтов, В.Г. Система управления рисками и мониторинг экономической безопасности Российской Федерации: федеральный уровень, первый опыт / В.Г. Старовойтов, Н.В. Старовойтов // Развитие и безопасность. – 2019. – № 4. – С. 26-35. – ISSN 2713-2633.

159. Таштамиров, М.Р. Финансовые инновации и цифровые технологии в банковской деятельности: институциональный взгляд / М.Р. Таштамиров // Вестник Чеченского государственного университета им. А.А. Кадырова. – 2023. – № 2 (50). – С. 57-70. – ISSN 2072-3121.

160. Ткачева, М.В. Проблемы обеспечения экономической безопасности банковской деятельности / М.В. Ткачева, Е.Е. Бичева // Современная экономика: проблемы и решения. – 2023. – № 6 (162). – С. 104-113. – ISSN 2078-9017.

161. Токарев, К.К. Цифровизация банковского сектора экономики / К.К. Токарев, Т.П. Носова // Modern Science. – 2021. – № 4-1. – С. 172-176. – ISSN 2414-9918.

162. Харченко, Е.В. Банковские риски: создание новой системы управления / Е.В. Харченко, Е.Т. Гринько // Вестник Луганского государственного университета имени Владимира Даля. – 2022. – № 4 (58). – С. 148-151. – ISSN 2522-4905.

163. Цветкова, О.Н. Анализ цифровизации банковской сферы в России / О.Н. Цветкова // Самоуправление. – 2023. – № 2 (135). – С. 1286-1289. – ISSN 2221-8173.

164. Черная, Е.Г. Экономическая безопасность коммерческого банка в условиях цифровизации / Е.Г. Черная // Вестник ВИЭПП. – 2022. – № 2. – С. 54-56. – ISSN 2658-6886.

165. Чернобровкина, Е.Б. Национальная платежная система как элемент инфраструктуры национальной безопасности / Е.Б. Чернобровкина // Юридическая наука. – 2023. – № 6. – С. 52-56. – ISSN 2220-5500.

166. Чумаков, В.А. Методики оценки рисков информационной безопасности банков: экономико-правовой аспект / В.А. Чумаков // Финансовая экономика. – 2022. – № 4. – С. 74-76. – ISSN 2075-7786.

167. Чумаченко, Е.А. Особенности институционального устройства Российской антиотмывочной системы и ее влияние на эффективное функционирование банковской системы / Е.А. Чумаченко, Е.И. Бричка, Т.И. Демиденко // Финансовая экономика. – 2023. – № 7. – С. 75-80. – ISSN 2075-7786.

168. Шафран, С.И. Обеспечение финансовой безопасности, банковского сектора экономики РФ , как элемента национальной безопасности / С.И. Шафран, П.В. Хакимова, А.А. Садчикова // Уральский научный вестник. – 2023. – № 7. Том 10. – С. 138-148. – ISSN 1561-6908.

169. Шахбазова, М.С. Методологические аспекты управления в сфере менеджмента / М.С. Шахбазова // Журнал прикладных исследований. – 2023. – № 2. – С. 62-65. – ISSN 2949-1878.

170. Щелканов, А.А. Экономическая безопасность кредитных организаций: риск ДБО и принципы управления / А.А. Щелканов, А.Ю. Форгунова // Ученые записки Международного банковского института. – 2020. – № 2 (32). – С. 146-159. – ISSN 2413-3345.

171. Щербакова, Н.В. Цифровые технологии в банковском секторе РФ: особенности и сопутствующие угрозы / Н.В. Щербакова // Вестник Кемеровского государственного университета. Серия: Политические, социологические и экономические науки. – 2021. – № 1 (19). Том 6. – С. 136-146. – ISSN 2500-3372.

172. Щетинникова, А.Д. Цифровизация и внедрение дистанционного обслуживания в банковской сфере / А.Д. Щетинникова // Вестник экономики, права и социологии. – 2020. – № 1. – С. 168-172. – ISSN 1998-5533.

173. Якунина, Д.Н. Финансовая стратегия коммерческого банка: оценка эффективности и определение возможностей развития / Д.Н. Якунина, Л.Б. Парфенова, А.А. Пугачев // Вестник Тверского государственного университета. Серия: Экономика и управление. – 2019. – № 2. – С. 31-40. – ISSN 2219-1453.

174. Янченко, Е.В. Риски организации в условиях цифровизации экономики / Е.В. Янченко // Креативная экономика. – 2022. – № 6. Том 16. – С. 2239-2256. – ISSN 1994-6929.

Источники на иностранном языке

175. Aldasoro, I. Operational and cyber risks in the financial sector / I. Aldasoro, L. Gambacorta, P. Giudici, T. Leach // BIS Working Papers. – 2020. – № 840. – P. 2-37. – ISSN 1020-0959.

176. Bank for International Settlements : website. – Basel. – URL: https://www.bis.org/ (дата обращения: 12.08.2023). – Текст : электронный.

177. Banking models after COVID-19: Taking model-risk management to the next level / McKinsey : website. – New York. – Текст : электронный. – URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/banking-models-after-covid-19-taking-model-risk-management-to-the-next-level (дата обращения: 22.08.2023).

178. Banking risk assessment methodology puts risk into focus / Crowe : website. – Chicago. – Текст : электронный. – URL: https://www.crowe.com/insights/banking-risk-assessment-methodology-puts-risk-into-focus (дата обращения: 22.08.2023).

179. Basic DEA models additive models / Deaos.com : website. – Richmond Hill. – Текст : электронный. – URL: https://www.deaos.com/en-us/models/search#!/ShowTyp-grid (дата обращения: 22.08.2023).

180. Boardroom Cybersecurity Report 2023 / Cybercrime Magazine : website. – Washington. – Текст : электронный. – URL:

https://cybersecurityventures.com/cybersecurity-boardroom-report-2023/ (дата обращения: 22.08.2023).

181. Charnes, A. Evaluating program and managerial efficiency: An application of data envelopment analysis to program follow through / A. Charnes, W. Cooper, E. Rhodes // Management Science. – 1981. – № 27. – P. 668-697. – ISSN 1526-5501.

182. Charnes, A. Measuring the efficiency of decision making units / A. Charnes, W. Cooper, E. Rhodes // European journal of operational research. – 1978. – № 2. Volume 6. – P. 429-444. – ISSN 0377-2217.

183. Cooper, W. Introduction to Data Envelopment Analysis and Its Uses: With DEA-Solver Software and References / W. Cooper, L. Seiford, K. Tone // Springer. – 2006. – 388 p. – ISBN 978-0-387285-80-1.

184. Cressey, D. Other People's Money: A Study in the Social Psychology of Embezzlement / D. Cressey. – Montclair : Patterson Smith, 1973. – 191 p. – ISBN 978-0-875852-02-7.

185. Cybercrime and the financial industry in the United States - Statistics & Facts / Statista : website. – New York. – Текст : электронный. – URL: https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/ (дата обращения: 22.08.2023).

186. Cybersecurity and Technology Risk in Virtual Banking / ISACA : website. – Schaumburg. – Текст : электронный. – URL: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-and-technology-risk-in-virtual-banking (дата обращения: 22.08.2023).

187. Cybersecurity in a post-pandemic world / Deloitte : website. – London. – Текст : электронный. – URL: https://www2.deloitte.com/us/en/pages/advisory/articles/financial-services-cybersecurity-global-organizations.html (дата обращения: 22.08.2023).

188. Cybersecurity is number one risk for global banks, but geopolitical risk tops European banks’ concerns / EY : website. – London. – Текст : электронный. – URL: https://www.ey.com/en_gl/newsroom/2023/01/cybersecurity-is-number-

one-risk-for-global-banks-but-geopolitical-risk-tops-european-banks-concerns (дата обращения: 22.08.2023).

189. Cybersecurity: 2022 Banking Industry Survey / KPMG : website. – Amstelveen. – Текст : электронный. – URL: https://kpmg.com/us/en/articles/2022/cybersecurity.html (дата обращения: 22.08.2023).

190. Digital Risk Office / University of Illinois System : website. – Springfield. – Текст : электронный. – URL: https://www.vpaa.uillinois.edu/digital_risk_management#:~:text=The%20term%20digital%20risk%20encompasses,ICT%20accessibility%2C%20and%20risk%20management. (дата обращения: 22.08.2023).

191. Digital risk: Transforming risk management for the 2020s / McKinsey : website. – New York. – Текст : электронный. – URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s (дата обращения: 22.08.2023).

192. Farrel, M.J. The measurement of Productive efficiency / M.J. Farrel. – Oxford : Journal of the Royal Statistical Society, 1957. – № 3. Volume 120. – P. 253-290. – ISSN 0952-8385.

193. Hopkin, P. Fundamentals of risk management : understanding, evaluating, and implementing effective risk management / P. Hopkin. – London : The Institute of Risk Management, 2010. – 358 p. – ISBN 978-0-7494-5942-0.

194. Knight, F. Risk, Uncertainty and Profit / F. Knight. – London : Forgotten Books, 2018. – 399 p. – ISBN 978-1-440084-72-0.

195. Leading concerns about the future of digital life / Pew Research Center : website. – Washington. – Текст : электронный. – URL: https://www.pewresearch.org/internet/2019/10/28/5-leading-concerns-about-the-future-of-digital-life/ (дата обращения: 22.08.2023).

196. Markowitz, H. Portfolio Selection / H. Markowitz. – Salt Lake City : The Journal of Finance, 1952. – № 1. Volume 7. – P. 77-91. – ISSN 1540-6261.

197. Matt, C. Digital Transformation Strategies / C. Matt, T. Hess, A. Benlian // Business & information systems engineering. – 2015. – № 57 (5). – P. 339-343. – ISSN 1867-0202.

198. Oracle. Cloud Applications and Cloud Platform : [website]. – Austin. – URL: https://www.oracle.com/ (дата обращения: 22.08.2023). – Текст : электронный.

199. Seiford, L. Modeling undesirable factors in efficiency evaluation / L. Seiford, J. Zhu // European Journal of Operational Research. – 2022. – № 142. – P. 16-20. – ISSN 0377-2217.

200. The future of bank risk management. – Текст : электронный. – DOI отсутствует. – URL: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/pdfs/the_future_of_bank_risk_management.pdf (дата обращения: 22.08.2023).

201. Tripe, D. Using DEA to investigate bank safety and soundness – which approach works best? / D. Tripe. – Leeds : Journal of Financial Economic Policy, 2010. – № 3. Volume 2. – P. 237-250. – ISSN 1757-6385.

202. What Is Digital Risk? / Proofpoint : website. – Sunnyvale. – Текст : электронный. – URL: https://www.proofpoint.com/us/threat-reference/digital-risk (дата обращения: 22.08.2023).

203. What is Digital Risk? Definition and Protection Tactics / UpGuard : website. – Sydney. – Текст : электронный. – URL: https://www.upguard.com/blog/digital-risk (дата обращения: 22.08.2023).

204. What is IT change management / Atlassian : website. – Sydney. – Текст : электронный. – URL: https://www.atlassian.com/itsm/change-management (дата обращения: 22.08.2023).

Приложение А

(информационное)

Основные макроэкономические показатели развития экономики Российской Федерации в 2021–2022 гг.

Таблица А.1 – Макроэкономические показатели развития экономики Российской Федерации в 2021–2022 гг.

Наименование показателя	Январь - сентябрь 2021 г.	Январь - сентябрь 2022 г.
Валовой внутренний продукт, млн рублей	92 231 713,6	105 324 730,4
Валовой внутренний продукт, прирост в процентах к предыдущему году	4,6	-2,0
Индекс потребительских цен, прирост в процентах к декабрю предыдущего года	5,3	10,5
Инвестиции в основной капитал, прирост в процентах к предыдущему году	7,6	7,8
Ввод в действие жилых домов, прирост в процентах к предыдущему году	29,4	26,5
Оборот розничной торговли, прирост в процентах к предыдущему году	9,0	-5,5
Реальные располагаемые денежные доходы населения, прирост в процентах к предыдущему году	4,3	-1,7
Реальная заработная плата работников организаций, прирост в процентах к предыдущему году	3,0	-1,5
Уровень общей безработицы (в среднем за месяц), в процентах	5,0	4,0
Курс доллара США (среднегодовой), руб./долл.	74,0	69,3
Средняя цена на нефть марки «Юралс», долл. США/баррель за год	66,2	82,4

Источник: составлено автором по материалам [55].

Приложение Б

(информационное)

Основные макроэкономические показатели банковского сектора Российской Федерации в 2019–2022 гг.

Таблица Б.1 – Макроэкономические показатели банковского сектора Российской Федерации в 2019–2022 гг.

Показатель	01.01.2019	01.01.2020	01.01.2021	01.01.2022	01.01.2023
1	2	3	4	5	6
Активы банковского сектора, млрд руб.	86 232	88 796	103 842	120 310	134 516
в процентах к валовому внутреннему продукту (далее – ВВП)	83,0	81,0	96,8	92,0	88,8
Справочно: совокупные активы банковского сектора без вычета сформированных резервов и налога на прибыль, млрд руб.	94 084	96 581	112 506	129 064	144 607
Собственные средства (капитал) банковского сектора, млрд руб.	10 269	10 981	11 413	12 605	13 348
в процентах к ВВП	9,9	10,0	10,6	9,6	8,8
в процентах к активам банковского сектора	11,9	12,4	11,0	10,5	9,9
Корпоративные кредиты и кредиты, предоставленные физлицам, включая просроченную задолженность, млрд руб.	52 912	56 654	64 804	74 949	83 377
в процентах к ВВП	50,9	51,7	60,4	57,3	55,1
в процентах к активам банковского сектора, в том числе:	61,4	63,8	62,4	62,3	62,0
корпоративные кредиты, включая просроченную задолженность, млрд руб.	38 011	39 004	44 760	50 346	56 385
в процентах к ВВП	36,6	35,6	41,7	38,5	37,2
в процентах к активам банковского сектора	44,1	43,9	43,1	41,8	41,9
кредиты, предоставленные физлицам, включая просроченную задолженность, млрд руб.	14 901	17 651	20 044	24 603	26 991
в процентах к ВВП	14,3	16,1	18,7	18,8	17,8
в процентах к активам банковского сектора	17,3	19,9	19,3	20,4	20,1
в процентах к денежным доходам населения	25,4	28,2	31,5	34,9	34,1
Кредиты банков в инвестициях организаций всех форм собственности в основной капитал (без субъектов малого предпринимательства), млрд руб.	1 531	1 436	1 530	1 953	2 062
в процентах к инвестициям организаций всех форм собственности в основной капитал (без субъектов малого предпринимательства)	11,2	9,8	9,9	11,0	9,7

Продолжение таблицы Б.1

1	2	3	4	5	6
Вложения в ценные бумаги, млрд руб.	11 484	12 012	16 151	17 289	19 449
в процентах к ВВП	11,1	11,0	15,0	13,2	12,8
в процентах к активам банковского сектора, из них:	13,3	13,5	15,6	14,4	14,5
вложения в долговые ценные бумаги	10 857	11 500	15 705	16 824	19 058
вложения в долевые ценные бумаги	494	455	413	427	362
учтенные векселя	133	57	32	38	29
Вклады физлиц, млрд руб.	28 459	30 412	32 834	34 695	36 619
в процентах к ВВП	27,4	27,7	30,6	26,5	24,2
в процентах к активам банковского сектора	33,0	34,2	31,6	28,8	27,2
в процентах к денежным доходам населения	48,4	48,6	51,6	49,2	46,3
Депозиты и средства корпоративных клиентов, млрд руб.	28 005	28 146	34 067	39 885	46 653
в процентах к ВВП	27,0	25,7	31,7	30,5	30,8
в процентах к активам банковского сектора	32,5	31,7	32,8	33,2	34,7
Справочно:	-	-	-	-	-
Показатель, млрд руб.	1.01.19	1.01.20	1.01.21	1.01.22	1.01.23
ВВП	103 862	109 608	107 315	130 795	151 456
Инвестиции организаций всех форм собственности в основной капитал (без субъектов малого предпринимательства)	13 641	14 725	15 438	17 708	21 347
Денежные доходы населения	58 782	62 532	63 692	70 492	79 076

Источник: составлено автором по материалам [56].

Приложение В

(информационное)

Структура рыночного риска банковского сектора Российской Федерации в 2021–2022 гг.

Таблица В.1 – Показатели структуры рыночного риска банковского сектора Российской Федерации

В процентах

Риск	01.01.2021		01.01.2022		01.10.2022		01.12.2022		01.01.2023	
	к совокупному капиталу	Удельный вес в рыночном риске	к совокупному капиталу	Удельный вес в рыночном риске	к совокупному капиталу	Удельный вес в рыночном риске	к совокупному капиталу	Удельный вес в рыночном риске	к совокупному капиталу	Удельный вес в рыночном риске
Величина рыночного риска всего, в т. ч.:	47,6	100,0	44,1	100,0	36,8	100,0	35,2	100,0	36,1	100,0
процентного риска (ПР)	31,0	65,1	26,5	60,1	17,2	46,9	15,4	43,9	16,5	45,8
фондового риска (ФР)	8,1	16,9	5,7	12,9	3,5	9,5	4,1	11,6	4,7	13,0
валютного риска (ВР)	5,2	10,8	5,7	12,9	14,9	40,4	15,0	42,6	14,2	39,4
товарного риска (ТР)	3,4	7,1	6,3	14,2	1,2	3,2	0,7	1,9	0,7	1,8
Количество КО, единиц	277	-	250	-	241	-	230	-	240	-
Доля активов КО в совокупных активах банковского сектора, в процентах	93,0	-	92,6	-	93,2	-	93,6	-	93,6	-

Источник: составлено автором по материалам [56].

Приложение Г

(информационное)

Исходные показатели кредитных организаций для проведения расчетов с помощью метода анализа среды функционирования

Таблица Г.1 – Данные по ПАО «Сбербанк»

Период	Активы-нетто, тыс. руб.	Собственный капитал, тыс. руб.	Кредитный портфель, тыс. руб.	Привлеченные средства физлиц, тыс. руб.	Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	Доля наличности в составе активов-нетто, в процентах	Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	Активность лоро-счетов, относительные единицы (соотношение оборотов и активов-нетто)	Прибыль (норма прибыли к капиталу, в процентах)
1	2	3	4	5	6	7	8	9	10
фев.22	39 010 597 352	5 120 838 908	27 802 501 288	14 743 149 317	1,48	2,00	0,06	0,46	2,00
янв.22	39 011 694 414	5 157 642 836	27 470 992 294	15 279 984 689	2,11	2,00	0,08	0,66	24,00
дек.21	39 246 019 913	5 071 037 128	27 005 799 220	14 679 637 313	1,64	2,00	0,05	0,55	23,00
ноя.21	37 951 421 413	5 030 416 173	26 299 046 160	14 601 197 015	1,71	2,00	0,06	0,59	21,00
окт.21	37 525 958 139	5 024 518 226	25 920 506 225	14 689 443 113	1,72	2,00	0,06	0,60	19,00
сен.21	37 280 761 224	4 929 239 556	25 606 710 436	14 592 488 212	1,71	2,00	0,06	0,56	17,00
авг.21	36 853 428 192	4 840 320 486	25 292 533 888	14 559 902 328	1,68	2,00	0,06	0,57	15,00
июл.21	36 113 954 875	4 722 319 772	24 897 055 097	14 543 268 599	1,71	2,00	0,06	0,60	13,00
июн.21	36 207 216 696	4 639 680 633	24 503 948 361	14 555 998 196	1,45	2,00	0,05	0,47	11,00
май.21	36 268 614 616	4 970 053 114	24 275 129 605	14 900 467 278	1,66	2,00	0,05	0,52	8,00
апр.21	35 636 236 150	4 854 789 531	24 018 189 087	14 374 879 529	1,62	2,00	0,05	0,52	6,00
мар.21	34 635 033 186	4 786 442 330	23 826 924 858	14 349 202 806	1,40	2,00	0,04	0,41	4,00

Продолжение таблицы Г.1

1	2	3	4	5	6	7	8	9	10
фев.21	34 582 356 193	4 757 173 013	23 718 289 916	14 314 659 776	1,24	2,00	0,03	0,38	2,00
янв.21	34 416 825 176	4 741 066 308	23 777 228 189	14 788 836 676	1,92	2,00	0,05	0,52	16,00
авг.20	31 624 779 473	4 692 205 668	21 909 753 601	13 986 105 731	1,59	2,00	0,03	0,46	9,00
июл.20	31 111 328 028	4 537 146 347	21 457 449 951	13 891 865 526	1,42	2,00	0,05	0,40	7,00
июн.20	30 501 693 348	4 873 464 994	21 446 149 642	13 517 867 012	1,23	2,00	0,03	0,32	6,00
май.20	30 732 603 849	4 701 217 149	21 595 926 336	13 724 593 729	1,30	2,00	0,03	0,40	5,00
апр.20	30 627 516 202	4 644 592 548	21 645 947 027	13 522 363 259	1,59	2,00	0,05	0,47	5,00
мар.20	28 999 568 660	4 624 728 636	20 839 111 401	13 139 143 460	1,41	2,00	0,03	0,41	3,00
фев.20	28 694 864 393	4 746 458 425	20 487 392 784	12 906 727 868	1,32	2,00	0,04	0,39	2,00
янв.20	28 735 660 247	4 675 646 947	20 413 930 146	13 283 673 101	1,86	2,00	0,05	0,44	19,00
дек.19	28 888 213 881	4 525 375 414	20 242 734 123	12 737 017 696	1,47	2,00	0,04	0,40	18,00
ноя.19	28 994 650 427	4 520 556 888	19 987 701 841	12 725 279 222	1,56	2,00	0,04	0,48	17,00
окт.19	29 182 739 982	4 460 915 877	19 764 863 097	12 816 073 290	1,43	2,00	0,04	0,47	15,00
сен.19	29 061 462 235	4 560 510 560	19 570 693 417	12 838 237 116	1,60	2,00	0,03	0,56	14,00
авг.19	28 701 227 557	4 510 352 502	19 205 743 399	12 802 818 446	1,53	2,00	0,04	0,49	12,00
июл.19	28 499 771 900	4 444 268 030	19 120 289 257	12 864 518 235	1,38	2,00	0,04	0,49	11,00
июн.19	28 445 787 450	4 440 421 072	19 214 563 667	12 806 933 170	1,31	2,00	0,03	0,43	8,00
май.19	28 469 515 595	4 383 674 568	19 199 561 601	12 901 538 527	1,42	2,00	0,04	0,47	7,00
апр.19	28 234 337 695	4 305 071 228	19 283 652 637	12 543 708 271	1,33	2,00	0,03	0,46	5,00
мар.19	28 192 869 157	4 119 360 326	19 325 143 386	12 534 611 179	1,25	2,00	0,04	0,42	3,00
фев.19	27 753 426 094	4 399 458 622	19 294 293 025	12 264 207 288	1,12	2,00	0,02	0,37	2,00
янв.19	28 480 253 737	4 344 740 493	19 483 734 007	12 690 010 237	1,51	2,00	0,03	0,40	19,00
дек.18	27 702 661 442	4 287 330 543	19 069 861 802	12 020 961 143	1,34	2,00	0,03	0,41	18,00
ноя.18	27 289 334 653	4 210 200 147	18 893 633 768	12 032 671 995	1,34	2,00	0,04	0,46	17,00
окт.18	26 782 810 028	4 199 610 040	18 726 892 476	11 771 898 313	1,28	2,00	0,03	0,43	15,00
сен.18	26 669 443 690	4 260 563 704	18 738 749 948	11 959 939 574	1,38	2,00	0,03	0,50	14,00
авг.18	26 241 207 677	4 226 718 789	18 306 005 501	11 895 421 438	1,36	2,00	0,04	0,45	12,00

Продолжение таблицы Г.1

1	2	3	4	5	6	7	8	9	10
июл.18	26 074 494 156	4 127 576 770	18 107 340 682	11 862 212 318	1,31	2,00	0,04	0,46	11,00
июн.18	25 619 220 620	4 055 115 544	17 910 660 744	11 686 718 884	1,35	2,00	0,04	0,44	8,00
май.18	25 432 763 052	3 917 083 356	17 636 281 210	11 742 768 309	1,34	2,00	0,06	0,44	7,00
апр.18	24 646 881 355	3 866 132 060	16 922 361 196	11 420 072 186	1,34	2,00	0,06	0,45	5,00
мар.18	24 376 928 137	3 772 034 148	16 760 207 512	11 408 475 296	1,20	2,00	0,06	0,46	3,00
фев.18	24 232 760 517	4 023 200 945	16 695 830 873	11 209 546 297	1,11	2,00	0,05	0,44	2,00
янв.18	24 545 496 661	3 959 693 152	16 688 879 935	11 614 406 022	1,60	2,00	0,08	0,49	18,00
дек.17	23 982 602 380	3 886 162 023	16 683 720 648	11 008 983 954	1,35	2,00	0,10	0,51	17,00
ноя.17	23 824 314 176	3 782 057 956	16 417 780 114	10 924 733 760	1,34	2,00	0,09	0,46	16,00
окт.17	23 644 180 372	3 711 548 179	16 276 147 598	10 962 022 907	1,23	2,00	0,07	0,49	14,00
сен.17	23 684 067 797	3 694 397 893	16 271 823 109	8 989 756 938	1,34	2,00	0,00	0,51	12,00
авг.17	23 663 809 381	3 653 136 759	16 194 659 464	8 986 550 275	1,30	2,00	0,00	0,47	11,00
июл.17	23 187 813 592	3 591 197 297	15 851 836 090	8 956 753 283	1,32	2,00	0,00	0,52	9,00
июн.17	22 700 327 515	3 546 197 597	15 444 681 711	8 894 887 430	1,20	2,00	0,00	0,43	8,00
май.17	22 697 196 100	3 473 762 350	15 448 403 415	8 936 002 343	1,12	2,00	0,00	0,42	6,00
апр.17	22 430 308 834	3 381 264 842	15 271 106 813	8 857 784 607	1,26	2,00	0,00	0,49	5,00
мар.17	22 668 899 972	3 339 552 238	15 426 062 638	8 905 093 975	1,00	2,00	0,00	0,37	3,00
фев.17	22 823 664 279	3 430 778 192	15 528 387 905	10 827 932 300	0,93	2,00	0,04	0,36	2,00
янв.17	23 134 556 584	3 382 253 163	15 656 813 241	10 913 937 697	1,47	2,00	0,08	0,49	16,00

Источник: составлено автором по материалам [54].

Таблица Г.2 – Данные по «Банк ВТБ» (ПАО)

Период	Активы-нетто, тыс. руб.	Собственный капитал, тыс. руб.	Кредитный портфель, тыс. руб.	Привлеченные средства физлиц, тыс. руб.	Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	Доля наличности в составе активов-нетто, в процентах	Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	Активность лоро-счетов, относительные единицы (соотношение оборотов и активов-нетто)	Прибыль (норма прибыли к капиталу, в процентах)
1	2	3	4	5	6	7	8	9	10
фев.22	19 666 332 471	1 701 117 296	12 017 041 081	5 043 217 339	1,68	2,00	0,01	0,31	0,00
янв.22	19 412 039 126	1 802 070 892	12 078 202 867	5 100 141 334	2,36	2,00	0,02	0,49	13,00
дек.21	19 675 193 141	1 822 320 341	12 066 440 792	4 848 598 241	1,85	2,00	0,01	0,35	13,00
ноя.21	19 444 721 952	1 844 838 195	12 138 540 834	4 723 226 518	1,80	2,00	0,02	0,35	13,00
окт.21	19 662 119 794	1 840 728 967	12 085 458 659	4 711 883 392	1,74	2,00	0,02	0,35	11,00
сен.21	19 306 252 813	1 831 569 498	12 015 736 571	4 731 975 703	1,73	2,00	0,03	0,34	10,00
авг.21	19 057 547 331	1 813 220 962	11 951 564 911	4 702 638 768	1,86	2,00	0,03	0,40	9,00
июл.21	18 779 394 600	1 811 721 842	11 624 533 777	4 675 944 214	1,76	2,00	0,03	0,41	7,00
июн.21	18 507 404 635	1 719 380 097	11 566 152 693	4 632 118 861	1,52	2,00	0,01	0,33	7,00
май.21	18 120 114 240	1 691 594 220	11 469 557 729	4 723 623 985	1,86	2,00	0,02	0,40	5,00
апр.21	17 603 317 918	1 686 409 367	11 094 905 265	4 627 619 512	1,88	2,00	0,02	0,37	5,00
мар.21	17 402 988 038	1 638 124 901	11 108 522 670	4 593 434 913	1,56	2,00	0,01	0,29	4,00
фев.21	17 176 974 803	1 634 561 003	11 073 792 383	4 624 154 097	1,32	2,00	0,01	0,26	1,00
янв.21	17 104 719 603	1 680 426 760	11 191 062 243	4 640 929 610	2,17	2,00	0,03	0,47	3,00
авг.20	16 039 764 461	1 642 989 450	10 929 504 446	4 411 523 388	1,61	2,00	0,02	0,35	3,00
июл.20	15 466 712 752	1 675 381 610	10 392 352 607	4 348 853 206	1,51	2,00	0,02	0,32	3,00
июн.20	15 259 953 950	1 662 669 765	10 438 548 158	4 329 667 290	1,30	2,00	0,02	0,26	3,00
май.20	15 518 266 452	1 644 753 525	10 500 980 107	4 428 403 225	1,52	2,00	0,02	0,39	3,00
апр.20	15 624 191 118	1 699 308 711	10 532 843 360	4 518 877 406	1,62	2,00	0,02	0,31	2,00

Продолжение таблицы Г.2

1	2	3	4	5	6	7	8	9	10
мар.20	14 350 698 069	1 673 384 444	10 106 100 804	4 443 101 663	1,37	2,00	0,03	0,25	1,00
фев.20	14 341 093 368	1 676 208 263	10 028 547 519	4 305 272 617	1,29	2,00	0,01	0,27	1,00
янв.20	14 578 238 863	1 725 803 765	10 197 032 367	4 316 486 471	1,63	2,00	0,02	0,34	13,00
дек.19	14 782 708 034	1 724 828 047	10 340 388 626	4 183 250 351	1,31	2,00	0,03	0,27	10,00
ноя.19	14 757 168 569	1 699 503 621	10 388 111 886	4 158 607 608	1,39	2,00	0,02	0,29	10,00
окт.19	14 835 940 576	1 679 085 267	10 528 616 747	4 145 050 176	1,35	2,00	0,01	0,26	8,00
сен.19	15 217 660 152	1 665 692 255	10 641 340 926	4 171 595 442	1,38	2,00	0,01	0,25	8,00
авг.19	14 611 990 788	1 652 738 873	10 382 350 664	4 070 391 154	1,53	2,00	0,02	0,24	8,00
июл.19	14 381 483 067	1 638 040 099	10 402 948 154	4 058 321 513	1,51	2,00	0,01	0,25	7,00
июн.19	14 604 792 290	1 630 306 651	10 345 534 980	4 040 830 886	1,48	2,00	0,01	0,21	6,00
май.19	14 613 216 133	1 615 211 219	10 238 313 105	4 022 900 517	1,71	2,00	0,02	0,28	3,00
апр.19	14 030 598 667	1 611 455 076	9 953 156 982	3 918 895 772	1,50	2,00	0,01	0,23	3,00
мар.19	14 114 563 376	1 605 063 907	10 007 214 144	3 888 307 528	1,39	2,00	0,01	0,27	3,00
фев.19	13 896 557 888	1 628 437 192	9 904 373 806	3 804 672 794	1,34	2,00	0,01	0,25	1,00
янв.19	14 362 917 235	1 574 887 217	10 001 727 617	3 829 626 296	1,74	2,00	0,02	0,32	16,00
дек.18	14 274 721 332	1 589 244 629	9 919 843 423	3 607 968 337	1,56	2,00	0,02	0,23	13,00
ноя.18	14 114 633 905	1 572 607 750	9 755 179 578	3 554 972 093	1,71	2,00	0,06	0,27	9,00
окт.18	13 700 957 751	1 553 783 388	9 667 807 400	3 563 239 587	1,54	2,00	0,02	0,31	9,00
сен.18	13 343 899 558	1 583 663 029	9 100 113 212	3 643 082 468	1,81	2,00	0,02	0,28	7,00
авг.18	12 812 958 348	1 510 439 357	8 756 541 476	3 554 489 503	1,56	2,00	0,02	0,34	7,00
июл.18	13 048 977 095	1 434 324 401	8 629 457 246	3 517 252 514	1,41	2,00	0,02	0,34	6,00
июн.18	12 759 860 116	1 449 163 257	8 339 070 137	3 424 427 273	1,37	2,00	0,02	0,22	4,00
май.18	12 861 138 648	1 421 153 785	8 309 408 883	3 406 716 177	1,47	2,00	0,03	0,26	4,00
апр.18	12 438 730 841	1 395 345 315	8 438 105 876	3 301 186 864	1,50	2,00	0,02	0,35	3,00
мар.18	12 305 840 774	1 384 371 234	8 194 436 862	3 124 816 479	1,47	2,00	0,03	0,28	2,00
фев.18	12 439 208 594	1 446 263 291	8 110 833 502	3 091 220 824	1,28	2,00	0,02	0,23	1,00
янв.18	10 016 423 568	1 427 533 769	5 936 927 730	608 981 962	1,52	2,00	0,03	0,49	10,00
дек.17	9 704 544 658	1 421 442 035	5 704 014 701	574 226 585	1,35	2,00	0,02	0,39	9,00

Продолжение таблицы Г.2

1	2	3	4	5	6	7	8	9	10
ноя.17	9 681 358 385	1 397 274 113	5 723 128 524	566 653 550	1,39	2,00	0,03	0,35	8,00
окт.17	9 747 577 352	1 391 238 201	5 683 985 577	559 369 523	1,32	2,00	0,03	0,53	8,00
сен.17	9 623 386 947	1 061 710 135	5 550 026 699	508 372 912	1,66	2,00	0,00	0,45	8,00
авг.17	9 584 864 324	1 050 663 814	5 560 318 033	492 215 890	1,37	2,00	0,00	0,38	7,00
июл.17	9 432 920 797	1 050 786 920	5 532 109 734	478 698 927	1,32	2,00	0,00	0,47	3,00
июн.17	9 371 920 317	1 080 735 999	5 576 446 550	462 160 307	1,19	2,00	0,00	0,33	2,00
май.17	9 695 279 943	1 114 058 493	5 532 658 651	451 245 542	1,11	2,00	0,00	0,32	2,00
апр.17	9 622 224 703	1 074 455 520	5 487 293 052	446 172 652	1,38	2,00	0,00	0,35	1,00
мар.17	9 740 166 100	1 024 231 079	5 502 530 967	474 265 469	0,96	2,00	0,00	0,31	1,00
фев.17	9 890 098 755	1 012 062 684	5 605 073 488	528 952 881	1,00	2,00	0,01	0,51	1,00
янв.17	9 727 241 921	1 056 469 156	5 609 107 344	535 564 990	1,74	2,00	0,10	0,69	7,00

Источник: составлено автором по материалам [28].

Таблица Г.3 – Данные по АО «Тинькофф Банк»

Период	Активы-нетто, тыс. руб.	Собственный капитал, тыс. руб.	Кредитный портфель, тыс. руб.	Привлеченные средства физлиц, тыс. руб.	Активность клиентских счетов, относительные единицы (соотношение оборотов по клиентским счетам и активов-нетто)	Доля наличности в составе активов-нетто, в процентах	Активность счетов нерезидентов, относительные единицы (соотношение оборотов по счетам нерезидентов и активов-нетто)	Активность лоро-счетов, относительные единицы (соотношение оборотов и активов-нетто)	Прибыль (норма прибыли к капиталу, в процентах)
1	2	3	4	5	6	7	8	9	10
фев.22	1 289 889 040	208 040 988	686 465 508	683 510 206	9,32	2,00	0,02	0,00	2,00
янв.22	1 307 440 320	204 595 102	672 576 145	690 222 829	10,09	2,00	0,03	0,00	26,00
дек.21	1 164 999 590	187 370 439	656 508 722	614 499 502	11,57	2,00	0,02	0,00	25,00
ноя.21	1 144 844 230	146 836 583	635 480 914	590 996 515	11,16	2,00	0,02	0,00	32,00
окт.21	1 099 287 510	148 571 539	621 650 151	569 552 144	10,31	2,00	0,02	0,00	27,00
сен.21	1 027 170 800	151 246 789	607 819 951	552 774 053	10,27	2,00	0,02	0,00	25,00
авг.21	989 286 327	138 689 655	590 528 120	534 628 935	11,18	2,00	0,02	0,00	18,00
июл.21	963 404 560	131 299 403	581 610 153	514 515 310	12,93	2,00	0,03	0,00	18,00
июн.21	979 506 615	128 365 063	557 361 922	497 960 524	10,32	2,00	0,03	0,00	15,00
май.21	953 146 703	125 540 067	526 394 999	500 857 297	11,70	2,00	0,03	0,00	12,00
апр.21	907 714 016	124 128 624	500 687 779	469 711 749	12,18	2,00	0,03	0,00	11,00
мар.21	880 369 532	123 941 112	475 579 990	457 663 040	10,24	2,00	0,01	0,00	10,00
фев.21	862 236 302	123 906 354	460 429 073	445 259 529	9,89	2,00	0,01	0,00	6,00
янв.21	882 545 498	121 349 928	446 030 505	458 551 495	10,85	2,00	0,03	0,00	30,00
авг.20	752 006 943	124 468 709	406 030 750	396 780 485	6,66	1,00	0,01	0,00	16,00
июл.20	706 811 456	125 588 120	395 491 576	383 712 185	6,14	1,00	0,01	0,00	14,00
июн.20	686 630 238	123 913 101	390 472 569	371 970 499	4,95	1,00	0,02	0,00	11,00
май.20	670 500 250	121 807 197	392 219 945	362 268 148	5,04	1,00	0,02	0,00	11,00

Продолжение таблицы Г.3

1	2	3	4	5	6	7	8	9	10
апр.20	639 998 621	120 767 070	398 928 065	342 655 282	5,48	1,00	0,02	0,00	11,00
мар.20	650 937 784	119 512 462	393 764 732	342 916 714	3,90	1,00	0,02	0,00	10,00
фев.20	609 333 313	116 029 210	388 324 095	329 871 546	3,60	1,00	0,01	0,00	8,00
янв.20	618 305 946	111 714 078	380 766 918	336 213 666	4,17	1,00	0,03	0,00	28,00
дек.19	580 376 837	111 505 416	378 657 644	310 665 936	3,56	1,00	0,01	0,00	27,00
ноя.19	574 870 271	105 952 828	373 901 597	303 453 422	3,66	1,00	0,03	0,00	26,00
окт.19	550 686 257	102 043 119	374 682 922	294 020 629	3,41	1,00	0,01	0,00	24,00
сен.19	531 553 391	99 731 226	365 833 440	289 225 417	3,64	1,00	0,02	0,00	22,00
авг.19	505 208 367	99 244 159	350 378 169	278 349 670	3,85	1,00	0,12	0,00	20,00
июл.19	497 208 955	97 548 652	342 622 553	269 336 823	3,18	1,00	0,01	0,00	15,00
июн.19	481 083 543	91 784 783	324 652 364	258 133 199	3,07	1,00	0,03	0,00	14,00
май.19	467 480 463	89 017 597	306 986 439	253 102 638	3,26	1,00	0,02	0,00	13,00
апр.19	454 645 988	84 506 775	292 047 183	239 082 542	2,91	1,00	0,04	0,00	12,00
мар.19	428 202 607	78 177 115	269 858 164	234 215 901	2,78	1,00	0,02	0,00	10,00
фев.19	415 734 972	76 815 165	256 924 277	225 946 171	2,62	1,00	0,09	0,00	7,00
янв.19	424 903 388	75 510 934	252 476 907	234 533 089	2,67	1,00	0,06	0,00	23,00
дек.18	395 127 824	78 510 454	241 941 675	212 711 697	2,39	1,00	0,02	0,00	22,00
ноя.18	384 226 060	76 699 249	228 868 808	205 446 347	2,49	1,00	0,02	0,00	20,00
окт.18	368 258 556	72 779 347	219 018 785	197 006 895	2,19	1,00	0,03	0,00	19,00
сен.18	359 309 718	74 375 211	210 644 328	194 156 552	2,29	1,00	0,02	0,00	16,00
авг.18	338 928 913	72 519 739	203 994 118	184 445 342	2,18	1,00	0,02	0,00	14,00
июл.18	326 645 000	71 014 257	197 308 440	176 519 527	2,05	1,00	0,02	0,00	13,00
июн.18	328 632 990	69 814 057	193 332 138	169 137 261	1,81	1,00	0,02	0,00	10,00
май.18	321 387 372	68 127 771	185 503 448	165 659 044	1,90	1,00	0,04	0,00	9,00
апр.18	307 271 980	67 969 378	180 216 352	156 619 725	1,91	1,00	0,04	0,00	9,00
мар.18	298 258 691	66 968 179	172 403 212	152 836 955	1,64	1,00	0,01	0,00	6,00
фев.18	293 156 400	65 840 625	170 991 596	148 173 303	1,58	1,00	0,01	0,00	4,00
янв.18	298 578 241	63 896 818	166 280 931	153 368 786	2,15	0,00	0,10	0,00	29,00

Продолжение таблицы Г.3

1	2	3	4	5	6	7	8	9	10
дек.17	279 933 208	64 146 037	170 595 054	141 001 209	1,79	0,00	0,03	0,00	28,00
ноя.17	273 450 589	62 566 704	162 921 380	139 489 974	1,98	0,00	0,02	0,00	27,00
окт.17	267 551 581	60 325 390	159 721 077	137 189 242	2,10	0,00	0,03	0,00	25,00
сен.17	262 559 313	59 640 033	156 284 577	86 529 469	2,35	0,00	0,00	0,00	21,00
авг.17	253 256 963	58 906 127	148 983 921	84 964 470	2,40	0,00	0,00	0,00	19,00
июл.17	243 823 814	57 183 469	142 564 319	82 611 767	2,39	0,00	0,00	0,00	26,00
июн.17	216 097 082	54 050 377	138 158 253	80 512 003	2,19	0,00	0,00	0,00	22,00
май.17	210 377 004	51 816 504	133 960 722	77 291 381	2,14	0,00	0,00	0,00	19,00
апр.17	197 120 697	52 351 967	130 721 353	77 152 246	2,01	0,00	0,00	0,00	15,00
мар.17	193 116 981	35 003 209	126 497 211	78 087 246	1,79	0,00	0,00	0,00	10,00
фев.17	189 566 914	34 186 643	124 253 677	115 517 392	1,57	0,00	0,01	0,00	6,00
янв.17	193 978 753	33 405 726	120 713 495	120 449 480	2,10	0,00	0,08	0,00	34,00

Источник: составлено автором по материалам [58].