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

На правах рукописи

Сипратов Ростислав Олегович

МОДЕРНИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

5.2.4. Финансы

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата экономических наук

Научный руководитель — Рудакова Ольга Степановна,
доктор экономических наук, профессор

Москва – 2023

Оглавление

Введение

Актуальность темы исследования обусловлена тем, что в текущих реалиях развития «цифровой экономики» одним из важнейших критериев эффективной банковской деятельности является политика внедрения современных инновационных технологий.

Банковская система Российской Федерации на современном этапе развития динамично трансформируется, что определяет потребность создания обновленных стратегий устойчивого развития, повышение сложности организации работы финансовых рынков и разнообразие форматов предоставления банковских продуктов и услуг.

В настоящий момент времени среди финансово-кредитных институтов наблюдается повышение конкуренции за привлечение и удержание клиентов. С этой целью они вынуждены применять весь перечень имеющихся ресурсов, а также внедрять новые бизнес-модели, разнообразные новаторские методики функционирования на рынке, актуальные продукты и услуги, современные финансовые инструменты. Инновации являются основополагающим фактором устойчивости работы и развития банковской отрасли, а также обеспечивают стабильное увеличение эффективности и маржинальности банковской деятельности.

Технологии дистанционного банковского обслуживания в настоящее время выступают одним из основных конкурентных преимуществ кредитных организаций. Уровень и многообразие предоставляемых клиентам продуктов и услуг имеет непосредственное влияние на оценку их удовлетворенности и степени лояльности, что имеет прямое воздействие на размер прибыли самих банков.

Дистанционное банковское обслуживание позволяет значительно усовершенствовать банковское обслуживание клиентов и повысить его качество за счет создания динамичной информационной среды, а также

сокращения времени обслуживания клиентов в сравнении с классической моделью работы банковских институтов с клиентами.

Несмотря на обширный перечень преимуществ использования технологий дистанционного банковского обслуживания, развитие электронного банкинга оказывает значительное влияние на расширение профилей типичных банковских рисков. Данное обстоятельство обуславливает необходимость существенного пересмотра требований к системе риск-менеджмента кредитных организаций, а также совершенствования банковского надзора за использованием данных технологий.

На основании вышеизложенного можно утверждать, что тематика диссертационного исследования соответствует одной из наиболее актуальных задач в области банковской деятельности - совершенствование системы управления банковскими рисками, возникающими при трансформации информационного контура кредитных организаций в условиях осуществления дистанционного банковского обслуживания.

В 2022 году количество хакерских атак на российские банки возросло более чем в 20 раз, а объём несанкционированных операций, совершенных без согласия клиентов кредитных организаций, возрос на 11% по сравнению с прошлым годом. Причинами этого являются политически мотивированные действия хакеров и мошенников, зачастую координируемые не только на уровне криминальных образований, но и на уровне государственных структур стран, не относящихся к дружественным, уход с рынка вендоров, выпускающих системы защиты, и проблемы с привлечением к ответственности киберпреступников, которые находятся за рубежом.

Данная тенденция может крайне негативно повлиять на доверия клиентов банковских организаций к применению каналов дистанционного банковского обслуживания.

Необходимость модернизации системы управления рисками дистанционного банковского обслуживания в целях реализации механизма устойчивого развития кредитной организации, недостаточная практическая

разработанность поставленной задачи в современных условиях определяют значимость исследования и свидетельствуют об актуальности темы.

Несмотря на актуальность темы, вопросы, связанные с проблемами риск-менеджмента в рамках реализации дистанционного банковского обслуживания клиентов, остаются недостаточно разработанными.

Степень разработанности темы исследования. Вопросы, рассматриваемые в работе в различные периоды времени, изучались как отечественными учеными, так и зарубежными. Существенный вклад в изучение вопросов определения сущности системы дистанционного банковского обслуживания и последствий проявления рисков, связанных с её развитием, внесли О.И. Лаврушин, И.В. Ларионова, А.В. Турбанов, А.В. Тютюнник, О.С. Рудакова, Г.С. Панова, Е.Ф. Авдокушин.

Научные исследования Г.Н. Белоглазовой, Л.П. Кроливецкой, О.А. Гавриловой, Т.В. Нестеренко, А.М. Тавасиева, В.В. Трофимова дают различные представления об определении дистанционного банковского обслуживания.

Теория управления рисками банковской деятельности разобрана в работах Н.А. Амосовой, Н.П. Барынькиной, Н.И. Валенцевой, О.Ю. Городецкой, О.Г. Коваленко, И.В. Ларионовой, Н.Э. Соколинской, Е.В. Травкиной, М.Х. Халиловой и др.

Достаточно подробное описание различных способов проведения электронных платежей и сопутствующих им рисков отражено в работах Д.А. Кочергина, А.С. Обаевой, С.В. Криворучко.

Перечень рисков информационной безопасности подробно рассмотрен такими авторами: П.В. Ревенковым, Р.В. Костенко, И.А. Тутаевым, Л.В.Ляминым.

Перспективам развития экосистем как элемента цифровизации банковского сектора посвящены работы ученых-экономистов: Н.И. Быкановой, А.И. Гвоздаревой, О.А. Ивановой, А.К. Канторoевой, В.Е. Косарева, О.Е. Никонец, Рудаковой О.С. Модели совершенствования системы

банковского надзора в условия цифровизации банковского сектора отражены в научных трудах: С.Е. Дубовой, М.А. Абрамовой, Д.А. Рабаданова, Ф. Р. Гаджимурадова, С. Е. Гриценко, В. М. Еремеева и Н.Н. Бочарова.

Необходимо отметить вклад зарубежных авторов в разработку аналитических и контрольных инструментов системы управления рисков дистанционного банковского обслуживания, таких как J. McMillan, B. King, B. Mashali, D. Coderre, J. Harchekar, J. Kang и др.

Несмотря на большой интерес к проблематике анализа системы управления рисками дистанционного банковского обслуживания, на данный момент отсутствует единый подход к определению понятия дистанционного банковского обслуживания и его содержательному наполнению, не представлен комплексный унифицированный подход к анализу и оценке рисков дистанционного банковского обслуживания. Не реализован комплексный подход к анализу банковского надзора в целях минимизации рисков в сфере дистанционного банковского обслуживания. Все это затрудняет проведение всестороннего исследования, приводит к многовариантности и противоречивости выводов по результатам анализа.

Объектом исследования выступает система управления рисками дистанционного банковского обслуживания, предлагаемого коммерческими банками клиентам.

Предметом исследования выступают теоретические и методические подходы, методы и инструменты модернизации системы управления банковскими рисками дистанционного банковского обслуживания в современных условиях.

Область исследования соответствует п. 4. «Банки и банковская деятельность. Банковская система», п. 5. «Банковское регулирование. Система банковского надзора и ее элементы» Паспорта научной специальности 5.2.4. Финансы (экономические науки).

Цель исследования состоит в развитии теоретических положений, разработке методических подходов и практических рекомендаций по

модернизации системы управления рисками дистанционного банковского обслуживания в современных условиях.

Исследование предполагает постановку и решение следующих **задач**:

- систематизировать основополагающие теоретические подходы к формированию системы управления банковскими рисками и определить специфику построения ее организационных основ в банковской деятельности;

- установить факторы, которые оказывают наиболее значительное влияние на расширение профилей банковских рисков в условиях дистанционного банковского обслуживания;

- провести классификацию всего перечня рисков, связанных с расширением использования технологий дистанционного обслуживания банковских клиентов, выявить их главные преимущества и недостатки, а также разработать авторскую классификацию данного типа рисков;

- предложить рекомендации по повышению качества регулирования финансовой стабильности банковского сектора в разрезе использования систем дистанционного обслуживания путём модернизации системы управления рисками;

- предоставить практические рекомендации по минимизации риска недоверия к использованию банками цифровых технологий;

- произвести анализ российской и зарубежной практики управления банковскими рисками в рамках системы дистанционного банковского обслуживания;

- разработать авторскую методику оценки рисков дистанционного банковского обслуживания;

- разработать рекомендации по модернизации системы управления банковскими рисками дистанционного банковского обслуживания.

Научная новизна исследования заключается в развитии теоретических и методических положений о модернизации системы управления рисками дистанционного банковского обслуживания (далее - ДБО), а также разработке практических рекомендаций по ее осуществлению: разработке аналитического

инструментария комплексной оценки, анализа и управления рисками ДБО для сложившейся в банке модели ведения бизнеса, предусматривающего использование инновационных финансовых технологий.

Положения, выносимые на защиту. Наиболее значимые результаты, обладающие научной новизной и выносимые на защиту:

1) Дополнена и уточнена классификация рисков, связанных с расширением использования технологий дистанционного обслуживания банковских клиентов (С. 50-52). В частности, выделены шесть уникальных рисков (риск недостаточного банковского надзора в сфере ДБО, риск повышения уровня монополизации банковского сектора, риск недоверия клиентов к использованию банками цифровых технологий, риск применения некорректной моделей оценки риска, риск недостаточной цифровизации банковской инфраструктуры бэк-офиса, риск кибер-мошенничества), минимизация которых необходима для дальнейшего развития банковской отрасли, что создает условия для обоснования потребности в модернизации системы управления рисками дистанционного банковского обслуживания на макро- и микроуровне банковской системы.

2) Доказана гипотеза о том, что с ростом объёма использования цифровых каналов обслуживания клиентов возрастают и показатели риска кибер-мошенничества, негативно влияющего на финансовую стабильность банковского сектора (С. 57-61). На основании проведения факторного анализа, а также применения статистико-математических и эконометрических методов выявлена тенденция, которая сигнализирует о необходимости модернизации системы управления рисками дистанционного банковского обслуживания в целях поддержания финансовой стабильности банковского сектора.

3) Разработаны практические рекомендации по минимизации риска недоверия клиентов к использованию банками цифровых технологий (С. 78-80). Отмечено, что наиболее результативной мерой является создание единого рейтинга банков на основе критериев оценки уровня защищенности персональных данных клиентов, который стимулирует банки к

добросовестному поведению по отношению к персональным данным своих клиентов. Готовность человека доверять цифровым инновациям, чтобы полностью понимать и пользоваться ими, является важнейшим фактором для дальнейшего развития в области банковской цифровизации.

4) Доказано, что внедрение Open API в работу банковского сектора станет драйвером для разработки инновационных технологий и значительно увеличит доступность банковских продуктов для клиентов кредитных организаций, что нивелирует воздействие риска монополизации (С. 105-111). На основе анализа зарубежного опыта определено, что данная инновация значительно увеличит доступность банковских продуктов для клиентов кредитных организаций. Предложенная технология уменьшает воздействие риска монополизации: применение открытых интерфейсов, позволяющих получать равный доступ к информации для всех участников обмена данными, в отечественной практике ведёт к увеличению конкурентоспособности малых субъектов кредитного рынка за счет демонополизации доступа к данным пользователей.

5) Разработана комплексная модель оценки риска информационной безопасности, как одного из основных видов проявления рисков дистанционного банковского обслуживания, базирующаяся на методах и индикаторах оценки рисков, стрессовых параметрах и статистическом аппарате для проведения стресс-тестирования (С. 127-129). Благодаря смешанной структуре оценки, модель помогает учитывать как финансовые, так и нефинансовые факторы.

6) Построена модель управления рисками на основе системы Business Intelligence, которая позволяет повысить качество системы управления риском, а также обозначены направления её дальнейшей модернизации (С. 151-153). Анализ опыта российских и зарубежных кредитных организаций позволил выделить лучшие направления модернизации системы управления рисками, разработанные с учётом специфики электронного банкинга, основным из которых представляется применение инструмента Business Intelligence,

основанного на проведении анализа массивов данных и их последующего преобразования в актуальную для пользователей информацию.

Теоретическая и практическая значимость работы. Теоретическая значимость работы состоит в развитии методического инструментария организации риск-менеджмента банка в целях предотвращения финансовых и репутационных потерь при оказании клиентом услуг через каналы удалённого обслуживания. Предложенная модель классификации рисков омниканальности, а также алгоритм их оценки и мониторинга, задает целый ряд направлений дальнейшей разработки проблемы модернизации системы управления рисков дистанционного банковского обслуживания.

Практическая значимость работы определяется тем, что основные выводы и положения исследования ориентированы на их применение в деятельности Банка России и коммерческих банков. Применение предложенного аналитического инструментария способствует повышению качества процедур анализа, оценки и управления рисками дистанционного банковского обслуживания. Полученные результаты ориентированы на их практическое использование в аналитической работе сотрудников отдела рисков коммерческих банков.

Методология и методы исследования. Теоретической основой диссертации послужили фундаментальные и прикладные исследования отечественных и зарубежных специалистов в области дистанционного банковского обслуживания и анализа рисков.

Информационную основу исследования составили материалы Базельского комитета по банковскому надзору, нормативные документы и аналитические обзоры Банка России, Ассоциации российских банков, данные статистических исследований ведущих рейтинговых агентств, а также Росфинмониторинга и Росстата, внутренние разработки коммерческих банков, законодательные и нормативные акты Российской Федерации, исследования различных авторов, принимавших участие в международных конференциях и семинарах, российская и зарубежная монографическая литература, публикации

различных авторов в периодической печати, доступные справочные ресурсы в сети Интернет, собственные расчеты и проведенные исследования.

В рамках исследования были использованы общенаучные методы, такие как анализ и синтез, сравнение, а также моделирование. Кроме того, были применены эмпирические методы, методы использования экспертных оценок, обработку статистических данных. База исследования была подкреплена арсеналом инструментов экономико-статистического анализа, включая методы определения средних величин и методы экспертных оценок.

Степень достоверности, апробация и внедрение результатов исследования. Степень достоверности результатов подтверждается достаточным количеством наблюдений, современными методами исследования, которые соответствуют поставленным в работе цели и задачам. Выводы и рекомендации, сформулированные в диссертации, подкреплены убедительными фактическими данными. Полученные теоретические и практические результаты данного диссертационного исследования обсуждены на нескольких научных конференциях и получили положительную оценку на указанных мероприятиях. Основные положения и результаты рассмотрены и одобрены на следующих научных конференциях: на VIII Международной научно-практической конференции «Инновационные аспекты развития науки и техники» (г. Саратов, НОО «Цифровая наука», 12 мая 2021 г.), на VIII Международной научно-практической конференции «Научно-инновационные исследования и разработки» (г. Саратов, НОО «Цифровая наука», 12 сентября 2022 г.), на научно-практической конференции «Сценарии развития банковского сектора России в условиях новой реальности» (Москва, Финансовый университет, 14 марта 2023 г.).

Материалы диссертации используются в практической деятельности публичного акционерного общества "ТРАНСКАПИТАЛБАНК". В частности, используется разобранный методический подходов к оценке риск-факторов при обеспечении информационной безопасности кредитной организации. По материалам исследования внедрена предложенная модель управления рисками

на основе системы Business Intelligence. Выводы и основные положения диссертации помогают в распознавании негативных тенденций и угроз финансовой устойчивости банков.

Материалы диссертации используются Департаментом банковского дела и монетарного регулирования Финансового факультета ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» в преподавании учебной дисциплины «Диджитализация, финтех и инновации в финансовых институтах», «Современные платежные системы и технологии».

Апробация и внедрение результатов подтверждаются соответствующими документами.

Публикации. Основные положения и результаты исследования отражены в 8 публикациях общим объемом 4,7 п.л. (авторский объем 4,2 п.л.), в том числе 6 работ общим объемом 4,05 п.л (авторский объем 3,55 п.л.) опубликованы в рецензируемых научных изданиях, определенных ВАК при Минобрнауки России.

Структура и объем диссертации определены целью, задачами и логикой исследования. Диссертация состоит из введения, трех глав, заключения, списка литературы из 104 наименований и 4 приложений. Текст диссертации изложен на 183 страницах, содержит 27 рисунков, 11 таблиц и четыре формулы.

Глава 1
Теоретические основы модернизации системы управления рисками дистанционного банковского обслуживания

1.1 Сущность, формы и основные принципы функционирования системы дистанционного банковского обслуживания

Банковская система Российской Федерации на современном этапе развития динамично трансформируется, что определяет потребность создания обновленных стратегий устойчивого развития, повышение сложности организации работы финансовых рынков и разнообразие форматов предоставления банковских продуктов и услуг. В настоящий момент времени среди финансово-кредитных институтов наблюдается повышение конкуренции за привлечение и удержание клиентов. Чтобы этого достичь, от банков требуется применить весь перечень имеющихся ресурсов.

В текущих реалиях развития «цифровой экономики» одним из важнейших критериев эффективной банковской деятельности является политика внедрения современных инновационных технологий. Данное утверждение формируется из перечня предпосылок, которые определяют сформировавшиеся на настоящий момент тенденции в экономике.

Первой из предпосылок выступает взаимодействие кредитных организаций с их клиентской базой, основывающееся на принципах взаимовыгодного партнерства. Из этого следует, что банковские институты видят свой интерес не исключительно в сбережении, а также в увеличении объема финансовых ресурсов своих клиентов, которое достигается предоставлением им самых современных банковских продуктов и услуг, способствующих росту их деятельности, уменьшению денежных потерь, повышению деловой активности и нормы прибыльности. Следующим фактором возникновение принципиально новых видов кредитных услуг

является планомерное возрастание конкуренции между банками в борьбе за клиентов. Третьей предпосылкой можно выделить появление новейших информационных технологий вследствие ускорения развития научно-технического прогресса.

Стоит отметить, что нововведения, которые применяются в банковском секторе, отражаются не только в технических и технологических инновациях. Параллельно постоянно внедряются новые бизнес-модели, разнообразные новаторские методики функционирования на рынке, актуальные продукты и услуги, современные финансовые инструменты. Инновации являются основополагающим фактором устойчивости работы и развития банковской отрасли, а также обеспечивают стабильное увеличение эффективности банковской деятельности. На основании выделенных предпосылок все большее развитие получает форма банковского обслуживания, которая осуществляется дистанционно.

Теоретические подходы к определению сущности системы дистанционного банковского обслуживания, которая уже активно применяется банками на современном этапе, являются предметом пристального изучения учёными-экономистами. На основе анализа научной литературы, которая посвящена вопросу функционирования системы дистанционного банковского обслуживания, попытаемся раскрыть содержание вопроса в данной главе.

В научной и экономической литературе проводится активная дискуссия об определении дистанционного банковского обслуживания. В таблице 1.1 предоставлен анализ определений термина «дистанционное банковское обслуживание», которые были сформулированы различными авторами, изучающими теоретический аспект данного вопроса.

Один из институтов группы Всемирного банка определяет понятие дистанционного банковского обслуживания как: «инновационное использование информационных и коммуникационных технологий для предоставления финансовых услуг посредством каналов, альтернативных традиционным банковским филиалам и банкоматам» [91].

Таблица 1.1 – Определения термина «дистанционное банковское обслуживание», сформулированные учёными-экономистами

Учёные-экономисты	Предложенное определение сущности дистанционного банковского обслуживания
Белоглазова Г.Н., Кроливецкая Л.П.	Данные авторы полагают, что дистанционное обслуживание клиентов определяется как форма оказания банковских услуг, при которой клиент лично не посещает банковское отделение
Гаврилова О.А., Нестеренко Т.В.	Под удалённым банковским обслуживанием следует понимать оказание услуг клиентам кредитной организации на основании применения информационных технологий и через сеть Интернет
Рудакова О.С.	Определяет понятие как электронные услуги, которые оказываются банками с помощью применения средств вычислительной техники и телекоммуникаций
Тавасиев А.М.	Под дистанционным обслуживанием необходимо понимать предоставление коммерческим банком услуг своим клиентам без непосредственного взаимодействия самого клиента и специалиста кредитной организации
Трофимов В.В.	Представляет дистанционного банковского обслуживания как получение клиентами услуг от банковской организации на расстоянии

Источник: составлено автором по материалам [20; 23; 24; 26; 41].

По определению Базельского комитета по банковскому надзору, дистанционный банкинг включает в себя предоставление розничных и незначительных по масштабу банковских продуктов, а также небольших электронных платежей и других банковских услуг электронным способом [80].

Как можно заметить, в существующей учебной и научной литературе определения дистанционного банковского обслуживания имеют схожие черты, в частности, что реализация удаленного обслуживания клиентов производится через информационно-телекоммуникационные средства связи.

Несмотря на то, что тематика изучения темы дистанционного банковского обслуживания широко освещена в научной литературе и характеризуется достаточно высоким уровнем научной разработанности, можно сделать вывод об отсутствии единого толкования рассматриваемого понятия, что усложняет его понимание и практическое применение.

Таким образом, автор приходит к выводу, что дистанционное банковское обслуживание необходимо считать собирательным понятием, которое можно характеризовать как предоставление услуг и продуктов коммерческими

кредитными организациями путем предоставления распоряжений со стороны клиентов банка без непосредственного визита в банковские отделение с использованием современных информационно-коммуникационных технологий.

В контексте определения понятия «дистанционное банковское обслуживание» необходимо рассмотреть следующие термины: дистанционная банковская операция, а также дистанционные банковские услуги и продукты. Любому банковскому продукту всегда можно соотнести некоторую услугу как процесс формирования данного банковского продукта. В свою очередь, банковская услуга заключается в осуществлении определённых операций. Дадим определения этим терминам.

Дистанционная банковская операция — это совокупность связанных между собой действий, производимых кредитной организацией, направленных на исполнение конкретных задач по обслуживанию клиента, которые производятся при помощи информационно-телекоммуникационных средств связи. Дистанционная банковская услуга, в свою очередь, представляет собой комплекс систематизированных дистанционных банковских операций, проводимым банком. Дистанционный банковский продукт – это совокупный результат дистанционных банковских операций, совершенных банком, целью которых является определённый уровень реализации потребностей клиентами. Дистанционный банковский продукт отражается в границах банковских регламентов, а также имеет качественные, количественные и ценовые характеристики.

Дистанционное банковское обслуживание позволяет значительно усовершенствовать банковское обслуживание клиентов и повысить его качество за счет создания динамичной информационной среды, также уменьшению сроков обслуживания клиентов, в сравнении с классической моделью работы банковских институтов с клиентами.

Ученые-экономисты А.В. Тютюнник, А.В. Турбанов в своих работах подчеркивают многоуровневый характер системы дистанционного банковского обслуживания [17].

Представляется целесообразным поддержать их мнение, поскольку логика исследования обусловливает необходимость определения понятия «система дистанционного банковского обслуживания» на макро- и микроуровнях.

На уровне кредитной организации система дистанционного банковского обслуживания представляет собой комплекс установленных в банке аппаратно-программных средств, при помощи которых услуги клиентам оказываются в удаленном формате.

В широком смысле «система дистанционного банковского обслуживания» - банковскую деятельность, в области предоставления электронных финансовых услуг [18]. На макроуровне система ДБО включает элементы банковского надзора, контроля и законодательной регламентации.

Исходя из предмета исследования, необходимо также обозначить понимание границ термина «модернизация», которое будет применяться в рамках данного исследования.

В широком смысле «модернизация» — это процесс усовершенствования чего-либо в соответствии с современными требованиями посредством ввода различных обновлений.

Модернизируются в основном машины и оборудование, производственно-технологические и социально-экономические процессы. Усовершенствовать можно не только товары и услуги, но и технологию их производства. Данный тезис применим и к банковским технологиям. В отличие от модернизации товарного производства процесс модернизации технологий, в том числе банковских, или другого нематериального актива не имеет предметной осязаемой формы, но проявляется в результате внедрения обновленной программы, которая улучшает качество банковской деятельности (повышение качества управления риском за счет внедрения передовой банковской технологии) [70].

В современной мировой практике становится заметным изменение облика финансовых услуг. Компании используют новейшие технологии для

модернизации деятельности, а цифровизация изменяет картину привычной конкуренции и размывает границы между различными секторами экономики. Компании формируют цифровые экосистемы для того, чтобы привлечь как можно большее количество клиентов. Происходит «миграция» традиционных бизнесов – банки осуществляют поиск моделей диверсификации своей деятельности.

В общемировой практике финансовые экосистемы начали свое функционирование на базе крупнейших технологических компаний, у которых был доступ к огромным массивам данных из-за обладания развитой клиентской базой. В связи с этим на современном этапе всё отчётливее поднимается проблема конкуренции между банками и крупными финтех-компаниями.

На данном этапе развития ставится вопрос о возможности полноценного замещения кредитно-финансовых институтов передовыми технологическими корпорациями. Существует мнение, что такое вытеснение возможно, и даже в условиях отсутствия традиционных банков финансовая система останется жизнеспособной (J. McMillan) [88]. С другой стороны, существует мнение, что в условиях существования товарно-денежных отношений классические кредитные организации продолжат свое развитие (О.И. Лаврушин) [54].

Рассмотрение сущности системы дистанционного банковского обслуживания невозможно без определения принципов функционирования этой системы [44]. К ним относятся:

Принцип безотказности и устойчивости. Система должна быть подготовлена к функционированию в любых условиях, ее работоспособность не должна зависеть от стрессовых или чрезвычайных ситуаций в новых геополитических условиях. Восстановление работоспособности (при ее нарушении) должно занимать минимальное время. Для выполнения данного принципа, кредитным организациям необходимо разработать ряд мер, которые позволят повысить автономность работы информационных систем.

Принцип эффективности. Данный принцип выражается в экономической целесообразности функционирования дистанционных систем обслуживания для

кредитной организации, они должны быть рентабельными за счёт сокращения расходов по обслуживания клиентов в отделениях банка.

Принцип безопасности, реализация который производиться с двух направлений: для банковской организации и для её клиентов. Риски, связанные с нарушением условий данной «безопасности», играют важнейшую роль в ходе дальнейшего исследования.

Принцип удобства, заключающийся в необходимости создания комфортной для пользователей среды и интерфейса. Системе следует быть интуитивно понятной в использовании, её освоение должно занимать и минимальное количество времени.

Принцип оперативности, который определяется своевременным откликом системы на входящие запросы пользователей, а также быстрое получение информации и проведение транзакций.

Кроме того, необходимо выделить ряд специфических свойств, которые должны быть присущих системе дистанционного банковского обслуживания:

а) целостность: все элементы системы состоят в непосредственной взаимосвязи, и предназначены для основной цели - формирование эффективной модели обслуживания пользователей, которая дает возможность минимизировать издержки и полностью удовлетворять потребности клиентов кредитных организаций;

б) целенаправленность: общая цель функционирования системы дистанционного банковского обслуживания превалирует над отдельными целями ее составных элементов;

в) делимость: система дистанционного банковского обслуживания может быть поделена на самостоятельно функционирующие элементы, каждый из которых является системой;

г) структурированность: элементы системы дистанционного банковского обслуживания имеют горизонтальную структуру;

д) адаптивность: дистанционное банковское обслуживание приспосабливается к имеющимся условиям внешнего и внутреннего характера;

е) управляемость: как и элементы системы, так и вся система дистанционного банковского обслуживания подлежит управлению;

ж) надежность: система способна устойчиво функционировать в стрессовых условиях.

Также необходимо выделить три основные характеристики, которыми обладает дистанционное банковское обслуживание:

а) комфортный рабочий график взаимодействия между клиентом и коммерческим банком;

б) дистанционное банковское обслуживание отличается гибкостью в оказании услуг клиенту банка;

в) имеется разнообразный перечень возможностей по работе с финансовыми инструментами.

Рассмотрим основные преимущества дистанционного банковского обслуживания для клиентов:

а) Использование информационных и платежных сервисов в режиме постоянной доступности, а также предоставление возможности управления собственными счетами и оформленными банковскими продуктами в любой момент времени.

б) Быстродействие и оперативность обработки входящих запросов и проведения банковских операций.

в) Способность системы обеспечить постоянный мониторинг и анализ собственных платежей и поручений, а также предоставление актуальной финансовой информации (курсы валют, ближайшие отделения, банкоматы, терминалы, изменения тарифов, лимитов и условий банковских продуктов и услуг) [75].

Внедрение технологий дистанционного банковского обслуживания имеет позитивные аспекты не только для пользователей данных продуктов и услуг, но и для банковских организаций. Рассмотрим преимущества дистанционного банковского обслуживания для самого банка:

а) Сокращение затрат за счет снижения стоимости обслуживания клиентов. Обслуживание клиентов в отделениях обходится банкам значительно дороже, нежели развитие систем дистанционного банковского обслуживания, потому как если реализовать второй вариант, то срок окупаемости вложенных затрат снижается, а получаемая прибыль растет.

б) Повышение уровня обслуживания потенциальных клиентов банка с помощью создания удаленных каналов обслуживания, в том числе через терминалы или банкоматы, что способствует уменьшению времени проведения банковских операций.

в) Снижение объема операционных ошибок, которые сопряжены с человеческим фактором, благодаря формированию шаблонов по ранее проведены операциям в «личном кабинете» клиента, что даёт возможность повысить качество совершаемых операций и ограничить возможные риски и потери кредитных организаций.

г) Качественное внедрение и постоянное развитие системы дистанционного обслуживания позволяет банку получать максимальную эффективность от своей деятельности и расширять свой бизнес путем продаж различных банковских продуктов и привлечения новых клиентов, направленных на долгосрочное сотрудничество.

Таким образом, пользователям удалённых банковских систем предоставляется надлежащий перечень банковских услуг и продуктов в удобном для них формате и месте. Все вышеперечисленные преимущества способствуют увеличению объёма прибыли банков, что выступает важным фактором преимущества в конкуренции на банковском секторе, позволяя использовать дополнительные ресурсы для развития и увеличения доли рынка.

Достигнутый этап развития современных технологий повышает популярность использования услуг дистанционного обслуживания. Во-первых, это обусловлено желанием клиента иметь возможность пользоваться услугами банка в любое время и в любом месте, тем самым экономя свое личное время.

Во-вторых, расширение использования дистанционного обслуживания в перспективе позволит банкам снизить расходы, генерируемые в ходе проведения большого спектра операций. Развитие системы дистанционного обслуживания крупнейшими банками стимулирует внедрение и разработку таких систем в остальных кредитных организаций.

Необходимо отметить, что пандемия, вызванная эпидемией COVID-19, стала бустером роста заинтересованности клиента в получении банковских услуг посредством использования дистанционного обслуживания.

В результате, в условиях всеобщей самоизоляции дистанционное банковское обслуживание стало полноценной альтернативой посещению банковского отделения, а также, получило значительный толчок к развитию. С начала пандемии охват пользователей интернет-банкинга, мобильного банка и других способов дистанционного обслуживания существенно увеличился за счет притока пользователей, ранее не использовавших указанные банковские услуги [31].

В основе системы дистанционного банковского обслуживания важным условием является обеспечение должного уровня конфиденциальности и безопасности при обмене информации между банком и его клиентом. Клиенты имеют возможность не только владеть информацией о состоянии своих счетов, а также и управлять ими, используя находящиеся у них под рукой средства коммуникации.

Дистанционное банковское обслуживание реализует ряд функций: функция информационная, функция коммуникаций, а также функция осуществления транзакций.

Информационная функция удаленного обслуживания клиентов банка связана с обеспечением качественного информирования клиентов по вопросам условий оказания услуг банка и их изменениям, а также по вопросам, касающимся состояния лицевых счетов и проведенных по ним операций.

Коммуникационная функция выражается в оказании консультационной помощи работниками банка в режиме дистанционного обслуживания. Например, прием заявки на блокировку счетов либо на получение кредита.

Функция проведения транзакций состоит в удаленном проведении финансовых операций. Примером может служить оплата товаров и услуг, перевод денежных средств на счета частных лиц и организаций.

Помимо наличия различных функций дистанционное банковское обслуживание может быть представлено в нескольких формах. К основным из них относятся:

а) Система «Банк-Клиент». Данная система считается классической версией удаленного банковского обслуживания. Клиент устанавливает программу, которая содержит полную информацию о его счетах и операциях, произведенных в определенном финансовом учреждении. Информация, предоставляемая программой, является достоверной и оперативно обновляется благодаря применению комплекса каналов связи в рамках использования сети Интернет.

Для совершения операций с использованием данной программы необходимо заключить договор с банком, произвести требующиеся действия по установке, войти в систему с помощью ключей электронной подписи. Система «Банк-Клиент» обладает множеством преимуществ, основным из которых является значительное упрощение работы клиента с банком, выраженное в возможности пользоваться обширным функционалом удаленно.

б) Система «Интернет-банкинг». Данная форма банковского обслуживания клиентов также имеет названия – «Онлайн-банк», система «Интернет-Клиент». Для обеспечения работы данного вида дистанционного банковского обслуживания необходимо подключение к сети Интернет. К основным преимуществам системы «Интернет-банкинг» относятся – простота практического применения и отсутствие необходимости в установке дополнительных программ [39].

в) Система «Банк-телефон» или «Мобильный банкинг», «Телефонный банкинг», а также «СМС-банкинг». Взаимодействие банка с клиентом в рамках данной системы сроится на использовании мобильной связи. В зависимости от конкретного банка спектр предлагаемых функций мобильного банка может существенно отличаться. Классический функционал телефонного банкинга включает в себя следующие опции: предоставление информации о банковских счетах клиента, о. текущем балансе, осуществлении платежных операций, предоставление выписок за определенный период и подтверждающих отчетов об оплате услуг и совершенных операциях.

г) Система удаленного обслуживания с эксплуатацией внешних сервисов – осуществление взаимодействия между банком и клиентом посредством использования аппаратов самообслуживания.

Дистанционное обслуживание с использованием банкоматов и терминалов широко распространено в России и за рубежом и является крайне востребованным. В результате взаимодействия с указанными техническими средствами клиент может получить ряд банковских услуг без посещения офиса, поэтому данная форма обслуживания также входит в сферу дистанционного банковского обслуживания.

Для обеспечения качественного функционирования дистанционного банковского обслуживания необходимо привлекать специалистов в сфере информатизации, информационной безопасности, юридического сопровождения. Помимо этого, важно установить взаимодействие всех подразделений кредитной организации и обеспечить интеграцию систем дистанционного банковского обслуживания с другими банковскими системами в целях оптимизации. Внутреннее устройство банка, проводимые в нем процессы, а также возможные варианты взаимодействия с клиентами, системы дистанционного обслуживания должны быть определены и встроены в техническую систему банка.

В целях удержания стабильного положения банка на рынке возрастает важность управления и развития отношений с клиентами – удержание уже имеющихся клиентов и повышение их лояльности, а также привлечение новых.

В последние годы в Российской Федерации в сфере дистанционного банковского обслуживания наблюдаются масштабные изменения. Электронный банкинг планомерно превращается в функциональный цифровой офис.

Если на начальных этапах развития в дистанционных системах был представлен ограниченный спектр предлагаемых услуг и продуктов, то сейчас их объём значительно увеличился. В частности, приложения мобильного банка уже в настоящее время дают возможность пользователям подключать необходимую услугу прямо с телефона. Без необходимости применения персонального компьютера, и тем более, личного посещения отделения банка. Помимо этого, все больше банков (например, как ПАО Сбербанк, АО «Альфа-банк», АО «Тинькофф Банк») начинают предоставлять банковские услуги через мобильное приложение не только физическим, но и юридическим лицам. Кроме того, динамично трансформируются методы терминального обслуживания, а также способы оплаты товаров и услуг.

Необходимо отметить, что при общем динамичном развитии каналов дистанционного банковского обслуживания, качество предоставляемого сервиса в кредитных организациях разного уровня имеет существенные различия, обусловленные трудоёмкостью и высоким уровнем затрат на формирования данных систем.

Во-первых, при формировании и модернизации конкурентоспособной системы дистанционного банковского обслуживания следует принять ряд основополагающих решений о том, каким будет процесс построения данной системы, во-вторых, определить наиболее эффективные пути её разработки.

Создание системы дистанционного банковского обслуживания для банка может быть осуществлено тремя разными способами:

а) Самостоятельная разработка. Метод применим только для крупных кредитных организаций, располагающих значительными ресурсами, поскольку

является сопряжет с очень большими затратами. Основным преимуществом данного способа выступает независимость от внешних компаний, поэтому все права на разработанное программное обеспечение будет принадлежать только банку, кроме того, будет учтена любая специфика данной кредитной организации. Среди недостатков выделяются значительные затраты при процессе разработки.

б) Делегирование разработки сторонней компании. Данный способ используют банки, которые из-за ограниченности имеющихся ресурсов не могут создать собственное подразделение по разработке систем дистанционного банковского обслуживания. Среди преимуществ покупки готового продукта можно выделить экономичность, оперативный запуск и систему, проверенную на опыте использования в других организациях.

Данный метод имеет целый ряд возможных недостатков:

1) Возникновение финансовых проблем у компании-вендора приведёт к замедлению или остановке разработки необходимого программного обеспечения.

2) Для устойчивого развития кредитной организации следует создать собственный штат специалистов, которые будут разрабатывать и усовершенствовать системы дистанционного банковского обслуживания непосредственно под потребности своего банка.

3) На программное обеспечение распространяется патентное право, поэтому оно остаётся собственностью правообладателя. Поэтому появляется необходимость покупать лицензию или оплачивать регулярную подписку на возможность использования и обслуживания программного обеспечение.

в) Комбинированная разработка. Метод состоит в формировании в банке необходимой для выполнения конкретных задач команды и привлечение сторонних вендоров для помощи в реализации продукта. Основным преимуществом данного способа выступает то, что банк получает разработку системы по индивидуальному плану, а не готовое «коробочное» решение, а также сохраняет все права на неё. По мнению автора работы, представляется

наиболее приемлемым способом для банковских организаций, поскольку разработка осуществляется как сотрудниками банка, так и привлеченными специалистами из передовых IT-компаний, что способствует обмену опытом.

Метод состоит в формировании в банке необходимой для выполнения конкретных задач команды и привлечение сторонних вендоров для помощи в реализации продукта. Основным преимуществом данного способа выступает то, что банк получает разработку системы по индивидуальному плану, а не готовое «коробочное» решение, а также сохраняет все права на неё.

При разработке мобильных приложений в техническом аспекте, как правило, кредитные организации делают выбор между двумя вариантами разработки:

а) Увеличение количества доступного функционала, которое приводит к значительному усложнению архитектуры приложения. Элементы управления должны содержать в себе объёмные функциональные блоки: единая лента операций, справочник контрагентов и сотрудников, система управления документами, онлайн-чат с историей коммуникаций. При этом необходима логическая взаимосвязь всех функций с контекстом пользовательских действий, чтобы учитывать все возможные технические сценарии.

б) Создание самостоятельного приложения для реализации обособленных групп задач. В данном случае необходимо обеспечение контекстных связей между сервисами, чтобы сформировать единую среду авторизации и цельность всей системы банковских приложений.

Создание системы дистанционного банковского обслуживания, включающей в себя интернет-банкинг и мобильный банкинг, и дальнейшее поддержание ее функционирования подразумевает значительные финансовые вложения. На рисунке 1.1 продемонстрирована динамика изменения уровня затрат ПАО Сбербанк на цифровизацию.

Источник: составлено автором по данным [94].
Рисунок 1.1 - Затраты ПАО Сбербанк на технологическую трансформацию

В 2020 году было зафиксировано, что затраты ПАО Сбербанк на технологическую модернизацию увеличились на 6,9% (7,7 млрд рублей в абсолютном значении) по сравнению с предыдущим годом и составили 118,8 млрд рублей. Данные сведения были представлены в отчетности банка от 17 мая 2021 года.

Помимо создания и усовершенствования систем дистанционного банковского обслуживания необходимо провести подготовительные мероприятия на остальных уровнях: обеспечить отделы необходимым оборудованием, провести подробный инструктаж сотрудников, изучить возможности интеграции систем дистанционного обслуживания с уже функционирующими банковскими системами, наладить работу со смежными компаниями и провайдерами.

Дистанционное банковское обслуживание в основном регулируется посредством федеральных нормативно-правовых актов и актов Центрального банка Российской Федерации [2].

Гражданский кодекс Российской Федерации предусматривает, что при заключении договора между банком и клиентом, оказание услуг, связанных с распоряжением денежных средств, может производиться дистанционно. Документы должны отвечать следующим требованиям:

- иметь в своем составе соответствующие признаки, по которым можно определить, что они соответствуют желаниям сторон в соответствии с заключенным договором, что указано в п. 2 ст. 434 Гражданского кодекса Российской Федерации [1];

- документы должны быть подписаны участниками сделки.

Зачастую формат дистанционного оказания услуг подразумевает наличие электронной подписи. Электронная цифровая подпись является полноценной заменой оригинальной подписи субъекта сделки и является подтверждением подлинности документа. В рамках проведения расчетных операций с платежными картами функцию подтверждения может заменить персональный идентификационный номер (далее – ПИН).

В банковской сфере правовая защита персональных данных гарантируется Федеральными законами о «О персональных данных», «Об информации, информационных технологиях и о защите информации», «О национальной платежной системе».

Федеральный закон Российской Федерации «О персональных данных» содержит статьи о необходимости обеспечения безопасности и целостности личных данных. К самым значимым мерам по защите персональных данных в рамках данного законодательного акта можно отнести: изменения данных, их распространение, снятие копий, ликвидация сведений, блокировка доступа к информационным данным в результате получения несанкционированного пользования данными. Помимо рекомендуемых мер безопасности за субъектом, владеющим персональными данными, закрепляется обязанность предпринимать действия по поддержанию сохранности этих данных. Обозначенные меры безопасности могут носить технический, юридический, организационный характер [5].

Объектом регулирования данного федерального закона являются права и обязанности организации, возникающие в ходе проведения удаленного обслуживания клиентов банка, также часть операций может контролироваться на уровне государства.

Федеральный закон «О национальной платежной системе», включает в себя статью, в которой перечислены основные механизмы обеспечения безопасности личных сведений частных лиц при совершении операций в рамках использования систем дистанционного банковского обслуживания [4].

В данном законе зафиксирована обязанность финансового учреждения обеспечивать защиту персональных данных клиента, а также любой другой информации, которая подлежит защите в рамках российского законодательства.

В соответствии с 9 статьей данного закона определен порядок и условия использования электронных средств платежа (далее – ЭСП).

Необходимо отметить, что проблема несовершенства действующего законодательства в области отношений, возникающих в процессе реализации банковских услуг через сети Интернет, требует особого внимания.

Ограничений в плане законодательства для развития дистанционного банковского обслуживания в России не предусмотрено, однако в данном случае необходимо провести совершенствование в законодательной базе для создания более эффективной и конкурентоспособной системы дистанционного банковского обслуживания.

Совершенствование системы возможно при принятии следующих законодательных норм:

а) Разработка и издание Центрального банка Российской Федерации специального нормативного акта, раскрывающего особенности дистанционного банковского обслуживания (раскрывая вопросы как взаимодействия банков с клиентом, так и основные условия договора о присоединении к дистанционному банковскому обслуживанию).

б) Издание нормативного акта Центрального банка Российской Федерации о необходимости банков создавать программы обучения и переобучения сотрудников для работы с системами дистанционного банковского обслуживания.

Кроме того, для укрепления регулирования системы дистанционного банковского обслуживания предлагаются следующие практические рекомендации:

- детально и подробно предусматривать в банковских документах (прежде всего в инструкциях и правилах об открытии, ведении и закрытии банковских счетов) принципы осуществления дистанционного банковского обслуживания, права и обязанности как банков, так и клиентов;

- установить во внутрибанковских правилах обязанности банков по идентификации лиц, которые распоряжаются банковскими счетами в рамках дистанционного банковского обслуживания, и необходимость в обязательном порядке предоставлять клиентом соответствующую информацию и документы для банка, исходя из необходимости исполнения требований ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

- важно помнить, что при работе с определенными категориями договоров или финансовыми инструментами существует требования по соблюдению простой письменной формы документа.

Необходимо отметить, что вопросы организации дистанционного банковского обслуживания очень сложны и специфичны, поэтому Банк России разработал ряд конкретных мероприятий по организации и корпоративному управлению, при использовании банками дистанционных форм обслуживания. система дистанционного банковского обслуживания дает возможность в управлении и использовании различного рода банковской информации применять ее эффективнее и с наименьшими временными потерями.

Таким образом, подводя основные итоги данного параграфа, необходимо отметить следующее. Анализ взглядов отечественных и зарубежных ученых на вопросы сущности, роли и экономического содержания системы дистанционного банковского обслуживания дал возможность сделать вывод об отсутствии единого толкования рассматриваемого понятия, что усложняет его понимание и практическое применение. Данный факт потребовал считать

дистанционное банковское обслуживание собирательным понятием, которое складывается из основных специфических характеристик данного вида банковских услуг.

Кроме того, по результатам рассмотрения форм и основных принципов функционирования систем дистанционного банковского обслуживания были выявлены основные этапы создания данных систем в коммерческих банках, а также проанализированы преимущества использования технологий удаленного обслуживания и их недостатки, которые, в частности, сопряжены с рисками банковской деятельности.

С учетом вышеизложенного дальнейшим шагом представляется исследование специфики современной системы управления рисками банковской деятельности. Более подробно данные положения рассмотрены в следующем параграфе.

1.2 Специфика современной системы управления рисками банковской деятельности и обоснование необходимости ее модернизации

Согласно экономическим научным исследованиям выявлено, что риски банковской деятельности обладают признаками экономической категории «риск», на основании таких характеристик как конфликтность, результативность и неопределенность [30].

Свойство конфликтности определяется существованием ряда противоречий между объективно возникающими рисковыми ситуациями и их субъективной оценкой.

Характеристика результативности риска отражается в возможности несовпадения запланированных показателей деятельности экономических агентов с их фактическими показателями.

Неопределенность риска взаимосвязана с проблемами в анализе и оценке количественного выражения вероятности наступления результатов событий, а также и степени их проявления.

Таким образом, на основании трёх определяющих характеристик, описанных выше, мы можем определить банковский риск как присущая финансовой деятельности возможность отклонения от ожидаемых заранее показателей в результате наступления событий, связанных с внутренними факторами (например, неэффективная организационная структура, низкая квалификация персонала) и внешними факторами (резкое изменение экономической конъюнктуры, появление новых технологий и прочие).

Риски в значительной степени взаимозависимы, и события, которые влияют на одну область риска, несут за собой последствия для ряда других категорий рисков. Таким образом, высшее руководство банков должно придавать большое значение улучшению способности идентифицировать, оценивать масштаб и контролировать общий уровень принимаемых рисков.

К основным видам рисков банковской деятельности, анализируемых риск-подразделениями, относятся:

а) Кредитный риск — возможное уменьшение стоимости активов банка, которое связано с отсутствием у заемщика возможности или желания выполнять условия кредитного договора по возврату заемных денежных средств и начисленных по ним процентов.

Кредитный риск портфеля банка зависит как от внешних, так и от внутренних факторов. К внешним факторам относятся состояние экономики, резкие колебания цен на акции, валютные курсы и процентные ставки, а также торговые ограничения, экономические санкции и политика правительства. Внутренние факторы: это недостатки кредитной политики, неадекватно определенные лимиты кредитования, недостатки в оценке финансового положения заемщиков, чрезмерная зависимость от обеспечения и неадекватное ценообразование, отсутствие механизма проверки кредитов и постсанкционного надзора.

Вероятность проявления кредитного риска возрастает при выдаче крупных займов одному заемщику или взаимозависимой группе заемщиков.

Можно утверждать о том, что саамы важным этапом для предотвращения кредитного риска является процедура одобрения и выдачи кредитного продукта.

б) Рыночный риск. Понятие рыночных рисков заключается в вероятности возникновения у кредитной организации ухудшения финансовых результатов и убытков, возникающих из-за изменения рыночной стоимости активов. Важной особенностью рыночного риска является его зависимость от состояния конъюнктуры финансового рынка.

В составе рыночного риска можно выделить три его основных проявления в виде фондового, валютного и процентного рисков.

Фондовый риск отражается в риске появления экономических потерь банка, возникающих из-за отрицательных колебаний на фондовом рынке. Из-за соответствующих изменений стоимость ценных бумаг и производных финансовых инструментов, находящихся в торговом портфеле кредитной организации, может резко снижаться.

Валютный риск - риск образования отрицательных финансовых результатов в связи с негативным изменением курсов иностранных валют, приносящим потери при проведении банковских операций.

Определение процентного риска состоит в возможности уменьшения полученной прибыли (или появления финансового убытка) вследствие неблагоприятного изменения значений процентной ставки.

в) Риск потери ликвидности. Риск потери банковской ликвидности связан с неспособностью кредитной организации своевременно и в полном объеме обеспечить погашение имеющихся на отчетную дату обязательств, которая ведет к возникновению финансовых убытков.

Риск ликвидности банков возникает из-за финансирования долгосрочных активов краткосрочными обязательствами, что делает обязательства подверженными риску пролонгации или рефинансирования.

г) Операционный риск. Операционный риск рассматривается как возможность возникновения финансовых потерь, проявляющихся из-за

несоответствия характеру и масштабам деятельности Банка и требованиям действующего законодательства, внутренних процедур исполнения банковских операций и других сделок, их нарушения сотрудниками Банка и иными лицами (вследствие непреднамеренных или умышленных действий, а также бездействия), несоразмерности функциональных возможностей используемых кредитной организацией информационных, технологических и других систем и их отказов (любых нарушений функционирования), а также в результате негативного воздействия внешних событий.

д) Правовой риск - риск возникновения у Банка убытков вследствие:

- несоблюдения Банком требований нормативных правовых актов и заключенных договоров;

- допускаемых правовых ошибок при осуществлении своей деятельности (неправильные юридические консультации или неверное составление документов, в том числе при рассмотрении спорных вопросов в судебных органах);

- несовершенства правовой системы (противоречивость законодательства, отсутствие правовых норм по регулированию отдельных вопросов, возникающих в процессе деятельности Банка);

- нарушения контрагентами нормативных правовых актов, а также условий заключенных договоров.

е) Риск потери деловой репутации. Репутационный риск - риск возникновения у банка финансовых потерь в результате уменьшения числа клиентов, а также контрагентов, из-за формирования в обществе негативного представления о финансовой устойчивости данного банка, качестве предоставляемых услуг или характере деятельности в целом. Репутация банка представляет собой обобщенную оценку обществом сильных и слабых сторон деятельности Банка, данная оценка генерируется в результате влияния значительного количества факторов. Деловая репутация банка строится на протяжении десятилетий, но, как и в любой другой сфере, может быть разрушена в минимально короткий срок. Репутация банка является одним из

важнейших критериев, лежащих в основе выбора клиентом банка для дальнейшего обслуживания.

ж) Страновой риск - риск негативного финансового результата у банка в результате неисполнения иностранными контрагентами (юридическими, физическими лицами) обязательств из-за экономических, политических, социальных изменений, а также вследствие того, что валюта денежного обязательства может быть недоступна контрагенту из-за особенностей национального законодательства (независимо от желания и финансового положения самого контрагента).

и) Региональный риск - риск, возникающий в связи с предоставлением кредита или в ходе инвестирования в конкретном регионе. Данная категория риска сформирована за счет наличия разницы в уровнях социально-экономического развития регионов, сложившихся с учетом политических, экономических, национальных, социальных факторов, а также состояния инвестиционного и налогового климата.

к) Отраслевой риск. Отраслевой риск представляет собой вероятность ухудшения экономических показателей конкретной отрасли в рамках данного отраслевого направления либо в сравнении со смежными отраслями. Уровень отраслевого риска, а также состояние предприятия в целом тесно взаимосвязаны с текущей стадией жизненного цикла отрасли и трендами характерными для внутриотраслевой конкуренции. Руководствуясь информацией об устойчивости предприятий отрасли относительно других отраслей, можно корректировать оценку отраслевого риска.

Стабильное и прибыльное функционирование в долгосрочной перспективе является основной целью развития для большинства банков. Для минимизации рисков и негативных последствий кризисных явлений кредитным организациям необходимо внедрять эффективную и динамичную систему управления рисками.

Управление банковскими рисками складывается из мероприятий, направленных на прогнозирование рисковых событий и составлению плана по минимизации ущерба при их наступлении.

Определение системы управления рисками можно представить как в широком, так и в узком смысле [25].

В широком смысле классическая система управления банковскими рисками включает такие элементы как: выполнение международных стандартов; денежно-кредитная политика и регулирование денежно-кредитных отношений, проводимых органами государственной власти; деятельность Центрального Банка Российской Федерации; механизмы государственного надзора, которые могут напрямую или косвенно оказывать влияние на состояние банковской системы страны.

В узком смысле система управления рисками – это комплекс формальных правил, нормативных актов, документов и мероприятий, необходимых для превентивной идентификации рисков, их оценки, анализа, составления плана по реагированию, а также разработки мер по разрешению последствий и поддержанию целевого уровня рисков.

Механизм управления рисками состоит из перечня элементов, которые отвечают за поддержание устойчивого функционирования и развития банковской отрасли страны, благодаря формированию эффективной системы управления рисками. Механизм управления рисками базируется на трех основных уровнях:

а) Международный уровень, на котором осуществляется стабильное сотрудничество банковских систем разных стран, роль регуляторов на данном уровне играют международные финансовые институты.

б) Макроуровень, включающий механизм управления рисками, который ответственен за устойчивую работу системы управления банковскими рисками на национальном уровне, включая выполнения предписания национального банковского регулятора.

в) Микроуровень, действующий внутри одной банковской организации. Механизм управления рисками на данном уровне обеспечивает эффективную деятельность организационных структур банка, отвечающих за выполнение предписаний банковского надзора, функционирование риск-менеджмента, исполнения целей по финансовым показателям и показателям ликвидности.

Общие параметры системы управления рисками должны включать в себя следующие элементы:

– Комплексный подход к измерению рисков.

– Утвержденную Советом директоров политику управления рисками, которая должна соответствовать долгосрочным бизнес-стратегиям банка.

– Руководящие принципы для управления процессом принятия рисков, включая развернутую структуру пруденциальных лимитов.

– Эффективную современную информационную систему управления для отчетности, мониторинга и контроля рисков.

– Обособленное подразделение управления рисками, независимое от операционных департаментов с четким разграничением уровней ответственности.

Основной проблемой при создании соответствующей организационной структуры управления рисками является выбор между централизованной и децентрализованной структурой. Глобальная тенденция заключается в централизации управления рисками с функцией управления денежными средствами, чтобы извлечь выгоду из информации о совокупных рисках, естественном взаимозачете рисков, экономии за счет масштаба и упрощения отчетности перед высшим руководством.

На международном уровне применяется комитетный подход к управлению рисками. На организационном уровне общее управление рисками поручается независимому комитету по управлению рисками или исполнительному комитету высшего руководства, который подчиняется непосредственно Совету директоров.

Цель создания данного комитета - предоставить одной группе специалистов полную ответственность за оценку общих рисков, с которыми сталкивается банк, и определение уровня рисков, который будет допустим в интересах банка. Функции комитета по управлению рисками заключаются в основном в выявлении, мониторинге и измерении профиля риска банка. Комитет также разрабатывает политики и процедуры, анализирует модели рисков по мере развития рынков, а также выявляет новые риски. В политике управления рисками должны быть четко прописаны количественные пруденциальные ограничения по различным сегментам операций банков.

На международном уровне наблюдается тенденция к установлению лимитов риска в терминах стандартов портфеля или кредита под риском (кредитный риск), прибыли под риском и стоимости под риском (рыночный риск). Комитет разрабатывает стресс-сценарии для измерения воздействия необычных рыночных условий и отслеживания расхождений между фактической волатильностью стоимости портфеля и прогнозируемой с помощью мер риска. Комитет также должен контролировать соблюдение различных параметров риска операционными департаментами.

В то время как Комитет по управлению активами и пассивами занимается различными типами рыночного риска, Комитет по кредитной политике контролирует кредитный риск, риск контрагента и страновой риск. Таким образом, управление рыночными и кредитными рисками в банках осуществляется параллельным двухсторонним подходом. Банки также могут создать единый комитет для комплексного управления кредитными и рыночными рисками. Как правило, политики и процедуры в отношении рыночного риска сформулированы в политиках управления активами-пассивами банка и процессов управления банковскими рисками.

Управление банковскими рисками в условиях относительно стабильной внешней среды значительно отличается от управления рисками в период финансового кризиса, что отражено в таблице 1.2.

Таблица 1.2 - Управление банковскими рисками в условиях стабильной среды и в период финансового кризиса - основные отличия

Показатели	Управление банковскими рисками в условиях:	
	стабильной среды	кризиса
Объекты управления	Риски, связанные с активно-пассивными операциями банка и с организацией его хозяйственной деятельности	Риски, связанные со значительными и непредсказуемыми изменениями факторов внешней среды
Субъекты управления	Члены наблюдательного совета и другие работники банка, задействованные в управлении банковскими рисками	Антикризисные менеджеры, временные рабочие группы, кураторы национального регулятора
Цель управления рисками	Избежать значительного негативного отклонения от запланированных показателей деятельности банка	Избежать банкротства, преодолеть кризисную ситуацию с минимальными потерями
Уровень ресурсной обеспеченности	Высокий уровень обеспеченности ресурсами при эффективной деятельности банка	Ограниченность финансовых ресурсов вследствие значительного увеличения рисков внешней среды
Скорость принятия и качество управленческих решений	Взвешенный и постепенный процесс принятия управленческих решений	Высокая вероятность принятия ошибочных решений по причине необходимости быстрого реагирования на значительные изменения факторов внешней среды
Уровень рискованности деятельности	Уровень рискованности, который является приемлемым для банка	Высокий уровень рискованности деятельности по причине значительного изменения факторов внешней среды
Уровень информационной поддержки управленческих решений	Стандартный уровень информационной и аналитической поддержки управленческих решений	Значительное увеличение объема расчетов, аналитических и диагностических процедур

Источник: составлено по материалам [33].

Основной целью совершенствования системы управления банковскими рисками является достижение и поддержание устойчивого и эффективного развития банков за счет противодействия негативному влиянию факторов внешней и внутренней среды и минимизации последствий такого влияния, что показано в таблице 1.3.

Таблица 1.3 - Характеристика современной концепции управления банковскими рисками

Элементы	Характеристика
Цель	Достижение устойчивого развития банков путем результативного противодействия негативному воздействию факторов внутренней и внешней среды
Задание	Улучшение управления банком с помощью применения внешних инструментов влияния на эффективность управления банковскими рисками и внутренних организационно-экономических направлений управления рисками в условиях финансового кризиса
Объект	Риски, возникающие в процессе осуществления активно-пассивных операций банка и его хозяйственной деятельности
Субъект	Члены наблюдательного совета, исполнительных органов, руководители центров ответственности банка и другие работники банка, задействованные в управлении банковскими рисками, внешние антикризисные менеджеры, кураторы национального регулятора, специалисты, работающие в системе гарантированного возмещения банковских депозитов
Внешние направления реализации концепции	1) Риск-ориентированный банковский надзор 2) Дифференциация гарантированной суммы возмещения вклада физического лица в зависимости от уровня процентной ставки по депозиту 3) Дифференциация суммы календарного взноса в институты по гарантированному возмещению банковских вкладов (депозитов) физических лиц в зависимости от значения интегрального показателя оценки эффективности управления банковскими рисками
Внутренние направления реализации концепции	1) Страхование банковских рисков 2) Стратегия развития банка 3) Управление рисками по центрам ответственности банка

Источник: составлено по материалам [33].

Основание риск-ориентированного надзора способствует поддержанию стабильного функционирования банковской системы. Фокус внимания Центрального банка смещается с контроля за формальным выполнением кредитными организациями существующих пруденциальных требований в область эффективного риск-менеджмента с целью повышения уровня банковской ликвидности и капитала. Для развития риск-ориентированного направления зачастую используют интегральный показатель эффективности управления рисками. Данный показатель учитывает показатели достаточности капитала, рентабельности, ликвидности и качество активов, и показатель результативности управления рисками - качество управления рисками.

В настоящее время система управления банковскими рисками непосредственно связана с внедрением страхования банковских рисков. Успешное и эффективное взаимодействие банка и страховой компании может быть достигнуто путем согласования сторонами основных тезисов:

– Признание необходимости долгосрочных и значительных вложений для страхования банковских рисков.

– Ответственный подход к выбору формы взаимодействия и продукта, отвечающим основным задачам и целям сотрудничества.

– Наличие единого представления о дальнейшей стратегии развития банка на финансовом рынке.

Процесс управления рисками делится на идентификацию, оценку и мониторинг, контроль масштаба и концентрации, разработку мер по поддержанию оптимально допустимого баланса между доходностью и принимаемыми рисками, и на раскрытие информации о рисках и принимаемых мерах по их минимизации и контролю.

Повышение стандартов качества и эффективности системы управления банковскими рисками может быть достигнуто путем внедрения внутренних и внешних механизмов реализации современной концепции управления рисками в банковской сфере. Данная концепция в своей основе содержит следующие компоненты: переход на риск-ориентированный банковский надзор, дифференциация размера страхового взноса в зависимости от финансового состояния банка и эффективности системы риск-менеджмента; разграничение функции управления рисками по центрам ответственности, внедрение страхования банковских рисков и применение низкорискованной стратегии развития банка.

Резюмируя основные положения данного параграфа, необходимо отметить следующее. Анализ специфики современной системы управления рисками банковской деятельности позволил систематизировать и раскрыть содержание основных видов рисков банковской деятельности, анализируемых риск-подразделениями.

Дальнейшим логичным шагом представляется исследование влияния систем дистанционного банковского обслуживания на расширение профиля банковских рисков. Более подробно данные положения рассмотрены в следующем параграфе.

1.3 Влияние расширение профилей рисков дистанционного банковского обслуживания на банковскую систему Российской Федерации

Система дистанционного банковского обслуживания — это одна из инноваций, успешно внедренных банками по всему миру. Поэтому, оценивая риски дистанционного банковского обслуживания, нельзя не затронуть понятие «риски банковских инноваций».

Научная литература трактует понятие «риск банковских инноваций» следующим образом: опасность образования ущерба из-за реализации инновационных мероприятий; совокупность последствий, которые могут произойти в связи с осуществлением решений при инновационной деятельности; измеримая вероятность потери финансовых активов [61].

Определения сходятся в том, что риск банковских инноваций — это неблагоприятные последствия применения новых технологий и методов в банковской сфере.

Система управления рисками в коммерческом банке формируется под воздействием ряда внешних и внутренних факторов. К факторам внешней среды относятся:

а) Особенности современной макроэкономической среды, основными составляющими которой являются - состояние национальной экономики, денежно-кредитной политики, внутренней и внешней политики, степень государственного влияния, уровень социально-экономического развития.

б) Направление политики главного регулятора рынка банковских услуг, характеризующееся определением пределов риска, утвержденных

соответствующими нормативными актами, а также регулированием уровня ликвидности и ключевой ставки.

в) Постоянное развитие и повышение эффективности институтов финансовых рынков.

г) Наличие конкурентной среды на рынке банковских услуг.

К факторам внутренней среды можно отнести особенности и направление долгосрочной стратегии развития конкретного коммерческого банка.

Рассмотрим риски, возникающие в результате применения банками дистанционного обслуживания своих клиентов, и к их причинам.

Прогресс в области информационных технологий и рост числа способов сетевого взаимодействия между банком и клиентом усложняет и расширяет банковские риски. Информационный контур банковской деятельности меняется, в нем появляются новые элементы: каналы связи, провайдеры, клиенты «нового типа».

Можно выделить четыре основных источника рисков в системе дистанционного банковского обслуживания. К ним относятся:

– деятельность клиентов кредитной организации;

– деятельность исполнителей (то есть работников кредитной организации);

– использование информационных технологий;

– использование каналов связи между клиентом и кредитной организацией.

В дистанционном банковском обслуживании присутствуют две стороны: клиент и банк. Банк может и не участвовать в операции в прямом смысле, как это происходит в классическом банковском обслуживании. Однако он, пусть даже косвенным образом, участвует в совершении операции или предоставлении услуги. Выбор двух других источников риска объясняется следующим: информационные технологии — это способ передачи данных, а каналы связи (терминалы, смартфоны и пр.) — это средство коммуникации между клиентом и банком. То есть эти четыре стороны участвуют в процессе

дистанционного банковского обслуживания. Соответственно, причин возникновения рисков дистанционного банковского обслуживания может быть множество, но все они попадут в одну из четырех групп источников.

Дистанционное банковское обслуживание подвержено специфическим видам риска, к основным из них относятся: [63]

1) Изменение профиля кредитного риска.

Дистанционное предоставление банковских услуг упускает возможность дополнительной проверки клиента, поскольку лишает сотрудника банка визуального контакта с клиентом. Вместе с тем, сложности возникают и в вопросе проверки обеспечения/залога или составления договора кредита.

2) Изменение профиля стратегического риска.

Профиль стратегического риска изменяется в связи со снижением качества определения потребностей клиента среди предлагаемых банковских услуг и, следовательно, нецелесообразным распределением затрат при дистанционном обслуживании. Включение нерентабельных услуг и продуктов в программу обслуживания или бесплатное пользование программами дистанционного обслуживания ведет к значительному увеличению затрат и снижению прибыли банка.

Категория стратегических рисков также включает в себя неверно выбранные и неоправданно используемые системы технического обеспечения дистанционного банковского обслуживания, ввиду отсутствия необходимой компетенции либо допущения ошибок на уровне органов управления. Отсутствие проработанного стратегического плана развития банка приводит к подобным последствиям. В стратегическом плане развития банка должны быть продемонстрированы этапы внедрения, развития и использования технологий дистанционного банковского обслуживания. Качественно составленный план неразрывно связан с реальностью и учитывает вероятные изменения макроэкономических условий. Несоблюдение данных условий грозит значительными потерями уже на стадии разработки систем дистанционного банковского обслуживания.

Для исполнения намеченного стратегического плана необходимо достаточное обеспечение финансовыми и человеческими ресурсами, но это не всегда возможно. Факторы, влияющие на уровень стратегического риска, обычно связывают с ошибками, допущенными при определении дальнейшего вектора развития. В частности, при неверном выборе конкретных видов дистанционного банковского обслуживания, неправильном учете необходимых технических условий для его реализации или подборе провайдеров, повышается риск возникновения.

Внедрение дистанционной банковской системы, а также постоянная поддержка ее функционирования и развития, требует значительных расходов, в условиях их низкой рентабельности. В связи с чем проявление стратегического риска может возрастать, в том числе из-за необходимости отказа от услуг обслуживающих организаций-провайдеров и информационных систем, взаимодействующих с ними.

3) Операционный риск.

Основным условием увеличения операционного риска в результате применения дистанционного банковского обслуживания, выступают ошибки функционирования разного вида, например, разрывы соединения между пользователем и банком в процессе осуществления обслуживания. Кроме того, к факторам операционного риска относятся сбои в работе программного обеспечения, информационных систем, нарушения целостности передачи данных информационно-телекоммуникационных сетей, неточности в соблюдении протоколов использования, технические аварии у организаций-провайдеров. Данные уязвимости способны стать результатом возрастания объема сетевых атак, а также получение третьими лицами неправомерного доступа к информационным ресурсам банковской организации.

4) Риск потери деловой репутации.

Данный вид риска непосредственно связан с качеством защиты персональных данных клиентов – информации об их счетах, совершаемых операциях, а также наличием случаев массовой передачи банковских баз

данных сторонним лицам и организациям. Низкий уровень безопасности влечет за собой рост киберпреступлений в рамках дистанционного банковского обслуживания.

Ещё одним фактором, который негативно влияет на деловую репутацию банка, являются технологические ошибки в работе банковских приложений, из-за которых некоторые функции дистанционного банковского обслуживания становятся недоступны для клиента.

5) Правовой риск.

Изменение уровня правового риска в рамках дистанционного банковского обслуживания может иметь целый ряд причин.

Например, в результате нарушения поставщиками информационных услуг норм законодательства Российской Федерации, связанных с расположением провайдера или филиала банка в юрисдикции другого государства.

Следующей причиной возникновения данного вида риска выступает низкоэффективное устройство правовой деятельности банка, которая может привести к нарушениям в действиях персонала коммерческого банка при осуществлении взаимодействия с контрагентами. Данный пункт включает ошибки при составлении договоров на оказание услуг по работе с банковской информацией, в том числе особенности обозначения ответственности поставщиков услуг при неисполнении обязательств по обеспечению функционирования дистанционного банковского обслуживания, которые в свою очередь способны стать причиной неспособности банка выполнить свои обязательства перед клиентами.

6) Риск ликвидности.

Неполадки и сбои в программном обеспечении, регулирующем дистанционное обслуживание клиентов, либо в работе провайдеров, повышают риск ликвидности, так как могут привести к временной потере платежеспособности. Неполадки могут быть зафиксированы в результате

действий провайдера, работников финансовой организации либо форс-мажорных обстоятельств, не зависящих ни от одной из сторон.

В связи с вышеизложенным, банкам необходимо ответственно подходить к выбору обслуживающих организаций, в частности провайдеров, так как в настоящее время качество работы удаленных сервисов приобретает критическую важность для клиентов. Вследствие возрастает потребность в высоком уровне безопасности, надежности сети и добросовестности сотрудников. Помимо вышеуказанных видов рисков необходимо выделить и киберриски.

Вследствие развития системы дистанционного банковского обслуживания перечень основных принципов управления рисками подвергся изменениям, в него стали включать следующие риски:

- безопасности;
- обезличивания индивидуальности;
- отмывания денег;
- хищений персональных данных;
- мошенничества со счетами;
- отрицания операций.

Более того, еще появились риски, возникающие в связи с компьютерной обработкой данных, такие как риски:

- ошибок;
- непредусмотренного раскрытия информации;
- прерывания транзакций;
- мошенничества;
- неэффективного планирования.

Вопрос исследования банковских рисков в условиях дистанционного банковского обслуживания ставится многими мировыми банками. Банк Нидерландов в процессе изучения теоретической базы основных рисков, с которыми сталкиваются представители отрасли, выделяет следующие «новые риски» [21]:

– риск контролируемости (причина возникновения недостаточные функциональные характеристики контрольных систем);

– риск управляемости (причиной возникновения которого является неудовлетворительная гибкость банковских ИТ);

– риск целостности (данный вид риска обусловлен недостаточной полнотой, точностью поступающей банковской информации, а также возможной несвоевременностью поступления);

– риск эксклюзивности (возникает в связи с низким уровнем защищенности персональной информации и банковских данных);

– риск пользователя (риск, причиной которого является возможное неправильное использование системы дистанционного банковского обслуживания со стороны клиента).

Самостоятельно разработанная классификация банковских рисков была предложена и в США Управлением контроля денежного обращения. В рамках данной классификации были выделены следующие виды рисков, связанные с дистанционным банковским обслуживанием (электронными банковскими операциями) [85]:

– риски, возникающие в результате выбора некорректной стратегии выбора деловых операций;

– правовые риски;

– риски поддержания конфиденциальности банковской информации;

– риски, связанные с планированием непрерывности банковских операций;

– риски, связанные с подтверждением прав пользователя;

– риски компьютерных преступлений и отмывания денег.

Проведя анализ различных классификаций рисков дистанционного банковского обслуживания, автор выделил следующий перечень специфических рисков, которые присущи только электронным банковским операциям:

а) Риск информационной безопасности. Поддержание и усиление безопасности является одним из главных сдерживающих факторов развития сферы дистанционного банковского обслуживания клиентов. При этом уровень технических систем находится на достаточно высокой ступени.

б) Риск низкой доступности восприятия интерфейсов. Большинство систем дистанционного банковского обслуживания ориентировано на использование являются продвинутыми пользователями, таким образом, охват их потенциального использования снижается.

в) Риск технических сбоев в работе. Пользователи отмечают, что в работе с системами интернет-банкинга часто сталкиваются с ситуациями, когда проводятся профилактические мероприятия, предоставляется неактуальная информация, происходят сбои в работе и возникают сложности со входом. Решение данной проблемы является комплексным и требует значительного количества времени.

г) Риск кибер-мошенничества. Банк, использующий систему дистанционного банковского обслуживания, может сталкиваться с ситуациями, при которых заявки, приходные ордеры и запросы поступают не от клиентов, а со стороны злоумышленников. К мошенничеству с использованием электронных средств относятся все случаи мошенничества с использованием банковских переводов или Интернета. Особенно распространен фишинг - использование мошенником электронной почты, текстовых сообщений, телефонных звонков или других методов связи для получения банковских реквизитов жертвы.

Механизм управления банковскими рисками базируется на трех основных уровнях: международном, макроуровне и микроуровне. На основании этого автором исследования разработана классификация уникальных рисков, дистанционного банковского обслуживания, отраженных в таблице 1.4, которые отличаются наименьшей разработанностью в экономической литературе на макро- и микроуровне банковской системы (международный

уровень не представляется возможным для модернизации в текущих геополитических условиях).

Таблица 1.4 – Авторская классификация уникальных рисков дистанционного банковского обслуживания

Уровень системы управления рисками ДБО	Уникальный риск дистанционного банковского обслуживания	Описание природы риска
Макроуровень	Риск недоверия к использованию банками цифровых технологий	Финансовые технологии продолжают стремительно развиваться, готовность и способность человека доверять этим цифровым инновациям, чтобы полностью понимать и пользоваться ими, является важнейшим фактором для дальнейшего развития в области банковской цифровизации
	Риск недостаточного банковского надзора в сфере	Весь перечень мероприятий Центрального Банка, направленных на модернизацию надзорной банковской деятельности за кредитными организациями, обязан приобрести наиболее комплексный характер, а также непрерывно совершенствоваться на каждом уровне системы, в первую очередь для уменьшения проявления негативных финансовых последствий для пользователей цифровых услуг кредитных организаций банковского сектора страны
	Риск повышения уровня монополизации банковского сектора	Получение конкурентных преимуществ за счёт развития омниканального банкинга требует от кредитных организация существенного размера капитала, которым обладают только крупнейшие игроки рынка, а построение собственной банковской экосистемы доступно только самым крупным банкам России
Микроуровень	Риск применения некорректной моделей оценки	В качестве основополагающего критерия в цифровизации банковской деятельности выступает внедрение корректных моделей количественной оценки не только финансовых, но и нефинансовых рисков
	Риск недостаточной цифровизации банковской инфраструктуры бэк-офиса	При высоком уровне цифровизации предоставления банковских продуктов и услуг, на данном этапе имеется значительная необходимость в повышении автоматизации бэк-офиса, в том числе, в части управления рисками
	Риск кибер-мошенничества	Основополагающим условием, которое предполагает наиболее полное обеспечения гарантий непрерывной работоспособности информационно-технологических систем банка выступает их системная надежность и устойчивость при осуществлении возможных киберпреступлений со стороны злоумышленников

Источник: составлено автором.

Подробное описание предложений по минимизации данных рисков путём модернизации системы управления рисками дистанционного банковского обслуживания как на макроуровне, так и на уровне кредитной организации предложено автором во 2 и 3 главах диссертации.

Возникновение новых разновидностей угроз непосредственно связано с совершенствованием технологий. Эксперты исследовательского центра по вопросам политики и экономики Brookings Institution (США) пришли к выводу, что появление нового поколения беспроводных сетей связи может снизить уровень защищенности соединения. Скорость передачи данных посредством сетей нового пятого поколения будет увеличена в 20 раз по сравнению с текущими значениями сетей 4G/LTE, продолжительность задержки снизится в 5 раз. Помимо изменений в качестве и скорости соединения, сети станут более децентрализованными и менее зависящими от физического оборудования. В подобных условиях система реагирования и защиты от атак также должна использовать актуальные технологии и соответствовать последним стандартам качества для противостояния возможным угрозам [81].

Существенной проблемой остается возможность утечки информации, в связи с чем кредитные организации и их клиенты рискуют понести значительные убытки.

Основным фактором риска в данном вопросе, как и в большинстве других, является человеческий фактор. Утечки данных чаще происходят в связи с действиями сотрудников, а не наличием несовершенств в системах киберзащиты. Около 69% организаций называют ключевой причиной утечки информации наличие правонарушителей внутри компании [74].

Нарушение конфиденциальности и сохранности данных не всегда вызвано преступными мотивами, часто утечки информации происходят в виду невнимательности, безответственности, недостаточного уровня компетенции сотрудника в вопросах киберграмотности либо по вине клиента.

В настоящее время в качестве основных видов мошенничества в рамках дистанционного банковского обслуживания наиболее распространены техники

социальной инженерии. Схемы составляются посредством изучения сложившихся моделей поведения людей, привычек, оформившихся стереотипов. Для манипулирования используются психологические и социологические приемы. Воздействие может быть произведено путем внушения чувства страха, воодушевления возможностью получения выигрыша или компенсации. Потеря бдительности клиента приводит к утечке конфиденциальных данных и финансовым потерям.

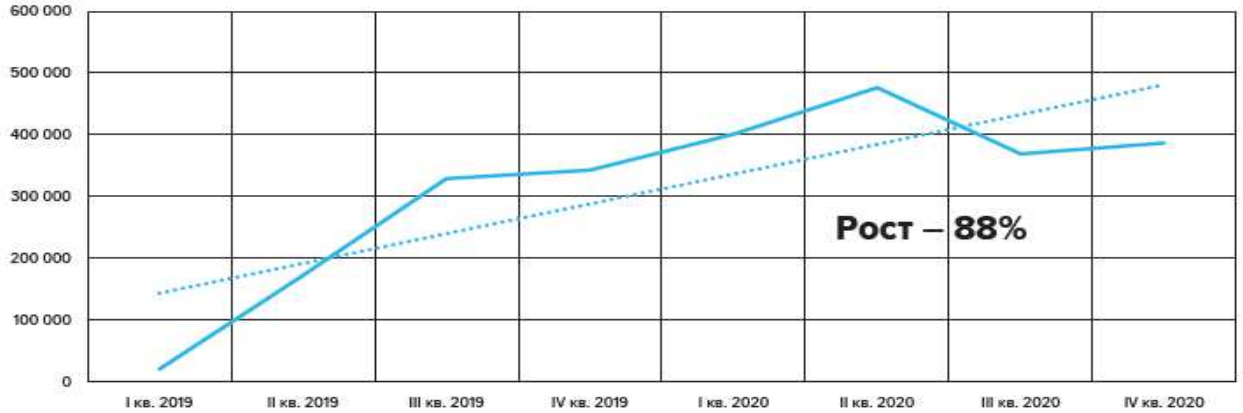
Несмотря на многообразие возможных сценариев, злоумышленники преследует три основные цели:

а) Получить доступ к счетам клиента посредством полученной конфиденциальной информации.

б) Заставить клиента перечислить денежные средства на счет мошенников самостоятельно.

в) Получить доступ к счетам клиента посредством использования приложения удаленного управления.

В марте 2020 года в условиях распространения коронавирусной инфекции в России был зафиксирован всплеск числа кибератак на сервисы дистанционного банковского обслуживания, как видно на рисунке 1.2. Введение режима удаленной работы большинством организаций кредитно-финансовой сферы, а также возросшее использование банковских приложений и онлайн сервисов, в условиях самоизоляции, может быть главной причиной такого роста.



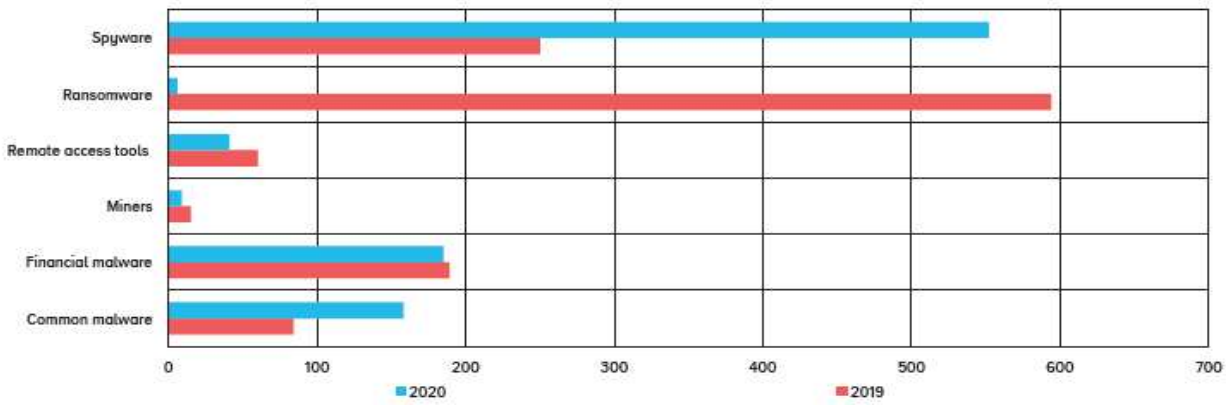
Источник: составлено автором на материалах [57].

Рисунок 1.2 - Общее количество атак на клиентов кредитных организаций, 2019-2020 годы

Соответственно в этот же период Банк России зафиксировал: расширение разнообразия вредоносного программного обеспечении (далее - ВПО), увеличение числа мошеннических рассылок (фишинговых рассылок) и оживление хакерского сектора, мошеннических группировок.

В 2020 году было зафиксировано 968 компьютерных атак, содержавших 1300 образцов ВПО. Наиболее популярным видом распространения ВПО остается использование электронной почты. В 2019 году лидирующую позицию в структуре исследованного объема ВПО занимали программы-шифровальщики (50%), шпионское ПО составляло порядка 20% - рисунок 1.3. В 2020 году доля шпионского ПО увеличилась более чем в два раза и составила 58%, на втором месте оказалось финансовое ВПО (13%).

В 2019–2020 годах самой значимой угрозой для клиентов организаций кредитно-финансового сектора была группа злоумышленников RTM. Кроме того, в 2019 году был отмечен рекордный рост запросов относительно участившихся случаев обнаружения программ-шифровальщиков. Данные программы в качестве вложения либо ссылки на скачивание рассылались по электронной почте, для активации необходимо было открыть файл или перейти по ссылке.



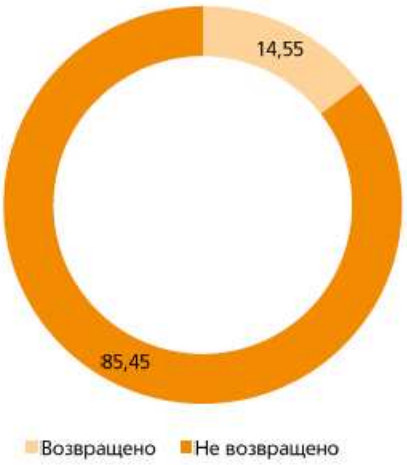
Источник: составлено автором на материалах [101].
Рисунок 1.3 - Распределение ВПО по классам, 2019-2020 годы

В 2020 году массовых кампаний больше не отмечалось и выявлялись лишь отдельные факты получения рассылок с приложением программ-шифровальщиков.

В 2019–2020 годах было получено 17 сообщений о попытках взлома банкоматов. В большинстве случаев (44%) использовались специальные приспособления для вскрытия устройства в целях извлечения денежных средств из банкоматных кассет. Помимо взлома банкоматов злоумышленники часто прибегают к кэш-треппингу, суть которого заключается в физической блокировке системы выдачи наличности. Около 32% случаев связаны именно с этим видом мошенничества.

За 2020 год банки возместили потерпевшим клиентам сумму в размере 935 млн руб. (около 15 процентов), что отражено рисунке 1.4. Низкий уровень возмещения можно объяснить тем, что в результате противоправных действий клиенты сами нарушают условия кредитного договора с банками, которые предусматривают необходимость сохранения конфиденциальности платежной информации. Центральный Банк Российской Федерации планирует изменение процедуры компенсации похищенных средств гражданам.

Безопасность в сфере информационных угроз занимает значительную роль, и её значение для финансовых институтов в ближайшее годы будет только возрастать. Приоритетной задачей является сохранение баланса между безопасностью данных и комфортным использованием банковских приложений. Благодаря трансформации систем риск-менеджмента банки смогут обеспечивать сохранность и безопасность данных, что значительно повысит доверие к банковской системе Российской Федерации в целом.



Источник: составлено автором на материалах [101].
Рисунок 1.4 - Возмещение пострадавшим клиентам, проценты

Наряду с безусловными преимуществами дистанционного банковского обслуживания для банков и их клиентов при этом видоизменяются традиционные и появляются новые виды рисков. В связи с этим важным аспектом изучения данной проблемы является влияние развития угроз риска информационной безопасности на устойчивость банковского сектора в целом.

Финансовую стабильность рассмотрим, как результат деятельности субъектов банковской отрасли по минимизации величины отклонений временной функции фактических показателей банковского сектора за анализируемый период времени от прогнозных значений, характеризующих равновесные значения этих показателей на среднесрочную перспективу. При этом равновесные значения показателей финансового рынка вычисляются на основе ежеквартальных данных за период наблюдения, равный предшествующему плановому периоду.

Математическая модель оценки стабильности банковского сектора России будет иметь вид как показано в формуле (1)

$$SI\ (t) = \sqrt{\frac{1}{s}\sum_{k=t-s}^{t-1} d(k)}\ , \qquad (1)$$

где SI (t) - индекс стабильности финансовых рынков;

t - период анализа;

s - период оценки (s=18 месяцев, 6 кварталов);

d(k) - ежемесячный прирост показателя банковского сектора.

При этом d(k) вычисляется по формуле (2)

$$d(k)=(x_k-y_k)^2, \qquad (2)$$

где $(x_k-y_k)^2$ - величина среднеквадратического отклонения фактических значений y_k от трендовых x_k.

При недостаточном объёме информации о методиках планирования показателей, необходимо опираться на понимание того, что для предшествующих периодов существует некоторая равновесная модель и она влияет на соответствующий уровень регулирования системы, и позволяет целесообразно моделировать прогнозы, в соответствии с результатами использования этой модели планирования.

Таким образом, получим функцию SI (t), которая определяет значение среднекватратического отклонения фактических значений показателей от трендовых за период, в котором оценивается качество возможностей банковской системы риск-менеджмента противостоять угрозам кибермошенничества. Значения временной функции будут являться количественными индикаторами финансовой стабильности банковского сектора. Качественная же оценка стабильности будет основываться на этих количественных индикаторах и состоять из 5 уровней (по понижению уровня стабильности) и иметь шаг, равный 2%, как указано в таблице 1.5.

Таблица 1.5 - Уровни стабильности банковской системы

Уровни стабильности	Критерии
Высокий	$0\,\% \leq SI\,(t) < 2.0\,\%$
Выше среднего	$2.0\,\% \leq SI\,(t) < 4.0\,\%$
Средний	$4.0\,\% \leq SI\,(t) < 6.0\,\%$
Ниже среднего	$6.0\,\% \leq SI\,(t) < 8.0\,\%$
Низкий	$8.0\,\% \leq SI\,(t)$

Источник: составлено автором.

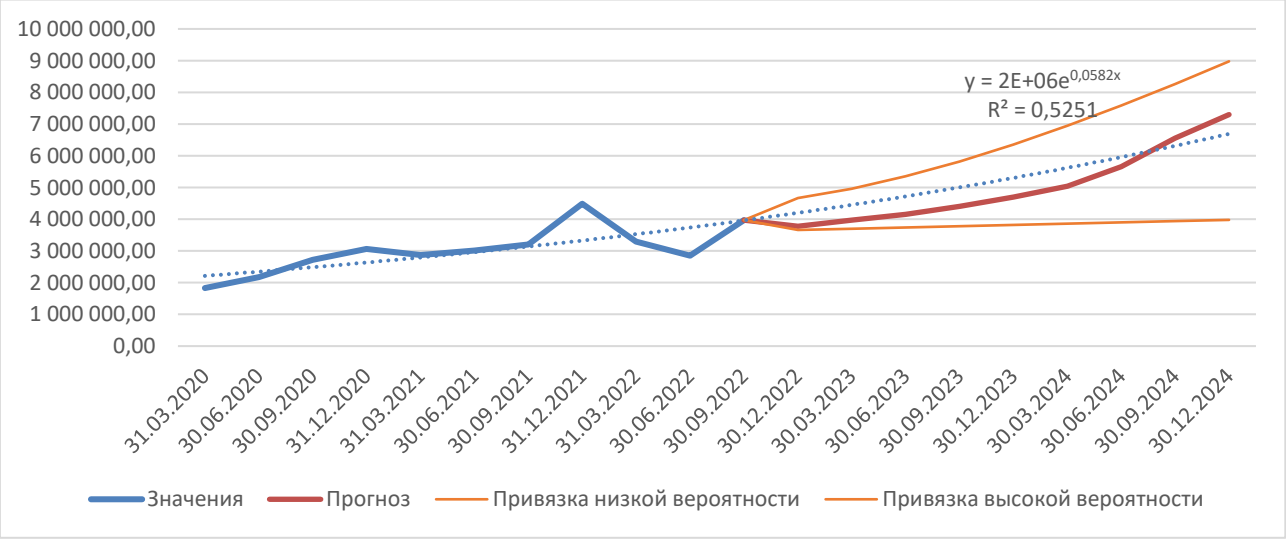
Выбор шага выбран согласно рекомендациям Базель III, отклонение фактических значений показателей от равновесного уровня в течение периода 4-х кварталов в размере 2,0 п.п. служит сигналом для применения антициклической надбавки [80]. Следовательно, годовое отклонение циклической компоненты от равновесного уровня может составить 8,0 п.п.

Уровень глубины анализа устойчивости может быть повышен на основании поведения самой функции SI (t). Эффективное управление устойчивостью системы можно наблюдать при монотонном убывании функции. Рост функции говорит о переходе в более негативное состояние управления:

прогноз и факт значительнее расходятся, по сравнению со средними показателями среднеквадратичного отклонения за исследуемый период.

Апробация разработанных индикаторов и критериев оценки финансовой стабильности применяется к российскому банковском рынку на основе ежеквартальных данных об объемах операций, совершенных без согласия клиентов финансовых организаций, за период 2014-2022 гг. Выбор периода анализа обусловлен наличием официальных данных Банка России, находящихся в открытом доступе. Автором исследования выдвинута гипотеза о том, что с ростом объёма использования цифровых каналов обслуживания клиентов возрастает и показатель риска кибер-мошенничества, негативно влияющая на показатель финансовой стабильности банковского сектора [69].

С помощью построения эконометрической модели был спрогнозирован показатель объема несанкционированных операций в отношении клиентов кредитных организаций. Построение прогноза включает 3 сценария, различающихся моделью роста: линейной, экспоненциальной и логарифмической. Оптимальным сценарием по результату прогнозирования была принята экспоненциальная модель роста, согласно которой объём несанкционированных операций в 2023 году возрастёт на 23%, а в 2024 году на 37%. Расчёт показан в приложении В, а результат в виде графика модели отображён на рисунке 1.5.



Источник: составлено автором.

Рисунок 1.5. Прогноз объема несанкционированных операций, тыс. руб.

Для подтверждения возможности технологического развития банковского обслуживания влиять на уровень мошеннических операций в информационной сфере обслуживания клиентов необходимо провести исследование текущей корреляции объема несанкционированных операций и объёма IT затрат банков. Проведя необходимые расчёты при помощи инструментария программы EXCEL, используя статистические данные автоматизированной системы обработки инцидентов (АСОИ ФинЦЕРТ) и объёмы бюджетов на инновационное развитие банков, мы получили значение корреляции равное 0,7937, так как оно входит в диапазон от 0,7 до 0,9, следовательно, значимость данного фактора влияния – высокая, расчёты приведены в приложении Б.

На основании данной корреляции была построена эконометрическая модель, показывающая изменение динамики финансовой стабильности банковского сектора, под действием фактора противозаконных операций со счетами клиентов, вызванных развитием использования дистанционного обслуживания. Нисходящий характер графика подтверждает гипотезу о том, что с ростом объёма использования цифровых каналов обслуживания клиентов возрастает и показатель риска кибер-мошенничества, негативно влияющая на показатель финансовой стабильности банковского сектора, расчёты приведены в приложении Г.

Источник: составлено автором.

Рисунок 1.6. Динамика финансовой стабильности банковского сектора, в процентах (на основании соотношения объема несанкционированных операций и объёма IT затрат банков)

На основании статистико-математических и эконометрических методов была сформулирована и доказана гипотеза о том, что с ростом объёма использования цифровых каналов обслуживания клиентов возрастает и показатель риска кибер-мошенничества, негативно влияющий на показатель финансовой стабильности банковского сектора.

На основании проведённого эконометрического исследования можно сделать вывод, что с ростом объёма использования цифровых каналов обслуживания клиентов возрастает и показатель риска кибер-мошенничества, негативно влияющий на показатель финансовой стабильности банковского сектора, наблюдается превышение отклонение фактических показателей финансовой стабильности от нижней границы критерия ($8.0 \leq SI(t)$). Тем не менее, анализ графика, представленного на рисунке 1.6 показывает, в течение анализируемого периода финансовая стабильность данного сегмента рынка начала улучшаться вплоть до первого квартала 2022 года, что может быть связано со значительным изменение геополитических факторов, способных оказать влияние на проявления риска информационной безопасности.

Данная тенденция сигнализирует о необходимости повышения качества регулирования финансовой стабильности банковского сектора в разрезе использования систем дистанционного обслуживания путём модернизации системы управления рисками.

Таким образом, в данном параграфе рассмотрены факторы, оказывающие влияние на расширение профилей рисков дистанционного банковского обслуживания. По результатам выявлено, что внедрение и использование технологий дистанционного банкинга не только вносит изменения в профиль стандартных банковских рисков, но и формирует специфический перечень банковских рисков, которые присущи только электронным банковским операциям.

На основании выделения характерных особенностей отечественного и международного опыта управления риском разработана новая классификация рисков, связанных с расширением использования технологий дистанционного

обслуживания банковских клиентов. Предложенная классификация предоставила возможность для обоснования потребности модернизации системы управления рисками дистанционного банковского обслуживания на макро- и микроуровне банковской системы.

С учетом основных результатов по первому разделу диссертации (приведены ниже) в следующей главе представляется целесообразным исследовать систему управления рисками дистанционного банковского обслуживания на макроуровне на основании анализа российской и зарубежной практики.

Анализ взглядов отечественных и зарубежных ученых на вопросы сущности, роли и экономического содержания системы дистанционного банковского обслуживания позволил сделать вывод об отсутствии единого толкования рассматриваемого понятия, что усложняет его понимание и практическое применение. Данный факт потребовал считать дистанционное банковское обслуживание собирательным понятием, которое складывается из основных специфических характеристик данного вида банковских услуг.

По результатам рассмотрения форм и основных принципов функционирования систем дистанционного банковского обслуживания были выявлены основные этапы создания данных систем в коммерческих банках, а также проанализированы преимущества использования технологий удаленного обслуживания и их недостатки, которые, в частности, сопряжены с рисками банковской деятельности.

Анализ специфики современной системы управления рисками банковской деятельности позволил систематизировать и раскрыть содержание основных видов рисков банковской деятельности, анализируемых риск-подразделениями.

Рассмотрены факторы, оказывающие влияние на расширение профилей рисков дистанционного банковского обслуживания. По результатам было выявлено, что внедрение и использование технологий дистанционного банкинга не только вносит изменения в профиль стандартных банковских

рисков, но и формирует специфический перечень банковских рисков, которые присущи только электронным банковским операциям.

На основании выделения характерных особенностей отечественного и международного опыта управления риском была разработана новая классификация рисков, связанных с расширением использования технологий дистанционного обслуживания банковских клиентов. Классификация отличается от имеющихся не только разделением на уровни банковской системы, но и выделением новых, наиболее ярко проявляющихся рисков дистанционного банковского обслуживания как на уровне банковской системы, так и, непосредственно, кредитной организации. В соответствии с этим выделены шесть уникальных рисков, минимизация которых необходима для дальнейшего развития банковской отрасли. Предложенная классификация предоставила возможность для обоснования потребности модернизации системы управления рисками дистанционного банковского обслуживания на макро- и микроуровне банковской системы.

На основании проведенного эконометрического исследования была подтверждена гипотеза о то, что с ростом объёма использования цифровых каналов обслуживания клиентов возрастает и показатель риска кибер-мошенничества, негативно влияющий на показатель финансовой стабильности банковского сектор.

Данная тенденция сигнализирует о необходимости повышения качества регулирования финансовой стабильности банковского сектора в разрезе использования систем дистанционного обслуживания путём модернизации системы управления рисками.

Глава 2
Анализ системы управления рисками дистанционного банковского обслуживания на макроуровне

2.1 Влияние инновационных технологий дистанционного банковского обслуживания на процесс модернизации системы управления рисками

Внедрение инновационных технологий в финансовую и банковскую отрасль является стимулом для развития финансового рынка. Цифровая трансформация в данной сфере предполагает применение новых технологий, которые направлены на увеличения качества предоставления услуг и взаимодействия участников кредитного рынка друг с другом, а также на увеличение числа транзакций.

На сегодняшний день термин «инновация» получает все большее распространение в научной литературе, так как мы живем в период активного развития научно-технического прогресса и постоянного появления новых технологий. Под инновацией подразумевается процесс создания нового продукта или новой технологии, а, следовательно, и нового уклада жизни, так как эта инновация будет сопровождать нас в течение определенного времени, развиваясь и трансформируясь [29].

Трансформация банковского сектора тесно взаимосвязана от разработки современных инновационных технологий банковского обслуживания, а создание и модернизация данных технологий, в свою очередь, обуславливаются потребностями воспроизводственного процесса и курсом на создание «цифровой» экономической системы государства.

Основной целью внедрения банковских инновационных технологий выступает создание конкурентных преимуществ и увеличения экономической эффективности кредитных организаций. Данные экономические параметры лежат в основе развития современной банковской отрасли.

В связи с развитием цифровой экономики и возрастанием роли банков в качестве основных посредников, кредитными организациями был взят курс на продвижение комплексных продуктов. Вместе с появлением данных продуктов меняется внутренняя структура основных банковских институтов. Для расширения сферы использования инновационных продуктов необходимо организовать специальную среду, которая бы соответствовала современному уровню развития банковской сферы.

Разработка инновационных технологий и своевременное обновление имеющихся продуктов становится приоритетным вектором развития для банковских организаций в условиях постоянного повышения требований со стороны потенциальных клиентов. Стремление к оптимизации капитала, сокращению операционных расходов, а также использование наиболее прогрессивных моделей ведения бизнеса является отличительной особенностью современной банковской системы.

В таких условиях банки готовы вкладывать больший объем ресурсов в модернизацию технологий для качественной перестройки бизнес-процессов с целью выработки наиболее точной и оперативной системы реагирования на запросы клиентов в рамках осуществления дистанционного банковского обслуживания [22].

Использование дистанционных банковских услуг клиентами ведет к снижению операционных издержек банка и поэтому является приоритетным направлением. Автоматизация части процессов сокращает временные затраты и позволяет перевести задействованных ранее специалистов для работы в сферах, требующих личного взаимодействия с клиентом.

На основании анализа научной и экономической литературы можно выделить несколько критериев, по которым можно классифицировать формы банковских инноваций, проводимые кредитно-финансовыми институтами на современном этапе. Результаты данной классификации представлены автором в таблице 2.1:

Таблица 2.1 - Классификация банковских инноваций

Критерии классификации	Виды инновации
Время	Новые и оперативные
Новизна	Техническая и потребительская
Объект взаимодействия	Продукт, услуга, бизнес-процесс
Скорость внедрения	Быстрые, нарастающие, скачкообразные и равномерные
Влияние на потребителя	Функциональное и фундаментальное
Задача	Улучшить функциональность банковских продуктов, улучшить безопасность предоставляемых услуг
Уровни распространения	Международный, региональный и локальный

Источник: составлено по материалам [39].

Важным фактором, оказывающим влияние на развитие дистанционного банковского обслуживания, является уровень финансовой грамотности, адаптивности и образа жизни населения региона внедрения. Помимо данных условий важную роль играет тип поведения банка в рамках активной конкурентной борьбы.

Конкурентным преимуществом при внедрении инновационных технологий является участие в процессах глобализации.

Глобализация является одним из важных и необходимых факторов при внедрении банками инновационных технологий и новых продуктов, что позволит им выстоять в конкурентной борьбе.

Технологии стали неотъемлемой часть широкого спектра банковских услуг, таких как – оплата товаров и услуг, выдача ссуд, открытие сберегательных счетов, услуги страхования, помощь в инвестировании. Таким образом, прослеживается четкая ориентация на удовлетворение разнообразных нужд клиента. Комплексы финансово-информационных решений могут быть разработаны под конкретные банки и финансово-технические компании, предоставляющие узкий спектр услуг, с учетом специфики их деятельности. Модернизация финансового рынка невозможна без трансформации подходов регулятора.

К основным целям развития финансовых технологий следует отнести:

– стимуляция развития конкуренции;

– качественный рост и расширение ассортимента финансовых услуг;

– работа над снижением рисков и издержек;

– создание системы безопасности финансовых технологий;

– повышение общего уровня развития технологий в России.

В результате международного обмена опытом в сфере банковской деятельности российскими банками были внедрены инновационные стратегии, способствующие повышению эффективности функционирования и управления технологическими процессами [40]:

– Выявление проблемных сфер развития в процессе осуществления мониторинга банковской среды;

– поддержка нововведений в инновационной сфере;

– выработка стратегий, включающих в себя комплекс скоординированных коллективных действий, с целью достижения поставленных задач.

Банковские инновации представляют собой продукт, созданный для расширения клиентской базы и поддержания уже имеющейся заинтересованности. Инновационные банковские технологии главным образом являются частью операционной сферы взаимодействия банка и клиента и выражаются в своевременном оказании необходимых услуг и предоставлении электронных ресурсов.

Классификация банковских инноваций позволяет представить количество этапов, необходимых для создания и внедрения нового продукта, впоследствии способного привлечь новых клиентов и повысить эффективность работы банка.

Таким образом, инновационные технологии, применяемые в банковской сфере, повышают финансовую независимость кредитной организации, благодаря оптимизации основных процессов, повышению качества предоставления услуг, снижению операционных расходов.

Важным условием конкурентной борьбы с высокотехнологическими компаниями для коммерческих банков выступает соблюдение общемировых технологических тенденций по развитию FinTech компонентов: роботизация, геймификация, преобладание технологий Big Data, а также управление рисками информационного сектора и создание стратегии, ориентированной на трансформацию бизнес-процессов, учитывая развитие цифровой экономики.

Анализируя инновационные финансовые технологии, Банк России выделил перечень наиболее перспективных, которые могут существенно улучшить процессы банковского обслуживания клиентов и управления банковскими рисками. Данными технологиями являются:

- «Big Data» и аналитика больших данных (разнообразные средства, способы и подходы к обработке структурированных и неструктурированных видов данных с целью проведения анализа под конкретные запросы и цели) [72].

- Мобильные технологии (мобильный банкинг, который дает возможность оперативно получать актуальную информацию и осуществлять управление средствами на счете в банке посредством использования сотового телефона либо планшета).

- Искусственный интеллект («искусственный интеллект» и технологии машинного обучения широко применяются банками при оценке кредитных рисков и в связанных с ними направлениях, таких как распознавание случаев мошенничества, взыскание задолженностей и кредитный скоринг).

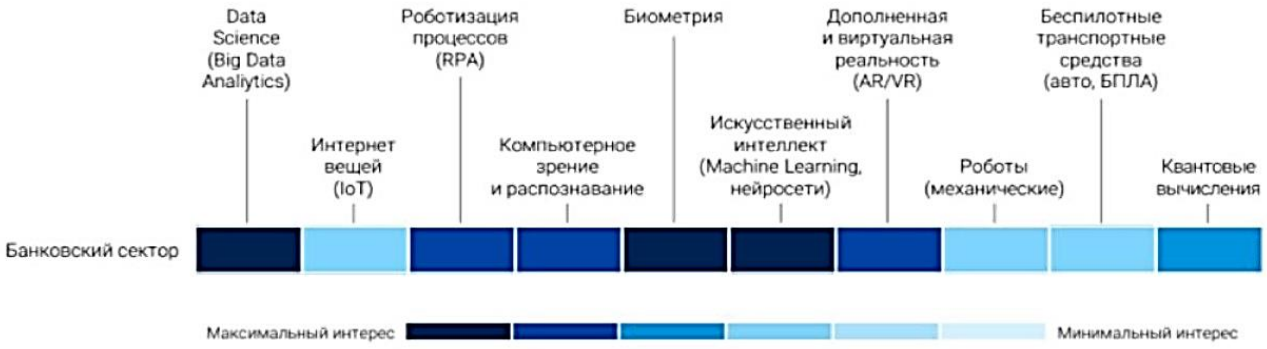
- Роботизация (позволяет существенно ускорить процесс проведения банковских операций, увеличить производительность бэк-офисных и фронт-офисных процедур в банке, снизить сроки обработки обращений клиентов, и, как следствие, значительно улучшить качество клиентского сервиса).

- Биометрия (применение технологии идентификации плательщика посредством чтения биометрических данных (оттиски лица и голоса, радужная оболочка глаза, отпечатки пальцев или геометрия поверхности ладони)).

Биометрическая идентификация сегодня проводиться по двум категориям признаков: физиологическим и поведенческим [53].

- Облачные технологии (технологии, которые дают возможность обеспечить виртуализацию процесса информационного взаимодействия между клиентами и работниками банка, с использованием облачных сервисов, что позволяет обеспечить конечным потребителям дистанционный доступ к услугам, вычислительным и прикладным ресурсам посредством сети Интернет).

По результаты исследования KMDA «Цифровая трансформация в России» было выявлено, что российские компании, специализирующиеся в работе в банковском секторе, проявляют наибольший интерес в применении или активно применяют среди прочих такие технологии, как большие данные, искусственный интеллект (Machine Learning и нейросети), биометрия. Фрагмент тепловой карты интереса российских компаний к цифровым технологиям представлен на рисунке 2.1.



Источник: Аналитический отчет «Цифровая трансформация России» [96].
Рисунок 2.1 – Фрагмент тепловой карты интереса российских компаний к цифровым технологиям по результатам исследования KMDA в 2020 г.

Искусственный интеллект (далее - ИИ) для банковского сектора открывает широкие возможности для повышения качества обслуживания клиентов, демократизации финансовых услуг, повышения кибербезопасности и защиты прав потребителей [3], а также усиления управления рисками.

Примеры использования организованы в три категории, выделяя потенциальные области возможностей для банковского сектора.

а) Повышение качества взаимодействия банк-клиент: голосовой банковский помощник, предварительные консультации робота-помощника, аутентификация по биометрическим данным, разделение клиентов по сегментам (например, с помощью настроенного веб-сайта для обеспечения наиболее релевантного предложения), целевые предложения клиентов.

б) Оптимизация внутренних банковских процессов: отчетность о работе систем, прогнозное обслуживание и поддержка принятия решений, автоматизация процессов сортировки документов и извлечения данных, система оценки кредитоспособности, организация работы с жалобами, обработка документов KYC (KnowYour Customer) и т. д.

в) Развитие систем безопасности и мониторинга рисков: проверка соблюдения существующих требований, система обращений по обнаружению аномалий, противодействие коррупции и отмыванию денег AML, прогнозирование пороговых значений пропускной способности, систем обнаружение мошеннических операций и их предотвращение, прогнозирование киберрисков, мониторинг платежных транзакций.

Одной из вероятных тенденций в модернизации российского банковского сектора выступает реализация инновационной технологии блокчейн. Блокчейн –распределенная база данных, в которой содержится информация относительно всех транзакций, проведенных участниками системы, сохраняющаяся в виде «цепочки блоков». Главным преимуществом данной технологии перед классическими банковскими транзакциями является полное отсутствие посредников, ввиду того что блокчейн не имеет центрального регулирующего органа, а операции контролируются самими участниками.

Блокчейн имеет высокие перспективы по внедрению в банковскую отрасль России, но для этого, в первую очередь, должны быть урегулированы все вопросы с законодательством.

Одной из основных тенденций развития банковского сектора в последние несколько лет можно выделить попытку создания крупнейшими кредитными организациями собственных экосистем.

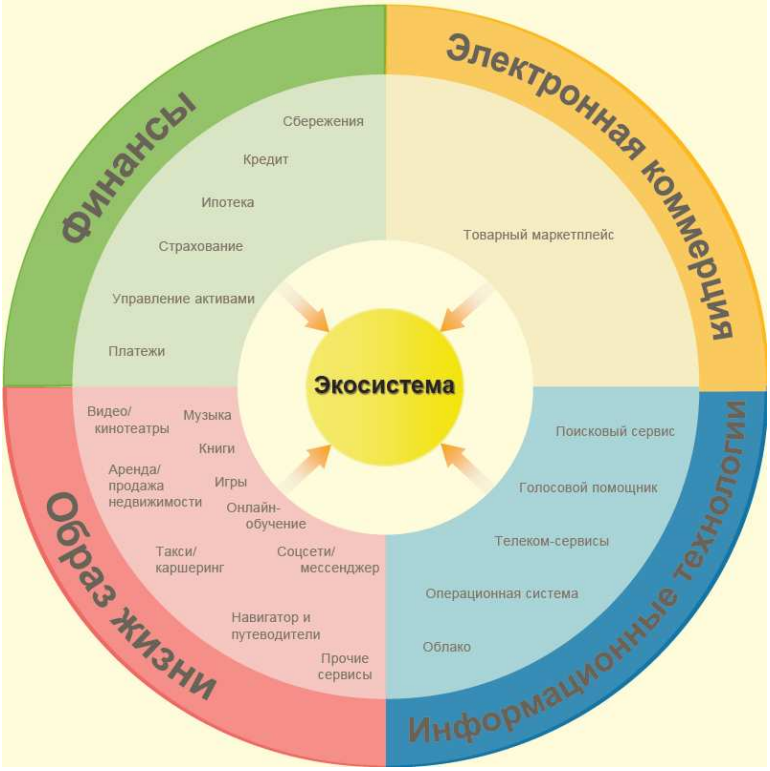
Для укрепления своих позиций банки подбирают оптимальные модели диверсификации своей деятельности.

Особенностью развития российских экосистем является лидирующая роль финансового сектора. Увеличиваются объемы инвестиций банковского сектора в компании, являющиеся частью новой цифровой экономики. Среди крупнейших банковских организаций отмечается ускорение темпов развития цифровых платформ и формирования собственных экосистем, объединяющих сервисы целого спектра отраслей экономики. ПАО Сбербанк является одним из первых банков, начавших работу в направлении цифровизации. С 2016 года компания работает над построением своей собственной экосистемы. Основой бизнес-модели является предоставление широкого спектра услуг (финансовых, образовательных, медицинских, развлекательных, услуг в сфере строительства, продажи потребительских товаров, транспортировки грузов) физическим и юридическим лицам [100].

Понятие финансовая экосистема включает в себя совокупность различных сервисов, предоставляемых группой компаний, которые позволяют клиентам пользоваться всеми необходимыми услуги в рамках одной цифровой платформы. В настоящее время конкурентная борьба идет за удержание лояльности основной массы клиентов к конкретной экосистеме. В ближайшие годы эта конкуренция будет расти. Организация, которая сможет привлечь в свою экосистему и удержать в течение длительного периода наибольшее количество клиентов – станет основным выгодоприобретателем [46].

На рисунке 2.2 представлена классификация сервисов, созданных для удовлетворения большинства основных ежедневных потребностей клиента, которые разделяются на четыре основных сферы активности.

Экосистему не следует путать с мобильным приложением банка, в котором доступны в основном только финансовые услуги. В экосистеме пользователям предоставляется доступ не только к финансовым продуктам, но и лайфстайл-сервисам, а также маркетплейсу.



Источник: составлено автором в статье [68].
Рисунок 2.2 - Структура стандартной цифровой экосистемы

Создание экосистемы требует значительных финансовых вложений, поэтому крупным банкам с многомиллионной клиентской базой, уже сложившейся репутацией и имиджем обычно проще достичь положительного результата, чем в случае с небольшими банками. Материальная нагрузка при создании экосистемы с нуля становится слишком большой для таких компаний, данные затраты могут не окупиться в будущем. По этой причине высоко развитые цифровые экосистемы распространены только среди крупнейших финансовых организаций [42].

Ведущие банки, которые образовывают свои цифровые экосистемы, в дальнейшем будут конкурировать за лояльность клиентов посредством качества проработки экосистем и многообразием ассортимента предоставляемых финансовых и нефинансовых услуг в рамках данных экосистем. Поэтому в ближайшем будущем основное внимание будет уделяться возможности внедрения лучших технологических решений из имеющихся и создания новых инновационных сервисов.

Более подробно использование инновационных банковских технологий разберем на примере ПАО Сбербанк.

В банковском секторе повсеместно внедряются технологии чат-ботов и робоэдвайзинга. Данные технологии позволяют информировать об особенностях продуктов и сервисов, осуществлять учет личных финансов, отвечать на вопросы пользователя без вмешательства сотрудника банка в режиме реального времени. Автоматизация взаимодействия банка с клиентом значительно снижает операционные расходы, позволяя доставлять необходимую информацию в любое удобное для клиента время.

Кроме того, использование технологий искусственного интеллекта в банковской системе позволяет обработать большие объемы данных, оценить платежеспособность и кредитный рейтинг клиента, а также оформить одобрение на выдачу кредита. В ПАО Сбербанк уже используется технология, позволяющая за семь минут создать цельный финансовый портрет клиента при одобрении либо отклонении решения о выдаче займа [94].

ИИ способен провести отбор кандидатов на получение займа и отсеять 1500 претендентов всего за 9 часов. Важным фактором эффективности работы систем, основанных на технологиях ИИ, является способность к самообучению и самосовершенствованию, а также возможность одновременной работы на многих устройствах.

Эффективным способом распространения технологий ИИ может стать внедрение их возможностей в структуру экосистемы для дальнейшего сближения с конечным потребителем, разрабатывая персонализированные наиболее подходящие клиенту предложения. В связи с этим был начат переход ПАО Сбербанк в форму глобальной экосистемы «Сбер», который длится больше пяти лет [94].

Искусственный интеллект может отвечать за целый спектр функций – таких как организация безопасных транзакций, создание и оптимизация процедур биометрической аутентификации, осуществление персональной помощи клиентам. Данную практику начали внедрять и менее крупные банки.

Реализация банкоматов с биометрией и идентификация по голосу и лицу в SberID — является дополнительным подтверждением того, ПАО Сбербанк является лидером в реализации инновационных финансовых технологий в банковском секторе, объединив экосистему финансовых и нефинансовых сервисов повседневной жизнедеятельности человека и бизнеса под единым узнаваемым брендом. Реализация данного проекта направлена на удовлетворение все возрастающих потребностей розничных клиентов, корпораций и государства.

В целях обеспечения полного контроля над своим информационно-технологическим пространством ПАО Сбербанк выстраивает бизнес-проекты на базе своей собственной облачной цифровой платформы, названной «Платформа V», в которой V - общепринятое обозначение скорости. Базовый функционал данной платформы реализуется на базе Open Source - открытых исходных решений, что позволяет ПАО Сбербанк оставаться технически самостоятельным. В настоящее время платформа вышла на новый высокий уровень надежности, повышению которого послужило внедрение технологии Autonomous Operations, призванной максимально устранить влияние человеческого фактора на процесс принятия операционных решений [94].

Помимо внутренних технологических сервисов ПАО Сбербанк стал выводить на рынок новые технологические банковские продукты. Этому способствовали:

- смена вектора развития общества и бизнеса, в частности, в сторону глобальной цифровизации в связи с постепенной цифровой трансформацией мира; особенно повлияли на эту тенденцию пандемия вируса Covid-19;

- радикальное изменение ИТ-ландшафта ПАО Сбербанк: был сформирован целый спектр высококлассных технологических решений, лучшие из которых предложены рынку.

ПАО Сбербанк превращается в наиболее активно развивающегося представителя на рынке виртуальных ассистентов. Осенью 2020 года ПАО Сбербанк выпустил виртуального помощника «Салют», чьи способности

значительно обширнее, по сравнению с традиционными мобильными приложениями. Он может использоваться для проигрывания фильмов или музыки, для заказа продуктов, предварительной записи к врачу и общения на самые разнообразные темы. «Салют» способен распознавать речь, текстовые сообщения, касания и даже различные жесты. Помимо виртуального помощника была выпущена линейка умных устройств, которая на данный момент состоит из ТВ-приставки SberBox и смарт-дисплея SberPortal. Работа данных устройств нацелена на расширение возможностей взаимодействия с умным помощником. Работа виртуального ассистента в рамках приложения Сбербанк Онлайн ограничивается финансовой спецификой, а SberBox и SberPortal расширяют возможности предоставления клиентам банка нефинансовых услуг. Сбер также планирует встраивать ассистента в устройства партнеров.

Начав работу виртуальной платформы SmartMarket для всех контрагентов, ПАО Сбербанк открыл для них возможность доступа к более чем ста миллионам пользователей собственной экосистемы. Сотрудничество между компаниями-разработчиками и банком взаимовыгодно и базируется на схеме распределения дохода.

Введение инновационных технологий в кредитный процесс, к примеру, 94% займов банк выдает без предоставления справок, а 97% заявок на кредиты обрабатываются в автоматическом режиме за пару минут, обеспечивает лидерство ПАО Сбербанк в сфере розничного кредитования (на его долю приходится 42,3% рынка, на долю жилищного кредитования - 54%). При этом развитие услуг «Кредитный потенциал» и «Покупай со Сбером» повлияло на наращивание розничного кредитного портфеля банка, который на 31 декабря 2021 года достиг 9 308 млрд рублей и по сравнению с предыдущим годом вырос на 18,1%. С помощью сервиса «Кредитный потенциал» в 2021 году было предоставлено 537 тыс. кредитов на сумму 136 млрд рублей, это в 5 раз превосходит результат 2020 года [94].

На период действия ограничительных мер 2020 - 2021 годов с помощью сервиса «Покупай со Сбером» запущен инновационный процесс кредитования покупок через терминалы торгового эквайринга, к которому уже подключено более 10 тысяч партнеров.

ПАО Сбербанк активно реализуются инновационные проекты по развитию безналичных платежей. В 2021 году доля безналичного оборота по розничным операциям банка составила 71%. Услуга «Мои операции», позволяющая совершать оплату регулярных услуг без необходимости повторного ввода реквизитов, завоевывает популярность, так за декабрь 2021 года посредством Сбербанк Онлайн было проведено в 1,5 раза больше платежей, чем за аналогичный период 2020 года. С 2020 года начал работу инновационный платежный онлайн-сервис SberPay. Основным достоинством данного продукта является высокая скорость совершения транзакций - они проходят всего в три касания.

В большинстве компаний экосистемы «Сбер» уже принимают платежи с помощью SberPay [94]. При этом ПАО Сбербанк продолжает активно совершенствовать сервис «Заплати QR». Так к концу 2021 года уже более 273 тысяч торговых точек принимают платежи по QR-коду от ПАО Сбербанк.

Внедрение инновационных технологий способствовало становлению ПАО Сбербанк в качестве высоко технологичной компании, которая предоставляет своим клиентам доступ к современнейшим услугам и сервисам, а также это позволило усилить свои позиции по всем направлениям российского финансового рынка. Модернизация процессов привела к повышению эффективности работы внутри банка, но также усилила конкурентные преимущества в целом. Необходимо учитывать, что широкое внедрение инновационных технологий должно находиться под пристальным вниманием и контролем для обеспечения постоянного совершенствования уровня кибербезопасности.

Финансовые технологии продолжают стремительно развиваться, готовность и способность человека доверять этим цифровым инновациям,

чтобы полностью понимать и пользоваться ими, является важнейшим фактором для дальнейшего развития в области банковской цифровизации.

Риск недоверия к использованию банками цифровых технологий выступает как одна из преград для дальнейшей модернизации инновационных банковских технологий [55].

Под влиянием цифровых технологий происходит трансформация доверия:

– изменение иерархии лояльности клиентов как основы доверия в сторону комфортности, постоянного доступа, большей информированности, скорости и дешевизны при получении финансовых услуг;

– «вторжение в личное пространство» клиентов как оборотная стороны изменения иерархии предпочтений;

– возникновение противоречивого отношения к цифровым технологиям из-за наличия комплекса информационных, технических и киберрисков;

– принуждение клиентов к выбору между подтвержденной временем лояльностью к классическим финансовым институтам и основанной на технологических достоинствах привлекательностью их новых конкурентов на рынке банковских услуг – компаний-финтехов и компаний-бигтехов;

– формирование дифференцированного поколенческого поведения клиентов финансовых институтов в цифровую эпоху.

Стоит отметить, что в настоящее время нет единого комплексного измерителя индекса цифрового доверия. Известны исследования и доклады, изучающие и объясняющие отдельные ключевые элементы доверия. Барометр доверия Эдельмана измеряет уровень доверия в разных странах и в различных отраслях. Индекс восприятия коррупции Трансперенси Интернешнл дает количественную оценку того, как граждане воспринимают свой государственный сектор.

Для оценки доверия к участникам финансового рынка целесообразно использовать подход, применяемый при расчете Индекса цифрового развития (DEI) 2017. При этом с целью интегральной оценки доверия важно ввести три показателя: оценка цифровой инфраструктуры финансового рынка, оценка уровня отношения к цифровым финансовым технологиям и опыт пользователей, а также оценка поведения клиентов.

На основе проведенного анализа влияния цифровой трансформации на участников финансового рынка, можно сформулировать следующие предложения.

В целях обеспечения сохранности персональных данных необходимо продолжить совершенствование законодательства, в том числе повысить ответственность за их хранение. В качестве меры защиты целесообразно увеличить размер штрафов, путем внесения соответствующих положений в Кодекс об административных правонарушениях (далее - КоАП). По состоянию на март 2023 сумма максимального штрафа за утерю персональных данных клиентов для компаний не превышает 500 тыс. руб., что несравнимо мало для крупных кредитных организаций.

Вместе с тем, крупный бизнес опасается скорее репутационных потерь, нежели штрафа. Для финансовых организаций действенной мерой может стать формирование репутационных рисков (например, рейтинг недобросовестных хранителей данных). Создание доступной доверительной цифровой среды – репутационный фактор, который вызывает общественный резонанс, повышая доверие и лояльность к кредитной организации.

Создание единого рейтинга банков на основе критериев оценки уровня защищенности персональных данных клиентов позволит выявить лидеров в сфере обеспечения информационной безопасности и защиты персональных данных, выступающих локомотивом в этой области, а публикация результатов в сети Интернет естественным образом стимулирует банки к добросовестному поведению по отношению к персональным данным своих клиентов. С этой целью можно рекомендовать российским рейтинговым агентствам при

определении рейтингов учитывать такой критерий как добросовестность в хранении персональных данных.

Помимо этого, можно рекомендовать Банку России учитывать данный показатель при оценке финансовой устойчивости кредитных организаций.

Переход к электронным договорам (дистанционное предоставление услуг), отсутствие культуры работы с электронными договорами порождает у клиентов неуверенность в надежности работы банковских сервисов. И если при традиционном банкинге бумажной договор является для клиента гарантией для споров в суде, то нужен некий аналог гаранта для электронных договоров, специальный репозиторий (по аналогии Федеральным законом от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы»). Как вариант решения вопроса можно предложить размещать сведения о счетах, открытых дистанционным образом, в личном кабинете налогоплательщика. В этом случае у клиента появляется уверенность в сохранении информации во внешнем доверенном ресурсе даже в случае форс-мажорных ситуаций в банке.

Таким образом, резюмируя основные результаты исследования по данному параграфу, целесообразно отметить следующее. Были обозначены наиболее перспективные тенденции по модернизации услуг дистанционного банковского облуживания. Кроме того, автором определены наиболее перспективные инновационные технологии банковской сферы и основные области их применения: улучшение качества обслуживания клиентов и применение новых методов в управлении банковскими рисками, в том числе, в области оценки данных рисков.

Даны практические рекомендации по минимизации риска недоверия к использованию банками цифровых технологий. Отмечено, что наиболее результативной мерой является создание единого рейтинга банков на основе критериев оценки уровня защищенности персональных данных клиентов, который стимулирует банки к добросовестному поведению по отношению к персональным данным своих клиентов.

С учетом изложенного следующим действием представляется необходимым исследовать специфические особенности подходов, которые используются при оценке рисков дистанционного банковского обслуживания. Данные положения рассмотрены подробно в следующем параграфе.

2.2 Совершенствование банковского надзора в целях минимизации рисков в сфере дистанционного банковского обслуживания

За последние годы было отмечено усиление взаимозависимости между финансовым, реальным и банковским секторами экономики. Данная тенденция характерна не только для России, но и для всего мира в целом. В указанных условиях основополагающей в рамках поддержания финансовой стабильности экономики становится система банковского надзора, функционирование которой является зоной ответственности макрорегуляторов.

Право осуществление банковского надзора в Российской Федерации принадлежит Центральному Банку России. Основными задачами в сфере банковского надзора являются, во-первых, достижение устойчивого функционирования и развития банковской системы в стране, а во-вторых, гарантия защиты интересов всех субъектов банковской деятельности на законных основаниях.

Методология банковского надзора, принятая в Российской Федерации, соответствует общемировым стандартам, так как Банк России официально принял к рассмотрению и внедрению рекомендации в сфере банковского надзора со стороны Базельского комитета. Основным же документом Базельского комитета, который регламентирует спектр необходимых параметров функционирования информационных систем кредитных организаций, а также принципы наиболее эффективного построения системам управления рисками, в первую очередь операционными, выступает стандарт «Принципы эффективного агрегирования данных о рисках и составления отчетности о рисках» [80].

В перечне важнейших задач, стоящих пред регулированием банковской системы на современном уровне функционирования в первую очередь следует выделить: создание банковской инфраструктуры, требуемой для наиболее функциональной работы всего рыночного механизма, что предполагает осуществление беспрерывного проведения расчетных операций, формирование современных банковских продуктов и услуг, увеличение разнообразия финансовых технологий и осуществление банковских операций с производственным сектором экономики страны [29].

Для наиболее результативной деятельности в рамках надзорного блока, в первую очередь следует точно определить основную задачу банковского риск-ориентированного надзора в области дистанционного банковского обслуживания, состоящая в своевременном получении информации, которая требуется для проведения точного анализа формирования, трансформации и расширения применения банковских информационных технологий, а также разработки рекомендаций по модернизации данного канала взаимодействия с пользователями банковских услуг.

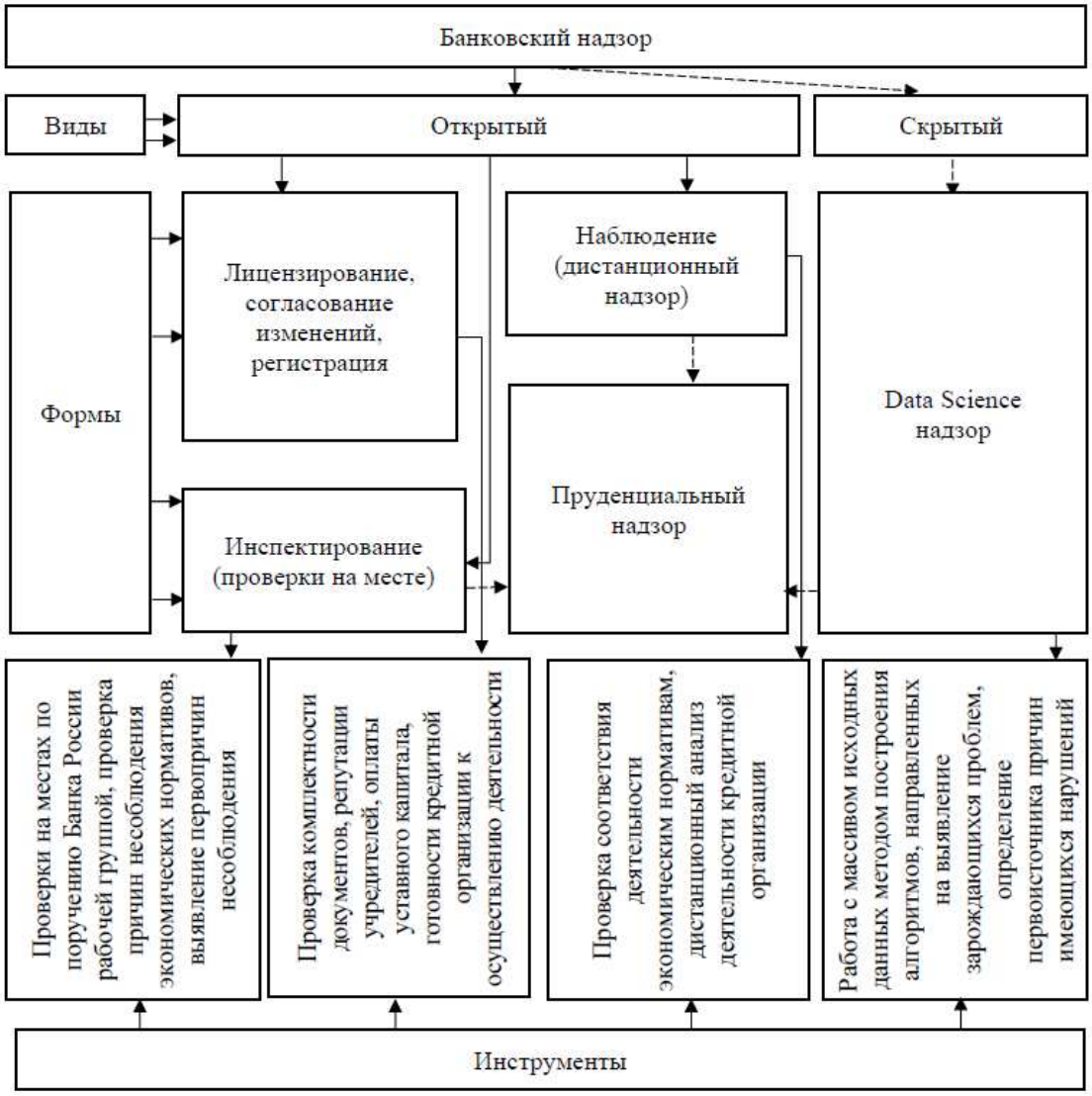
Исходя из основной цели в виде формирования и поддержания устойчивости и надежности функционирования национальной банковской системы в целом, а следовательно, и отдельно взятых банковских организаций, которые и формируют эту систему, с точки зрения риск-ориентированного надзора наравне с применением современных информационных технологий дистанционного обслуживания клиентов банка – стоит вопрос о необходимости формирования специальных методов управления банковскими рисками, включая их определение, мониторинг и оценку.

Таким образом, кредитные организации, применяющие технологии дистанционного банковского обслуживания, должны обнаруживать оценивать и проводить анализ рисков и осуществлять управление рисками пруденциальным образом.

Банковский надзор состоит из наблюдения Банка России за полным соблюдением кредитно-финансовыми организациями действующего

законодательства, которое регламентирует банковскую деятельность. Кроме того, мегарегулятор контролирует выполнение финансовых нормативов и правил бухгалтерской отчетности [101].

Анализ текущего состояния банковского надзора в России на современном этапе развития банковского сектора предполагает выделение основных инструментов его осуществления, которые подробно отраженные на рисунке 2.3.



Источник: составлено автором на материалах [78].

Рисунок 2.3 - Виды, формы и инструменты банковского надзора центральных банков

На основании предложенной схемы, необходимо сделать уточнение, что пруденциальный надзор представляется, по нашему мнению, одной из разновидностей одновременно несколько форм проверок: наблюдения и инспектирования ввиду того, что следование установленным нормативам

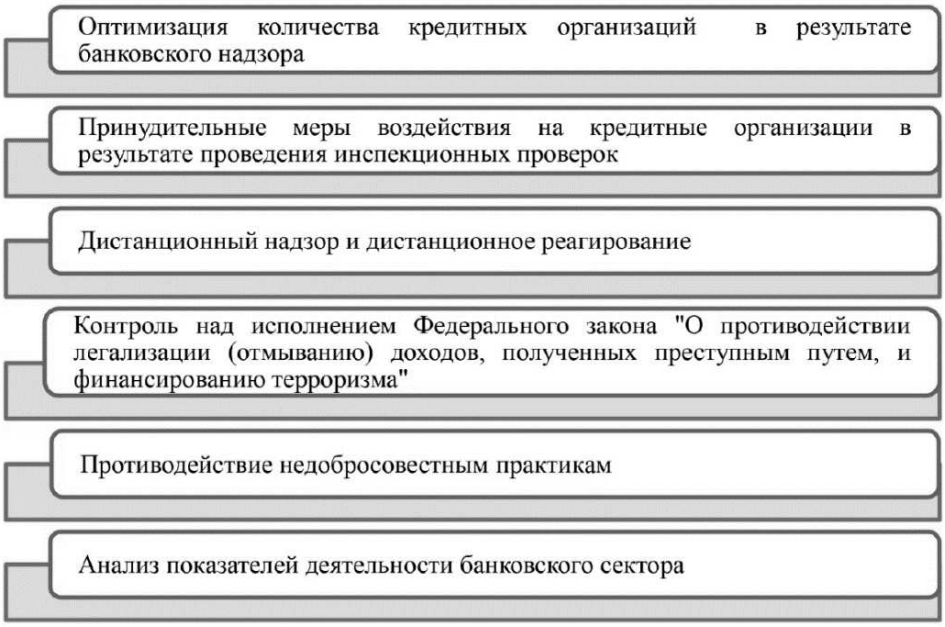
может проверяться регулятором как на этапе текущего, так и на этапе последующего банковского надзора.

Кроме того, отдельно следует выделить такую форму надзора, как Data Science надзор. В ходе осуществления данного вида надзора осуществляется анализ значительных массивов данных с помощью формирования специальных алгоритмов, основной задачей которых является своевременное определение появляющихся проблем в деятельности кредитной организации, мониторинг первоисточника возможных правонарушений.

За последнее десятилетие значительно развился тренд на повышение консолидации банковской отрасли, которая в соответствии со стратегией Правительства России должна повлиять на увеличение уровня конкурентной среды банковской сферы и прекращению деятельности субъектов, осуществляющих недобросовестную деятельность. Главными задачами осуществления банковского надзора выступают создание устойчивого функционирования банковских организаций, защита прав и интересов всех субъектов осуществления финансовых услуг, а также борьба с легализацией доходов, полученных незаконным путем [14].

В процессе анализа эффективности банковского регулирования и надзора Банка России, по нашему мнению, необходимо отталкиваться от следующих критериев, представленных на рисунке 2.4.

За последнее время в области банковского надзора и регулирования банковской деятельности были произведены значительные изменения. Данные изменения повлияли на уровень качества предоставляемых услуг и усилили внимание к защите интересов клиентов. Среди положительных изменений следует отметить повышение устойчивости и стабильности развития банковского сектора. Трансформация банковской деятельности, проявляющаяся в виде создания и совершенствования собственных экосистем, платформ небанковских услуг и усложнения основных процессов, должна быть рассмотрена с точки зрения возможности появления новых рисков для самих банков, их партнеров, инвесторов и клиентов.



Источник: составлено автором [72].

Рисунок 2.4 - Критерии для анализа эффективности банковского регулирования и банковского надзора в Российской Федерации

Неотъемлемой сферой деятельности Центрального Банка и кредитных организаций ввиду развития технологий и появления новых угроз является повышение качества банковского регулирования и эффективности надзора в новой цифровой экономике.

Предоставив подробный разбор контура типичных рисков банковской деятельности, на которые главным образом воздействуют технологии дистанционного банковского обслуживания, следует определить наиболее вероятные источники возникновения рисков, основанные на отличительных чертах функционирования информационных систем.

Любые операции с информацией, включая формирование, хранение, обработку и передачу, осуществляются при помощи информационно-технического оборудования, определенного в каждом конкретном кейсе. В то же время, специфические риски, возникающие вследствие влияния технологических факторов, всегда сопряжены с тремя главными первопричинами:

а) некорректной работой систем дистанционного банковского обслуживания, сопровождающейся техническими ошибками;

б) неверным использованием аппаратно-программного обеспечения информационных систем банковского обслуживания;

в) несанкционированным доступом к использованию программ, входящих в перечень систем дистанционного банковского обслуживания, как правило, вызванным утечкой или кражей конфиденциальных данных.

Совершенствование методологической деятельности, которая производится в области осуществления банковского надзора, наряду с формированием рекомендаций для банковских структур по отношению к процедурам регулирования, необходимым для создания качественных процессов риск-ориентированного надзора, необходимо осуществлять последовательно решая данные вызовы. Принимая во внимание тот факт, что все проводимые операции между кредитными организациями и их контрагентами, включая клиентов банка, осуществляемые при помощи автоматизированных информационных каналы связи, основаны на банковских системах аппаратно-программного обеспечения, наиболее комплексным подходом было бы рассмотрение и информационных систем, находящихся в контуре управления внутри банка, и данных технического средств внешних пользователей.

С позиции банковского надзора, крайне важно иметь информацию относительно того, какие субъекты имеют права доступа к информационно-технически ресурсам банковской организации, к каким базам данных может быть предоставлен доступ через эти каналы информации и какие служебные полномочия обеспечены данным видом доступа.

Основополагающим условием, которое предполагает наиболее полное обеспечения гарантий непрерывной работоспособности информационно-технологических систем банка выступает их системная надежность и устойчивость при осуществлении возможных киберпреступлений со стороны злоумышленников [15].

Размеры прямых и косвенных финансовых убытков кредитной организации, также как и объём предполагаемых штрафов за обнаруженные

нарушения, находятся в прямой зависимости не только от количества производимых банковских операций, осуществляемых в формате дистанционного обслуживания, но и от уровня запаса безопасности информационных систем, а периода их восстановления, в случае проявления технических сбоев.

Стоит отметить, что помимо кредитных организаций регулятором также производится взаимодействия с непосредственными потребителями финансовых услуг. Создаётся специализированная справочная служба для клиентов банковского сектора, которая занимается подготовкой информационных материалов, предупреждающего и рекомендательного характера. В России данную функцию выполнят подразделение Центрального Банка – ФинЦЕРТ, занимающееся мониторингом киберпреступлений.

Можно заметить, что задачи дистанционного банковского обслуживания неразрывно взаимосвязаны с широким информационным освещением надзорной функции для населения. Кроме того, предоставляемая информационная база не менее важна для сотрудников, входящих в подразделение банковского инспектирования. Особое внимание данному сегменту выделяется в связи с тем, что непосредственно инспекторы банковского надзора непосредственно взаимодействуют как с автоматизированными системами банков, так и с деятельностью сотрудников отдела внутреннего контроля и собственной безопасности в рамка банковской структуры.

Роль эффективного правового регулирования банковской деятельности состоит в создании оптимальной нормативно-правовой среды для осуществления эффективного управления банковскими рисками с целью повышения устойчивости и надежности банковской системы. Среди наиболее важных направлений совершенствования правового регулирования в первую очередь следует обратить внимание на следующие:

– формирования четко регламентируемого законодательного статуса использования информационных технологий в сфере финансового взаимодействия;

– совершенствование правового статуса криптовалют и легитимизация их применения в рамках платёжного и сберегательного средства в рамках российской экономики;

– разработка необходимых регламентов для осуществления операций с криптовалютами.

Проведение данных реформ даст возможность трансформировать процесс банковского регулирования согласно основным трендам современного экономического и технологического развития, облегчит соблюдение законных интересов всех субъектов банковского рынка в целом.

Весь перечень мероприятий Центрального Банка, направленных на модернизацию надзорной банковской деятельности за кредитными организациями, обязан приобрести наиболее комплексный характер, а также непрерывно совершенствоваться на каждом уровне системы, в первую очередь для уменьшения проявления негативных финансовых последствий для пользователей цифровых услуг кредитных организаций банковского сектора страны.

В рамках процесса диджитализации кредитно-финансовых технологий и услуг важным направлением становится совершенствование методов использования искусственного интеллекта, накопление биометрических массивов информации, портативных инноваций в сфере роботизации и открытых интерфейсов [32].

Кроме того, в сфере улучшения информационной инфраструктуры обязательно требуется осуществления массивного комплекса мероприятий в направлении формирования и поддержании устойчивого функционирования электронных платформ.

Вышеперечисленные современные технологии информационного развития стали особенного актуальны в период распространения пандемии

коронавируса в 2020-2021 годах, что стало драйвером их ускоренного внедрения. Вместе с тем, на текущий момент времени все данные инновации требуют постоянную правовую и финансовую проработку и актуализации в соответчики с постоянно меняющимися условиями функционирования банковской системы Российской Федерации.

Например, на текущий момент был выполнен проект по формированию процесса электронного документооборота между банковскими структурами и подразделениями банковского надзора Центрального банка, организованного в формате обмена информации в рамках личного кабинета. Указанные нововведения были включены в нормы федерального законодательства в рамках законопроекта, вступавшего в силу 03.11.2017, под названием № 4600-У «О порядке взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и другими участниками информационного обмена при использовании ими информационных ресурсов Банка России, в том числе личного кабинета».

В результате применения технологического решения в виде личных кабинетов кредитных организаций для проведения удаленного банковского надзора и реагирования, было замечено значительное увеличение качества осуществления надзорной деятельности, что в свою очередь, повысило скорость и эффективность принятию решений надзорными подразделениями Центрального Банка [101].

Кроме того, применение личных кабинетов в надзорной деятельности позволила Центральному Банку значительно увеличить скорость обмена ежедневными формы банковской отчетности, что даёт возможность своевременно проводит мониторинг и анализ необходимых информационных данных. Это минимизирует сложности, связанные с территориальной отдаленностью некоторых банковских организаций, так как позволяет моментально передать надзорным подразделением запросы или предписания по выявленным нарушениям. Данное информационное взаимодействия требует

применение усиленный электронных подписей, что значительно повышает безопасность данных.

Трансформация банковской отрасли по пути совершенствования практик регулирования ее цифровизации и информационно-программного обеспечения нацелено на увеличение качества доступности и повышения уровня оказываемых банковских операций.

При помощи построения и совершенствования элементов банковской инфраструктуры симметрично с достижениями производственно-технического прогресса и применения современных инновационных технологий банковской деятельности возможно добиться наиболее полного исполнения запросов пользователей финансовых приложений.

Мегарегулятор и субъекты банковского рынка начинают применение современных технологий во многих направлениях организации своей работы как для требований повышения эффективности внутренних процессов, так и для ускорения дистанционного взаимодействия между друг другом. Обоснованное применение технологических решений даёт возможность сократить финансовые издержки, увеличивает производительность банковской деятельности и привлекательность предлагаемых клиентам продуктов, сокращает проявление всех типов банковских рисков. В направлении использования инновационных технологий мегарегулятором и банками особенно выделяются два основных блока – SupTech и RegTech.

Regulatory Technology – комплекс технологичных решений, применяемых банками и финансовыми компаниями для увеличения качества исполнения регуляторных требований Банка России.

Supervisory Technology – комплекс технологичных решений, внедренных Центральным банком в целях развития уровня результативности в рамках осуществления контроля и надзора за субъектов рынка.

Машинное обучение – система аппаратных методов искусственного интеллекта, которая, благодаря автоматическому улучшению, способна распознавать неочевидные взаимосвязи в массивных базах данных. Машинное

обучение применяется во многих секторах экономики для произведения предиктивного анализа и оптимизации процессов. На банковском рынке машинное обучение применяется для установления и оценки рисков, мониторинга финансовых аномалий и предотвращения мошеннических действий. Также, при помощи технологии машинного обучения и анализа нейросетей происходит разработка и настройка чат-ботов.

Проведенное исследование позволило нам разработать классификацию этапов (интервалов) эволюции машинного обучения в банковском надзоре на основе соответствующих событий в банковском секторе, технологического развития, что отражено на рисунке 2.5.

Источник: составлено по материалам [72].
Рисунок 2.5 - Классификация этапов эволюции машинного обучения в банковском надзоре

Внедрение методов машинного обучения демонстрирует положительную динамику изменений в работе кредитных организаций, в частности отмечается значительная экономия ресурсов, совершенствование качества отдельных процессов и повышение уровня эффективности функционирования в целом.

За последнее время глубокое обучение и машинное обучение использовались в банковской деятельности для оценки кредитного риска, в более широком смысле его использование сводилось к составлению прогнозов относительно возможности банкротства кредитной организации. Использование данных подходов позволяет учитывать модели прошлых

решений для поиска оптимальных стратегий и сценариев развития исходя из текущих показателей, а также предсказывать хаотические события будущего.

Исследования в области машинного и глубокого обучения основаны главным образом на данных, доступных для общего пользования, характеризующих динамику рынка. Специализированные исследования на базе изучения банковского и финансового сектора в данной области отсутствуют, поэтому становится невозможным оценить необходимость повсеместного внедрения машинного обучения в этих сферах.

В условиях коронакризисной и постковидной экономики (IV-V этапы) к основным векторам совершенствования в сфере SupTech и RegTech, по нашему мнению, следует отнести:

– внедрение единой модели данных поднадзорных организаций, которая даст возможность сократить расходы субъектов рынка на подготовку к постоянно увеличивающимся регуляторным требованиям по предоставлению данных отчетности, становящимися все более комплексными, а также улучшит прозрачность информационных данных для полного анализа поднадзорных банков;

– оптимизация объема данных, поступающих от финансовых учреждений, с целью сокращения давления на контролируемые организации;

– внедрение системы учета реального потребления информации Центральным банком, которая позволит существенно повысить эффективность нагрузки как на контролируемые учреждения, так и на собственные внутренние системы;

– разработка рекомендаций и предложений по внедрению облачных технологий на финансовом рынке, которые позволят сократить трудозатраты, оптимально организовать процедуру обеспечения информацией поднадзорных организаций;

– использование методики стресс-тестирования рабочих процессов банков, которая позволяет провести полные анализ и оценку

киберустойчивости финансово-информационной среды в данный отрезок деятельности по заранее подготовленному сценарию;

– разработка методики «Know your customer», означающую трансфер банковским структурам данных о значении показателя комплаенс-риска вероятной клиентской базы, текущих пользователях и их контрагентов на постоянной основе для осуществления процедур контроля по противодействию легализации доходов, полученных преступным путем. Данные действия позволяют уменьшить количество кейсов по использованию превентивных ограничительных мер со стороны кредитно-финансовых организаций при обнаружении рисков незначительного уровня;

– повсеместное внедрение применения биометрических данных для совершенствования процедуры идентификации пользователей в личном кабинете участников информационного взаимодействия на платформе Банка России, что приведёт к оптимизации и повышению безопасности идентификации клиентов при осуществлении процедур допуска;

– организация рабочих процессов по расчетно-кассовому обслуживанию клиентов и их представителей в подразделениях Центрального банка с применением технологий биометрической идентификации, что значительно уменьшит время на обслуживание клиентов и позволит повысить безопасность процесса выдачи и приема наличных денежных средств;

– улучшение качества мониторинга проводимых операций на наличие противозаконных действий и формулирование необходимых рекомендаций по RegTech-технологиям в области анализа транзакций для субъектов банковского сектора.

На современном этапе развития банковской деятельности последующая модернизация осуществления регулирования банковского рынка должна базироваться на выполнение следующего перечня целей:

– Формирование многогранной аналитической системы, которая необходимо интегрировать в регламент поведения надзорного процесса. Комплекс мер даст возможность воплотить всеобщую

технико-информационную помощь при процессе принятии финансовых решений. Основной задачей формирования данной структуры выступает улучшения достоверности и актуальности надзорных оценок относительно состояния устойчивости кредитных организаций.

– Разработка средств и практик для повышения эффективности сотрудничества Центрального Банка с представителями компаний аудиторского контроля, чья профессиональная деятельность направлена на оказании услуг кредитным организациям в части консультационных мероприятий.

– Создание стимулирующего эффекта регулирования, выражающегося в направлении влияния на банки такими способами, которые заставят кредитные организации модернизировать систему управления операциями, как следствия, позволяя улучшить финансовый результат. Одной из возможных программ в рамках данного метода развития выступает последовательное улучшение качества реализации механизма проектного финансирования.

– Последующая модернизация метода пропорционального регулирования, которое находится в зависимости от комплексности проводимых банками операций [40].

Таким образом, резюмируя основные результаты исследования по данному параграфу, целесообразно отметить следующее. Были обозначены основные особенности функционирования системы банковского надзора в Российский Федерации. Кроме того, автором определены наиболее перспективные направления его совершенствования, включая использование инновационных разработок банковской сферы, таких как способы машинного обучения, а также SupTech и RegTech технологии, и основные направления их применения: поддержание устойчивого функционирования национальной банковской системы в условия применения дистанционного-банковского обслуживания, а также обеспечение полной защиты законных интересов каждого субъекта банковской деятельности.

Одной из самых значимых тенденций трансформации банковской системы выступает формирование необходимой системы поддержания устойчивости российских кредитных организаций, которая даст возможность сохранить их независимость от информационных систем зарубежного производства и сформировать отечественную, надежную систему обеспечения безопасности.

С учетом изложенного следующим логичным шагом представляется исследовать опыт России и зарубежных стран в части управления банковскими рисками в рамках системы дистанционного банковского обслуживания.

2.3 Анализ российской и зарубежной практики управления рисками в области системы дистанционного банковского обслуживания

Стабильность банковской системы зависит от многих факторов: нарастание кризисных явлений, конкуренции, усложнение банковских продуктов и услуг, повышение зависимости банков от технических средств обеспечения, и, конечно, финансовая устойчивость банков. Риски, как уже отмечалось, непосредственно присутствуют в банковских операциях и влияют на финансовое положение банков и на всю банковскую систему в целом. Глобализация хозяйственных процессов, участие банков на международном рынке банковских услуг порождают заимствование в системе контроля и регулирования финансовыми рисками коммерческих банков у многих стран.

Для банковской практики всех экономически развитых странах модернизация системы управления рисками играет важную роль в общей стратегии кредитной организации.

В зарубежной практике по характерным особенностям можно структурировать и выделить четыре основных формы систем оценки рисков и финансового состояния банковского института: комплексные системы оценки, системы финансовых коэффициентов, рейтинговые системы оценки банковских

рисков и статистические модели. Например, в США широко применяется рейтинговая система оценки рисков CAMELS [84].

Вместе с тем, итальянская система PATROL и французская система ORAP сформированы на аналогичных принципах, что и CAMELS. Особенность рейтинговых систем оценки рисков заключается в том, что они базируются на большом диапазоне данных, а также включают в себя вспомогательные исследования. Например, источником информации французской системы ORAP являются обширные базы данных Банковской комиссии и Банка Франции, а также данные самих кредитных организаций и привлекаемых аудиторов.

В пределах данной методики предусматриваются пруденциальные коэффициенты, рассчитывается балансовая и внебалансовая активность, анализируется финансовый риск, определяются качественные параметры систем управления риска и внутреннего контроля.

Итальянская система PATROL также базируется на анализе достаточности капитала, качества управления, ликвидности, кредитов и расчета доходности.

Однако рейтинговые системы отражают достоверно только текущее состояние коммерческого банка.

Суть совокупность финансовых коэффициентов и группового анализа состоит в том, что финансово-экономическое состояние положение кредитной организации анализируется с использованием перечня финансовых коэффициентов.

Для каждой страны данный набор показателей различен. Безусловно, рассчитанные показатели являются информационной базой для руководителей, так как они могут определить качество принятых ими управленческих решений, для определения рискованности операций клиентам и наконец, для инвесторов, так как они могут определить с помощью коэффициентов риск вложений и потенциальную прибыль банка. В систему финансовых коэффициентов входит методика BAKIS, используемая Центральным банком Германии и включающая

расчет 47 коэффициентов. Главным недостатком данной системы является сложность вычислений коэффициентов, однако данный расчет дает всестороннее заключение банка [84].

В сопоставлении с рейтинговыми и коэффициентными системами оценки рисков, в рамках статистической модели основной фокус направлен на потенциальное экономико-финансовое положение кредитной организации и появлению рисков, на базе сведений о деятельности банковского института, полученных от надзорных органов. После чего производятся расчеты для определения банков с минимальной и повышенной вероятностью банкротства. К статистическим моделям относятся система SAABA, используемая во Франции и состоящая из трех диагностических блоков.

Согласно представленной методике, в первом блоке главный интерес обращён к кредитному портфелю банка, в следующем блоке – к субъектам, являющимся держателями акций кредитной организации и в последнем блоке – состоянию менеджмента ликвидности и прибыльности банковской структуры. В целом показатели объединяются, и дается оценка надежности: один балл - устойчивый банк, пять баллов на грани банкротства.

И наконец, комплексная система оценки банковских рисков, основной задачей которой выступает оценка всей системы финансовых рисков кредитной организации, в том числе особенности её структурной организации. На проведение указанной методики требуется большое количество финансовых и временных ресурсов.

К данной категории относятся системы RATE и RAST. Содержание методики RAST, разработанной в Нидерландах, состоит в том, что банковский институт делится на отдельные структурные подразделения по выделенным функциональным признакам. В рамках методики RATE, применяемой Банком Англии, производится оценка риска (Risk Assessment), входят инструменты надзора (Tools) и осуществляется оценка эффективности применения инструментов надзора (Evaluation).

Несмотря на все вышеуказанные системы выявления и оценки банковских рисков, присущих определенной стране с учетом особенностей их банковской системы, выделяют единые стандарты банковской деятельности в целях контроля над финансовыми рисками банка, укрепления банковской системы, как на национальном, так и на международном уровне.

Чтобы представлять направления по модернизации систем управления рисков дистанционного банковского обслуживания, необходимо определить перечень наиболее вероятных угроз безопасности для банковских приложений. Десять наиболее значимых угроз были выделены на основании данных проекта Open Web Application Security и описаны в таблице 2.2.

Таблица 2.2 – Перечень основных угроз для приложений удалённого банковского обслуживания

Название угрозы	Описание угрозы
Обход архитектурных ограничений	Эта уязвимость охватывает злоупотребление особенностями платформы, обхода ограничений. Затрагивает системы контроля безопасности, которые являются частью мобильной операционной системы
Небезопасное хранение данных	К ней относятся небезопасное хранение и непреднамеренные утечки данных
Небезопасная передача данных	Недостаточное подтверждение достоверности источников связи, неверные версии SSL, недостаточная проверка согласования, передача конфиденциальных данных в открытом виде
Небезопасная аутентификация	Эта уязвимость относится к аутентификации конечного пользователя или неверное управление сеансами
Слабая криптостойкость	Применение криптостойких алгоритмов для передачи информации. Эта категория описывает варианты ненадлежащего использования криптографических элементов, недостаточной криптостойкости.
Небезопасная авторизация	Эта уязвимость описывает недостатки авторизации стороне клиента
Контроль содержимого клиентских приложений	Эта категория рассматривает контроль за входными данными: переполнение буфера, а также другие ошибки на уровне кода, где решением является необходимость переписать код, который работает на мобильном устройстве
Модификация данных	Эта категория описывает изменение исполняемых файлов, локальных ресурсов, перехват вызовов сторонних процессов, и динамическую модификацию памяти
Анализ исходного кода	Эта уязвимость включает в себя анализ бинарных файлов для определения исходного кода, библиотек, алгоритмов. Может быть использовано для поиска уязвимостей приложения, извлечения критичной информации
Скрытый функционал	Часто разработчики включают в код приложений скрытые функциональные возможности, которые не предназначены для общего пользования

Источник: составлено автором на материалах [62].

На основании анализа приведённых в таблице данных, можно определить, что часть из них являются специфическими только для мобильного банкинга. Принимая во внимание особенную природу угроз информационной безопасности, характерных для систем удалённого обслуживания, проявляется необходимость создания комплекса мероприятий и инструментов для уменьшения вероятности наступления указанных выше угроз.

Как уже отмечалось, в России механизмы управления финансовыми рисками опираются на зарубежный опыт, но с учетом особенностей развития банковской системы и экономики в целом в стране. Рассмотрим общие механизмы управления финансовыми рисками, которые включают:

1) управление активами и пассивами;

2) страхование;

3) хеджирование;

4) диверсификация.

Управление активами и пассивами заключается в анализе восприимчивость баланса кредитной организации к разнообразным колебаниям одного или нескольких факторов, а также в количественной оценке воздействия неожиданных изменений в данных факторах.

Основной целью мероприятий по управлению активами и пассивами выступает формирование действенных стратегий для осуществления задач по менеджменту риска и составлению точной, согласованной и актуальной отчётности.

Данный метод не предполагает отвлечение средств на внесение страховых платежей, образование резерва, а предполагает эффективно действующую обратную связь между объектом управления и центром принятия решений.

Страхование предполагает передачу большей части риска от страхователя к страховщику, то есть основной целью страхования выступает возмещение имущественного ущерба от проявления риска, но никак не на уменьшение вероятности проявления рисков.

Хеджирование — это нейтрализация риска изменения цены актива в будущем за счет проведения определенных финансовых операций, хеджирование предполагает заключение сделки на срочных рынках с целью страхования от возможных потерь. Хеджирование так же как и страхование требует отвлечения дополнительных ресурсов, но хеджирование существенно ограничивает или исключает для банка валютные, процентные, ценовые риски с помощью форвардных, фьючерсных и опционных контрактов. Цель хеджирования - не получение прибыли, а стремление обезопасить себя от неблагоприятного движения цен, преодолев пики курсовых колебаний, хеджирование позволяет:

- застраховаться как от падения, так и от повышения цен на базовый актив;
- зафиксировать стоимость платежа;
- застраховать сделку.

И наконец, диверсификация рисков подразумевает уменьшение вероятности риска вследствие распределения средств между различными активами, цена и доходность которых слабо коррелируемы между собой. Диверсификация минимизирует концентрацию отдельных видов рисков. Данный метод является одним из наиболее популярных способов снижение кредитных и рыночных рисков при формировании портфеля банковских ссуд и финансовых активов соответственно.

Управление финансовыми рисками коммерческих банков в России во многом опирается на опыт развивающих и развитых зарубежных стран. Однако в полной мере нельзя перенести в отечественную банковскую систему зарубежный опыт, поскольку нужно учитывать, что в каждой стране определенный уровень развития финансового рынка, банковской системы, и экономики в целом, наличие полномочий у надзорных органов, ведения учета и отчетности и многих важных показателей, характеризующих экономическое положение каждой страны.

Таким образом, проанализировав основные методы управления финансовыми рисками, применяемые как в России, так и в зарубежных странах,

можно сделать вывод, что, учитывая специфику развития банковской системы в каждой стране, способы оценки и выявления банковских рисков имеет как отличительную особенность, так и схожие характерные черты. Также следует отметить, что международные стандарты, принятые Базельским комитетом имеют широкое распространение во многих развитых и развивающих странах.

Так и в России, Базельские соглашения нашли отражение при расчете собственных средств, основного капитала для покрытия рыночного, кредитного и операционного риска. Помимо международных стандартов, принятые Базельским комитетом по оценки и выявлению банковских рисков, существуют множество систем оценки рисков за рубежом, такие как CAMELS, SAABA, FIMS,RAST, RATE и многие другие методы управления рисками. Исходя из вышесказанного, можно сказать, что управление финансовыми рисками основа риск-менеджмента, многообразие способов выявления и оценки рисков постоянно требует совершенствования, изменения, как в России, так и за рубежом.

Наиболее перспективным направление по модернизации системы управления риском дистанционного банковского обслуживания по всему миру выступает внедрения инновационных информационных технологий в систему риск-менеджмента банка.

Широкое распространение среди западных стран получила технология BigData, которая осуществляет хранение, анализ и сортировку структурированных и неструктурированных массивов данных большого объема.

Еще одной важной функцией данной технологии является повышение сохранности информационных ресурсов, а также снижение вероятности доступа к ним со стороны несанкционированных лиц.

Пользуясь возможностями технологии больших данных, можно добиться повышения качества контроля за основными процессами и настроить более точный обмен обратной связью с клиентами банка. Подходы данной технологии могут быть использованы при анализе осуществляемых

финансовых транзакций, в данном направлении работает американская технологическая компания IBM, специализирующаяся на производстве программного обеспечения, систем хранения данных, серверного оборудования. В результате использования системы больших данных компанией был отмечен рост распознавания мошеннических операций на 15%, что позволило предотвратить на 60% больше хищений денежных средств [82].

Положительное влияние технологии больших данных также выражается в повышение результативности выполнения запроса клиента вследствие ускорения организации взаимодействия с ним. Также в связи с повышением точности планирования производства расходы на предоставление сервисных услуг сокращаются.

Один из крупнейших банков в мире – HSBC – использует технологии Big data для борьбы с мошенничеством в сфере кредитных карт. С помощью инструмента процесс идентификации стал результативнее в несколько раз в течение нескольких недель. Данная инновация позволила раскрыть преступные махинации, совокупный ущерб от которых потенциально мог составить более 10 млн долларов.

Среди особенно активно используемых финансово-экономических инноваций выделяется технология блокчейн, которая даёт возможность сохранять массивы данных в общем доступе. Данные открыты для всех без возможности редактирования или удаления. Технология блокчейн широко применяется в сфере управления финансами и другими ресурсами кредитных организаций, также она обеспечивает работу системы международных расчетов. Преимущество применения технологии блокчейн состоит в возможности снижения операционных расходов и повышении прозрачности и безопасности использования других информационных технологий [67].

Каждая финансовая операция фиксируется, составляя «информационную цепочку», расположенную в хронологическом порядке. Данный метод позволяет отследить последовательность и законность проведения транзакций кредитными клиентами и организациями. В списке основных пользователей

блокчейна уже закрепились крупнейшие мировые банки – UBS, GoldmanSachs, JP Morgan и Barclays.

Помимо этого, для совершенствования данной технологии, а также для продвижения блокчейна в финансовой торговле технологическая компания Microsoft скооперировалась с Bank of America MerrillLynch.

На текущем этапе развития банковского сектора в качестве меры по препятствованию несанкционированному доступу к коммерческим сведениям, составляющим банковскую тайну, все большую популярность набирает биометрическая идентификация. В российской практике данная инновация получила распространение недавно, но уже на текущий момент активно внедряется все большим количеством кредитных организаций, так как помогает повысить надежность взаимодействия с клиентом. Например, метод идентификации клиента по отпечатку пальца уже апробирован в отделениях банков АО «Альфа-Банк» и ПАО Сбербанк.

В результате обмена опытом с иностранными партнерами в 2018 году были внесены изменения, касающиеся информационной безопасности, в Федеральный закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Центральный Банк России совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации оказал содействие в создании единой биометрической системы, созданной на базе ПАО «Ростелеком», позволяющей производить удаленную биометрическую идентификацию для предоставления государственных и финансовых услуг.

Для выявления и оценки правовых факторов риска кредитной организации используются различные методы выявления и получения информации о клиентах и бенефициарах дистанционного банковского обслуживания вплоть до приобретения бухгалтерских фирм.

Одним из основных правил ведения сотрудничества в соответствии с федеральным законодательством Российской Федерации является принцип «знай своего клиента». Обмен информацией между отделами и сотрудниками

должен быть четко регламентирован по срокам, форме и возможности доступа. Данная мера позволяет снизить уровень правовых рисков. Грамотное распределение полномочий и обязанностей позволяет сэкономить время на дублировании функций и снизить расходы на персонал. Степень эффективности управления рисками в сфере права может быть оценена с помощью специальных контрольных мероприятий.

В соответствии с базовым сценарием реагирования на инциденты в информационных банковских системах, специалистам кредитной организации необходимо выполнить следующий ряд действий:

а) По факту поступления сведений о происшествии с дистанционной банковской системой необходимо идентифицировать пострадавшего клиента и платежи, подвергшиеся мошенническим действиям.

б) Сформировать протокол происшествия, в котором будет указаны все данные, необходимые для ликвидации негативных последствий.

в) При условии, что платежные поручения не исполняются, провести процедуру их отмены.

г) Передать информацию в банк-получатель письмом на официальном бланке о произошедшем событии блокировке операций по счетам лиц, подозревающихся в мошенничестве, кроме того, необходимо выслать информационное письмо в органы внутренних дел о факте совершенного преступления.

д) Получить логи пострадавшего клиента из автоматизированной банковской системы за необходимый промежуток времени.

е) Опросить пострадавшего клиента, для получения дополнительных сведений об инциденте.

Степень формализации процессов планирования, исследования и контроля является одним из основных факторов снижения правовых рисков. Формализация указанных процессов происходит путем создания соответствующих нормативно-правовых регламентов под конкретные операции.

Для дистанционного банковского облуживания стандартизированы основные банковские операции – процедуры и технологии. Распределяются «зоны ответственности» банка и клиента.

Для снижения уровня правовых рисков в сфере дистанционного обслуживания также необходимо внедрение технических мер противодействия. Адрес операционного узла, по которому осуществляются банковские операции клиентов, представляет собой конфиденциальную информацию. Эти сведения предоставляются исключительно для зарегистрированных пользователей системы удаленного банковского обслуживания в соответствии с порядком, установленным банком. При всех режимах функционирования площадки в рамках интернет-банкинга процесс взаимообмена данными между банком и клиентом должен производиться с использование криптографических технических средств. Электронный документооборот между кредитной организацией и клиентами через операционную площадку предполагает применение средств удостоверения подлинности электронных сообщений, контроля их целостности и проверки подлинности, включая электронную подпись.

Таким образом, грамотно составленная модель управления правовыми рисками позволяет снизить вероятность угроз и размер потенциального ущерба для кредитной организации. Современным банкам необходимо действовать сразу в двух направлениях – расширении лояльной клиентской базы и повышении безопасности проведения транзакций в сфере дистанционного банковского обслуживания.

В последнее десятилетие в экономиках значительного числа стран мира, в том числе в Российской Федерации, можно проследить тренд по повышению уровня доступности финансовых данных. В финансовом и банковском секторах, в первую очередь, это отражается в росте объёма использования программных интерфейсов (далее - API). Их применяют для повышения эффективности и скорости обмена цифровыми данными в процессе

формирования мобильных сервисов, а также для интеграции новых сегментов финансовых экосистем.

Наибольшее распространения в современной финансовой системе получили Открытые API. Основным характерным признаком, отличающим их от внутренних или партнерских API, является то, что они имеют архитектуру построения по открытым правилам, предоставляя при этом одинаковый доступ к цифровым данным для всех пользователей информации.

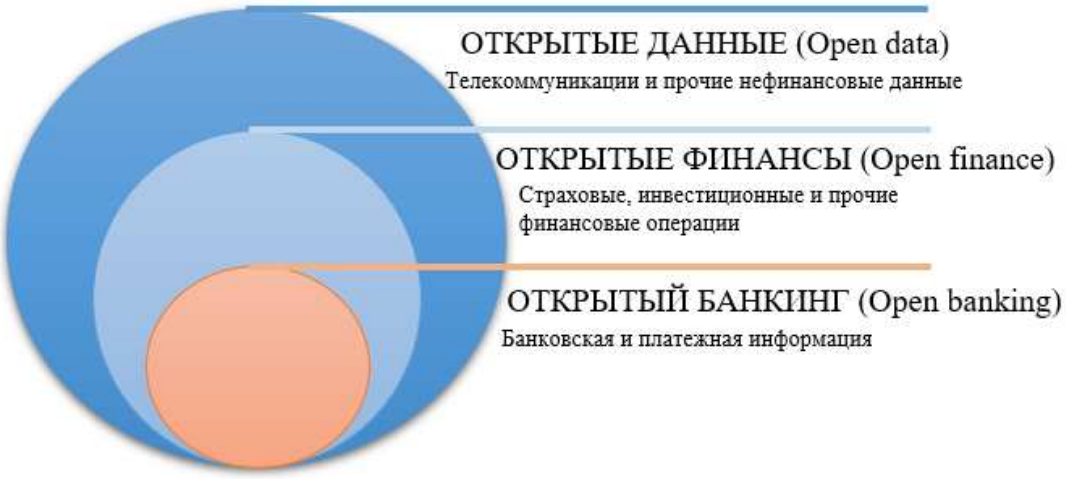
В рамках определения Центрального банка Российской Федерации Open API представляют из себя аппаратно-программные интерфейсы, используемые финансовыми структурами (в рамках требований Банка России) для осуществления взаимной передачи цифровой информации между провайдерами услуг (при обязательном согласии клиента) в рамках своей профессиональной деятельности.

В настоящее время применение интерфейсов Open API происходит в пределах 3 основных моделей (уровнях) обмена информации о клиенте, отраженных на рисунке 2.6:

а) Открытый банкинг. Осуществляется только через интеграцию между кредитными организациями, предусматривает передачу банковской и платежной информации о клиентах.

б) Открытые финансы. Осуществляется только через интеграцию между всеми субъектами финансовой системы: кредитными организациями, микрофинансовых организаций, страховыми агентами и биржевыми брокерами. Дополнительный объём информации о клиентах: страховые инвестиционные операции.

в) Открытые данные. Предполагают вовлеченность всех субъектов объединенной финансовой экосистемы в рамках передачи информации о клиенте. Добавляется пласт информации о покупательских предпочтениях, использовании услуг телекоммуникации и прочих нефинансовых данных о клиентах.



Источник: составлено автором [71].

Рисунок 2.6 - Уровни передачи данных на основе Открытых API

Обобщающей характеристикой, которая присуща всем уровням передачи данных на основе Открытых API, выступает возможность реализации трансфера финансовой информации клиента только при получении его согласия. Основополагающее различие моделей состоит в перечне пакетов данных, в рамках которых осуществляется обмен информации.

Для интеграции модели открытых финансов необходима постепенная разработка и введение стандартов Открытых API в каждом сегменте финансового рынка. Стоит отметить, данный процесс сопряжен с образованием дополнительного риска в виде появления серьезных конкурентных преимуществ у компаний нефинансового сектора, особенно экосистем крупнейших FinTech организаций. Так как данные экосистемы, с одной стороны, смогут извлечь выгоду от банковской информации о клиентах кредитных организаций, при этом для них требования об открытии и передаче данных будут носить лишь рекомендательный порядок.

Центральный банк идентифицировал данную проблему, поэтому уже сейчас начинается проработка необходимых условий и возможностей для последующего преобразования модели открытых интерфейсов API на уровень открытых данных, что будет обеспечивать равную вовлеченность и обязанности для всех субъектов трансфера данных.

Присоединение кредитной организации к интерфейсу модели Open Banking включает в себя 2 основных этапа. В первую очередь, следует разработать и осуществить выполнение необходимых стандартов Open API. После чего, необходимо обновление аппаратно-технической сертификации IT-систем банковской организации.

Классификацию в рамках стандартизации систем Open API, отражающая объёмы предаваемых данных, которую можно изобразить схематически в виде пирамиды, была отражена автором на рисунке 2.7.

Источник: составлено автором [71].
Рисунок 2.7 - Уровни стандартизации Open API

Перечень стандартов, которые обязательны к исполнению, сравнительно небольшой, вместе с этим на этом уровне будет покрываться самый большой объём передачи данных. Информация, обработку которой описывают данные стандарты, является наиболее значимой для цифровой безопасности клиента.

На следующем уровне расположены стандарты, которые обладают рекомендательным статусом. Объём предаваемых данных над данном уровне значительно меньше, информация не имеет столь критического значения.

Главной целью стандартов данного перечня выступает уменьшение объёма затрачиваемых ресурсов участников финансового рынка, участвующих в передаче данных. Наиболее инновационным уровнем выступает перечень партнерских стандартов API, необходимых для интеграции в бизнес-процессы партнёрских площадок.

Кроме разработки необходимых стандартов API, в числе прочих инфраструктурных обновлений следует выделить модернизацию системы информационной безопасности, а также создание специализированной платформы для коммерческих согласий клиентов на операции с их финансовыми данными. Основной для разработки данной платформой может послужить для инфраструктура Цифрового профиля, которая была запущена ещё в 2020 году.

Одним из основных лидером является по использованию технологий обмена платёжными данными выступает ПАО Сбербанк, которое предложило финансовому рынку, маркетплейсам и телекоммуникационным компаниям открыть друг другу данные для обмена клиентской информацией. Таким образом, ПАО Сбербанк выступает за внедрение открытых интерфейсов Open API в виде модели открытых данных.

У телекомов и маркетплейсов огромное количество клиентской информации, которая может быть полезна банкам и страховщикам. То же самое относится и к данным, собираемым финансовыми институтами.

В «Концепции внедрения открытых API на финансовом рынке», опубликованной в начале ноября, Центральный банк предлагал внедрять Open API сначала на финансовом рынке и только потом распространять эту практику на другие отрасли в виде открытых данных.

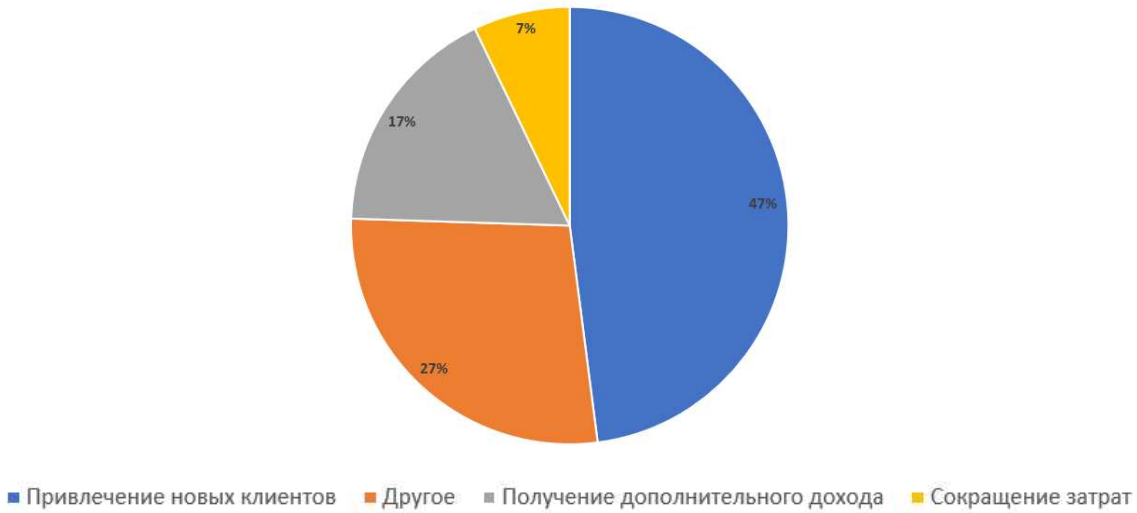
Предложенную ПАО Сбербанк идею поддерживают Банк ВТБ, Промсвязьбанк, Совкомбанк, Росбанк, «Тинькофф банк» и МКБ. Ряд банков уже внедрили в свои инфраструктуры открытые интерфейсы в рамках проекта ассоциации «Финтех» — среда открытого банкинга [58].

«Ростелеком» уже несколько лет движется навстречу концепции Open data, развивает и выводит на рынок сервисы на основе больших данных, которые помогают повышать эффективность бизнеса заказчиков. В то же время полноценный открытый доступ повышает риски компрометации данных, кратно увеличивая периметр кибератак.

«Билайн» готов предоставлять обезличенные агрегированные данные финансовым организациям на коммерческой основе. В целом компания поддерживает обмен данными, но отмечает, что он должен быть взаимным и на партнёрской основе. По комментариям представителя Tele2, необходимо понять, о каких именно данных идёт речь в рамках обмена в концепции Open data. Банки и операторы связи владеют персональной и коммерчески чувствительной информацией, которую нельзя публиковать в открытом доступе. Поэтому, пока нет чётко прописанной концепции, инициативы ПАО Сбербанк сложно реализовать.

Преимущества применения открытых интерфейсов API. Среди векторов для повышения эффективности, которые получает кредитная организация может в результате интеграции открытых программных интерфейсов выделяются модернизация осуществления онлайн-кредитования пользователей банковских услуг путём подбора персонализированных продуктов.

По данным опроса менеджеров кредитных организаций относительно основных преимуществ внедрения Open API, проведённого деловым порталом TAdviser, была составлена диаграмма, отражённая на рисунке 2.8. Основным положительным влиянием открытых интерфейсов было названо расширение клиентской базы (47%), также значительным преимуществом выступает получение дополнительного дохода (17%).



Источник: составлено автором [71].

Рисунок 2.8 - Преимущества интеграции Open API для банков России

На текущем этапе развития банковского сектора Российской Федерации наблюдается уменьшение количество кредитных организаций, при которой ключевую роль начинают играть крупнейшие банки, обладающие значительным капиталом для развития, в том числе в сфере операций с информационными данными. Данная тенденция приводит к возникновению риска монополизации использования данных.

На текущий момент банковский сектор России характеризуется высокой степенью концентрации банковского капитала. По основным показателям, определяющим степень монополизации банковской отрасли, наблюдается устойчивый рост за последние 5 лет.

Данная тенденция, во многом, вызвана развитием технологий дистанционного банковского обслуживания. Получение конкурентных преимуществ за счёт развития омниканального банкинга требует от кредитных организаций существенного размера капитала, которым обладают только крупнейшие игроки рынка, а построение собственной банковской экосистемы доступно только самым крупным банкам России.

Доля 200 крупнейших по активам кредитных организаций на российском банковском рынке за последние десять лет характеризовалась стабильным увеличением на февраль 2022 года достигла 99,69% (наибольший показатель за последние 10 лет). Доля пяти крупнейших банков возросла до 66,01%, а индекс Херфиндаля – Хиршмана находится на уровне умеренной монополизации, но имеет тренд к возрастанию. Расчёты показателей произведены автором в рамках Приложения А, результаты расчёта отражены в таблице 2.3.

Таблица 2.3. - Концентрация банковской деятельности

Показатель	Февраль 2022	Декабрь 2019	Декабрь 2017
Доля 200 крупнейших по активам банков, в процентах	99,69	99,58	99,47
Доля пяти крупнейших кредитных организаций, в процентах	66,01	63,69	62,33
Индекс Херфиндаля – Хиршмана	1 452	1 423	1 414

Источник: составлено автором на основании данных [101].

Применение открытых интерфейсов, позволяющих получать равный доступ к информации для всех участников обмена данными, ведёт к увеличению конкурентоспособности малых субъектов кредитного рынка за счет демонополизации доступа к данным пользователей.

Кроме того, открытые интерфейсы предоставляют ряд преимуществ, обеспечивающих более комфортный и эффективный пользовательский опыт клиентов банка.

а) Повышения уровня конкуренции будет заставляет кредитные организации повышать качество работы со своими клиентами, уменьшать взымаемую плату за обслуживание банковских операций, вместе с тем, расширяя перечень предлагаемых финансовых продуктов и услуг для привлечения новых пользователей.

б) Клиенты смогут более эффективно отслеживать и управлять своим финансовыми данными при помощи платформы согласий, что повысит информационную защищённость пользователей.

в) Использование Open API позволит персонализировать предлагаемый банковский продукт, так как в перечень предложений будут включены только самые актуальные для клиента банковские предложения.

Риски в рамках применения открытых интерфейсов API.

С точки зрения информационной безопасности подобный обмен данными несет в себе определенные риски. Но даже если добиться полностью защищенного обмена, все упирается в надежность хранения данных у конкретных участников бизнес-процесса. И вот в таком случае, уровень максимальной защиты этих данных будет равен силе защиты самого слабого участника обмена.

Второй ключевой момент — право пользователя на конфиденциальность. Подобный обмен должен быть согласован самим клиентом. Иначе получается, что бизнес имеет полную картину того, что из себя представляет личность. Он будет знать не только ее текущие расходы, доходы и траты, но вкусы и

предпочтения. И вот в таком разрезе защищать уже надо не пользовательские данные, а самих пользователей от вмешательства в их жизнь и влияния на нее.

Третий ключевой момент – ответственность участников бизнес-процессов за утечку консолидированных данных. Одно дело, если утекли паспортные данные без привязки их к доходу. И совсем другое — когда цифровой слепок информации, который достаточно четко характеризует персону, попадает в несанкционированный доступ к злоумышленникам. Чем больше людей имеет доступ к информации, чем выше сложность системы, тем более она требовательна в обслуживании. И тем выше цена ошибки и возможной утечки данных.

В контуре применения интерфейсов Open API следует выделить следующие риски, влияющие на всех участников финансового рынка, и пути минимизации их воздействия:

Риски ненадлежащего поведения поставщиков услуг, включая намеренный отказ от взаимодействия через Открытые API. В целях минимизации данного риска необходимо на законодательном уровне определить основные права и обязанности субъектов передачи финансовой информации с помощью Open API.

Риски разглашения конфиденциальной информации. Для уменьшения проявления данного риска следует разработать дополнительные стандарты информационной безопасности аппаратно-программного обеспечения при интеграции открытых интерфейсов.

Риски предоставления поставщиками данных недостоверной информации. В целях минимизации данного риска имеет смысл сформировать специализированное структурное подразделение в рамках Центрального Банка, которое будет заниматься мониторингом актуальности и корректности проходящих через интерфейсы Open API данных.

Неготовность инфраструктуры поставщиков данных для раскрытия в обязательном порядке Open API. Развитие использования данной технологии на банковском рынке необходимо производить поэтапно, чтобы у всех

участников было достаточно времени для построения необходимой инфраструктуры [64].

Таким образом, идея Open data требует всесторонней защиты и очень бережного обращения. Сейчас данные – это актив. Раз данные чего-то стоят, ими не будут делиться просто так. В данном вопросе ключевой блокер — само понятие открытых данных, которое нужно ввести законодательно, а также определить, что не может являться открытыми данными.

Без этого, на практике, банки сразу столкнуться со множеством законодательных барьеров: персональные данные, коммерческая тайна, авторское право, информация ограниченного доступа. Если данные были получены из общих баз знаний или из интернета, то это еще не открытые данные, а общедоступные. Нужно сформулировать требования к обработке и хранению открытых данных. Без законодательного определения открытых данных и определения в подведомственных структурах правил к обработке таких данных, концепция Open data не имеет смысла.

Внедрение Open API в работу банковского сектора станет драйвером для разработки инновационных технологий, даст импульс для формирования конкурентной среды, а также значительно увеличит доступность банковских продуктов для клиентов кредитных организаций. Кроме того, услуги банков также подлежат интеграции в бизнес-схемы контрагентов, например, маркетплейсов, что позволит увеличивать прибыль за счёт синергетического эффекта.

Таким образом, резюмируя основные итоги по данному параграфу, целесообразно отметить следующее. На основе анализа опыта российских и зарубежных кредитных организаций были выделены лучшие практики по управлению банковскими рисками в рамках системы дистанционного банковского обслуживания.

Таковыми можно назвать применения банками инновационных технологий в целях снижения воздействия возникающих рисков и модернизации системы управления рисками электронного банкира в целом.

Среди них стоит особо выделить применение технологии «Больших данных» для защиты информационных ресурсов от хищения, технологии блокчейн для обеспечения безопасность использования электронных систем и биометрической идентификации.

Внедрение Open API в работу банковского сектора станет драйвером для разработки инновационных технологий, а также значительно увеличит доступность банковских продуктов для клиентов кредитных организаций.

Кроме того, данная технология уменьшает воздействие риска монополизации: применение открытых интерфейсов, позволяющих получать равный доступ к информации для всех участников обмена данными, ведёт к увеличению конкурентоспособности малых субъектов кредитного рынка за счет демонополизации доступа к данным пользователей.

С учетом основных результатов по второму разделу диссертации (приведены ниже) в следующей главе представляется целесообразным исследовать основные пути модернизации системы управления рисками дистанционного банковского обслуживания кредитной организации, в том числе, в области внутреннего контроля кредитной организации, и в направлении обеспечения безопасности в области киберрисков.

В рамках главы обозначены наиболее перспективные тенденции по модернизации услуг дистанционного банковского облуживания. Кроме того, автором определены наиболее перспективные инновационные технологии банковской сферы и основные области их применения: улучшение качества обслуживания клиентов и применение новых методов в управлении банковскими рисками, в том числе, в области оценки данных рисков.

Даны практические рекомендации по минимизации риска недоверия к использованию банками цифровых технологий. Отмечено, что наиболее результативной мерой является создание единого рейтинга банков на основе критериев оценки уровня защищенности персональных данных клиентов, который стимулирует банки к добросовестному поведению по отношению к персональным данным своих клиентов. Готовность человека доверять

цифровым инновациям, чтобы полностью понимать и пользоваться ими, является важнейшим фактором для дальнейшего развития в области банковской цифровизации.

Обозначены основные особенности функционирования системы банковского надзора в Российский Федерации. Кроме того, автором определены наиболее перспективные направления его совершенствования, включая использование инновационных разработок банковской сферы, таких как способы машинного обучения, а также SupTech и RegTech технологии, и основные направления их применения: поддержание устойчивого функционирования национальной банковской системы в условия применения дистанционного-банковского обслуживания, а также обеспечение полной защиты законных интересов каждого субъекта банковской деятельности.

Анализ опыта российских и зарубежных кредитных организаций позволил выделить лучшие практики по управлению банковскими рисками в рамках системы дистанционного банковского обслуживания.

Таковыми можно назвать применения банками инновационных технологий в целях снижения воздействия возникающих рисков и модернизации системы управления рисками электронного банкира в целом. Среди них стоит особо выделить применение технологии «Больших данных» для защиты информационных ресурсов от хищения, технологии блокчейн для обеспечения безопасность использования электронных систем и биометрической идентификации.

Внедрение Open API в работу банковского сектора станет драйвером для разработки инновационных технологий, а также значительно увеличит доступность банковских продуктов для клиентов кредитных организаций. Данная технология уменьшает воздействие риска монополизации: Применение открытых интерфейсов, позволяющих получать равный доступ к информации для всех участников обмена данными, ведёт к увеличению конкурентоспособности малых субъектов кредитного рынка за счет демонополизации доступа к данным пользователей.

Глава 3
Направления модернизации системы управления рисками дистанционного банковского обслуживания в рамках кредитной организации

3.1 Особенности подходов к оценке рисков дистанционного банковского обслуживания

Как было выявлено ранее, на текущий момент банки находятся в реалиях среды крайне высокой конкуренции, в связи с чем, менеджмент кредитных организаций вынужден искать новые пути по получению конкурентных преимуществ. Одним из основных методов для достижение данной цели служит внедрение и развитие инновационных технологий дистанционного банковского облуживания, которое способствует сокращению операционных расходов и расширению возможностей по эффективному обслуживанию клиентов. В данном направлении развития кредитные организации столкнулись с новым видом конкурентов - финтех–компаниям, которые отличаются динамичным развитием на протяжении последних лет. Они также предлагают своим клиентам разнообразные финансовые сервисы, в том числе, по осуществлению платежей и переводу денежных средств, зачастую предоставляя свои услуги на более выгодных условиях чем классические банковские институты [47].

Чтобы справится с данной конкуренцией, кредитным организациям необходимо сокращать время выпуска новых банковских продуктов на рынок, что также требует внедрение способов по экономии времени на комплексный анализ сопутствующих рисков. Быстрое появление новых продуктов требует от регулирующих органов такой же оперативности в изучении уязвимости программ и составлении регламентирующих документов, способных компенсировать возможные угрозы информационной безопасности.

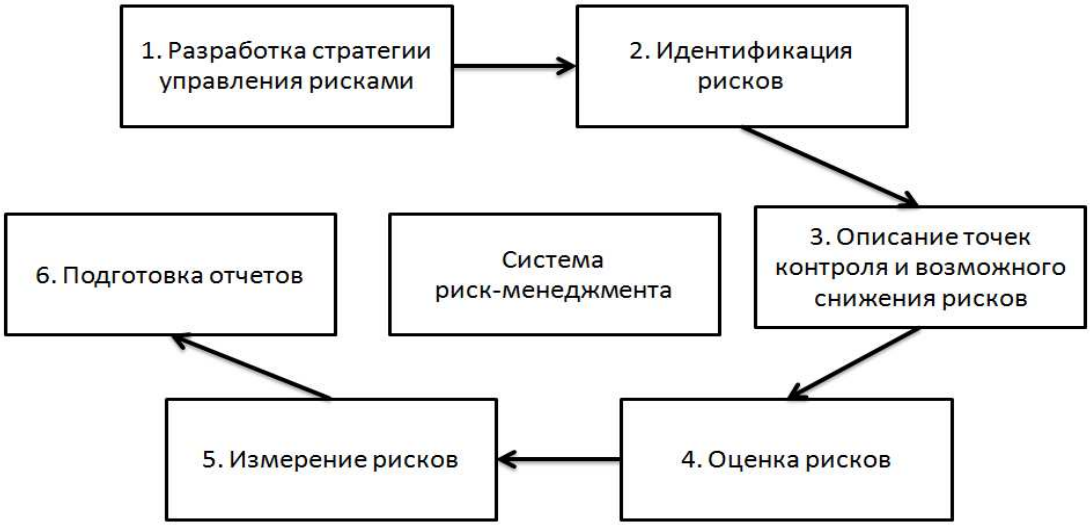
Еще более важное значение в данных условиях приобретает вопрос рационального распределения финансирования в пользу служб информационной безопасности. Так как внедрение новых продуктов должно происходить вместе с адаптацией к ним элементов поддержания безопасности.

Помимо увеличения скорости внедрения банковских продуктов и защитных механизмов необходимо повышать эффективность анализа основных рисков. Качественная система анализа рисков позволяет сократить расходы и перенаправить финансирование в подразделения, для которых это необходимо в первую очередь.

Таким образом, мы приходим к выводу о том, что все банки сталкиваются с потребностью в модернизации системы оценки риска, которая способствует уменьшению объёма неблагоприятных событий и улучшает финансовый результат организации.

Менеджмента риска представляет из себя комплексную систему, которая состоит из взаимосвязанных элементов, складывающихся в единый процесс, целью которого является принятие решений в условиях неопределенности, возникающей при банковской деятельности.

Согласно методологии, процесс управления риском дистанционного банковского обслуживания осуществятся кредитным организациями в несколько этапов как показано на рисунке 3.1.



Источник: составлено автором на материалах [16].
Рисунок 3.1 – Этапы системы управления риском

Важным сопутствующим элементом также является мониторинг принимаемых мер с точки зрения их эффективности, проводимый на основании данных о потерях вследствие реализации рисков.

Как было отмечено, оценка риска выступает элементом процесса управления риском, сущность которого заключается в совокупности аналитических мероприятий, которые позволяют:

- идентифицировать неблагоприятные события, которые могут принести финансовый ущерб, а также причины их возникновения;

- определить вероятность их проявления, а также возможные последствия;

- указать перечень факторов, способствующих уменьшению вероятности возникновения нежелательных результатов риска.

Приоритетной целью деятельности по оценке риска выступает выявление на основании объективных данных информации, которая требуется для принятия взвешенного решения по возможным способам минимизации выявленного риска.

Оценка риска помогает кредитным организациям в обеспечении следующего ряда функций:

- определение возможных неблагоприятных событий и влияния их последствий на наступление значительных финансовых потерь для кредитной организации, способных привести к нарушению операционной деятельности;

- появляется возможность провести сравнение уровня риска с показателями аналогичных банковских организаций;

- получение информации о возможности вывода новых банковских продуктов на рынок рисков, сопряженных с данным процессом;

- минимизация случаев появления новых инцидентов на основании исследования предыдущего опыта управления рисками;

- анализ риска на всех этапах жизненного цикла банковских продуктов.

Методы оценки банковских рисков подразделяются на качественные, количественные и смешанные.

Качественная оценка риска – метод, который характеризуется высокой долей субъективности проводящего исследование эксперта, остаточной неопределенностью и противоречивостью. Данный метод не подходит для качественного финансового планирования и анализа профиля риска в целом. В качественных методах оценки риск определяется на основании субъективных описательных параметрах вместо использования математических методов.

Количественная оценка риска – метод оценки риска, основывающийся на использовании данных, включающий в себя процесс моделирования и задействующий математический и статистический инструментарий. Данный метод отличается масштабируемостью, адаптивностью к любой корпоративной модели управления, гибкостью и возможностью неоднократного повторения. Зачастую используется в целях принятия решений относительно стратегического инвестирования и вопросов страховании риска.

Кроме того, классификация методов оценки риска банковской деятельности производится по критерию «применение математических методов». На основании наиболее применимых элементов математического аппарата выделяют следующие методы оценки риска [50]:

а) Эконометрические методы, которые базируются на инструментах линейного и многомерного дискриминантного анализа, регрессионного анализа, анализа выживаемости, дающего возможность дать оценку возможности наступления события (например, дефолта портфеля).

б) Метод нейронных сетей – модель, в основе которой лежит идея использования алгоритмов искусственного интеллекта, которые имитируют процессы работы головного мозга человека. Основной задачей данной модели является описание процесса появления банковского риска и управление им.

в) Методы математического программирования, позволяющие на основании точных расчётов определить оптимальные параметры банковских

продуктов или наиболее эффективное распределение клиентов в кредитном портфеле банка.

г) Экспертные методы осуществляются высококвалифицированными специалистами с целью последовательного моделирования этапов процесса оценки риска. Для проведения экспертных методов необходимы следующие составляющие: основные логические правила, необходимые для вывода данных, информация касательно количественных и качественных показателей объекта исследования и блок для ввода ответов на вопросы информационной системы.

На текущий момент математические методы оценки риска используются как вспомогательные модели, однако, благодаря их активному развитию, они получают все большее распространение. Особенно актуальны они при оценке рисков дистанционного банковского обслуживания.

В настоящее время дистанционное банковское обслуживание все больше проникает в повседневную жизнь клиентов и выступает незаменимым элементом сервисов, которые предоставляются кредитными организациями. Поскольку часть рисков электронного банкинга носит специфический характер, методы их оценки могут носить характерные отличия.

В практике большинства государств в качестве основного метода оценки риска организациями выступает измерение экономической стоимости риска или возможных потерь ValueatRisk (VaR). Под данным терминам выступает методика количественной оценки вероятности финансового риска, основанная на параметре стоимостной меры риска. Экономическая суть предложенной методики заключается в переводе значений уровня риска финансово-кредитной организации в определённые денежные единицы. Чтобы произвести расчёт вероятности наступления рисков банки используют статистику, накопленную за долгосрочный период. Это создаёт препятствие для применения данной методики в оценке рисков дистанционного банковского обслуживания России, поскольку временной горизонт статистки, необходимый для точного анализа, ещё не достиг оптимальных значений.

Помимо этого, риск в сфере удаленного банковского облуживания сопряжен с рядом факторов, которые не поддаются количественной оценке. Чтобы дополнить инструментарий методики VaR ведущие экономисты разработали смешанные методики оценки и управления рисков в системах дистанционного банковского обслуживания. Данные методики представляют из себя комбинацию профессиональной экспертизы и самооценки, где расчёт параметров риска производится на основании его факторов. Данная комплексная экспертиза помогает с высокой долей достоверности количественно оценить риски, которые связаны дистанционным банковским облуживанием, а также выделяет сферы для дальнейшего анализа [19].

Таким образом, мы можем прийти к выводу, что специалисты в области управления рисков информационной безопасности преимущественно применяют качественные методы оценки рисков ввиду того, что для количественной оценки обязательным условием является наличие ревалентной статистики по нахождению уязвимостей информационных систем банка, случаям и способам кибер-атак на них. С учётом того факта, информационно-программное обеспечение, конфигурация внутренних банковских систем и сами способы проявления угроз динамично трансформируются, то своевременно собрать необходимую статистику для оценки рисков представляется тяжелой задачей.

Наряду с очевидными преимуществами развития технологий дистанционного банковского обслуживания коммерческих банков, данный процесс влечёт за собой расширение перечня банковских рисков. В основном меняется их структура, риски усложняются в техническом плане, меняется их профиль.

Вместе с прогрессом в развитии банковских технологий возрастает необходимость в совершенствовании системы регулирования сферы риск-менеджмента, особенно в видах деятельности, связанных с электронным банкингом. В данном вопросе можно выделить два направления:

1) усложнение профиля операционного риска путем расширения его базы за счет внедрения новейших технологий дистанционного банковского обслуживания;

2) повышение основных требований в рамках оформления контура информационной безопасности банковского учреждения, который связан с серьезным повышением количества преступлений, ориентированных на пользователей дистанционных банковских услуг [76].

При внедрении технологий электронного банкинга наибольшему расширению подвергся профиль операционного риска. Базельский комитет по банковскому надзору, выступая одни из основных создателей методологии оценки банковских рисков в мире, подготовил ряд документов по модернизации банковского надзора, в рамках которых предлагает банковским институтам формировать резерв под операционный риск, в который также включается резерв и под риски кибер-безопасности, принимая во внимание динамичное изменение информационных технологий. Согласно данным рекомендациям, формируется система управления операционным риском при внедрении технологий электронного банкинга, представленная на рисунке 3.2.

Риск-аналитики и сотрудники службы внутреннего контроля обязаны владеть методиками по оценке риска возникновения кибератак, выявлять наличие технических уязвимостей и несовершенств в системе, уметь рассчитывать возможный масштаб ущерба и прослеживать взаимосвязь конкретных факторов риска с масштабом финансовых, репутационных и других потерь.

В силу того, что банковский сектор на современном этапе в последнее время представляет собой, возможно, наиболее благоприятную сферу деятельности для кибер-мошенников, что подтверждается статистическими данными о росте объёма зафиксированных случаев киберпреступлений в деятельности кредитных организуй на территории Российской Федерации и всего мира, целесообразно заниматься разработкой мер, ориентированных на формирование высокого уровня информационной безопасности.

Источник: составлено автором на материалах [62].

Рисунок 3.2 – Системы управления операционным риском в технологиях электронного банкинга

Основная задача банковского риск-менеджмента состоит в оптимизации банковских бизнес-процессов.

Перед ведущими организациями банковского сектора возникает задача по созданию обновленных методов и процессов по оценке рисков, которые сопряжены со спецификой работы систем дистанционного банковского обслуживания и функционирования банков в киберпространстве [103].

Для начала необходимо определить сущность термина «киберпространство» и его ключевые особенности.

На основании международного стандарта ISO/IEC 27032:2012, определением киберпространства следует считать «комплексную среду, которая образовалась вследствие взаимосвязи подсоединенных к системе «Интернет» пользователей, аппаратно-программного обеспечения и сервисов, не существующую в материальной форме». Следовательно, кибербезопасность трактуется как «соблюдение конфиденциальности, целостности и доступности информации в киберпространстве» [11].

В области банковской деятельности было сформировано специфическое понятие как «риск воздействия кибератак», с помощью которого возможно определить норму увеличения классических банковских рисков, проявляющихся по причине проведение кибератак на системы дистанционного банковского обслуживания организаций кредитно-финансовой сферы [48].

Под сущностью кибератак следует определить действия хакеров, инсайдерские происшествия и нарушения в работе банковских информационных систем.

Для точной оценки риска воздействия кибератак не следует ограничивать анализ исключительно на внутренней среде кредитно-финансовой организации, необходимо также досконально изучить потенциал и ресурсы лиц, занимающихся преступлениями в цифровой среде.

Выделим основные методы оценке рисков дистанционного банковского обслуживания. В соответствии с ГОСТ Р ИСО/МЭК 31010:2011 «Менеджмент риска. Методы оценки риска», оценка риска может быть осуществлена с разным уровнем детализации при помощи применение единственного или сразу некоторых методов различной степени сложности.

Общее количество методов оценки риска, описанное в данном стандарте, составляет 31, но для оценки рисков в сфере дистанционного банковского обслуживания наиболее актуальны только несколько из них:

– Метод «Дельфи» – обработка комплексной оценки сообщества экспертов, представляющих свою точку зрения самостоятельно и анонимно, обладая при этом правом изучить оценки прочих экспертов.

– Структурированный анализ сценариев методом «что, если» - метод обработки сценариев, основанный на использовании фразы-подсказки «что, если» для идентификации рисков и формирования сценариев их развития.

В модернизации системы управления риска воздействия кибератак самых существенных достижений добились научные объединения и организации в отрасли информационных технологий, которые сформировали разнообразные методики оценки рисков.

- Risk Analysis and Management Method (CRAMM), разработанная в Великобритании;

- методика анализа и управления рисками RiskWatch из США;

- ГРИФ 2006, разработанный российской компанией «Digital security Office»;

- руководство по управлению рисками от компании Microsoft.

Вышеуказанные методы предоставляют возможность определить масштабы риска воздействия кибератак и требуемый объём вложений в системы минимизации риска информационный безопасности для того, чтобы гарантировать уровень её наибольшей результативности. Российские программы для оценки рисков сводятся только к продукту «ГРИФ 2006», что обуславливает вопрос необходимости дополнительных инвестиций в данном направлении.

Совершенствование финансовых услуг усложняет структуру финансовых технологий, способствует повышению их разнообразия и диверсификации рискового портфеля. В последние десятилетия по всему миру были отмечены существенные изменения в основных принципах деятельности коммерческих банков.

Помимо появления широкого спектра возможностей вследствие изобретения новых финансовых инструментов возникла необходимость регулирования ранее не учитываемых видов риска и создания соответствующих стандартов для управления ими.

Серия международных стандартов ISO/IEC 27000 включает стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC). Каждый из них направлен на исследование определённых задач по управлению информационной безопасностью и минимизации возможных рисков.

Кроме этого, комплекс документов по стандартизации Центрального банка Российской Федерации содержит единый подход к обеспечению информационной безопасности организаций банковской системы (далее -ИББС) и рекомендации по стандартизации (РС) с учётом требований российского законодательства. Фундаментальный стандарт в рассматриваемой сфере – СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

Невзирая на то, что имеется большое количество моделей оценки кибер-рисков, перед автором была поставлена задача по созданию собственной методике оценки рисков дистанционного банковского обслуживания, так как при подборе актуального метода можно столкнуться с последовательность сложностей:

– большинство методов плохо справляются с значительными объемами рассматриваемой информации, а также большому числу банковских процессов;

– нерациональность выбора методов, которым необходима оценка стоимости активов, в связи с тем, что ценность некоторых активов банка проблематично посчитать (например, оценить количественную ценность продукта «Сбербанк Онлайн»);

– отсутствие универсальности в применении методов сценарного анализа, основанных на том, что вероятность воплощения в жизнь события равняется произведению вероятностей всех инцидентов, которые являлись его причиной. Представленные модели применимы не ко всем типам риска. Например, они могут быть эффективны для анализа сбоев в программе, но не ревалентны для оценки риска кражи информации;

– проблема применения балльных методов оценки рисков, так для их использования требуется серьезная доработка, позволяющая связывать значительное количество факторов, оказывающих влияние на риск [52].

Стоит отметить, риск информационной безопасности является лишь одним из проявлений общего контура рисков дистанционного банковского обслуживания. Для каждого риска дистанционного обслуживания формируется перечень возможных угроз и мер защиты.

Наиболее перспективной является разработка модели оценки именно данного вида риска, поскольку основополагающим условием, которое предполагает наиболее полное обеспечения гарантий непрерывной работоспособности информационно-технологических систем банка выступает их системная надежность и устойчивость при осуществлении возможных киберпреступлений со стороны злоумышленников.

Оценка риска информационной безопасности по авторской методике проводится в 3 этапа:

Начальный этап заключается в определении системы риск-факторов для оцениваемого типа риска. Для каждого риска дистанционного обслуживания формируется перечень возможных угроз и мер защиты. Веса каждого фактор могут быть скорректированы экспертом, в качестве примера, примем равные весовые коэффициенты для каждого вероятности фактора и разные для факторов ущерба.

Следующий этап заключается в получении экспертной оценки риск-факторов. Необходимо обособленно производить оценку каждого риск-фактор по пятиуровневой шкале. Критерии оценки основаны на показателях вероятности и возможного ущерба, подробная характеристика которых дана на рисунке 3.3.

Таким образом, вероятность риска составляет 56,25% по формуле (3)

$$0.25 * 50\% + 0.25 * 25\% + 0.25 * 75\% + 0.25 * 75\% = 56{,}25\%, \quad (3)$$

Ущерб риска составляет 45% по формуле (4)

$$0.20 * 25\% + 0.1 * 75\% + 0.4 * 25\% + 0.3 * 75\% = 45\%. \quad (4)$$

Весовые коэффициенты	0,25	0,25	0,25	0,25
Вероятность ***56,25%***	Риск-факторы			
	Частота кибератак	Степень информационной защиты банка	Тип злоумышленника	Методы атаки
Очень высокая 95%	Раз в день	Очень низкая	Сотрудник банка	Использование ВПО
Высокая 75%	Раз в неделю	Низкая	**Хакерская группировка**	**Социальная инжинерия**
Средняя 50%	**Раз в месяц**	Средняя	Хакер-профессионал	Хакинг
Низкая 25%	Раз в квартал	**Высокая**	Начинающий хакер	Поиск веб-уязвимостей
Очень низкая 5%	Раз в год	Очень высокая	Лицо без квалификации	Подбор учётных данных

Весовые коэффициенты	0,20	0,10	0,40	0,30
Ущерб ***45,00%***	Риск-факторы			
	Тип украденных данных	Вероятность штрафа	Время остановки процессов	Огласка в СМИ
Очень высокая 95%	Данные платёжных карт	Очень высокая	Более одного дня	Международная
Высокая 75%	Персональные данные	**Высокая**	В течение дня	**Федеральная**
Средняя 50%	Учётные данные	Средняя	Менее часа	Региональная
Низкая 25%	**Переписка**	Низкая	**Менее 15 минут**	Локальная
Очень низкая 5%	Неконфиденциальная информация	Очень низкая	Без остановки процессов	Отсутствует

Источник: составлено автором.

Рисунок 3.3 - Критерии оценки риск факторов вероятности и ущерба

На заключительном этапе производится вычисление рейтинга информационной безопасности.

Главная особенность заключается в том, что имеется возможность совместить значительное количество полученных экспертных мнений и весовых коэффициентов в одном значении рейтинга риска (R).

Данные вычисления не только помогают принять во внимание весь объём мнений экспертов, но и различия в показателях весовых коэффициентов, что положительно сказывается на объективности оценки. Рейтинг риска (R), выраженный числовым значением от 0 до 1, и соответствующий ему уровень риска, можно определить по указанным в таблице 3.1 значениям.

Таблица 3.1 – Система определения соответствующего рейтингу (R)уровня риска.

Рейтинг риска	Низкий	Средний	Высокий	Критический
R	$0,25 < R$	$0,25 \leq R \leq 0,5$	$0,5 \leq R \leq 0,75$	$0,75 > R$

Источник: составлено автором.

Уровень риска определяется средневзвешенной по факторам риска, что в нашем примере составляет 50,81%, что соответствует высокому уровню риска.

Таким образом, резюмируя основные результаты по данному параграфу, целесообразно отметить следующее. Был комплексно рассмотрен механизм оценки рисков дистанционного банковского обслуживания. Выделены основные методы, применимые с учётом для специфики электронного банкинга, обоснованы два основных направления, в которых необходимо производить совершенствование системы риск-менеджмента: регулирование расширения профиля операционных рисков банка и противодействие участившимся случаям кибер-преступлений.

Разработана комплексная модель оценки риска информационной безопасности, как одного из основных видов проявления рисков дистанционного банковского обслуживания, базирующаяся на методах и индикаторах оценки рисков, стрессовых параметрах и статистическом аппарате для проведения стресс-тестирования. С учетом изложенного следующим действием представляется необходимым исследовать методы по оптимизации систем внутреннего контроля банков. Данные положения рассмотрены подробно в следующем параграфе.

3.2 Оптимизация системы внутреннего контроля кредитной организации в направлении обеспечения безопасности дистанционного банковского обслуживания и страхования киберрисков

Важное значение в формировании механизма по управлению рисками имеет эффективно функционирующая система внутреннего контроля банка. Правильно выстроенная система внутреннего контроля в финансово-кредитных организациях вступает незаменимой частью комплексной системы управления деятельностью банка и позволяет сохранять экономической стабильности и способствует повышению конкурентоспособности ввиду более высокой прибыльности операционной деятельности.

Риск-ориентированный внутренний контроль — комплекс мероприятий, направленных на установление возможных рисков, проявляющихся при осуществлении банковской деятельности. Механизм формируется на базе беспрерывного исполнения контрольных процедур по всей работе банковских организации.

В области исполнения механизмов внутреннего контроля в финансов-кредитных организациях, использующих при предоставлении банковских продуктов и услуг каналы дистанционного обслуживания, необходимо использовать не только стандартные методы управления банковскими рисками, но и опираться на рекомендации, предложенные к исполнению Базельским комитетом по банковскому надзору. Данная деятельность предполагает формирование эффективных стратегических решений по предоставлению пользователям услуг через аппаратно-информационное обеспечение, построение системы постоянного мониторинга рисков.

На основании комплекса данных рекомендаций предусматривается, что в основную стратегию кредитной организации включены положения по установке, использованию и модернизации компонентов электронного банкинга, основные показатели, которые позволяют предоставить адекватную

оценку результатов функционирования всего банка и его отдельно взятых департаментов.

Распределение полномочий между подразделениями банка в сфере управления рисками дистанционного банковского обслуживания следует осуществлять наиболее рационально, для того чтобы сохранить актуальность, всеобъемлемость и ревалентость информирования топ-менеджмента банка по средствам предоставления своевременной отёчности:

– относительно статуса и особенностей функционирования технического обеспечения дистанционного обслуживания;

– об обнаруженных ошибках в работе информационного-технического сектора кредитной организации;

– о полном перечне банковских рисков, сопряженных с работой финансово-информационных систем;

– об успешности реализации механизмов по регулированию банковских рисков ДБО;

– о методиках принятия решений при реализации последствий, которые оказать негативное влияние на защиту, финансовую стабильность или банковской организации.

К описанным процедурам наиболее эффективно задействовать департаменты банка, которые вовлечены в процессы реализации дистанционного обслуживания клиентов и контролируют использование цифровых средств, реализацию технической безопасности, правовое регулирование действий банковской организации, исполнение процессов обеспечения внутреннего контроля.

В регламентной документации банковских подразделений, деятельность которых связана с контролем дистанционного банкинга и мониторингом функционирования осуществляющих его информационных систем, обязательно требуется назначить ответственные органы управления из структурных департаментов банка:

– в делегации компетенций среди субъектов управления банковской структуры (советом директоров, исполнительным директором, финансовым директором, руководителем службы внутреннего контроля);

– диверсификация требований к ответственности для банковских подразделений и сотрудников, в должностные инструкции которых входят обязанности по выполнению операций в контуре дистанционного обслуживания клиентов, также и управление системой рисков, связанных с реализацией электронного банкинга;

– фиксация допустимых значений в проявлении банковских рисков, согласованной внутри банковской организации при функционировании систем удаленного обслуживания;

– установление механизма передачи информации для выбранных органов управления банка о найденных проявлениях в области банковских рисков и реализация мероприятий, направленных на снижение возможных убытков организации.

Для формирования предпосылок, способствующих наиболее результативному управлению системой рисков, следует сформировать внутрибанковские регламенты, в рамках которых будут сформулированы основополагающие принципы минимизации каждого типа банковских рисков. Данные документации по контролю над системой рисков с учетом применения технологий дистанционного обслуживания должны быть согласованы с советом директоров [8].

Система управления рисками, сопряженными с использованием технологий электронного обслуживания клиентов, состоит из определения, оценки, мониторинга и сокращения воздействия риска.

В принятых политиках банка желательно сразу обозначить главные принципы риск-менеджмента:

— механизмы определения, оценки и мониторинга рисков;

— ведущие методики по организации контроля и минимизации воздействия рисков;

— регламент передачи о результатах мониторинга до менеджмента финансовой организации.

Для осуществления внутреннего контроля не менее важным представляется процесс распределения полномочий среди вовлечённых подразделений кредитной организации, возможное воплощение которого представлено в таблице 3.2.

Таблица 3.2 – Распределение полномочий по осуществлению внутреннего контроля банка

Роль в системе управления рисками	Полномочия сотрудника
Аналитик финансовых рисков	- анализ отдельных проявлений финансового риска; - формирование сводного отчёта по рискам
Риск-менеджер	- проводят комплексную оценку финансовых рисков; - составляют и обновляют документацию, оформляющую осуществление внутреннего контроля
Руководитель направления финансовых рисков	- осуществляют оценку внутреннего контроля; - принятие решения об изменении операционных бизнес-процессов
Топ-менеджмент	- организация и осуществление внутреннего контроля составления финансовой отёчности кредитной организации в целом; - формирование сводного дэшборда; - принятие решения об изменении стратегических бизнес-процессов

Источник: составлено автором на материалах [90].

Банковские организации имеют возможность создания собственных методов оценки риска, как например ПАО Сбербанк, модель оценки риска которого была приставлена в прошлой главе, либо пользоваться методиками, уже применяемыми в банковской практике.

Осуществление контроля за организацией банковской системы управления рисками необходимо производить на непрерывно, в порядке, определёнными внутренними регламентами финансовой организации, приятыми на уровне высшего руководства.

Регулярность осуществления мониторинга рисков следует устанавливать, опираясь на уровень его значимости для сохранения непрерывности проведения кредитно-финансовой деятельности организации и эффективности банковских операций.

Организация контроля за актуальным выявлением, последующей оценки и осуществлением комплекса мер по уменьшению проявления банковских рисков, вызванных использованием технологий дистанционного обслуживания, а также формирование перечня необходимых рекомендаций в данной области необходимо делегировать сотрудникам департамента внутреннего контроля.

В рамках предложений по построению механизма внутреннего аудита при наличии в банке каналов ДБО, следует принимать во внимание положения Базельского комитета по банковскому надзору о некорректности единообразного подхода, поскольку банковские аппаратно-технические программы имеют индивидуальную архитектуру построения, а следовательно, и общего контура сопряженных рисков, методик и инструментов внутреннего контроля.

Особенно значимым для коммерческих банков предстаёт персональный учет всего спектра характеристик установленных инновационных технических решений.

В значительном количестве банковских организаций, использующих технология дистанционного банкинга, обобщенная характеристика комплекса процедур внутреннего контроля должна включать базовые возможности содержания и реализации функционала внутреннего контроля в данном коммерческом банке.

Было выявлено, что обобщенное проведение процессов внутреннего контроля банка может опираться на модели непрерывного циклического процесса менеджмента (модели Деминга) и включать разделение этапов модели на стадии формирования системы электронного банкинга, часто определяемые при реализации данных систем [89].

Составные элементы механизма процедуры по организации внутреннего контроля должны быть осуществлены последовательно, на каждом из этапов формирования системы электронного банкинга, показанных на рисунке 3.4.

Источник: составлено автором на материалах [62].
Рисунок 3.4 - Этапах жизненного цикла системы электронного банкинга

В 2022 году список основных целей киберпреступников помимо перехвата финансовой информации дополнился дестабилизацией политической ситуации в связи с началом специальной военной операции. С конца февраля 2022 года значительно участились массированные DDoS атаки. Эксперты отмечают двадцатикратное увеличение количества кибератак. Помимо количества стремительно увеличилась продолжительность атак, так по данным исследования «Лаборатории Касперского» в феврале-марте 2021 года атаки продолжались в рамках 12 минут, в феврале-марте 2022 года средняя продолжительность составила 30 часов. Чаще всего объектами киберпреступлений становились персональные данные учетных профилей [95].

Вероятность нарушения кибербезопасности российских кредитных организаций повысилась с введением санкционного режима и включением в SDN-лист со стороны западных стран-партнеров. Данные меры приводят к невозможности пролонгирования сроков использования и обновления

лицензионного зарубежного ПО, в связи с чем возникает экстренная необходимость в переводе всей банковской системы на альтернативные либо национальные ПО. Попытка смены информационный и технологической базы в сжатые сроки грозит повышением уязвимости для киберпреступлений.

В ходе проведения исследования мирового рынка киберстрахования агентством PwC было выявлено, что лидером в данной области является США, на долю американских компаний приходится 90% всего страхового обеспечения. В условиях расширения профиля риска киберпреступлений лишь треть компаний имеет достаточный уровень киберпокрытия. [104]

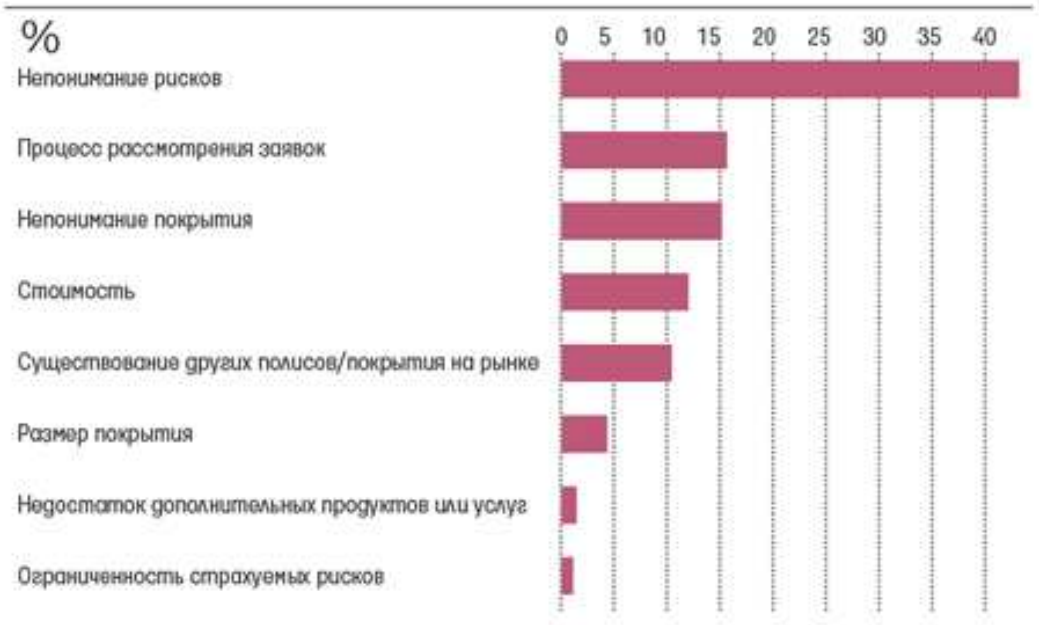
Процесс развития рынка киберстрахования в России на данный момент находится в фазе активного роста, спрос крупного бизнеса на услуги страхования киберрисков за период с 2021 г. по 2022 г. возрос на 60%, такое изменение было зафиксировано в исследовании «АльфаСтрахования».

Полис киберстрахования это страховый продукт, созданный с целью обеспечения безопасности юридических лиц и их клиентов от рисков, возникающих в рамках широкого использования информационных технологий, хранения и обработки большого объема конфиденциальных данных.

Покрытие страхового полиса включает в себя возмещение потерь, возникающих в связи с кражей, изменением или уничтожением хранящихся данных, которые, в свою очередь, происходят в результате кибератак. Возмещению подлежат такие негативные последствия, как простои операционной деятельности, увеличение убытков, выплаты клиентам в случае утечки данных, так же вызванные киберпреступлениями.

Эволюция современных технологий и цифровизация сферы экономики и финансов привносят значительные изменения в традиционные методы страхования. Расширяется программа применения цифровых технологий для упрощения организации взаимодействия людей и организаций, повышения качества жизни и роста благосостояния общества. В рамках реализации программы «Цифровая экономика РФ», внедряются наиболее технологичные решения [98].

Выводом большинства исследований об особенностях рынка киберстрахования является обнаружение зависимости его формирования от множества факторов, сдерживающих уровни продаж страховых полисов, покрывающих убытки от киберрисков. К таким факторам относятся недостаточная проработанность правовой базы, отсутствие принятых общемировых стандартов оценки ущерба и общего понимания сущности киберриска, что можно заметить на рисунке 3.5.



Источник: составлено автором на материалах [73].

Рисунок 3.5 - Факторы, сдерживающие развитее рынка киберстрахования, проценты

К препятствиям на текущем этапе формирования рынка киберстрахования в России следует отнести:

1) Недостаточный уровень опыта страховых компаний в оценке вероятности риска и потенциального ущерба, также этот фактор замедляет процесс создания единой системы стандартов для работы с киберрисками.

2) Отсутствие сформированной нормативной-правовой базы, позволяющей определять меру ответственности в отношении преступлений, совершаемых против информационной безопасности.

3) Темпы модернизации информационных технологий способствуют структурному видоизменению и адаптации киберрисков, что повышает вероятность их возникновения.

4) В условиях санкций отсутствует возможность перестраховки рисков со стороны зарубежных компаний.

5) Зависимость внутренних информационных систем от обслуживающих организаций-партнеров, обеспечивающих их функционирование.

Имплементация инновационных решений и информационных технологий электронного банкинга делает необходимым процесс по трансформации системы внутреннего контроля на базе формирования методологических предложений, направленных на деятельность в рамках системы дистанционного банковского обслуживания. Мероприятия внутреннего контроля должны осуществляться на регулярной основе, выступая незаменимой составляющей банковских бизнес-процессов ввиду внедрения в них методов регулирования, указанных на рисунке 3.6.

Источник: составлено автором на материалах [62].

Рисунок 3.6 - Организация внутреннего контроля над системой ДБО

Сотрудник службы внутреннего аудита должен производить регулярный мониторинг по выявлению рисков, связанных с работой информационно-технических систем и оказания услуг электронного банкинга. Сотрудники СВК,

выполняющие профессиональные задачи по управлению системой риск-менеджмента, должны обладать необходимыми квалификаций и навыками, а также эффективно производить анализ источников появления банковских рисков.

Детальность банка, не обедающего значительно проработанной стратегией развития, в том числе включающую вопросы функционирования информационных технологий дистанционного обслуживания клиентов, будет недостаточно эффективна, чтобы выиграть конкуренцию у других кредитных организаций в условиях динамично изменяющегося рынка.

Продуманная стратегия развития коммерческого банка должна включать регламенты по актуальному и соответствующему угрозе комплексу мероприятий по противодействию действиям злоумышленников и других банковских организаций.

В случае, если у банка нет данного документа, появляется вероятность уменьшения прибыльности банковской деятельности, и как следствие, лишение конкурентных преимуществ и потеря лояльности клиентов, и их дальнейший отток.

Использование банковских технологий электронного обслуживания значительно увеличивает требования необходимых компетенций среди топ-менеджмента коммерческого банка. Значимым фактором выступает особенность стратегического мышления руководителя кредитной организации относительно модернизации технологических возможностей банка.

Поэтому обоснованным является нахождение в кругу руководства банка специалиста, обладающего высокой квалификацией в сфере функционирования компьютерных систем, способного распознать появления основных источников риска в данной области.

В связи с этим ответственному менеджеру из высшего руководства кредитно-финансовой структуры, в перечень должностных полномочий которого включены задачи по осуществлению системы контроля за технологиями ДБО, имеет смысл проходить регулярные тренинги по

повышению профессиональных навыков области информационно-технологических систем.

Избрании в состав Совета директоров лиц, обладающих высокой квалификацией в области IT, будет способствовать повышению качества осуществления контролирующей и регуляторной деятельности в сфере использования систем удаленного банковского обслуживания коммерческого банка, а также позволит осуществлять взвешенные стратегические решения в области следующих вопросов:

– создания в рамках банковской структуры инновационных технологий оказания удалённого обслуживания клиентов;

– проведения коммерческим банком грамотной маркетинговой политики для увеличения спроса на услуги электронного банкинга и повышения маржинальности банковских операций;

– формирования сетки тарификации в рамках пользования информационными системами;

– определение наиболее выгодных условий договоров с пользователями и провайдерами дистанционных банковских услуг.

Уровнем заинтересованности топ-менеджеров и бенефициаров кредитной организации в модернизации системы информационных технологий электронного банкинга обуславливается эффективность реализации бизнес-процессов на всех уровнях функционирования дистанционного обслуживания банковских пользователей.

По причине значительного расширения профиля типичных банковских рисков к сотрудникам, занимающим должности в службе внутреннего контроля, имеет смысл запрашивать повышенные требования к их профессиональным навыкам и компетенциям.

С началом использования в кредитно-финансовых организациях элементов электронного обслуживания клиентов, методы работы службы внутреннего контроля необходимо расширить информацией и необходимыми

положениями по порядку оценки и мониторинга новых банковских рисков организации.

Сотрудниками департамента управления рисками следует в полной мере понимать, в какой степени новые источники, сопряженные с применением информационных технологий, оказывает воздействие на трансформацию профиля типичных банковских рисков.

Риск-ориентированный внутренний контроль представляется наиболее финансово привлекательным и экономически целесообразным, в том случае, если регуляторные процессы регламентируют весь спектр банковских рисков, осуществляются непрерывно и совместно с применением аппаратно-технического оборудования по внутреннему контролю. Мероприятия по ликвидации обнаруженных нарушений, в данном случает, проводятся в наиболее оперативные сроки, а сотрудниками службы внутреннего контроля работают с наибольшей производительностью.

В главном российском нормативном документе по внутреннему контролю — Положении № 242-П — функции службы внутреннего контроля связаны только с выявлением и управлением регуляторным риском (комплаенс-риском) кредитной организации. В то же время в п. 3.1. Положения № 242-П, среди прочего, указано направление системы внутреннего контроля по «контролю за функционированием системы управления банковскими рисками и оценка банковских рисков». Но так как служба внутреннего контроля входит в систему внутреннего контроля, п. 4(1).1 указанного Положения, описывающий функции СВК в кредитной организации, необходимо уточнить и расширить функционал СВК. Этот функционал должен быть гораздо шире и совмещать в себе регулирование и реализацию системы управления всем перечнем выявленных рисков банковской организации.

Процесс определения данных рисков произойдёт по ходу формирования спектра бизнес-процессов, определения сотрудников, которые отвечают за них в рамках банковской деятельности, при цифровизации контрольных процессов службы внутреннего контроля кредитной организации. Для данных целей

требуется комплексная автоматизация всего процесса осуществления внутреннего контроля, установка актуального аппаратно-технического обеспечения, а также увеличение количества работников службы внутреннего контроля путём рекрутинга специалистов высшей квалификации в данной области.

После анализа действующих на сегодняшний день российских нормативных документов по внутреннему контролю автор пришел к выводу о том, что требуется составить один небольшой, но информативный правовой акт, включающий главные определения в рамка процесса внутреннего контроля, основные этапы его осуществления, функционал сотрудников подразделений банка, методика и особенности банковского мониторинга, а также коммуникацию службы внутреннего контроля банка с надзорными подразделениями мегарегулятора.

В процессе создания данного нормативного документа имеет смысл основываться на примерах международных стандартов в сфере внутреннего контроля, а также принимать во внимание специфические черты функционирования отечественного банковского рынка, уже внедрённые и успешно применяемые нормативные акты по внутреннему контролю. Так, одним из возможных вариантов выступает актуализация и расширение уже имеющегося Положение № 242-П, о котором упоминалось ранее.

Специалисты подразделения по осуществлению внутреннего контроля и их профессиональные компетенции также выступают значимым условием формирования наиболее совершенного комплекса риск-ориентированного внутреннего контроля, весь персонал департамента обязан регулярно проходить курсы по повышению квалификации.

В частности, взаимосвязь между участием работников организации в управлении рисками и системой их премирования отражена в международном документе по внутреннему контролю, внутреннему аудиту и управлению рисками — Guidance on the 8th EU Company Law Directive.

Таким образом, резюмируя основные результаты исследования по данному параграфу, целесообразно отметить следующее. Были обозначены основные особенности функционирования службы внутреннего контроля кредитных организаций в разрезе продолжающегося процесса цифровизации банковской деятельности. Кроме того, автором определены наиболее перспективные направления его совершенствования, включая разработку эффективной стратегии на уровне всего банковского менеджмента, которая должна включать процессы своевременного реагирования на вызовы со стороны функционирования информационных систем.

Представлены предложения по совершенствованию Положения № 242-П, регламентирующему вопросы внутреннего контроля, а также методов повышения квалификации высшего руководства банка и сотрудников службы внутреннего контроля и аудита.

Дополнительной мерой контроля рисков в рамках системы дистанционного банковского обслуживания выступает полис страхования киберрисков, который представляет из себя современный страховой продукт для обеспечения безопасности кредитных организаций и их клиентов от рисков, сопряженных с применением информационных технологий, хранением персональных данных в электронном виде, взаимодействием с ИТ-инфраструктурами.

С учетом изложенного следующим действием представляется необходимым исследовать основные направления модернизации системы управления рисками в рамках предоставления дистанционного банковского обслуживания. Данные положения рассмотрены подробно в следующем параграфе.

3.3 Рекомендации по модернизации системы управления рисками дистанционного банковского обслуживания

Оказать существенное влияние на вектор развития дистанционного банковского обслуживания могут следующие факторы:

Расширение базы клиентов, пользующихся мобильным банковским приложением. В связи с ростом популярности дистанционного обслуживания концепция «банк в кармане» получает признание среди клиентов и самих банковских структур. Банки вынуждены снижать тарифы за обслуживание для вовлечения большего числа клиентов в связи с высокой конкуренцией. Для поддержания уровня комиссионных сборов кредитным организациям необходимо увеличивать охваты населения банковскими услугами. Происходит рост спроса на удаленное банковское обслуживание. Показатель темпа прироста пользователей мобильных приложений значительно выше того же показателя среди пользователей интернет-банкинга.

Рост качества предоставляемого сервиса. Современный потребитель нуждается в качественном разностороннем удовлетворении своих потребностей.

На первый план выходят простота и удобство исполнения.

В настоящее время выбор банка зависит не только от ассортимента предоставляемых услуг, но и от оформления и интуитивности интерфейса. Например, среди современных способов аутентификации можно выделить распознание по отпечатку пальца, лица или голоса с помощью встроенных в смартфон датчиков.

Тенденция к унификации сменяется стремлением максимально персонализировать систему дистанционного банковского обслуживания. Удаленное банковское обслуживание должно соответствовать интересам и удовлетворять интересы различных групп клиентов. Персонализация клиента может быть достигнута с помощью подбора индивидуальных цветовых решений, набора услуг, способов подтверждения транзакций. Банкам необходимо будет подготовить клиентов к данным изменениям, чтобы постепенно люди смогли перестроить свои привычки.

Таким образом, персонализация становится неотъемлемой частью системы дистанционного банковского обслуживания в России.

В ходе проведения анализа дистанционного банковского обслуживания были выявлены три основные проблемы:

1) Недостаточный уровень заинтересованности менеджеров отдела дистанционного банковского обслуживания при работе с клиентами приводит к повышению вероятности риска упущенной выгоды. В связи с этим в динамике изменений объема чистого комиссионного дохода было отмечено значительное снижения.

2) В анализе отдела благосостояния был выявлен низкий показатель продаж страховых продуктов, обеспечивающих кредитный портфель. Снижение данного показателя приводит к увеличению кредитного риска, связанного с вероятностью невыплат по предоставленному займу.

3) В отделе контактного и бесконтактного обслуживания было зафиксировано повышение показателя операционного риска, влекущее за собой снижение доходов банка.

Для уменьшения негативного влияния от выявленных проблем предлагаются следующие решения:

Увеличение чистого комиссионного дохода и снижение риска упущенной выгоды возможно при выполнении следующих условиях:

– Повышение осведомленности клиента о дополнительных банковских продуктах и их преимуществах на стадии приема заявки на кредит;

– Обеспечение индивидуальных условий и акций для дополнительной мотивации клиента;

– Усовершенствование системы покрытия долга, внедрение дополнительных возможностей при приобретении других банковских продуктов, таких как страхование.

Снижение показателя кредитного риска, связанного с невозвратом денежных средств и мошеннической деятельностью возможно при следующих условиях:

– Внедрение системы повторной аутентификации клиента непосредственно перед проведением финансовой операции с целю подтверждения личности и оценки психоэмоционального состояния;

– Наиболее полное указание информации о резервных счетах клиента при заключении сделок в дистанционном формате при отсутствии возможности списания денежных средств со счета клиента.

Возможным улучшением может стать изменение процедуры подачи заявки на кредит. Например, кредитование посредством дистанционного банковского обслуживания может быть предоставлено только клиентам, получившим соответствующее предложение от банка. Клиенты, не получившие предложение, могут подать заявку удаленно с дальнейшим посещением отделения банка для подтверждения личности и оформления стандартной процедуры.

Данные нововведения могут снизить рисковую нагрузку и укрепить конкурентоспособность банка в сфере дистанционного банковского обслуживания.

Важно, чтобы стремление к улучшению финансовых показателей банка соответствовало выбранной стратегии развития и не противоречило укреплению положения банка среди конкурентов.

Рассмотрим пример имплементации указанных рекомендаций в практику кредитных организаций, в частности оценим размер затрат на риск-менеджмент и возможные положительные изменения показателей эффективности.

Разберем последовательность внедрения данных решений:

1) Обратный звонок от оператора колл-центра с целью идентификации личности, подтверждения намерения клиента в оформлении кредитного договора, а также предоставления информации о преимуществах единовременного оформления услуг страхования жизни и работы.

2) Предоставление специального кредитного тарифа и скидки на дополнительные банковские услуги в качестве поощрения клиента за самостоятельность в процессе дистанционного обслуживания.

Указанные рекомендации не несут за собой значительных расходов кроме затрат на разработку системы лояльности со специальными предложениями и акциями. Внедрение данных мер может привести к снижению операционного и кредитного риска за счет обеспечения задолженности клиента страховым продуктом. Все эти рекомендации помогут сохранить кредитный портфель банка на высоком уровне.

Для решения задачи связанным с уменьшением кредитного риска, а именно не только с невозвратами денежных средств по наступлению страхового случая, но и с возможной мошеннической деятельностью необходимо:

– Провести интеграцию системы распознавания клиента допустим перед подачей заявки звонок из колл–центра клиенту для установки личности и проверки психологического состояния клиента.

– В электронном договоре указывать все счета клиента как резервные для разрешения списания денежных средств в счет погашения задолженности при долгосрочной просрочке.

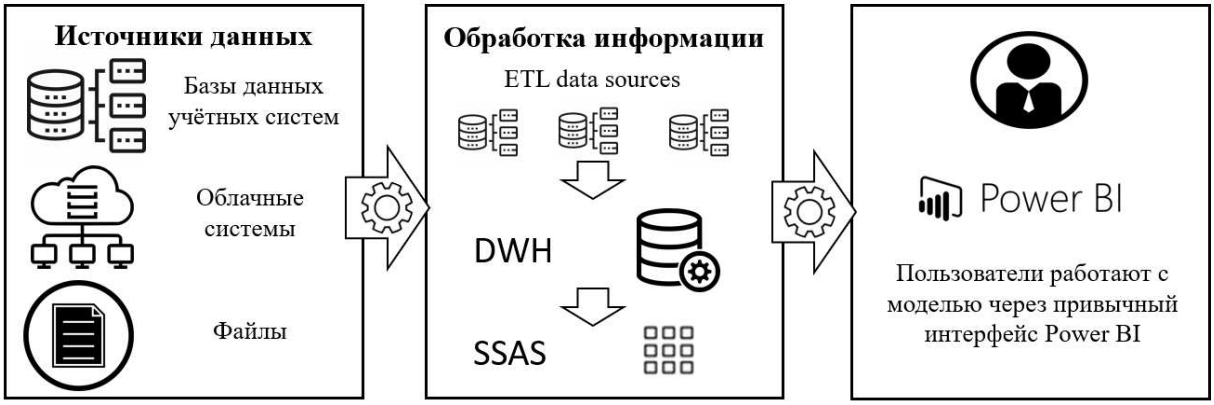
Кроме того, имеется способность по редактированию системы направления заявки на получение услуг кредитования, например, производить одобрение на предоставление кредитной операции через технологии удалённого банковского обслуживания исключительно пользователям, которым было направлена индивидуальная информация по уникальному кредитному предложению от кредитной организации, для той группы пользователей банковского приложения, кому указанное предложение не было направлено – предоставить возможность подачу кредитной заявки через банковское приложение, но с последующим визитом в операционное отделения банка для идентификации и подписания договора.

На текущем этапе развития банковского рынка конкурентоспособность отдельно взятой кредитной организации основана на том, насколько быстро высший менеджмент получает актуальную финансовую информацию для того,

чтобы принять наиболее эффективное решение в рамках динамично изменяющихся условия банковской деятельности.

Технология Business Intelligence является совокупной системой способов и инструментария для трансформации больших объёмов несистематизированной информации в лёгкие для восприятия финансовые метрики. На текущем этапе развития цифровой экономики BI-системы применяются во многих отраслях, среди которых ведущие позиции занимают кредитные организации. Business Intelligence, как активно развивающаяся технология, занимает важное место при разработке стратегии по управлению всем видами рисков в банке.

Ввиду того, что кредитные организации используют в своей операционной деятельности широкий перечень аппаратно-информационных систем, главной задачей Business Intelligence выступает обработка имеющихся баз данных и вывод наглядной для анализа информации - для принятия более точных управленческих решений [65]. Последовательность блоков аналитической BI-системы отражена на рисунке 3.7.



Источник: составлено на материалах [70].
Рисунок 3.7 - Блоки аналитической BI-системы

Чтобы понимать сферы применения BI-системы в банковской деятельности необходимо рассмотреть структуру инструментария Business Intelligence. Так, на рисунке 3.8 схематически изображено устройство методов по регулирования бизнес-процессов на основании использования данной технологии.

Источник: составлено на материалах [70].
Рисунок 3.8 - Портфель инструментов Business Intelligence

Исходя из данной структуры, ведущим блок по эксплуатации BI-систем в банке выступает управление финансовыми рисками. Главная цель риск-менеджмента заключается в том, чтобы разработать наиболее эффективную стратегию банковского бизнеса в зависимости от проявления возможных рисков. Следовательно, основная задача BI-систем в данной сфере – своевременно сформировать требуемый перечень данных, на основании которого будет разработана система управления рисков.

Технология BI служит двум основным целям:

- мониторинг финансового и операционного состояния банка. Это традиционная роль BI. Многие организации используют подобные «запаздывающие» индикаторы для выявления тенденций или особенностей событий прошлого. Например, они весьма полезны при изучении случаев кибермошенничества;

- регулирование операций организации с помощью предупреждений, извещений, ключевых показателей эффективности и инструментальных панелей, которые создаются в результате анализа операционных потоков данных. Основные индикаторы прогнозной аналитики или управляемых возможностей принятия решений используются для регулирования ситуаций в случае каких-либо нарушений. Именно эти индикаторы представляют основной вклад BI в опережающее управление рисками.

В таблице 3.3 представим преимущества для кредитной организации после внедрения и использования системы BI.

BI-система агрегирует данные, полученные другими IT-системами, и занимается их обработкой. Таким образом банку необходима система, способная собирать и анализировать большие объемы информации. Важной чертой указанных систем должно быть представление массивов данных в формате, используемом в BI-системах.

Таблица 3.3 – Преимущества использования технологии Business Intelligence

Преимущество Business Intelligence	Описание воздействия
Повышения показателя прибыли кредитной организации	- увеличение объёма продаж с помощью использования аналитики клиентской базы; - оптимизация предложений в ходе сравнительного анализа маржинальности кредитных продуктов
Оптимизация маркетинговый стратегий	- привлечение долгосрочных клиентов путём выявления целевых потребностей; - мониторинг всех показателей, влияющих на развитие клиентского опыта
Качественный клиентский сервис	- своевременное выявление причин оттока клиентов; - повышение уровня лояльности клиентов
Управление финансовыми рисками кредитной организации	- мониторинг всех показателей эффективности банка; - точное прогнозирование для управления финансовыми последствиями
Повышение показателей эффективности IT-департамента банка	- сокращение затрат на разработку и тестирование финансовых отчётов; - повышение эффективности построения запросов

Источник: составлено автором на материалах [27].

Анализ особенностей Business Intelligence позволяет сделать вывод об активном развитии данного направления. Одно из направлений развития BI-систем заключается в их интеллектуализации и самосовершенствованию. Вторым важным направлением является глобализация с учетом распространения Интернет-технологии. Проявляется тенденция представления в качестве Web-сервисов Web-ориентированных приложений, доступ к которым осуществляется посредством использования метаданных и принципов онтологий.

В построения модели управления рисками на основе системы Business Intelligence имеет смысл выделить 5 основных элементов:

1) Автоматизированные банковские системы (АБС).

АБС выступают основным источником информации по производимым банковским процессам и операциям. По результатам рабочего дня – все финансовые данные, сформированные операционными подразделениями, из автоматизированных систем мигрируют в банковское хранилище данных.

2) Банковское хранилище данных.

Банковское хранилище данных включает в себя полный перечень финансовой информации, систематизированной по заданным банковскими специалистами критериям.

3) Витрины по каждому виду риска.

Следующим шагом выступает построение специальных витрин данных, которые включают подробную информацию по каждому типу банковских рисков. Данные витрины следует оптимизировать для удобной визуализации, так как сотрудники управления рисков на их основании будут принимать решения в области регулирования уровня рисков.

4) BI приложение – Microsoft Power BI.

Приложение Microsoft Power BI является наиболее удобным для целей визуализации и мониторинга финансовых данных банковскими субъектами, которые участвуют в принятии управленческих решений в сфере риск-менеджмента;

Кроме того, следует настроить онлайн-доступ BI приложения к источникам внешней финансовой информации для анализа и сравнения с общебанковскими тенденциями, к данным источникам относятся:

– Нормативные показатели и статистические данные, подготовленные Центральным Банком Российской Федерации.

– Данные ведущих рейтинговых агентств (Росстат, Эксперт РА).

– Сайты, являющиеся агрегаторами банковских и финансовых данных, такие как СПАРК-Интерфакс, Банки.ру и другие.

5) Система логирования.

Неотъемлемой частью составляемой модели управления рисками выступает система логирования, которая необходима для фиксации всех типов событий в системе BI. Система логирования даст возможность вовремя идентифицировать возникающие в модели ошибки, а также помогает с оценкой качества работы всех процессов.

Для успешного функционирования модели необходимо сформировать механизм по редактированию показателей, определяющих параметры работы с рисками. Дополнительным этапом является обратное взаимодействие с системами АБС. Необходимо предусмотреть наличие механизма для автоматической передачи информации, основанной на установленных параметрах управления риска, в автоматизированные банковские системы – для определения кредитных лимитов, процентных ставок и других операционных показателей, которые необходимо скорректировать для поддержания оптимального уровня риска.

Таким образом, модель можно визуализировать и представить в виде блок-схемы - рисунок 3.9.

В качестве следующего мероприятия предлагается внедрение полноценной услуги электронного документооборота. Наиболее востребованной услугой является EInvoicing, позволяющий банкам привлекать новых клиентов и сохранять старых.

Важным направлением сервиса электронного документооборота считается процесс обмена конфиденциальными документами между контрагентами. Сервис позволяет создавать, загружать и изменять юридически значимые документы перед их передачей.

Заключительным этапом предлагается внедрение облачной системы АБС, разработанную специалистами Центра Финансовых Технологий. Система АБС представляет из себя объектно-ориентированную систему, направленную на автоматизацию современной банковской деятельности.

Источник: составлено автором.
Рисунок 3.9 - BI модель по управлению рисками

Автором определены следующие основные тенденции по развитию BI-платформ в банковском секторе:

- Курс на импортозамещение.
- Self-Service в широком смысле.
- Большие данные, повышенная производительность и быстрая СУБД.
- Продвинутая аналитика и голосовые помощники.
- Переход на единую платформу BI: облачные технологии.

Особое внимание необходимо уделить проблеме безопасности. Дистанционное банковское обслуживание предоставляет обширный функционал – доступ к имеющимся счетам, возможность осуществления переводов и покупки валюты и т.д. В связи с этим системы дистанционного обслуживания должны отвечать новейшим требованиям безопасности в отношении всех направлений работы с данными. Помимо соответствия требованиям для системы банковского обслуживания крайне важна возможность ручного внесения изменений в систему в случае форс-мажорных обстоятельств, требующих немедленного вмешательства.

Кредитные организации, осуществляя свою деятельность рамках повышенной конкуренции, не намерены тратить на создание высокого уровня информационной безопасности больше капитала, чем их основные конкуренты, так как это может привести к падению маржинальности их кредитно-финансовых операций. Клиенты банковских организаций, свою очередь, как правило, направляют фокус большего внимание на удобство предоставления банковских услуг и продуктов, чем на обеспечение их безопасности.

В связи с этим возникает необходимость рационального компромисса, в основе которого будут учтены основные принципы информационной безопасности:

– стоимость организации зашиты не может превышать стоимость объекта защиты (информационных ресурсов);

– стоимость защиты должна быть экономически выгодна, а его использование удобно клиенту, при этом величина расходов на преодоление такой защитной системы для киберпреступников должна приводить к нецелесообразности хищения информации.

Операционный риск, сущность которого состоит в возможности недополучения прибыли и появления убытков ввиду сбоев и нарушения выполнения ежедневных банковских операций, относится к основной группе рисков, регулируемых СЭБ.

Проявлениями операционного риска могут стать нарушения в процессах хранения, обмена и обработки банковской информации, такие как – изменение, удаление, кража данных, злоупотребление доступом к информации в результате технических сбоев в работе информационных систем банка, а также в результате хакерских атак, мошеннических действий клиентов и работников банка. Причинами технических сбоев могут послужить перегрузки в связи с недостаточной производительностью аппаратных мощностей и программного обеспечения, а также точечные DoS-атаки, нарушающие работу серверов банка.

Сотрудничество банков с компаниями, разрабатывающими для них специализированные программы, с одной стороны, позволяет снизить издержки на содержание отдельного информационного подразделения и найм высококвалифицированных специалистов в сфере IT. Достигаемая экономия особенно существенна для малых финансовых учреждений. С другой стороны, данное бизнес-партнерство ставит банк в зависимое положение, эффективность его работы и репутация в целом начинают зависеть от сторонних организаций, не связанных друг с другом, а также не специализирующихся на особенностях ведения банковской деятельности.

Реализация комплекса мероприятий по модернизации системы управления рисков кредитных организаций поднимает уровень запросов к профессиональным навыкам сотрудников кредитных организаций и повышает вероятность проявления негативных факторов при трансформации на все более комплексные информационные решения.

Можно предположить, что в перспективнее развития банковской отрасли информационные угрозы будут становиться всё более комплексными. Уже на текущем этапе значительное число кибер-атак представляют собой комбинации разнообразных типов воздействия на контур банковской безопасности. Организация информационной защиты при помощи исключительно традиционных технических средств, как например, сигнатурные антивирусы, в скором времени может привести к увеличению числа успешных киберпреступлений.

Коммерческие банки, которые формируют систему защиты только от распространённых угроз, подвергаются повышенному риску в связи с тем, что злоумышленники непрерывно совершенствуют технологии инновационных вирусных систем [37].

В процессе проведения мероприятий по идентификации пользователей банковских услуг необходимо соблюдать следующие рекомендации:

— создать и имплементировать профильные механизмы, сопряженные с операциями по открытию банковских счетов, а также предоставлением банковских услуг клиентам, которые не имеют открытых счетов в кредитной организации;

— производить тщательную проверку идентификационных документов, удостоверяющих личность клиента, чтобы предотвратить открытие банковского счёта злоумышленниками;

— запрашивать дополнительные данные относительно профессиональной деятельности пользователя, включая информацию о размерах и источниках его доходов, а также непосредственно о природе возникновения активов, которые участвуют в совершаемой банковской операции;

— уточнять цель, для которой производится открытие счета, а также иметь исчерпывающую информацию о перечне банковских операций, которые обычно запрашивает данный клиент. При создании нового счёта представитель кредитной организации должен сразу определять категорию риска клиента, для формирования направлений дальнейшего взаимодействия.

Таким образом, резюмируя основные результаты исследования по данному параграфу, целесообразно отметить следующее. Были выявлены основные направления модернизации системы управления рисками, разработанные с учётом специфики электронного банкинга, основным из которых представляется применение инструмента Business Intelligence, основанного на проведении анализа массивов данных и их последующего преобразования в актуальную для пользователей информацию. Данная технология позволит увеличить рентабельность банка, повышая его

конкурентоспособность на рынке, а также способствует подготовке максимально прозрачной отчётности.

В третьей главе комплексно рассмотрен механизм оценки рисков дистанционного банковского обслуживания. Выделены основные методы, применимые с учётом для специфики электронного банкинга, обоснованы два основных направления, в которых необходимо производить совершенствование системы риск-менеджмента: регулирование расширения профиля операционных рисков банка и противодействие участившимся случаям кибер-преступлений.

Разработана комплексная модель оценки риска информационной безопасности, как одного из основных видов проявления рисков дистанционного банковского обслуживания, базирующаяся на методах и индикаторах оценки рисков, стрессовых параметрах и статистическом аппарате для проведения стресс-тестирования.

Комплексно рассмотрен механизм функционирования службы внутреннего контроля кредитных организаций в разрезе продолжающегося процесса цифровизации банковской деятельности. Кроме того, автором определены наиболее перспективные направления его совершенствования, включая разработку эффективной стратегии на уровне всего банковского менеджмента, которая должна включать процессы своевременного реагирования на вызовы со стороны функционирования информационных систем.

Представлены предложения по совершенствованию Положения № 242-П, регламентирующему вопросы внутреннего контроля, а также методов повышения квалификации высшего руководства банка и сотрудников службы внутреннего контроля и аудита.

Дополнительной мерой контроля рисков в рамка системы дистанционного банковского обслуживания выступает полис страхования киберрисков, который представляет из себя современный страховой продукт для обеспечения безопасности кредитных организаций и их клиентов от рисков,

сопряженных с применением информационных технологий, хранением персональных данных в электронном виде, взаимодействием с ИТ-инфраструктурами.

Анализ опыта российских и зарубежных кредитных организаций позволил выделить лучшие направления модернизации системы управления рисками, разработанные с учётом специфики электронного банкинга, основным из которых представляется применение инструмента Business Intelligence, основанного на проведении анализа массивов данных и их последующего преобразования в актуальную для пользователей информацию. Данная технология позволит увеличить рентабельность банка, повышая его конкурентоспособность на рынке, а также способствует подготовке максимально прозрачной отчётности.

Заключение

В текущих реалиях развития «цифровой экономики» одним из важнейших критериев эффективной банковской деятельности является политика внедрения современных инновационных технологий. Инновации являются основополагающим фактором устойчивости работы и развития банковской отрасли, а также обеспечивают стабильное увеличение эффективности и маржинальности банковской деятельности.

Результатом проведенных исследований стала реализация поставленной в диссертации цели – развиты теоретических положения, разработаны методические подходы и практические рекомендаций по совершенствованию системы управления банковскими рисками дистанционного банковского обслуживания и оптимизации её параметров.

Проведенное исследование позволило внести предложения по модернизации системы управления рисками дистанционного банковского обслуживания в целях механизма устойчивого развития всей банковской отрасли.

В первой главе работы проведён анализ взглядов отечественных и зарубежных ученых на вопросы сущности, роли и экономического содержания системы дистанционного банковского обслуживания позволил сделать вывод об отсутствии единого толкования рассматриваемого понятия, что усложняет его понимание и практическое применение. Данный факт потребовал считать дистанционное банковское обслуживание собирательным понятием, которое складывается из основных специфических характеристик данного вида банковских услуг.

Дистанционное банковское обслуживание удалось характеризовать как предоставление услуг и продуктов коммерческими кредитными организациями путем предоставления распоряжений со стороны клиентов банка без непосредственного визита в банковские отделение с использованием современных информационно-коммуникационных технологий.

По результатам рассмотрения форм и основных принципов функционирования систем дистанционного банковского обслуживания были выявлены основные этапы создания данных систем в коммерческих банках, а также проанализированы преимущества использования технологий удаленного обслуживания и их недостатки, которые, в частности, сопряжены с рисками банковской деятельности.

Анализ специфики современной системы управления рисками банковской деятельности позволил систематизировать и раскрыть содержание основных видов рисков банковской деятельности, анализируемых риск-подразделениями.

Рассмотрены факторы, оказывающие влияние на расширение профилей рисков дистанционного банковского обслуживания. По результатам было выявлено, что внедрение и использование технологий дистанционного банкинга не только вносит изменения в профиль стандартных банковских рисков, но и формирует специфический перечень банковских рисков, которые присущи только электронным банковским операциям.

На основании выделения характерных особенностей отечественного и международного опыта управления риском была разработана новая классификация рисков, связанных с расширением использования технологий дистанционного обслуживания банковских клиентов. Классификация отличается от имеющихся не только разделением на уровни банковской системы, но и выделением новых, наиболее ярко проявляющихся рисков дистанционного банковского обслуживания как на уровне банковской системы, так и, непосредственно, кредитной организации. В соответствии с этим выделены шесть уникальных рисков, минимизация которых необходима для дальнейшего развития банковской отрасли. Предложенная классификация предоставила возможность для обоснования потребности модернизации системы управления рисками дистанционного банковского обслуживания на макро- и микроуровне банковской системы.

На основании проведенного эконометрического исследования была подтверждена гипотеза о то, что с ростом объёма использования цифровых

каналов обслуживания клиентов возрастает и показатель риска кибер-мошенничества, негативно влияющий на показатель финансовой стабильности банковского сектор. Данная тенденция сигнализирует о необходимости повышения качества регулирования финансовой стабильности банковского сектора в разрезе использования систем дистанционного обслуживания путём модернизации системы управления рисками.

Во второй главе работы обозначены наиболее перспективные тенденции по модернизации услуг дистанционного банковского облуживания на макроуровне. Кроме того, определены наиболее перспективные инновационные технологии банковской сферы и основные области их применения: улучшение качества обслуживания клиентов и применение новых методов в управлении банковскими рисками, в том числе, в области оценки данных рисков.

Даны практические рекомендации по минимизации риска недоверия к использованию банками цифровых технологий. Отмечено, что наиболее результативной мерой является создание единого рейтинга банков на основе критериев оценки уровня защищенности персональных данных клиентов, который стимулирует банки к добросовестному поведению по отношению к персональным данным своих клиентов.

Обозначены основные особенности функционирования системы банковского надзора в Российский Федерации. Кроме того, определены наиболее перспективные направления его совершенствования, включая использование инновационных разработок банковской сферы, таких как способы машинного обучения, а также SupTech и RegTech технологии, и основные направления их применения: поддержание устойчивого функционирования национальной банковской системы в условия применения дистанционного-банковского обслуживания, а также обеспечение полной защиты законных интересов каждого субъекта банковской деятельности.

Анализ опыта российских и зарубежных кредитных организаций позволил выделить лучшие практики по управлению банковскими рисками в

рамках системы дистанционного банковского обслуживания кредитных организаций России.

Таковыми можно назвать применения банками инновационных технологий в целях снижения воздействия возникающих рисков и модернизации системы управления рисками электронного банкира в целом. Среди них стоит особо выделить применение технологии «Больших данных» для защиты информационных ресурсов от хищения, технологии блокчейн для обеспечения безопасность использования электронных систем и биометрической идентификации.

Внедрение Open API в работу банковского сектора станет драйвером для разработки инновационных технологий, а также значительно увеличит доступность банковских продуктов для клиентов кредитных организаций. Данная технология уменьшает воздействие риска монополизации: Применение открытых интерфейсов, позволяющих получать равный доступ к информации для всех участников обмена данными, ведёт к увеличению конкурентоспособности малых субъектов кредитного рынка за счет демонополизации доступа к данным пользователей.

В третьей главе предложены направления развития системы управления рисками дистанционного банковского обслуживания. Сформирована система предложений для внедрения в работу.

Комплексно рассмотрен механизм оценки рисков дистанционного банковского обслуживания. Выделены основные методы, применимые с учётом для специфики электронного банкинга, обоснованы два основных направления, в которых необходимо производить совершенствование системы риск-менеджмента: регулирование расширения профиля операционных рисков банка и противодействие участившимся случаям кибер-преступлений.

Разработана комплексная модель оценки риска информационной безопасности, базирующаяся на методах и индикаторах оценки рисков, стрессовых параметрах и статистическом аппарате для проведения стресс-тестирования.

Комплексно рассмотрен механизм функционирования службы внутреннего контроля кредитных организаций в разрезе продолжающегося процесса цифровизации банковской деятельности.

Кроме того, определены наиболее перспективные направления его совершенствования, включая разработку эффективной стратегии на уровне всего банковского менеджмента, которая должна включать процессы своевременного реагирования на вызовы со стороны функционирования информационных систем.

Представлены предложения по совершенствованию Положения № 242-П, регламентирующему вопросы внутреннего контроля, а также методов повышения квалификации высшего руководства банка и сотрудников службы внутреннего контроля и аудита.

Дополнительной мерой контроля рисков в рамка системы дистанционного банковского обслуживания выступает полис страхования киберрисков, который представляет из себя современный страховой продукт для обеспечения безопасности кредитных организаций и их клиентов от рисков, сопряженных с применением информационных технологий, хранением персональных данных в электронном виде, взаимодействием с ИТ-инфраструктурами.

Анализ опыта российских и зарубежных кредитных организаций позволил выделить лучшие направления модернизации системы управления рисками, разработанные с учётом специфики электронного банкинга, основным из которых представляется применение инструмента Business Intelligence, основанного на проведении анализа массивов данных и их последующего преобразования в актуальную для пользователей информацию. Данная технология позволит увеличить рентабельность банка, повышая его конкурентоспособность на рынке, а также способствует подготовке максимально прозрачной отчётности. В результате автором построена модель управления рисками на основе системы Business Intelligence.

Список литературы

Нормативные правовые акты и иные официальные документы

1. Российская Федерация. Законы. Гражданский кодекс Российской Федерации. Часть первая : федеральный закон : [принят Государственной Думой 21 октября 1994 года]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 14.02.2021).

2. Российская Федерация. Законы. О банках и банковской деятельности : федеральный закон № 395-1 : последняя редакция : [принят съездом народных депутатов РСФСР 02 декабря 1990 года]. – Справочно-правовая система «Консультант Плюс» : Законодательство : Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 14.02.2021).

3. Российская Федерация. Законы. О защите прав потребителей : Федеральный закон № 2300-1 : редакция от 08 декабря 2020 года : [принят Верховным Советом Российской Федерации 7 февраля 1992 года]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 14.02.2021).

4. Российская Федерация. Законы. О национальной платежной системе : федеральный закон № 161-ФЗ : последняя редакция : [принят Государственной Думой 14 июня 2011 года : одобрен Советом Федерации 22 июня 2011 года]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 14.02.2021).

5. Российская Федерация. Законы. О персональных данных : федеральный закон № 152-ФЗ : последняя редакция : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф.– Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_ LAW_61801/ (дата обращения: 14.02.2021).

6. Российская Федерация. Законы. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : федеральный закон № 115-ФЗ : последняя редакция : [принят Государственной Думой 13 июля 2001 года : одобрен Советом Федерации 20 июля 2001 года]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 14.02.2021).

7. Российская Федерация. Законы. О Центральном банке Российской Федерации (Банке России) : федеральный закон № 86-ФЗ : последняя редакция : [принят Государственной Думой 27 июня 2002 года]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc _LAW_37570/ (дата обращения: 14.02.2021).

8. Российская Федерация. Законы. Об организации внутреннего контроля в кредитных организациях и банковских группах : [положение Банка России от 16 декабря 2003 № 242-П]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc _LAW_46304/ (дата обращения: 14.02.2021).

9. Российская Федерация. Законы. О требованиях к защите информации в платежной системе Банка России [положение Банка России от 23 декабря 2020 года № 747-П]. – Справочно-правовая система «Консультант

Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_377008/ (дата обращения: 14.02.2021).

10. Российская Федерация. Законы. О порядке расчета кредитными организациями величины рыночного риска : [положение Банка России от 03 декабря 2015 года № 511-П]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc _LAW_190828/ (дата обращения: 14.02.2021).

11. Российская Федерация. Законы. О порядке проведения Банком России оценки качества систем управления рисками и капиталом, достаточности капитала кредитной организации и банковской группы : [указание Банка России от 07 декабря 2015 года № 3883-У]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc _LAW_190733/ / (дата обращения: 14.02.2021).

12. Российская Федерация. Законы. О форме и порядке раскрытия кредитной организацией (головной кредитной организацией банковской группы) информации о принимаемых рисках, процедурах их оценки, управления рисками и капиталом : [указание Банка России от 07 августа 2017 года № 4482-У]. – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc _LAW_282236/ (дата обращения: 14.02.2021).

13. Российская Федерация. Законы. Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах : [письмо Банка России от 30 июня 2005 года № 92-Т : с изменениями от 12 октября 2016 года] – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия

Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_54347/ (дата обращения: 14.02.2021).

14. Российская Федерация. Законы. О рекомендациях Базельского комитета по банковскому надзору «Принципы агрегирования рисков и представления отчетности по рискам» : [письмо Банка России от 27 мая 2014 года № 96-Т] – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_163915/ (дата обращения: 14.02.2021).

15. СТО БР ИББС-1.2-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 : Стандарт Банка России : издание официальное : принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399 : введен взамен СТО БР ИББС-1.2-2010 : дата введения 2014-06-01 / подготовлен Центральным банком Российской Федерации – Справочно-правовая система «Консультант Плюс»: Законодательство: Версия Проф. – Текст : электронный. – URL: http://www.consultant.ru/document/cons_doc_LAW_163807/ (дата обращения: 14.02.2021).

Книги, диссертации и иные научные труды

16. Банковское дело : учебник ; под редакцией О.И. Лаврушина. – 12-е издание, стереотипное. – Москва : КНОРУС, 2016. – 800 с. – ISBN 978-5-406-04591-6.

17. Банковское дело : операции, технологии, управление / Александр Турбанов, Александр Тютюнник. - Москва : Альпина Паблишерз, 2010 (Ульяновск : Ульяновский Дом печати). - 681 с. - ISBN 978-5-9614-1082-2.

18. Банковское дело : учебник для вузов / Н.Н. Мартыненко, О.М. Маркова, О.С. Рудакова, Н.В. Сергеева; под редакцией Н.Н. Мартыненко. – 2-е издание, исправленное и дополненное. В 2 частях. Часть 1. – Москва : Издательство Юрайт, 2020. – 217 с. – (Высшее образование). – ISBN 978-5-534-08398-9. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.urait.ru/bcode/451916 (дата обращения: 28.02.2021).

19. Банковское дело : учебник для вузов / Н.Н. Мартыненко, О.М. Маркова, О.С. Рудакова, Н.В. Сергеева. – 2-е издание, исправленное и дополненное. В 2 частях. Часть 2. – Москва : Издательство Юрайт, 2020. – 368 с. – (Высшее образование). – ISBN 978-5-534-08470-2. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.urait.ru/bcode/451917 (дата обращения: 14.02.2021).

20. Банковское дело. Организация деятельности коммерческого банка : учебник и практикум для академического бакалавриата / Г. Н. Белоглазова, Л. П. Кроливецкая ; под редакцией Г. Н. Белоглазовой, Л. П. Кроливецкой. — 3-е издание, переработанное и дополненное. — Москва : Издательство Юрайт, – 2016. — 545 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-8390-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/394351 (дата обращения: 31.05.2021).

21. Развитие финансовых рынков и банков в миропорядке открытого информационного доступа : монография ; под редакцией И.Е. Шакер. – Москва : Русайнс, 2020. – 264 с. – 500 экз. – ISBN 978-5-4365-5549-2.

22. Риск-менеджмент в коммерческом банке : монография ; под редакцией И.В. Ларионовой. – 1-е издание. – Москва : Издательство Кнорус, – 2016. – 456 с. – 100 экз. – ISBN 978-5-406-02907-7.

23. Рудакова, О.С. Банковские электронные услуги : учебное пособие для вузов / О.С. Рудакова. – Москва : Вузовский учебник : ИНФРА-М. – 2011. – 399 с. – ISBN 978-5-9558010-0-1.

24. Тавасиев, А. М. Банковское дело. Технологии обслуживания клиентов банка : учебник для среднего профессионального образования / А. М. Тавасиев. — 2-е издание, переработанное и дополненное. В 2 частях. Часть 1. — Москва : Издательство Юрайт, 2020. — 301с. — (Профессиональное образование). — ISBN 978-5-534-11424-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/453605 (дата обращения: 13.02.2022).

25. Травкина, Е.В. Управление рисками в современном банке : учебное пособие / Е.В. Травкина, Е.И. Мешкова. — Москва : КноРус, – 2021. — 216 с. — ISBN 978-5-406-06549-5.

26. Трофимов, В. В. Информационные системы и технологии в экономике и управлении : учебник для академического бакалавриата / В. В. Трофимов [и др.] ; под редакцией В.В. Трофимова. — 4-е издание, переработанное и дополненное. — Москва : Издательство Юрайт, 2018. — 542 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-00259-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/412460 (дата обращения: 13.02.2022).

Статьи, опубликованные в периодических изданиях

27. Авдокушин, Е. Ф. Глобальная цифровая экономика: сравнительный анализ развития ИКТ России и стран Северо-Восточной Азии / Ким Ючжон, Е. Ф. Авдокушин // Вопросы новой экономики. - 2019. - № 3. - С. 4-13. - ISSN 1994-0556.

28. Алехина, Е.С. Страхование как фактор развития долгосрочного банковского кредитованияреального сектора экономики / Е.С. Алехина // European Social Science Journal. – 2019. – № 10 (37). – С. 383-390. – ISSN 2079-5513.

29. Амосова, Н.А. Функциональная и институциональная трансформация банковского сектора экономики в условиях смены технологического уклада. Воспроизводство России в XXI веке: диалектика

регулируемого развития к 80-летию выхода в свет книги Дж. М. Кейнса ≪Общая теория занятости, процента и денег≫ / Н.А. Амосова // под редакцией Р.М. Нуреева, М.Л. Альпидовской. – Москва : Финансовый университет, 2016. – С. 479–485. – ISBN 978-5-7942-1336-2.

30. Барынькина, Н.П. Риски и перспективы развития дистанционного банковского обслуживания / Н.П. Барынькина, В.Е. Сазанская // Экономические и гуманитарные науки. – 2020. – № 4. – С. 28-37. – ISSN 2073-7424.

31. Бердюгин, А.А. Риск воздействия кибератак на системы дистанционного банковского обслуживания / А.А. Бердюгин // Информационная безопасность в банковско-финансовой сфере. – 2018. – с. 149-154. – ISBN 978-5-907100-90-9.

32. Бирюков, М. В. Экономические перспективы использования технологии дистанционного банковского обслуживания / М. В. Бирюков, Н.А. Климова, Т.В. Гостищева // Вестник Белгородского университета кооперации, экономики и права. – 2018. – № 1. – С. 159-167. – ISSN 2223-5639.

33. Бобыль, В. Современная концепция управления банковскими рисками / В. Бобыль // Банковский вестник. – 2017. – № 11. – С. 43 - 48. – ISSN 2071-8896.

34. Болотнова, Е.А. Экосистемы в банковской системе РФ: проблемы и перспективы / Е.А. Болотнова, А.А.Храмченко // Естественно-гуманитарные исследования. – 2022. – № 39. – С. 75-82. – ISSN 2309-4788.

35. Быканова, Н.И. Формирование экосистем банков в условиях цифровизации банковского пространства. / Н.И. Быканова, Ю.А. Соловей // Экономика. Информатика. – 2020. – № 1. – С. 91-10. – eISSN 2687-0932.

36. Ваганова, О.В. Развитие системы Open Banking в России / О. В. Ваганова, Н.И. Быканова, Д.В. Гордя, В.Н. Голубоцких // Современная экономика: проблемы и решения. – 2022. – №1 (145). – С. 27 - 37. – ISSN 2078-9017. – DOI: 10.17308/meps.2022.1/2752

37. Варламова, Т.П. Риски дистанционного банковского обслуживания клиентов и пути их снижения / Т.П. Варламова // Математическое и компьютерное моделирование в экономике, страховании и управлении рисками. – 2019. – № 4. – С. 126-130. – ISSN 2686-9659.

38. Васильев, Н.И. Риски дистанционного банковского обслуживания и пути их минимизации / Н.И. Васильев // Матрица научного познания. – 2021. – № 1. – С. 78-81. – ISSN 2541-8084.

39. Венгеровский, Е.Л. Инновации интернет-банкинга как фактор конкурентоспособности кредитных организаций на современном рынке банковских услуг / Е.Л. Венгеровский // Банковское право. – 2018. – № 1. – С. 47-52. – ISSN 1812-3945.

40. Гаврилин, А.В. Направления развития банковского бизнеса в условиях цифровизации экономики / А.В. Гаврилин, Н.Д. Гераскина // Финансовые рынки и банки. – 2021. – № 1. – С. 42-45. – ISSN 2658-3917.

41. Гаврилова, О.А., Интернет-банкинг как инновационный вид сетевых финансовых отношений / О.А. Гаврилова, Т.В.Нестеренко // Вестник Волгоградского государственного университета. Серия 10: инновационная деятельность. – 2010. – № 4. – С. 11-18. – ISSN 2305-7815.

42. Гвоздарева А.И. Внедрение цифровых экосистем в финансовой сфере: будущее российских банков / А.И. Гвоздарева, Л.Ю. Кожокина // Российский экономический интернет-журнал. – 2020. – № 2. – С. 17. – eISSN 2218-5402.

43. Дукян, С.С. Возможности и угрозы цифрового (открытого) банкинга в условиях внедрения API-интерфейса / С.С. Дукян, С.Н. Татаркин // Государственное и муниципальное управление. Ученые записки. – 2022. – № 1. – С. 89 - 95. – ISSN 2079-1690. – DOI: 10.22394/2079-1690-2022-1-1-89-95.

44. Дьякова, О.Н. Содержание системы дистанционного банковского обслуживания / О.Н. Дьякова // Современные проблемы науки и образования. – 2015. – № 1-1. – С. 511. – eISSN 2070-7428.

45. Есипов, А.В. Совершенствование бизнес-модели и регулирования деятельности кредитных организаций в условиях внедрения высоких финансовых технологий/ А.В. Есипов // Ученые записки международного банковского института. – 2018. – № 3. – С. 28-39. – ISSN 2413-3345.

46. Иванова, О. А. Анализ перспектив развития и конкуренция экосистем банков в условиях цифровизации [Текст] / О.А. Иванова, Н.В. Смирнова // Проблемы экономики и юридической практики. – 2020. – № 4. – С. 43-47. – ISSN 2541-8025.

47. Зернова, Л.Е. Актуальные проблемы использования дистанционных технологий в коммерческом банке / Л.Е.Зернова // Международный научно-исследовательский журнал. – 2012. – № 4-4. – С. 128-132. – ISSN 2303-9868.

48. Зиниша, О.С. Применение дистанционного банкинга: риски совершения несанкционированного доступа и пути их минимизации / О.С. Зиниша, Т.О. Стрельникова // Вектор экономики. – 2019. – № 4. – С. 100-109. – ISSN 2500-3666.

49. Канторoева, А.К. Маркетплейс как инновационный элемент экосистемы коммерческого банка / А.К. Канторoева // вестник академии государственного управления при президенте Кыргызской республики. – 2020. – № 27. – С. 202-207. – ISSN 1694-5433.

50. Коваленко, О. Г. Экономическая сущность банковских рисков и их классификация / О. Г. Коваленко // АНИ: экономика и управление. – 2013. –№ 3. – С. 11-14. – ISSN 2309-1762.

51. Косарев, В.Е. Экосистема как новая модель развития банка / В.Е. Косарев, Г.М. Иараджули // Финансовые рынки и банки. – 2020. – № 1. – С. 58-62. – ISSN 2658-3917.

52. Костенко, Р.В. Безопасное использование систем дистанционного банковского обслуживания: риски совершения несанкционированных операций и пути их минимизации / Р.В. Костенко, М.А. Скворцова // Вестник современных исследований. – 2018. – № 27 – С. 227-229. – ISSN 2541-8300.

53. Криворучко, С.В. Биометрическая идентификация: сущность и риски применения технологии в платёжной индустрии / С.В. Криворучко, М.Д. Фуфаев // Международный журнал гуманитарных и естественных наук. – 2021. – № 2-3. – С. 39-42. – ISSN 2500-1000.

54. Лаврушин, О.И. О модернизации регулирования и новых моделях развития банковской деятельности / О.И. Лаврушин // Экономика. Налоги. Право. – 2018. – № 3. – С. 14–19. – ISSN 1999-849X.

55. Ларионова, И.В. Синергия рентабельности и рисков институтов банковского сектора в контексте финансовой стабильности / И.В. Ларионова, Е.И. Мешкова // БАНКОВСКИЕ УСЛУГИ. – 2022. – № 2. – С. 2-11. – ISSN 2075-1915.

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

57. Мартыненко, Н.Н. Риски ускоренного внедрения дистанционного банковского обслуживания населения в условиях пандемии: причины, следствия, направления сдерживания / Н.Н. Мартыненко // Финансовые рынки и банки. – 2020. – № 6. – С. 75-80. – ISSN 2658-3917.

58. Мартюкова, В.М. Возможности открытых интерфейсов API для регионального финансового рынка России / В.М. Мартюкова, М.Н. Ермакова // Современные технологии управления. – 2020. – № 3 (93). – eISSN 2226-9339.

59. Матюшкина, И.А. Инновационные банковские технологии: сущность и этапы развития / И.А. Матюшкина, Е.А. Щербина // Экономика и предпринимательство. – 2020. – № 4. – С. 62-65. – ISSN 1999-2300.

60. Никонец, О.Е. Дистанционное банковское обслуживание как элемент экосистемы современного банка / О.Е. Никонец, К.А. Попова // Вестник Волжского университета им. В.Н. Татищева. – 2020. – № 1. – С. 280-292. – ISSN 2076-7919/

61. Никулина, О.В. Исследование перспектив развития финансовых инноваций в банковском бизнесе / О.В. Никулина, О.Э. Чулаевский //

ЭКОНОМИКА: ТЕОРИЯ И ПРАКТИКА. – 2023. – № 2 (70). – С.77-84. – ISSN 2224-042X.

62. Ревенков, П.В. Оценка рисков информационной безопасности в условиях применения систем мобильного банкинга / П.В. Ревенков, Д.С. Крупенко // Вопросы кибербезопасности. – 2019. – № 2. – С. 21-28. – ISSN 2686-9659.

63. Ревенков, П.В. Источники киберрисков в условиях функционирования экосистем / П.В. Ревенков, А.Г. Чебарь, А.А. Бердюгин // В центре экономики. – 2022. – № 1. – С. 1-11. – ISSN 2713-2242.

64. Рзаева, В.В. Развитие деятельности открытого банкинга на основе внедрения технологий открытых интерфейсов программирования / В.В. Рзаева, М.А. Мамедов // Национальная безопасность / NOTA BENE. – 2021. – № 4. – С. 41- 52. - ISSN 2073-8560. – DOI: 10.7256/2454-0668.2021.4.36312.

65. Рудакова, О. С. Трансформация бизнес-моделей банков в цифровой экономике / О. С. Рудакова // Банковское право. – 2017. – № 4. – С. 50-54. – ISSN 1812-3945.

66. Сироткин, А.С. Особенности трансформации способов ведения банковского розничного бизнеса в современных условиях / А.С. Сироткин // Креативная экономика. – 2019. – № 5. Том 13. – С. 979-990. – ISSN 1994-6929.

67. Сливянчук, Ю.В. Управление рисками в системе дистанционного банковского обслуживания / Ю.В. Сливянчук // Высокие технологии и инновации в науке. – 2020. – № 11 – С. 191-194. – ISBN 978-5-6044175-9-1.

68. Сипратов, Р.О. Анализ перспектив развития экосистем как элемента цифровизации банковского сектора / Р.О. Сипратов // Экономика и предпринимательство. – 2021. – № 10. – С. 1247-1252. – ISSN 1999-2300.

69. Сипратов, Р.О. Метод оценки влияния мошеннических операций в сфере дистанционного обслуживания на стабильность банковского сектора / Р.О. Сипратов, О.С. Рудакова // Сберегательное дело за рубежом. – 2022. – № 2. – С. 15-23. – ISSN 2782-5949.

70. Сипратов, Р.О. Применение технологии Business Intelligence в целях модернизации системы управления рисками кредитной организации / Р.О. Сипратов, О.С. Рудакова // БАНКОВСКИЕ УСЛУГИ. – 2023. – № 1. – С. 9-15. – ISSN 2075-1915.

71. Сипратов, Р.О. Пути минимизация рисков в рамках применения открытых интерфейсов API в банковской системе России / Р.О. Сипратов // Финансовая экономика. – 2022. – № 12. – С. 343-347. – ISSN 2075-7786.

72. Сипратов, Р.О. Совершенствование системы банковского надзора в условия цифровизации экономики России / Р.О. Сипратов // CHRONOS. – 2022. – № 7. – С. 67-70. – eISSN 2658-7556.

73. Сипратов, Р.О. Страхование киберрисков в условиях функционирования банковских экосистем / Р.О. Сипратов // Финансовая экономика. – 2022. – № 8. – С. 134-139. – ISSN 2075-7786.

74. Тутаев, И.А. Анализ проблем обеспечения информационной безопасности приложений мобильного банка / И.А. Тутаев // Информационная безопасность в банковско-финансовой сфере. – 2018. – С. 224-226. – ISBN 978-5-907100-90-9

75. Халитова, А.З. Интернет-банкинг как форма дистанционного банковского обслуживания: сущность, преимущества и риски / А.З. Халитова, З.Ф. Шарифьянова // Дневник науки. – 2018. – № 12. – С. 34-42. – ISSN 2541-8327.

76. Цурова, Л.А. Анализ тенденций возникновения новых вызовов для риск-менеджмента банка / Л.А. Цурова // Экономика и предпринимательство. – 2017. – № 2. – С. 1043-1047. – ISSN 1999-2300.

77. Цхададзе, Н.В. Эффективность использования дистанционных технологий в предоставлении банковских услуг / Н.В. Цхададзе // Экономика: вчера, сегодня, завтра. – 2018. – № 3А. Том 8. – С. 358-367. – ISSN 2222-9167.

78. Шабанкова, О.А. Методы управления банковскими рисками в условиях современной экономики / О.А. Шабанкова // Вектор экономики. – 2020. – № 3. – С. 43 - 54. – ISSN 2500-3666.

Источники на иностранных языках

79. Aithal, P. S. A Customized and Flexible Ideal Mobile Banking System using 5G Technology / P.S. Aithal, K. Prasad // International Journal of Management, Technology, and Social Sciences. – 2017. – P. 25-37. – ISSN 2581-6012. – Текст: электронный. – DOI: 10.5281/zenodo.820860.
- URL:https://www.researchgate.net/publication/318147859_A_Customized_and_Flexible_Ideal_Mobile_Banking_System_using_5G_Technology (дата обращения: 20.02.2021).

80. Basel Committee on Banking Supervision (BCBS) : official website. – URL: https://www.bis.org/BCBS/ (дата обращения: 15.11.2020). – Текст : электронный.

81. Coderre, D. Computer-Aided Fraud Prevention and Detection: A Step-by-Step Guide / D. Coderre // Hoboken : J.Wiley & Sons, 2009. - 280 p. – URL:https://www.wiley.com/en-us/Computer+Aided+Fraud+Prevention+and+Detection3A+A+Step+by+Step+Guide-p-9780470392430 (дата обращения: 20.02.2023). – Текст : электронный.

82. Harchekar, J. Digitalization in Banking Sector / J. Harchekar // International Journal of Trend in Scientific Research and Development/ – Special Issue 2020. – P. 103-109. – ISSN: 2456-6470. – Текст : электронный. – URL: http://www.ijtsrd.com/papers/ijtsrd18681.pdf. (дата обращения: 20.02.2021).

83. Kang, J. Mobile payment in Fintech environment: trends, security challenges, and services / J. Kang // Human-centric Computing and Information Sciences. 2018. – ISSN 2192-1962. – Текст : электронный.
– DOI: 10.1186/s13673-018-0155-4. – URL: https://hcis-journal.springeropen.com/articles/ 10.1186/s13673-018-0155-4 (дата обращения: 20.02.2021).

84. Khalilzadeh, M. Risk identification and prioritization in banking projects of payment service provider companies: an empirical study / M. Khalilzadeh, L. Katoueizadeh, E. Kazimieras // Frontiers of Business Research in China. – Volume 14, 2020.– ISSN 1673-7431. – Текст : электронный. – DOI: 10.1186/s11782-020-00083-5. – URL: https://fbr.springeropen.com/articles/ 10.1186/s11782-020-00083-5 (дата обращения: 20.02.2021).

85. King, B. Bank 4.0: Banking everywhere, never at a Bank / B. King // Singapore: John Wiley & Sons Ltd/ – 2018. 352 p. – URL: https://www.wiley.com/en-us/Bank+4+0%3A+Banking+Everywhere%2C+Never+ at+a+ Bank-p-9781119506522 (дата обращения: 20.02.2023). – Текст : электронный.

86. Mallesha, C. Study on Trends in Digital Banking Sector / C. Mallesha, R. Reddy // International Journal for Research in Applied Science & Engineering Technology. – Volume 7, 2019. – P. 202-211. – ISSN: 2321-9653. – Текст : электронный. – DOI: 10.22214/ijraset.2019.10033 – URL: https:// www.ijraset.com/fileserve.php?FID=25275 (дата обращения: 20.02.2021).

87. Mashali, B. Development of E-banking channels and market share in developing countries / B. Mashali, A. Nazaritehrani // Financial Innovation. – Volume 6, 2020. – ISSN 2199-4730. – Текст : электронный. – DOI 10.1186/s40854-020-0171-z. – URL: https://jfin-swufe.springeropen.com/articles/ 10.1186/s40854-020-0171-z (дата обращения: 20.02.2021).

88. McMillan, J. The End of Banking: Money, Credit, and the Digital Revolution = Конец банковского дела: деньги, кредит и цифровая революция / J. McMillan // Independence press, 2014. – P. 56–80. – ISBN 978-3952438510.

89. Zhuming, Chen The transition from traditional banking to mobile internet finance: an organizational innovation perspective - a comparative study of Citibank and ICBC / Chen Zhuming, Li Yushan, Wu Yawen, Luo Junjun // Financial Innovation. – ISSN 2199-4730. – Текст : электронный. – DOI: 10.1186/s40854-017-0062-0. – URL: https://jfin-swufe.springeropen.com/ articles /10.1186/s40854-017-0062-0 (дата обращения: 20.02.2021).

Электронные ресурсы

90. Ассоциация Российских Банков : официальный сайт. – Москва, 2021. – URL: https://arb.ru/ (дата обращения: 24.02.2022). – Текст : электронный.

91. Группа Всемирного банка : официальный сайт. – Москва. – URL: https://www.vsemirnyjbank.org/ (дата обращения: 31.05.2021). – Текст : электронный.

92. Доклад для общественных консультаций Экосистемы: подходы к регулированию. Центральный банк Российской Федерации : официальный сайт. – Москва. – Текст : электронный. – URL: https://cbr.ru/Content /Document/File/119960/Consultation_Paper_02042021.pdf (дата обращения: 17.12.2021).

93. Московская биржа : официальный сайт. – Москва. – URL: https://www.moex.com/ (дата обращения: 16.02.2021). – Текст : электронный.

94. ПАО Сбербанк: официальный сайт. – Москва. – URL: https://www.sberbank.com/ (дата обращения: 31.05.2021). – Текст : электронный.

95. Портал информационного агентства «Хабр» : Киберстрахование на российском рынке. – Москва. – URL: https://habr.com/ru/company/cloud4y/blog/454278/ (дата обращения: 01.06.2022). – Текст : электронный.

96. Правительство Российской Федерации : официальный сайт. – Москва. – URL: http://government.ru (дата обращения: 19.02.2021). – Текст : электронный.

97. Рейтинговое агентство «Эксперт РА» : официальный сайт. – Москва. – URL: https://raexpert.ru/researches/credit_org/bank3/ (дата обращения: 16.02.2021). – Текст : электронный.

98. ТАСС : информационное агентство России : [сайт]. – Москва. – URL: http://tass.ru (дата обращения: 26.02.2021). – Текст : электронный.

99. Федеральная служба государственной статистики: официальный сайт. – Москва. – URL: https://rosstat.gov.ru/ (дата обращения: 19.02.2021). – Текст : электронный.

100. Финансовый супермаркет «Банки.ру» : официальный сайт. – Москва. – URL: https://www.banki.ru/wikibank/sistemnyiy_risk_bankovskogo_sektora/ (дата обращения: 19.02.2021). – Текст : электронный.

101. Центральный банк Российской Федерации : официальный сайт. – Москва. – URL: http://government.ru (дата обращения: 19.02.2021). – Текст : электронный.

102. Экосистемы: подходы к регулированию, 2021 // Доклад для общественных консультаций. – Москва. – Текст : электронный. – URL: https://cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf (дата обращения: 03.06.2022).

103. Positive Technologies : Актуальные киберугрозы: I квартал 2021 года. – Москва. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (дата обращения: 01.06.2022). – Текст : электронный.

104. PricewaterhouseCoopers : Insurance 2020 & beyond: Reaping the dividends of cyber resilience. – Москва. – URL: https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html (дата обращения: 02.06.2022). – Текст : электронный.

Приложение А

(информационное)

Расчёт концентрации банковской деятельности

				Февраль, 2022	Значение		Декабрь, 2019	Значение		Декабрь, 2017	Значение
			Доля 200 крупнейших по активам банков		99,69%	Доля 200 крупнейших по активам банков		99,58%	Доля 200 крупнейших по активам банков		99,47%
			Доля пяти крупнейших кредитных организаций		66,01%	Доля пяти крупнейших кредитных организаций		63,69%	Доля пяти крупнейших кредитных организаций		62,33%
	Показатель: Активы нетто		Индекс Херфиндаля – Хиршмана		1 452	Индекс Херфиндаля – Хиршмана		1 423	Индекс Херфиндаля – Хиршмана		1 414
Позиция в рейтинге	Название банка	Номер лицензии	Февраль, 2022, тыс. рублей	Доля банковского сектора,2022 В процентах	(MSi)^2 (2022)	Декабрь, 2019, тыс. рублей	Доля банковского сектора,2019 В процентах	(MSi)^2 (2019)	Декабрь, 2017, тыс. рублей	Доля банковского сектора,2017 В процентах	(MSi)^2 (2017)
1	СберБанк	1481	39 109 367 769,00	32,1799	1035,544	28 973 297 245,00	32,1308	1032,3863	23 633 271 356,00	33,0903	1094,9668
2	ВТБ	1000	19 825 106 187,00	16,3124	266,0957	14 483 875 051,00	16,0623	257,9978	9 353 664 727,00	13,0966	171,5208
3	Газпромбанк	354	8 934 718 940,00	7,3516	54,0466	6 614 267 527,00	7,3351	53,8034	5 613 397 081,00	7,8596	61,7739
4	Национальный Клиринговый Центр	3466	6 215 472 254,00	5,1142	26,155	3 669 008 617,00	4,0689	16,5556	3 213 300 548,00	4,4991	20,2421
5	Альфа-Банк	1326	6 141 402 076,00	5,0533	25,5354	3 687 383 320,00	4,0892	16,7218	2 699 694 089,00	3,78	14,2884
6	Россельхозбанк	3349	4 219 609 693,00	3,472	12,0546	3 297 821 385,00	3,6572	13,3752	3 117 836 187,00	4,3655	19,0572
7	Московский Кредитный Банк	1978	3 670 971 328,00	3,0205	9,1237	2 336 368 302,00	2,591	6,7132	1 884 617 801,00	2,6388	6,9631
8	Банк Открытие	2209	3 414 829 360,00	2,8098	7,8949	2 486 671 061,00	2,7577	7,6047	2 159 564 309,00	3,0237	9,1429
9	Совкомбанк	963	1 988 001 169,00	1,6358	2,6757	1 189 403 020,00	1,319	1,7398	697 561 010,00	0,9767	0,9539
10	Райффайзен Банк	3292	1 625 463 058,00	1,3375	1,7888	1 222 474 196,00	1,3557	1,8379	870 017 477,00	1,2182	1,4839
11	Росбанк	2272	1 572 439 546,00	1,2938	1,674	1 211 831 538,00	1,3439	1,8061	928 934 469,00	1,3007	1,6917
12	Тинькофф Банк	2673	1 269 767 136,00	1,0448	1,0916	562 700 458,00	0,624	0,3894	273 233 059,00	0,3826	0,1464
13	ЮниКредит Банк	1	1 224 676 668,00	1,0077	1,0154	1 417 952 803,00	1,5725	2,4727	1 172 446 752,00	1,6416	2,6949
14	Россия	328	1 212 197 343,00	0,9974	0,9948	1 026 998 192,00	1,1389	1,2971	805 820 426,00	1,1283	1,273
15	Всероссийский Банк Развития Регионов	3287	1 205 474 258,00	0,9919	0,9838	660 723 139,00	0,7327	0,5369	431 027 296,00	0,6035	0,3642
16	Траст	3279	1 114 536 931,00	0,9171	0,841	1 422 586 170,00	1,5776	2,4889	643 465 927,00	0,901	0,8117
17	Банк ДОМ.РФ	2312	869 059 991,00	0,7151	0,5113	299 968 986,00	0,3327	0,1107	335 514 006,00	0,4698	0,2207
18	Банк «Санкт-Петербург»	436	818 669 639,00	0,6736	0,4538	721 126 793,00	0,7997	0,6395	591 946 236,00	0,8288	0,6869
19	Ситибанк	2557	717 193 993,00	0,5901	0,3482	579 239 280,00	0,6424	0,4126	498 253 026,00	0,6976	0,4867
20	СМП Банк	3368	703 479 969,00	0,5788	0,3351	476 640 479,00	0,5286	0,2794	365 576 162,00	0,5119	0,262
21	Новикомбанк	2546	697 694 038,00	0,5741	0,3296	457 395 587,00	0,5072	0,2573	293 197 506,00	0,4105	0,1685
22	Ак Барс	2590	688 163 491,00	0,5662	0,3206	612 287 305,00	0,679	0,4611	444 969 319,00	0,623	0,3882
23	БМ-Банк	2748	630 054 957,00	0,5184	0,2688	507 431 766,00	0,5627	0,3167	612 422 850,00	0,8575	0,7353
24	Банк Уралсиб	2275	609 824 901,00	0,5018	0,2518	531 386 135,00	0,5893	0,3473	550 536 496,00	0,7708	0,5942
25	Почта Банк	650	565 377 606,00	0,4652	0,2164	514 203 228,00	0,5702	0,3252	234 319 922,00	0,3281	0,1076
26 - 358	////	////	////	////	////	////	////	////	////	////	////
359	Инэко	3520	100 470,00	0,0001	0	91 380,00	0,0001	0	21 653,00	0	0
			121 533 660 692,00			90 173 059 162,00			71 420 580 402,00		

Источник: составлено автором.

Рисунок А.1 – Расчёт концентрации банковской деятельности, произведённый в программе Excel

Приложение Б

(информационное)

Расчёт корреляции объема несанкционированных операций и объёма IT затрат банков

Период	Объем несанкционированных операций, тыс. руб.	Объем несанкционированных операций, в процентах к объёму IT затрат банков
41 729,00	315 200,00	0,13%
41 820,00	317 300,00	0,13%
41 912,00	459 400,00	0,18%
42 004,00	547 500,00	0,22%
42 094,00	612 600,00	0,18%
42 185,00	1 308 000,00	0,39%
42 277,00	2 031 900,00	0,61%
42 369,00	869 900,00	0,26%
42 460,00	605 700,00	0,18%
42 551,00	586 500,00	0,17%
42 643,00	722 600,00	0,21%
42 735,00	1 055 000,00	0,31%
42 825,00	651 800,00	0,16%
42 916,00	669 800,00	0,16%
43 008,00	569 400,00	0,14%
43 100,00	639 900,00	0,15%
43 190,00	636 700,00	0,15%
43 281,00	773 800,00	0,19%
43 373,00	756 200,00	0,18%
43 465,00	686 800,00	0,17%
43 555,00	1 328 000,00	0,31%
43 646,00	1 368 000,00	0,32%
43 738,00	1 901 770,00	0,45%
43 830,00	1 828 730,00	0,43%
43 921,00	1 830 299,50	0,40%
44 012,00	2 177 427,51	0,48%
44 104,00	2 716 549,83	0,60%
44 196,00	3 058 853,16	0,67%
44 286,00	2 873 356,49	0,56%
44 377,00	3 013 664,38	0,59%
44 469,00	3 206 473,23	0,62%
44 561,00	4 488 735,90	0,87%
44 651,00	3 294 160,94	0,60%
44 742,00	2 848 614,92	0,52%
44 834,00	3 973 456,54	0,72%

Период	Динамика IT-затрат российских банков, тыс. руб.	
2014	251 414 000,00	
2015	331 252 000,00	
2016	342 767 000,00	
2017	414 161 000,00	
2018	415 313 000,00	
2019	426 444 000,00	
2020	456 000 000,00	
2021	514 000 000,00	
2022	551 890 000,00	Прогноз

Коэффициент корреляции	0,7937

ВЫВОД ИТОГОВ

Регрессионная статистика	
Множественны	0,793668003
R-квадрат	0,629908898
Нормированн	0,618694016
Стандартная о	718766,3431
Наблюдения	35

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*ачимость F*
Регрессия	1	2,9E+13	2,9E+13	56,1672	1,3E-08
Остаток	33	1,7E+13	5,2E+11		
Итого	34	4,6E+13			

	Коэффициенты	*артная о татисти*	*-Значени*	*ижние 95*	*ерхние 95*	*ижние 95,*	*ерхние 95,0%*
Y-пересечени	-2769010,78	590728	-4,68745	4,6E-05	-3970857	-1567165	-3970857	-1567165,1
Переменная X	0,042532412	0,00568	7,49448	1,3E-08	0,03099	0,05408	0,03099	0,0540786

Источник: составлено автором.

Рисунок Б.1 – Расчёт корреляции объема несанкционированных операций и объёма IT затрат банков, произведённый в программе Excel

Приложение В

(информационное)

Прогноз объема несанкционированных операций

Временная шкала	Значения	Прогноз	Привязка низкой вероятности	Привязка высокой вероятности
31.03.2020	1 830 299,50			
30.06.2020	2 177 427,51			
30.09.2020	2 716 549,83			
31.12.2020	3 058 853,16			
31.03.2021	2 873 356,49			
30.06.2021	3 013 664,38			
30.09.2021	3 206 473,23			
31.12.2021	4 488 735,90			
31.03.2022	3 294 160,94			
30.06.2022	2 848 614,92			
30.09.2022	3 973 456,54	3 973 456,54	3 973 456,54	3 973 456,54
30.12.2022		3 778 037,30	3 661 769,79	4 666 553,63
30.03.2023		3 968 847,65	3 701 451,68	4 957 431,48
30.06.2023		4 148 591,48	3 741 133,57	5 349 572,51
30.09.2023		4 403 054,34	3 780 815,46	5 821 541,09
30.12.2023		4 700 566,53	3 820 497,35	6 357 452,19
30.03.2024		5 038 436,44	3 860 179,24	6 946 926,88
30.06.2024		5 652 672,47	3 899 861,14	7 583 116,93
30.09.2024		6 559 365,56	3 939 543,03	8 261 281,73
30.12.2024		7 299 419,45	3 979 224,92	8 977 961,41

Источник: составлено автором.

Рисунок В.1 – Расчёт прогноза объема несанкционированных операций, в тыс. руб., произведённый в программе Excel

Приложение Г

(информационное)

Динамика финансовой стабильности банковского сектора

	Объем несанкционированных операций, в процентах к объёму IT затрат банков				
31.03.2014	0,13				
30.06.2014	0,13	0,67%			
30.09.2014	0,18	0,447841			
31.12.2014	0,22	0,191772			
31.03.2015	0,18	-0,150773			
30.06.2015	0,39	1,135162			
30.09.2015	0,61	0,55344			
31.12.2015	0,26	-0,571879	0,16691	54,58043%	
31.03.2016	0,18	-0,327104	-0,15619	2,92110%	
30.06.2016	0,17	-0,031699	-0,17961	2,18791%	
30.09.2016	0,21	0,232055	-0,10242	11,18704%	
31.12.2016	0,31	0,460006	-0,02164	23,19789%	
31.03.2017	0,16	-0,488681	-0,07821	16,84863%	
30.06.2017	0,16	0,027616	0,11126	0,69961%	
30.09.2017	0,14	-0,149895	-0,04642	1,07076%	
31.12.2017	0,15	0,123815	-0,05267	3,11478%	
31.03.2018	0,15	-0,007761	-0,08377	0,57771%	
30.06.2018	0,19	0,215329	0,06112	2,37814%	
30.09.2018	0,18	-0,022745	0,16215	3,41870%	
31.12.2018	0,17	-0,091775	0,01201	1,07721%	
31.03.2019	0,31	0,883134	0,41907	21,53523%	32,16%
30.06.2019	0,32	0,03012	0,28883	6,69330%	26,31%
30.09.2019	0,45	0,390183	0,3844	0,00334%	25,91%
31.12.2019	0,43	-0,038406	0,21438	6,39033%	26,48%
31.03.2020	0,40	-0,064013	0,09974	2,68161%	25,31%
30.06.2020	0,48	0,189656	0,065	1,55397%	22,05%
30.09.2020	0,60	0,247596	0,01521	5,40030%	20,11%
31.12.2020	0,67	0,126007	0,15051	0,06003%	19,99%
31.03.2021	0,56	-0,16664	-0,01228	2,38260%	20,23%
30.06.2021	0,59	0,048831	0,0484	0,00002%	19,67%
30.09.2021	0,62	0,063978	0,03037	0,11292%	19,58%
31.12.2021	0,87	0,399898	0,15031	6,22962%	20,27%
31.03.2022	0,60	-0,316511	-0,03952	7,67266%	21,01%
30.06.2022	0,52	-0,135253	-0,07476	0,36596%	20,89%
30.09.2022	0,72	0,394873	0,14239	6,37462%	18,11%

Источник: составлено автором.

Рисунок Г.1 – Расчёт динамики финансовой стабильности банковского сектора, в зависимости от изменения объема несанкционированных операций, произведённый в программе Excel