МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

имени М.В. Ломоносова

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра предпринимательского права

Курсовая работа по теме:

«Правовые проблемы осуществления ИТ-аутсорсинга в банковской сфере»

Выполнил студент 310 группы

Рабаданов Рабадан Расулович

Научный руководитель

к.ю.н., доцент

Лаутс Елизавета Борисовна

Дата представления курсовой работы в учебный отдел:

«___»_____ 202__ г.

Дата сдачи научному руководителю: «___»_____ 202__ г.

Дата защиты курсовой работы: «___»_____ 202__ г.

Оценка: _____

Москва

2025 г.

Оглавление

Введение

На данный момент аутсорсинг, являясь крайне эффективной технологией менеджмента, набирает всю большую популярность среди принципов управления предприятиями в бурно развивающихся международных межфирменных связях[1]. Во многом, это обуславливается способностью упомянутого инструмента в минимизации издержек бизнеса и, как следствие, способствует высокой экономической целесообразности использования рассматриваемой конструкции. Почва же для развития данного института в комфортных для него условиях была только торпедирована цифровизацией современной экономики. И в своей работе я бы хотел многопланово и рельефно рассмотреть, как цифровизация трансформировала бизнес-процессы в одной из тех сфер, что выступает «важным элементом стратегической независимости России»[2] - банковской сфере. Концентрируясь при этом на функционировании института ИТ-аутсорсинга, особенностях его действующего правового регулирования, возможных направлениях модернизации банковского законодательства, регламентирующего само существование данной конструкции в РФ и многое другое.

Актуальность этого исследования заключается в том, что к настоящему моменту в мировой практике развитых государств сформировалась новая модель международного разделения труда и межфирменной кооперации, выраженная в форме аутсорсинга, который предоставляя компаниям возможность привлекать внешних исполнителей для реализации непрофильных процессов, позволяет осуществлять с большей эффективностью, экономичностью и профессионализмом периферийную деятельность организации. И в российских банковских реалиях аутсорсинговые услуги в сфере информационных технологий получили огромное распространение, за которым никак не поспевает

[1] Михнева С.Г., Маркеева Г.А. Технологии аутсорсинга как современный инструмент формирования бизнес-моделей: [Электронный ресурс] // Известия ВУЗов. Поволжский регион. Общественные науки. 2015. №1 (33). С. 239. URL: https://cyberleninka.ru/article/n/tehnologii-autsorsinga-kak-sovremennyy-instrument-formirovaniya-biznes-modeley. (дата обращения: 02.03.2025).

[2] Путин В.В. Выступление на заседании Совета безопасности. 2022.

законодатель, не установивший даже легального определения данного института, консервируя законопроект, посвященной подобному «использованию чужих ресурсов», оставляя его тем самым в т. н. «законодательной пробке». Тем временем всё расширяющие правовые проблемы, лакуны и коллизии, наличие практики и отсутствия законодательного урегулирования предоставления IT-аутсорсинга в банковской сфере не устраняют, а только способствуют потенциальной инфракции прав и свобод человека и законных интересов организаций.

Целью данной работы является выявление и анализ правовых проблем осуществления ИТ-аутсорсинга в банковской сфере, а также поиск путей их разрешения.

Для достижения цели исследования были поставлены следующие задачи: изучить природу аутсорсинговой модели как таковой и ее закрепление в российской правовой действительности, рассмотреть нормативную регламентацию и сферы ее применения в контексте ИТ, выявить потенциальные риски и средства управления ими, включая зарубежный опыт их регулирования, проследить наличествующие правовые пробелы, а также способы их преодоления и восполнения, проанализировать перспективы законодательного регулирования и страхования киберрисков в рамках ИТ-аутсорсинга.

Объектом данной работы выступает отечественный и зарубежный опыт банковского регулирования вопросов ИТ-аутсорсинга, мнения ученой среды, а также проект ФЗ, посвященный предмету исследования.

Предмет исследования: ИТ-аутсорсинг, применяемый субъектами БС РФ, как еще должным образом нормативно не зарегулированный институт банковского права, но при этом все активнее используемый кредитными организациями.

В работе использованы общенаучный диалектический метод, исторический, системный, формально-логический, сравнительно-правовой методы и метод анализа и синтеза.

Степень разработанности темы в правовой литературе можно оценить как среднюю. В российской юридической литературе существуют некоторые исследования, посвященных анализу различных аспектов правового регулирования ИТ-аутсорсинга в банковской сфере. Российские авторы обращают внимание на проблемы, касающиеся особенностей режима осуществления ИТ-аутсорсинга банковскими организациями. Эту проблематику рассматривали, в частности, Лаутс Е. Б., Шиткина И. С., Л.В. Санникова, А. Нурутдиновна, Л.Г. Кисурина, Харламова Е.Е., Коломасова Р.А., Брагинский М. И., Витрянский В. В., Махмудов Э.Э., Минева О.К., Михнева С.Г.

Представленная работа состоит из введения, трех глав и заключения. Главы выстроены в соответствии с принципом выведения частного из общего – сначала рассматривается более широкие или общие вопросы, а после исследуются специальные институты.

Глава 1. Природа аутсорсинга и его правовое регулирование в банковской сфере.

§1. Понятие и правовое закрепление аутсорсинга

Для того, чтобы наиболее полно рассмотреть регулирование аутсорсинговой модели в целом и в банковском секторе в частности, сначала необходимо представить общую концепцию изучаемой категории, находящуюся вне правовой плоскости и в большей степени циркулирующей вокруг управленческой и экономической систем, оседая при этом в самых различных бизнес-сферах.

Прежде всего стоит отметить, что современные управленческие парадигмы акцентируют внимание на преодолении одной из наиболее значимых проблем, характерных в наши дни, - ограниченности темпорального ресурса, который, обладая свойствами невосполнимости, создает необходимость в его оптимальном распределении с целью максимизации конкурентных преимуществ хозяйствующего субъекта. И здесь важно отметить, что значительный объем таких операционных процессов как бухучет, клининг, охрана и, например, обеспечение информационной инфраструктуры не относится к основным направлениям деятельности компании[1]. Данное обстоятельство снижает динамичность принятия стратегических и тактических решений, а также приводит к отвлечению ресурсов от развития ключевых компетенций и, как следствие, к утрате конкурентных позиций на рынке. Эмпирические данные, полученные в результате независимых исследований, свидетельствуют о том, что делегирование непрофильных функций специализированным внешним исполнителям позволяет сократить операционные издержки в среднем на 30% от совокупных затрат на их реализацию[2]. И в решения данного вопроса разумно обратиться к центральной категории данной курсовой работы – аутсорсинг.

---

[1] Минева О.К., Каширская Л.В. Нормативно-правовое обеспечение процесса аутсорсинга и аутстаффинга персонала: [Электронный ресурс] // Вестн. Том. гос. ун-та. 2018. №430. С. 188 URL: https://cyberleninka.ru/article/n/normativno-pravovoe-obespechenie-protsessa-autsorsinga-i-autstaffinga-personala. (дата обращения: 03.03.2025).

[2] Butterworth G., Kuchler M., S.Westdijk Outsourcing in Europe An in-depth review of drivers, risks and trends in the European outsourcing market. 2013. EYGM Limited. All Rights Reserved. P. 32.

С английского, «outsource - outside resource using» можно перевести как «использование чужих (внешних) ресурсов», что в целом и описывает всю суть данного инструмента[1]. Аутсорсинг состоит в передаче организацией некоторых своих функций и сфер деятельности, как правило, периферийных, на выполнение экстернальному и специализированному исполнителю подобных услуг.

При этом, анализируя данную конструкцию, следует иметь в виду ее многоаспектность. В научной литературе аутсорсинг рассматривается как многогранное явление, исследуемое в рамках экономической, управленческой и правовой наук. Кроме того, в ученой среде упоминаются и различные виды аутсорсинга, выделяемые в зависимости от характера передаваемых функций: производственный, бухгалтерский, кадровый (управление персоналом), логистический, IT-аутсорсинг, BPO[2], KPO[3]. Причем последние три разновидности называют даже триадой основных форм аутсорсинга[4], что, вполне вероятно, связано с тем, что почти любые аутсорсинговые услуги мы можем сегментировать на те, в которых депонируются знания, бизнес-процессы или информационные технологии. Однако, в рамках данной главы не представляется возможным децентрализация внимания на все аспекты и разновидности аутсорсинговой концепции, и, напротив, акцентуация взгляда на юридическую природу рассматриваемой нами категории и ее проявлении в банковском секторе не просто целесообразно, но и необходима. Прежде, чем перейти к этому, важно окончательно отметить все смысловые точки общей конструкции аутсорсинга, чтобы исключить всякую неясность в идентификации данного понятия среди других, на первый взгляд, схожих с ним.

В целях такой дифференциации сначала необходимо обратиться к системообразующим признакам изучаемой категории, конституирующим ее суть, так сказать. Если обычно достаточно взглянуть на дефиницию какого-либо

---

[1] Махмудов Э.Э. Аутсорсинг: достоинства и недостатки: [Электронный ресурс] // Science Time. 2016. №4 (28). С. 514 URL: https://cyberleninka.ru/article/n/autsorsing-dostoinstva-i-nedostatki. (дата обращения: 15.04.2025).
[2] BPO – business process outsourcing
[3] KPO – knowledge process outsourcing
[4] Михнева С.Г., Маркеева Г.А. Указ.соч. С. 239.

понятия, чтобы вычленить его основные черты и уловить его правовую природу, то в нашем случае легального определения аутсорсинга в РФ на данный момент нет, тогда как доктринальные воззрения ученых-правоведов значительно разнятся друг от друга[1]. Договор аутсорсинга, будучи возмездным по своей правовой природе, предполагает обязательство заказчика по оплате услуг, оказываемых исполнителем. При этом размер и порядок осуществления выплат определяются соглашением сторон и могут быть обусловлены как достижением конкретного результата, так и объемом фактически выполненных работ[2]. Здесь, кстати, можно отметить интересную особенность применения договора аутсорсинга в фиктивной форме, заключаемого с имплицитной целью уклонения от уплаты налогов, как это было, например, в деле № А07-30893/2022[3].

Исполнитель, действуя в рамках договора аутсорсинга, обладает значительной степенью автономии, используя собственные ресурсы, методологию и технологические решения для реализации переданных функций. Заказчик, в свою очередь, не вмешивается в оперативный процесс выполнения задач, ограничиваясь контролем за достижением оговоренных результатов[4]. Важнейшей характеристикой аутсорсинга является передача не единичных задач, а целостного комплекса функций или бизнес-процессов, что существенно отличает его от классических договорных конструкций, таких как подряд или возмездное оказание услуг, которые, как правило, ограничиваются выполнением конкретных работ или предоставлением отдельных услуг[5]. Данное обстоятельство подтверждается и позицией суда, в одной из решений которой было указано: «предмет договора аутсорсинга может включать в себя выполнение работ, оказание услуг, а в некоторых случаях и создание продукта»[6].

---

[1] Минева О.К., Каширская Л.В. Указ.соч. С. 189.
[2] Гражданское право: Учебник / Под ред. А. П. Сергеева, Ю. К. Толстого. Т. 2. М.: Проспект, 2020. С. 324.
[3] Постановление Арбитражного суда Уральского округа от 28 мая 2024 г. № Ф09-2735/24 по делу № А07-30893/2022 // Документ опубликован не был. СПС «КонсультантПлюс».
[4] Брагинский, М. И., Витрянский, В. В. Договорное право. Книга третья: Договоры о выполнении работ и оказании услуг. М.: Статут, 2011. С. 415.
[5] Егорова, М. А. Гражданско-правовые договоры: теория и практика. М.: Статут, 2018. С. 247.
[6] Апелляционное определение СК по гражданским делам Московского городского суда от 04 октября 2023 г. по делу N 33-41352/2023 // Документ опубликован не был. СПС «КонсультантПлюс».

Таким образом, аутсорсинг вне всяких сомнений обладает уникальными признаками, которые позволяют разграничить его от иных договорных инструментариев. Однако, как отмечалось раннее, в науке нет единого мнения по поводу правовой природы данного института, поэтому далее считаю необходимым рассмотреть эти контрадикторные друг другу воззрения на юридическую принадлежность аутсорсинговой конструкции тому или иному договорному типу, оформив и сведя их для упрощения восприятия в три основных подхода. Так, Л.Г. Кисурина в своей работе[1] предлагает концептуальное осмысление данного явления, акцентируя внимание на его содержательной близости к договору возмездного оказания услуг (далее ДВОУ), регламентированному нормами 39 главы ГК РФ[2], отражение чего можно найти и в судебной практики, допускающей рассмотрение аутсорсинговых отношений с призмы данной договорной конструкции[3]. Это сходство проявляется как в предмете договора, который заключается в выполнении определенных действий (услуг) в интересах заказчика, так и в возмездном характере возникающих обязательств, в силу чего разумно применять правила данного договора для восполнения пробелов в правовом регулировании рассматриваемых нами общественных отношений. При этом оба договора направлены на достижение схожих экономических целей — оптимизацию бизнес-процессов посредством привлечения внешних ресурсов за той разницей, что аутсорсинг предполагает более глубокую интеграцию исполнителя в процессы заказчика, что может включать не только выполнение отдельных задач и проектов, но и управление целыми функциональными направлениями деятельности организации на постоянной и устойчивой основе. В контексте дискуссии о правовой природе аутсорсинга как гражданско-правового института аналогичную позицию занимает и А. Нурутдиновна[4], однако, в монографии «Обязательства об оказании

[1] Кисурина Л.Г. Сложные сделки: учет, налоги и право // М.: «Экономика и жизнь», 2007. С. 239.
[2] «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 года № 14-ФЗ // Собрание законодательства Российской Федерации от 29 января 1996 г. № 5 ст. 410.
[3] Постановление Арбитражного суда Уральского округа от 1 ноября 2024 г. № Ф09-6252/24 по делу № А60-50442/2023 // Документ опубликован не был. СПС «КонсультантПлюс».
[4] Нурутдинова А. Заемный труд: особенности правового регулирования // Хозяйство и право. 2004. № 9. С. 22.

услуг в российском гражданском праве»[1] Л.В. Санникова выдвигает принципиально иную позицию, противопоставляя ее вышеупомянутому распространенному подходу, согласно которому аутсорсинг может быть квалифицирован в рамках (ДВОУ). Автор аргументированно критикует подобные попытки, указывая на их методологическую ошибочность и недостаточную обоснованность с точки зрения доктринальных и нормативных оснований гражданского права. Л.В. Санникова ставит в центр нашего внимания тот факт, что отношения, возникающие между организацией, предоставляющей специалистов определенного профиля и квалификации, и организацией-пользователем, носят безусловно гражданско-правовой характер, обуславливая это такими фундаментальными признаками, как имущественная природа данных отношений, их возникновение между самостоятельными и равноправными субъектами гражданского оборота, а также базирование на принципах автономии воли и свободы договора. Но несмотря на эти признаки, автор настаивает на том, что аутсорсинг не может быть сведен к классическому ДВОУ, предусмотренному главой 39 ГК РФ[2]. По мнению Л.В. Санниковой[3], специфика аутсорсинга заключается в его комплексном характере, который выходит за рамки простого оказания услуг. Аутсорсинг предполагает не только выполнение определенных действий (услуг), но и передачу части функций или процессов одной организации другой, что включает в себя элементы управления, координации и интеграции в бизнес-процессы заказчика. Такой подход, по мнению автора, не позволяет квалифицировать аутсорсинг в качестве поименованного ДВОУ, поскольку его содержание существенно шире и сложнее.

В связи с этим Л.В. Санникова предлагает рассматривать договор аутсорсинга как непоименованный договор, который, в соответствии с

---

[1] Санникова Л.В. Обязательства об оказании услуг в российском гражданском праве : дис. ... доктора юридических наук : 12.00.03 / Санникова Лариса Владимировна; [Место защиты: Ин-т государства и права РАН]. - Москва, 2007. – С. 98.

[2] «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 года № 14-ФЗ // Собрание законодательства Российской Федерации от 29 января 1996 г. № 5 ст. 410.

[3] Санникова Л.В. Указ. соч.

принципом свободы договора[1], может быть заключен сторонами в рамках гражданско-правовых отношений, даже если он прямо не предусмотрен законодательством, если при этом не вступает с ним в противоречие. Я нашел релевантную позицию суда и на данный доктринальный подход: «Договор аутсорсинга является договором, не поименованным в Гражданском кодексе Российской Федерации, поэтому стороны были свободны в определении его условий».[2] Такой договор, по мнению вышеупомянутого ученого-правоведа, следует относить к группе обязательств по совершению иных действий, что позволяет учитывать его уникальные особенности и обеспечивать гибкость в регулировании. Третья же трактовка природы договора аутсорсинга, которая больше всего мне близка, и, по сути, развивает мысль о непоименованном договоре, подводит нас к идее смешанного договора. Так, И.С. Шиткина в своей статье «Договор предоставления персонала: что это такое?»[3] выдвигает концепцию, согласно которой договор аутсорсинга следует квалифицировать как смешанный договор, сочетающий в себе элементы различных гражданско-правовых договоров, а также отдельные аспекты, присущие трудовым правоотношениям. Упомянутый автор акцентирует внимание на том, что правовая природа аутсорсинга не может быть сведена к какому-либо одному поименованному договору, предусмотренному ГК РФ. Вместо этого она предлагает рассматривать его как комплексный правовой феномен, который включает в себя элементы ДВОУ, договора подряда, а в некоторых случаях — даже трудового договора. Однако, в отличие от классического ДВОУ, аутсорсинг не предполагает, что аутсорсер берет на себя обязательства по выполнению конкретных работ или оказанию услуг в области управления, производства, строительства и т.п. Его обязательство ограничивается исключительно предоставлением персонала, соответствующего заранее согласованным

[1] «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 года № 14-ФЗ // Собрание законодательства Российской Федерации от 5 декабря 1994 г. № 32 ст. 3301.
[2] Постановление Двадцатого арбитражного апелляционного суда от 15 октября 2018 г. № 20АП-3216/18 // Документ опубликован не был. СПС «КонсультантПлюс».
[3] Шиткина И.С. Договор предоставления персонала: что это такое? // Хозяйство и право. 2004. №1. С. 99.

требованиям по квалификации, численности и иным параметрам. Автор особо подчеркивает, что смешанный характер договора аутсорсинга проявляется в его двойственной природе: с одной стороны, он регулирует гражданско-правовые отношения между организациями, а с другой - затрагивает трудовые аспекты, связанные с использованием предоставленного персонала. И.С. Шиткина обосновывает необходимость признания договора аутсорсинга непоименованным смешанным договором, который, в соответствии с принципом свободы договора (статья 421 ГК РФ[1]), может включать в себя элементы различных правовых институтов. Такой подход позволяет учитывать специфику аутсорсинга как гибкого инструмента экономического взаимодействия, который не укладывается в рамки традиционных договорных конструкций, но при этом соответствует общим принципам гражданского права. И.С. Шиткина также подчеркивает, что смешанный характер аутсорсинга требует тщательного правового регулирования, особенно в части разграничения гражданско-правовых и трудовых аспектов, чтобы избежать конфликтов и правовой неопределенности. Ее концепция способствует более глубокому пониманию аутсорсинга как самостоятельного правового явления, которое, хотя и не поименовано в ГК РФ, играет важную роль в современной предпринимательской практике. Например, в решении по делу N А41-50703/2[2] суд пришел к выводу, что на основе принципа свободы договора возможно возникновение аутсорсинговых отношений, оформляемых как смешанный, т. е содержаний элементы различных конструкций, предусмотренных законом и иными правовыми актами. Обобщая рассмотренные подходы, я могу констатировать, что в научной среде отсутствуют существенные разногласия относительно содержательной составляющей договора аутсорсинга, однако дискуссии о выборе оптимальной правовой формы для его оформления остаются актуальными. На мой взгляд, в условиях отсутствия четкого законодательного

[1] «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 года № 14-ФЗ // Собрание законодательства Российской Федерации от 5 декабря 1994 г. № 32 ст. 3301.
[2] Постановление Десятого арбитражного апелляционного суда от 27 марта 2025 г. № 10АП-2585/25 по делу № А41-50703/2021 // Документ опубликован не был. СПС «КонсультантПлюс».

регулирования аутсорсинга, вопросы соотношения его сущностных характеристик с поименованными или непоименованными договорными конструкциями, предусмотренными действующим законодательством, находятся в состоянии теоретической неопределенности, которая может быть устранена лишь посредством будущей легализации данного института. Правовая природа договора аутсорсинга остается предметом научных дискуссий, разрешение которых возможно исключительно через законодательное закрепление одного из существующих доктринальных подходов, при этом сущностно выбор того или иного подхода в нормативных предписаниях не может принести вреда или особенной пользой перед другими, оставшимися в научном забвении, так как содержательно ученые говорят об одном и том же явлении, облечь которое мы можем в то или иное название и типовую форму. В настоящее время, ввиду наличия правовых лакун и отсутствия официальной интерпретации сущности аутсорсинговых услуг, на практике допускается множественность вариантов реализации данных правоотношений, которые оформляются с использованием уже доступным субъектам гражданского оборота правовым инструментарием. Так, в целях реализации целей аутсорсинговых моделей применяются «например, договор поставки программного обеспечения и оборудования, договор возмездного оказания услуг для оформления аутсорсинга, договор аренды для использования элементов IT-инфраструктуры, договор на техническое обслуживание информационных и технических систем, договор о защите конфиденциальной информации и др.»[1]. Поэтому я считаю, что принятие решения, легализующего одну из договорных форм применения аутсорсинговый отношений, должно сопровождаться лишь устоявшейся предпринимательской практикой, которая сама выделит потребности и нужду в тех или иных правилах, присущих тому или иному договору, с которым бы фактические стороны аутсорсинга хотели бы сообразовать своё поведение.

[1] Лаутс Е.Б. Экспертно-аналитическое заключение по правовым основам организации функционирования рынка IT-аутсорсинга в банковской сфере. С. 5.

§2. Сферы применения ИТ-аутсорсинга в банковской сфере

Аутсорсинг, будучи крайне эффективным инструментом в увеличении КПД и уменьшении расходной части любого бизнеса, не мог остаться незамеченным банковской сферой, которая в условиях цифровой экономики неизбежно трансформируется и берет на вооружение рабочие аутсорсинговые модели, интегрируя их в свою повседневную деятельность, позволяя кредитным организациям концентрироваться на стратегических задачах, минимизируя вовлеченность в непрофильные процессы, что усиливает их адаптивность ко всякой динамике во внутренней среде и внешней конъюнктуре рынка. Экономически аутсорсинг снижает транзакционные издержки, открывает доступ лучшим практикам внешних провайдеров, новейшим технологиям и формирует пути для дополнительного дохода, так, банки, функционирующие как ПАО, могут улучшить свои финансовые показатели, такие, как например, удельный доход на подчиненного, что можно увеличить за счет сокращения сотрудников и передачи части функций на аутсорсинг[1]. Технически он повышает надежность услуг, обеспечивая гибкость масштабирования без значительных капиталовложений в кадры и инфраструктуру, что критически важно в нестабильной экономической среде[2]. Можно сказать, что аутсорсинг выступает не только как инструмент оптимизации затрат, но и как стратегический ресурс для повышения конкурентоспособности и устойчивости банковских структур в долгосрочной перспективе.

В контексте эволюции аутсорсинговых практик в банковском секторе, испытывающем значительное расширение спектра услуг, передаваемых внешним провайдерам, помимо традиционного аутсорсинга call-центров[3], который остается востребованным инструментом клиентского обслуживания, также передают на внешнее обслуживание такие направления, как разработка и

[1] Харламова Е.Е., Череватова А.С. Аутсорсинг в банковской сфере // Управление. Бизнес. Власть. №1 (10). 2016. С. 52.
[2] Бравар Ж. Л. Эффективный аутсорсинг: понимание, планирование и использование успешных аутсорсинговых отношений. - Москва, 2010. – С. 251.
[3] Харламова Е.Е., Череватова А.С. Указ. соч. С. 53.

поддержка веб-платформ, телекоммуникационные услуги, автоматизация бизнес-процессов, управление проектами и обеспечение информационной безопасности. Но особое внимание здесь заслуживает именно ИТ-аутсорсинг, который не только способствует снижению операционных издержек, но и обеспечивает доступ к передовым технологическим решениям, что становится критически важным в условиях растущей цифровизации финансовой отрасли.

ИТ-аутсорсинг представляет собой делегирование на договорной основе специализированному субъекту (третьему лицу) полного цикла функций, связанных с разработкой, модернизацией, вводом в эксплуатацию, сопровождением и выводом из эксплуатации информационных систем и их компонентов, включая средства защиты информации, а также обработку и хранение данных, при условии, что в отсутствие аутсорсинга эти функции реализовывались бы силами самой организации[1].

Этот вид аутсорсинга позволяет банкам сосредоточиться на стратегических задачах, делегируя техническую поддержку, разработку программного обеспечения и управление ИТ-инфраструктурой специализированным компаниям, выступая драйвером инновационного развития банковских институтов и центральным элементом современных аутсорсинговых стратегий в банковской сфере.

Так, например, в деле № А40-46729/2022 суд рассматривал деятельность АО «ЮНИС Лабе Солюшинз», являющуюся по сути ИТ-аутсорсером, установив среди основных направлений деятельности разработку и внедрение программного обеспечения, информационных систем и аналитических приложений, интеграцию приложений и сервисов в рамках ИТ-аутсорсинга для различных направлений и в т. ч. банковской, так среди ее клиентов в судебном решении указан ООО «Сетелем Банк» (нынешний «Драйв Клик Банк»)[2].

---

[1] Проект федерального закона № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/404786-8?ysclid=m9or9re2ur26153037.

[2] Постановление Девятого арбитражного апелляционного суда от 25 октября 2022 г. № 09АП-66459/22 по делу № А40-46729/2022 // Документ опубликован не был. СПС «КонсультантПлюс».

И в целом полагается разумным выделить несколько ключевых направлений, наиболее подверженных аутсорсинговой практики в сфере IT. Во-первых, передача на аутсорсинг функций, связанных с эксплуатацией технологической инфраструктуры, включая обслуживание вычислительных мощностей, поддержку телекоммуникационных систем и устройств самообслуживания, разработку и сопровождение специализированного банковского ПО.

При этом последнее связывается с обеспечением технического функционирования специализированного ПО, включая мобильные банковские приложения, системы аналитики больших данных и платформы дистанционного обслуживания клиентов, что, в свою очередь, позволяет сократить время вывода продуктов на рынок и минимизировать затраты на содержание внутренних команд разработчиков)

Данные процессы регламентируются как внутренними стандартами кредитных организаций, так и нормативными требованиями Банка России, в частности, стандартами, указаниями и положениями, устанавливающими особые условия для аутсорсинга критически важных IT-функций.

Такой технологический аутсорсинг позволяет банковским структурам избежать капиталоемких инвестиций в собственную ИТ-инфраструктуру, обеспечивая при этом необходимую масштабируемость и отказоустойчивость систем, что свидетельствует нам о высокой степени эффективности и полезности ИТ-аутсорсинга в банковском секторе, обуславливая актуальность и выгоду применения ИТ-аутсорсинга в данной сфере.

Аутсорсинг процесса обработки и хранения данных, включая использование внешних центров обработки данных и облачных сервисов становится все более популярной практикой в различных секторах экономики, где кредитные организации не становятся исключением. Однако, важно заметить, что этот аспект требует особого внимания с точки зрения соответствия

требованиям ФЗ «О персональных данных» № 152-ФЗ[1] и ФЗ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ[2], устанавливающим жесткие стандарты локализации данных и защиты информационных систем.

Поэтому в том числе особую значимость приобретает аутсорсинг функций обеспечения информационной безопасности, включая мониторинг киберугроз, защиту персональных данных и реализацию требований регуляторов. Данный вид аутсорсинга требует особых договорных конструкций, четко разграничивающих ответственность между кредитной организацией и подрядчиком, что особенно актуально в свете требований ФЗ «О безопасности критической информационной инфраструктуры» № 187-ФЗ[3], предписывающих банкам обеспечивать особую защиту ключевых информационных активов.

Но на мой взгляд, здесь стоит отметить, что современное правовое регулирование банковского ИТ-аутсорсинга в целом нуждается в дальнейшем совершенствовании, особенно в части разработки специализированных нормативных актов, учитывающих специфику передачи на аутсорсинг технологически сложных банковских процессов.

Поскольку по моему мнению требование создания сбалансированной правовой модели, которая, с одной стороны, обеспечит необходимую гибкость для развития инновационных технологий, а с другой - гарантирует защиту интересов всех участников финансового рынка, должна быть главенствующей целью законодателя в регулировании данного вопроса для того, чтобы наиболее продуктивным образом использовать все преимущества должным образом не закрепленной аутсорсинговой конструкции, но при этом сохранить и не навредить стабильности и безопасности БС РФ в части ее применения в инновационной сфере информационных технологий.

---

[1] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.

[3] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 (часть I) ст. 4736.

Но кроме всего, в конце хотелось бы вновь отметить, что мы можем отметить высокую роль и значимость ИТ-аутсорсинга в развитии деятельности банковских структур в России, где еще в 2015 году они занимали 14% всего объема аутсорсинговых услуг, сохраняя интенсивный рост данного направления «использования чужих ресурсов» в дальнейшем, что и обусловило пронизывание данной аутсорсинговой модели в современном цифровом банкинге России, являющимся одним из главных трендов банковского дела, на данный момент[1].

Таким образом, ИТ-аутсорсинг в банковской сфере представляет собой сложный, многогранный институт, сочетающий в себе элементы экономической оптимизации, технологической модернизации и, к сожалению, фрагментарного правового регулирования, тогда как его дальнейшее развитие будет определяться как потребностями банков в повышении операционной эффективности, так и функционированием и продвижением эволюционных механизмов регуляторных подходов, направленных на минимизацию сопутствующих рисков.

В этой связи исследование правовых аспектов аутсорсинговых отношений конкретно в банковской сфере, стабильность и эффективность которой критически важна для нормального протекания различных экономических процессов в государстве, сохраняет высокую актуальность, требуя при этом углубленного анализа как на доктринальном, так и на нормативном практическом уровнях.

Однако, кроме всего, депонирование критически значимых функций экстернальным исполнителям (подрядчикам) сопряжена с комплексом правовых, технологических и экономических рисков, требующих системного подхода к их регулированию и управлению, а также отдельной главы курсовой работы, посвященной этому вопросу, в которой будет возможно наиболее полно и рельефно рассмотреть особенности антикризисного управления ИТ-аутсорсинга в банковской сфере.

[1] Самочетова Н. В., Амосова Н. А. Цифровой банкинг как новое направление развития банковского дела // Экономика и социум. 2017. №3 (34). С. 1742.

Глава 2. Правовое обеспечение минимизации рисков использования ИТ-аутсорсинга в банковской деятельности

§1. Регуляторные требования управления рисками в ИТ-аутсорсинге

В условиях стремительной эволюции финансовых технологий в РФ правовые механизмы минимизации рисков, порождаемых «услугами, связанными с хранением, передачей и обработкой информации в соответствующих информационных системах и их компонентах, необходимыми для осуществления банковских операций, которые оказываются кредитным организациям специально привлеченными для этих целей третьими лицами»[1], приобретают особую актуальность, что и обуславливает научную и практическую значимость настоящего исследования. В соответствии с Положением Банка России от 8 апреля 2020 г. N 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[2], кредитные организации обязаны обеспечивать соответствие аутсорсинговых практик строгим стандартам информационной безопасности и непрерывности бизнес-процессов, при этом, встречая отсутствие единой доктринальной трактовки понятия «ИТ-аутсорсинг» и его легализации в российской правовой системе, несмотря на его косвенное упоминание в ФЗ «О национальной платежной системе» № 161-ФЗ[3] и ФЗ «О банках и банковской деятельности» № 395-1-ФЗ[4], создается база для формирования правовых лакун, повышающих риски злоупотреблений и киберугроз. Кроме того, международный опыт, а в частности, директивы ЕБРР[5] и Базельского комитета по банковскому надзору демонстрирует необходимость адаптации лучших практик риск-менеджмента к национальному правовому полю. И целью данной главы логично будет сделать формирование понимания

[1] Лаутс Е.Б. Экспертно-аналитическое заключение по правовым основам организации функционирования рынка IT-аутсорсинга в банковской сфере. С. 2

[2] Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» // «Вестник Банка России» от 2 июля 2020 г. № 51.

[3] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // Собрание законодательства Российской Федерации от 4 июля 2011 г. № 27 ст. 3872.

[4] Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. № 27 ст. 357.

[5] Европейский банк реконструкции и развития.

правового обеспечения минимизации рисков ИТ-аутсорсинга в банковской сфере через структуризацию рисков (правовых, операционных, репутационных) на основе классификаций Банка России, а также разделяемых в ученой среде, анализ регуляторных требований, изучение вопросов ответственности сторон аутсорсинговых отношений. Практическая значимость данных действий настоящего исследования заключается в возможности использования выводов Банком России при актуализации надзорных требований, кредитными организациями при построении систем комплаенса, а также законодателем при модернизации ГК РФ и иных ФЗ, регламентирующих отношения в изучаемой нами сфере. Таким образом, представленная глава направлена на формирование целостной правовой модели управления рисками ИТ-аутсорсинга, сочетающей баланс между гибкостью бизнес-процессов и соблюдением стабильности финансовой системы. Важно отметить, что в современной парадигме цифровой экономики привлечение сторонних провайдеров для реализации информационно-технологических функций представляет собой объективную необходимость, обусловленную требованиями экономической рациональности и оптимального распределения ресурсов. Данный подход получил широкое распространение в корпоративной практике как инструмент повышения операционной эффективности и обеспечения конкурентных преимуществ[1].

Технологии облачных вычислений формируют инновационную модель предоставления ИТ-услуг, позволяющую субъектам хозяйственной деятельности минимизировать капитальные затраты на создание собственной инфраструктуры. В рамках данной модели обеспечивается доступ к распределенным вычислительным мощностям, включая сетевые архитектуры и серверные комплексы, системы хранения и обработки данных, специализированное программное обеспечение. Вышеуказанные ресурсы предоставляются специализированными операторами на основе адаптивной сервисной модели, характеризующейся высокой степенью масштабируемости,

[1] Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375 (дата обращения: 20.03.2025).

оптимальным соотношением стоимости и производительности, гибкостью конфигурации под конкретные бизнес-задачи, возможностью оперативного перераспределения мощностей. Такая архитектура IT-обеспечения позволяет организациям концентрироваться на профильной деятельности, делегируя технологические функции профессиональным провайдерам услуг. Вместе с тем, реализация аутсорсинговых моделей в банковской сфере порождает не только очевидные конкурентные преимущества, но и формирует комплекс специфических факторов риска и регуляторных вызовов. Данные риски носят системный характер, проявляясь как на микроуровне в отдельных финансовых организациях, так и на макроуровне, посягая на стабильность всей БС РФ в целом. Банк России еще в 2022 году в своем докладе для общественных консультаций[1] отметил, что в независимости от того, является ли поставщик услуг сторонней организацией или входящим в одну банковскую группу с кредитной организацией-заказчиком, он продолжает рассматриваться как сторона аутсорсинговых отношений, деятельность которой порождает мультипликацию рисков, требующую должного управления и урегулирования. И в своей работе я бы хотел выделить несколько групп юридических угроз, которые освещаются в документах главного органа в сфере банковского надзора.

Первым ключевым риском является концентрация критической инфраструктуры у ограниченного круга провайдеров. Как отмечается в Докладе Банка России, использование услуг ограниченного числа поставщиков создает риск возникновения системных узких мест[2]. Эта проблема ярко проявилась в декабре 2021 года, когда сбой в работе облачного сервиса Amazon Web Services привел к масштабным перебоям в работе крупнейших онлайн-сервисов[3]. Стандарт ИББС в п. 10.3 рекомендует, чтобы организация обеспечивала возможность перевода критически важных процессов на собственные ресурсы

[1] Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375 (дата обращения: 20.03.2025).
[2] Там же.
[3] Сбой в работе облачного сервиса Amazon привел к отключению многих сайтов: [Электронный ресурс] // РБК. URL: https://www.rbc.ru/quote/news/short_article/61b05cf79a7947293b8bc9cf?ysclid=m9o2o8ip6x67408593 (дата обращения: 20.03.2025).

или ресурсы другого поставщика[1]. Для минимизации данного риска предлагается введение количественного ограничения на долю одного провайдера в ИТ-бюджете банка (не более 30%), что соответствует международной практике диверсификации поставщиков критически важных услуг.

Второй существенный риск связан с непрозрачностью цепочек субподряда. Многоуровневый аутсорсинг затрудняет контроль за качеством оказываемых услуг и соблюдением требований информационной безопасности. Яркой иллюстрацией этого риска стала утечка данных клиентов Альфа-Банка в марте 2020 года, произошедшая, предположительно, через компанию-субподрядчика, разрабатывавшую мобильное приложение для вышеупомянутой кредитной организации[2]. Стандарт ИББС в п. 6.6 взывает к тому, чтобы организация обеспечивала контроль за соблюдением требований информационной безопасности всеми участниками цепочки оказания услуг. В качестве правового механизма минимизации данного риска предлагается закрепить в ГК РФ принцип солидарной ответственности банка и провайдера за действия субподрядчиков по аналогии со ст. 403 ГК РФ.

Третья группа рисков связана с несоответствием комплаенс-требованиям при трансграничной передаче данных. Как указано в Докладе, использование иностранных поставщиков облачных услуг создает риски несоблюдения требований законодательства о локализации данных[3]. Стандарт ИББС в п. 6 говорит о необходимости наложения рестриктивных механизмов для передачи информации ограниченного доступа в информационные системы, расположенные за пределами Российской Федерации. Для решения этой проблемы предлагается введение системы обязательной сертификации облачных

---

[1] Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации: [Электронный ресурс] // Банк России. URL: https://cbr.ru/statichtml/file/59420/st-14-18.pdf (дата обращения: 20.03.2025).

[2] Масштабной утечкой в российском банке занялся ЦБ: [Электронный ресурс] // Lenta.ru. URL: https://lenta.ru/news/2020/07/28/alfa/?ysclid=m9o2ss3yth887249378 (дата обращения: 20.03.2025).

[3] Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375 (дата обращения: 20.03.2025).

провайдеров ЦБ РФ с публичным рейтингом их соответствия требованиям кибербезопасности.

Четвертым значимым риском является несоблюдение требований бесперебойности и доступности критически важных сервисов. Исходя из идейной сути стандарта ИББС организация должна обеспечивать доступность критически важных информационных систем при использовании услуг аутсорсинга. Однако на практике многие банки сталкиваются с проблемами обеспечения должного уровня SLA (Service Level Agreement)[1]. В 2015 году продолжительный сбой в работе процессингового центра одного из крупных аутсорсеров привел к нарушению работы 140 банков, клиенты которых не могли воспользоваться финансовыми услугами по переводу денежных средств и оплате товаров и услуг в течение 5 часов 20 минут[2]. Доклад Банка России[3] особо отмечает, что требования к времени восстановления критически важных систем должны быть согласованы с провайдером в обязательном порядке. Для минимизации данного риска предлагается введение обязательных требований к максимально допустимому времени простоя (RTO - Recovery Time Objective) для различных категорий систем (например, не более 15 минут для платежных систем), разработка типовых SLA-шаблонов для различных видов аутсорсинговых услуг и создание системы штрафных санкций за нарушение показателей доступности.

Пятый существенный риск связан с недостаточным контролем за изменениями в аутсорсинговых решениях. Проблема «теневых изменений» в аутсорсинговых решениях особенно актуальна в условиях использования SaaS-решений (облачных сервисов, предоставляемых внешними исполнителями для автоматизации банковских процессов, позволяющей использовать ПО без его локализации и самостоятельного обслуживания.). Неконтролируемые изменения

[1] SLA – это дополнение к соглашению об аутсорсинге между организацией БС РФ и поставщиком услуг, определяющее предоставление сервиса с заданным уровнем качества.
[2] Процессинг банковский карт UCS допустил рекордный сбой: [Электронный ресурс] // Spbitru. URL: https://spbit.ru/news/processing-bankovskih-kart-ucs-dopustil-rekordnyy-sboy-116466?ysclid=m9o2x1go57230463196 (дата обращения: 20.03.2025).
[3] Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375 (дата обращения: 20.03.2025).

в облачных сервисах могут привести к нарушению бизнес-процессов кредитной организации, поэтому, например, как указано в докладе, ЦБ Саудовской Аравии ввёл обязательную авторизацию – «предварительное разрешение регулятора перед передачей любых сведений в облако до подписания договора об аутсорсинге облачных сервисов»[1]. Упомянутый раннее пункт 10.3 Стандарта ИББС помимо всего говорит о том, чтобы все изменения в аутсорсинговых решениях согласовывались с банком-заказчиком. Для решения этой проблемы предлагается введение обязательного реестра изменений для критически важных аутсорсинговых решений, разработка механизма «заморозки» изменений в периоды высокой нагрузки (например, в конце отчетного периода) и создание тестовой системы для предварительной проверки всех обновлений.

Шестым заслуживающим внимание риском может послужить нарушение требований по защите персональных данных при использовании иностранных решений. Несмотря на требования ФЗ-152[2], многие банки продолжают сталкиваться с проблемами при использовании иностранных ИТ-решений. Так, в письме ФНС от 26 июня 2024 г. № 08-242780 указано, что «использование при обработке персональных данных пользователей интернет-ресурса с применением сервиса Google Analytics предполагает трансграничную передачу их персональных данных на территорию иностранного государства, в связи с чем оператору необходимо направить в адрес Роскомнадзора уведомление о намерении осуществлять трансграничную передачу персональных данных»[3] в соответствии с ч. 3 ст. 12 ФЗ №-152. Анализируя понимание банковского регулирования аутсорсинга, можно подчеркнуть, что использование иностранных ИТ-решений должно всегда сопровождаться дополнительными мерами по защите персональных данных[4]. Пункт 6.9 стандарта ИББС упоминает

[1] Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375 (дата обращения: 20.03.2025).
[2] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.
[3]Письмо Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 26 июня 2024 г. № 08-242780 «О результатах рассмотрения обращения» // Справочно-правовая система «Гарант». База данных «Законодательство».
[4] Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375 (дата обращения: 20.03.2025).

о важности проведения оценки соответствия иностранных решений требованиям российского законодательства, и для минимизации данного риска можно предложить создание реестра, так сказать, «проверенных» иностранных ИТ-решений, соответствующих требованиям российского законодательства, разработка методики оценки уровня защиты данных в иностранных решениях и введение обязательного шифрования всех данных, передаваемых в иностранные системы.

Проведенный анализ центральных групп рисков ИТ-аутсорсинга, на мой взгляд, демонстрирует необходимость комплексного подхода к их регулированию. Особое внимание следует уделить совершенствованию нормативной базы, в частности, разработке специализированного положения Банка России по управлению рисками аутсорсинга, созданию системы мониторинга и контроля за аутсорсинговыми сервисами, а также развитию отечественной ИТ-инфраструктуры как альтернативы иностранным решениям. Перспективным направлением дальнейших исследований может стать разработка системы раннего предупреждения рисков аутсорсинга на основе технологий искусственного интеллекта и машинного обучения. Помимо этого, суммируя выводы после прослеживания различных групп рисков, я бы отдельно вновь выделил, что юридическая угроза, порождаемая аутсорсингом информационных технологий, носят не просто операционный, но системно-трансграничный характер, затрагивая ключевые аспекты финансовой стабильности, информационной безопасности и суверенитета данных. В отличие от классических форм аутсорсинга (линейная ограниченная корреляция), ИТ-аутсорсинг формирует сетевую модель взаимозависимости, при которой сбой у одного провайдера может спровоцировать т. н. «каскадный эффект» в работе множества кредитных организаций. Этот факт требует переосмысления традиционных подходов к риск-менеджменту и перехода к превентивному регулированию в парадигме новой концепции регуляции не аутсорсинговых контрактов, но целых экосистем в сфере ИТ.

§2. Международный опыт управления рисками в ИТ-аутсорсинге

В условиях стремительной цифровизации финансовых услуг и глобализации технологических цепочек управление рисками ИТ-аутсорсинга становится одной из квинтэссенций обеспечения устойчивости всей банковской и финансовой систем в целом. И если в предыдущем параграфе были рассмотрены национальные регуляторные механизмы, то здесь мы попробуем провести анализ международного опыта, позволяющего выявить как универсальные принципы минимизации рисков, так и уникальные правовые решения, сформированные в ответ на вызовы, предъявляемые тем или иным правовым системам.

Так, особого внимания заслуживает проблема регуляторного арбитража, когда поставщики услуг сознательно выбирают юрисдикции с наиболее либеральными требованиями, создавая тем самым «серые» зоны ответственности. Европейский Союз, столкнувшись с этой угрозой после многочисленных отказов облачной инфраструктуры, разработал комплексный ответ в форме Директивы DORA (Digital Operational Resilience Act), вступившей в силу в этом году.

Данный нормативный акт вводит беспрецедентные по своей строгости требования, включая обязательство финансовых организаций обеспечивать надзорным органам прямой доступ к данным, обрабатываемым любым звеном аутсорсинговой цепочки, что фактически устраняет традиционные границы между регуляторными режимами различных стран.

Примечательно, что DORA устанавливает принцип пропорциональной ответственности, когда за нарушения со стороны аутсорсера санкции применяются одновременно и к поставщику, и к банку-заказчику, создавая тем самым мощный стимул для тщательного контроля за деятельностью контрагентов.

Не менее интересен опыт США, где регулирование строилось на сочетании жестких стандартов информационной безопасности и гибких рыночных механизмов. Gramm-Leach-Bliley Act (GLBA) – это ключевой американский

закон о финансовой модернизации 1999 года, а его Safeguards Rule представляет собой свод требований по защите конфиденциальной клиентской информации.

В рамках этого регулирования финансовые институты обязаны обеспечивать соответствие аутсорсеров стандартам NIST SP 800-53 (фундаментальный документ Национального института стандартов и технологий США, содержащий исчерпывающий перечень мер по защите информационных систем), требующие не просто формального соблюдения договорных обязательств, а глубокую интегрированность в устанавливаемые ими предписания во все аспекты взаимодействия с поставщиками услуг.

После масштабной кибератаки на SolarWinds в декабре 2020 году, когда злоумышленники через обновление программного обеспечения этой компании получили доступ к системам множества правительственных агентств и корпораций, включая банки, американские регуляторы осознали, что даже один ненадежный поставщик может поставить под угрозу всю финансовую систему[1]. В ответ на это они ввели концепцию «критически важных третьих сторон»[2] (Critical Third Parties, CTP) - особый статус, который присваивается компаниям, предоставляющим услуги, способные повлиять на работу множества банков одновременно.

Речь идет о таких поставщиках, как облачные провайдеры (AWS, Microsoft Azure), платежные системы или разработчики ключевого банковского ПО, поскольку если такой поставщик окажется уязвимым, это может вызвать цепную реакцию сбоев в десятках финансовых организаций.

Чтобы предотвратить подобные риски, FFIEC (Federal Financial Institutions Examination Council), объединение американских финансовых регуляторов, выпустил уточненные правила аутсорсинга (Outsourcing Guidance). Согласно этим правилам, банки должны проверять не только своих прямых подрядчиков, но и всех, кто стоит за ними в цепочке поставок, через процедуру

[1] SolarWinds SEC Filing, Form 8-K от 14.12.2020, С. 3-5.
[2] Interagency Guidance on Third-Party Relationships: Risk Management, С 32.

due diligence - комплексную проверку надежности контрагента[1]. Теперь под контролем находятся три уровня аутсорсинга: прямые исполнители (первый уровень), например, компания, разрабатывающая для банка мобильное приложение, субподрядчики - второй уровень, такие как облачный хостинг, на котором это приложение работает, если его наняла сама IT-компания, а не банк, а также поставщики третьего уровня и глубже, к примеру, сервис кибербезопасности, защищающий этот облачный хостинг.

Раньше банки часто не знали, кто именно обрабатывает их данные на втором или третьем уровне, но теперь FFIEC требует, чтобы банковские организации могли отслеживать всю цепочку и убедиться, что каждое звено соответствует стандартам безопасности.

Это особенно важно, потому что, например, если банк нанял компанию для разработки онлайн-банка, а та использует дешевый хостинг с уязвимостями, хакеры могут взломать не только этот хостинг, но и сам банк. Новые правила обязывают банк проверять и разработчика, и хостинг, и даже подрядчиков хостинга, если они имеют доступ к банковским данным, тем самым закрывая «слепые» зоны в аутсорсинге и заставляя банки глубже анализировать, кому они действительно доверяют свои технологии.

В отличие от западных моделей, азиатские регуляторы делают акцент на защите цифрового суверенитета, что проявляется в жестких ограничениях на трансграничную передачу данных и требованиях локального присутствия поставщиков критически важных услуг.

Гонконгский валютно-финансовый комитет, например, прямо запрещает хранение банковских данных за пределами специального административного района без явного разрешения надзорных органов[2], а саудовский SAMA (Saudi

[1] Customer Due Diligence Requirements for Financial Institutions: [Электронный ресурс] // URL: https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions (дата обращения: 24.03.2025).

[2] Pramodh Rai A Guide to Hong Kong Monetary Authority Outsourcing Regulations: [Электронный ресурс] // URL: https://cybersierra.co/blog/hong-kong-monetary-authority-outsourcing-regulations/ (дата обращения: 24.03.2025).

Arabian Monetary Authority) и вовсе требует физического присутствия ключевых аутсорсеров на территории королевства[1].

Подобные меры, хотя и могут рассматриваться как избыточные с точки зрения либеральной экономической модели, на практике доказали свою эффективность в условиях роста геополитической напряженности и технологического протекционизма[2].

Особую роль в формировании международных стандартов управления рисками в финансовом секторе играют такие документы, как PCI DSS (Международный отраслевой стандарт, обязательный для всех участников платежных систем: Visa, Mastercard и др., введенный для изолирования платежной среды от других IT-систем, а также защиты данных держателей карт) и ISO/IEC 27001 (добровольный международный стандарт по управлению ИБ), которые, несмотря на свой статус (ISO/IEC 27001 формально рекомендательный), фактически стали обязательными для любого серьезного участника рынка.

Требования о немедленном уведомлении при инцидентах, закрепленные в PCI DSS, или положения о регулярной отчетности по информационной безопасности из ISO 27001 в т. ч. создают универсальный язык взаимодействия между банками и поставщиками, гармонизируя различия национальных законодательств[3].

Синтезируя интернациональный опыт, можно выделить несколько ключевых направлений для совершенствования Российской правовой системы.

Во-первых, это внедрение механизмов сквозного надзора по аналогии с DORA, позволяющих регуляторам получать доступ ко всем звеньям аутсорсинговой цепочки.

---

[1] SAMA Third Party Compliance-How to Be Better Positioned as a Financial Institution: [Электронный ресурс] // URL: https://itbutler.sa/blog/sama-third-party-compliance-how-to-be-better-positioned-as-a-financial-institution/ (дата обращения: 24.03.2025).

[2] IMF «Regional Financial Regulation in Asia» (Working Paper WP/22/45, p. 12-14)

[3] Lifshits Ilya, Ponamorenko Vladislav. International financial standards in the global legal order and in EU and EAEU law // Russian Law Journal. 2020. №3. URL: https://cyberleninka.ru/article/n/international-financial-standards-in-the-global-legal-order-and-in-eu-and-eaeu-law (дата обращения: 18.03.2025).

Во-вторых, введение градации поставщиков по уровню критичности их услуг с дифференцированными требованиями к каждой категории.

В-третьих, ужесточение санкций за сокрытие инцидентов и нарушение сроков их раскрытия, т. к. подобные меры, сочетающие лучшие практики разных государств, позволят сформировать сбалансированную модель регулирования, которая, с одной стороны, не будет сковывать технологическое развитие, а с другой – надежно защитит банковскую систему от системных рисков, порождаемых недобросовестными или неподготовленными аутсорсерами.

В конечном счете, именно такой комплексный и адаптивный подход должен лечь в основу современной парадигмы управления рисками ИТ-аутсорсинга в банковской сфере РФ.

Но кроме этого, в данной главе я пришел к выводу о необходимости конвергенции международных стандартов и национального правопорядка в этой области, т. к. анализ регуляторных практик Базельского комитета, ЕБРР и зарубежных юрисдикций, включая крайне успешный опыт Саудовской Аравии в части авторизации облачных сервисов, свидетельствует о том, что российское законодательство нуждается в целенаправленной и регулируемой гармонизации с глобальными трендами в сфере правового поля действия ИТ-аутсорсинга, но с учетом специфики локализации данных и технологического суверенитета.

В частности, на мой взгляд, требует отдельного законодательного закрепления обязательная привязка к, так сказать, цифровому резидентству, чтобы размещение критической инфраструктуры и первичных серверов данных было необходимо и возможно исключительно на территории РФ.

Глава 3. Модернизация законодательства об ИТ-аутсорсинге в банковской сфере

§1. Правовые пробелы ИТ-аутсорсинга в области банковского законодательства

На данный момент банковская система РФ все больше вовлекает использование цифровых технологий в свою деятельность, что неизбежно сопровождается увеличением объема передаваемых функций на ИТ-аутсорсинг. Тем не менее, законодательство в этой области не просто не поспевает за бурно развивающейся отраслью банковского дела, а скорее продолжает находиться в атрофированном состоянии, отличаясь фрагментарностью и отсутствием единой концептуальной основы, порождая при этом существенные правовые лакуны, способные дестабилизировать функционирование финансовой системы.

Одной из важнейших проблем служит отсутствие легального закрепления дефиниций ИТ-аутсорсинга и облачных услуг, что приводит к терминологической неопределенности и разночтениям в правоприменительной практике. Законопроект № 404786-8 в ст. 1[1] прямо предусматривает введение юридических определений аутсорсинговых и облачных услуг, а также их поставщиков в федеральное законодательство, что позволит устранить коллизии в квалификации договорных отношений. В частности, судебные инстанции зачастую сводят сложные аутсорсинговые отношения к возмездному оказанию услуг в рамках главы 39 Гражданского кодекса[2], игнорируя их комплексную природу. Подобный подход создает предпосылки для некорректной квалификации договорных обязательств и злоупотреблений со стороны недобросовестных контрагентов.

Не менее острой проблемой выступает нормативная неупорядоченность правового статуса поставщиков ИТ-услуг, поскольку действующие

[1] Проект федерального закона № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/404786-8?ysclid=m9or9re2ur26153037.

[2] «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 года № 14-ФЗ // Собрание законодательства Российской Федерации от 29 января 1996 г. № 5 ст. 410.

нормативные акты не устанавливают единых критериев их надежности. Вышеупомянутый законопроект в статье четвертой вводит обязательную аккредитацию ИТ-аутсорсеров Банком России, включая требования к их финансовой устойчивости, уровню кибербезопасности и наличию лицензий на работу с банковскими данными.

В противном случае кредитные организации вынуждены самостоятельно проводить оценку потенциальных рисков, что увеличивает операционную нагрузку и создает дополнительные угрозы с одной стороны, а с другой – подрывает стабильность элемента финансовой системы, с той точки зрения, что подобная нормативная размытость положения поставщиков ИТ-услуг снижает стандарт поведения заказчика и лица, предоставляющего ИТ-услуги, не будучи связанным необходимыми, но нигде не закрепленными требованиями.

В связи с чем введение института обязательной аккредитации поставщиков со стороны Банка России могло бы стать эффективным механизмом в восполнении наличествующего пробела в регулировании ИТ-аутсорсинга.

Например, можно было бы ввести трёхуровневую аккредитацию провайдеров, перейдя на новый институциональный дизайн регуляторного мониторинга, где первый относится к критическим системам, требующий обязательное резидентство в РФ, высокий уровень капитала, ежеквартальный аудит Банка России, а также сертификацию ФСТЭК (Федеральная служба по техническому и экспортному контролю России - в IT-сфере указанная организация устанавливает правила для защиты информации на всех этапах от создания программ до эксплуатации сетей). Второй уровень бы касался вспомогательных сервисов, где необходимо была бы финансовая устойчивость в целом, соответствие ISO 27001 с выборочными проверками. Наконец третий уровень бы был связан с незначительными функциями, выполнение которых требовало бы простого соблюдения федерального законодательства, а действия сковывались уведомительным порядок совершения.

Особую сложность представляет правовая неопределённость трансграничного аутсорсинга, так, в соответствии сущностными предписаниями

рассматриваемого законопроекта, размещение критически важных банковских данных за пределами РФ допускается только в исключительных случаях с санкции ЦБ РФ, что прямо коррелирует с сущностными требованиями Федерального закона № 152-ФЗ «О персональных данных»[1] в части локализации данных, а также положений Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»[2]. В этой связи считаю необходимым законодательное закрепление прямого запрета на размещение критически важных банковских данных за пределами Российской Федерации, а также разработать механизмы контроля за деятельностью субподрядчиков, функционирующих в иностранных юрисдикциях, в целях снижения потенциальных ИТ-угроз, которые могут исходить, например, от недружественных государств.

Проблема «теневых изменений» в SaaS-решениях также находит отражение в законопроекте, шестая статья которого обязывает поставщиков вести реестр изменений критических систем и согласовывать обновления с банками-заказчиками, так сказать разрешительный порядок, обеспечивающий безопасность и стабильность всех структур ценой снижения динамичности совершения действий аутсорсеров.

Актуальный вопрос защиты банковской тайны решается введением в ст. 8 и 9 специального режима конфиденциальности для поставщиков услуг и их должностных лиц, деятельность которых связывают с требованиями Банка России, ФЗ-№115, а также санкционируют путем указания предписаний на привлечение к ответственности, установленной законодательством РФ, за разглашение конфиденциальной информации. Отсутствие же требований к резервированию инфраструктуры может быть восполнено нормами,

[1] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.
[2] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 (часть I) ст. 4736.

предписывающими обязательное дублирование критических систем и разработку планов аварийного восстановления.

Наконец, проблема гармонизации с международными стандартами (ISO 27001, PCI DSS) также частично решается положениями ст. 9, требующими от аутсорсеров соответствия признанным стандартам кибербезопасности.

Таким образом, законопроект № 404786-8[1] системно адресует все выявленные пробелы, предлагая: четкие юридические дефиниции, аккредитационную модель регулирования, меры контроля трансграничных операций, прозрачные механизмы ответственности. На мой взгляд это все необходимо иметь в нормативном регулировании, но претворяя это в правовую жизнь, следует помнить, что легальная дефиниция аутсорсинга должна отражать его комплексный характер, не игнорировать публично-правовую составляющую (требования Базеля, федеральное законодательство и регуляторные стандарты ЦБ РФ), а также отражать сетевую природу взаимодействия, то есть многоуровневые цепочки субподрядчиков. Вместе с этим институционально преобразовать действующее в правовое регулирование в то, что будет поистине способно обеспечить стабильность БС РФ с должной степенью эффективности. Помимо этого, возможно использование AI-мониторинга для более динамичного сопровождения аутсорсинговых решений на рынке, а также поднятие вопросов юрисдикционного контроля с экстерриториальным действием российских стандартов для субподрядчиков.

Кроме того, всегда, разумеется, следует иметь в виду, что его принятие потребует дополнительной проработки вопросов: баланса между безопасностью и «innovation-friendly» регулированием, адаптации малых банков к новым требованиям, создания инфраструктуры для надзора за аутсорсерами. Но в любом случае я считаю, что только комплексная, системная и последовательная

[1] Проект федерального закона № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/404786-8?ysclid=m9or9re2ur26153037.

реализация этих мер позволит обеспечить устойчивое основание и развитие ИТ-аутсорсинга в банковском секторе без ущерба для его финансовой стабильности.

§2. Перспективы законодательного регулирования и страхования киберрисков ИТ-аутсорсинга в банковской сфере

Не менее важной проблемой, требующей обращение нашего внимание на нее, является разработка продуктивных и результативных механизмов страхования киберрисков. В условиях роста числа кибератак и увеличения масштабов потенциального ущерба, покрытие рисков в этой области становится важным инструментом минимизации имущественных вреда и обеспечения устойчивости БС РФ. Однако, в РФ данный институт пребывает в стадии «зародыша», что обусловлено как отсутствием четкой нормативной базы, так и спецификой самих киберрисков, которые отличаются высокой динамичностью и сложностью прогнозирования.

Первое, на что стоит обратить внимание относительно развития страхования киберрисков в контексте ИТ-аутсорсинга – это формирование специализированных страховых продуктов, адаптированных под потребности банковского сектора, подобные решения должны учитывать не только прямые убытки, связанные с утечкой данных или нарушением работы информационных систем, но и косвенные последствия, включающие репутационные риски, штрафные санкции со стороны регуляторов и судебные издержки. «Основными мировыми компаниями, оказывающими услуги по страхованию от кибер-рисков являются: Lloyd’s of London, Zurich North America, AIG, Chubb»[1]. На международном рынке наличествует тенденция формирования синдикатов для страхования крупных киберрисков, что позволяет, во-первых, минимизировать финансовую нагрузку на отдельные страховые компании, а во-вторых, улучшить условия предоставления страховых продуктов для различных клиентов.

Значительным аспектом является также определение границ ответственности сторон аутсорсингового договора, что требует детальной проработки условий страхования и четкого разграничения рисков между банком

[1] Коломасова Р.А. Мировые тенденции страхования информационных рисков и проблемы его внедрения в российскую практику // E-Scio. 2019. №6 (33). URL: https://cyberleninka.ru/article/n/mirovye-tendentsii-strahovaniya-informatsionnyh-riskov-i-problemy-ego-vnedreniya-v-rossiyskuyu-praktiku (дата обращения: 19.03.2025).

и поставщиком услуг. Законодательное закрепление обязательных требований к страхованию киберрисков для кредитных организаций, использующих ИТ-аутсорсинг, могло бы стать следующим шагом в укреплении финансовой стабильности сектора. В качестве примера можно обратиться к опыту Европейского Союза, где Директива DORA предусматривает обязательное наличие страхового покрытия для критически важных ИТ-услуг (у нас именуются как существенные функции[1]). В РФ подобные меры могли бы быть реализованы через внесение соответствующих поправок в Федеральный закон № 395-1-ФЗ «О банках и банковской деятельности» или через нормативные акты Банка России. При этом важно обеспечить баланс между обязательными и добровольными механизмами страхования, чтобы не создавать избыточную нагрузку на участников рынка. Еще одним перспективным направлением является развитие рынка перестрахования киберрисков, что особенно актуально в условиях ограниченной емкости отечественного страхового рынка. Создание специализированных пулов или государственных гарантийных механизмов могло бы способствовать распределению рисков и повышению доступности страховых продуктов для малых и средних банков.

Особого внимания заслуживает вопрос стандартизации условий страхования и методик оценки киберрисков, которые уже включает в условия договоров страхования на практике, как это осуществляется СБЕРом[2]. В настоящее время отсутствуют единые подходы к определению размера страховых сумм, франшиз и критериев наступления страхового случая в рамках передачи функций кредитных организаций по ИТ-аутсорсингу, что создает почву для правовых споров. Разработка типовых договоров страхования, утвержденных Банком России, а также внедрение стандартизированных методик

[1] Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации: [Электронный ресурс] // Банк России. URL: https://cbr.ru/statichtml/file/59420/st-14-18.pdf (дата обращения: 26.03.2025).

[2] Решение Мценского районного суда Орловской области от 29 октября 2024 г. по делу № 2-1-894/2024 // Документ опубликован не был. СПС «КонсультантПлюс».

оценки рисков могли бы значительно повысить транспарентность и результативность данного института.

Наконец, важным аспектом является интеграция страхования киберрисков в систему управления рисками банковских организаций. Это предполагает не только заключение страховых договоров, но и регулярный мониторинг угроз, аудит защитных мер аутсорсеров и разработку планов реагирования на различные киберинциденты. Страхование должно стать частью комплексной стратегии кибербезопасности, дополняя технические и организационные меры защиты.

Суммируя все вышеизложенное, я бы сказал, что формирование результативной системы страхования киберрисков в банковском ИТ-аутсорсинге требует комплексной трансформации нормативно-правовых и рыночных механизмов, где краеугольным камнем должно стать законодательное закрепление в ФЗ «О банках и банковской деятельности» конкретных требований к страховому покрытию критически важных ИТ-услуг, включая установление параметров минимального обеспечения, принципов солидарной ответственности банков и аутсорсеров при киберинцидентах, а также четких критериев финансовой устойчивости специализированных страховщиков. Параллельно необходимо развивать специализированные страховые продукты, адаптированные к специфике цифровых рисков - модульные полисы, покрывающие как прямые убытки от системных сбоев и регуляторных санкций, так и косвенные последствия в виде репутационного ущерба, с применением динамических франшиз, коррелирующих с уровнем киберзащиты аутсорсера, и интеграцией страховых условий непосредственно в SLA-договоры. Институциональное же развитие страхового рынка должно идти по пути создания национального пула киберрисков под контролем ЦБ РФ, сочетающего механизмы государственных гарантий для системообразующих кредитных организаций с возможностями перестрахования в международных синдикатах. Принципиальное значение здесь также приобретает разработка единых стандартов оценки и управления рисками, включающих унифицированные

методики на базе адаптированных аналогов PCI DSS (международный стандарт безопасности данных платежных карт, разработанный для защиты от мошенничества и утечек PCI SSC (Payment Card Industry Security Standards Council), обязательный аудит ИТ-инфраструктуры аутсорсеров аккредитованными CERT-лабораториями (Computer Emergency Response Team - команда кибербезопасности, отвечающая на различные киберинциденты: атаки, утечки, вирусы), а также внедрение распределенных реестров для прозрачной фиксации страховых случаев.

Реализация такой модели превратит страхование из инструмента компенсации убытков в действенный механизм превентивного управления киберугрозами, где страховые премии становятся экономическим стимулом для внедрения международных стандартов информационной безопасности, показатели страхового покрытия - объективными индикаторами устойчивости для надзорных органов, а совокупный страховой потенциал рынка - элементом стратегического резервирования национальной финансовой системы. Этот подход органично вписывается в современную парадигму «регулируемой самоорганизации» цифровой экономики, обеспечивая оптимальный баланс между рыночными механизмами риск-менеджмента и государственным надзором за стабильностью критической банковской инфраструктуры.

На мой взгляд, исследование в этой области продемонстрировало необходимость законодательного регулирования и страхования киберрисков ИТ-аутсорсинга в банковской сфере посредством именно новой концептуальной модели страхования, так как в традиционной форме мы не сможем учесть все публично-правовые регуляторы, частноправовые механизмы и технические решения в покрытии рассматриваемых киберрисков. На макропруденциальном уровне ключевым моментом становится введение обязательного минимального покрытия для критически важных банковских функций по аналогии с вышеуказанными требованиями DORA, дополненное созданием национального пула киберрисков под управлением ЦБ РФ, который, в свою очередь, должен включать государственные гарантии для системно значимых организаций и

механизмы квази-перестрахования через международные финансовые институты. На уровне частного права особое значение приобретает разработка стандартизированных SLA-протоколов, предусматривающих динамические франшизы, автоматизированные выплаты при фиксации CERT-триггеров и использование смарт-контрактов для решения вопроса с убытками. Технологический сторона вопроса предполагает внедрение распределенных реестров для фиксации инцидентов, AI-актуариев для точной оценки рисков и обязательную сертификацию страховщиков по стандартам киберзащиты. Ключевыми инновациями могут послужить инструменты секьюритизации, такие как гибридные продукты, покрывающие не только прямые убытки, но и косвенные: регуляторные санкции, а также репутационные риски, оцениваемые через анализ соцсетей, например. Помимо этого, в контексте страхования киберрисков новым стандартом защиты данных, снижая риски утечек и кибератак, может стать квантовая криптография, которая теоретически не взламывается, так как обусловлена не вычислительной мощностью, а законами квантовой механики, Таким образом, предлагаемая концепция переосмыслит саму природу риска в цифровую эпоху, закладывая основы новой правовой рациональности, ориентированной на проактивное моделирование киберзащиты, а не реактивного регулирования.

Заключение

В ходе проведенного исследования были всесторонне рассмотрены правовые проблемы применения ИТ-аутсорсинга в банковской сфере, что позволило сформулировать ряд теоретических и практических выводов, а также предложить направления совершенствования законодательства в данной области.

ИТ-аутсорсинг, будучи сложным многоаспектным явлением, представляет собой передачу банком части своих технологических ИТ-функций внешнему исполнителю с целью оптимизации затрат и повышения эффективности бизнес-процессов. В работе обосновано, что правовое регулирование аутсорсинга в банковской сфере требует дифференцированного подхода, учитывающего как экономическую целесообразность, так и необходимость минимизации сопутствующих рисков для стабильности банковской системы в целом. Анализ российского законодательства позволил выявить фрагментарность нормативного закрепления аутсорсинговых отношений, что создает правовую неопределенность при заключении соответствующих договоров, в этой связи представляется необходимым уточнение понятийного аппарата, включая легальное определение ИТ-аутсорсинга, скрупулёзного закрепление особенностей и правил его осуществления. Особое внимание в исследовании уделено вопросам управления рисками, возникающими при передаче критически важных ИТ-функций третьим лицам, трансграничном и многоуровневом аутсорсинге, опасности нарушения охраняемой законом тайны и защиты персональных данных, а также многое другое. Изучение регуляторных требований национальных и международных практик позволило выделить ключевые направления минимизации рисков: обеспечение должного уровня информационной безопасности, контроль за качеством услуг аутсорсера, сохранение банком стратегического управления переданными процессами и т. д. Международный же опыт продемонстрировал тенденцию к ужесточению надзора за аутсорсингом в финансовом секторе, что выражается в введении обязательных стандартов Due Diligence, требований к локализации данных и

механизмов оперативного реагирования на инциденты. В российской практике подобные меры пока носят в основном рекомендательный характер, что повышает уязвимость кредитных организаций перед киберугрозами и нарушениями непрерывности бизнес-процессов. Важнейшим выводом работы является констатация наличия значительных правовых пробелов в регулировании ИТ-аутсорсинга в банковской сфере. В частности, требуют детализации вопросы распределения ответственности между банком и аутсорсером в случае утечки данных или сбоев в работе систем, а также механизмы страхования киберрисков. Автором изучен законопроект № 404786-8, телеологическим основанием которого и была попытка устранить фундаментальные проблемы в регулировании ИТ-аутсорсинга и создать рамки для будущего детализированного банковского регулирования данного направления. Нами также было обоснована необходимость разработки специализированного законодательного акта, который бы устанавливал: четкие критерии допустимости передачи тех или иных функций на аутсорсинг, обязательные требования к договорам ИТ-аутсорсинга, включая SLA, порядок взаимодействия с надзорными органами при использовании внешних поставщиков.

Перспективным направлением развития правового регулирования является также внедрение системы страхования киберрисков, связанных с аутсорсингом. В работе предложена новая концептуальная модель страхования, располагающая достаточными инструментами для покрытия киберрисков и предполагающая обязательное страхование ответственности аутсорсеров за нарушения информационной безопасности, что позволит банкам минимизировать финансовые потери в случае реализации угроз.

Таким образом, проведенное исследование позволило не только выявить ключевые правовые проблемы применения ИТ-аутсорсинга в банковской деятельности, но и предложить конкретные механизмы их решения на законодательном и практическом уровнях. Дальнейшее развитие данной темы может быть связано с углубленным изучением международных стандартов, а

также разработкой методик оценки эффективности аутсорсинговых моделей с учетом современных технологических вызовов. Иными словами, ИТ-аутсорсинг в банковской сфере – это не просто инструмент оптимизации, а тест на зрелость правовой системы в условиях цифровой революции, а его регулирование должно эволюционировать от «латания дыр» к проактивному моделированию правовых режимов, где гибкость бизнес-процессов сочетается с жесткостью киберзащиты, по-настоящему становясь новой юридической реальностью, где банковское право является «цифровым» по умолчанию.

Список использованных источников

I. Нормативно-правовые акты

1. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 года № 14-ФЗ // Собрание законодательства Российской Федерации от 5 декабря 1994 г. № 32 ст. 3301.
2. «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 года № 14-ФЗ // Собрание законодательства Российской Федерации от 29 января 1996 г. № 5 ст. 410.
3. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. № 27 ст. 357.
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.
5. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.
6. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // Собрание законодательства Российской Федерации от 4 июля 2011 г. № 27 ст. 3872.
7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 (часть I) ст. 4736.
8. Письмо Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 26 июня 2024 г. № 08-242780 «О результатах рассмотрения обращения» // Справочно-правовая система «Гарант». База данных «Законодательство».

9. Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» // «Вестник Банка России» от 2 июля 2020 г. № 51.
10. Проект федерального закона № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/404786-8?ysclid=m9or9re2ur26153037.

II. Учебники, комментарии и монографии

1. Гражданское право: Учебник / Под ред. А. П. Сергеева, Ю. К. Толстого. Т. 2. М.: Проспект, 2020. С. 324.

III. Научные статьи и диссертации

1. Бравар Ж. Л. Эффективный аутсорсинг: понимание, планирование и использование успешных аутсорсинговых отношений. - Москва, 2010.
2. Брагинский, М. И., Витрянский, В. В. Договорное право. Книга третья: Договоры о выполнении работ и оказании услуг. М.: Статут, 2011.
3. Егорова, М. А. Гражданско-правовые договоры: теория и практика. М.: Статут, 2018.
4. Кисурина Л.Г. Сложные сделки: учет, налоги и право // М.: «Экономика и жизнь», 2007.
5. Коломасова Р.А. Мировые тенденции страхования информационных рисков и проблемы его внедрения в российскую практику // E-Scio. 2019. №6 (33). URL: https://cyberleninka.ru/article/n/mirovye-tendentsii-strahovaniya-informatsionnyh-riskov-i-problemy-ego-vnedreniya-v-rossiyskuyu-praktiku.
6. Махмудов Э.Э. Аутсорсинг: достоинства и недостатки: [Электронный ресурс] // Science Time. 2016. №4 (28). URL: https://cyberleninka.ru/article/n/autsorsing-dostoinstva-i-nedostatki.
7. Минева О.К., Каширская Л.В. Нормативно-правовое обеспечение процесса аутсорсинга и аутстаффинга персонала: [Электронный ресурс] // Вестн. Том. гос. ун-та. 2018. №430. URL:

https://cyberleninka.ru/article/n/normativno-pravovoe-obespechenie-protsessa-autsorsinga-i-autstaffinga-personala.

8. Михнева С.Г., Маркеева Г.А. Технологии аутсорсинга как современный инструмент формирования бизнес-моделей: [Электронный ресурс] // Известия ВУЗов. Поволжский регион. Общественные науки. 2015. №1 (33). URL: https://cyberleninka.ru/article/n/tehnologii-autsorsinga-kak-sovremennyy-instrument-formirovaniya-biznes-modeley.
9. Нурутдинова А. Заемный труд: особенности правового регулирования // Хозяйство и право. 2004. № 9.
10. Самочетова Н. В., Амосова Н. А. Цифровой банкинг как новое направление развития банковского дела // Экономика и социум. 2017. №3 (34).
11. Санникова Л.В. Обязательства об оказании услуг в российском гражданском праве : дис. ... доктора юридических наук : 12.00.03 / Санникова Лариса Владимировна; [Место защиты: Ин-т государства и права РАН]. - Москва, 2007.
12. Харламова Е.Е., Череватова А.С. Аутсорсинг в банковской сфере // Управление. Бизнес. Власть. №1 (10). 2016. С. 52.
13. Шиткина И.С. Договор предоставления персонала: что это такое? // Хозяйство и право. 2004. №1.
14. Butterworth G., Kuchler M., S.Westdijk Outsourcing in Europe An in-depth review of drivers, risks and trends in the European outsourcing market. 2013. EYGM Limited. All Rights Reserved.

IV. Судебная практика:

1. Постановление Двадцатого арбитражного апелляционного суда от 15 октября 2018 г. № 20АП-3216/18 // Документ опубликован не был. СПС «КонсультантПлюс».
2. Постановление Девятого арбитражного апелляционного суда от 25 октября 2022 г. № 09АП-66459/22 по делу № А40-46729/2022 // Документ опубликован не был. СПС «КонсультантПлюс».

3. Постановление Десятого арбитражного апелляционного суда от 27 марта 2025 г. № 10АП-2585/25 по делу № А41-50703/2021 // Документ опубликован не был. СПС «КонсультантПлюс».
4. Апелляционное определение СК по гражданским делам Московского городского суда от 04 октября 2023 г. по делу N 33-41352/2023 // Документ опубликован не был. СПС «КонсультантПлюс».
5. Постановление Арбитражного суда Уральского округа от 28 мая 2024 г. № Ф09-2735/24 по делу № А07-30893/2022 // Документ опубликован не был. СПС «КонсультантПлюс».
6. Постановление Арбитражного суда Уральского округа от 1 ноября 2024 г. № Ф09-6252/24 по делу № А60-50442/2023 // Документ опубликован не был. СПС «КонсультантПлюс».
7. Решение Мценского районного суда Орловской области от 29 октября 2024 г. по делу N 2-1-894/2024 // Документ опубликован не был. СПС «КонсультантПлюс».

V. Иные источники

1. Лаутс Е.Б. Экспертно-аналитическое заключение по правовым основам организации функционирования рынка IT-аутсорсинга в банковской сфере.
2. Масштабной утечкой в российском банке занялся ЦБ: [Электронный ресурс] // Lenta.ru. URL: https://lenta.ru/news/2020/07/28/alfa/?ysclid=m9o2ss3yth887249378.
3. Процессинг банковский карт UCS допустил рекордный сбой: [Электронный ресурс] // Spbitru. URL: https://spbit.ru/news/processing-bankovskih-kart-ucs-dopustil-rekordnyy-sboy-116466?ysclid=m9o2x1go57230463196.
4. Путин В.В. Выступление на заседании Совета безопасности. 2022.
5. Сбой в работе облачного сервиса Amazon привел к отключению многих сайтов: [Электронный ресурс] // РБК. URL:

https://www.rbc.ru/quote/news/short_article/61b05cf79a7947293b8bc9cf?ysclid=m9o2o8ip6x67408593.

6. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации: [Электронный ресурс] // Банк России. URL: https://cbr.ru/statichtml/file/59420/st-14-18.pdf.
7. Управление рисками аутсорсинга на финансовом рынке: доклад Банка России: [Электронный ресурс] // Банк России. URL: https://cbr.ru/press/event/?id=14375.
8. Customer Due Diligence Requirements for Financial Institutions: [Электронный ресурс] // URL: https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions.
9. IMF «Regional Financial Regulation in Asia» (Working Paper WP/22/45).
10. Interagency Guidance on Third-Party Relationships: Risk Management.
11. Lifshits Ilya, Ponamorenko Vladislav. International financial standards in the global legal order and in EU and EAEU law // Russian Law Journal. 2020. №3. URL: https://cyberleninka.ru/article/n/international-financial-standards-in-the-global-legal-order-and-in-eu-and-eaeu-law.
12. Pramodh Rai A Guide to Hong Kong Monetary Authority Outsourcing Regulations: [Электронный ресурс] // URL: https://cybersierra.co/blog/hong-kong-monetary-authority-outsourcing-regulations/.
13. SAMA Third Party Compliance-How to Be Better Positioned as a Financial Institution: [Электронный ресурс] // URL: https://itbutler.sa/blog/sama-third-party-compliance-how-to-be-better-positioned-as-a-financial-institution/.
14. SolarWinds SEC Filing, Form 8-K от 14.12.2020.